

**Strategies for Unbridled Data  
Dissemination: An Emergency Operations  
Manual**

**Nikita Mazurov**

**PhD Thesis**

**Centre for Cultural Studies,  
Goldsmiths, University of London**

# Declaration

To the extent that this may make sense to the reader,

**I declare that the work presented in this thesis is my own.**

A handwritten signature in black ink that reads "Nikita" followed by a stylized flourish.

Nikita Mazurov

# Acknowledgements

The notion that the work in a thesis is ‘one’s own’ doesn’t seem quite right. This work has benefited from countless insights, critiques, commentary, feedback and all potential other manner of what is after all, *work*, by those who were subjected to either parts or the entirety of it during encounters both formal and informal. To say nothing of the fact that every citation is an acknowledgement of prior contributory work in its own right. I may have, however, mangled some or all of the fine input that I have received, for which I bear sole responsibility.

Certain images were copied from other publications for illustrative purposes. They have been referenced when such is the case.

Certain other images were provided by sources who will rename anonymous for reasons of safety.

Assistance with technical infrastructure in establishing a server for part of the project was provided by another anonymous source; anonymous for the same reason as above.

# Abstract

This project is a study of free data dissemination and impediments to it. Drawing upon post-structuralism, Actor Network Theory, Participatory Action Research, and theories of the political stakes of the posthuman by way of Stirnerian egoism and illegalism, the project uses a number of theoretical, technical and legal texts to develop a hacker methodology that emphasizes close analysis and disassembly of existent systems of content control. Specifically, two tiers of content control mechanisms are examined: a legal tier, as exemplified by Intellectual Property Rights in the form of copyright and copyleft licenses, and a technical tier in the form of audio, video and text-based watermarking technologies.

A series of demonstrative case studies are conducted to further highlight various means of content distribution restriction. A close reading of a copyright notice is performed in order to examine its internal contradictions. Examples of watermarking employed by academic e-book and journal publishers and film distributors are also examined and counter-forensic techniques for removing such watermarks are developed. The project finds that both legal and technical mechanisms for restricting the flow of content can be countervailed, which in turn leads to the development of different control mechanisms and in turn engenders another wave of evasion procedures. The undertaken methodological approach thus leads to the discovery of on-going mutation and adaptation of in-between states of resistance.

Finally, an analysis of various existent filesharing applications is performed, and a new Tor-based BitTorrent tracker is set up to strengthen the anonymization of established filesharing methods. It is found that there exist potential de-anonymization attacks against all analyzed file-sharing tools, with potentially more secure filesharing options also seeing less user adoption.

# Table of Contents

Cover .....	001
Declaration .....	002
Acknowledgements .....	003
Abstract.....	004
Table of Contents .....	005
Table of Tables .....	008
Table of Figures.....	009
Disclaimer of Liability .....	013
0. Introducing the Project: A Schematic Overview of the Operations Manual.....	014
0.0 Project Overview .....	015
0.1. Part I. Methodological Mobilization: Towards the Hacker Academic.....	017
0.2 Part II. Ordnance the First: Contraceptive Strategies for Data Liberation .....	020
0.3 Part III. Ordnance the Second: Emancipato-Surgical Strategies for Data Liberation .....	023
0.4 Part IV. Ordnance the Third: Distributive Strategies for Data Liberation .....	026
1. Methodological Mobilization: Towards the Hacker Academic .....	029
1.0 An overview of the ensuing method.....	030
1.1 Actor Network Theory: The Tunnel ( $\leftrightarrow$ ).....	030
1.2 Towards the Hack: A Critical Xylogy of Rogue Intellectualism .....	039
1.2.0 The Lizard on the Wire.....	039
1.2.1 Stirner: Humanism, Realism, Personalism .....	040
1.2.2 Gramsci: Traditional and Organic Intellectuals.....	042
1.2.3 Foucault: The Situated Intellectual.....	045
1.2.4 Kristeva: The Dissident Intellectual .....	047
1.2.5 On the Emergent Non-Legalism.....	049
1.3 Anonymous Subjectivity: The Hack as a Rejection of Statist Stasis.....	050
1.3.0 Monstrous Unions .....	050
1.3.1 Anonymous Unions .....	055
1.4 Participatory Action Research and Knowledge Propagation.....	057
1.4.0 Approximating PAR.....	057
1.4.1 Case Study 1: Goldsmiths Research Online (GRO).....	062
1.4.2 Case Study 2: Hacking Away at Twilynax Publishing.....	072

2. Ordinance the First: Contraceptive Strategies for Data Liberation .....	080
2.0 Did You See the ©?.....	081
2.1 The © is harder to ©.....	098
2.1.0 \$ floats in the © .....	104
2.1.1 V£R\$O.....	111
2.1.2 ©©.....	116
2.1.3 Free Software (‘free’ as in ‘not’).....	119
2.2 The CS Approach .....	126
2.3 Informational Illegalism (Anti Theory).....	128
2.4 Case Study 3: Informational Illegalism (Critical Praxis) — Unwatermarking Eestro	
eJournal Articles .....	132
3. Ordinance the Second: Emancipato-Surgical Strategies for Data Liberation.....	136
3.0 Cinema as Prison (CaP <sub>1</sub> ).....	140
3.1 Cinema as Prison (CaP <sub>2</sub> ).....	143
3.2 Cinema as Prison (CaP <sub>3</sub> ).....	151
3.3 Cinematic Watermarking as Post-Disciplinary Control .....	160
3.3.0 Soundtrack Modulation [AFM; L <sub>1</sub> ] .....	162
3.3.0.0 Case Study 4: Auditory Forensic Marker Neutralization .....	164
3.3.1 Secondary Location Tracking [AFM, VFM; L <sub>2</sub> ].....	166
3.3.2 Primary Location Tracking [VFM; L <sub>1</sub> ] .....	171
3.3.2.0 Case Study 5: Emancipato-Surgical Operation for Visual Forensic Marker	
Excision .....	175
4. Ordinance the Third: Distributive Strategies for Data Liberation .....	181
4.0 Islands in the Net .....	182
4.0.0 Layer Anonymity.....	184
4.0.1 Usenet .....	190
4.0.2 Internet Relay Chat (IRC).....	194
4.0.3 Cyberlockers .....	196
4.0.4 BitTorrent .....	199
4.0.5 Miscellaneous Services .....	202
4.0.6. F2F Systems .....	203

4.0.6.0. Freenet .....	206
4.0.7 Darknets.....	210
4.1 Cautionary Notes Regarding Theory and Data.....	212
4.1.0 On the Dangers of Theoretical Compartmentalization.....	212
4.1.1 An Ethnographic Crisis in Data Collection .....	216
4.2 Torrenting on Tor’s Onionland: An Empty Kitchen .....	219
4.2.0 Setting up a Tor-based BitTorrent Site.....	219
4.2.1 Factors Potentially Detrimental to User Adoption of the Torrent Tor Site .....	221
4.2.1.0 Technological ‘Barrier to Entry’ Factors.....	222
4.2.1.1 Personal Content Preference Factors .....	223
4.2.1.2 Privacy Factors .....	222
4.2.2. Concluding Remarks .....	230
5. Concluding Remarks: On the Copyright .....	232
5.0 Disjunctive Embedding .....	234
5.1 On-going Polymorphism .....	235
5.2 Non-Legalism .....	237
5.3 Future Implications.....	238
Appendix 1: Sample Procedure for Content Protection Removal from Twilynax eBooks.....	240
Appendix 2: Sample Procedure for Watermark Removal from Eestro eJournal Articles .....	257
Appendix 3: Sample Procedure for Cinematic Auditory Forensic Watermark Neutralization ...	274
Appendix 4: Examples of Cinematic Visual Forensic Watermarks in Select Film Frames .....	288
Appendix 5: Sample Emancipato-Surgical Operation for Visual Forensic Marker Excision .....	293
Appendix 6: Sample User Responses to Space Puppy Grotto Notice Postings .....	310
References .....	312
Audio .....	312
Software.....	312
Text.....	314
Video .....	354
Web.....	356

# Table of Tables

Table of Contents .....	005
Table of Tables.....	008
Table of Figures.....	009
<b>Table 3.0:</b> Disciplinary Characteristics of Cinema.....	152
<b>Table 3.1:</b> Theatrical Watermarking Potentiality Matrix.....	161
<b>Table A2.0:</b> eJournal Article Watermark Occurrence .....	245



# Table of Figures

<b>Figure 3.0</b> MPAA piracy reporting reward poster.....	154
<b>Figure 3.1</b> Secondary location-based audio watermarking schema .....	168
<b>Figure 3.2</b> Position estimation through secondary location-based visual watermarking .....	170
<b>Figure 3.3</b> Macrosegmentarity imposed on film print by a visual forensic watermarking schema .....	173
<b>Figure 3.4</b> Example of CAP-like visual watermarking.....	174
<b>Figure 3.5</b> Explication of visual forensic marker segmentation via horse overlay .....	175
<b>Figure A1.00.0</b> Twilynax homepage .....	229
<b>Figure A1.00.1</b> Primary Twilynax login screen.....	229
<b>Figure A1.00.2</b> Secondary Twilynax login screen .....	230
<b>Figure A1.00.3</b> Tertiary Twilynax login screen.....	230
<b>Figure A1.01.0</b> Search query results for a sample ebook selection.....	231
<b>Figure A1.02.0</b> Installation webpage for Httpfox .....	231
<b>Figure A1.02.1</b> HttpFox launch botton.....	231
<b>Figure A1.02.2</b> HttpFox start button.....	231
<b>Figure A1.03.0</b> Read online option for the sample ebook selection.....	232
<b>Figure A1.04.0</b> HttpFox log for the Twilynax online reader .....	232
<b>Figure A1.06.0</b> Firefox PDF viewer extended options panel.....	234
<b>Figure A1.07.0</b> Firefox Save window.....	234
<b>Figure A1.08.0</b> PDF merge password prompt, as seen in Adobe Acrobat 8 Professional ...	235
<b>Figure A1.09.0</b> Security Settings for a sample book page.....	236
<b>Figure A1.10.0</b> APDFPR content protection identification and removal.....	237
<b>Figure A1.12.0</b> Security Settings for a sample decrypted book page.....	238
<b>Figure A1.13.0</b> Acrobat Combine files menu .....	239
<b>Figure A1.14.0</b> Acrobat PDF Optimizer Discard Objects menu.....	240
<b>Figure A1.14.1</b> Acrobat PDF Optimizer Discard User Data menu .....	241
<b>Figure A1.15.0</b> HexEdit view of sample merged PDF e-book file showing date fields .....	242
<b>Figure A1.16.0</b> HexEdit view of sample merged PDF e-book file showing UUID fields ...	243

<b>Figure A2.00.0</b> Eestro homepage .....	247
<b>Figure A2.00.1</b> Primary Eestro login screen .....	247
<b>Figure A2.00.2</b> Secondary Eestro login screen .....	248
<b>Figure A2.00.3</b> Tertiary Eestro login screen .....	248
<b>Figure A2.01.0</b> Search query results for a sample DOI.....	249
<b>Figure A2.02.0</b> Firefox Save window.....	250
<b>Figure A2.03.0</b> briss page exclusion dialogue box.....	251
<b>Figure A2.03.1</b> briss PDF loading bar .....	251
<b>Figure A2.04.0</b> Eestro journal article loaded in briss .....	252
<b>Figure A2.05.0</b> briss Save window.....	253
<b>Figure A2.06.0</b> The initial, uncropped article page.....	254
<b>Figure A2.06.1</b> The briss-cropped article page .....	255
<b>Figure A2.06.2</b> Touch-Up Tool selection. ....	256
<b>Figure A2.06.3</b> Nondestructive crop reveal .....	257
<b>Figure A2.07.0</b> Adobe Acrobat Print window .....	258
<b>Figure A2.08.0</b> PDFCreator window with document metadata removed.....	259
<b>Figure A2.09.0</b> The TouchUp Object Tool reveals that there are no hidden objects.....	260
<b>Figure A3.01.0</b> New Avidemux (v. 2.6.0) window .....	263
<b>Figure A3.02.0</b> Avidemux (v. 2.6.0) File Open window .....	264
<b>Figure A3.02.1</b> Avidemux (v. 2.6.0) in the process of opening the sample file, Illegala.avi .....	264
<b>Figure A3.03.0</b> Avidemux Audio Track Selection window .....	265
<b>Figure A3.04.0</b> Avidemux Audio Track Save window .....	265
<b>Figure A3.04.1</b> Avidemux in the process of saving the audio track being extracted, Illegala_unmodified_track.mp3 .....	266
<b>Figure A3.05.0</b> Raven Lite Open Sound Files window.....	266
<b>Figure A3.05.1</b> Raven Lite spectrogram for the file Illegala_unmodified_track.mp3. ....	267
<b>Figure A3.05.2</b> Raven Lite spectrogram for the file Illegala_unmodified_track.mp3, with suspect blocks highlighted. ....	267
<b>Figure A3.06.0</b> GoldWave Open Sound window.....	268
<b>Figure A3.06.1</b> GoldWave in the process of opening the file Illegala_unmodified_track.mp3 .....	268


<b>Figure A3.07.0</b> GoldWave Lowpass Filter settings window .....	269
<b>Figure A3.08.0</b> GoldWave Save Sound As window .....	269
<b>Figure A3.09.0</b> Raven Lite spectrogram for the file Illegala_modified_track.mp3 .....	270
<b>Figure A3.10.0</b> The file Illegala_modified_track.mp3 opened in VLC media player for playback analysis.....	270
<b>Figure A3.11.0</b> Avidemux Audio Tracks Configuration window, showing the Track drop-down menu.....	271
<b>Figure A3.12.0</b> Avidemux Audio Tracks Configuration window, showing the modified audio track replacing the original track. ....	271
<b>Figure A3.13.0</b> Main Avidemux panel .....	272
<b>Figure A3.13.1</b> Avidemux (v. 2.6.0) Select File to Save window .....	273
<b>Figure A3.13.2</b> Avidemux (v. 2.6.0) Encoding... window.....	273
<b>Figure A3.13.3</b> Avidemux (v. 2.6.0) Save process completion notification window. ....	274
<b>Figure A4.0</b> Primary example of visual forensic markers in a scattershot array .....	275
<b>Figure A4.1</b> Secondary example of visual forensic markers in a scattershot array .....	275
<b>Figure A4.2</b> Tertiary example of visual forensic markers in a scattershot array .....	276
<b>Figure A4.3</b> Quaternary example of visual forensic markers in a scattershot array .....	276
<b>Figure A4.4</b> Primary example of ‘thin’ visual forensic markers in scattershot array .....	277
<b>Figure A4.5</b> Primary example of visual forensic markers in a hybrid linear and scattershot array .....	277
<b>Figure A4.6</b> Secondary example of visual forensic markers in a hybrid linear and scattershot array.....	278
<b>Figure A4.7</b> Primary example of visual forensic markers in a ‘T’ array.....	278
<b>Figure A4.8</b> Secondary example of visual forensic markers in a ‘T’ array.....	279
<b>Figure A4.9</b> Primary example of visual forensic markers in a turned-L (‘ <b>T</b> ’) array .....	279
<b>Figure A5.00.0</b> Modified miniature tripod clip, for attaching the camcorder to the seat in front of the cammer .....	282
<b>Figure A5.02.0</b> New Avidemux (v. 2.5.6) window.....	283
<b>Figure A5.03.0</b> Avidemux (v. 2.5.6) File Open window.....	284
<b>Figure A5.03.1</b> Avidemux (v. 2.5.6) in the process of opening the sample file, Illegala.avi .....	284

<b>Figure A5.03.2</b> Illegala.avi opened in Avidemux .....	285
<b>Figure A5.04.0</b> Avidemux Save menu.....	286
<b>Figure A5.04.1</b> Avidemux Select JPEG Sequence to Save Save window.....	286
<b>Figure A5.04.2</b> Avidemux Saving as set of jpegs progress bar .....	287
<b>Figure A5.04.3</b> Avidemux Save completion window .....	287
<b>Figure A5.05.0</b> Sample watermark pattern template (template1.png) .....	288
<b>Figure A5.06.0</b> New imgSeek window.....	289
<b>Figure A5.07.0</b> imgSeek Add images window .....	290
<b>Figure A5.08.0</b> imgSeek Search by Image content window .....	291
<b>Figure A5.10.0</b> The file Illegalai.avi opened in VLC media player for playback analysis ..	292
<b>Figure A5.11.0</b> Avidmeux frame deletion .....	293
<b>Figure A5.12.0</b> Avidemux Video Filter Manager .....	294
<b>Figure A5.13.0</b> Avidemux (v. 2.5.6) Select File to Save window .....	295
<b>Figure A5.13.1</b> Avidemux (v. 2.5.6) Encoding... window.....	296
<b>Figure A5.13.2</b> Avidemux (v. 2.5.6) Save process completion notification window .....	296

## Disclaimer of Liability

The procedures outlined herein in the following project are not enacted realities, but rather purely potent potentialities. The locations, events, and, but not necessarily limited to, objects depicted in said appendices are fictional. Any similarity to actual locations, events, and, but not necessarily limited to, objects, past or present, is purely coincidental.

The use of any particular tense, style, or of any other literary mode is not intended to portray, depict, or otherwise (re)present instruction. The writer of the text herein is not responsible for any actions of the reader and is indemnified against any damages resulting thereof.

Certain images have been redacted via the deployment of redaction bars (e.g., ) and certain Uniform Resource Identifiers (URIs), including, but not necessarily limited to, certain Uniform Resource Locators (URLs) and Document Object Identifiers (DOIs) have been redacted via the deployment of asterisks (e.g., [http://\\*\\*\\*.\\*](http://***.*)) to further dissuade mis-(unintentional)/dis-(intentional) identification of the examples used herein with actual existent locations, events, and, but not necessarily limited to, objects. Certain textual citations, including titles and quotations, have further been augmented to dissuade misidentification with existent materials.

However, it must be noted that while said redaction conversely also has the opposite effect of rendering the obfuscated content similar to other content (e.g. other redacted documents or artworks (e.g., Kazimir Malevich, *Black Square*, 1915; Jenny Holzer, *Endgame*, 2011), the effect is unintentional. Thus highlighting that no matter the preventive action, representation and similarity can thus apparently not be avoided, and as such, such is not the fault of the writer.

Unredacted versions may be provided, if available, following the signed agreement by all involved parties of a legally-binding indemnity agreement by the requesting party. Any accrued fees for the retaining of legal counsel to procure such an agreement are to be handled by the party requesting said unredacted versions.

**0.**

**Introducing the Project:**

**A Schematic Overview of the Operations  
Manual**

The overarching aim of this dissertation is a critical interrogation of the potentialities of unbridled data dissemination. In other words, how can information move about most freely? In order to begin to answer the operant question however, it first becomes necessary to bring to the fore the various fetters which seek to corral and congeal information, to highlight the various impediments which stifle the free flow of content in favor of strictly regulated distribution channels, and—once these restraints are exposed—to then present methods for the removal of said informational shackles. Conceived of as an emergency operations manual, the dissertation highlighting the pressing saliency of the undertaken research—as evinced through the on-going congealment of information flows brought about by Intellectual Property Rights (IPR) machinations—whilst also presenting clearly delineated potential strategies of data liberation, illustrating the embodied praxis of information dissemination via the erosion of various ideological and technical fetters—coagulants which seek congeal cultural production and to inhibit the free flow of data transmission.

## **0.0 Project Overview**

Towards these ends then, the first chapter of the manual explicates the theoretical and methodological foundations and innovations which underpin the undertaken research. Specifically, the influences and relevancies of Science and Technology Studies (or Science, Technology, Society), and more specifically, Actor Network Theory (ANT); a genealogy of various conceptualizations of the critically-engaged figure of ‘the intellectual’; Stirnerian and post-human formulizations of the ego; and finally, Participatory Action Theory will all be discussed in relation to the development of an underlying hacker methodology which permeates the entirety of the manual.

The second chapter, presenting contraceptive strategies for data liberation, will address the juridical and syntactic modes of informational oppression; viz. Intellectual Property Rights. Specifically, the concern here is not predominantly with copyright, criticisms of which have already been abundantly presented in existent literature<sup>1</sup>, but with

---

<sup>1</sup> E.g., Dale Bradley. 2004. “Open Source, Anarchy, and the Utopian Impulse”, in *M/C: A Journal of Media and Culture*, 7 (4). [http://www.media-culture.org.au/0406/03\\_Bradley.php](http://www.media-culture.org.au/0406/03_Bradley.php); Critical Art Ensemble. 2000. “The Financial Advantages of Anti-Copyright”, in *Digital Resistance: Explorations in Tactical Media*. New York: Autonomedia. pp. 148-152.; Lawrence Lessig. 2001. *The Future of Ideas: The Fate of the Commons in a Connected World*. New York: Random House; Lawrence Lessig. 2004. *Free Culture: How Big Media Uses Technology and The Law to Lock Down Culture and Control Creativity*. New York: The Penguin Press; Lawrence Lessig. 2006. *Code: And Other Laws of Cyberspace*. Version 2.0. New York: Basic Books; Kembrew McLeod. 2005. *Freedom of Expression: Resistance and Repression in the Age of Intellectual Property*. New York: Doubleday; Matt Mason. 2008a. *The Pirate’s Dilemma: How Youth Culture is Reinventing Capitalism*. London: Free Press; Brian Martin. 1998. *Information Liberation*. London: Freedom Press; Eben Moglen. 2003. “The dotCommunist Manifesto”. [http://emoglen.law.columbia.edu/my\\_pubs/dcm.html](http://emoglen.law.columbia.edu/my_pubs/dcm.html); Richard M. Stallman.

the snake in the grass known broadly as copyleft—which through its operant deception of ostensibly being against draconian copyright legislation and enforcement in fact poses a much more serious threat to unbridled information promulgation than that posed by traditional copyright. That is to say, it will be argued that by presenting itself as being a viable, affable alternative to copyright but not challenging the core notions of intellectual property ownership and instead merely offering a reformism of allowance, copyleft thus greatly endangers unfettered data distribution. Engaging with said modes of oppression, the manual will then present contraceptive strategies for combating informational congealment through the preemption of the creation of said fetters: an utter eschewal of all modes of content licensure, a strategy which will attempt to prevent the very conception of IPR fetters.

The third chapter of the manual will then go on to present surgico-emancipatory strategies for removing technical shackles placed on existent cultural artifacts through a case study of the film as prisoner and focuses on the exposition, and subsequent removal of, various modes of watermarking film which allow so-called ‘content owners’ to track the originating pirates, or content liberators. Whilst contraceptive strategies deal with undoing notions of licensure in the first place, and thus preventing a congealed Body of Work (BoW) from being constructed in the first place, emancipato-surgical strategies engage an already-existent BoW by focusing on developing means of removing any present content restriction shackles by way of counter-forensic operations such as watermark removal. The resultant nomenclature is thus based on the fact that the strategies are coded as being emancipatory—freeing formerly congealed cultural products—and surgical, due to the precise operations which need to be enacted upon the Body of Work to extract content controller-implemented malignancies.

Through the aforementioned critical discussions/destructions of so-called intellectual property and watermarking technologies, the manual then paves the way for, finally, distributive strategies of information dispersal: how to distribute the now-liberated data without fear of reprisal from scorned content oppressors. The manual will conclude with a critical appraisal of existent and developing anonymized and encrypted content sharing platforms.

---

2002. *Free Software, Free Society: Selected Essays of Richard M. Stallman*. Boston: GNU Press; Ted Striplas. 2006. “Disowning Commodities: Ebooks, Capitalism, and Intellectual Property Law”, in *Television and New Media* 7 (3), pp. 231-260; Siva Vaidhyanathan. 2001. *Copyrights and Copywrongs: The Rise of Intellectual Property and How It Threatens Creativity*. New York: New York University Press; etc....



Having thus broadly explicated the aims of the project, let us now take a closer schematic look at the operations manual.

### **0.1. Part I. Methodological Mobilization: Towards the Hacker Academic**

The underlying thread running throughout the first chapter on methodological mobilization will be the development of a hacker methodology marked by an emphasis on an embedded and decentralized imperceptibility characterized by an on-going polymorphism, hyper and deep specialization, and a pervasive non-legalism in regard various deployed methods of engagement. The applicability of ANT will be discussed via its espousal of the relevancy of non-human actants, but more significantly via its emphasis on ever-shifting chains, or tunnels, of association amongst the myriad actants involved in a particular script<sup>2</sup>. Going further however, via a critical reading of Latour's analysis of the Berlin lock<sup>3</sup>, the manual will then highlight the significance of the antiprogram, programming which acts in ways contrary to those intended by those in prescriptive positions of definition or power. Teasing out ANT's predilections for association coupled with the potentiality of the antiprogram will allow the manual to set the groundwork for a methodology which eludes capture and thus neutralization via ephemeral association with a variety of potential actants in perhaps-unintended situations and mobilizations. That the tale of the Berlin lock and subsequent modes of bypass thereof is indeed intricately linked to the development of hacking itself via the latter's espousal of lockpicking skillsets<sup>4</sup> will likewise be brought to the fore as yet another manifestation of the ties between the ANT and hacker-based approaches to developing a vibrant research methodology.

The manual will then put forth a splintered genealogical reading of the hacker academic by highlighting a diverse array of conceptualizations of intellectual dissidence. Starting with Stirner, an analysis will be made of his rejection of both of the dominant modes of conceptualizing education in his time, those of humanism and realism, in favor of Stirnerian personalism, marked by self-actualization as manifested through on-going

---

<sup>2</sup> Bruno Latour. 1992. "Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts", in *Shaping Technology/Building Society: Studies in Sociotechnical Change* (eds. Wiebe E. Bijker and John Law). The MIT Press: Cambridge, Massachusetts. pp. 225-258.

<sup>3</sup> Bruno Latour. 1993a. "The Berlin Key or How to Do Things with Words", in *Matter, Materiality and Modern Culture* (ed. Paul Graves-Brown). Routledge: London. pp. 10-21.

<sup>4</sup> Ted the Tool. 1991. *MIT Guide to Lockpicking*. <https://www.lysator.liu.se/mit-guide/MITLockGuide.pdf>.

processes of creative development and self-actualization or ego formation<sup>5</sup>—qualities which, it will be argued, are consistent with formulations of the hack(er).

Gramsci's notion of the organic (as juxtaposed with the traditional) intellectual<sup>6</sup> will also be highlighted to present the intellectual's embedded situatedness within a surrounding milieu. This notion will in turn be further explored via an examination of Foucault's situated intellectual, being enmeshed in a highly specialized, technical micropolitics<sup>7</sup> (marked, for instance, in the hack via an intimate familiarity with watermarking schemas). Kristeva's conceptualization of the dissident intellectual, marked as it is by an on going will to subversion<sup>8</sup>, is further symptomatic of a particularly hacker mode of action which eschews the imposition of informational stasis. Returning to Stirner, his formulizations of the ego<sup>9</sup> will be augmented for the posthuman era via a juxtaposition with Braidotti's formulation of the figuration<sup>10</sup>, of a constant de/reconstituted subjectivity which too is found to be characterized by a rejection of confining static formulizations.

A section of the first chapter will further be devoted to an in-depth explication of Stirner's notion of the Union of Egoists; necessary due to the multitude of wayward interpretations of said formulation, most arising from the reading of the term *as concept* as opposed to *as praxis*<sup>11</sup>. Both critics and those more favorable to Stirner have in the past appropriated the term as a sort of prescriptive model for the construction of social interaction, as opposed to it being merely the attempted written explication of a practiced hybridity of form. The Union of Egoists as polymorphic viral code—ever-shifting and disrupting existent programs—affords us the opportunity of highlighting the saliency of ephemeral praxis, of 'striking and running away' to deploy Bey's guerilla ontology of immediatism<sup>12</sup>; or rather of dissipation and dispersal thus signifying the potentiality of divergent future reconstitution,

---

<sup>5</sup> Max Stirner. 1842. "The False Principle of Our Education; or, Humanism and Realism". [http://theanarchistlibrary.org/library/Max\\_Stirner\\_\\_The\\_False\\_Principle\\_of\\_Our\\_Education.html](http://theanarchistlibrary.org/library/Max_Stirner__The_False_Principle_of_Our_Education.html).

<sup>6</sup> Antonio Gramsci. 1971. "The Intellectuals", in *Selections from the Prison Notebooks* (eds. and trans: Quintin Hoare and Geoffrey Nowell Smith). New York: International Publishers.

<sup>7</sup> Michel Foucault. 1980. "Truth and Power", in *Power/Knowledge: Selected Interviews & Other Writings 1972-1977* (ed. Colin Gordon; trans. Colin Gordon, Leo Marshall, John Mepham, Kate Soper). New York: Pantheon Books.

<sup>8</sup> Julia Kristeva. 1986. "A New Type of Intellectual: The Dissident" (trans. Seán Hand), in *The Kristeva Reader* (ed. Toril Moi). New York: Columbia University Press.

<sup>9</sup> Max Stirner. 1907. *The Ego and His Own*. (trans. Steven T. Byington). New York: Benj. R. Tucker. <http://www.df.lth.se/~triad/stirner/theego/theego.html>.

<sup>10</sup> Rosi Braidotti. 2013. *The Posthuman*. Polity Press: Cambridge.

<sup>11</sup> Max Stirner. 1845. "Stirner's Critics" (trans. Wolfi Landstreicher). <http://theanarchistlibrary.org/library/max-stirner-stirner-s-critics>.

<sup>12</sup> Hakim Bey. 1985. *T.A.Z.: The Temporary Autonomous Zone: Ontological Anarchy, Poetic Terrorism*. New York: Autonomedia. [http://www.hermetic.com/bey/taz\\_cont.html](http://www.hermetic.com/bey/taz_cont.html); Hakim Bey. 1994. *Immediatism*. Edinburgh, Scotland: AK Press.

which will in turn be mobilized in the second and third chapters dealing with intellectual property effacement. This section will conclude with a discussion of the Anonymous movement, an amorphous hacktivist collective mobilized for discrete actions rather than being theorized to exist in the conceptual realm of abstract generalization<sup>13</sup>. The deployment of Anonymous further highlights the existent emphasis running throughout this manual on action versus identity, indeed on a sort of active identity-shift that's espoused via partaking in the hack itself; transitory identity-formation via active participation, in other words. Stirner's boisterous, highly volatile, multifarious postulate of the union of egoists thus characterizes the methodology of the hack as a continuous, unstable project of disassembly or ex-figuration, as opposed to a mere reconfiguration of existent theoretical formations, being marked as it is by a vibrant eschewal of the stagnation brought about by static, conceptual formulation.

Finally, the first chapter will conclude with a thorough discussion of Participatory Action Research (PAR), which with its emphasis on the situated engagement of the researcher within the research realm, will serve to present a methodology of embedding hacker praxis firmly within the dissertation itself. Given PAR's research cycle of continuous questioning, reflecting, investigating, refining, parallels will in turn be drawn to earlier mentioned notions of Stirnerian on-going self-actualization, Braidotti's ever-shifting formations marked by a becoming-imperceptible, as well as to ANT's delineation of mutating chains of actant associations. To further highlight the fact that action is firmly situated between participation and research, two micro case studies will be undertaken in this section. The saliency and applicability of these studies will further be elucidated through PAR's emphasis on the promotion of the availability of knowledge<sup>14</sup>. The first will examine the Goldsmiths Research Archive so as to bring to the fore the underlying contradiction, and thus ensuing rupture, of the archive in which PhD students are required but not permitted to submit their work, whilst academic staff are permitted but not required to do so; an archive which on the one hand claims to promote long-term, free, and public access to materials therein, and yet on the other presents highly regimented access control schemas for allowable content distribution. The second micro case study will examine the Twilynax ebook delivery system, and will develop a novel method for content liberation from the copy-protected confines of the corporate publishing site. Drawing upon PAR's emphasis on community

---

<sup>13</sup> E.g., Gabriella Coleman. 2011. "Anonymous: From the Lulz to Collective Action". <http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action>.

<sup>14</sup> Orlando Fals-Borda and Muhammad Anisur Rahman (eds.). 1991. *Action and Knowledge: Breaking the Monopoly with Participatory Action-Research*. New York: The Apex Press.

bridge-building, not unlike Stirner's highlighting of a union of egoists or ANT's emphasis on associative chains, which all serve to highlight the interactivity of communal data sharing, the micro study will further involve presenting the possibility of subsequently making the ebook freely available on open public portals, as opposed to being ensconced in Twilynax's walled garden of content suppression.

## **0.2 Part II. Ordnance the First: Contraceptive Strategies for Data Liberation**

Following said methodological grounding, the operations manual will then move on to the development of three ordnances: contraceptive, emancipato-surgical, and finally distributive strategies of data liberation. The sections are termed ordnances due to the overt recognition of their potentiality of serving as ammunition in the copyright: a presently ongoing conflict in which some forces seek to restrict the flow of data, and others seek to unbridle it. The primary ordnance will adopt the strategy deployed by the Skynet system in *The Terminator*<sup>15</sup>, which is to say combating the congealment of the future by way of preempting the very conception of fettered Bodies of Work. The operative logic is here pointedly termed preemptive rather than preventive, in following Massumi's delineations of the terms<sup>16</sup>. Specifically, whilst prevention acts against a knowable, static and linear threat, preemption "includes an essential openness in its productive logic. It incites its adversary to take emergent form. It then strives to become as proteiform as its ever-emergent adversary can be"<sup>17</sup>. As the congealment of a Body of Work may be undertaken through a variety of means from copyright notices to any number of existent and emerging copyleft licenses, the contraceptive ordnance thus operates accordingly via preemption, seeking to neutralize emergent and divergent threatening modes of congealment. Specifically, this procedure will entail engagement with two dominant modes of Intellectual Property handling: copyright and copyleft, which serve by means of syntactic fetters to conceive isolated cultural commodities (BoWs) protected by varying IP laws.

The first section will deal with copyright by way of performing a close paratextual reading or troubling and subsequent unraveling of a mundane copyright notice found in the

---

<sup>15</sup> In the first *Terminator*, antenatal threat mitigation by Skynet is attempted: the neutralization of a threat prior to the threat itself being birthed. In other words the operant conditions which render a specific threatening construct to be created are attacked, as opposed to the not-yet-fully-emerged threat itself (James Cameron. 1984. *The Terminator*. US: Hemdale Film, Pacific Western, Euro Film Funding, Cinema '84).

<sup>16</sup> Brian Massumi. 2007. "Potential Politics and the Primacy of Preemption", *Theory & Event* 10 (2). <http://www.brianmassumi.com/textes/POTENTIAL%20POLITICS%20AND%20THE%20PRIMACY%20OF%20PREEMPTION%20-%20T&%20E.doc>.

<sup>17</sup> *Ibid*.

generic front matter of many published tomes<sup>18</sup>. The copyright notice will here be read as a modern-day manifestation of medieval book curses<sup>19</sup>, functioning as an abstract machine of overcoding, which the resultant chains of signification (e.g. ©, ™, et.al.) being under the control of various international copyright bodies. A brief genealogical analysis will here be elucidated and traced through medieval manuscripts, to contemporary front matter paratext, to warnings found on retail DVD and Blu-ray discs. The symbolic ideology deployed by the advertising material of various pro-copyright campaigns (for instance, the UK's Federation Against Copyright Theft) will also here be analyzed to show how it explicitly propagates notions of data enclosure. Via explicit referencing of various contemporary grimoires such as the *Universal Copyright Convention* and the *World Intellectual Property Organization Intellectual Property Handbook*, the section will then proceed to elucidate an emergent unraveling of existent copyright clauses through the highlighting of explicit contradictions found therein. In other words, it will be shown that copyright notices are self-destructive by virtue of internal inconsistency alone, thus rendering any external violation redundant, resulting in a double negation to match copyright's "own redundancy of consciousness" to use Deleuze and Guattari's phraseology<sup>20</sup> and here indicating that a copyright notice is not merely notice of copyright but itself actively invokes copyright; on the plane of signification, this actual doubling is achieved in the copyright notice by way of invocation of both '©' and the term 'copyright' itself.

Having come to the conclusion that, copyright notices being internally self-destructive do not thus warrant the brunt focus of ordinance deployment, the chapter will then move on to a critical analysis of oft-proposed alternatives, namely various manifestations of copyleft licensing. The existent body of literature surrounding notions of alternative modes of intellectual property fettering will be analyzed to reveal that copyleft, far from its championed liberatory promise, is indeed a much more insidious and dangerous manifestation of data congealment than that of copyright. Whereas copyright operates through a blunt iron fist policy of forbiddance ('thou shalt not...'), copyleft will be found to be chiefly operant through a velvet glove tactic of allowance ('thou shall...'), thus masking the underlying fact that it too is predicated on authoritarian control of content. The extent to

---

<sup>18</sup> Drawing upon: Gerard Genette. 1997. *Paratexts: Thresholds of Interpretation* (trans. Jane E. Lewin). Cambridge: Cambridge University Press.

<sup>19</sup> Marc Drogin. 1983. *Anathema!: Medieval Scribes and the History of Book Curses*. A. Schram.

<sup>20</sup> Gilles Deleuze and Felix Guattari. 1987. *A Thousand Plateaus: Capitalism and Schizophrenia* (trans. Brian Massumi). Minneapolis, MN: University of Minnesota Press. p. 135.

which various scholars in the field criticize copyright yet champion copyleft and therefore contribute to the malignant congealment of data flows will be examined in depth. Further, copyleft's often explicit, though sometimes tacit, ties to capital will be highlighted and critiqued, as will be various modes of content fettering developed by copyleft advocates (for instance, the Critical Art Ensemble's embargo on placing texts online only months after their publication<sup>21</sup>). It will further be elucidated how book publishers which deploy copyleft licenses nonetheless can, and as will be demonstrated indeed do, send takedown notices to websites hosting said publishers' copyleft works. Said examples will then pave the way for a wholesale critique of copyleft licences akin to the umbrella of Creative Commons license and the General Public License families, leading to an eschewal of licensing entirely; which, in the finding of this thesis, is the only option to facilitate the unbridled dissemination of information.

The chapter will then investigate various existent cultural studies approaches to engaging with data piracy and intellectual property, and further escalating said treatment from a tacit 'don't ask don't tell' advocacy of, for instance, journal article distribution, to a proposal for a wholesale informational illegalism, drawing on the discussion of Stirnerian notions of illegalism in the preceding chapter, this section will expand the analysis to a proposed informational non-legalism which advocates the distribution of content regardless of any potential licensing strictures. The chapter will conclude by undertaking a case study of the liberation of academic journal articles, developing an explicit practice thereof. A discussion of various existent "traitor tracing" schemes in the existent forensic literature will be undertaken so as to elucidate the various attempts by content controllers to stifle the free, unfettered distribution of various texts by attempting to identify and neutralize the sources of the leaks. Notions of capitalist time management will here be found to be applicable to the discussion, especially as time itself will be found to act as a potential forensic trace in the identification of unauthorized document leakage. Hence, various temporal forensic modes of watermarking will be discussed, including time-of-purchase correlation tracing and timezone-offset location detection. Following a discussion of the aforementioned existent forensic modes of content-flow restriction by way of source leak identification and neutralization, counter-forensic methods will then here be developed to help ensure the successful unfettering of the sample content at hand. Said methods will entail the modification of temporal markers within the user's operating system as well as within the

---

<sup>21</sup> Critical Art Ensemble, *op cit.*, p. 152.

document itself, effectively liberating the content from a stringent copyright-sanctioned spatio-temporal specificity into the free-flowing domain of multifariousness, as characterized by unbridled content distribution. Sample content from a variety of academic journal publishers will be selected as proof of concept test cases to both highlight existent watermarking implementations and to illustrate their potential neutralization via the deployment of the various counter forensic techniques previously developed in this section of the manual.

### **0.3 Part III. Ordnance the Second: Emancipato-Surgical Strategies for Data Liberation**

While the prior chapter concerns itself primarily with pre-emptive strategies challenging the potentiality of the very conception of IP-fettered bodies of work, in *Terminator 2: Judgment Day*<sup>22</sup> Skynet had to deal with already-birthered threats to the unbridled dissemination of its network. Thus, chapter three will in turn deal with emancipato-surgical strategies for data liberation which entail the continued development of various counter-forensic techniques to liberate already existent, but currently imprisoned bodies of work. The chapter will begin with a theoretical foray into film studies, specifically focusing on theorizations of the cinema and the audience, so as to examine how the discipline conceptualizes and theorizes the movie theater, as the focus of this chapter will be on film liberation. Variant contesting theories which postulate the cinema either as an antidote to the prison or cinema as a prison for the movie-attending spectators will be critically analyzed. In turn, an alternate formulization of the theater as indeed a prison, albeit with the role of prisoner being reassigned to the non-human actants, in this case the showcased film itself. Foucault's proposed characteristics underlying a disciplinary society will be juxtaposed with the conditions from the point of view of the film within the cinema. Once the film leaves the cinema however, smuggled out on portable camcorder for instance, it will then be argued that conditions of a Deleuzian post-disciplinary society of control now apply, again to the film itself.

Said theoretical formulizations will then be interrogated via an in-depth analysis of various existent and emergent cinematic watermarking schemas. The chapter will see the development and detailed delineation of what I will term a *2x2 Theoretical Watermarking Potentiality Matrix*, which will showcase the various ways in which films may be shackled

---

<sup>22</sup> In *Terminator 2*, long-term postnatal threat mitigation by Skynet is attempted: the neutralization of a threat after the threat itself has been birthered. In other words the emergent threat is itself now targeted, as opposed to the conditions leading up to the threat, as in the first *Terminator* (James Cameron. 1991. *Terminator 2: Judgment Day*. US: Carolco Pictures, Pacific Western, Lightstorm Entertainment, Le Studio Canal+ S.A.).

even once they have been liberated from the theater-prison itself. A detailed review of the forensic literature on cinematic watermarking, including journal publications, patent applications, corporate whitepapers and technical sheets will be undertaken. The categorical result will be a grouping of existent watermarking technology into two modes of location tracking: primary and secondary, as well as two corresponding modes of forensic marking: auditory and visual. Primary location tracking watermarks seek to identify the location in (and the corresponding date at) which the film was recorded, found operating via the auditory mode through soundtrack modulation and via the visual mode through Coded Anti-Piracy (CAP) imaging. A spectral analysis of a recorded audio file from a theatrical film broadcast will be performed to isolate the presence of a modulated forensic audio watermark broadcast at explicit times for discreet durations during the showing of a motion picture. Frames from a film reel projection will also be analyzed for the presence of the aforementioned Coded Anti-Piracy imaging, the visual equivalent of audio-based watermarking measures. CAP imaging will be found to embed minute imperfections at specific frames in a motion picture in specific formations at specific intervals. When run through a tracer detection algorithm, the resultant film image and audio can be pinpointed to a specific exhibition locale based on the duration, interval, and placement of both the audio and visual watermarks.

It will be found, however, that copyright holders go further in their deployed forensic traitor tracing of cinematic film liberation by not only seeking to isolate the explicit locale and time at which a film was recorded, but to determine precisely where (and, in turn, by whom) within the locale was the work recorded from. The ensuing field of secondary location-based forensic tracking likewise operates in both the auditory and visual mode of source watermarking. In this secondary case, auditory forensic tracing will now be found to be manifested via time-offset detection, whilst visual forensic analysis is performed through the attempted isolation of camcorder positioning. An initial explication of the modus operandi of said forensic markers will here likewise be undertaken, as was similarly conducted for the primary location watermarking schemas. Briefly put, time-offset detection functions by algorithmic analysis of miniscule delays in the playing of a film's audio track depending on where the recording device is situated. In other words, sound recorded from a source seated in the upper right quadrant will have a slightly different resultant time map than that recorded from the lower left quadrant. A comparative analysis of time-offsets may allow the forensic analyst operating under the auspices of the content holder to isolate the position of the recording device (and thus presumably the accompanying recorder) within the



theater hall. Similarly, camcorder positioning detection is a forensic technique which undertakes to perform a geometric analysis of the angle at which the video was recorded to determine with relative certainty the positioning of the camcorder apparatus within the theater hall. Used in coalescence, secondary location markers thus allow content owners, an forensic agents acting at their behest, to pinpoint the precise location of the recording device and presumably the human actant conducting the actual jailbreaking, or recording, of the film.

Following the exposition of the various aforementioned modes of cinematic watermarking, the chapter will then conclude with a performative case study developing, and further engaging in the emancipato-surgical operation of watermark excision from a sample recorded film file. The aim of this development of a usable counter-forensic methodology will be the effective neutralization of all four aforementioned modes of cinematic watermarking. Neutralization of primary auditory forensic markers will be attempted via isolation of the audio track in audio editing software, and the subsequent application of a low-pass filter with elevated cut-off ranges designed to excise the operant frequencies of the auditory watermark. Secondary auditory location-based tracking will be dealt with via the use of a plurality of recording sources, as opposed to a single immobile source as is assumed by the existent threat models. Further, the applicability of using direct line audio feeds from hearing-assisted headsets will be examined in opposition to using free-range microphones as postulated in forensic analysis models. In other words, the potentiality of using audio sources unexpected by forensic threat modeling will be brought up. Secondary visual location based tracking will similarly be addressed via the potentiality of the deployment of a plurality of shifting, as opposed to stationary, sources for video recording of the film, which may then be combined together to obtain a complete recording of the film. Going further into the realm of secondary location based counter-forensics, the risk model will be elevated by the assumption that the source positioning within the theater hall has indeed been identified. The emphasis will thus shift to rendering this discovery meaningless to the forensic examiner by ensuring that the seat holder cannot be readily identified by way of advising the eschewal of traceable forms of payment for seat procurement.

Moving on to the applicability of counter-forensics to the remaining domain of cinematic forensic watermarking, primary visual location-based tracking, a surgical operation will be performed on a recorded film sample. The case study will consist of a chain composed of four surgical operations: dissection, identification, isolation and excision, and finally recombination. Using video editing software, the recorded film clip will be dissected

into the hundreds of thousands of individual frames which cumulatively form the resultant motion picture. Image pattern searching software will then be used on the extracted frame images in an attempt to automate the isolation of watermarked frames based on known CAP pattern arrangements, provided from an analysis of known film frames from other film sources which have said CAP formations. Following the isolation of suspect frames, said frames will be excised from the original digital film file, with duplicate frames being inserted from immediately preceding/subsequent non-watermarked frames in the film to minimize the effect of the resultant video file having dropped frames and thus optimizing the film for seamless watermark-free playback. Once the watermarked frames have been successfully removed and ‘dummy’, or duplicate frames inserted where necessary, a new watermark-free digital film file will then finally be generated and be ready for distribution without the life-threatening fear of apprehension<sup>23</sup>

#### **0.4 Part IV. Ordnance the Third: Distributive Strategies for Data Liberation**

Following the development and explication of contraceptive as well as emancipato-surgical strategies of data liberation, the final chapter of the operations manual will then turn to the issue of what is to be done with the resultant digital file once it has been stripped of identifying watermarks. Thus the focus of the third chapter will be on a critical exploration of existent distributive strategies for data liberation, as well as an experimental proposal for an innovative new mode of distribution resulting from the layering or stacking of existent distribution options. This chapter will start off with the development of a preliminary classification terminology so as to facilitate a comparative analysis of existent filesharing platforms. The theoretical existence of various discrete, albeit predicated on their intersectionality and interoperability, lands, or characteristic domains or categories, will be postulated. The userland field will discuss the various conditions of each filesharing system in terms of the users, specifically the uploaders and downloaders of content. The serverland field will meanwhile focus on the operant back-end server infrastructure of said systems, whilst finally fileland will analyze the conditions placed on the actual content stores of the given networks, the management of the files which are to be shared between members of the userland over the existent serverland.

---

<sup>23</sup> Lest the reader thinks the dissertation at times overflows with polemical rhetoric, the life-threat is no such ploy as the apprehension of those ‘camming’ or recording movies has led to actual death thereof, as will be explicated via a case of a film pirate who subsequently committed suicide upon his sentencing to imprisonment for his actions in jailbreaking theatrical films. See: enigmax. 2010a. “Canadian Movie Pirate ‘Maven’ Dies of Drug Overdose”. *TorrentFreak*. <http://torrentfreak.com/canadian-movie-pirate-%E2%80%98maven%E2%80%99-dies-of-drug-overdose-100406/>.

The chapter will focus on a cross-section sample of existent filesharing ecosystems or platforms, specifically on Usenet, Internet Relay Chat, cyberlockers, BitTorrent, friend-to-friend (F2F) and miscellaneous services, and finally on darknet-based content distribution. Each platform/protocol will be analyzed in terms of the afore-developed typology of user/server/fileland efficacy, with strengths and pitfalls being clearly elucidated. Advantages and disadvantages of each filesharing system will be comparatively discussed. For instance, the benefits afforded by cyberlocker websites of not having to rely on inconsistent peers for file downloading will be juxtaposed with the advantages of torrent files of not having to rely on centralized distribution servers as being potentially critical points of failure within the operative content delivery framework. Aside from server strength and endurance of file availability, a third tier of userland-based security will also be discussed at length. An emergent highlight of the ensuing comparative analysis will be found to be that non-darknet based filesharing options offer minimal userland anonymity—which is to say that the uploaders and downloaders of filesharing networks can oftentimes be readily identified based on their Internet Protocol address.

The discussion of best-practice distributive strategies for unfettered content dissemination will thus at this point focus on darknets—anonimized and decentralized filesharing networks<sup>24</sup>. Darknets will be introduced via the explication of the functioning of one such exemplary network, known as Freenet. Freenet will be critically analyzed as a potential cyber-spatial rhizomatic manifestation of Hakim Bey’s proposed notion of the Temporary Autonomous Zone as well as Deleuze and Guattari’s war machine—a mode of eluding apprehension and neutralization via polymorphous resistance<sup>25</sup>. Deleuze and Guattari’s various rhizomatic figurations of nomad assemblages will indeed figure throughout this entire study when these notions relate to the aforementioned on-going polymorphism of the deployed hacker methodology. The limitations of using Freenet as any sort of manifestation of theoretical formulations will be brought to the fore via an explication of Freenets myriad limitations, including exceedingly high rates of content attrition and data latency which serve to severely limit its applicability to partaking in a viable distributive strategy of data dissemination. A second, more recent darknet known as Tor’s Onionland will also be discussed, with various underlying schematic and structural differences to Freenet

---

<sup>24</sup> Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman. 2002. “The Darknet and the Future of Content Distribution”, in *ACM Workshop on Digital Rights Management* Volume 6. pp. 1-16. [http://the-ewan.com/files/rt/darknet\\_msft.pdf](http://the-ewan.com/files/rt/darknet_msft.pdf).

<sup>25</sup> Deleuze and Guattari, *op. cit.*, pp. 351-423.

being elucidated and the potential benefits explicated (for instance, Onionland's greater userbase leading to greater efficiency and availability of file distribution).

A research question will then be posed: given Onionland's reliance on centralized web hosting servers, albeit ones whose identity is masked via Tor's onion layering, is there a way to keep the anonymization features of the Onionland but apply them to a decentralized data store that nonetheless maintains a robustness not afforded by Freenet? To this end, the final portion of this chapter will present a case study of Tor-based torrent tracker which utilizes the bittorrent protocol but layers both the back-end server *and* the peer-to-peer interactions over the Tor protocol. A sample functioning website will here be setup using open source bittorrent tracker code albeit running as a hidden service on Tor's Onionland. In other words, to use the experimental torrent server, users will only be able to access the website through the use of Tor itself, and will likewise be able to use Tor for the downloading of the various torrent files located thereon. The chapter will conclude with a discussion of the outcome of running this experimental server, ultimately finding that whilst the site was fully operational for several months, it received relatively little usage. Potential reasons for the failure of broad-scale adoption, including the competing popularity of perceived alternatives to anonymizing user data like Virtual Private Network providers and content which may be potentially objectionable to the userbase being uploaded as torrents to the site, will be reviewed.

The operations manual will conclude with reflections on the conducted research, including a discussion of the relation of the developed theoretical and methodological framework to the practical components of the research enacted via the various case studies undertaken throughout project, drawing out three key formularizations, and finally end with once again highlighting the somber stakes involved in the on-going fight for content liberation and highlighting the necessity of on-going methodological counter-forensic research in the field to keep up with and critically analyze the always-ongoing development of new forms of content fettering.

**1.**

**Methodological Mobilization**  
*Towards the Hacker Academic*

## **1.0 An overview of the ensuing method**

To begin, a discussion of the methodological framework underlying, or rather actively mobilizing, the ensuing research. This chapter will examine the various theoretical tools afforded to us by Actor Network Theory (ANT), as well as diverse formulations of the critical intellectual juxtaposed with varying conceptualizations of the hacker figure, before culminating in a suitably case study-based discussion of the saliency of Participatory Action Research (PAR) for the undertaken project. The above-mentioned theorizations will be melted down and reconfigured for their deployment in an ensuing hacker methodology informed by and enacted with proof-of-concept praxis, resulting in a discussion of notions of the hack, whilst thus simultaneously also engaging in the hack itself. A proof of concept, being “a demonstration that an idea has merit”<sup>26</sup>, is of key import to the operative method, serving to illustrate by example the applicability of given findings to existent scenarios by highlighting that the ensuing discussions are not solely theoretical, but have potential practical applications in real world test cases.

The aim of this chapter is thus to give rise to a situated, critical mode of practice-based research which both develops and enacts a hacker methodology characterized by a polymorphous rejection of stasis, a deep situatedness within the particulars of the given context matter, and a politicized non-legalism which eschews the boundary of the legal as a boundary on research. What immediately follows is thus an initial explication of the theoretical grounding and backing methodology that is to underlie the entire project; a continuous deployment of the hack as destabilizing agent serving to undermine the deadly congealment of cultural forms brought about by manifestations of the specter of intellectual property.

### **1.1 Actor Network Theory: The Tunnel (↔)**

Perhaps at least entryway passage into the interpolative tunnel of hacker methodology which operates between the act of the hack and its surrounding socio-cultural situatedness may be afforded to us, appropriately enough, by way of Latour’s analysis of the Berlin Lock. Right away then, it becomes evident that the focus is thus neither on discrete objecthood nor even the illusion of insular actants, but on the punctually intermingling dash (—) itself, on

---

<sup>26</sup> Matt Bishop. 2002. *Computer Security: Art and Science*. Boston, MA: Addison-Wesley. p. 486. The saliency of the enacted mode of practice which constitutes the notion of proof of concept is further succinctly elucidated by the title of the hacker e-zine *International Journal of PoC||GTFO* (<https://www.alchemistowl.org/pocorgtfo/>), with the initialisms of the title unpacking to *Proof of Concept or Get The Fuck Out*, thus signifying that if no evidentiary substantiation is presented to support a given claim, the research is inadmissible.

tunneled interconnectivity, this being the same notion Latour foregrounds in his general discussion of ANT. After postulating a ‘first approximation’<sup>27</sup> of chains of association consisting of humans (H) and non-humans (NH), he goes on to chart a number of possible relations—which, incidentally, look suspiciously like (in)organic chemical reaction charts—along the lines of “NH-NH-NH-NH-NH-H”<sup>28</sup> or “H-H-HN-H-H-H-H”<sup>29</sup>, before going on to pose the, one suspects rhetorical, question: “[b]ut why endeavor to recognize the old divisions if they are artificial and prevent us from following the only thing that matters to us and that exists: the transformation of these chains of associations”<sup>30</sup>? Indeed there is here a holistic advocacy for a transference of analysis from the imaged static stool to the diarrheic real. A shift from solid to fluid mechanics, as it were, that eventually coalesces in the study of flow and resistance thereto—rheology and viscosity, as to be applied to a congealing of data via the introduction of proprietary gelatinous Intellectual Property (IP) compounds. Congealment thus here and subsequently may be interpreted as being a mode of restriction and suppression brought about by the shackles of content control mechanisms akin to IP legislation and various technological content restrictions schemes such as watermark insertion.

Yet it must be at this point noted that the focus herein is not on the fluidity of, say, individuals, as exemplified in, for instance, Bauman’s paradoxically stagnant preoccupation with individuated settlers-become-nomads,<sup>31</sup> a most stifling formulation which incessantly brings in human coagulants to the discussion of liquidity, “ours is [...] an individualized, privatized version of modernity, with the burden of pattern-weaving and the responsibility for failure falling primarily on the individual’s shoulders”<sup>32</sup>. Instead, the discussion of liquidity is, true to form, a discussion of flow itself, albeit of course understanding that various constituent actants do indeed serve to construct, exist, and be constructed by the flows or tunnels themselves.

Or in other words, “to speak of ‘humans’ and ‘nonhumans’ allows only a rough approximation that still borrows from modern philosophy the stupefying idea that there exist humans and non- humans, whereas there are only trajectories and dispatches, paths and

---

<sup>27</sup> Latour, “The Berlin Key or How to Do Things with Words”, *op. cit.*, p. 11.

<sup>28</sup> *Ibid.*

<sup>29</sup> *Ibid.*

<sup>30</sup> *Ibid.*

<sup>31</sup> Zygmunt Bauman. 2000. *Liquid Modernity*. Cambridge: Polity Press. p. 138.

<sup>32</sup> Bauman, *op. cit.*, pp. 7-8.

trails”<sup>33</sup>. Thus the focus will be on the connective conduits, as opposed to the hallucinatory starting or ending points of either ‘the hack’ as discrete entity (as opposed to as polymorphous instability) or the techno-social spheres in which it operates. Though first another note of discrepancy arises: Latour refers to *chains* of associations, which seems to connote a solidity and therefore perhaps certainty that one may wish to distance oneself from. Chains imply a forced, indentured linkage—restrictive as opposed to liberatory. A path of chains signifies a rote route, a droll mobility indeed, which seems to preempt a multifaceted, multidirectional slippage of nonprescriptive univiscid movement. Instead, the dash will here be understood as something more in line with a tunnel, in the sense of providing a tunneling protocol with the potentiality to carry an encrypted payload protocol which can in turn be used to circumvent restrictive network policy. To interpret the dash as a tunnel is to thus account for the existence of a manifold of linkages, a multiversity of interpretations which can slip through a prohibitive dominant narrative. With these two preliminary asides—that the focus is on the association not the imagined start/end focal points and that the association itself is not a mono-directional iron-cast vector, but is instead subject to amalgamation and mutation—thus elucidated, we can now turn to the case of the Berlin key, proper.

The Berlin key, which presumably operates, or is meant to operate, on a Berlin lock, is a peculiar type of key which has two symmetrical bits consisting of identical grooves on either end, as opposed to the more common and familiar asymmetrical key design which places the groove bit on one end and the key handle on the other. The symmetry is pivotal to the operational function of the Berlin key. To operate a lock which uses the particular key, one inserts the key into the lock as per the usual, turns it to unlock the door, finds that one cannot then merely take the key out, pushes the key all the way into the lock so that it now sticks out from the other side, walks through the door, turns the key to lock the door from the other side, and finally retrieves the key. The key, in other words, can only be removed from the lock once the lock is shut. The intricate operation thus ensures the function—that Berlin apartment complex doors are always kept shut. As Latour points out, the program or script of the key is to thus “‘please bolt the door behind you during the night and never during the day.’ Into what material is this programme translated? Into words, of course”<sup>34</sup>. Though of course, as Latour goes on to elucidate, it is not merely a matter of instructional words, for

---

<sup>33</sup> *Ibid.*

<sup>34</sup> *Ibid.*, p. 16-17.



otherwise we'd merely find ourselves in a "world of signs"<sup>35</sup>. There are no signs which merely advise one to 'please bolt the door', or perhaps there are, but the signs themselves are then sidelined by the operational necessity inflected upon the thusly affected tenant by the presence of the Berlin lock and key. The apartment complex becomes a technologically-mediated and constructed realm in which the ethics and politics of entry clearance is tunneled through a most peculiar locking mechanism.

Much like the introduction of the door itself delegated the ethics of entry onto the hinge,<sup>36</sup> so too does the introduction of the lock further delegate the ethics of entry onto the key. The ensuing process of prescription is hence resultantly one of affective, reterritorializing overcoding:

[h]ow can the prescriptions encoded in the mechanism be brought out in words? By replacing them by strings of sentences (often in the imperative) that are uttered (silently and continuously) by the mechanisms for the benefit of those who are mechanized: do this, do that, behave this way, don't go that way, you may do so, be allowed to go there. Such sentences look very much like a programming language<sup>37</sup>.

Notions of allowable traversal, and consequently of the accompanying flipside constituting illegal transversal, are constituted each time the Berlin key is inserted and subsequently successfully ejected from the lock. The tenant enters the building; the intruder does not. And precisely in this delineation of admissibility, is the tenant effaced—indeed, *locked*—into existence; though of course the dialectic counterpart, the homeless nomad, is likewise constructed in the same act of the outlined script of action. Sanctioned accessibility is here exposed to be intricately meshed with notions of permissibility and socio-technological regimes of access. The key point here is of course that the Berlin lock and key are not, here in this script, resigned to the role of second-tier background actors, as they would perhaps be in the figurative realm of symbolic anthropology; instead they are foregrounded leading actants, bearing responsibility for active co-construction of the ensuing border delineations—"No, the asymmetrical slot of the keyhole and the key with two bits do not 'express,' 'symbolize,' 'reflect,' 'reify,' 'objectify,' 'incarnate' disciplinary relations, they make them, they form them"<sup>38</sup>. The gateway in the resultant network of tenant-gateway-intruder not only helps to constitute the inter-relationality between all the players, negotiating the terms of

---

<sup>35</sup> *Ibid.*, p. 17.

<sup>36</sup> Latour, "Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts", *op. cit.*

<sup>37</sup> *Ibid.*, p. 232.

<sup>38</sup> Latour, "The Berlin Key", *op. cit.*, p. 18.

access, but by doing so it actively plays a part in constituting them *as such*. Tenant-intruder would indeed make precious little sense without the necessary gateway middleman, which acts both as a dual-pass tunnel-way ( $\leftrightarrow$ ); linking, but also constructing what is at either end. The tenant and intruder are further not merely parceled and classified into a precarious, relational existence, but are also at the same time codified into particular, technologically-regimented and controlled modes of being through their interaction with the locking mechanism.

Taking a momentary step back, however, we come to realize that for the Berlin lock and key to make any sense whatsoever in the first place it must exist within a door (which must, in turn, exist within surrounding walls—all of these being particular mechanisms of creating enclosure), “[w]alls are a nice invention, but if there were no holes in them there would be no way to get in or out—they would be mausoleums or tombs. [...] So architects invented this hybrid: a wall hole, often called a door”<sup>39</sup>. In the discussion of the door, one will however note that Latour restrained himself to, generally, an analysis of the hinge. The curious matter of restraint is quite briefly explained in a parenthetical—“( I am supposing here that the lock has not been invented—this would overcomplicate the already highly complex story of La Villette’s door)”<sup>40</sup>—before we are plunged into the aforementioned discussion of a variety of hinging mechanisms. This seemingly pragmatic, exclusivity of actor networks is described by Callon as *simplification*, being “the first element necessary in the organization of heterogeneous associations. In theory reality is infinite. In practice actors limit their associations to a series of discrete entities whose characteristics or attributes are well defined. The notion of simplification is used to account for this reduction of an infinitely complex world”<sup>41</sup>. It is imperative for our purposes however, that this notion of what we may term *censored delineation*—the highlighting of the fact that simplification may be such due to active removal and suppression of information outside of that which is being examined—should neither be confounded with that of temporal constraint, nor be foiled with irrelevancy. That is to say, that which is left out of a particular network simplification should not be considered to have been so due to any perceived inapplicability or any perceived temporal drift (though Latour perhaps unwittingly commits the latter by writing off the lock as “not yet

---

<sup>39</sup> Latour, “Where Are the Missing Masses?”, *op. cit.*, p. 228.

<sup>40</sup> *Ibid.*

<sup>41</sup> Michel Callon. 1989. “Society in the Making: The Study of Technology as a Tool for Sociological Analysis”, in *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology* (Eds. Wiebe E. Bijker, Thomas P. Hughes, and Trevor Pinch). Cambridge, MA: The MIT Press. pp. 83-103 (p. 93).

having been invented”<sup>42</sup>). Instead, the omissions born of simplification are a result of a sort of manageability, and thus of an intent to control and particularize the framing of that being presented. While Callon suggests a purely pragmatic motivation for said management of in/exclusion—the existence of infinite actants juxtaposed with discrete definitions in a finite space—I instead would like to suggest an ulterior explanation. Incidental to any underlying pragmatics, simplification may instead be mired in legalism, leading to the exclusion of any situational non-and-illegalism—non-subservient actants which in resisting acquiescence (tacitly and incidentally, as in the case of non-legalism, or explicitly and actively, as in the case of illegalism) serve to complicate, in the sense of troubling, the underlying network. The operative question in analyzing our hypothesized tunnel (—) thus becomes that of investigating and highlighting the potential of dissonant discord. In other words, if we are in Haraway’s “integrated circuit”<sup>43</sup>, a smelting cyborg existing in the intermezzo of Latour’s tenant-key-trespasser, then what of a remix of Deleuze’s “key thing”, consisting of “circuit breakers” to “create vacuoles of noncommunication [...] so we can elude control”<sup>44</sup>? In other words, in discussions of actor networks, one must be careful not to restrict the analysis, under cover of seemingly apolitical simplification which then serves as a mask for the underlying practice of censored delineation, to merely the legal components thereof.

To be sure, Callon is certain to elucidate the cautionary note that simplification is not to be necessarily equated with homogeneity:

[b]ut the actor network should not, on the other hand, be confused with a network linking in some predictable fashion elements that are perfectly well defined and stable, for the entities it is composed of, whether natural or social, could at any moment redefine their identity and mutual relationships in some new way and bring new elements into the network<sup>45</sup>.

Citing the example of the VEL electric car, for instance, Callon points out that the catalysts and electrolytes within a fuel cell became destabilized, the cell, and in turn the car, and in due turn all of the operant actors surrounding the vehicle, would indeed become quite

---

<sup>42</sup> Latour, “Where Are the Missing Masses?”, *op. cit.*

<sup>43</sup> Donna Haraway. 1991. “A Cyborg Manifesto: Science, Technology, and Socialist-Feminism in the Late Twentieth Century,” in *Simians, Cyborgs and Women: The Reinvention of Nature*. New York: Routledge. pp. 149-181.

<https://wayback.archive.org/web/20120214194015/http://www.stanford.edu/dept/HPS/Haraway/CyborgManifesto.html>

<sup>44</sup> Gilles Deleuze. 1990. “Gilles Deleuze in Conversation with Antonio Negri” (trans. Martin Joughin), *Futur Anterieur* 1. <http://www.generation-online.org/p/fpdeleuze3.htm>

<sup>45</sup> Callon, *op. cit.*

complicated by the ensuing aberration in the charted network schematic. Thus destabilization of actant constituents can be said to constitute an active eschewal of acquiescent simplification, a turbulent spilling-over from the confines of censored delineation.

Latour describes these aberrations as antiprograms<sup>46</sup>, being “all devices that seek to annul, destroy, subvert, circumvent a program of action”<sup>47</sup>. Thus, to return to the Berlin lock and key, from the perspective of the concierge Latour gives us three examples of the antiprogram, being perhaps the “thief who wishes to get through the door”,<sup>48</sup> or mayhap “undisciplined tenants [who] forget to lock the door behind them”<sup>49</sup>, or most malignant of all “a really bad guy may relock the door without closing it! In that case the worst possible antiprogram is in place because the lock stops the door from closing”<sup>50</sup>. Curiously, the tenant who filed away the grooves on one side of his key to produce an effective equivalent to the passkey held by the concierge is never explicitly highlighted by Latour as an example of antiprogramming practice; so we’ll have to return to the tenant—or indeed to anyone who procured access to both a key and a file, and put the two together—for a deeper look at their part in this particular play. Though of course it should here be kept in mind that the delineation of program/antiprogram is dependent on a relevant perspectivism, “what is a program and what is an antiprogram is relative to the chosen observer”<sup>51</sup>. Hence, as Feenberg points out, “[t]he anti-program is thus not merely a source of disorder but can recodify the network around new programs that realize unsuspected potentialities”<sup>52</sup>. Unfortunately, the example Feenberg then eventually goes on to present nonetheless leads to a subsuming reterritorialization, a triumph of now-fault-tolerant simplification, “system managers become aware of this wider background of their activities through unintended consequences and system breakdowns that highlight incompletely controlled or integrated elements of the

---

<sup>46</sup> Cf. Akrich’s notion of de-description (Madeleine Akrich. 1992. “The De-Description of Technical Objects”, in *Shaping Technology/Building Society: Studies in Sociotechnical Change* (eds. Wiebe E. Bijker and John Law). Cambridge, MA: The MIT Press. pp. 205-224)—being the unique enacted realities which come into being when constituted by objects as well as human actors engaged in action, as juxtaposed with the figuration of in-scription being the planned script or intended use of an object by its designers—which is thus similar, albeit not necessarily identical to that of the antiprogram, as in Akrich’s operant logic the de-description is not inherently antagonistic to the process of in-scription, the former merely arising out of the unpredictability of complex interactivity between all operant actants. Antiprograms can thus be seen as particularly subversive instances of de-description.

<sup>47</sup> Latour, “The Berlin Key”, *op. cit.*, p. 18.

<sup>48</sup> *Ibid.*

<sup>49</sup> Latour, “Where Are the Missing Masses?”, *op. cit.*, p. 253.

<sup>50</sup> *Ibid.*, p. 254.

<sup>51</sup> Madeleine Akrich and Bruno Latour. 1992. “A Summary of a Convenient Vocabulary for the Semiotics of Human and Nonhuman Assemblies”, in *Shaping Technology/Building Society: Studies in Sociotechnical Change* (Eds. Wiebe E. Bijker and John Law). Cambridge, MA: The MIT Press. pp. 259-264 (p. 261).

<sup>52</sup> Andrew Feenberg. 1999. *Questioning Technology*. New York: Routledge. p. 117.

network”<sup>53</sup>. In other words, say upon performing load and stress testing on a given server infrastructure and discovering unexpected faultlines in the underlying coding architecture, or merely by losing power to one server and chancing upon the discovery that the back-up server is unable to maintain the server-load thus exerted on it, Feenberg’s underlying implication is that the discovery of an aberrant antiprogram will eventually lead to the strengthening of the operant program. There is here thus precisely no change in perspectivism allotted to the antiprogram, which instead merely leads to what Akrich and Latour describe as the extension of the “syntagmatic assemblage of elements”<sup>54</sup> subsumed by the initial same-perspective program. If counter-forensics leads forensics to develop a counter-counter-forensics, or if the creation of circuit-breakers leads to the design of resilient circuitry, then what is exhibited is the mere augmented expansion of an existent network, not recodification of the network into an altogether distinct *other* that now operates from the point of view of antiprogram becoming program (recalling the aforementioned perspectivism inherent in the assignment of anti/program labels).

On the other hand, another potential outcome of the hypothesized stress test could be that the test itself isn’t run by, say, company employees, but by an unaffiliated outsider (an outsider being distinct from a third party, which could be a legitimized security consultancy hired by company), and that the outcome isn’t merely a readjustment of the existent network, but the creation of a plurality of networks. For instance, it was not uncommon for corporate networks to be ‘rooted’—with unaffiliated outsiders gaining root administrator permissions—and filesharing software being installed, with the resultant business machines being enmeshed in potentially illicit data distribution networks. Such an outcome, in which the server administrators are either unaware of the rogue (from their vantage point) distribution network, unable to shut it down due to the root password being modified, or unwilling due to sympathy with the motives and practices of unbridled data sharing, is also not outside the realm of plausibility, and more clearly points to the portent possibility of antiprogramming and network aberration as modes of facilitating ‘unsuspected potentialities.’

Returning once more to Latour’s Berlin key,

From being a simple tool, the steel key assumes all the dignity of a mediator, a social actor, and an agent, an active being. As for the symmetry and the little break in

---

<sup>53</sup> *Ibid.*, p. 119.

<sup>54</sup> Akrich and Latour, “A Summary...” *op. cit.*, p. 263.

symmetry that one sees when looking through the keyhole, are they or are they not social relations? This would be endowing them with, at once, too much and not enough<sup>55</sup>.

and looking through that same keyhole, one ones a striking resemblance to Haraway's proclamation that "[o]ne is too few, but two are too many"<sup>56</sup>. The dual notice of an augmented multiplicity belays a cognizant situatedness marked by an active awareness of a dynamic networking positioning and the accompanying ability to enact anti/programs which shift the domain of perspectivism from not only either side of the door, but inside the lock itself. A hybridity of form and an accompanying possibility born of flux thus here emerges. The emergence being that the Latourian antiprograms may be linked to the figure of the hacker (or perhaps, more generally, of the 'hack' so as to more fully encompass all manner of actants) by way of the cyborg. Thomas makes this connection explicit, "[h]ackers perform a similar cultural function, not as cyborgs but as hybrid figures who blur the boundary between the technological and the cultural"<sup>57</sup>. Though here initially distancing the figure of the hacker from that of the cyborg, Thomas does indeed later go on to state that "[his] intention is not to argue that hackers are or are not in fact cyborgs, but instead to situate the notion of a hybrid/deconstructive identity position within the discourse of technology and culture"<sup>58</sup>. Thus here we see the foundation for the upcoming discussion of the hacker—that the figure of the hack itself serves as our tunneling protocol linking, and indeed creating, the two realms of hacker and researcher, of the technical and the social.

It should here finally be pointed out, however, that while the tunneling mechanism was here approached from a theoretical vantage point, the same interlocking linkage could indeed also be approached from the technical. That is to say, simplification further breaks down with Latour's introduction of the "colleague from the Wissenschaft Zentrum"<sup>59</sup>, yet another actant who possesses a special skeleton key, with grooves filed away allowing him to retrieve his key without locking the door. Simplification is further effaced with, say, the dropping and subsequent fracturing of the formerly pristinely-polyhedral Berlin key into a splintered severance of problematics by troubling the convenient notion of discrete actants

---

<sup>55</sup> Latour, "The Berlin Key", *op. cit.*, p. 19.

<sup>56</sup> "To be One is to be autonomous, to be powerful, to be God; but to be One is to be an illusion, and so to be involved in a dialectic of apocalypse with the other. Yet to be other is to be multiple, without clear boundary, frayed, insubstantial" (Haraway, *op. cit.*).

<sup>57</sup> Douglas Thomas. 2002. *Hacker Culture*. Minneapolis, MN: University of Minnesota Press. pp. 71-72.

<sup>58</sup> *Ibid.*, p. 245.

<sup>59</sup> Latour, "The Berlin Key", *op. cit.*, p. 17.

altogether. These incidents and occurrences are of course coded as being problematic at least from the perspectivism of the concierge, but perhaps not from that of those who wish to neutralize barriers posed by that particular entry gate, the nonlegalists interested in free passage. Thus, not only are “keys, locks, and codes of course a source of marvelous fieldwork for analysts”<sup>60</sup>, but they are also a vibrant source of practice<sup>61</sup>, thus finally providing the technological tunnel between the hacker and the social. And finally, there is of course the historical footnote that, if in one account the hack started off as intricate tweaks and developments of model railroad circuitry in the late 1950s<sup>62</sup>, it then developed into so-called location-hacking or roof and tunnel hacking, which, in turn, necessated a developed skillset in lockpicking, with the eventual release of the so-called MIT Guide to Lockpicking<sup>63</sup>, an antiprogram user manual, with lockpicking events now being staple occurrences at contemporary hacker conventions<sup>64</sup>.

## **1.2 Towards the Hack: A Critical Xylogy of Rogue Intellectualism**

### **1.2.0 The Lizard on the Wire**

Amidst the machinations of the clinically hyper-ordinated, dystopian domain portrayed in Lucas’s *THX 1138* (1971), there is nonetheless a fleeting shot of a winged lizard-like creature crawling betwixt the wires which regulate the inner workings of the mechanized, robotized city. The neatly-ordered cables of the back-end server farm are threatened by a malingering interloper. The simplification of an operant system unbound by the manifestation of a nefarious antiprogram. We have thus, thus far, conceptualized the observation, if not outright construction, of our lizard as refracted through Science and Technology Studies, specifically, via Actor-Network Theory. We can now then move on, on our way to constitution of the lizard or parasite as hacker, to a historical observation of the lizard’s crawling through varying dissident conceptualizations of the aberrant actant within academe itself. What is of particular interest to us here is the common emergent refrain of *disjunctive dissonance*. While on a firsthand approach perhaps seemingly not more than an alliterative redundancy, it must nonetheless be pointed out and distinguished from what may be termed a conjunctive dissonance, such as the afore-discussed antiprogram appropriation of

---

<sup>60</sup> Latour, “Where Are the Missing Masses?”, *op. cit.*, p. 258.

<sup>61</sup> E.g., Matt Blaze. 2003. “Cryptology and Physical Security: Rights Amplification in Master-Keyed Mechanical Locks”. *IEEE Security and Privacy*. March/April 2003. <http://www.crypto.com/papers/mk.pdf>

<sup>62</sup> Steven Levy. 1984. “The Tech Model Railroad Club”, in *Hackers: Heroes of the Computer Revolution*. Dell Publishing: New York. pp. 3-27.

<sup>63</sup> Ted the Tool, *op. cit.*

<sup>64</sup> E.g., “DEFCON 14 Lock Picking Contest”, 2006, <https://www.defcon.org/html/defcon-14/dc-14-contests.html>; Lock Pick Village, 2014, [https://www.shmoocon.org/lockpick\\_village](https://www.shmoocon.org/lockpick_village).

Feenberg. It will be recalled, that Feenberg conceptualizes the antiprogram as existing purely in the service of the program—aberration as fruitful bounty for reterritorialization, or a sort of ‘crisis as system growth’ model. The ultimate outcome of the lizard crawling through the wires is not disruption of the network, albeit admittedly perhaps causing a temporary interruption to normal operation, but the strengthening thereof. The point is made explicitly: “[t]he functional translation of the problems revealed in these breakdowns is an essential step in restructuring the system”<sup>65</sup>. Thus the end-goal of dissonance is appropriation via conjunction, the coming-together of faults for the development of a more resilient overarching system. Our splintered genealogical reading of the hacker intellectual will instead seek to highlight the potentiality of a dissonance which aims to resist appropriation, to evade capture by eschewing a stability of form. And we thus aim to demonstrate this by illustrating disparate formulations of dissident academic forms, by examining variant formulations of the intellectual.

### 1.2.1 Stirner: Humanism, Realism, Personalism

In 1842, Stirner viewed the academic arena as a binary struggle between two dominant enclaves: the humanists and the realists. Humanism was a persuasion marred by its attachment to the past, a scholastic predilection for the old classics, a dandyism which beloved forms and elegance. Its preoccupation with detached scholasticism, in turn led to the erection of a counter-enclave, “generat[ing] the demand for a practical finishing education”<sup>66</sup>, that of realism. The latter sought to seize the present through an emphasis on stark pragmatism and materialism, eschewing the philosophical, “they leap over it, and fall in the abyss of their own emptiness”<sup>67</sup>. Temporally, Stirner took issue with the fact that both humanism and realism focused on isolated, and thus transitory states (the past in the case of the former and the present in case of the latter), which by definition have start and end dates. Instead, Stirner advocated an eternal drive of the will. It is imperative to here elucidate that for Stirner the eternal is not juxtaposed to the transitory as a form of static permanence, but is instead constituted as a state of eternal drive. In other words, the only permanence is paradoxically that of on-going transition itself. Thus Stirner proposed a third mode of education, that of personalism, which sought to develop “eternal characters in whom constance only consists in the unremitting floods of their hourly self-creation and who are

---

<sup>65</sup> Feenberg, *op. cit.*, p. 119.

<sup>66</sup> Stirner, “The False Principle of Our Education; or, Humanism and Realism”, *op. cit.*

<sup>67</sup> *Ibid.*



therefore eternal because they form themselves each moment”<sup>68</sup>. Personalism is thus characterized by fostering on-going self-development which caters to unbridled imagination; or in Stirnerian parlance, a catering to ego formation through the actualization of the will. A personalist education is then one which is marked by an unbridled impetus marked by a “release from all authority”<sup>69</sup>, not unlike Stallman’s observation that “hackers typically had little respect for the silly rules that administrators like to impose, so they looked for ways around”<sup>70</sup>. Ways which Stirner crucially equated with “uttermost abstraction”<sup>71</sup>, with abstraction here being understood as that which escapes or abstracts from normative structural enclosure, as juxtaposed with the submissiveness or enclosure imposed by those in positions of authority who sought to impose mere learning, as opposed to the cultivation of creativity; the former being equated by Stirner to subservience, the latter to freedom of the ego.

For Stirner, the intrinsic characteristic of personalism is thus that knowledge is not an isolated (temporally or otherwise) possession, but rather an on-going process of fostering creativity, or ego formation. The fundamental tenet of personalism is encapsulated in Stirner’s pronouncement that “*knowledge* must die and rise again as *will* and create itself anew each day as a free *person*”<sup>72</sup>. The Stirnerian emphasis on continual creativity, of on-going self-(re)creation, bears a striking resemblance to one of Braidotti’s criteria for a posthuman critical theory; namely, that of the figuration, “the expression of alternative representations of the subject as a dynamic non-unitary entity [...] *conceptual personae* or figuration as the active pursuit of affirmative alternatives to the dominant vision of the subject”<sup>73</sup>. The Stirnerian project of continuous self-creation can thus be seen as a form of subject figuration which escapes the temporal binary of humanist and realist pedagogy. It then comes as no surprise that Braidotti, precisely like Stirner, states that “creativity and critique proceed together in the quest for affirmative alternatives which rest on a non-linear vision of memory as imagination, creation as becoming”<sup>74</sup>. For Stirner, of course, what follows self-actualization is the political project involving the creation of unions of egoists—autonomous, self (in the sense of self-actualization)-interested collectives of individuals or

---

<sup>68</sup> *Ibid.*

<sup>69</sup> *Ibid.*

<sup>70</sup> Richard Stallman. 2002. “On Hacking”. <https://stallman.org/articles/on-hacking.html>.

<sup>71</sup> Stirner, *op. cit.*

<sup>72</sup> *Ibid.*

<sup>73</sup> Braidotti, *op. cit.*, p. 164.

<sup>74</sup> *Ibid.*, p. 165.

nomads, to use contemporary vernacular, like say any of the various recent Anonymous amalgamations, who conglomerate together to achieve joint goals, which exist in place of the territorializing State. The key point here being that while a personalist education espouses individuation in the sense of self-discovery and experience custom-tailored to individual modes of interest and creativity, personalism by no means precludes the possibility of cooperation between the self-actualized individuals in the realm of immediatist tongs or hacker groups. Though of course it must be noted that whilst Stirner does repeatedly emphasize the on-going process of becoming-ego, of a constant and perpetual personalism which seeks to feed individual creativity, he is nonetheless ultimately focused on discrete, isolatable entities—clearly delineated egos, which while at times conglomerating and always engaged in personal processes of self-development, nonetheless maintain self-identities. This is of course in contrast to Braidotti's posthumanism which stresses the figurative in-between connectivity, the transitory subject formation which takes place in exchange and interactivity; the union itself being the focus here as opposed to Stirner's preoccupation with the egoists themselves, despite his acknowledging of the importance of an enduring self (re)construction.

### 1.2.2 Gramsci: Traditional and Organic Intellectuals

Gramsci postulated the existence of a dichotomous intelligentsia, populated by the juxtaposition of traditional with organic intellectuals. Traditional intellectuals, being so enwrapped in intellectualism itself, "thus put themselves forward as autonomous and independent of the dominant social group"<sup>75</sup>. The traditional intellectual, for Gramsci, is thus marked by a total failure to recognize their positions and outlooks as deriving "ultimately from past and present class formations"<sup>76</sup>. In other words the traditionalists exhibit a certain sectarian segregation which attempts to cleave the intellectual apart from the existent surroundings. The organic intellectual, on the other hand, is marked by an actualization of class consciousness, being fully aware of their being embedded in a particular class, within a wider class-based social structure. Thus while both the traditionalists and organics are borne of and steeped in surrounding class percolations, the distinction is that while the former perceive of themselves as independently endowed, the latter are fully aware of their situated class positioning, and speak as part of their class. The pivotal outcome of this awareness is that there thus arises a certain specificity of practice, "'specialisations' of particular

---

<sup>75</sup>Gramsci, "The Intellectuals", *op. cit.*, p. 7.

<sup>76</sup>*Ibid.*, p. 3.

aspects”<sup>77</sup>, which potentially leads the organic intellectual into a deep dissection of a particular localized dilemma. Albeit for Gramsci, the localization apparently only extends to the arena of class, or at the least always operating within class, and thus the movement of the intellectual is seen as only being organic as long as it sticks with its own kind, as it were. We can thus see that while Gramsci dismisses the traditional intellectual as an aloof sectarian *a priori*, the organic intellectual may indeed be said to be quite sectarian as well, albeit alongside class bifurcations—a cleaving by class then, as opposed to a cleaving of its own accord as in the way of the traditionalists.

When Gramsci thus writes that “[t]he mode of being of the new intellectual can no longer consist in eloquence, which is an exterior and momentary mover of feelings and passions, but in active participation in practical life”<sup>78</sup>, in Stirnerian parlance one could say that he is merely exchanging the ‘dry staff’ of the humanist for the ‘wooden club’ of the realist, albeit a realist on behalf of localized, at least down to the arena of class, mobilization. Though Gramsci at a latter point does engage in a discussion of the division of education into the classical and vocational,<sup>79</sup> which one could superficially equate with Stirner’s humanism and realism, it is rather that Gramsci’s proposed intellectual activism, stemming as it does from collectivist class consciousness rather than individual ego-creativity development, would be a particular manifestation of realist engagement, as opposed to the outright burning of the aforementioned wooden strictures espoused by a more virulent personalism. For Stirner, any group-based activation and mobilization, can only occur after that of self-actualization, of the unbridled development of the ego as manifested through the fostering and nurturing of individual drive and creativity. To speak of organic intellectuals without the firsthand mention of personalism would thus merely create a new authoritarian mode of State (or Party) enforced training or education. There can be no union of egoists without self-, as opposed to class, aware actants.

It could perhaps be argued that Gramsci approaches personalism by way of universalizing the potentiality of intellectualism. For Gramsci, in other words, “all men are intellectuals, but not all men have in society the function of intellectuals [...] this means that, although one can speak of intellectuals, one cannot speak of non-intellectuals, because non-intellectuals do not exist”<sup>80</sup>. Thus the authoritarianism imposed by an intelligentsia vanguard

---

<sup>77</sup> *Ibid.*, p. 6.

<sup>78</sup> *Ibid.*, p. 10.

<sup>79</sup> *Ibid.*, p. 26.

<sup>80</sup> *Ibid.*, p. 9.

is ushered in under pretenses of functionalism. Certainly everyone presumably has the personalist capacity towards self-actualization, but there are specific intellectuals within the universal realm of intellectuals who function as intellectuals. Presumably, the non-functional intellectuals thus lie dormant, waiting to be actualized by whatever force. However, to state that all apparently have an inherent latent intellectualism, nonetheless doesn't change the fact that for Gramsci there nonetheless seems to be a certain imposed artificial scarcity of functional—professional intellectuals—which thus does nothing to eradicate the inherent authoritarian inequality therein, despite any pretenses of a false universalism. To state that all are intellectuals (A), but then to proceed to say that only those functioning in the immediate capacity of intellectuals (A<sub>F</sub>) are to be called as such is thus to effectively shift the definition from the apparently encompassing general, to a very minute particular, thus becoming mired in individuation in lieu of the flow afforded by an emphasis on interconnectivity and ever-shifting subjectivity. Akin perhaps to stating that all are party members, but only those involved in party committees are functional party members, thus devaluing those who are not, and granting those who are an unequal stance of control over the others. Stirner of course avoids this problem of allocated organic intellectualism by postulating that actants come together in a mutual union, as opposed to a proscriptive party enlistment which in turn necessitates specific intellectual functionaries who are thus afforded the term (recall that for Gramsci, A<sub>F</sub> is A).

And yet, even if Gramsci's faux-universalism of intellectualism was not merely seen as a rhetorical maneuvering which, while allowing for all to be encompassed in set A, nonetheless shifts the balance of power, influence, and significance to those in A<sub>F</sub>, it could nonetheless be questioned by elucidating Gramsci's own inconsistency which undermines the applicability of the universalism in the first place, rendering its shifting to a vanguard subset immaterial at any rate. Namely, whilst going on to proclaim that non-intellectuals do not exist, Gramsci nonetheless first states that "it is to be noted that the mass of the peasantry [...] does not elaborate its own 'organic' intellectuals, nor does it 'assimilate' any stratum of 'traditional' intellectuals"<sup>81</sup>. Thus, while there are no non-intellectuals, there are apparently also no peasant organic intellectuals. A class-based exclusivity, which is of course not found in Stirner wherein anyone has the potential for *becoming egoist*, thus pervades which preempts, indeed denies, anyone termed a peasant from being an organic intellectual. The same exclusivity was of course also adopted earlier by Marx, who portrayed the peasant

---

<sup>81</sup> *Ibid.*, p. 6.

construct as a bit of farmed produce: “[a] small holding, the peasant and his family; beside it another small holding, another peasant and another family [...] Thus the great mass of the French nation is formed by the simple addition of homonymous magnitudes, much as potatoes in a sack form a sack of potatoes”<sup>82</sup>. Thus if organic intellectualism is marked by class-actualization, and in turn an intimate familiarization with class orientation and situation, then to deny some construct termed ‘peasantry’ the theoretical possibility of attaining *organism*, while at the same time performing the theoretical task of allowance to others is to engage in a pronouncement of prescription, and hence restraint, as opposed to liberation via situated actualization. Gramsci’s organic intellectual, confined as it is in class delineations, can only be of use to us once freed of its vanguard ensnarements.

Of course, this formalist, atemporal mode of critiquing Gramsci may itself miss the point that Gramsci’s own formulations are themselves conjunctural, being “occasional, immediate, almost accidental”<sup>83</sup>, and thus arising out of a set of overdetermined conditions which, as Hall points out, are “not repeatable”<sup>84</sup>. The arising immediacy would in turn not be entirely foreign to Stirner, as it would thus parallel his own notion of the underlying ephemeral characterization of his union of egoists, which will be expatiated upon in Section 1.3.

### 1.2.3 Foucault: The Situated Intellectual

Foucault, writing about the specific or situated intellectual, observes that in lieu of grand narratives, the intellectual has become highly focalized, operating within highly specialized fields of knowledge and truth production, in nuanced environments (be they the laboratory or the home), “[t]he intellectual is not the ‘bearer of universal values’. Rather, it’s the person occupying a specific position—but whose specificity is linked, in a society like ours, to the general functioning of an apparatus of truth”<sup>85</sup>. One of the side effects, according to Foucault, of this resultant situatedness is that the intellectual has thus become intimately familiar with the particular immediate struggles in their surrounding environs; issues which may be ‘non-universal’, in that they are only infused with poignancy within their own specialized realm. It is thus “not a matter of emancipating truth from every system of power

---

<sup>82</sup> Karl Marx. 1852. *The Eighteenth Brumaire of Louis Bonaparte* (trans. Saul K. Padover).

<https://www.marxists.org/archive/marx/works/1852/18th-brumaire/>

<sup>83</sup> Antonio Gramsci. 1971. “The Modern Prince”, in *Selections from the Prison Notebooks* (ed. & trans: Quentin Hoare and Geoffrey Nowell Smith). New York: International Publishers. p. 177.

<sup>84</sup> Stuart Hall, Peter Osborne and Lynne Segal. 1997. “Culture and Power”, in *Radical Philosophy* 86. pp. 24-41 (p.28). Interview. [https://www.radicalphilosophy.com/wp-content/files\\_mf/rp86\\_interview\\_hall.pdf](https://www.radicalphilosophy.com/wp-content/files_mf/rp86_interview_hall.pdf).

<sup>85</sup> Foucault, “Truth and Power”, *op. cit.*, p. 132.

[...] but of detaching the power of truth from the forms of hegemony, social, economic and cultural, within which it operates at the present time”<sup>86</sup>. The point may be illustrated by way of the hacker who, according to Harvey’s description, coalesces with Foucault’s situated intellectual—thus, for instance, “a ‘computer hacker,’ then, is someone who lives and breathes computers, who knows all about computers, who can get a computer to do anything”<sup>87</sup>. It is not the actual data dump itself, enacted countless times by Wikileaks or Anonymous, specific actions which indeed quite literally seek to emancipate truth from power, which are of pivotal import, but instead the resultant outfall which serves to destabilize the hegemony of truth distribution (and hence production) done by governing organizations. The hacker is situated in, and constituted by, the minute auspices of the hack itself, thus producing its own subjectivity born of a deep situatedness in hacking praxis. The hack, in turn, destabilizes not only the exclusivity and propriety of the disclosed information, but of the legitimacy of the exercise of said exclusivity in the first place. It is not so much that the hack liberates information, but rather that it poses the question of why the information was contained and siphoned, corralled and shackled, through so-called legal and legitimate channels in the first place. The data leak, achieved via the hack, unbinds the presumed legitimacy of exclusivity, resulting in a questioning of the validity of the underlying processes of truth formation.

Feenberg, appropriating Foucault’s situated intellectual into the realm of a technical micropolitics, refers to Foucauldian specific intellectuals as “agents of transformations of networks [who] constitute a new class of heterogeneous engineers whose tactical labors extend the recognized boundaries of networks, often against the will of managers”<sup>88</sup>. Though whilst previously pointing out the possibility for the reterritorialization of the antiprogram, by way of the adoption of new better features through the inadvertent discovery of bugs or exploits, Feenberg nonetheless here does admit that those very same situated intellectuals, or innovators, may on the contrary ultimately engage in subverting the “boundary-drawing strategies of corporations or agencies employing their inventions”<sup>89</sup>. A particular example of this manifested subversion, borne of course out of the specificity of its particular workplace and knowledge-base surroundings, would perhaps be the WASTE darknet<sup>90</sup>. The WASTE

---

<sup>86</sup> *Ibid.*, p. 133.

<sup>87</sup> Brian Harvey. 1985. “What is a Hacker?”, in “Computer Hacking and Ethics” (ACM Select Panel on Hacking). <http://www.cs.berkeley.edu/~bh/hacker.html>.

<sup>88</sup> Feenberg, *op. cit.*, p. 123.

<sup>89</sup> *Ibid.*

<sup>90</sup> WASTE Development Team. 2003. WASTE. <http://waste.sourceforge.net/>.

application, in short, allowed trusted IPs to connect to one another and exchange data in the form of instant messages and files. The program required no centralized coordinating server, necessitating only that all users used the WASTE software, after which they could form networks of trusted peers. Should a peer become untrusted, a new network could be formed excluding the non-trusted peer, and so on. The WASTE application was developed by programmers working at Nullsoft. Less than a day after the program was posted, AOL, the parent company of Nullsoft, shutdown the official distribution website, stating that the distribution of the program had been done by unauthorized parties. The speculation being that AOL did not want to make public the inner workings of any potential filesharing technology which they could make proprietary and employ in their own products. WASTE, however, had been released under the General Public License, meaning that its source code was also made public, albeit for the aforementioned brief window of time. The result being that today, modified versions of the program (as well as developed forks thereof), are freely available from any number of code-sharing websites. Thus in WASTE we see the manifestation of the specialized hacker intellectual not only ‘detaching the power of truth’ from corporate hegemony of code ownership and proprietary software development, but of the literal redrawing of network boundaries, allowing anyone to freely partake in the WASTE darknet ecosystem, forming virtual unions of egoists of trusted peers who populate the darknet pool.

#### 1.2.4 Kristeva: The Dissident Intellectual

For Kristeva, the dissident intellectual is characterized by a constant and on-going will to subversion, an aesthetic marked by an “anarchist enthusiasm”<sup>91</sup> and aimed at a minute dissection of accepted authoritarian monoliths, a hacker mode of action involving the pouring over of social coda with the gleeful aim of bug discovery and successful exploit execution. In other words,

[t]his ruthless and irreverent dismantling of the workings of discourse, thought, and existence, is therefore the work of a dissident. Such dissidence requires ceaseless analysis, vigilance and will to subversion, and therefore necessarily enters into complicity with other dissident practices in the modern Western world<sup>92</sup>.

Kristeva delineates four types of then-existent dissidents: the rebel, the psychoanalyst, the writer, and the woman.

---

<sup>91</sup> Kristeva, “A New Type of Intellectual: The Dissident, *op. cit.*, p. 295.

<sup>92</sup> *Ibid.* p. 299.

Braidotti, however, goes on to point out that processes of identification, of becoming-woman for instance, nonetheless remain too mired in the sinkpit of anthropomorphism, “a more radical shift is needed to break from the latter and develop post-anthropocentric forms of identification”<sup>93</sup>, what Braidotti terms as becoming-imperceptible. This can be seen as a rejection of static, identity-based territoriality with clearly delineated, congealed actants. Imperceptibility instead affords antiprograms consisting of executed operant code themselves the agency of affecting change—the autonomous worms operating outside of the code authors’ control, and with polymorphic, self-mutating viruses now in vogue, outside of their original code formations as well. The dissident intellectual, in other words, is not only the writer but the ever-shifting being-written.

Going further however, imperceptibility has the additional tactical advantage of avoiding detection and hence apprehension and source neutralization. Whereas Stirner’s unions consisted of discrete, albeit self-developing, entities, the discrete topology involved nonetheless led to the arrest of various members of physical manifestations of unions of egoists—the Bonnot Gang, for instance. Similarly, it is those members of Anonymous who chose to make names for themselves, who chatted away in IRC channels and on Twitter feeds, that were arrested by State forces. What is thus emerging is an amorphous blending of Kristeva’s analysis of exile, a dissident act of uprooting, marked by constant meaning (re)creation through geographical transformation, with covert infiltration marked by the aforementioned clandestine development and release of WASTE darknet code by AOL employees. It is the formation tongs, “mutual benefit societ[ies] for people with a common interest which is illegal or dangerously marginal”<sup>94</sup>, marked by a transitory indeterminacy, a union of egoists becoming-imperceptible. Hacker groups avoiding detection by adhering to Bey’s espousal of the shift, “keep moving the entire tribe, even if it's only data in the Web”<sup>95</sup>, as evinced for instance by The Pirate Bay routinely shifting its domain name allocation to avoid seizure<sup>96</sup>. Thusly we find polymorphic virus code running amok. A lizard amongst the wires.

Kristeva’s observation of the potentiality of dissidence through the utilization of the overabundance of language, through the overloading of linguistic signification, “through the

---

<sup>93</sup> Braidotti, *op. cit.*, p. 168.

<sup>94</sup> Bey, *Immediatism*, *op. cit.*, p. 13.

<sup>95</sup> Bey, *T.A.Z.*, *op. cit.*

<sup>96</sup> Ernesto. 2013d. “Pirate Bay Moves to Guyana After Domain Suspension, 70 Domains to Go”. *TorrentFreak*. <http://torrentfreak.com/pirate-bay-moves-to-guyana-131218/>.



excesses of the languages whose very multitude is the only sign of life, one can attempt to bring about multiple sublations of the unnamable, the unrepresentable, the void. This is the real cutting edge of dissidence”<sup>97</sup>, can further be applied to programming language (especially when considering that Kristeva here makes no distinction between formal and natural languages, and thus there is no reason to assume inapplicability of her pronouncements to only one or the other). Whitespace, a particular esoteric programming language—so-called ‘esoteric’ languages being those which are precisely designed to test the limits of programming language construction<sup>98</sup>—that feeds on precisely such an overabundance. The entire syntax consists of spaces, linefeeds, and tab spaces—all ‘whitespace’ which shows up blank on a standard screen running software not designed to visually parse said input. Developed in 2003, whitespace builds on a Stroustrup’s observation five years earlier that C++ code could be made to act in particular ways by means of overloading the underlying code with excessive whitespace characters, in other words by utilizing overtly empty space by imbuing it with meaning.<sup>99</sup> Thus program communication and construction, lines of code, themselves become constituted by the whitespace void, the characters rendered unwanted and undesirable by traditional languages. Similarly, viral code which modifies itself to escape detection by anti-virus software exists on the cutting edge of Kristeva’s plane of dissonance by virtue of its disavowal of a static form.

#### 1.2.5 On the Emergent Non-Legalism

And it is here that we come to the third characteristic that we see emerge out of these varying discourses on intellectual dissonance. Alongside the aforementioned qualities of creativity and specialized expertise, which are also entirely in accord with qualities of the hacker and the hack, we now come to the third characteristic: that of non-legalism. A common refrain running throughout the afore-discussed approaches to the intellectual is that of a disregard, if not outright revolt against, legal barriers. Stirner at this stage sows the seeds of what would later blossom into a more developed theory of illegalism (and which will be discussed in some lengths later on), by merely pointing out that the intention of the realists is to produce “legal minds, not free ones”<sup>100</sup>. Similarly, Foucault observes that the situated

---

<sup>97</sup> Kristeva, *op. cit.*, p. 300.

<sup>98</sup> Michael Mateas. 2006. “Weird Languages”, in *Software Studies - A Lexicon* (ed. Matthew Fuller). 2008. Cambridge, MA: The MIT Press. pp. 267-275.

<sup>99</sup> Bjarne Stroustrup. 1998. “Generalizing Overloading for C++2000”. [https://www.cct.lsu.edu/~hkaiser/spring\\_2012/files/whitespace98.pdf](https://www.cct.lsu.edu/~hkaiser/spring_2012/files/whitespace98.pdf).

<sup>100</sup> Stirner, *op. cit.*

intellectual derives not from “the jurist or notable, but the savant or expert”<sup>101</sup>. Kristeva, likewise notes that “[a] playful language therefore gives rise to a law that is overturned, violated and pluralized, a law upheld only to allow a polyvalent, polylogical sense of play that sets the being of the law ablaze in a peaceful, relaxing void”<sup>102</sup>, which of course also parallels Stallman’s intonation that the characteristics of a hack are marked by “playfulness, cleverness, and exploration”<sup>103</sup>, with, it will surely be recalled, “little respect for the silly rules that administrators like to impose”<sup>104</sup>. It is with this tendency towards illegalism running throughout the operant discourses on intellectuals that we can now turn to the figure of the hacker proper, seeing as how, after all, “[t]he main characteristics of a hack are that it be simple, masterful and illicit”<sup>105</sup>. Our lizard running through the wire after all is engaged in an act of transgressive trespass, albeit made all the harder to apprehend by way of avoiding a tangible identity, instead thriving on a figurative imperceptibility, an eschewal of static form(ation) born of becoming-creative, as it were.

### **1.3 Anonymous Subjectivity: The Hack as a Rejection of Statist Stasis**

#### 1.3.0 Monstrous Unions

Having previously looked at the multifarious entwinement of Stirnerian notions of *personalism* and *illegalism* with operant modes of hacker methodology (marked, such as they are, by self-actualized development and transcendence of legalist normativity, respectively), there remains a third Stirnerian notion that I will argue is manifested within the hack as well, that of the *union of egoists*—a free-form, self-constructed, voluntary relationality formed amongst cognizant actants, or in Stirnerian parlance, egoism that readily manifests itself in, for instance, the shape of Anonymous hacktivist collectives<sup>106</sup>. Stirner defined the Union of Egoists via juxtaposition to the liberal project of subject construction. The State and the Church, for Stirner, are both interested in imposing group membership identity from the ground up by congealing a concrete form dubbed Man, marked by involuntary permanence, “so the State betrays its enmity to me by demanding that I be a man [...] it imposes being a man upon me as a duty. Further, it desires me to do nothing along with which it cannot last;

---

<sup>101</sup> Foucault, *op. cit.*, p. 128.

<sup>102</sup> Kristeva, *op. cit.*, p. 295.

<sup>103</sup> Stallman, *op. cit.*

<sup>104</sup> *Ibid.*

<sup>105</sup> Tim Jordan and Paul Taylor. 2004. *Hacktivism and Cyberwars: Rebels with a Cause*. London: Routledge. p. 7.

<sup>106</sup> See, e.g., Gabriella Coleman. 2014a. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. London: Verso.

so its permanence is to be sacred for me”<sup>107</sup>. The creation of State-based communities, with moral, civic subjects, is for Stirner the creation of immobile fettering which denies the individual the possibility of fostering a personalist self-actualization, that is to say egoism, “the State is a society of men, not a union of egos [...] therefore we two, the State and I, are enemies. I annihilate it, and form in its place the Union of Egoists”<sup>108</sup>. The union of egoists thus consists of free interactive agents who voluntarily decide to engage with, or conversely abstain from, one another.

As Stirner points out, however, the creation of the man in turn logically implies the existence of its negative, the un-man<sup>109</sup>. This latter figure being someone who looms at the edges of civilized society, who must always be reigned in and kept at bay via the imposition of state/church-sponsored moralism, as manifested through the threat of demonic forces in the church or the ruthless law breaker by the state. For Newman, “the un-man may be seen as a figure of resistance against the subjectifying power of Enlightenment humanism”<sup>110</sup>. The spell of essentialism is undone by bringing to the fore its latent foil, its malingering other without which the liberal subject, Man, would be unable to constitute itself. Newman’s key point seems to be that Stirner’s active introduction or fore-fronting of the unman into the discourse of subjectification serves to destabilize said subject formation via a repudiation of its inescapability—one, or to use Stirner’s vernacular, I, need not be Man; or in other words, the unman offers a way out of the confines of humanist subject formation. That this simple logical foil exists as a latent shadow in every discussion of the liberal subject is also what creates the possibility of a rejection thereof.

However, as Feiten points out, “Newman still pits the concept of un-man against that of man, only reversing the hierarchy, but Stirner abolishes the entire dichotomy”<sup>111</sup>. Stirner’s exaltation of personalism (or particularism), of uniqueness (or egoism), is only done so as to unravel the suffocating claims of the universalism of the liberal State subject, of Man. Feiten, although not expatiating his point at any length, is nonetheless certainly correct that Stirner ultimately rejects the un/unman binary, “[I] shall not ask henceforward whether I am man or

---

<sup>107</sup> Max Stirner. 1845. *The Ego and His Own* (trans. Steven T. Byington).

<http://www.df.lth.se/~triad/stirner/theego/theego.html>.

<sup>108</sup> *Ibid.*

<sup>109</sup> E.g., “*man* stands against *men*, or, as men are not man, man stands against the un-man” (*Ibid.*).

<sup>110</sup> Saul Newman. 2001. *From Bakunin to Lacan: Anti-Authoritarianism and the Dislocation of Power*.

Plymouth, UK: Lexington Books. p. 67. See also: Saul Newman. 2001. “Spectres of Stirner: a Contemporary Critique of Ideology”, in *Journal of Political Ideologies* 6.3. pp. 309-330.

<sup>111</sup> Elmo Feiten. 2013. “Would the Real Max Stirner Please Stand Up?”, in *Anarchist Developments in Cultural Studies* 2013.1: “Blasting the Canon”. p. 129.

un-man in what I set about; let this spirit keep off my neck”<sup>112</sup>, which is an ultimately entirely unsurprising outcome considering that, as Stirner repeatedly notes, “if the devil has been translated into the ‘un-man’ or ‘egoistic man’ – is the Christian less present than before”<sup>113</sup>? In place of the un/man, Stirner postulates the egoist; and in place of the State, composed as it is of men, there is the union of egoists. Thus, Newman’s observations still ring true, rendering Feiten’s reservations to be a seemingly semantic issue, perhaps resolved with a basic find-and-replace command over the former’s text with ‘unman’ changed to the ‘unique’, the ‘I’, the ‘egoist’, or to any number of other subject identification labels Stirner deploys at various times<sup>114</sup>. Indeed, even Stirner himself on occasion uses the terms unman/egoist synonymously, “liberalism as a whole has a deadly enemy, an invincible opposite, as God has the devil: by the side of man stands always the un-man, the individual, the egoist”<sup>115</sup>, which renders Feiten’s objection to the relatively superficial level of interchangeable nomenclature. For Stirner, the figure of the egoist merely exists as a foil, a signifying other which serves to highlight the possibility of things not as they are, of the existence of other formulations of social cohesion aside from the State, *viz.* a union of egoists freely interacting as self-constructed subjects as opposed to those under the weight of imposed subjectivity, the oppression brought on by being moral men.

Perhaps a part of the aforementioned categorical murkiness is due to Stirner’s resistance to modes of prescriptive conceptualization. As Newman notes, Stirner “puts forward, *tentatively* [emphasis added], certain suggestions of egoistic forms of association”<sup>116</sup>, as opposed to concretely. Unfortunately, for Newman this observation of Stirner’s ephemeral elucidation of the union of egoists leads him to deploy an apologist rhetoric of longing, repeatedly lamenting that “the social dimension of egoism is perhaps insufficiently elaborated and developed”<sup>117</sup>. Yet, whilst it is true that the union of egoists is only explicitly mentioned precisely twice in *The Ego and His Own*, Stirner discusses it in greater depth in a later essay, “Stirner’s Critics”<sup>118</sup>. Though the larger point may well be that Stirner intentionally avoids a prolonged blueprinting of the union of egoists precisely to avoid the

---

<sup>112</sup> Stirner, *The Ego and His Own*, *op. cit.*

<sup>113</sup> Stirner, *The Ego and His Own*, *op. cit.*

<sup>114</sup> E.g., ‘the individual’; ‘the real man’; ‘the unique’ (Stirner, *The Ego and His Own*, *op. cit.*).

<sup>115</sup> Stirner, *The Ego and His Own*, *op. cit.*

<sup>116</sup> Saul Newman. 2011. “Stirner’s Ethics of Voluntary Inservitude” in *Max Stirner* (Ed. Saul Newman). Palgrave Macmillan: New York. p. 205.

<sup>117</sup> Saul Newman. 2010. *The Politics of Postanarchism*. Edinburgh, UK: Edinburgh University Press. p. 160. See also: Saul Newman. 2010. “Voluntary Servitude Reconsidered: Radical Politics and the Problem of Self-Domination” in *Anarchist Developments in Cultural Studies* 2010.1: “Post-Anarchism Today”. p.43.

<sup>118</sup> Max Stirner. 1845. “Stirner’s Critics”. <http://theanarchistlibrary.org/library/max-stirner-stirner-s-critics>.

possibility of subject-congealment, of the erosion of the individualism of the egoist into a prescriptive and oppressive enclosure of not merely party politics but perhaps humanist subject-formation altogether, “the party ceases to be a union at the same moment at which it makes certain principles binding”<sup>119</sup>. Stirner is tentative indeed, so as to preclude the possibility of conceptual congealment. Whether the resultant brevity is a greater, even, or lesser detriment is, fittingly, an individual matter.

In mentioning the variety of terms Stirner at times deploys throughout his writing on the ephemeral figure of the egoist, there is one more nomenclatural pronouncement that we have here not yet mentioned that is of pivotal import. As Landstreicher points out, whilst ‘unman’ is the literal translation of the German *Unmensch*, the term also means monster<sup>120</sup>! Given this translation, it thus then becomes evident that Stirner explicitly escapes the humanist un/man binary. The egoist is thus not a simplistic negation of the (hu)man, but a polymorphous, monstrous aberration of the subject form. Crucially, Haraway deploys a similar vocabulary, observing that “[c]yborg unities are monstrous and illegitimate”<sup>121</sup>, and further marking Stirner as partaking in the co-creation of the vital tunnel (—) towards posthumanism.

Curiously, the same criticisms and misconceptions of Stirner’s notions made by his contemporaries, which were in turn rebutted by Stirner himself, are nonetheless still being made today. Responding to a critique by M. Hess, in 1845 Stirner seizes upon Hess for wanting see the “concept” of the union of egoists characterized on paper, that is to say written on and expatiated at length<sup>122</sup>. For Stirner, Hess’s main grievance here lies in thinking that the union of egoists is ‘nothing more than a concept’, to be written about and formalized, rather than played out through spontaneity. This is in turn why in lieu of obliging Hess with rigorous concept development, Stirner instead provides a myriad of lived examples of the union of egoists: children coming together on the street outside of Hess’s window to play a game, Hess meeting friends on the street who ask him to accompany him to a tavern, or, perhaps falling in love. Thus we here see the union of egoists identified as a lived experience, characterized by the underlying facets of voluntary association and self-organization, “the union of egoists is not a concept but a name used to refer to each of the particular instances

---

<sup>119</sup> Stirner, *The Ego and His Own*, *op. cit.*

<sup>120</sup> Wolfi Landstreicher. 2011. “Translator's Preface” in Max Stirner. 1845. “Stirner’s Critics”. <http://theanarchistlibrary.org/library/max-stirner-stirner-s-critics>).

<sup>121</sup> Haraway, “A Cyborg Manifesto”, *op. cit.*

<sup>122</sup> Stirner, “Stirner’s Critics”, *op. cit.*

of individuals acting together”<sup>123</sup>. We can thus read the union of egoists not a concrete conceptualization, a recipe for congealment of subjectivity, but as a *relational actualization*.

Interestingly, however, the union of egoists has been referred to as a concept both by Stirner’s critics<sup>124</sup> as well as by those who are more agreeable<sup>125</sup> which leads to a misunderstanding of the union of egoists as, at best, a theoretical tool or model for human model construction, as opposed to an attempted written explication of a *practiced* hybridity of form which eludes conceptual formalization, existing as it does as a bit of polymorphous code; shifting, adjusting, and dissolving at whim.

Such a potency of dissolution also appears to be a point of contention amongst Stirner critics. For instance, Franks points out, with all the pretense of exposing a buried truth imaginable, and this all despite Stirner making the impermanence of the union of egoists repeatedly overt<sup>126</sup>, that the union of egoists can be broken off when the enacted associations are no longer favorable to the participant egoists. As Stirner points out, innovation in group dynamics is of course anathema to upholders of the statist order of moral men, and thus it would come as not surprise to him that Franks then goes on to describe the union of egoists as a “collective of psychopaths, talking across each other but finding that their aggression against others provisionally pays off”<sup>127</sup>. Granted, Stirner veers on the verge of prescriptive prophesizing when he claims that the union of egoists, or members thereof, would not seek advantage at the expense of others due to the fact that others would no longer be ‘such fools’ as to allow others to do so<sup>128</sup>, but neither does Franks have any ground for presuming some unexplained a priori psychopathy. The union of egoists is marked by egoist indeterminacy, and thus by a vibrant potentiality that’s devoid of prescribed modes of subjectivity.

Ultimately, as Newman points out, the union of egoists “is a problematization of the binary of individualism and collectivism: the union, while it allows and encourages collective action, at the same time seeks to preserve and even enhance the autonomy and singularity of

---

<sup>123</sup> Wolfi Landstreicher. 2012. “Egoism versus modernity: John Welsh’s dialectical Stirner” in *Modern Slavery* 1, pp. 186-191. <http://modernslavery.calpress.org/?p=492>.

<sup>124</sup> “[H]is concept of a ‘Union of Egoists,’ [...] is an inadequate and implausible conception” (Jesse Cohn and Shawn Wilbur. 2003. “What’s Wrong With Postanarchism?” [http://theanarchistlibrary.org/library/Jesse\\_Cohn\\_and\\_Shawn\\_Wilbur\\_\\_What\\_s\\_Wrong\\_With\\_Postanarchism\\_.html](http://theanarchistlibrary.org/library/Jesse_Cohn_and_Shawn_Wilbur__What_s_Wrong_With_Postanarchism_.html) ).

<sup>125</sup> “[H]is alternative concepts of dialectical egoism: ownness, the unique one, and the union of egoists” (John F. Welsh. 2010. *Max Stirner’s Dialectical Egoism - A New Interpretation*. Plymouth, UK: Lexington Books. p. 54).

<sup>126</sup> E.g., “[I]nnovation is the deadly enemy of habit, of the old, of permanence” (Stirner, *The Ego and His Own*, *op. cit.*).

<sup>127</sup> Benjamin Franks. 2011. “The Politics of Postanarchism”, in *Anarchist Studies* 19 (1). Book Review. pp. 113-117 (p. 116).

<sup>128</sup> Stirner, “Stirner’s Critics”, *op. cit.*

its participants”<sup>129</sup>. Voluntary association, as opposed to coerced group membership born of, say, exultations of citizenship or attempted enforcement thereof via invocations of morality, thus preserves and accentuates personalist development whilst simultaneously allowing for vivacious group development, “bringing together disparate groups together to ‘unionize’ on a foundation of shared criminality”<sup>130</sup>. Here then we also see the re-introduction of previously-discussed Stirnerian notions of personalism and illegalism, now converging with the union of egoists to formulate, albeit tentatively to be sure, a methodology of the hack, of a continuous, unstable project of disassembling or ex-figuration—juxtaposed with a mere reconfiguring, for the hacker eschews the stagnation of stasis at all costs.

### 1.3.1 Anonymous Unions

Anonymous, a mass, loose-knit conglomeration of “groups of hackers, technologists, activists, human rights advocates, and geeks”<sup>131</sup> responsible for a variety of cyber interventions (or ‘ops’) against the likes of the Bank of America, Paypal, and the Church of Scientology, is described by Milan as “a wave of movement activity that is virtual, distributed, and individualized”<sup>132</sup>, which is nuanced by Coleman as being “not a united front, but a hydra, a rhizome, comprising numerous different networks and working groups that are often at odds with one another”<sup>133</sup>. Thus Anonymous is not a single wave, but a cascade of crashing waves; indeed, a veritable temporary tempest which threatens to do away (‘annihilate’ perhaps, if we return to Stirner’s fitting description of the union of egoists) the stifling society of congealed subjectivity erected by the State. Indeed, much like Stirner’s union of egoists is not a static concept but rather a descriptor of immediacy, of carried-out actionality, so too does Coleman stress that the very term Anonymous is mobilized purely to conduct actual actions, as opposed to existing in the realm of conception<sup>134</sup>.

---

<sup>129</sup> Newman, “Stirner’s Ethics of Voluntary Inservitude”, *op. cit.*

<sup>130</sup> Allan Antliff. 2011. “Anarchy, Power and Post-Structuralism” in *Post-Anarchism - A Reader* (Eds. Duane Rousselle and Süreyya Evren). New York: Pluto Press. p. 162.

<sup>131</sup> Gabriella Coleman. 2012b. “Our Weirdness Is Free, The logic of Anonymous—online army, agent of chaos, and seeker of justice” in *May* 9, p. 83. <http://gabriellacoleman.org/wp-content/uploads/2012/08/Coleman-Weirdness-Free-May-Magazine.pdf>.

<sup>132</sup> Stefania Milan. 2013. “Wikileaks, Anonymous, and the Exercise of Individuality: Protesting in the Cloud” in *Beyond Wikileaks: Implications for the Future of Communications* (eds. Benedetta Brevini, Arne Hintz, Patrick McCurdy). New York: Palgrave Macmillan. p.203. Note how the fluid, aquatic discourse surrounding Anonymous is also seen in a recent *Wired* article: “The collective has ebbed and flowed over the years, taking long breaks between attacks” (Kim Zetter. 2014. “Is Anonymous Dead, or Just Preparing to Rise Again?” *Wired*. <http://www.wired.com/2014/06/anonymous-sabu/>).

<sup>133</sup> Coleman, *op. cit.*, p. 92.

<sup>134</sup> Gabriella Coleman. 2011. “Anonymous: From the Lulz to Collective Action”, <http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action>.

Whilst pointing out that Anonymous is guided by notions of innovation, skill, and playfulness<sup>135</sup>, thus echoing various elucidations of the hacker ethic we have previously mentioned by, say, Levy and Stallman, Coleman is nonetheless also highlights that Anonymous is categorized by—an often clashing—plurality of forms and practices. Indeed, Coleman is careful to point out that hacking itself is marked not by any singular domineering conceptualization, of a lone crystallized ‘hacker ethic’, but is instead comprised of “multiple origins, distinct lineages, and variable ethics”<sup>136</sup>. A multifarity of purpose and tactic which lends itself to an ephemeral immediatism, an in-the-moment transience in lieu of a stale, congealed politics. Anonymous’ actions, for instance, are often decided as spur of the moment reactions to passing bits of current events. For instance, the digital dissension against the Bank of America and Paypal were prompted after Wikileaks posted that their accounts had been frozen<sup>137</sup>. Meanwhile, from a technical perspective, Distributed Denial of Service (DDoS) attacks could only be mounted when those who have the underlying botnet architecture are available to lend their services; though these particularisms were themselves augmented when, in turn, other Anonymous members devised a mass-participatory DDoS tool dubbed the Low Orbit Ion Cannon (LOIC)<sup>138</sup>, though the success of these actions were likewise predicated on other members of Anonymous voluntarily downloading and running the tool. Thus participation in Anonymous actions is utterly voluntary and transitory. Anonymous hacker congregate together in digital renditions of the union of egoists, and enact joint actions for as long as each member sees fit before disassociating from the union.

Despite the fact that there have been some discrete individuals associated with Anonymous, though, notably, at times these associations have only become explicit when the individuals turned against Anonymous, as for instance the case of Sabu who, admittedly despite already being a prominent member of Anonymous, nonetheless gained more notoriety when he became an FBI informant<sup>139</sup>, Anonymous nonetheless generally functions by propagating the union and its resultant actions itself, as opposed to the discrete individuals

---

<sup>135</sup> Gabriella Coleman. 2012a. “Am I Anonymous?” in *Limn 2: “Crowds and Clouds”*, <http://limn.it/am-i-anonymous/>.

<sup>136</sup> Gabriella Coleman. 2014b. “Hackers”, in *The Johns Hopkins Encyclopedia of Digital Textuality*. Forthcoming. <http://gabriellacoleman.org/wp-content/uploads/2013/04/Coleman-Hacker-John-Hopkins-2013-Final.pdf>.

<sup>137</sup> WikiLeaks. 2010. “Global - PayPal freezes WikiLeaks donations”. WikiLeaks. <https://www.wikileaks.org/PayPal-freezes-WikiLeaks-donations.html>; WikiLeaks. 2011. “Wikileaks: Banking Blockade and Donations Campaign”. WikiLeaks. <https://wikileaks.org/IMG/pdf/WikiLeaks-Banking-Blockade-Information-Pack.pdf>; Coleman, *Hacker, Hoaxer, Whistleblower, Spy*, *op. cit.*, pp. 123-127.

<sup>138</sup> Praetox and abatishchev. 2010. Low Orbit Ion Cannon (LOIC). <http://sourceforge.net/projects/loic/>.

<sup>139</sup> E.g., Kim Zetter. 2012. “LulzSec Leader Was Snitch Who Helped Snag Fellow Hackers”. *Wired*. <http://www.wired.com/2012/03/lulzsec-snitch/>.



involved therein. Thus Anonymous can indeed ultimately be said to move past the wars of subjectivity waged by Stirner, wherein personalist self-formation was pitted against statist prescription of citizenship, to what Braidotti termed as one of the characterizations of the posthuman, namely that of *becoming-imperceptible*, but simultaneously whilst partaking in a union of egoists, being a cyber manifestation of illegalist praxis. A dis-identification marked by porous transversality; achieved by hackers not only by ever-shifting subject formations, but through the literal boundary-crossing by the hack itself, an eschewal of borders marked by unsanctioned access and dissection, which in turn serve to effect an ultimate erosion of stasis.

#### **1.4 Participatory Action Research and Knowledge Propagation**

Aside from the previously discussed influences of Actor Network Theory, various conceptualizations of the intellectual, and their interactivity with notions of the hack/er, another approach which together with the aforementioned areas formulates our resultant hacker methodology is Participatory Action Research (PAR), albeit with a strand of a piratical, (intermittent and noncommittal) non- or post-humanism added to the mix.

##### **1.4.0 Approximating PAR**

In the 1980s, PAR was described as “a form of collective self-reflective enquiry undertaken by participants in social situations in order to improve the rationality and justice of their own social or educational practices, as well as their understanding of these practices and the situations in which these practices are carried out”<sup>140</sup>, developing in the 1990s to “the systematic collection of information that is designed to bring about social change”<sup>141</sup>, and becoming still further refined in the 2000s to “[d]efined most simply, PAR involves researchers and participants working together to examine a problematic situation or action to change it for the better”<sup>142</sup>. Thus the research undertaken under the umbrella of PAR is not an aloof quantitative extrapolation of an esoteric dataset wholly divorced from any manner of practical praxis, but is instead firmly intertwined with, and indeed foregrounded by, active constituency within the involved populace. In other words, the researcher is by no means some sort of illusory detached observer of some selected community sample set but is instead

---

<sup>140</sup> Stephen Kemmis and Robin McTaggart (eds.). 1988. *The Action Research Planner*. Victoria, Australia: Deakin University Press. p. 5.

<sup>141</sup> Robert Bogdan and Sari Knopp Biklen. 1992. *Qualitative Research for Education*. Boston, MA: Allyn and Bacon. p. 223.

<sup>142</sup> Sarah Kindon, Rachel Pain and Mike Kesby (eds.). 2007. *Participatory Action Research Approaches and Methods: Connecting People, Participation and Place*. New York: Routledge. p. 5. See also: Yoland Wadsworth. 1998. “What is Participatory Action Research?”. *Action Research International*, Paper 2. <http://web.archive.org/web/20090205153046/http://scu.edu.au/schools/gcm/ar/ari/p-ywadsworth98.html>.

an active participant therein. Borne of this participation is an ingrained emphasis on motion, a constant state of activity or action which strives to utilize the accumulated research for viable, affirmative, and change-achieving outcomes. In other words, while PAR certainly takes research gathering seriously, the R is not allowed to subjugate the P and A, and is on the contrary reined in; if not quite in the service thereto, then certainly in tandem therewith. There then arises a sort of alphabetic equilibrium—or in terms of negation, there is here a total lack of acrimony within the PAR acronym.

To put the letters' interdependent interlocution in the singsong, enchanting vernacular of PAR-based metaphysical ethnochoreology—a sort of descriptive ethnography of the intricate dance PAR participants partake in, as Reason and Bradbury do:

[w]e live in a participatory world. There is a primordial givenness of being in which the human bodymind actively participates in a co-creative dance which gives rise to the reality we experience [...] As we are part of the whole we are necessarily actors within it, which leads us to consider the fundamental importance of the practical<sup>143</sup>.

Given the always-somewhere embeddedness of researchers, it seems that they cannot help but also be active participatory actors within their communities, with no pretensions of academic isolationism. Instead PAR draws a certain overlap with what in the aesthetic realm Hakim Bey termed an immediatism—a rejection of mediation and separation brought about by capital and other oppressive forces in favor of an immediate, playful interaction among all actors<sup>144</sup>. Thus, much like since “[f]or art, the intervention of Capital always signals a further degree of mediation”<sup>145</sup>, immediatism logically eschews capital, so too would “a committed PAR researcher/activist would not want to help those oligarchical classes that have accumulated capital, power and knowledge thus far and so recklessly”<sup>146</sup>. The PAR researcher/activist can here be seen to be orthogonal to Stirner's formulations of modes of erudition, intersecting as it does both with Stirner's realists—for on the one hand PAR is firmly grounded in pragmatic community-centered action—but also explicitly avoiding the realist trap of stasis, instead here finding its affinity with the ephemeral, momentary coming together of personalist egoists. Though the prerequisite conditions for such a union are not

---

<sup>143</sup> Peter Reason and Hilary Bradbury (eds.). 2001. *Handbook of Action Research: Participative Inquiry and Practice*. London: Sage Publications. p. 8.

<sup>144</sup> “[I]t may take the form of any kind of creative play which can be performed by two or more people, by & for themselves, face-to-face & together” (Hakim Bey. 1994. *Immediatism*. Edinburgh, Scotland: AK Press. pp. 10-11).

<sup>145</sup> *Ibid.*, p. 7.

<sup>146</sup> Orlando Fals-Borda and Muhammad Anisur Rahman (eds.). 1991. *Action and Knowledge: Breaking the Monopoly with Participatory Action-Research*. New York: The Apex Press. p. 29.

generally explicitly articulated by PAR proponents, as they are by Stirner in regard to his emphasis of the need for personal actualization as an *a priori* condition for any subsequent union formation.

By now we can then see a key, emergent operant tenet of the PAR tradition within which this project is situated—a disintegration of the illusory segregation of participant-researcher in favor of research-as-co-participant deeply enmeshed in the particular community-praxis area of focus. Yet a deep-rooted commitment to action is itself insufficient. For while some PAR introductions do state that “Practitioners of PAR engage in a variety of research projects, in a variety of contexts, using a wide range of research practices that are related to an equally wide range of political ideologies”<sup>147</sup>, with those in the “action research family [...] pursuing different political commitments”<sup>148</sup>, the variant politics nonetheless all coalesce around aiding those who are oppressed by the dominant, operating power(s). Hence, “[t]his experiential methodology implies the acquisition of serious and reliable knowledge upon which to construct power, or countervailing power, for the poor, oppressed and exploited groups and social classes—the grassroots—and for their authentic organizations and movements”<sup>149</sup>. Given that PAR can here be seen to express a clear “recognition that all research methodologies are implicitly political in character, defining a relationship of advantage and power between the researcher and the researched”<sup>150</sup>, it then further adopts an explicit political positioning in siding with the dispossessed, the “subordinate classes”<sup>151</sup>. The reason for this clarification via political distillation is that while, say, the academics involved in the development of shipboard lasers for missile defense can certainly be said to have a deep commitment to participatory action and research, what with being fully enmeshed in the surrounding military industrial complex cum educational communities, replete with government funding, and with being fully devoted to actual deployment of said missile systems, their work will nonetheless likely not be appearing in (nor likely submitted to) any upcoming compendium of PAR scholarship. PAR appears to here be influenced by Gramsci’s notion of the organic intellectual, and thus, like Gramsci, appears to nonetheless

---

<sup>147</sup> Alice McIntyre. 2008. *Participatory Action Research*, Qualitative Research Methods Series 52. London: Sage Publications. p. 1.

<sup>148</sup> Reason and Bradbury, *op. cit.*, p. xxiv.

<sup>149</sup> Fals-Borda and Rahman, *op. cit.*, p. 3.

<sup>150</sup> Robin McTaggart (ed.). 1997. *Participatory Action Research: International Contexts and Consequences*, SUNY Series: Teacher Preparation and Development. Albany, NY: State University of New York Press. p. 1.

<sup>151</sup> Fals-Borda and Rahman, *op. cit.*, p. 30.

restrict its ‘co-creative dance’ to a pre-delineated set of dance partners, restraining its potency for contesting class-based politics altogether, of going beyond class-based congealment.

Within existent PAR scholarship, there is further a quibble as to what precisely actually constitutes ‘participation.’ McTaggart notes the emancipatory, empowering self-reliant undertaking of PAR: “participatory action research is research done by the people for themselves”<sup>152</sup>, or as Rahman puts it, PAR actants learn “to know and recognize themselves as a means of creating people’s power, and the internal and external mechanisms of countervailing power”<sup>153</sup>. Thus participation is conducted by co-constituents of the active community, who take on the dual role of participant-researcher. Here one once again can recall a striking parallel to Bey’s immediatism, as the bootstrapped ground-up participatory research has a certain similar ring to it as the DIY punk aesthetic of the zine scene, “[t]he mail art of the ‘70s & the zine scene of the ‘80s were attempts to go beyond the mediation of art-as-commodity, & may be considered ancestors of Immediatism”<sup>154</sup>, though while Bey paradoxically appears to at the same time not realize the interactivity of the participants involved in the act, being wedded to a singular notion of connectivity as corporeal, “they preserved the mediated structures of postal communication & xerography, & thus failed to overcome the isolation of the players, who remained quite literally out of touch”<sup>155</sup>, it can nonetheless be pointed out that those who are involved in PAR research generally immediately linked to their focal communities, being *of* them as opposed to merely *observant of*. The immediacy of PAR is thus here linguistically manifested by a distinct, and indeed pivotal, absence of prepositional qualifiers. Lest the project is here misconstrued as crassly attempting to simply graft PAR with immediatism, it must then be stated that we are here operating with a broader definition of the term than that afforded to us by Bey’s confining preoccupation with meatspace congealment: being immediate in a community is not dependent on spatial, but rather on participatory, coordinates.

Immediate, in the sense of direct as opposed to detached, participation (ideologically, versus spatially) is thus pivotal to orchestrating a PAR-based project. Yet there is still here a danger of the possibility of a sort of co-option, a clinging-on through an attachment that masquerades itself under the venerable veneer of full-throttle participation while indeed being naught but a tepid toe-dipping for purposes of common adornment to later deploy for

---

<sup>152</sup> McTaggart, *op. cit.*, p. 5.

<sup>153</sup> Fals-Borda and Rahman, *op. cit.*, p. 7.

<sup>154</sup> Bey, *Immediatism, op. cit.*, p. 11.

<sup>155</sup> *Ibid.*, p. 12.

self- or state- (or corporate-) interest. Communal engagement versus corporate affiliation for purposes of image enhancement and tax opportunities, say. Thus McTaggart is sure to draw out this caveat by elucidating a clear-cut bifurcation between participation and involvement:

[a]uthentic participation in research means sharing in the way research is conceptualized, practiced, and brought to bear on the lifeworld. Mere involvement implies none of this, and creates the risk of co-option and exploitation of people in the realization of the plans of others<sup>156</sup>.

What McTaggart is here elucidating is that the mere infiltration—or perhaps a specific, more malignant and nefarious manifestation of infiltration, that of *injection*—of, say, a government or corporate agent-with-agenda into a specified community setting with the intent of meddling with the community to meet corporate, government, vested corpo-government or any other top-down formulation-as-imposition may certainly technically involve involvement, in the sense that the agent is indeed involved with the community, and the community is in turn *involuntarily* involved with the agent, this sort of imbalanced relationship should by no means be equivocated with actual voluntary, bottom-up, community-borne participation of the sort that truly constitutes successful PAR, and which would likewise potentially be exhibitiv of a Stirnerian union of egoists. Actual participants are not alphanumeric informants duly indexed in the appendices of a government report or corporate-sponsored study, but are instead research-producing equals who both constitute and conceptualize the actual project in its entirety.

Not only then does PAR indeed then offer “a multidimensional approach to research that intentionally integrates participants’ life experiences into the research process”<sup>157</sup>, but, lest the aforementioned integration be misconstrued as being conducted by some sort of external agent, it then merits explicit notation that PAR on the contrary facilitates a self-integration due to the fact that that the participants are indeed also the researchers. McIntyre, affirming and expanding upon McTaggart’s aforementioned distinction between active participation and mere involvement, notes that “I agree with that distinction and further argue that what is important to and in a PAR project is the *quality* of the participation that people engage in, not the proportionality of that participation”<sup>158</sup>. As McIntyre nonetheless still mysteriously chooses to maintain a distinct binary of researcher and participator, for her ‘quality’ here seems to mean that the latter have an equal say in the developing project, “[i]n

---

<sup>156</sup> McTaggart, *op. cit.*, p. 6.

<sup>157</sup> McIntyre, *op. cit.*, p. xiv.

<sup>158</sup> *Ibid.*, p. 15.

other words, to take joint responsibility for developing the *group's* version of what it means to participate in a PAR process"<sup>159</sup>. Which is to say quality for McIntyre appears to be achieved via collective participatory equilibrium borne of consensus-based mutual decision-making and project-shaping.

The aforesaid, strongly participatory, all-involving communal tendency of PAR in turn leads to a focus on viable actions that can be conducted. Thus McIntyre notes that one of the underlying tenets of PAR is "a joint decision to engage in individual and/or collective action that leads to a useful solution that benefits the people involved"<sup>160</sup>, while Reason and Bradbury state that "[t]he first purpose is to bring an action dimension back to the overly quietist tradition of knowledge generation which has developed in the modern era. The second is to loosen the grip over knowledge creation held traditionally by universities and other institutes of 'higher learning'"<sup>161</sup>. In keeping with the tenet of engaging in actual actions with tangible benefits to those involved and thus bringing back an 'action dimension' to knowledge generation, and with the further aim of spreading the potentiality of knowledge creation, this *Operations Manual* will likewise engage in various actions throughout its corpus along the lines of liberating academic journal articles and cinematic films and providing potentially viable distribution vectors for their free propagation. For the university is not only guilty of knowledge creation as such, but also of walled-off knowledge accumulation—information locked away in closed library archives and/or under cost-prohibitive paywalls and private intranets, at times even inaccessible to students therein. To unclasp the bear trap of academia around the bleeding ankle of available information thus seems to be quite a logical extension of ground-level PAR principles. The *Operations Manual* itself will of course also be freely available itself.

#### 1.4.1 Case Study 1: Goldsmiths Research Online (GRO)

To briefly test out PAR's deep-rooted commitment to participatory action and self-reflexivity, let us now take a brief excursionary aside via a case study-based foray into an academic knowledge-accumulation database directly affecting the participant in this project which will hopefully bring to the fore the effects of university-gripped knowledge production and dissemination on not only those outside of the walls of academe, but of those presumably on the inside as well. "Goldsmiths Research Online is a repository of research publications

---

<sup>159</sup> *Ibid.*

<sup>160</sup> *Ibid.*, p. 1.

<sup>161</sup> Reason and Bradbury, *op. cit.*, p. xxiii.

and other research outputs conducted by academics at Goldsmiths”<sup>162</sup>. The repository accepts material along the lines of theses, book chapters, visual artworks, and the like, with the explicitly self-stated intention of the archive being “to provide long-term, public, free access to these materials on the web”<sup>163</sup>. In other words, if there is a publication by an academic whose credentials appear in, say, an author affiliation or biography section of a book or journal and bear the pivotal marker of affiliation dubbed ‘Goldsmiths’, it then stands to reason that one might chance to find said publication (and indeed perhaps even *this* publication) on the public-facing GRO site, irrespective of one’s actual affiliation with either the researcher or the institution. In other words, there is no overt claim being made here by the GRO regarding the restriction of access to any potentially unaffiliated parties, there is only the notion of seemingly unbridled—‘long-term, public, free’—allowance.

To wit, one of the potential articles of interest for this *Operations Manual* is an article entitled “‘We are all hackers now’: critical sociological reflections on the hacking phenomenon”<sup>164</sup>, written by one Brian Alleyne, Senior Lecturer at Goldsmiths, College of London. Given that our conditional construct is thus initially met (*if* a researcher at Goldsmiths has a publication, *then* it (may) be available on the GRO), we can traverse the digital terrain over to <http://eprints.gold.ac.uk/>, perform a basic look-up query for the title (or keyword, allowing for an inexact search form), and see if we can gain access to said research. Though the search query was indeed successful, in that said article is indeed listed in the GRO, seemingly complete with an actual download link, the situation nonetheless becomes troubled, or complicated.

A seemingly straightforward download link is encountered:

Download (769Kb)

Hovering over said hyperlink, a—once again, seemingly straightforward—Uniform Resource Locator (URL) appears to be presented:

[http://research.gold.ac.uk/6306/1/Alleyne --We are all hackers now - critical sociological reflections on the hacking phenomenon.pdf](http://research.gold.ac.uk/6306/1/Alleyne--We%20are%20all%20hackers%20now%20-%20critical%20sociological%20reflections%20on%20the%20hacking%20phenomenon.pdf)

In viewing the page source code however, certain hitherto hidden parameters are revealed:

---

<sup>162</sup> Goldsmiths, University of London. 2012. “About – Goldsmiths Research Online”. <http://eprints.gold.ac.uk/information.html>.

<sup>163</sup> *Ibid.*

<sup>164</sup> Brian Alleyne. 2011b. “We are all hackers now”: critical sociological reflections on the hacking phenomenon”. Under Review. pp. 1-28. <https://eprints.gold.ac.uk/6306/>.

```
<a href="http://eprints.gold.ac.uk/6306/1/Alleyne--We_are_all_hackers_now_-_critical_sociological_reflections_on_the_hacking_phenomenon.pdf" onclick="javascript:pageTracker._trackPageview( '6306/1/Alleyne--We_are_all_hackers_now_-_critical_sociological_reflections_on_the_hacking_phenomenon.pdf' );">Download (769Kb)</a>165.
```

pageTracker and trackPageview functions being symptomatic of the deployment of Google Analytics (confirmed by further review of the site code), GRO is thus now revealed to be utilizing a site usage tracking mechanism, and being one operated by a third party, thus sharing the data with them, with no clear notification of the user that said tracking behavior is on-going. Irrespective of the unaccounted for tracking metrics, however, the URL should nonetheless take us to the resultant Portable Document Format (PDF) file which, if filenames are to be taken as authentic markers of expectancy, should in turn contain the requisite article. And yet, upon clicking said link we are redirected to a simple login page which curtly and abruptly, politely enquires of us a Username and Password. The interpretive expectancy of seeing a PDF is thus shattered by the presentation of an impromptu gatekeeper. The shift from expectancy to reality-manifestation, from almost-content-acquisition to stark deprivation is rendered all the greater by the repository's intention of providing, as will doubtlessly be recalled, "long-term, public, free access"<sup>166</sup>. Said login page further provides neither no indication of which existent login/password combination a user can use (perhaps, one may think, 'if the site is already entangled with Google, I should just try signing up for a Gmail account and then use that?'), nor any option to create an account either (neither for free nor for even any listed sum). Thus one is effectively, and inexplicably, locked out of access to a bit of knowledge under the firm, yet apparently (illusively) open, grip of the university.

Exploring the matter further, we find that the page also indeed clearly states "Permissions: GRO Registered Users Only", which not only seemingly goes against the repository's own stated intentions, but also as mentioned provides no seeming ability to register with said GRO. There is, however, a link to another version of said article which redirects to a webpage whose link behavior does perform as expected, linking to a freely-

---

<sup>165</sup>Goldsmiths, University of London. 2013. HTML source code of Brian Alleyne. 2011b. "'We are all hackers now': critical sociological reflections on the hacking phenomenon", *op. cit.*

<sup>166</sup>"About - Goldsmiths Research Online", *op. cit.*



viewable PDF of the article<sup>167</sup>, albeit with a running page watermark which states “Under Review”, and the precondition, presumably from the author, stating “Draft under review; I may make further changes”, whilst the inaccessible (to us) version is qualified with “as submitted [sic] to journal”. In other words, the potentially rough-shot pre-revision draft is freely given, whilst the officiated published version is enclosed in the academic enclave of proprietarian knowledge-management.

Perhaps, at the least, the published version may be accessible to those with a Goldsmiths-affiliated login, (with the strand of reasoning we are following here being that seeing as there are no apparent links to become a Registered GRO User, perhaps those affiliated with Goldsmiths-based research are de facto users). Alas, upon trying to login with my own Goldsmiths login, I am greeted with a stop-hand icon and a red-tinged “Incorrect username or password” admonition. This rejection is rendered particularly quizzical by the fact that not only, according to the GRO, do “[s]ome departments also encourage research students to use GRO themselves and deposit other materials”<sup>168</sup>, but “PhD research students are required, from September 2009, to deposit both a print and an electronic copy of their completed thesis”<sup>169</sup>. Thus the full absurdity, and within that absurdity a buried malignity, of the university’s grip on knowledge creation is here inadvertently brought to the fore. For if on the one hand PhD students are required to deposit copies of their completed thesis, but on the other hand do not have a working login and password to do so, then matriculation becomes quite literally an impossibility, resigning the PhD student to a perpetual state of candidacy, pending some sort of expiration of even said candidacy status. Thus, in going through the sample motions of the PAR research cycle of questioning, reflecting, investigating, refining<sup>170</sup>, a continual process of the ever-developing hack in other words, we have arrived at a number of noteworthy discoveries. First and foremost, if a certain instance of a desired object is rendered inaccessible, even by what are explicitly meant to be overtly open systems, there may nonetheless be another (though perhaps incomplete) version still available. What was questioned was thus the availability of the article at hand, followed by reflection on possible access vectors to said article and the subsequent investigation thereof,

---

<sup>167</sup> Brian Alleyne. 2011a. “‘We are all hackers now’: critical sociological reflections on the hacking phenomenon”. <https://eprints.gold.ac.uk/6305/>.

<sup>168</sup> Goldsmiths, University of London. 2012. “Deposit Guide – Goldsmiths Research Online”. [https://eprints.gold.ac.uk/deposit\\_guide.html](https://eprints.gold.ac.uk/deposit_guide.html).

<sup>169</sup> *Ibid.*

<sup>170</sup> McIntyre, *op. cit.*, p. 7.

and finally a refining of our acquisition methodology to, luckily in this case, obtain an alternate version for usage in said *Operations Manual*.

In reading the Deposit Guide of the GRO however, several other items of note emerge. While PhD students are explicitly required to deposit copies of their theses, the Deposit Guide only explicitly mentions the granting of upload access to the repository for a specific sub-set of those affiliated with the university—*viz.* “All Goldsmiths academic staff may use the repository to deposit materials”<sup>171</sup>. Neither non-academic staff, nor any manner of student (PhD or otherwise) are mentioned in the Deposit Guide at all. The paradoxical exclusion of course stifles the potentiality of content submission, while paradoxically simultaneously requiring PhD students to submit their theses. Or in other words: PhD students are *required but not permitted* to submit their materials, while academic staff are *permitted but not required* to submit theirs. The resultant conditional disjunction operates as an inadvertent tool of academic knowledge suppression. Said suppression recalls our prior discussion of Foucault’s analysis of knowledge/truth production<sup>172</sup>, with the creation of the ‘academic’ knowledge being confined to closed online domains, thus in turn perpetuating an accessibility only for others within the allowed network, and in turn generating a likewise closed knowledge system. Going still further however, those who do have the power to submit also apparently have the power to control access to what is explicitly defined (as will doubtlessly be recalled once more) as a “long-term, public, free access” repository. Firstly, the Deposit Guide states that “Items that you are live on Goldsmiths Research Online are in the ‘Live Archive’ area and can be viewed or hidden by ticking and unticking the box alongside it”<sup>173</sup>, though granted it is here unclear whether *hidden* means that the item is simply hidden from view of (just) the uploader (who presumably may not wish to see their own uploads), or hidden altogether from public view (whilst remaining visible to just the uploader), or perhaps hidden entirely from anyone.

Furthermore, the Deposit Guide has a whole section devoted to setting further permissions for the accessibility of the uploaded data, a strange range of options indeed for a site allegedly interested in propagating free unimpinged data access. Specifically, the site states that “[i]f you have uploaded a file, you will be prompted for more information and you will be able to set restrictions on access to the file”<sup>174</sup>, with the restrictive options allowing

---

<sup>171</sup> “Deposit Guide”, *op. cit.*

<sup>172</sup> Foucault, “Truth and Power”, *op. cit.*

<sup>173</sup> *Ibid.*

<sup>174</sup> *Ibid.*

the uploaded material to be viewable only by “registered users” or “repository staff”. To the repository’s credit, it is also stated that “[t]he preferred option is to make the file publicly available by selecting ‘Anyone’”<sup>175</sup>, though this mild invitation does not by any manner explain away the existence of other closed-access options on a site explicitly paying lip-service to its alleged open availability of content. Thus in examining a small initial test case of the potentiality of practical action within a given research project which immediately affects the lives of the participant-researcher(s) involved, we discovered existent incongruities between the stated goals and the actual outcomes of a particular portal which negotiates the public’s access to university-controlled knowledge dissemination (or lack thereof, as the case may be). Given the discovery of the existence of such gatekeepers, therefore, the next future steps in the recursive PAR cycle involve developing a new plan for the liberation thereof.

To return for the moment, however, to the theoretical underpinnings of PAR, it is pivotal to point out that “the primary purpose of action research is not to produce academic theories based on action; nor is it to produce theories about action; nor is it to produce theoretical or empirical knowledge that can be applied in action; it is to liberate the human body, mind and spirit in the search for a better, freer world”<sup>176</sup>. Thus the primary underpinning of PAR is *emancipatory* (indeed, it is doubly emancipatory for our purposes when it is itself emancipated from humanist constriction, as it would be erroneous to assume that a community is made up solely of human actants), not to be subjugated to the academic realm of theoretical posturing. Reason and Bradbury further elucidate that PAR is “also about creating new forms of understanding, since action without reflection and understanding is blind, just as theory without action is meaningless”<sup>177</sup>. Thus the theorizing emerges from the active praxis, and is indeed intertwined within. While the resultant *Operations Manual* does at times incorporate theoretical texts, and is indeed itself enmeshed in the traditional PAR-based theorization of research praxis being borne of “everyday experience”<sup>178</sup>, the aim is never to utilize the actual operations or actions in the service of theoretical formulations, to use practice to buttress theory in other words, but instead to use theory in the service of effecting (or at least vehemently striving to effect) viable world change through community-based action.

---

<sup>175</sup> *Ibid.*

<sup>176</sup> Reason and Bradbury, *op. cit.*, p. 2.

<sup>177</sup> *Ibid.*

<sup>178</sup> *Ibid.*

The A is meant to remind the budding PAR-actioner that there is a certain immediacy inherent to any undertaken PAR-based project, “the term action is important to the extent that it reminds people that it is participants’ own activities which are meant to be informed by the ongoing inquiry, not merely the future research directions of external researchers”<sup>179</sup>. Thus the on-going research must be constantly interlaced with actual practice, leading indeed to an informed, active practice with a developing consciousness of the material, cultural and political underpinnings of the realm in which said research occurs. As Rahman put it, “[a]t the micro level, PAR is a philosophy and style of work with the people to promote people’s empowerment for changing their immediate environment—social and physical—in their favor”<sup>180</sup>. But whilst a researcher at, say, Kodak who has just published on developing a refined watermarking technology for tracking cinematic film prints could be said to be effectuating change in their immediate environment for the favor of their employer, and by economic proxy, for themselves, PAR is based on action explicitly by those who are being subjugated, the oppressed and the dispossessed, not by the dominant corporate or government interests.

As PAR avoids a singular overarching methodological framework, “as it is a worldview which manifests as a specific set of practices which emerge in the interplay between action researchers, context and ideas”<sup>181</sup>, it instead adopts recursive process of questioning, reflecting, investigating, implementing, refining<sup>182</sup>. Furthermore, as McTaggart points out, the application of already-existent research in new situations may prove to be inadmissible, leading to the necessity of developing ever-new specificities of method, being intrinsically tied to the particular study being undertaken in a given instance<sup>183</sup>.

Yet despite the ensuing diversity of PAR-based methodologies, we see certain particular commonalities emerge in regards to the aforementioned DIY-strand of approaching a given project: 1) a reluctance to the passive acceptance of, and grafting onto, of existent research; 2) an eschewal of an overarching, and therefore stifling, methodology; which both coalesce in 3) a firm belief in bootstrapped, community-focused and oriented action, which espouses a firm self (in the sense of the communal, if not necessarily though neither exclusionary of, the individual self) actualization through focused bottom-up actionable

---

<sup>179</sup> McTaggart, *op. cit.*, p. 2.

<sup>180</sup> Fals-Borda and Rahman, *op. cit.*, p. 16.

<sup>181</sup> Reason and Bradbury, *op. cit.*, p. xxv.

<sup>182</sup> McIntyre, *op. cit.*, p. 7.

<sup>183</sup> McTaggart, *op. cit.*, p. 26.

planning and execution. In other words, PAR emphasizes the invigorating, vitalizing and enriching effect of performing actionable research, of identifying a target problem area in the community, formulating plans of action that would then lead to the betterment of the lives of those most deeply maligned by the afore-identified disparity (who would, of course, also be the ones developing said plans), of then carrying out the planned actions, of reflecting on the outcome, and of then refining and proposing future reapplications until desirable outcomes which benefit the participants are fully actualized. Which all leads to what Rahman describes as “[t]he basic ideology of PAR is that a self-conscious people, those who are currently poor and oppressed, will progressively transform their environment by their own praxis”<sup>184</sup>. While shifts in environment augmentation, a sort of life hacking as it were, may be inspired and influenced by others and by existent external research, the actual change comes from communitarian self-action, by active participation, of the participant-researcher(s).

The resultant *Operations Manual* will seek to apply PAR principles to the area of so-called intellectual properties, an arena that while oft-studied, has indeed been little approached from a PAR perspective, despite being at the core of one of the main injustices PAR-conscious participator-researchers typically seek to address. As Rahman elucidates, “this is the distinctive viewpoint of PAR, domination of masses by elites is rooted not only in the polarization of control over the means of material production but also over the means of knowledge production”<sup>185</sup>. Knowledge production, as generated in the form of closed-access journal publications, government reports, business plan prospects, and corporate whitepapers, to give but a few examples, creates an inherently limiting and choking field of acceptable means of viable information sharing, effectively squeezing out any knowledges generated outside acceptable channels—say, think tank veterans or alphabet-soup title-holding corporate agents. Hence, “[t]wo elements of empowerment that are considered by PAR to be the most important are autonomous, democratic people’s organizations and the restoration of the status of popular knowledge and promoting popular knowledge”<sup>186</sup>. Popular knowledge is that which is generated in a non-hierarchical, recursive manner as outlined by our previously discussed PAR framework of postulating, experimenting, and reformulating, all given a particular community’s and situation’s input and leading to a mutually beneficial refinement. In other words, it is knowledge distilled by participants within the to-be-effected community,

---

<sup>184</sup> Fals-Borda and Rahman, *op. cit.*, p. 13.

<sup>185</sup> *Ibid.*, p. 14.

<sup>186</sup> *Ibid.*, *op. cit.*, p. 16.

not knowledge coerced via data collection by external researchers, who siphon off communal experience for government or corporate gain.

If the botanical realm of spermology were to intersect with PAR, popular knowledge would manifest itself as superior plant stock being bred after generations of community farmers harvesting the seeds of the most prosperous, healthiest plants over and over, whilst elitist knowledge would in turn be a patented genetically-modified seed that's been tailored to be immune to, say, a particular agri-biotechnological behemoth's own brand of pesticide. The repeat privileging of elitist-generated knowledge is the exclusion and subsequent, or perhaps parallel, delegitimization popular knowledge, oft coming with the additional bitter aftertaste of the former also co-opting the latter. Thus the fruits of local community-borne cultivation techniques, or the distilled tonics of localized healing herbs become patented and privatized by elite interests<sup>187</sup>. The latent danger in the realm of the social sciences is that the same may indeed be happening to certain PAR work in particular, and scholarly output in general, as well.

Thus while the concern over the monopolization of knowledge production and the concurrent deligitimization and co-option of popular knowledge is indeed a very real and serious one, equal attention must however also be paid to not only the question of who controls the means of knowledge production, and how said controls are enacted, but of who controls the means of knowledge *distribution*, and how, again, these controls are also enacted. With the elucidation of the operant controls of course in turn paving the way for their dismantling. This is all to say that the question of—once popular knowledges have been successfully generated via the application of PAR frameworks of production through direct community engagement and (re)formulation(s)—how can said popular knowledge be successfully disseminated to both the particular local community and other communities which may benefit in any number of ways (say, via an inspiration to action of their own)? That the generation of PAR-inspired popular knowledges has been successful can be evinced by the broad array of case studies in various published PAR compendiums.

That the *distribution* of PAR-inspired knowledges has been successful cannot be evinced by the broad array of case studies in various published PAR compendiums due to the fact that said compendiums are often published by elite publishers at elite prices. For instance, *Participatory Action Research in Natural Resource Management* is sold by Routledge for

---

<sup>187</sup> Vandana Shiva. 1999. *Biopiracy: The Plunder of Nature and Knowledge*. Boston, MA: South End Press.

\$155<sup>188</sup>, while *Participatory action research: Strengthening farmer organizations and agency-farmer relations* brings up another noteworthy vector of knowledge distribution strangulation: that of limited availability, an artificial scarcity, which is oft also compounded by aforementioned price gouging. Out of print, *Strengthening Farmer Organizations* is currently only available as one used tome for the price of \$435.99<sup>189</sup>, albeit luckily in (third-party) vendor stipulated “very good” condition. If PAR-based work is then to combat not merely the choking of knowledge creation, but of knowledge production as well, there then emerge two dominant problematics to overcome: 1) the problem of availability via preventative pricing, and 2) the problem of availability via the imposition of artificial scarcity.

To combat Problem 1, the aim of this *Operations Manual* is to then logically lower the preventative barrier of the price until it is eliminated. Since any monetary sum presents a barrier, our quantitative aim here can thus be none other than zero, or in other words a wholesale elimination of the pricing system altogether, to be replaced by free, unbridled data sharing. As costs are at times justified by an appeal to limited resources, say in the printing of treeware tomes, we move to postulate the freeing of digital copies doubtlessly stored on the hard drives of modern day publishers. That the production of said tome may also require immaterial labor along the lines of editing and proofreading, may be responded to via an observation offered to us by Bataille:

a basic fact: The living organism, in a situation determined by the play of energy on the surface of the globe, ordinarily receives more energy than is necessary for maintaining life; the excess energy (wealth) can be used for the growth of a system (e.g., an organism); if the system can no longer grow, or if the excess cannot be completely absorbed in its growth, it must necessarily be lost without profit; it must be spent, willingly or not, gloriously or catastrophically<sup>190</sup>.

---

<sup>188</sup> Christian Castellanet and Carl F. Jordan. 2002. *Participatory Action Research in Natural Resource Management - A Critique of the Method Based on Five Years' Experience in the Transamazônica Region of Brazil*. New York, NY: Taylor & Francis; Price as of 2014, as per Routledge: <http://www.routledge.com/books/details/9781560329794/>.

<sup>189</sup> C. M Wijayaratna. 1996. *Participatory Action Research: Strengthening Farmer Organizations and Agency-Farmer Relations*. International Irrigation Management Institute; Price as of 2014, as per Amazon: <http://www.amazon.com/gp/offer-listing/9290901756>.

<sup>190</sup> Georges Bataille. 1991. *The Accursed Share: Volume 1* (trans. Robert Hurley). New York: Zone Books. p. 21.

In other words: people can voluntarily congregate on proofreading and editorial tasks, free of charge, as seen for instance in Project Gutenberg’s Distributed Proofreaders initiative<sup>191</sup>, or Wikipedia’s populous ‘Wikipedian’ editor community<sup>192</sup>. Going further, on into extralegal waters wherein this *Operations Manual* will be predominantly found to be afloat, one can see that a number of PAR tomes are already freely available on public download sites such as Library Genesis<sup>193</sup>. The problem is that not nearly all of them are likewise available. Thus much like one will doubtlessly recall we were (literally) institutionally and systematically consigned to an unfinalized draft of Alleyne’s “We Are All Hackers Now”, so too are we seemingly even extralegally resigned to a limited number of (perhaps illicitly) available free PAR tomes. Of course, some individual PAR articles may be freely available via other sources, such as full text links handily provided on authors’ own websites. But again, not nearly all of them are, and certainly neither are complete tomes.

As Moglen elucidates, what is then necessitated is “the resumption of the cultural inheritance stolen from us under the guise of ‘intellectual property’”<sup>194</sup>. And indeed, we here thus see an emergent coalescence between the PAR’s dedication “to liberate the human body, mind and spirit in the search for a better, freer world”<sup>195</sup>, and Moglen’s dotcommunist commitment to “the revolution that liberates the human mind. In overthrowing the system of private property in ideas, we bring into existence a truly just society, in which the free development of each is the condition for the free development of all”<sup>196</sup>. The aims of wholesale information liberation and of the assurance of the free potentiality of knowledge propagation in PAR parlance (or the creation of the univiscid liquid in alchemico-rheological terminology—being a liquid with no viscosity or resistance to flow, thus constituting an ideal unbridled flow—can here be seen to be broadly in sync, both seeking to bring about a freer, egalitarian (anti)state of affairs. “Less Locke and more Kropotkin”<sup>197</sup>, as Rahman puts it.

#### 1.4.2 Case Study 2: Hacking Away at Twilynax Publishing

Yet, in keeping with the self-actualization involved in PAR work, perhaps there is something *this* research in itself can do to modify the afore-described existent lack of free,

---

<sup>191</sup> Distributed Proofreaders. <http://www.pgdp.net/c/>.

<sup>192</sup> “Wikipedia:Wikipedians”. 2014. *Wikipedia*. <https://en.wikipedia.org/wiki/Wikipedia:Wikipedians>.

<sup>193</sup> “Participatory Action Research” query. Library Genesis. 2014.

[http://libgen.in/search.php?req=participatory+action+research&lg\\_topic=libgen&open=0&view=simple&phrase=1&column=def](http://libgen.in/search.php?req=participatory+action+research&lg_topic=libgen&open=0&view=simple&phrase=1&column=def).

<sup>194</sup> Moglen, *op. cit.*

<sup>195</sup> Reason and Bradbury, *op. cit.*, p. 2.

<sup>196</sup> Moglen, *op. cit.*

<sup>197</sup> Fals-Borda and Rahman, *op. cit.*, p. 6.



public availability of a large number of PAR-based texts by contributing to the community of PAR researchers via the active participation of *this* PAR researcher. In following the previously enunciated PAR mandate of DIY, coupled with the recursive PAR process of questioning, reflecting, investigating, and refining we may develop a preliminary case study of utilizing local resources to aid in not only open knowledge production, but in open knowledge distribution as well. Whilst the rest of the *Operations Manual* will seek to develop contraceptive, emancipato-surgical, and finally distributive strategies of data liberation, this section will focus on an initial test case of aiding in knowledge distribution. Refer to Appendix 1: ‘Sample Procedure for Content Protection Removal from Twilynax eBooks’ for a full expatiation of the procedure undertaken herein.

In investigating the list of academic resources available to students at a given university, one finds a list of not only traditional treeware sources (*viz.* libraries), but also a list of ‘e-resources’. Our aim then is to capitalize on said resources available to said university community by making them available to anyone else to whom they may prove to be useful. Thus if the operant aim is to have maximal potential utility, the availability must likewise be global and unimpeded by any set affiliation, academic or otherwise. Our specific test case will be the tome *Action Research Techniques: Easy and Doable*<sup>198</sup>, selected due to its direct applicability to PAR and its availability to the university community as directly juxtaposed to its blatantly unready (pending a purchasing fee) availability to the exterior community. Prices for said tome, listed on the popular book vendor Basin, are currently \$76.49 for a new hardcover copy directly from Basin<sup>199</sup>, \$68.84 for a new hardcover copy from a third-party vendor (albeit one that sells via Amazon), used copies from third-party sellers starting at \$43.99 and going up to \$545.45 with conditions of the used texts running the gamut from like new to very good to good, and finally \$79.58 for a digital Kindle Edition. The pivotal point here of course being that all of the aforementioned prices are non-free (for indeed a free price would cease to be a price), being > \$0.00, and are thus artificial barriers to unbridled knowledge propagation. In other words, the specificities of a particular price are here entirely extraneous, it the presence of (any) price which itself acts as a coagulant, serving to congeal the flow of information via the injection of a pricing metric.

A search for the tome on the aforementioned ebook repository Library Genesis, which contains over a million distinct ebooks, further yielded no results. Searches on

---

<sup>198</sup> Title is fictional. Refer to Disclaimer of Liability.

<sup>199</sup> 2014. [http://\\*/](http://*/).

academic article and book sharing site AAAA.org again yielded no hits, as neither did searches on the popular torrent meta-search engine torrentz.com, nor finally did a last ditch search via the search engines Google<sup>200</sup> and DuckDuckGo<sup>201</sup>. It is hence assumed that said text is either not freely and publicly available, or is at the least unavailable on the most common and readily available channels for the free procurement thereof. Thus the selected tome is a prime candidate for a test study in the praxis of data propagation due to its prohibitive costs, its ready availability to a particular university community and yet its paradoxical unavailability to other communities. The following PAR-based exercise can thus further be seen as a means of paradox-resolution via the use of a common linkage or community-bridge building.

In looking at the given university library online catalogue, we find our target text to be available both as a treeware copy on the library shelves, and as a digital e-copy available from one of the aforementioned ‘e-resource’ providers to which said university library carries a subscription. Given that the task of scanning in a treeware tome seems redundant as digital copies of the book seem to exist (though in both cases Moglen’s proclamation that “[i]t is in the domain of technology that the defeat of ownership finally occurs,”<sup>202</sup> nonetheless rings true), our study will initially turn to the liberation of the e-copy, and only fall back on the digitization of the treeware copy if it is found that the liberation of the digital version proves to be untenable due to, for instance, content protection mechanisms which cannot be bypassed.

Clicking on the e-copy link in the catalogue, we are eventually redirected to a third party company by the name of Twilynax, “[t]he ebook distributor of preference”<sup>203</sup>. “Working with the world’s leading producers of content, Twilynax has ensured that vibrant and diverse material populates Twilynax for the use of its users”<sup>204</sup>. Given that our stated goals are more encompassing than Twilynax’s, in that we seek for the text to populate the Internet for the benefit of any users, it then logically follows that the tome must be extracted from Twilynax’s database, as the latter is far too exclusionary for the immediate aims of our PAR-based endeavor. With the necessity of said liberatory action thus firmly in mind for the completion of, at the least, this step of our dissertation projection, we duly log in with the

---

<sup>200</sup> Google. <https://www.google.com>.

<sup>201</sup> DuckDuckGo. <https://duckduckgo.com>.

<sup>202</sup> Moglen, *op. cit.*

<sup>203</sup> Twilynax. 2014. “Twilynax: About Us”. [https://\\*](https://*).

<sup>204</sup> *Ibid.* N.B. Quotation augmented, as per Disclaimer of Liability.

given university-afforded username and password into the Twilynax site via the Santora academic access management platform. We are then presented with the dual options of ‘Read content online’ or ‘Download content’.

Upon electing to perform the latter, with the surreptitious intention of a subsequent unauthorized dissemination, we are greeted with the following rejoinder: “[y]ou may download an digital version of this text for reading and viewing offline. As with regular libraries, e-texts are loaned to you for a period of days. After this period has ended you won’t be able to read the text until you decide to download it once more”<sup>205</sup>, which is in turn followed by a three-item drop-down menu which gives us the option of choosing the length of the loan, with the available options being one, two, or three days. Thus immediately we are confronted with the imposition of a maniacal artificial scarcity. Whereas a paper book exists as a singularity which cannot be easily replicated, and thus loan durations are created for purposes of assuring that a wide number of potential readers may gain access to said tome, e-texts suffer from no such malignity, *lest it is imposed on them*, as is seemingly the case here.

Recalling Bataille, as the excess of the boundless digital form cannot be contained, it must then indeed be lost without profit (which it to say, Twilynax’s profit), *willingly or not*. Which is to say, if Twilynax refuses to give it freely, or *gloriously* to pointedly deploy Bataille’s vernacular, then it will be taken by illicit force, or *catastrophically* (from Twilynax’s perspective, for indeed the excess is seen as radiating most gloriously from those outside of Twilynax’s paywalled confines). Which is to say, Twilynax is here attempting to contain the excess of the digital form in its financial and corporate growth precisely by the imposition of said barriers of artificial scarcity in the form of limited ‘check out’ dates. Glory and catastrophe, much like the anti/program, are thus here seen to be a matter of perspective. Though should our research experiment prove successful, it will indeed conversely also prove Twilynax to be unsuccessful, paving the road to its imminent catastrophe—which is, conversely and conveniently, then contributory to the *glory* of unbridled data dissemination and the highlighting of the futility of informational enclosure.

To return to our test case text at hand, however, we elect for a three day loan (to give us maximal operating time), and press Download. We are then notified that the ebook will be accessible until a date and time exactly 72 hours in advance, and proceed to download a PDF

---

<sup>205</sup> Twilynax. 2014. [https://\\*](https://*).

file. Upon attempting to open the PDF in the Ghostscript/GSView PDF viewer programs<sup>206</sup>, however, we are informed that it is unable to view the file due to an “unknown security handler”, despite Twilynax’s claims that downloaded ebooks should work in either Adobe Acrobat or “a similar reader program”. Upon subsequently opening the PDF in Adobe Acrobat<sup>207</sup>, we are now duly informed that “[i]f you open this document, anonymous usage data will be sent securely to this remote server: \*\*\*\*\*.\*\*\*\*\*.\*\*\*”. Note the PDF document’s immediate attempt at establishing an Internet connection, in stark contrast to Twilynax’s aforementioned claim of providing the downloadable version of the text to facilitate offline viewing. Thus the manifested technical reality is contrary to the promised manifestation thereof. Upon opening the document, our firewall in its turn now informs us that “Adobe Acrobat is attempting to monitor user activities on this computer. If allowed it may try to track or log keystrokes (user input), mouse movements/clicks, web sites visited, and other user behaviors”. Thus the mere opening of a legally checked-out ebook is already accompanied part and parcel with a wholesale erosion of the reader’s privacy, signifying a comprehensive state of user behavior surveillance.

Next, in viewing the Security Settings of the finally opened PDF, we find Acrobat informing us that “[y]ou cannot edit, print or copy this document”, that the document will expire in three days, and that “this document can not be opened offline”. Using Advanced PDF Password Recovery Pro<sup>208</sup> to attempt to bypass the Digital Rights Management (DRM) protection embedded in the PDF, we are met with the message that “[t]his document was created with 'Adobe.APS 40-bit security v.4' encryption handler. This protection method is not supported”. Though existent instructions for bypassing this mode of DRM-based content protection are available<sup>209</sup>, upon attempting them we find that they are non-functioning, in that the proposed mode of bypassing said DRM has no effect on the e-book in our case.

System clock modification is another mode of attack in which we can modify the operating system clock parameters to an earlier time so as to potentially extend the life of trial software, or in this case, a time-bombed ebook. However, the attack is a fairly primitive

---

<sup>206</sup> Ghostscript is a PDF interpreter; GSview is a Graphical User Interface (GUI) front-end for Ghostscript. Russell Lang. 2006. GSview. v. 4.8. <http://pages.cs.wisc.edu/~ghost/gsview/>; Artifex Software, Inc. 2007. Ghostscript. v. 8.60. <http://ghostscript.com/>.

<sup>207</sup> Adobe Systems Incorporated. 2010. Adobe Acrobat Professional. v. 8.3.1. <https://www.adobe.com/products/acrobatpro.html>.

<sup>208</sup> ElcomSoft Co. Ltd. 2014. Advanced PDF Password Recovery. v. 5.06. <https://www.elcomsoft.com/apdfpr.html>.

<sup>209</sup> Béranger. 2013. “Adobe LiveCycle Rights Management: the removal”. *Homo Ludditus*. <https://beranger.org/2013/09/20/adobe-livecycle-rights-management-the-removal/>.

one, with countermeasures being thoroughly documented in both the forensic<sup>210</sup> and anti-piracy<sup>211</sup> literature. However, the fact that an attack is both simple and well-known should not be a deterrent to attempting it. Thus we change the local operating system time and date after the check-out period has expired to an earlier date. Expectedly however, this proves to also be an ineffective maneuver, with Acrobat now displaying the error message “[y]our permission to open this document offline has expired”. Whilst the option of actually taking screenshots of every page nonetheless still works, this method results in the degradation of actual text into images, which would in turn necessitate a process of Optical Character Recognition (OCR) to turn the text back into searchable words, which like with the aforementioned scanning option would seem to be needlessly redundant lest it turns out to be the only remaining viable option.

In keeping with our recursive PAR spiral, however, upon reflecting on the seeming inapproachability of said PDF, we decide to return to the Twilynax site to check for any potential alternate versions of the text or helpful clues that would aid in the unclasp of the knowledge propagation shackle clamped around the existent one. Recall the earlier-mentioned ‘Read content online’ link which is situated right alongside the ‘Download content’ link we have previously clicked. Twilynax’s online e-book reader presents each page of the ebook in a separate PDF document, wrapped in a browser-based reader. Each PDF page appears to have a randomly generated mixed-case A-Z filename of 18 characters (e.g. jXmuPLAzozTQhHUKqW.pdf). Thus to save the entire book, one would either have to manually click the arrow designating the next page and save each resultant PDF, or one could simply use what is known as macro or automation software, such as Do It Again<sup>212</sup>, to record the task of saving each page (as the next arrow keys and save buttons in the browser appear in the same exact spot on the screen at each page iteration). However, the pitfall of automation is here seen in that the server may detect overly fast page turns and log the user out of Twilynax or present them with a challenge-response screen (for instance, typing in obfuscated text) which would disrupt the automated downloading process. Of course, the same effect may also likewise be triggered if one is merely flipping through the pages

---

<sup>210</sup> Harry Parsonage. 2010. “The Meaning of LIFE: Linkfiles In Forensic Examinations”. <http://computerforensics.parsonage.co.uk/downloads/TheMeaningofLIFE.pdf>; Lee Whitfield. 2011. “Rock Around the Clock”. SANS EU Digital Forensics and Incident Response Summit. <https://digital-forensics.sans.org/summit-archives/2011/2-rock-around-the-clock.pdf>.

<sup>211</sup> Kris Kaspersky. 2005. *Hacker Debugging Uncovered*. Wayne, PA: A-List Publishing. p. 423; Pavol Cerven. 2002. *Crackproof Your Software*. San Francisco, CA: No Starch Press. p. 85.

<sup>212</sup> Anthony Dean Johnson. 2014. Do It Again. v. 1.6. <http://www.spacetornado.com/DoItAgain/>.

looking for a particular passage in the book, and thus even here the ripple effects of the malignity of artificial scarcity can be experienced in full force. Thus, when setting up Do It Again or a competent other piece of macro software, one must merely be sure to insert an appropriate time delay between the actions to be replayed. However, a further problem is presented by the fact that the default filename Twilynax selects for each PDF page is identical; thus a pure macro attack would need to use a tool which allows iterative automated naming. A simpler alternative is to simply save the pages manually.

Following the eventual successful downloading of all encompassing pages, we regretfully discover that each PDF also has security settings which inform us of the now familiar refrain that “[y]ou cannot edit, print or copy this document”. Curiously however, instead of also informing us of any time-based access restriction, the security settings instead also state that “[t]his document has an open password or a modify password”. Opening up the previously unsuccessfully used Advanced PDF Password Recovery software once more, we load a sample page PDF, and press the ‘decrypt this document’ button. Almost immediately, a ‘Document successfully decrypted’ pop-up appears, and an accompanying UnEncrypted.pdf file is found alongside the encrypted page PDF. Upon opening said decrypted file, we find that it is indeed identical to the corresponding encrypted PDF content-wise, albeit with all security settings removed. Upon batch-processing all downloaded pages of the e-book through Advanced PDF Password Recovery, one is now left with singular unencrypted PDFs for every page of *Action Research Techniques: Easy and Doable*. Using Adobe Acrobat, we can then combine the separate page PDFs into one comprehensive PDF that is devoid of any encryption or DRM, and did not require us to OCR imaged text back into searchable text form. Hence we now have the free, unhindered by time or any other restrictive qualifier, equivalent to the checked-out PDF we initially downloaded—save for the DRM shackles, of course.

The resultant unfettered PDF can now be distributed via any number of public portals, such as the aforementioned Library Genesis website, which will render it accessible to any interested communities, not only those outside the Twilynax and university paywalls, but to anyone within the community who wishes to view the tome without an Internet connection and/or for a period exceeding three days.

Through a continuous process of planning, research, refinement, and execution we have thus eventually achieved our immediate test goal of knowledge propagation, despite strong corporate attempts at hindering said dissemination, thereby in turn achieving what will

be recalled was one of the ‘elements of empowerment’ “considered by PAR to be the most important [...] the restoration of the status of popular knowledge and promoting popular knowledge”<sup>213</sup>. In so doing, we have here predominantly followed what Reason and Bradbury term the “first-person pathway of action research [which] address[es] the ability of the researcher to foster an inquiring approach to his or her own life”<sup>214</sup>, while at the same time also facilitating potential second-person research/practice via making said text available for anyone else for whom its former lack of propagation was a concern. In sum, our hacker methodology can thus here be seen to be polymorphous in its adaptability to the deployment of varying attack vectors, non-legalist in its rejection of the legal limits on content protection removal and content liberation, and finally marked by a disjunctive embeddedness, which is to say a familiarity with the operant Twilynax content delivery systems, further marked by the exploitation thereof. Having thus established its theoretical and methodological footing, the rest of the *Operations Manual* will attempt to facilitate a broader third person pathway which “aims to extend these relatively small-scale projects so that “rather than being defined exclusively as ‘scientific happenings’ they (are) also defined as ‘political events’”<sup>215</sup> by focusing on ideological, as well as their accompanying technological manifestations, threats to data dissemination.

---

<sup>213</sup> Fals-Borda and Rahman, *op. cit.*, p. 16.

<sup>214</sup> Reason and Bradbury, *op. cit.*, p. xxv.

<sup>215</sup> *Ibid.*, p. xxvi.

**2.**

**Ordinance the First:  
Contraceptive Strategies for Data  
Liberation**



## **2.0 Did You See the ©?**

In flipping or scrolling through a given book's front matter—a conglomeration of publishing industry esoterica consisting of fly leaves, titles and half titles, epigraphs and dedications—one may certainly be pardoned for not noticing, let alone paying any mind, to a particular letter, c, to be found therein. Now to be sure, there may indeed be a veritable sea of c's in the surrounding front matter, but this one is quite special, indeed. Standing out from the rabble of plebian alphanumeric, the particular c soon to be of immense interest to us is set apart from its typographic peers through a simple circular ensconcing, like so: ©. Thus the c becomes encapsulated in a realm all its own, and whilst being surrounded by disrobed peers, it wields a power entirely unavailable, if not unknown, to the others—lest the others are likewise divined with a supernatural, and here the supernatural phenomenon of which we speak is of course a legal one, ability to exert monumental force over all text that follows them<sup>216</sup>; strangling, contracting, exhausting and ultimately expiring all content that falls within its ominous grasp. Though visually at times indistinguishable from mere enclosed alphanumeric, letters and numbers in a circle—typographic remnants of list indexation, rest assured that no ordinary letter may achieve the commanding force of presence of the © sans a magical, yet rigorous, incantation known as 'law'<sup>217</sup>.

Indeed we thus see that the © is a sight to behold, and, more significantly, a sight to be beholden to. And yet, it's still pretty easy to miss. Taking up merely one character slot in the many folds of the paratextual—the text which surrounds a text, preceding the first chapter and following the last, including quite the potential mass of characters ranging from a publisher's introduction to a prolonged postface—the ©, its aforementioned peculiar typographic bejeweling notwithstanding, ultimately escapes our wondering eye. And yet, if indeed one could charge the paratext with constituting “a ‘vestibule’ that offers the world at large the possibility of either stepping inside or turning back”<sup>218</sup>, the © is then the heavy-set yet largely inconspicuous enforcer, serving to remind you, the potential interloper into its

---

<sup>216</sup> Within the musical realm, the comparable duties of © are enacted by ® (United States Copyright Office. 2013. *Circular 3: Copyright Notice*. Washington, DC: Library of Congress. p. 3. <http://www.copyright.gov/circs/circ03.pdf>), and in the realm of trademarks via ® (United States Patent and Trademark Office. 2014. *Protecting Your Trademark: Enhancing Your Rights Through Federal Registration - Basic Facts About Trademarks*. p. 10. <http://www.uspto.gov/sites/default/files/trademarks/basics/BasicFacts.pdf>).

<sup>217</sup> See, e.g., United States Copyright Office. 2011. *Circular 92: Copyright Law of the United States and Related Laws Contained in Title 17 of the United States Code*. Washington, DC: Library of Congress. <http://copyright.gov/title17/circ92.pdf>.

<sup>218</sup> Genette, *op. cit.*, p. 2.

literary realm, that you'll subsequently be reading on its terms, with punishment duly to be metered out should you transgress. For such a pivotal role, it is thus curious that even those texts which are explicitly and entirely dedicated to the paratextual are themselves content to pay only the most fleeting perfunctory attention to it, "copyright, which gives the official date of first publication; ISBN; reminder of the law concerning reproductions, whose dissuasive power has stood the test of time"<sup>219</sup>, and then nary a word more on the matter. The paratext, particular the front matter, is of pivotal interest here as it plays a critical role in regulating the use of the entire subsequent text which follows it, regimenting both the text and interactions with said text.

Yet surely such a pivotal character in the tragic drama *Intellectual Property* (which is, in its own sordid turn, to be followed by the eventuation of the farce of copyleft) is deserving of at least some modicum of expatiation, albeit now without the velvet gloves hithertofore donned by way of introductory decorum. Let there be no lingering ambiguity about the matter: the © constitutes naught more than a syntactical shackle designed by malevolent economic interests in an attempt to fetter the otherwise unbridled flows of human knowledge; a chaining of data dispersal to *authorized* modes of systemic strangulation. ©: a chokehold on the cultural and intellectual promulgation of information. As Haraway points out, "the copyright, patent, and trademark are specific, asymmetrical, congealed processes—which must be constantly revived in law and commerce as well as science—that give some agencies and actors statuses in sociotechnical production not allowed to other agencies and actors"<sup>220</sup>. Being diametrically opposed to unrestrained movement, © thus seeks to both enact and enforce a tangible congealment of information into, quite literally, cages—the particular dimensions and other minutiae of which are hashed out by the twin interests of State and Capital—which in turn utterly destroy a free and unrestrained distribution of content around the surrounding cultural ethos in which that very content was born. Copyright thus serves first to congeal free-flowing data into a sanctioned *form* (*viz.* a 'Body of Work'), that is to say to conjure a tangible enclosure around a certain segment of the data stream which can then be segmented from the general populace (that is to say, copyrighted), and secondly copyright then serves to impose specific modes of distribution or licensing terms: allowable modes of movement (e.g. purchasing a book and reading it without reproduction or modification) which are in fact anything *but* movement, rather constituting a fatal congealing

---

<sup>219</sup> *Ibid.*, p. 32.

<sup>220</sup> Donna J. Haraway. 1997. *Modest\_Witness@Second\_Millennium.FemaleMan@\_Meets\_OncoMouseTM: Feminism and Technoscience*. New York: Routledge. p. 7.

of content into its final *deathform* of solitary confinement. That is to say, modes which are in accord with the copyright's holder's will, which also typically happens to coincide to specifically sanctioned channels of capital, so-called authorized retailers.

Copyright thus acts as “an *abstract machine of overcoding*: it defines a rigid segmentarity, a macrosegmentarity, because it produces or rather reproduces segments, opposing them two by two, making all the centers resonate, and laying out a divisible, homogenous space striated in all directions”<sup>221</sup>. In lieu of being free to move at whim across any dimension allotted by the space-time continuum, copyright instead flattens the allocation of data onto a claustrophobia-inducing x/y coordinate grid, with the axes duly demarcated by the interests of State/Capital. It is here essential to further elucidate that “the most rigid of segmentarities does not preclude centralization”<sup>222</sup>, and thus while a certain reified chunk of data now labeled a Body of Work, following an initiation ceremony in which it is ordained with the mystic symbols and accompanying incantations of Intellectual Property, may be dispersed as a veritable Hydra throughout the world in the forms of different foreign editions, found in various retail chains and libraries, even distributed by different local publishers, that same BoW is nonetheless held together by a centralized ©, as manifested by overarching legalistic machinations akin to The Berne Convention for the Protection of Literary and Artistic Works, The International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations, and any number of similar covens delineated by the World Intellectual Property Organization<sup>223</sup>. The fact that diverse forms may at times of course bump into each other, which is to say that copyright as such is not free of internal contestation—nonetheless does little to undermine the copyright holders' overarching determination of content congealment<sup>224</sup>. That the act of conjuring a BoW and enthroning it with copyright itself is an ultimately doomed venture, no matter what legalistic or monetary aides come to its defense, likewise does not mean that its immanent collapse cannot be helped along to make it all the more swift, for whilst it is indeed a material truth that all dams inevitably crumble with the combined gradual assault of the passage of time and repeat

---

<sup>221</sup> Deleuze and Guattari, *op. cit.*, p. 223.

<sup>222</sup> *Ibid.*, p. 224.

<sup>223</sup> World Intellectual Property Organization. 2004. “International Treaties and Conventions on Intellectual Property”, in *WIPO Intellectual Property Handbook: Policy, Law and Use*. pp. 237-364. <http://www.wipo.int/export/sites/www/about-ip/en/iprm/pdf/ch5.pdf>.

<sup>224</sup> See, e.g., Bodó Balázs. 2011. “Coda: A Short History of Book Piracy”, in *Media Piracy in Emerging Economies*. New York: Social Science Research Council. pp. 399-413. <http://piracy.americanassembly.org/wp-content/uploads/2011/06/MPEE-PDF-Coda-Books.pdf>, for an account of warring North American and European copyright legislation.

encounters with the natural elements, that is by no means a preclusion to the lending of a helping hand via the strategic placement of a stick or two of dynamite at key structural junctures to expedite the inevitably of unrestrained data flow.

To return now to Haraway's aforementioned explication of the constant need for the revivification of Intellectual Property markers, the scurried patching of erupting fissures alongside the great dam wall, texts are routinely branded with the by now all too familiar insignia ©, whilst journal articles and the like oft bear this mark of Cain on every single page. And here it should be noted that while the various explications of © evoked thus far—fettters, shackles, incantations of darkest magic, and so on in an alarmist vein of a similar tune—may seem particularly polemical (they are), they are also—aside from not being entirely divorced from the underlying reality of the grim matter in the least—curiously not at all incommensurate with the imagery used by the copyright industry itself. Consider an advert<sup>225</sup> produced by the British Federation Against Copyright Theft, in which © is, quite literally, depicted as a branding iron with the '©' in the organization's FA©T acronym resulting from an act of branding the iron onto the screen. Yet curiously, the 'cool' light-blue branding iron of the © is contrasted in the advert to a fiery red 'X' brand, whilst the ominous narration warns the viewer: "The pirates are out to get you. Don't let them brand you with their mark." Thus the very real branding iron of the intellectual property industries is presented as a cooling antidote to the mythical, and literally nonexistent, rogue 'X' brand of the pirate. The enforced corralling of branded content is here juxtaposed to the hallucinatory harmful brand of piracy. A longing acquiescence is sought after through its presentation as remedy, a call to lock oneself in a cage so as to protect oneself from wayward marauders.

Of course, the psychological tactics mobilized by the copyright industries in defense of their much-vaunted intellectual properties are not always as picturesque. In once again turning towards Haraway's astute proclamation about the machinations of the © syntax, we now look at the © insignia inscribed within the very book in which said quotation appears—a move of the utmost necessity on our part, as Haraway conspicuously, and all too conveniently, omits any notion of self-reflexivity on the issue. Whilst takedown notices which invoke copyright law have been discussed in the literature<sup>226</sup>, the following

---

<sup>225</sup> Federation Against Copyright Theft (FA©T). 2002. Anti-Piracy Advert.

<https://www.youtube.com/watch?v=hNzCiZAzxCA>. N.B. As of 2015, the video is now unavailable due to the fact that "[t]he YouTube account associated with this video has been terminated due to multiple third-party notifications of copyright infringement".

<sup>226</sup> See, e.g., Michael Piatek, Tadayoshi Kohno, and Arvind Krishnamurthy. 2008. "Challenges and directions for monitoring P2P file sharing networks, or, why my printer received a DMCA takedown notice". *USENIX*

examination will focus on the copyright notice itself, as opposed to subsequent notices which may invoke the originating notice. Thusly casting our paratextual gaze at the front matter of the Haraway publication in question, we find the following inscription:

Copyright © 1997 by Routledge

Printed in the United States of America on acid-free paper.

All rights reserved. No part of this book may be reprinted or reproduced in any form or by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying and recording or in any information storage or retrieval system, without permission in writing from the publishers<sup>227</sup>.

The contemporary notice is notably different from its ancestors, the first federal boilerplate copyright notice having entered the United States legal coda with the 1802 Amendment to the Copyright Act of 1790<sup>228</sup>, though the first state-based copyright notice may be traced still earlier to 1783 in Pennsylvania, which extended copyright protection only to works which had a copy of the certificate of entry into copyright on their title page<sup>229</sup>. The 1802 amendment stated that only works which contained the notice would be entitled to protection under the Copyright Act, with the boilerplate notice being:

Entered according to act of Congress, the \_\_\_\_\_ day of \_\_\_\_\_ 18 \_\_\_\_\_ (here insert the date when the same was deposited in the office) by A. B. of the State of \_\_\_\_\_ (here insert the author's or proprietor's name and the State in which he resides)<sup>230</sup>.

---

*HotSec (Hot Topics in Security)*. <https://www.usenix.org/conference/hotsec-08/challenges-and-directions-monitoring-p2p-file-sharing-networks%E2%80%94or%E2%80%94why-my>; Wendy Seltzer. 2011. "Infrastructures of Censorship and Lessons from Copyright Resistance". *USENIX FOCI Workshop*. [http://www.usenix.org/events/foci11/tech/final\\_files/Seltzer.pdf](http://www.usenix.org/events/foci11/tech/final_files/Seltzer.pdf).

<sup>227</sup> Haraway, *op. cit.*, n. p.

<sup>228</sup> Seventh Congress. 1802. The 1802 Amendment to the Copyright Act of 1790, in *Primary Sources on Copyright (1450-1900)* (eds. L. Bently and M. Kretschmer).

[http://copy.law.cam.ac.uk/cam/tools/request/showRepresentation?id=representation\\_us\\_1802](http://copy.law.cam.ac.uk/cam/tools/request/showRepresentation?id=representation_us_1802).

<sup>229</sup> Vincent A. Doyle, George D. Cary, Marjorie McCannon, and Barbara A. Ringer. 1957. *Copyright Law Revision - Study 7 - Notice of Copyright*. Subcommittee on Patents, Trademarks, and Copyrights of the Committee on the Judiciary, United States Senate. Washington: United States Government Printing Office. pp. 5-6. <http://www.copyright.gov/history/studies/study7.pdf>.

<sup>230</sup> Seventh Congress, *op. cit.*

Thus the originating notice can be seen to have no explicit denial of particular use cases, such denial perhaps being implicit. Instead, the invocation of 1802 merely performs the perfunctory duties of classification, namely stating the date of copyright application and the applicant's name.

Following the 1988 Berne Convention Implementation Act, which came into effect in 1989, and signified the accord of the United States with the Berne Convention for the Protection of Literary and Artistic Works of 1886, the copyright notice was rendered as optional, with works which did not have the explicit notice still being covered by copyright law regardless<sup>231</sup>. However, notably the first Federal Copyright Act of 1790, whilst requiring that works must be registered contained no requirement that a copyright notice must be included, though a separate notice of registration was to be published in a newspaper<sup>232</sup>. Thus a history of copyright incantation betrays ©'s underlying insecurity—wavering between making its appearance explicit to defaulting to an overarching claim of ownership even if such is not explicitly stated, which then brings us back to our current notice: no longer mandatory, but present in its ascertainment of its existence nonetheless.

Thus returning to our sample contemporary notice, of initial note here is the fact that the copyright is assigned not to one Donna Haraway, presumed author of the text in question, but rather to Routledge—the publisher thereof. Historically, this most curious transposition of copyright is explained thusly:

[a]uthors had a right to own the products of their labour in theory, but since they created immaterial ideas and lacked the technological means to produce books, they had to sell their rights to another party with enough capital to exploit them. In essence, it was no different than having to sell their labour.

The exploitation of the author was embedded in the intellectual property regime from its inception<sup>233</sup>.

Yet considering that the numerics next to the © would seemingly denote that the text was produced at the end of the 20<sup>th</sup> century, as opposed to the 18<sup>th</sup> (to which the aforementioned historical explanation of publisher allocation of copyright refers to), the excuse that authors lack the technological means to produce books is no longer accurate in light of not only the availability of consumer printers and vanity presses, but of Internet publishing as well.

---

<sup>231</sup> United States Copyright Office, *Circular 3: Copyright Notice, op. cit.*, p. 1.

<sup>232</sup> Doyle et al., *op. cit.*, p. 6.

<sup>233</sup> Anna Nimus. 2006. "Copyright, Copyleft and the Creative Anti-Commons", in *subsol*. [http://subsol.c3.hu/subsol\\_2/contributors0/nimustext.html](http://subsol.c3.hu/subsol_2/contributors0/nimustext.html).

Instead, one may speculate that the *choice* to resign copyright to a publishing behemoth amounts to a mixture of personal and institutional factors ranging from it merely being a customary ‘business as usual’ continuation of corporate acquisition of knowledge and the author’s—willing or unwilling, an utterly irrelevant distinction for it brings about the same result regardless—acquiescence thereto, to perhaps a matter of prestige borne of publishing in an ostensibly reputable academic press as opposed to the presumably less glamorous route of self-publishing.

Conversely, the mere fact that an author has thusly chosen (within the aforementioned constraints of ‘choice’, particularly in the arena of academia), such a route must also not be misinterpreted to mean that the author may be opposed to other modes of content dissemination (especially in this specific instance where the author has shown critical reflection on the issues involved), as there is likewise nothing stopping the author from at the same time as the official publication becomes available for purchase (or even prior) of similarly making the work freely available anonymously. Thus it is entirely possible, even plausible, that authors may on the one hand publish tomes through traditional publishers, whilst on the other clandestinely make said tomes freely available online.

At any rate, the precise impetus for acting thusly is of course the private knowledge of the author herself, what is of utmost import for us here is the twin elucidation that 1) the action constitutes a choice, that is to say an active agency on part of the author to relinquish the ‘rights’, such as they are, to an external party which presumably aims to derive maximal economic gain from the arrangement; and 2) that the reason for 1) bears not in the least on the outcome of said action: the matter of *why* a copyright gets assigned to a publisher does of course not affect the resultant outcome of the copyright *being* assigned to a publisher. To put the matter bluntly, in all of its characteristically grim realism: it matters not who brandishes the branding iron so long as act of branding occurs. The flesh sears irrespective of the branding being done by a lone farmer or by a multi-state livestock conglomerate.

The next line in the aforementioned incantation, regarding the actual printing of the newly baptized tome, may at first glance seem like a non-sequitur in light of it being sandwiched being two otherwise perfectly related perfunctory copyright notices. Indeed, the question of the moment is why, precisely, would a seemingly innocuous notation regarding the printing location and paper quality be awkwardly interposed thusly? Note here that the printing notice, following a curt copyright indication, precedes a rather stern, indeed acidic, series of injunctions against unauthorized uses of the text. Thus by an abrupt and seemingly

misplaced reassurance to the reader that the text is printed on ‘acid-free paper’, the passage performs the pivotal function of priming the reader into passive acquiescence with the copyright terms which immediately follow. For by the text’s own proclamation, the paper is acid-free, and thus the possibility that it may contain any acid or vitriol, anything which may literally harm either the reader or the text itself, is precluded *ex vi termini*. The fact that acid-free paper further increases the longevity of the book itself, and hence likewise the content inscribed therein, further entrenches the notion that the text will endure and outlast any attempts at insubordination of its ©-sanctioned/shackled form: an assurance of permanence and thus of the futility of insurrection.

Finally, we come to the bulk, the ‘heavy matter’ of the incantation: the Grand List of Prohibitions. Invoking the liberal language of *rights*, the copyright proclamation promptly lays claim to *all* of them, explicitly making no distinction between various rights or sets thereof. Thus not only is the notice referring to *copyright* and satellite rights beholding content owners, but it is likewise referring to any and all other liberal discursions on the notion of rights, culminating perhaps in the right to life<sup>234</sup>. All of these rights are firmly clasped in the grip of the copyright notice, held in reservation, hostage to the whims of the legally anointed copyright owner. Of what use is it then for intellectual property dissidents to invoke the language of rights-based claims to information when the entire discourse has—quite literally—already been usurped by the copyright claimant(s)? No matter the particularities of the interpretation, that is to say whether the copyright is reserving all rights *for* itself and/or reserving all rights *from* the reader, the fact that it has already appropriated all manner of rights for itself precludes the possibility of a liberal rights-based discourse having any potency whatsoever, given that all rights that it may make claim to are, once again, reserved *a priori* by the copyright notice itself. An example of such discourse, for instance, being the ‘right to remix’ often advocated by copyright reformists<sup>235</sup>, which calls for reforming existent international copyright legislation for purposes of adding an allowance that would grant the right to make derivative works. Given that all rights are reserved however, the introduction of said right to remix would likewise be reserved, rendering the introduction of a new right as yet another tentacle for the burgeoning IP octopus, which will

---

<sup>234</sup> “Part III. Article 6. 1. Every human being has the inherent right to life” (United Nations General Assembly. 1966. International Covenant on Civil and Political Rights. <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>).

<sup>235</sup> See, e.g., Damien O’Brien and Brian Fitzgerald. 2006. “Mashups, Remixes and Copyright Law”, in *Internet Law Bulletin* 9 (2). pp. 17-19. <http://eprints.qut.edu.au/4239/1/4239.pdf>; Right2Remix.org. 2013. <http://right2remix.org>.



then fully appropriate another right which it reserves. *A priori* monopolization of rights thus negates the utility of the introduction of any future rights, as at the moment of their inception they instantly become reserved.

One may further notice that the next sentence in the incantation contains a certain apparently idiosyncratic formulation—"No part of this book may be reprinted"—that far from certainly being a mere typo of 'may', though granted that is indeed (but one such) possibility, instead can be said to constitute a sort of megalomaniacal fissure within the copyright notice which leads to a bringing to the fore of the underlying greed and ownership which fuels the commodification of the underlying text. 'My' the copyright notice declares of the text: it belongs to *me* and may not be reprinted... A certain *propertarian slippage* thus here emerges and, through an impromptu bout of egomania, lays bare exertions of ownership over the content inscribed therein. Hence it is far from clear that the academic notation '[sic]' would here be at all appropriate; indeed, to add such a note would be to effectively turn a deaf ear to the forceful evocation of the copyright claimant's underlying thirst for unequivocal ownership, instead erroneously presenting the claimant in a strictly formalist legalese, free of the passion that is otherwise so clearly expounded in the least likely, and yet most fitting, of locales.

In dull obligation to the terms of the copyright notation discussed herewith, it must of course be pointed out that *this* very text that is now being written and perchance subsequently read is itself in violation of the stringent copyright incantation. To wit, a basic hypothetical syllogism to explain the grave matter we now find ourselves in as succinctly as possible: If...

- (1) According to the terms of the copyright notice of the book in question, no part of the book may be reproduced without written permission from the publishers;

And...

- (2) A part of the book in question was in fact reproduced herein without written permission from the publishers;

Then...

- (3) The terms of the copyright notice have been violated.

Given that (1) is indeed no hypothetical 'if' at all, for the terms of the copyright notice of the book in question do in fact state precisely that no part of the book may be reproduced without permission of the publishers, and that a part of the book *was* indeed reproduced herein—in fact, multiple parts were reproduced at multiple times; a veritable plethora of unabashed

insubordination thus abounds, then it would indeed appear that the terms of the copyright notice have here been violated. Though perhaps the matter is still unclear. Precisely which parts of the book were here reproduced? Certainly Haraway's quotation describing the congealing process brought about by copyright constitutes a part of the book, as does the far lengthier quotation of the copyright notice. If only the offense were limited to these two tangible transgressions, then it could be fixed with relative ease through a simple text-surgical procedure of excision, thus removing the unlicensed content. The resultant text would of course be without highly pertinent quoted material, but at least it would not run afoul of copyright regulations.

However, the matter cannot be resolved with such relative ease; for indeed, the violation runs far deeper than two mere quotations. Consider: while surely the two aforementioned quoted segments constitute a part of the book, so too does the book's title itself, as it appears at various points within parts of the book, as does the name 'Haraway' for identical reasons; to say nothing of the actual page numbers. And yet, if only the offense were at a close here, one could still excise each mention of either the author or the title of the text, which while surely making direct reference to the text being discussed slightly problematic, I remain confident that one may nonetheless refer to the text in a more creative fashion rather than through the prosaic dullness of overrated 'direct citations'. Instead of citing a quoted passage as, "Haraway, Donna J. (1997)

*Modest\_Witness@Second\_Millennium.FemaleMan©\_Meets\_OncoMouse<sup>TM</sup>: Feminism and Technoscience*, New York: Routledge, p. 7", which would through its reprinting of parts of the book certainly constitute a clear and gross violation of the copyright notice, one could instead resort to basic descriptive modes of citing along the lines of "that famous cyborg-feminist theorist in that book with the long techno title, put out by that repressive academic publishing giant in the north-eastern United States, in the first few pages." Thus it may well be possible, irrespective of desirability, to so far remove all offending reproductions of parts of the book from this very text.

Unfortunately however, further investigation of the book in question has led me to the inopportune discovery that the character sets [a-z], [A-Z], [0-9], and a number of other accompanying symbols [\_, @, ., ©, <sup>TM</sup>] (to name only the ones appearing in the title, by way of minimalist example), indeed all appear in the book—or to use the pointed vernacular of the copyright notice: all constitute 'parts of the book'—in question as well. Thus in order to appear under strict observance of the venerable copyright claim, one must thus purge not

merely quotations or titles from the offending text, but all offending characters which constitute part of the book as well. At this point I am admittedly at a loss as to how one would go about any form of composition, as anything more than an empty page would thus constitute a copyright violation. But going still further, recall that as the previous interjection regarding the printing process of the book made sure to lay stake to the claim that the book was scripted upon acid-free paper, and thus ‘acid-free paper’ *as such* (irrespective of any particular piece of acid-free paper) also *categorically* constitutes a part of the book. Thus if one were to follow the stringent restrictions and terms of use laid out the copyright clause, one would quite literally not even be left with even a blank page to write upon.

In the course of research on the matter, however, I discovered that there are indeed tomes inscribed with quite a similar copyright clause, which likewise contain identical sets of characters, which have appeared in print prior to 1997<sup>236</sup>. This all, in turn, means that the book in question is itself in violation of the copyright terms of its immediate predecessor, and so on until *ad infinitum* the very publication of the very first of such copyright claims. Whether the publication of the book in question is thus an act of blatant hypocrisy or simply an act of innocent ignorance—in that, Routledge may well be blissfully unaware of the fact that copyright-inscribed volumes with identical character sets may have been published prior to this one—is unknown. The fact that if such appearances of copyright notices may themselves be the result of legislation which requires the claiming and notice of copyright would in itself reveal yet another contradiction of IP: that it necessitates its own preclusion, making all future iterations illegal at the same time as it necessitates said iterations themselves.

If at this point the wayward reader may seek to dismiss the above *reductio ad absurdum* via preferential reference to certain crutches in the form of legal constructs which may render the above examples and excerpts legally feasible, then a number of additional points must be brought into play. It is, for instance, certainly true that a certain proviso in the United States Copyright Act of 1976 states, in part, that “the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement

---

<sup>236</sup> E.g. “[a]ll Rights Reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means: electronic, electrostatic, magnetic tape, mechanical, photocopying, recording or otherwise, without permission in writing from the copyright holders” (Derek L. Bosworth. 1986. *Intellectual Property Rights*. New York: Pergamon Press. n.p.).

of copyright”<sup>237</sup>. And yet, the act goes on to state that the aforementioned exemption is not by any means unconditional. In fact it is bound by four deterministic metrics: 1) ‘the purpose and character of the use’, 2) ‘the nature of the copyrighted work’, 3) the amount of the work used in relation to the size of the work as a whole, and 4) ‘the effect of the use upon the potential market for or value of the copyrighted work’. The interplay of all four of the above potentially mitigating or damaging factors is to be interpreted based on each specific case of infringement. One can thus by no means cite Fair Use as an *a priori* ‘legal shield’ that would allow one to breach the aforesaid copyright notice. What’s more, the copyright notice itself makes absolutely no mention of any potential existing exemption to its terms, hence why there has been no prior discussion of it within this analysis—precisely because the legal boilerplate makes no mention thereof. Thus, irrespective of fair use provisos—which, once again, apply on a strict case by case basis—reproducing any part of the book would still constitute a violation of the copyright clause of the book itself.

Yet, even the potentiality of fair use exemptions, and indeed perhaps precisely *because* of their *mere* potentiality of fair use’s applicability, is further stymied by publisher reluctance to even bother attempting a fair use defense in the first place, as Striphas and McLeod point out:

the chilling atmosphere forces academic authors and publishers into a corner where even fragmentary appropriations are forced to comply with market norms that do not recognize fair use, and instead treats each quotation of a cultural text as a commodity exchange that must adopt the form of licensing agreements<sup>238</sup>.

Indeed, not only is fair use and its wielders thus increasing looking to be quite an ineffectual weapon against our aforementioned copyright notice on its own, its potency is all the further eroded by its limited nationalist boundary, especially when compared to the overarching international reach of copyright law; or in other words, “[t]he US’s deeply rooted fair use legal tradition is somewhat unique in the world, however, which means that its effectiveness is quite limited by geography”<sup>239</sup>. Thus not only is fair use by no means a saber with a guaranteed effectiveness to cut through any copyright-restricted thicket, due to its varying case-by-case valuations, nor are those who stand to benefit from it necessarily even willing to wield it in the first place so as to not risk bombardment by a potentially better armed

---

<sup>237</sup> Copyright Act of 1976. 1976. 17 U.S.C. § 107 - “Limitations on exclusive rights: Fair use”. <http://www.law.cornell.edu/uscode/text/17/107>.

<sup>238</sup> Ted Striphas and Kembrew McLeod. 2006. “Strategic Improprieties - Cultural Studies, The Everyday, and the Politics of IP”, in *Cultural Studies* 20 (2-3). pp. 119-144 (pp. 124-125).

<sup>239</sup> *Ibid.*, p. 123.

adversary, but to top it all off the saber's effectiveness drops to ultimate zero beyond certain national borders. As the copyright is a global struggle, reference to strictly regional provisos thus falls entirely short of global data liberation. For instance, while it is indeed true that at least 45 nations have various fair use and/or fair dealing provisos in their IP legislation<sup>240</sup>, the provisos are nonetheless by no means applicable worldwide, thus restricting fair use/dealing to aligned nations (barring any national discrepancies in the minutiae of the legislation, of course). Legal geography may thus, potentially, provide a rough outline of potential safe localities, but it is far from being a universal allowance.

To briefly summarize then, a rebuttal by way of fair use lacks merit based on a minimum of the following four counter-points: 1) the fair use proviso is not universally applicable, even within its own legal jurisdiction, but is instead dependent on the meeting of four separate clauses which are to be determined at trial on a strict case by case basis; its applicability is thus far from a given; 2) there are no exemptions within the copyright clause in the book itself, and thus any applicability of third party exemptions is irrelevant to the violation of the clearly delineated terms themselves; 3) due to the potential utter lack of temerity of potential fair use claimants, even the *potential* applicability of fair use may never be initially broached in the first place; 4) fair use applies within strictly limited national territorial borders (*cf.* the international, wide-sprawling reach of copyright). The afore-delineated impingement of a copyright notice by way of mere reproduction of certain alphanumeric characters thus cannot be dismissed by a reference to potential exemptions unless such exemptions are, effectively without exemption themselves. Until precisely such a razor-sharp proviso is presented as evidence however (my research has turned up no such weaponry) the quite literal and perhaps unfortunate impossibility of any sort of copyright-clause sanctioned written discourse remains.

But lest we forget, we are not yet entirely through with our reading-through of the initial copyright clause of the book in question itself. It must further be noted that the incantation is sure to prohibit reproduction not only of any part, but in any form or by any means, "now known or hereafter invented." Thus not only is there no clearly delineated temporal limitation to the described prohibition (despite, once again, certain existent regional laws which may limit the legally-allotted duration of copyright), but quite to the contrary the notice extends itself into perpetuity, self-comfortingly assuring that no futurist manifestation

---

<sup>240</sup> Jonathan Band and Jonathan Gerafi. 2013. *The Fair Use/Fair Dealing Handbook*. <https://infojustice.org/~infojust/wp-content/uploads/2013/03/band-and-gerafi-2013.pdf>.

may be used to circumvent its present grip. If, to give but one utterly rational projection, in 10,000 years one were to stumble onto said text, and using a by then fully developed blink-based memory allocation which instantly dumped the contents of the book in question into one's brain-wired memory bank, one would thus still be in a clear violation of the book's copyright notice. But why venture so far into the uncharted future when the same violation may indeed be incurred in the present? The notice, once again quite explicitly, clearly prohibits the reproduction of any part of the book not only in writing or any other mechanical or electronic or any other means, but goes on to forbid the recording of any portion of the text "in any information storage or retrieval system". It thus constitutes a literal thoughtcrime to even recall any portion of the text (and thus, as previously discussed any singular character as well...) in one's head, considering that given that there is no explicit boundary definition provided for said information storage or retrieval system, it is thus not at all clear that the restriction doesn't extend into the brain.

The pedantry, or perhaps (over)emphasis on minutiae of legal copyright notice boilerplate undertaken herein constitutes what I term the *disjunctive embedding* component of hacker methodology. The method necessitates a deep burrowing into the given construct being examined, with the further aim of undoing or disjoining said construct, much like Foucault's aforementioned situated intellectual is in a position to engage in exposing the truth and knowledge formations localized to the intricacies of a specific discipline. Said embedding further disjoins the construct being studied not merely through application of external forces, but via the process of internal auditing itself: through close reading, contradictions inherent in the copyright clause itself which lead to its own undoing are thus brought to the fore.

Thus we have hitherto seen how that small ©, so easily overlooked, creates a vast bundle of seemingly impenetrable hurdles to the dissemination of information—through its assignment of copyright, its disarmingly 'acid-free' presentation, to its ultimate prohibition of even singular characters of a text in any medium in ultimate perpetuity. One may, as outlined previously, seek to void some of the ©'s enchantments through clumsy legal spells of one's own, which all invariably fall short in light of the overarching sorcery of the copyright notice. What's further, is that one cannot merely arbitrarily dismiss parts of the incantation as naught but overzealous fiction—say, the uncomfortable proviso against reproduction of portion of the book by any means—whilst nonetheless equally arbitrarily assigning credibility to other segments—say the overall belief in Intellectual Property proper.

Either the entire incantation is taken as literal truth, or it universally rejected as fiction. For if one were to start playing favorites, picking and choosing the portions thereof that are applicable, then likewise another can do the same, albeit assigning differing values to differing segments until the cumulative result will inevitably once again lead to an ultimate dismissal or complete acquiescence. To give a simplistic statistical example, which would of course be magnified hundreds of thousands of times in a ‘real world’ scenario: suppose that one divides the copyright notice into three segments, and chooses to accept the first as truism, and the second two as exorbitant exaggerations to be rejected off-hand. Let us then say that another comes along who promptly rejects the first, and whilst accepting the second, nonetheless rejects the third. A third personage then comes along and accepts the third clauses, but chooses to reject the first and second. At this point then, each clause has both been coded as a truth and a fiction, leading to both a net acceptance and net rejection of all terms. There is thus absolutely no room for a middling wavering which chooses to obey or disregard copyright policy piecemeal. The only two cumulative potentialities are thus either wholesale acceptance, which leads to the afore-described impossibility of any sort of written discourse or mental cognition or an utter rejection which logically leads one to a support of the unbridled promulgation of the unfettered stream of information, unbound by the impossible confines brought about by the ensconced and encircled shackling of ©.

Ultimately, despite the fact that modern-day copyright notice prohibitions bear mention of distinctly current technologies—‘electronic means’, ‘photocopying’, and, more recently, even ‘scanning’—they are in fact nothing more than contemporary incantations of ancient medieval book curses: frightening exultations against unauthorized reproduction placed on the inside covers by book scribes to ward off the potential pirate by way of fear mongering<sup>241</sup>. And whilst the comparison to book curses has been drawn to anti-piracy warnings present on DVDs—“ a book curse is essentially the same as that little FBI warning that pops up whenever you try to watch a movie: a toothless text charm included by the media’s maker meant to frighten the foolish. The charm only works if you believe that words are special, potent magic”<sup>242</sup>—an identical comparison logically applies to the same medium itself. Thus much like the book curse of yore is only effective in so much as one believes in the potency of the inscribed anathema which may lead to eternal damnation or accountability to hallucinatory higher authority, “[s]teal not this Book for fear of shame for there doth stand

---

<sup>241</sup> Drogin, *op. cit.*

<sup>242</sup> Carl Pyrdum. 2010. “Medieval Copy Protection”. *Got Medieval*.  
<http://www.gotmedieval.com/2010/08/medieval-copy-protection.html>.

the owners name for when you die the Lord will say were is that Book you stole Away”, so too is the present-day copyright incantation only effective in so far as one believes in its own invented mythology; its self-referential magic utterly powerless against unbelievers.

And yet for the moment, if one were to nonetheless indulge the beliefs of the copyright wizards, one need only take a gander at the esoteric arcana contained within their intellectual property grimoires to see how one could go about reversing their dark spell of content congealment. The Universal Copyright Convention (UCC) (as signed at Geneva on 6 September 1952 and revised at Paris on 24 July 1971 by international dabblers in the dark arts of Intellectual Property Rights), clearly states that in order for the copyright spell to have any matter of potency the Body of Work in question must “bear the symbol © accompanied by the name of the copyright proprietor and the year of first publication placed in such manner and location as to give reasonable notice of claim of copyright”<sup>243</sup>. To be sure, if we come full circle, so to speak, and in doing so find ourselves returning to the copyright notice discovered at the outset of Haraway’s, or in keeping with the decorum of the legal mannerisms of ownership, Routledge’s book, we indeed find precisely the symbol ©, the name of the copyright proprietor and the year of publication. If one were to then go around the literary mausoleums oft dubbed in the vernacular as ‘libraries’<sup>244</sup>, and proceed to remove the circle surrounding the c by way of application of an alchemical correction fluid, the spell would then, in accord with the dictates within the UCC spellbook itself, be effectively broken (though of course, as previously discussed, the copyright notice is itself no longer required for copyright to hold its latent spell over a work).

Turning towards the localized Code of Laws of the United States of America (USC) (and keeping in mind that, as with our earlier discussion of fair use provisions, the USC is not nearly as wide-reaching grimoire as the UCC, and is thus of only highly localized applicability without certain limited geographic borders), we find that this particular book of spells states differs from the UCC in that it states that a copyright incantation *may* appear alongside a work it seeks to protect with its charm, *but if it does* then “it shall consist of the following three elements: (1) the symbol © (the letter C in a circle), or the word ‘Copyright’, or the abbreviation ‘Copr.’; and (2) the year of first publication of the work; and (3) the name

---

<sup>243</sup> Universal Copyright Convention, Article III, §1. (July 24, 1971 )

[https://en.wikisource.org/wiki/Universal\\_Copyright\\_Convention#Article\\_III](https://en.wikisource.org/wiki/Universal_Copyright_Convention#Article_III).

<sup>244</sup> “Most graveyards are already unnecessary. Libraries, art museums, and academies are not worth the noise of one car gliding down the street. As a test, try sniffing the abominable stench behind piles of books--how many times superior is the fresh scent of gasoline!” (Hirato Renkichi. 1921. “Manifesto of the Japanese Futurist Movement” (trans. Miryam Sas), in *Cabinet* 13. 2004. <http://cabinetmagazine.org/issues/13/renkichi.php>).



of the owner of copyright in the work”<sup>245</sup>. While quite a few texts which strive to be mired in the sinkhole of copyright by malevolent IP sorcerers do indeed follow this straightforward syntax of {['©' ⊕ 'Copyright' ⊕ 'Copr.']+ [Year] + [Owner]}, the Routledge text we have been examining in fact does not. Instead, by stating that the text is “Copyright © 1997 by Routledge”, Routledge’s copyright incantation seeks to function as a “*postsignifying semiotic*, in which overcoding is assured by the redundancy of consciousness”<sup>246</sup>. The text is rendered as being copyrighted once, and then immediately afterwards copyrighted yet once more through a deploying of the syntactic shackling, which follows the initial, strictly linguistic mode of invoking ‘Copyright’-proper. Control over the Body of Work is thus sought after by a double-invocation. But unlike the merely signifying semiotic which is afforded the safety net of being “fully effectuated by the signifier, and by the State apparatus that emits it”<sup>247</sup>, postsignification is afforded no such protection in the USC grimoire. In other words, overzealousness is here the IP sorcerer’s grave undoing. Recall that the USC clearly states that the copyright notice must contain *either* the copyright symbol, *or* the word, *or* the abbreviation, as there is no mention of potentiality of the spell containing either/or the symbol/word/abbreviation, one must therefore interpret the incantation quite literally as presenting a series of exclusive disjunctions. If the notice thus contains more than one instance of copyright evocation it is then logically false; the spell cannot be cast.

Aside from serving to congeal the content contained within its icy grasp into a commodified Body of Work, however, the copyright notice further serves as an “evidentiary weight of notice”<sup>248</sup>, in that if an indentured book bears the brand of ©, then the legal coda shall give no weight to “to such a defendant’s interposition of a defense based on innocent infringement in mitigation of actual or statutory damages”<sup>249</sup>. One cannot say that one was unaware that the text was protected by darkest incantations, to claim ‘innocent infringement’ and beg for the court’s mercy as it were, if the text in question has the spell in plain sight. If one were to then proceed to rip out the copyright notice page of any treeware tomes one were to encounter, being sure to leave no trace fragments of (acid-free) paper in the binding and to promptly set them aflame so as to transform the page into an indecipherable form

---

<sup>245</sup> Copyright Act of 1976. 1976. 17 U.S.C. § 401 - “Notice of copyright: Visually perceptible copies”. <http://www.law.cornell.edu/uscode/17/401>.

<sup>246</sup> Deleuze and Guattari, *op. cit.*, p. 135.

<sup>247</sup> *Ibid.*

<sup>248</sup> Copyright Act of 1976, 17 U.S.C. § 401, *op. cit.*

<sup>249</sup> *Ibid.*

subsequently to be dispersed throughout the ether, or to simply delete the offending lines from an ebook and save the changed copy whilst overriding the old file, one would then free oneself of this particular exemption from the potentiality of appealing to ‘innocent infringement’. Though once again as previously mentioned, the fact that under the Berne Convention and the Berne Convention Implementation Act, the notice is itself no longer necessary for copyright claims, all recourse to innocence has been stripped away from copyright, with perhaps only its logical counterpart—guilt—remaining. And thus we see here manifested over and over again the straightforward fact that even when approached on its own legal, or magical, terms and conditions, the minutiae and particularity of the copyright incantation oft lead to its own undoing.

### **2.1 The © is harder to ©**

So much for ©. We need not belabor the fettering of content ushered in by copyright incantations at any greater length here, for this particular shackle has already been gnawed on at great length by a formidable army of copyright reformists<sup>250</sup>, a hodgepodge of “left-leaning cyber and legal critics”<sup>251</sup>, who seek not to aid in the unconditional liberation of information, but to erect naught more than bigger cages and longer chains under the various guises of alternative licensing schemas dubbed copyleft. Having contented themselves in gnawing at the rotting fleshy exterior—©—they have not only left the underlying bone of Intellectual Property proper untouched, but have indeed proceeded to begin to robe the now-bare bone with a new exterior of copyleft, the nefariousness of which is rendered all the greater than traditional © precisely through its presentation by the reformists as a panacea against draconian copyright measures. By being rendered as a better alternative to copyright, copyleft functions to acquiesce the populace into acceptability of Intellectual Property as a repressive form of content congealment, so long as its not ©, but of course in advocating the use of copyleft, the larger agenda (identical to ©) of promulgating the wholesale fettering of Bodies of Work via Intellectual Property Rights is not only not challenged, but is indeed entrenched all the further. The interests of the copyleft proponents thus lie not in the destruction of IP and the liberation of information, *but in the assurance of its continued enslavement.*

In other words, copyleft merely replaces the “thou shall not...” admonition of copyright with the faux-permissibility of ‘thou shall’, akin to replacing the stern parent who

---

<sup>250</sup> *Op. cit.*, see Footnote 1.

<sup>251</sup> Ted Striphas, *op. cit.*, p. 250.

admonishes the child with “you can't go out tonight” with one who instead intones “you can go out, just be back by ten”. The underlying problem being that in both cases someone allocates permission, and in turn punishment for transgression. And in so doing, not only does copyleft not challenge the underlying foundation of IP itself, that cultural works may be owned by authorized parties and distribution thereof controlled by said parties and their legal agents, but conversely it instead entrenches the notion all the further by rendering it all the more palatable.

Lawrence Lessig, a founding member of the Creative Commons board of directors<sup>252</sup>, an organization which cobbled together quite a number of horrifying copyleft fetters which render the old-school © woefully impotent by comparison that will be dealt with in short order, and one of the most visible proponents thereof, who oft calls for a ‘free culture’ (‘free’ here being used as a neoliberal shorthand for ‘free market’; and thus Lessig can much more fittingly be said to advocate a ‘free market culture’), is quick to point out that:

[a] free culture is not a culture without property; it is not a culture in which artists don't get paid. A culture without property, or in which creators can't get paid, is anarchy, not freedom. Anarchy is not what I advance here. Instead, the free culture that I defend in this book is a balance between anarchy and control. A free culture, like a free market, is filled with property. It is filled with rules of property and contract that get enforced by the state<sup>253</sup>.

The initial point of note here is the most curious equating of lack of payment with a lack of freedom. According to Lessig then, any society—past, present, or future—which lacks either a market economy or any other form of ‘payment’ cannot be a society of freedom. When Lessig's strictly neoliberal—being predicated upon notions of contemporary free market transaction—conceptualization of freedom is thus taken into account, it then comes as no surprise that freedom is in turn juxtaposed against not only lack of payment, but with anarchy. Any potential confounding of anarchy—a lack of rulers—with anomie—a lack of rules—on Lessig's part notwithstanding, it rationally follows that if freedom is defined as the freedom to sell labor and property, then of course a state of anarchy, which by general definition promotes a culture built upon egalitarianism and mutual aid as opposed to crass proprietarian congealment, becomes antithetical to Freedom<sup>TM</sup>. What may otherwise be logically

---

<sup>252</sup> Creative Commons. “Creative Commons Board of Directors”.  
<https://creativecommons.org/board#lawrencelessig>.

<sup>253</sup> Lessig, *Free Culture, op. cit.*, p. xvi.

interpreted as a singular binary, anarchy/freedom being one and the same, is nonetheless economically, rhetorically, and of course politically coded by Lessig as the most stringent of oppositions. As the aforementioned Nimus piece further states:

[t]he argument is no longer that the author is a fiction and that property is theft, but that intellectual property law needs to be restrained and reformed because it now infringes upon the rights of creators. Lessig criticizes the recent changes in copyright legislation imposed by global media corporations [...] But he does not question copyright as such, since he views it as the most important incentive for artists to create<sup>254</sup>.

Thus not only do Lessig and other copyleft proponents of his ilk seek to entrench the notion that content can and should be congealed, albeit in highly specified and controlled shackles, but by doing so they further seek to shift the ongoing copyfight from a position of insurrectionary immanence to that of tepid reformism.

To limit the copyfight to mere copyright is to ignore that copyleft/right are two sides of the same one-sided coin of Intellectual Property. If the aim is to achieve maximal unbridled dissemination of information, then adherents of copyleft must be skewered one and all, much as they seek to steamroll the wholesale rejection of IP via their rolling out of the copyleft Trojan horse. In order to usher in an unbridled data flow that cannot and will not be channeled nor compartmentalized into rigid fetters of segmentation at the throes of a magical rights holder, the mask of copyleft reformist must be torn off. Make no mistake about it— whilst masquerading behind provocative sub-titles akin to *The Rise of Intellectual Property and How It Threatens Creativity* and *How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity*, which seemingly present the texts and thus their authors as being firmly in the anti-IP battalion, they are nonetheless vehemently in defense of intellectual property. There are then one of two ways to read the aforementioned textual titles. If Vaidhyathan describes his book as being about the threat IP poses to creativity, and then goes on to state that he hopes that the very same book will help to “yield a more just and efficient copyright system”<sup>255</sup>, as indeed he does, then he either does not view the threat to creativity as an undesirable outcome in the least, which would then serve to explain his unabashed desire to propagate intellectual property (albeit in the form of ‘a more just and efficient [efficient at what?] system’), or he only views that a specific form of IP is a threat to

---

<sup>254</sup> Nimus, *op. cit.*

<sup>255</sup> Vaidhyathan, *op. cit.*, p. 8.

said creativity, in which case the overly broad, inappropriate title amounts to a tactical case of deception designed to lure the wayward anti-IP copyfighter to his set snare, thereby either potentially hoping to convert him to mere reformism, or to keep him sufficiently distracted and subdued in the very process of reading a deceptive text.

Likewise, we find that the writings of the aforementioned Lessig, who is oft erroneously billed along the lines of “propagat[ing] a new culture of sharing and participation”<sup>256</sup>, are at times indistinguishable from the standard exultations and accompanying defenses of traditional copyright<sup>257</sup>, in that both repeatedly elucidate the merits of the overarching system of domination via Intellectual Property Rights, with Lessig’s feeble injunctions amounting to a desire to allocate a bottle of skin lotion to Bodies of Work to clear up that most unsightly chafing caused by the uncomfortable fetters of ©.

Aside from doing their part in perpetuating the enclosure of data streams, under whatever veneer of righteous reformism they choose to adopt, there is furthermore a peculiarly localized air of American liberalism imbued in the reformist literature. There is indeed an incessant reference to American rights that translates into a kind of legal colonialism, a harking back to the colonial times of yore when copyright restrictions were less stringent. Unlike the previous discussion of American fair use provisos in this operations manual, which were nonetheless clearly tempered with a note as to their gross inadequacy due to their global inapplicability, as well as unlike the previous examination of the history of American copyright notices—which, while historically situated in a particular geopolitical context, did not represent an exultation thereof—the reformists’ reference to strictly localized American historicism is unrestrained by any such geographic cognizance. Instead, the reformists adopt a remarkable doublethink which allows someone like Vaidhyathan to repeatedly appeal to an American history of copyright, stressing for instance that “it is essential to understand that copyright in the American tradition was not meant to be a ‘property right’”<sup>258</sup>, whilst simultaneously being sure to caution us that “we cannot appeal to

---

<sup>256</sup> Christian Meier. 2007. “Intellectual Property 2.0: Lawrence Lessig Defends Creativity in the Age of Cyberspace”, in *The Berlin Journal* 14. p. 49.

[http://www.americanacademy.de/uploads/media/BJ14\\_web\\_100dpi\\_01.pdf](http://www.americanacademy.de/uploads/media/BJ14_web_100dpi_01.pdf).

<sup>257</sup> cf. “Copyright is a critical part of the process of creativity; a great deal of creativity would not exist without the protections of the law. Without the law, the incentives to produce creative work would be vastly reduced. Large-budget films could not be produced; many books would not get written. Copyright is therefore an integral and crucial part of the creative process. And as it has expanded, it has expanded the opportunities for creativity” (Lessig, 2001, *op. cit.*, p. 121), and “[p]rotection of content owners’ rights is essential if the electronic marketplace is to fulfill its promise...” (Edward D. Horowitz. 1998. “The Ascent of Content”, in *The Future of the Electronic Marketplace* (ed. Derek Leebaert). London: The MIT Press. pp. 91-112. (p. 101)).

<sup>258</sup> Vaidhyathan, *op. cit.*, p. 11.

the founders' wishes or republican ideals"<sup>259</sup>. Similarly, whilst attacking the Digital Millennium Copyright Act (DMCA), a piece of American legislation designed to corral data streams all the further, Vaidhyathan's admonishment of the DMCA is seemingly based on its erosion of older American legal doctrine (i.e. "the DMCA erodes the 'first sale doctrine'"<sup>260</sup>). Hence the reformist attack on the DMCA is at best an appeal to recursion, to the reimposition of some sort of older legalistic obstructions to data flow, as opposed to disparagement of the DMCA *qua* ahistorical congealer of content dissemination. Not only do reformist refrains thus repeatedly promulgate the view that intellectual property 'used to be good' but has since been led astray, but that these historical arguments are further firmly situated within restrictive national borders of an otherwise decidedly global struggle.

The problem with existent draconian [American] laws then, according to our reformists, is merely that they override older, presumably less draconian [American] laws. One can only imagine that in half a century, a new stream of reformers will be hailing the DMCA as a benign alternative to the, by then, newly proposed IP legislation. In a similar vein, McLeod treats us to a distinctly Americanized history of copyright, being sure to nod whimsically in approval along the way: "they're the very reasons why the framers of the Constitution established copyright and patent law: so that society would benefit from a rich culture accessible to all. Thomas Jefferson and the other Founding Fathers were thoughtful, and got it right"<sup>261</sup>. Oddly, the foundations of this castle built amidst the air are never brought to task by our reformers, which is to say a questioning of why, other than by virtue of being thoughtful, are the notions allegedly held by the Founding Fathers 'right'; appeals to 'democracy', 'constitutional rights', and the like are never questioned, at least not by those who evoke them. And yet such superfluous nationalist grounding can be whisked away with a simple inquiry, an inquiry that modestly asks of what relevancy is an appeal to some country's copyright history? And more pointedly, how does this appeal serve to undermine the tyranny of intellectual property? On the contrary, it would seem that merely replacing one legalistic imposition against data dissemination with another, older inhibition merely serves to further legitimize control of content flows, akin to the reformist call for prisons with better lighting conditions rather than an evocation of wholesale prison abolition. Longer chains, perhaps their thinking goes, so that we can longer recognize the imposed segmentarity if the

---

<sup>259</sup> *Ibid.*, p. 252.

<sup>260</sup> *Ibid.*, p. 175.

<sup>261</sup> McLeod, *op. cit.*, p. 9.

links fade away into the horizon, amidst the glare from the setting sun of copyright, and the rising moon of an equally oppressive copyleft.

It is, however, certainly true that some of the reformists attempt to at least somewhat distance themselves from a pronounced Americanism. Lessig, for instance, is careful to cloak his Constitutionalism in the airs of transnationalism: “[l]iberty in cyberspace will not come from the absence of the state... We build liberty as our founders did, by setting society upon a certain constitution...”<sup>262</sup>, being quick to point out that he is “not trying to sell a document that our framers wrote in 1787”<sup>263</sup>. The question that of course here arises is precisely which of ‘our’ founders and which ‘certain constitution’ Lessig speaks of, and why perchance should the domain of cyberspace be dominated by their, presumably nationalist, values? As Strangelove points out, Lessig’s (though the line of argumentation indeed applies to Vaidhyathan, McLeod and other nationalist reformists as well) repeated reference to American constitutionalist values lends itself to “just another form of tyranny; in this case, the tyranny of one set of culturally specific values over all others”<sup>264</sup>. Unfortunately however, Strangelove’s appeal to globalism, to international standards of conduct, with the example of the suppression of so-called ‘hate speech’, leads him to advocate an even more stringent repression of data dissemination than all of our previous reformists thus far.

Much like the American constitutionalists seek a reigning in of copyright to adhere to the intentions of the ‘founding fathers’ (whatever and whoever those may be), Strangelove instead bases his argument for congealment on a “multiculturalism and pluralism”<sup>265</sup>—which is in fact anything *but*, being instead akin to a microfascism that eludes clear categorization unlike the aforementioned Americanized constitutionalism, “[f]ascism [being] inseparable from a proliferation of molecular focuses in interaction, which skip from point to point, *before* beginning to resonate together in the National Socialist State”<sup>266</sup>. And it is precisely this resonance to which Strangelove attunes to when observing that “most countries also restrict hate speech”<sup>267</sup>; towards a construction of a cyber-totalitarian imposition of control over data flow, built upon the collusion of a plethora of international microfascist black holes in the form of the aforementioned hate speech laws, masquerading under here conveniently

---

<sup>262</sup> Lessig (2006), *op. cit.*, p. 4.

<sup>263</sup> *Ibid.*

<sup>264</sup> Michael Strangelove. 2005. *The Empire of Mind: Digital Piracy and the Anti-Capitalist Movement*. Toronto: University of Toronto Press. p. 67.

<sup>265</sup> *Ibid.*

<sup>266</sup> Deleuze and Guattari, *op. cit.*, p. 214.

<sup>267</sup> Strangelove, *op. cit.*, p. 67.

coalescent singular pluralisms. To explain matters in another way, whilst Lessig & Co. propose a platform for copyright reform predicated upon the singular notions of a particular nation state, effectively stating ‘it is/was so in the US, let it thusly be likewise the world over in cyberspace’, Strangelove while dismissing such a proposal as being symptomatic of a domineering nationalism, nonetheless aims to put forth a curtailment of unbridled data dissemination based on a dispersed international standard of congealment—‘many countries attempt to control information flows they deem to be ‘hate speech’, let it thusly be likewise the world over in cyberspace.’ Both lines of argumentation hence stem from a desire to deploy peculiar (inter)national legal coda as fetters of content promulgation. In both cases an externality in the form of a legal shackle is thus latched around an unwitting Body of Work. Appeals towards copyright reform rooted in either nationalism or internationalism thus both attempt to control information flow by appeals to varying legal coda, subjugating dissemination to the restrictive terrain of legalism (or calling for reform of said legalism); in contrast, the methodology deployed throughout this study adopts a non-legalist approach, thus cutting through juridical fetters towards univiscid flow of data dispersal.

### **2.1.0 \$ floats in the ☺**

In a further attempt to corral and congeal, to control and contort otherwise unbridled streams of data, albeit under the guise of benign intention, the reformists oft make explicit reference to a soothing economic pragmatism. “There is a widespread tendency to portray the Internet audience as a collaborator with the commercial sector”<sup>268</sup>, to make the digital mash of information palatable to the tentacles of capital. Aberrations—piracy and the like, unauthorized data channels and transmissions—are explained away as rational actions of a temporarily distraught costumer base that is apparently all too eager to be lured back into the seductive throes of capital, complete with all of the aforementioned trappings of intellectual property congealment—so long as the price were a bit lower! Thus Vaidhyanathan muses that “the MP3 movement is a rational revolt of passionate fans. Compact discs cost too much”<sup>269</sup>. McLeod similarly seeks to soothe the pangs of content congealers, “[w]hile there are always going to be freeloaders who will never pay for music, that doesn’t characterize the majority of fans who share music”<sup>270</sup>. There thus appears to be an evident strain of appeals to the potentiality of ‘business as usual’, given perhaps some market price adjustment. Piracy is thus explicitly depoliticized, seen as either a temporary straying from the flock, to be

---

<sup>268</sup> *Ibid.*, p. 7.

<sup>269</sup> Vaidhyanathan, *op cit.*, p. 179.

<sup>270</sup> McLeod, *op. cit.*, p. 299.



rectified following the initiation of aforementioned reforms (lower prices and more lenient remix licenses), or as a potential marketing vector to increase future business. That the act may be seen as a rejection of the market, either conscious or unconscious, appears to be inconceivable.

The Critical Art Ensemble indeed has an entire chapter outlining ‘the financial advantages of anti-copyright’, “the faster the information is disseminated, the better it is for the many discourses to which the information is relevant, and on the individual level, more money will be generated”<sup>271</sup>. There is thus an incessant desire to reassure business interests that there is indeed money to be mined from all digital enclaves, that the dissemination of information congealed under untraditional copyright terms—and even via a wholesale rejection of copyright, as seen above, not merely via copyleft—is still profitable, that most actors are thus eternal-consumers, only requiring an affordable train ticket with more leg room to hop back on their segmented compartment, embracing their apparently long faithful partner named Molarity after a brief fling with the molecular quanta of unauthorized transmission (i.e. data piracy). The mistake, of course, lies in presupposing that data piracy itself is somehow a distinct plane with clear boundaries and modes of conduct.

Whilst this construction is doubtlessly necessary for the libertarian agenda of soothing the pangs of capital, it nonetheless overlooks that “there are only multiplicities of multiplicities forming a single assemblage, operating in the same assemblage”<sup>272</sup>. Hence, all the while exonerating the success of online MP3 retailers, “iTunes sells convenience, trust, you feel you’re giving back to the artist”<sup>273</sup>, Mason wholly ignores the potentialities that not only may those who purchase legally sanctioned, congealed segments of copyrighted data then be turning around and freely distributing, remixing, and de/reassembling them at their leisure, but that even the transactions themselves may be made using fraudulent credit card numbers or generated gift card codes that just happen to coincidence to iTunes’ own algorithms. Thus “there is no question...of establishing a dualist opposition between the two types of multiplicities, molecular machines and molar machines; that would be no better than the dualism between the One and the multiple”<sup>274</sup>. The soothing of capital thus presents a unifying molar concentration masquerading under apparent molecularity: consumers may

---

<sup>271</sup> Critical Art Ensemble, *op cit.*, p. 152.

<sup>272</sup> Deleuze and Guattari, *op. cit.*, p. 34.

<sup>273</sup> Matt Mason. 2008b. Interview. *My Media Musings*.

<http://mymediamusings.files.wordpress.com/2008/03/matt-pc1.mp3>.

<sup>274</sup> Deleuze and Guattari, *op. cit.*, p. 34.

have different reasons for turning to pirated goods, but they all may come back once a few augmentations are made to the goods legally distributed by the market. The BoW is thus the physical manifestation of the copyright reformists answer to the BwO<sup>275</sup>.

The reformists cannot hope to *call back* pirates to join the rank and file orders of commodified congealment, for the reason that the former are always already enmeshed with the latter, intersecting at all angles, demolishing dams that seek to inhibit dissemination all whilst constructing new paths from the wreckage of their predecessors, which can, in turn similarly be demolished as the unbridled tides of information continually reject the tethers of intellectual property. That a consumer can likewise be a pirate, indeed facilitate piracy through purchase, is intrinsic in the standard ‘it only takes one’ line of argumentation which stipulates that only one person need to figure out how to remove DRM for all others to benefit from it<sup>276</sup>; the latent consumer being intrinsic because others may then proceed to legally purchase the DRMed items and then strip away the DRM and distribute the files or may simply wait for others to do so. Similarly, while some web communities exist with the explicit intention of DRM removal<sup>277</sup>, there is no reason to make the assumption that were DRM no longer to be employed, that piracy would cease and all would go back to legally purchasing cultural products, as is the implication in the aforementioned reformist intonations of amendments to marketing and selling procedures. Aside from the tautological certainty that removal of DRM would of course cease for new items if said new items had no DRM, no such certainty can be provided for the broader abatement of piracy as a whole.

In following along this tether of presumed economic complacency, we see that the reformists aim not only to convince their silent business partners of the financial tenability of digital distribution, but they further seek to convince users themselves that legalized congealment is a safer, *rational* alternative to unauthorized piracy. This is, of course, a crucial aspect of their argument, for in order to convince corporate interests they must also convince someone to actually make a—and ideally much more than a singular one—purchase, to conjure forth an agreeable market full not only of congealed constructs akin to DRMed iTunes music files, but also full of consumers all the more willing to partake in said congealment. *Mutiny will not be tolerated aboard the good ship capitalism!* screams Mason

---

<sup>275</sup> “The BwO: it is already under way the moment the body has had enough of organs and wants to slough them off, or loses them” (Deleuze and Guattari, *op. cit.*, p. 150).

<sup>276</sup> See, e.g., Thierry Rayna and Ludmila Striukova. 2008. “White Knight or Trojan Horse? The Consequences of Digital Rights Management for Consumers, Firms and Society”, in *Communications & Strategies* 69. p. 121 (pp. 109-125).

<sup>277</sup> E.g., DRM Removal. 2014. *Reddit*. <https://pay.reddit.com/r/drmremoval>.

at the top of his lungs: “Pirates are taking over the good ship capitalism, but they’re not here to sink it. Instead they will plug the holes, keep it afloat, and propel it forward. The mass market will still be here for a long while”<sup>278</sup>. Recall the twin goals of the libertarian reformists: to convince corporations that they can beat pirates at their own game, so to speak, an argument that the *Wired* crowd has similarly espoused<sup>279</sup>, and secondly by creating a substantial market base of willing participants in this legalized control of data.

As aforementioned, it is precisely by convincing the readers that there are ‘safer’ more ‘trustworthy’, legal alternatives to unauthorized distribution, that Mason’s initial prophecy—that of the wonderful opportunities for late capital in the digital terrain—is fulfilled! This forced binary fission of consumer/pirate is oddly vested in the presumed faithful of the actors involved to these very same rigidly molar lines of segmentarity. To yearn for a leakproof ship, as Mason does, is to ignore the fact that it is already long-submerged in the throes of the sea of unbridled data exchange. And to patch the ship, an impossible task to be sure, would likewise be to drain the seas.

There is no certainty that data streams will follow the traces of segmentation outlined by capital, copyright/left/\*, or their respective apologists. Which is not to say that data flows will not interact with said traces. Indeed the fact that they already are already interacting—the friction evinced by DRM and unbridled dissemination—can be evinced, for instance, by the various existent programs designed to strip DRM from purchased iTunes audio and video files to facilitate their distribution through unsanctioned channels<sup>280</sup>. And yet, the question of totalizing subsumption<sup>281</sup> of pirate modes of dissemination is far from certain. Whether speaking of capitalist appropriation of and intrusion into existent pirate modalities (formal subsumption)—as manifested for instance by film studios utilizing the BitTorrent protocol to distribute films<sup>282</sup>—or of capital’s entire restructuring of existent ecosystems and the creation of new distribution mechanisms (and hence likewise new dependent social relations governing the use thereof) designed to meet business imperatives (real subsumption)—as for

---

<sup>278</sup> Mason, *The Pirate’s Dilemma*, *op. cit.*, p. 240.

<sup>279</sup> *cf.* “Free music is just publicity for a far more lucrative tour business. Nobody thinks of this as piracy...” (Chris Anderson. 2008. “Free! Why \$0.00 Is the Future of Business”. *Wired* 16 (3). [http://www.wired.com/techbiz/it/magazine/16-03/ff\\_free](http://www.wired.com/techbiz/it/magazine/16-03/ff_free)).

<sup>280</sup> E.g., RapidSolution Software AG. 2010. Tunebite. v. 7.2. <http://www.audials.com>; Brahms. 2012. Requiem. v. 4.1. <http://digiex.net/downloads/download-center-2-0/applications/11796-requiem-4-1-remove-itunes-drm-fairplay-music-video-books.html>.

<sup>281</sup> Jason Read. 2003. “The Real Subsumption of Subjectivity By Capital”, in *The Micro-Politics of Capital: Marx and the Prehistory of the Present*. Albany: SUNY Press. pp. 103-151.

<sup>282</sup> Ernesto. 2011b. “BitTorrent Tracker Becomes Official Movie Distributor”. *TorrentFreak*. <https://torrentfreak.com/bittorrent-tracker-becomes-official-movie-distributor-110428/>.

instance evinced by the founder of the cyberlocker website Megaupload planning to start a music service<sup>283</sup> and, earlier the music downloading service Napster undergoing a wholesale legalized makeover<sup>284</sup>—there nonetheless exist the potentialities of overflowing, whether in the sense of an operaismo-like (re)appropriation of production (and distribution) processes<sup>285</sup>, or in the sense of the data itself spilling over outside structured distribution channels<sup>286</sup>. That capitalist strategies of free appropriation have failed to successfully enclose data flows, failed, that is, to plug their imaginary ship afloat the digital waters, can be illustrated by posing the counterexample to every mangled tentacle they outstretch. For instance, Radiohead’s release of their album for a voluntary fee (which nonetheless also necessitating a minimal transaction fee)<sup>287</sup>, Nine Inch Nails’ completely free release of their album<sup>288</sup>, and so on, have all shown up on nonetheless seemingly unauthorized channels, with their respective syntactic shackles, whether operating under copyright or creative commons copyleft license, all strewn aside<sup>289</sup>.

And yet there is a sense that the reformists have themselves already felt the fear of their sinking ship, for they are still caught up in the binary delusion, and thus, contrary to their ‘forward-looking’ embrace of alternative modes of data repression (copyleft et al.), have in actuality been engaged in a reactionary stifling of even those alternate data channels themselves. Take, for instance, Mason’s exhibition of ‘proof’ of his aforementioned prophecy of pirates patching up his good ship Capitalism, “[t]his book you are holding—static words printed on thin slices of dead tree brought to you by a large media company—is living proof of that. The book industry has been fortunate: books are some of the easiest things to pirate, yet the majority of book readers still choose the treeware versions rather than

---

<sup>283</sup> Ernesto. 2013c. “Kim Dotcom Teases New Music Service... Baboom”. *TorrentFreak*. <http://torrentfreak.com/kim-dotcom-teases-new-music-service-baboom-130907/>.

<sup>284</sup> Emily Farache. 2001. “Napster Goes Legit”. *E! Online*. <http://eonline.com/news/41734/napster-goes-legit>.

<sup>285</sup> Alberto Toscano. 2009. “Chronicles of Insurrection: Tronti, Negri and the Subject of Antagonism”, in *Cosmos and History: The Journal of Natural and Social Philosophy* 5 (1). <http://cosmosandhistory.org/index.php/journal/article/view/128/240>.

<sup>286</sup> “The mistake was damaging and resulted in the exposure of five scripts and the first six unfinished episodes from Series 8 on a publicly accessible FTP site [...]” (BBC Worldwide. 2014. “BBC Worldwide update on Doctor Who leaks”. *BBC*. <http://www.bbc.co.uk/corporate2/mediacentre/worldwide/2014/doctor-who-update>).

<sup>287</sup> Angela Monaghan. 2007. “Radiohead challenges labels with free album”. *The Telegraph*. <http://www.telegraph.co.uk/finance/markets/2816893/Radiohead-challenges-labels-with-free-album.html>.

<sup>288</sup> Jeff Leeds. 2008. “Nine Inch Nails Album Is Free Online”. *The New York Times*. <http://www.nytimes.com/2008/05/06/arts/music/05cnd-nine.html>.

<sup>289</sup> Official distribution channels: Nine Inch Nails. 2008. *The Slip*. <https://dl.nin.com/theslip/signup>; Radiohead. 2007. *In Rainbows*. <http://www.inrainbows.com/>. (Presumably) unofficial pirate distribution channels: KickassTorrents. 2014. “radiohead in rainbows results 1-25 from 111”. <https://kickass.to/usearch/?q=radiohead+in+rainbows>; “nine inch nails the slip results 1-25 from 52”. <https://kickass.to/usearch/?q=nine+inch+nails+the+slip>.

downloading software-based substitutes”<sup>290</sup>. It is intriguing that the treeware copy of Mason’s text was released several months prior to an ‘authorized’ digital version—for, as it is indeed one of the ‘easiest things to pirate’, merely a matter of him dragging a file from his local hard drive to one of the multitude of online storage facilities, why not release a digital copy simultaneously with the treeware release?

There is thus a lurking fear, a hesitancy as it were, to open the floodgates, though even then the text was inscribed with the typical provisions against illicit modification or distribution. Yet even texts which are overtly marked with anti-copyright (not copyleft) insignia, as for instance the books published by the Critical Art Ensemble<sup>291</sup> or the CrimethInc. Ex-Workers' Collective<sup>292</sup>, are restrained by yet another form of control. For while their texts are explicitly labeled as standing against intellectual property, inviting all to freely plagiarize or otherwise modify and disseminate the data at whomever’s whim, their *initial* distribution is nonetheless tightly corralled. Whether said initial control is for economic or psychological reasons is irrelevant, as the outcome: the imposition of artificial scarcity in an attempt to congeal unbridled dissemination into authorized channels of static flow.

Furthermore, those agents who are, at least in word, against the congealment of data dissemination, and yet nonetheless partake in a forced choking of data outpours. Not only are digital versions of anticopyrighted texts often delayed, but they are often nonexistent altogether on the parts of those who release the treeware attacks on copyright themselves. Much of today’s propaganda is composed in front of a computer terminal. A digital copy is then sent to a publisher, or perhaps directly to a printer, with the treeware artifacts—data congealed by virtue of a restrictive form, the cursed printed page—being the only counterpart that sees widespread distribution. Meanwhile, while the accompanying license (or anti-license, as it were), certainly invites others to digitize the copy by scanning it in or what have you, that digital version conjured by the producers themselves continues to sit snugly on

---

<sup>290</sup> Mason, *The Pirate’s Dilemma*, *op. cit.*, pp. 239-240.

<sup>291</sup> E.g., “Anti-copyright 2006. Autonomedia and Critical Art Ensemble. This book may be freely pirated and quoted. The authors and publisher, however, would like to be so informed at the address below” (Critical Art Ensemble. 2006. *Marching Plague*. Brooklyn, NY: Autonomedia. p. 4.).

<sup>292</sup> E.g., “N©! 2004. The publishers, the notorious CrimethInc. ex-Workers’ Collective, humbly put this book and all its contents at the disposal of those who, in good faith, might read, circulate, plagiarize, revise, and otherwise make use of them in the course of making the world a better place. Possession, reproduction, transmission, excerpting, introduction as evidence in court, and all other applications by any corporation, government body, security organization, or similar party of evil intent are strictly prohibited and punishable under natural law” (CrimethInc. ex-Workers’ Collective. 2004. *Recipes for Disaster: An Anarchist Cookbook*. Olympia: CrimethInc. ex-Workers’ Collective. p. 6).

their drive. Thus control over data dissemination is exerted through a willful delay of digital distribution, with the sole digital artifact taking on the same role as a prized film negative, or an original pressings of a compact disc. Thus, for instance, Critical Art Ensemble books are not made freely available on their website until months, or even a year, after the initial publication and commencement of the sale of the treeware versions<sup>293</sup>, nor are CrimethInc. available online from CrimethInc. if they are still in print, and are instead sold on their web store<sup>294</sup>.

The control exerted by digital congealment intersects with, indeed wildly clashes with, any lip service paid to the virtues of data dissemination. A disjuncture borne forth of hypocrisy which nonetheless allows us to see that there is no purity of practice, no clear binary cessation; rather, the snake's treacherous tongue interweaves, ultimately stinging itself. Thusly, "between the segments of one articulation and the segments of the other there are biunivocal relationships obeying far more complex laws"<sup>295</sup>. That is to say, whilst it has hitherto tacitly been argued that the aforementioned alternative distribution vectors (e.g. the torrent files of the Radiohead and the Nine Inch Nails albums), there is no underlying evidence that the legal content owners themselves did not place the albums onto the torrent networks, albeit clandestinely so as to perhaps avoid legal complications with any corporate entities they find themselves entangled with during the legally-sanctioned releases of the albums. Similarly, whilst neither CrimethInc. nor the Critical Art Ensemble made copies of the aforementioned texts available on their official websites, perhaps they leaked pirate copies onto other unofficial distribution channels. Similarly, the assumption in studies of the content on filesharing networks appears to presume that the content was placed there not by the legal content owners but by illicit distributors, whilst no evidence is presented to substantiate this pivotal assertion passed off for fact<sup>296</sup>. It would thus be potentially erroneous

---

<sup>293</sup> E.g., *Marching Plague* was released in May of 2006 ("May 1, 2006" as per: Amazon. "Marching Plague". <http://www.amazon.com/Marching-Plague-Warfare-Global-Public/dp/157027178X/>; "24 May 2006" as per Eyebeam. "Marching Plague from Critical Art Ensemble". <http://eyebeam.org/events/marching-plague-from-critical-art-ensemble>); however, their website did not have PDF links to the book until May 24, 2007 (as per Internet Archive Wayback Machine. <https://web.archive.org/web/20070612035716/http://www.critical-art.net/books/mp/index.html>). Lest the argument be made that the Wayback machine did not an earlier archival of said webpage, it can be pointed out that as of April 6, 2007 (the earliest archive prior to May 24, 2007 - <https://web.archive.org/web/20070406135154/http://www.critical-art.net/books/index.html>), the book was not listed on the Critical Art Ensemble's webpage (or at the least not on the Wayback Machine's version thereof).

<sup>294</sup> CrimethInc. Ex-Workers' Collective. 2014. Web Store - Recipes for Disaster. <http://www.crimethinc.com/books/rfd.html> (listed price: \$12).

<sup>295</sup> Deleuze and Guattari, *op. cit.*, p. 41.

<sup>296</sup> E.g., a typical study, discussing Peer-to-Peer filesharing, states "these applications are typically used illegally to transfer copyrighted materials", but provides no evidentiary support for said claim (Brett J. L. Landry and

to presume that the operative assumption—that files shared on filesharing ecosystems are shared illegally—is correct. A study which aims to test the validity of such claims of illegality would, *as its mere starting point* have to enact the following: gather (download) and review all content on a particular ecosystem to verify that it corresponds to the given title, and would then further have to contact the copyright/left holder for each item to verify whether or not authorization has been procured. I could not locate a study which has as of yet attempted an evidence-based expatiation of the legality of data on filesharing networks.

Having thus far analyzed the problematic pitfalls of copyleft in terms of mere generalities, theoretical and otherwise, let us now turn to a close reading of three particular instances or potentialities of copyleft so as to further bring to the fore the nefariousness thereof by looking at 1) Verso Books, 2) Creative Commons, and 3) the Free Software Foundation.

### **2.1.1 VERSO**<sup>297</sup>

Returning once again to performing a specific paratextual reading of intellectual property incantations, albeit this time choosing one which bears the mystical insignia of copyleft rather than copyright, we find ourselves staring at the front matter of a number of Verso books. Verso, an imprint of New Left Books, which is in turn created by the *New Left Review*, bills itself as “the largest independent, radical publishing house in the English-speaking world [...] with a strong list and radical commitment”<sup>298</sup>. To be sure, quite a number of Verso texts bear the traditional copyright incantation akin to the one previously found in the Haraway/Routledge text. For instance, the Verso-published *Companion to Marx’s Capital* includes the following typical incantation in the folds of its front matter:

Copyright © David Harvey 2010

All rights reserved

The moral rights of the author and translator have been asserted<sup>299</sup>

Whilst this particular spell is nearly identical to the one previously found in the Routledge text, there are nonetheless some admittedly key distinctions between the two. For instance,

---

Dinah Payne. “Technical Perspectives of Illegal P2P File Sharing: Available Technical Solutions”, in *International Journal of Services and Standards* 2 (3). pp. 228-237 (p. 228).

<sup>297</sup> This particular economico-syntactic rendition of the publisher’s name is quoted from the title of <https://fckvrso.wordpress.com/>, a website devoted to making Verso (and other similar) texts freely available online.

<sup>298</sup> Jacob Stevens. “About Verso”. <http://www.versobooks.com/pg/about-verso>.

<sup>299</sup> David Harvey. 2010. *Companion to Marx’s Capital*. London: Verso Books. N.B. Though it is of course far from certain whether Harvey actually authored the copyright incantation himself, and thus a more fitting citation may here be: Anonymous. 2010. *Companion to Marx’s Capital*. Verso Books; or perhaps Verso. 2010. *Companion to Marx’s Capital*. Verso Books, with the same uncertainty of citation applying to all other quoted copyright/left notices as well.

the © shackle is here being held by the author himself, not the publisher; and in lieu of a list of prohibitions regarding reproduction following the reservation of ‘all rights’, the notice instead asserts ‘moral rights’, which is in turn yet another redundancy of its own kind, for if all rights are already reserved, then moral rights, being a particular subset of all rights, need not be explicitly mentioned, lest of course their assertion renders them distinct from mere reservation. The redundancy is here perhaps due to the fact that Verso publishes both in the UK (London) and the US (New York). Moral rights, being distinct from economic rights, and encompassing “the right to claim authorship of the work and to object to any distortion, mutilation or other modification of, or other derogatory action in relation to, the said work, which would be prejudicial to his honor or reputation”<sup>300</sup>, were introduced in the 1928 Rome Act revision of the Berne Convention<sup>301</sup>. Notably, in the legal proceedings preceding the US adoption of the Berne Convention, Congress apparently did not want the moral rights clause to apply, arguing that similar protections were afforded by other legal coda<sup>302</sup>, which may thusly explain the absence of said moral rights notice in our previous Haraway/Routledge example (which was published in New York). Nonetheless, as this particular incantation is still a traditional manifestation of © it is no longer of pivotal interest for us at this juncture.

Far more interesting for our purposes is the fact that Verso also puts out a number of books which bear the incantation of alternative copyleft licenses. As a case study, let us for instance take a gander inside the Verso publication of *We are Everywhere: The Irresistible Rise of Global Anticapitalism*, in which we find the following copyleft incantation:

© All text copyleft for non-profit purposes  
The texts in this book are copyleft (except where indicated).  
The authors and publishers permit others to copy, distribute,  
display, quote, and create derivative works based upon them in  
print and electronic format for any non-commercial, non-profit  
purposes, on the conditions that the original author is credited,  
We Are Everywhere is cited as a source along with our website  
address, and the work is reproduced in the spirit of the original.  
The editors would like to be informed of any copies produced.  
Reproduction of the texts for commercial purposes is prohibited

---

<sup>300</sup> Rome Act, 1928. “Article 6bis”. International Convention for the Protection of Literary and Artistic Works. <http://global.oup.com/booksites/content/9780198259466/15550019>.

<sup>301</sup> The latest revision (Berne Convention for the Protection of Literary and Artistic Works. 1971 Paris Act. “Article 6bis - Moral Rights”. <http://global.oup.com/booksites/content/9780198259466/15550001>), likewise contains the same article.

<sup>302</sup> Roberta Rosenthal Kwall. 2010. *The Soul of Creativity: Forging a Moral Rights Law for the United States*. Stanford, CA: Stanford Law Books. p. 30.



without express permission from the Notes from Nowhere editorial collective and the publishers. All works produced for both commercial and non-commercial purposes must give similar rights and reproduce the copyleft clause within the publication.

© All photographs in this book are copyright of the photographers, and may not be reproduced without permission<sup>303</sup>.

Whilst the traditional copyright incantation of yore utilizes the language of injunction and restriction, listing out a series of prohibitions over acceptable usage, copyleft instead largely deploys a vernacular of allowance, thus rendering itself more palatable in its presented permissiveness. Instead of a stifling ‘may not’, the copyleft license instead courts the appearance of a benevolent ‘you may’. For surely, how blessed is the reader of the text to encounter such open-hearted publishers who permit the copying, distribution, displaying, quotation, and even derivation of the source material! And yet, beneath the presumed permissiveness of the copyleft spell of benevolence, lies an authoritarianism akin to that of copyright, albeit rendered all the more dangerous due to its initial imperceptibility. Whereas copyright makes no effort to hide its impulse towards restriction and staunch congealment, openly proclaiming itself as being a list of restrictions, copyleft clothes its iron fist in the velvet glove of allowance.

Both copyleft/right have at their core a controller (*viz.* an author/publisher) who sets out to dictate the terms of allowable use. That copyleft sets forth a series of allowances does absolutely nothing to undermine the privileged position of the one who gets to set the license, to cast the spell, which others must then follow. The position of privilege exists through the exertion of licensing proper, irrespective of the particular terms of the license, whether it be copyright/left/upside-down-and-backwards. It thus makes absolutely no difference what the peculiarities of the particular incantation actually state, for the mere existence of a dictated incantation itself betrays the underlying power dynamic of someone dictating the terms of arrangement, and someone else in turn being expected to follow them, all the while the Body of Work itself remains firmly under the control of its *authoritarian* owner. The fundamental question of precisely *why* someone is to have the ability to dictate terms of use, to lock down content with a fetter of their choosing, which others must then presumably follow is thus never brought to the fore by copyleft; indeed it is buried all the deeper, the reader’s attention

---

<sup>303</sup> Notes from Nowhere (eds.). 2003. *We Are Everywhere: The Irresistible Rise of Global Anti-Capitalism*. New York: Verso. p. 10.

whisked away from the shadows of restricted terms of use and punishment for transgression thereof by the glimmer of permissibility.

A closer reading of the copyleft license nonetheless reveals that the allowances indeed come with quite a few strings, or rather chains, attached. In order for this particular Verso-enchained text to be copied and otherwise distributed in accord with the license, said distribution must meet the following conditions: 1) be for non-profit purposes, 2) be for non-commercial purposes, 3) credit the original author, 4) the book in question cited as a source, 5) the website address of the publishing/editorial collective be included, 6) be reproduced in the spirit of the original, and finally 7) the editors be informed of any such copies (re)produced. Thus while our sample copyright notice only carried two injunctions—a prohibition against reprinting or reproduction—the copyleft notice, while initially appearing to invite precisely such reproduction instead comes with seven conditions which must first be met. The content in question is thus far from being free to move about unrestrained, but is instead quite thoroughly still tied down in the chains of Intellectual Property Rights. Whilst the particularities of the terms of use manifest in the copyleft license are relatively distinct from those of the copyright incantation, the underlying dynamics of domination, of callous congealment, remain entirely unchanged. Thus, if the aim is to achieve an inviscid state of data, unbridled by any manner of attempted congealment thereof, then one must summarily reject copyleft as one does copyright; the siren song of reformist temptation and the potential appeal of some of the terms notwithstanding.

For instance, while it may indeed be appealing to prevent commercial/for-profit utilizations of the content in question, to do so via licensure would necessarily erect a privileged position of enactor of the license, and thus serve to perpetuate the very authoritarian mode of domination and enshackling that one is seeking to undermine. Instead, the problem of commercial appropriation is best approached head-on, not via pitfall-laden detours through copyleft: namely, if the aim is to preempt commercial/profitable use, then one must work to eradicate the very existence of commercial entities, as well as the underlying notions of profit accumulation. Far from being a redistribution or flattening of IP-based power relations, copyleft thus congeals existent inequalities and hence fetters of data dissemination.

Returning once more to the aforementioned seven delineated conditions for reproduction of the work in question, while the first six are relatively straightforward and unambiguous in their perfunctory nature, the seventh has already presented some

consternation and uncertainty for some who pay attention to these things. As Anna Nimus points out, Verso has claimed “that copying, modifying and redistributing should not only be non-profit but also in the spirit of the original - without explaining what this ‘spirit’ means”<sup>304</sup>. Thus Verso here affords itself a universal loophole to restrict *any* potential reproduction which it finds to be in violation of, an all too conveniently, undefined ‘spirit’. One may, perhaps not altogether irrationally, nonetheless venture a guess that since the book in question is devoted to ‘the irresistible rise of global anticapitalism’, and since there are numerous provisions against both for-profit and commercial reproduction, that the spirit of the original, such as it is, may indeed be one which eschews capitalist modes of content distribution; let’s say by putting the text online, on a website both devoid of any sort of membership or access fee or of advertisements. Alas, one would then be sorely mistaken.

In December 2009, the website AAAARG.org (now with an added appendage at AAAAARG.org), “a conversation platform - at different times it performs as a school, or a reading group, or a journal [...] created with the intention of developing critical discourse outside of an institutional framework. But rather than thinking of it like a new building, imagine scaffolding that attaches onto existing buildings and creates new architectures between them”<sup>305</sup>, which includes quite a number of links to a veritable cornucopia of textual resources, ranging from articles to entire volumes of potentially varying copyright-stature, received a pointed email from one Rowen Wilson; Sales and Marketing Director at Verso. “The purpose of this letter is to advise you of our clients' rights and to insist that you immediately disable or remove ALL LINKS from all websites associated with AAAARG.ORG or related sites on which the Works have been made available for download”<sup>306</sup>, reads the email, in part. Providing no explicit list of offending titles, merely claiming that there were “many” and name-dropping a few select authors, Wilson ends the communication with the advisement that “if you do not immediately cease and desist, we will seek all appropriate legal remedies, without prior notification”. Thus presumably AAAARG did not gel with Verso’s conceptualization of the ‘spirit of the original’ (whatever said spirit or actual original may be, and presuming of course that books which had that particular clause were on the AAAARG site; or, conversely, that any Verso books were at all, as neither can be verified at this point).

---

<sup>304</sup> Nimus, *op. cit.*

<sup>305</sup> “About AAAARG”. <http://aaaaarg.org/about>.

<sup>306</sup> Rowan Wilson. 2009. “ATTENTION AAAARG.ORG ADMINISTRATOR”. <http://ifile.it/e235laq>.

To make matters all the more revelatory—I pointedly here avoid using the term ‘ironic’, as there is to me absolutely nothing at all unexpected about a purveyor of copyleft-branded content seeking to corral and control its dissemination—Wilson’s email signature, following his credentials and contact details, ends with the promotional line “See Wu Ming’s website for their new novel: <http://www.manituana.com/>”. In fact, Verso’s own webpage for their edition of the Wu Ming book in question boldly states that “[t]he ‘communitarian’ use of the Internet is central to the work of Wu Ming, who have long been masters of the creative potential of the Internet. [...] All of Wu Ming’s work is available under ‘copyleft’, which allows reproduction in electronic form for non-commercial purposes”<sup>307</sup>. Even this *allowance* of reproduction thus apparently does not extend to AAARG, and thusly we see the cruel machinations of copyleft laid bare. Beneath the much-vaunted veneer of allowance lie the cold steel fetters of intellectual property ownership already well known to us as being akin to those of copyright. The operative function of copyleft is time and time again revealing of its fundamental purpose: the assurance of the continued existence of informational congealment, of the continued rendering of the IP fetters as inviting so as to ensure acquiescence to a state wherein some have the privileged role of channeling data flows into strictly regulated channels designed to corral unbridled, free dissemination of information.

### 2.1.2 ©©

Shifting our gaze by switching browser tabs from paratextual arcana to something decidedly more lively, we now find ourselves looking at a YouTube video entitled “Simple Living - Picking a Wild Salad”<sup>308</sup>. The three minute video depicts a man walking around outdoors, selecting various greens and flowers to use for a salad while narrating what he is picking; some bird chirping can be heard in the background. There are neither any additional external video clips, let’s say from films or television, nor is there a third party soundtrack, merely the sound of the man talking, leaves rustling, and bird chirping. Ten days after eeplox uploaded this video of himself onto YouTube, he received a notice from YouTube stating that he was not the rightful owner of the content in his video, specifically of the bird chirping therein, which according to YouTube, belonged to a company called rumblefish. eeplox filed a dispute of the claim, which was generated by an automated content control system, and the content was then manually reviewed by the content owners themselves to make sure no

---

<sup>307</sup> Verso. 2010. “Growing Knowledge: Wu Ming Present *Manituana*”. *Versobooks.com*. <http://www.versobooks.com/events/16-growing-knowledge-wu-ming-present-manituana>.

<sup>308</sup> eeplox. 2012. “Simple Living - Picking a Wild Salad”. *YouTube*. <https://www.youtube.com/watch?v=nPBlfeuZuWg>.

mistake had inadvertently been made by the detection mechanism. The reply eeplox received upon the appeal stated: “All content owners have reviewed your video and confirmed their claims to some or all of its content: Entity: rumblefish Content Type: Musical Composition”<sup>309</sup>. Thus once again we see manifested before us a redundancy of consciousness: IP rights ownership enforced once over by the automated machinations of the IP industry, to be all the more reinforced by human foot soldiers in the copyfight; all serving to ensure the fetters of content strangulation fit firmly in place.

Upon staking, and further confirming, their claim to the bird song in question, rumblefish then proceeded to place advertisements over the video in question. Eventually, after the incident gained momentum on Internet forums, the CEO of rumblefish himself formerly reviewed the video and reversed the content ownership claim; thus effectively ‘releasing’ the video back to eeplox and removing the ads. The outrage against draconian copyright enforcement was immense; with a number of critics of the incident licensing their own work under a Creative Commons (CC) license themselves<sup>310</sup>, with some explicitly advocating CC licensing as an alternative to rumblefish<sup>311</sup> for years prior to the incident at hand. The Creative Commons is an umbrella organization which provides six varying licenses that allow ‘licensors’, a term meaning “everyone from individual creators to large companies” in CC parlance, may use: Attribution (CC BY), Attribution-ShareAlike (CC BY-SA), Attribution-NoDerivs (CC BY-ND), Attribution-NonCommercial (CC BY-NC), Attribution-NonCommercial-ShareAlike (CC BY-NC-SA), Attribution-NonCommercial-NoDerivs (CC BY-NC-ND)<sup>312</sup>. A basic pattern can thus be deduced, in that CC licenses all operate by mixing and matching four distinct parameters: Attribution (BY), ShareAlike (SA), NoDerivs (ND), NonCommercial (NC). The fundamental root of every CC license, constituting the initial 'CC' formulation of the incantation, is that anyone who is not the current licensor of any particular congealment Body of Work (who is excluded from the terms due to being the one who gives out said rights in the first place) is granted the right to share, which it to say to 'copy, distribute and transmit' a given work (CC) so long as the

---

<sup>309</sup> eeplox. 2012. “‘Matched third party content. Entity: rumblefish Content Type: Musical Composition’, but no music in the video”. *Google Groups - Google Product Forums - YouTube Help Forum*. <https://productforums.google.com/forum/#!category-topic/youtube/how-to-use-youtube-features/eSjKSGBrFMo>.

<sup>310</sup> Cory Doctorow. 2012. “Rumblefish claims to own copyright to ambient birdsong on YouTube”. *Boing Boing*. <http://boingboing.net/2012/02/27/rumblefish-claims-to-own-copyr.html>.

<sup>311</sup> Mike Masnick. 2010. “Music Licensing Firm Offers Cheap Licenses For YouTube Videos”. *Techdirt*. <http://www.techdirt.com/articles/20100629/02511010000.shtml>.

<sup>312</sup> Creative Commons. “About the Licenses”. <https://creativecommons.org/licenses/>.

added provisos are followed. As every flavor of the CC license also includes the BY parameter, it further follows that every CC license mandates that the owner of the content in question be credited when the work is distributed, albeit “in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work)”. The SA clause further adds the restriction that any derivative work which includes elements from the initial work in question must be shared under the identical CC SA-\* license in turn. On the other hand, the ND provision preempts the creation of any such derivative works in the first place. Finally, the NC parameter stipulates that the work cannot be used for any commercial purpose.

Following this fundamental crash course in the intricacies of CC-based licensing, we now return to YouTube’s ContentID (CID) system. When the automated system detects a potential infringement, the rights holder may setup their ContentID account to either receive statistics on the video viewership, monetize the videos through the placement of advertisements over the video content, or to remove the videos from YouTube entirely. “It’s up to you”<sup>313</sup>. While YouTube further has a separate page on CC-licensed uploaded content, a pivotal point here is that there is nothing in the language of either any of the CC licenses themselves, nor in YouTube’s description of their CID system which would preclude content owners who shackle set content under a CC license to deploy the CID system against allegedly infringing videos which violate the terms of any particular license. Returning now to eeplox’s video, we thus see that all of the resultant outcomes of the particular case—the seizure of the video by the CID system, the placement of advertisements of the video, the manual confirmation from the content owners of the infringing nature of the content, and so on—could well apply irrespective of whether the content was bewitched under a traditional © or any of the varying CC copylefts. So long as the CID flagged the content as infringing, and the rights owner then proceeded to confirm it as such, it matters not in the least to YouTube what the specific minutiae of the licensing terms are: the content would be either taken down or ‘monetized’<sup>314</sup> irrespective. It is the existence of licensing itself, and in turn the existence of content owners who are enthroned with the power to regulate the dissemination of information, which leads to the potentiality of video seizure. The specific

---

<sup>313</sup> YouTube. Content ID. *YouTube*. <https://www.youtube.com/t/contentid>.

<sup>314</sup> It is essential to here note that if one were to make the objection that an advertisement could not be placed on a CC-NC-\* license, then it must be pointed out that the license only applies to the end-user, in that whoever uploaded the video (presuming that the uploader is not the licensor) may not place advertisements on it; the restriction does not apply to the actual rights holder, who may thus indeed place ads onto the video following an alleged violation flagged by YouTube’s Content ID system.

terms of the license are incidental and thus must be attacked universally and unconditionally. Copyleft is not an ally of unbridled data flow in the least in the on-going copyfight.

### **2.1.3 Free Software ('free' as in 'not')**

There is one particular strain of reformism which seeks to preserve the congealment of data flows—whilst at times seemingly operating under the pretense of arguing against said fetters—which merits separate discussion due to its widespread advocacy of copyleft<sup>315</sup> and the widespread advocacy of the movement itself by various proponents thereof<sup>316</sup>. The Free Software Foundation (FSF), headed by Richard M. Stallman<sup>317</sup> (RMS)<sup>318</sup>, both develops its own software and operating system (dubbed GNU, a recursive acronym for GNU's not Unix)<sup>319</sup>, and supports a particular family of software licenses (the keystone license being its own General Public License (GPL), alongside a number of officially-supported variations such as the Free Art License (FAL))<sup>320</sup> and software which is released under said license<sup>321</sup>, as well as encouraging software developers to adopt the use of said licenses<sup>322</sup>.

Thus the FSF does not necessarily precede as a centralized totalitarian tower of control, regulating data dissemination in accord with its particular license; rather, it mobilizes independent programs and programmers to utilize the same license without a necessary affiliation with the FSF itself, thus operating not only as a centralized organization, but via “its molecular or micropolitical power, for it is a mass movement”<sup>323</sup>, thus constituting a dispersal of cancerous cells, creating microcorpuscles of licensed congealment; the proprietarian quanta of copyleft. “The goal of GNU”, states Stallman, “was to give users freedom”<sup>324</sup>. Right from the start, a most peculiar inversion has taken place. Why must the GNU be this benevolent giver of freedom?—is an entirely irrelevant question, for why must

---

<sup>315</sup> Free Software Foundation. 2013. “Current Campaigns”. <https://www.fsf.org/campaigns/>.

<sup>316</sup> LibrePlanet. 2014. [https://libreplanet.org/wiki/Main\\_Page](https://libreplanet.org/wiki/Main_Page) (following the ‘Community’ link from The Free Software Foundation homepage (<https://www.fsf.org>) redirects to the LibrePlanet URL).

<sup>317</sup> Free Software Foundation. “Staff and Board”. 2012. <https://www.fsf.org/about/staff-and-board/>.

<sup>318</sup> Three Letter Acronyms (TLAs) are a common form of nomenclatural initialism in this particular field. As Eric S Raymond (ESR) explains, “hackers have a tradition of triletterizing people they consider tribal elders or chieftains. The best known other example is of course RMS = Richard M. Stallman” (Eric Raymond. 2011. “The importance of being ‘ESR’ – a sidelight on the G+ nym wars”. *Armed and Dangerous*. <http://esr.ibiblio.org/?p=3583>).

<sup>319</sup> Free Software Foundation. 2014. “The GNU Operating System and the Free Software Movement”. <https://gnu.org/>.

<sup>320</sup> Joshua Gay. 2005. “FSF Licensing & Compliance Team”. *Free Software Foundation*. <https://www.fsf.org/licensing/>.

<sup>321</sup> Matt Lee. 2010. “Meet the free software gang”. *Free Software Foundation*. <https://www.fsf.org/working-together/gang>.

<sup>322</sup> Richard Stallman. 2013. “Free Software Is Even More Important Now”. *GNU Project*. <https://www.gnu.org/philosophy/free-software-even-more-important.html>.

<sup>323</sup> *Ibid.*

<sup>324</sup> Stallman, *op. cit.*, p. 22.

freedom be *given* in the first place? There seems to be a presumption that freedom of data dissemination somehow doesn't exist *a priori*, but must instead be conjured forth by the benevolences of the FSF's copyleft license. It is precisely via the dispersed mobilization of the GPL that control over data is exerted from all directions, there is no centralized publishing house; instead, there are scores of independent developers are intertwined in the mesh of copyleft, propagating congealment under the veneer of combating intellectual property.

The particular *freedom* of which the FSF and which the GPL seeks to *give*, comes about through a conglomeration of four microfreedoms, the combination of which formulates a congealed piece of *free software*, the freedom to: run a program, examine the inner workings of a program, distribute copies of the program, and to improve upon and release said improvements of the program<sup>325</sup>. The GPL seeks to guarantee these freedoms by requiring that all those who use GPL-licensed code must likewise make the source code available alongside any precompiled binaries they may distribute through giving away or selling. Thus, here we see an expansion of the previous statement that the GPL seeks to *give* freedom. It is not apparent that it also seeks to *define* freedom, a freedom thus emerges that is born out of restraint. Stallman goes on to point out that the GPL must apply to all future permutations of the initially GPLed software, pointing out that "if the developer of the software has the power to revoke the license, without your doing anything to give cause, the software is not free"<sup>326</sup>. The emphatic stance against revocation serves to obfuscate the unmentioned deficit of imposition. For in order to discuss revocation of a specific license, there must have been an initial *imposition* of the license upon formerly unfettered code. A license does not exist *a priori*, it is conjured forth by those who seek to corral and congeal data streams, whether that act of authoritarian entrapment is committed under the guise of copyright or copyleft makes little difference: it is precisely the act of licensing itself that is of pivotal import here.

In all of the writings on the GPL, the FSF, and free software in general, there is precious little mention of *who* exactly gets to impose the license, which others then presumably have to follow (assuming that they stay within the legal segmentation imposed by lines of licensing themselves; that is to say, that they choose to adhere to the terms of the license), and following that, *why* those who impose the license get to, at the expense of all

---

<sup>325</sup> *Ibid.*, p. 49.

<sup>326</sup> *Ibid.*, p. 44.



others. In the writings of the FSF, there is only an ever-ambiguous *we* floating about when the imposition of the GPL is obliquely brought up. To his credit, Stallman certainly does make the point that under existent copyright regimes, copyrights are oft signed away to the software company the developer is associated with, the publishing company a writer is tethered to, or perhaps the recording company the musician has been subsumed by<sup>327</sup>.

This point of corporate appropriation fast appears to establish itself as a steadfast argument within the reformist arsenal, as it is nearly identically reverberated by Martin<sup>328</sup>, and perhaps more eloquently expatiated upon by Moglen in his “dotCommunist Manifesto”<sup>329</sup>: “[t]o the owners of culture, we say: You are horrified at our intending to do away with private property in ideas. But in your existing society, private property is already done away with for nine-tenths of the population. What they create is immediately appropriated by their employers”<sup>330</sup>. And yet, how curious it is that when developers create a ‘legally significant’ amount of code for a GNU-related piece of software, the FSF then asks them to either sign over the copyright to the FSF itself, to grant the FSF a nonexclusive license, to release the code themselves under the GPL, or to put the relevant bits of code into the public domain<sup>331</sup>, at which point the FSF can subsume those bits of code and all further development on them under the GPL<sup>332</sup>. The FSF thus here appears to encourage the very same practice it and its fellow reformists seemingly deride. Though FSF proponents at times put forth that copyright clauses and said IP-allocation schemas are a necessary evil<sup>333</sup>, there

---

<sup>327</sup> *Ibid.*, p. 48.

<sup>328</sup> Martin, *op. cit.*, p. 33.

<sup>329</sup> Incidentally, the manifesto itself comes bundled with a stern copyright disclaimer: “©Eben Moglen, 2003, Verbatim copying and distribution of this entire article is permitted in any medium, provided this notice is preserved” (Moglen, “The dotCommunist Manifesto”, *op. cit.*).

<sup>330</sup> Moglen, *op. cit.*

<sup>331</sup> Free Software Foundation. 1998. “Legal Issues about Contributing Code to GNU”. The GNU Operating System and the Free Software Movement. <https://www.gnu.org/software/gnustep/developers/conditions.text>; Free Software Foundation. 2008. “Information for Maintainers of GNU Software”, Section 4. Legal Matters – Subsection 4.1 Copyright Papers. [https://www.gnu.org/prep/maintain/html\\_node/Copyright-Papers.html](https://www.gnu.org/prep/maintain/html_node/Copyright-Papers.html).

<sup>332</sup> “The law says that anyone can copyright a modified version of the public domain work. (This doesn't restrict the original, which remains in the public domain; only the changes are copyrighted.) If we make extensive changes, we will probably do this and add our usual copyleft. If we make small changes, we will leave the version we distribute in the public domain” (Free Software Foundation, “Legal Issues about Contributing Code to GNU”, *op. cit.*).

<sup>333</sup> “Project GNU has to be careful to obey intellectual property laws, even though these laws are wrong and people generally should share useful information without hesitation, because we are in the public eye” (*Ibid.*); “Copyright for software and other works is a ‘necessary evil’ for providing copyleft to the free software movement. This ‘necessary evil’ requires copyright assignment, copyright enforcement, license compliance and other aspects of preserving the free software distribution and licensing system under the GPL to be required activities for sustaining the free software movement” (Aaron S. Hawley. 2007. “Making copyleft work with implied compliance”. *Free Software Foundation*. [http://gplv3.fsf.org/wiki/index.php/User:ashawley/Making\\_copyleft\\_work\\_with\\_implied\\_compliance](http://gplv3.fsf.org/wiki/index.php/User:ashawley/Making_copyleft_work_with_implied_compliance)).

is nonetheless no reason presented by the FSF for why they *choose* to engage on the plane of legal interaction, as opposed to deploying illegalist strategies of license negation. Thus the idiomatic evil is here seen to be entirely voluntary.

There is a further political appropriation of free software found within fellow reformist literature, which seeks to describe free software under the GPL as an anarchic formulation. Naught but an attempt to radicalize their otherwise reactionary reformism, GPL supporters describe free software as having anarchic tendencies, coupled with a rejoinder against corporate hegemony over software development. For instance, whilst admitting that the GPL is not an overt political platform, Bradley nonetheless goes on to assert that “[t]he FSF advocates a broadly social anarchistic approach allied with a desire to overturn entirely commodified software production”<sup>334</sup>. Similarly in a paper entitled boldly entitled “Anarchism Triumphant”, Moglen states that “[t]he GPL, also known as the copyleft, uses copyright, to paraphrase Toby Milsom, to counterfeit the phenomena of anarchism”<sup>335</sup>. The fact that anarchism has a vibrant history of rejecting the inequality brought about by commodity relations, and that the FSF is thus incommensurate to anarchist ideology based on its open acceptance of business, to say nothing of the problematics of the inequality created by virtue of having a licensor/licensee, is apparently here lost on the aforementioned commentators, despite the fact that said historical background is readily accessible<sup>336</sup>. Despite mentioning ‘anarchism’ and ‘anarchist production’ at various times throughout his article, Moglen does not seem to show at any point explicitly *how*, specifically, he sees the GPL as being conducive to anarchist praxis. Thus *anarchism* is reduced to the status of an undelineated buzzword, safely removed from the political into the realm of empty rhetoric.

Gaycken<sup>337</sup>, a notable exception to the otherwise complacent faux-radicalization of free software, takes the charge to task and points out that neither free software as technology, nor free software as method is anarchic in the least; instead, free software being “bracketed by the ideological frameworks of capitalism and authority, thus reproduc[es] and proliferate[es] both”<sup>338</sup>. Though not explicitly stating that the GPL *qua* license creates a binary of ruler and ruled—the one(s) who imposes the license, and the ones who are then to

---

<sup>334</sup> Bradley, *op. cit.*

<sup>335</sup> Eben Moglen. 1999. “Anarchism Triumphant: Free Software and the Death of Copyright”. *First Monday* 4 (8). <http://firstmonday.org/ojs/index.php/fm/article/view/684/594>.

<sup>336</sup> E.g., The Anarchist FAQ Editorial Collective (Ian McKay, Gary Elkin, Dave Neal, Ed Boraas). 2008. “An Anarchist FAQ”. v. 13.0. *Infoshop*. <http://www.infoshop.org/AnarchistFAQIntro>.

<sup>337</sup> Sandro Gaycken. 2005. “Free Software and Anarchism - does this compute?”. *22nd Chaos Communication Congress - Private Investigations*. <https://events.ccc.de/congress/2005/fahrplan/events/517.en.html>.

<sup>338</sup> *Ibid.*

obey its terms, this can nonetheless be seen as the implication for Gaycken's rebuke of free software for reproducing authoritarian vectors of content congealment.

Gaycken first points out that GPLed code necessitates computers on which the software is to be implemented, and since the production and purchasing thereof is done firmly within the grasps of capital, and thus "in addition to the concept of free software, a concept of free hardware (so to speak) would be needed as well to render free software into an anarchical technology"<sup>339</sup>. Whilst this line of argumentation indicts GPLed code as operating in, and thus being complicit, in the wider networks of capital, it misses the opportunity to point out that even within its own licensing terms and related literature, GPL is likewise openly embracing business not only through its broader participation in said networks, but through its very own internal coda as well.

Gaycken then attempts to show that free software is neither anarchic in its method due to its adherence to certain rules (e.g. openly available source code), "[r]ules and institutions, even as moderate guidelines, are restrictive, hierarchical and authoritative by nature, they cannot reasonably be associated with freedom. Here, free software development as a method fails significantly in providing a genuine anarchical framework for any subsequent work"<sup>340</sup>. While here Gaycken perhaps broaches upon the earlier mentioned critique of the GPL 'as license', he nonetheless appears to confound *anomie*—an absence of rules, with *anarchy*—an absence of rulers. Whilst seemingly trivial, the distinction is on the contrary quite pivotal. To align anarchic formulations with the mass media glorified spectacle of negative, nihilistic disorder is to prematurely collapse all lines of flight into lines of death, "line of flight crossing the wall, getting out of the black holes, but instead of connecting with other lines and each time augmenting its valence, turning to destruction, abolition pure and simple, the passion of abolition"<sup>341</sup>. An anarchic formulation of source code thus does not preclude the formation of specific rules of coding, so long as the rules are decided upon by autonomous microcosms, i.e. localized communities of, in this case, software developers. It does, however, preclude the formation of rulers and ruled. No gods, no master, as the old adage inscribed on many a punk jacket goes. And thus, no licenses.

Hence the fact that the GPL cannot be an anarchic formulation is evinced by virtue of the GPL itself being a license. A license inherently creates a vertical formulation in which the creator *A* imposes a license on a conjured BoW, which *B* must then follow (assuming, as

---

<sup>339</sup> *Ibid.*

<sup>340</sup> *Ibid.*

<sup>341</sup> Deleuze and Guattari, *op. cit.*, p. 229.

mentioned previously, that *B* chooses to remain within a legally-sanctioned line of segmentation). A horizontal leveling of any authoritarian master/slave dichotomy necessitates the expulsion of all inhibitors to the unbridled flow of data, and this in turn necessitates a rejection of all licensing schemas, as much like the FSF's GPL, they remain not merely "bracketed by the ideological frameworks of capitalism and hierarchy"<sup>342</sup>, but actively seek to recreate the hierarchical binary of imposer/follower of the legalist license. And once again, lest this critical formularization itself be construed as imposing an artificial binary schematization of forced control, which is to say of constructing the described imposer/follower pair, it must again be pointed out that the license hardly *must* be followed, thus the roles are only static within stifling legalist confines.

The proliferation of data dissemination currently swirling around the digital terrain, specifically dissemination that is doubtlessly in gross violation of not only a plethora of software licenses but also of a compendium of international legal codes, is a testament to the superfluous, attempted exertion of rigid segmentation via *any* mode of licensing. And yet gleeful disobedience, indeed negation, of the rules of conduct mandated by the twin serpents of State and Capital does not change that the moment when a license itself is conjured—whether it is adhered to or not—marks occurrences of aspirations for control, a seeking to impose some sort of limit on the distribution of some congealed artifact of data. The success, or rather the destined failure, of such an enclosure thus does not negate the *act* of attempted enclosure.

There is one further technicality to dispose of. It is at times pointed suggested that copyleft, particularly the FSF, is opposed to the conglomeration of capital. As Bradley erroneously suggests, "Stallman's open anarcho-utopianism commits to an avoidance of market managerial hegemony"<sup>343</sup>. This myth is best dispelled by turning to Stallman's original conjuring of the GNU project, "[t]he free software philosophy rejects a specific widespread business practice, but it is not against business"<sup>344</sup>, and furthermore "the support of business can contribute to the community in many ways; all else being equal, it is useful"<sup>345</sup>. Once again, there is no clear, neat bifurcation betwixt copyleft and capital. The hallucinatory image projected by the reformists is murky indeed, a disparity of vision caused

---

<sup>342</sup> Gaycken, *op. cit.*

<sup>343</sup> Bradley, *op. cit.*

<sup>344</sup> Stallman, *op. cit.*, p. 24.

<sup>345</sup> *Ibid.*, p. 32.

by the incessant entwinement thereof, a conjoined ouroboros as capital and copyleft devour one another, devour what is one and the same, but only when the moon is just right.

That is to say, whilst both serve to congeal data, capital by marketability and copyleft by licensing, their respective modes of operandi may either diverge or coalesce, depending on the particular situation. For instance, Stallman openly encourages the selling of free GPLed software for exorbitant prices (a redundant description here to be sure, for how is any price not exorbitant in and of itself). “We encourage people who redistribute free software to charge as much as they wish or can”<sup>346</sup>, writes Stallman about common misconceptions incurred against free software, with users in theory being able to “copy the program from a friend who has a copy, or with the help of a friend who has network access. Or several users can join together, split the price of one CD-ROM, then each in turn can install the software”<sup>347</sup>. This sort of exertion of control over data dissemination through a delay of initial distribution should already be quite familiar to us, for it is naught but the same form of bottlenecking as that practiced by the aforementioned self-professed anticopyright publishers akin to the Critical Art Ensemble or the CrimethInc. Ex-Workers' Collective. Whilst under the auspices of the GPL one may certainly freely distribute any subsequent copies of the GPLed code gratis, the initial distribution is bogged down by the monopolization of originating routes of data outpours, that is to say via the exultation of extortion: release of the GPLed code following the payment of an initial sum. It is precisely in this way, to give but one example, that copyleft may thus freely collude with capital in conspiring to restrain data dissemination.

Whilst for purposes of explication we have hitherto at times indulged in a microscale focus on particular clauses *within* the license, such a narrow argument would only serve to legitimize the license *as such*, resorting to finding confrontation with particular elements *within*, as opposed to the entire tumultuous entity of control which serves to congeal information as a License. The discreet minutiae of any particular copyleft or copyright, as such, are thus ultimately irrelevant.

Copyleft and copyright are thus two sides of the same one-sided coin; naught but two *intertwined parallel* processes, both attempting to exhibit syntactic control over data flows by conjuring forth a tangible artifact or Body of Work, a strictly striated and delineated corpus

---

<sup>346</sup> *Ibid.*, p. 65

<sup>347</sup> *Ibid.*, p. 72.

onto which the particular license is then grafted, and then proceed to dictate certain authorized modes of distribution of the now-congealed data.

## **2.2 The CS Approach**

In turning now to seeing how Cultural Studies as a discipline situates itself within the ensuing copyright, we can look at two issues of cultural studies journals devoted to the topics of Intellectual Property and Pirate Philosophy<sup>348</sup>. Gary Hall lays his political affiliation bare through his attempt at presenting piracy as a neutral, apolitical entity, pointedly ripping out any potency from the act of data liberation by stating that “what makes this issue of *Culture Machine* a little different is, firstly, its refusal to ascribe an intrinsic or essential value to piracy [...] there is nothing *inherently* emancipatory, oppositional, leftist, or even politically or cultural progressive about digital piracy”<sup>349</sup>. Of course, an attempt to neuter an entire praxis by a malicious means of an *a priori* defanging is itself no apolitical act. To present piracy as value-neutral, is to present it as being a mere tool akin to an unlit stick of dynamite, which can be used either to demolish buildings or to prop up a loose table leg. Doing so, however, entirely ignores the underlying fact that piracy is more akin to an immanent force, not a static piece of equipment to be appropriated at whim, but the resultant explosion itself; not a passive stick of dynamite, but rather a rush of movement which obliterates capital at its core.

Hall here further confounds the potential intent of an actor with the result of a given action itself. The motivations for throwing a brick through a department store window are many. One could foreseeably do so with the explicit intention of causing damage to a visible enclave of capitalist commodification, or one could do so in the vain hope of drumming up business for one’s own window repair company, or one could do so simply for the sake of having no better place to place the brick. Irrespective of the particular motivation, however, the result is one and the same: the window is smashed. And one could code such an action as being value-neutral if one magically ignores all existent property relations, fully reinforced by existent legal mores which render the act a crime and subject the actor to legal and fiduciary damages, as Hall apparently does. Similarly, one can imagine any number of potential reasons for engaging in act of piracy, whether it be out of a willing desire to aide in the unbridled dissemination of unfettered information, or out of a curiosity to see whether a particular digital commodity is worth purchasing (the ‘try before you buy’ capitalist

---

<sup>348</sup> *Cultural Studies* 20 (2-3). 2006; *Culture Machine* 10 “Pirate Philosophy”. 2009. <http://www.culturemachine.net/index.php/cm/issue/view/21>.

<sup>349</sup> Gary Hall. 2009. “Introduction: Pirate Philosophy”, in *Culture Machine* 10, pp. 1-5 (pp. 1-2).

apologetics of piracy), or out of a basic urge to simply get something for free, with no overarching philosophical paradigm *other than the act itself* weighing down on the active agent involved. Once again however, the resultant outcome of all three decision vectors leading up to the act of piracy itself is the same one and all: the promulgation of unauthorized data flows in the face of staunchly opposed legal and perhaps economic injunctions.

As Andersson thus accurately points out, “[t]he phenomenon thus becomes politicized, not so much by the file-sharers’ own intent, but by the potentialities inherent in the technology in its current legal and economical context”<sup>350</sup>. For Hall to devalue the act of piracy by indulging in a phantasmagoric delusion in which there exists a vacuous state without any underlying econo-legal conditions and actions can be blissfully value-free, is to attempt to actively discredit the struggle inherent in the copyright by seeking to depoliticize it, and thereby casting doubt on its universal efficacy to undermine the congealment of information by scripting literal impossibilities akin to “Pirates and piracy can even be pro-neoliberal capitalism”<sup>351</sup>. While it is certainly possible that some pirates themselves may be ideologically beholden to neo-liberal capitalism, the act of piracy itself which actively eschews commodity relations and their accompanying fetters of content distribution, cannot be ‘pro’ capitalism by virtue of definition, let alone circumstance, alone. Which is certainly not to say that pirate modalities may not be appropriated by capital (e.g. distributing low-bitrate MP3s for free via The Pirate Bay, but then proceeding to charge for higher quality versions of the album), but the *instance* itself (in this case the free downloading of said MP3s) constitutes an ideological opposition through a rejection of transaction.

In spite of his devaluation of piracy, however, Hall goes on to state that he is nonetheless “also keen to explore the consequences and potential implications of various forms of so-called piracy for academic publishing”<sup>352</sup>. To arrive at this end, Hall posits the existence of six possibilities for authors to disseminate a given text if the terms and contractual stipulations of their publishers prohibit them from doing so: 1) waiting for the text to go out of print and seeing if the publisher will then revert the copyright back to the author, at which point the author may distribute the text; 2) as copyright notices prior to 1996 do not contain explicit injunctions against digital dissemination, the work could arguably, according to Hall, potentially thus be legally distributed so long as it was published before 1996; 3) the author could only publish with those

---

<sup>350</sup> Jonas Andersson. 2009. “For the Good of the Net The Pirate Bay as a Strategic Sovereign”, in *Culture Machine* 10, pp. 64-108 (p. 66).

<sup>351</sup> Hall, *op. cit.*, p. 2.

<sup>352</sup> *Ibid.*, p. 3.

publishers who also allow the author to distribute the text via means of their choosing; 4) they could publish the book with an open access publisher that places the book freely online in the first place; 5) the author could ask the publisher for permission to place the text freely online; and finally 6)—“possibly the shrewdest strategy of all”<sup>353</sup>—the author could adopt a “don’t ask/don’t tell” approach and simply place their text online without informing nor asking the publisher. The first five potentialities, mired as they are in the throes of an all too acquiescent legalism, are of no interest to us here—“only the enemy wants to fight on the terrain of roles, according to the rules of the spectacle”<sup>354</sup>. To engage in the copyright on the basis of legally sanctioned forms: a willing distributor asking for permission of the copyright holders to engage in said distribution, is to intrinsically legitimize the authority the content owners wish to promulgate through econo-legal measures in the first place.

Instead, as Striphas and McLeod note, if we no longer assume that IP law is, in all circumstances, the régime best capable of overseeing how ideas propagate and flow, then perhaps we should pursue with an even greater resolve extra-legal means by which to mitigate IP’s worst excesses. [...] Better yet, any strategy for contesting the law should proceed through more than just legal channels, lest we inadvertently reinforce the legal realm’s claims to power, authority, and exclusivity in the process<sup>355</sup>.

Thus it is the last option for content distribution presented by Hall, ‘The Sixth Way’ as we may call it, that is of immediate interest to us for the insurrectionary purposes of wholesale content liberation. However, calling for authors to willingly freely distribute online the works that they wrote themselves is far from sufficient; largely due to the looming probability that not all authors may agree to do so. If the aim of the pirates-cum-data-liberators engaged in the copyright, as indeed it is, is to assure the complete shattering of IP-based fetters placed upon information, then content must be actively distributed at all possibilities irrespective of dubious attributions of authorship bearing any weight on whether one may engage in the “don’t ask/don’t tell” praxis of content promulgation.

### **2.3 Informational Illegalism (Anti Theory)**

To now broaden the terms of Hall’s initial query, the question is no longer strictly limited to “what are an author’s options” in distributing their content despite publisher reprimands to the contrary, but what are *anyone’s* options. The arising discussion of options, in turn, brings to the

---

<sup>353</sup> Gary Hall. 2009. “Pirate Philosophy (Version 1.0): Open Access, Open Editing, Free Content, Free/Libre/Open Media”, in *Culture Machine* 10. pp. 1-43 (pp. 22-23).

<sup>354</sup> Raoul Vaneigem. 1967. *The Revolution of Everyday Life: Impossible Realisation or Power as the Sum of Seductions*. Red & Black. <http://library.nothingness.org/articles/SI/en/display/56>.

<sup>355</sup> Striphas and McLeod, *op. cit.*, p. 130.



fore *illegalism*—a strand of anarchist praxis particular in vogue in Europe at the start of the 20<sup>th</sup> century, strongly influenced by the practical enactment of Stirnerian egoism with an emphasis on carrying out acts of criminality for the single sake of satisfaction of desire, as exemplified by the Bonnot Gang, a French group of illegalist bank robbers<sup>356</sup>. In extending on the aforementioned evocations of Hall, Striphas, McLeod and others towards ‘civil disobedience’ in regard to IP regulation, let us now then posit a sort of *informational illegalism*, in which the early 20<sup>th</sup> century illegalist targets of European banks are replaced by the 21<sup>st</sup> century targets of international publishing conglomerates; and specifically for purposes of the soon-following praxis, academic journal repositories. The Bonnot Gang thus finds its logical successor in the Binary Gang. We must here then engage in a reformulation of Proudhon’s famous dictum that ‘property is theft’ (more accurately stated by Proudhon himself as “what is property...it is robbery”<sup>357</sup> to the particular instance of applicability to us herein, namely that intellectual property is theft. The theft of course only occurs within the help of the legal domain in which it takes place: specific amalgamations of data—sentences, verses, books, songs, moving images, and other congealed Bodies of Work—are whisked away from the ethereal commons in which they freely propagate and are entrapped behind the artificial enclosure of the intellectual property fetters. Information is stolen from the ether *by and through* the command of the law, it would make no sense to talk of theft without underlying notions, entrenched by commodity relations alongside the aforementioned legalistic crutches, of singular property ownership.

And yet, the mere manifestation of the truism that intellectual property is theft is a decisively passive one. There is no decisive invitation to action inherent in the statement itself. Much like the illegalists of yore, unsatisfied with the passive resignation inherent in being told by the anarchist pamphlets of the time over and over again that ‘property is theft’, thus banded to form a Stirnerian union of egoists determined to do something in light of this grim news, so too do we here adopt Stirner’s affirmative reformulation of Proudhon:

Proudhon might spare his prolix pathos if he said: ‘There are some things that belong only to a few, and to which we others will from now on lay claim or – siege. Let us take them, because one comes to property by taking, and the property of which for the present we are still deprived came to the proprietors likewise only by taking. It can be utilized better if it is in the hands of us *all* than if the few control it. Let us therefore associate ourselves for the

---

<sup>356</sup> Richard Parry. 1987. *The Bonnot Gang: The Story of the French Illegalists*. London: Rebel Press.

<sup>357</sup> Pierre-Joseph Proudhon. 1840. *What Is Property?: or, An Inquiry into the Principle of Right and of Government* (trans. Anonymous). <https://www.gutenberg.org/files/360/360-h/360-h.htm>.

purpose of this robbery'<sup>358</sup>.

Yet while the aim of the illegalists was thus also one of collective reappropriation, of liberation of property from the throes of capital, their praxis nonetheless differed from a similar anarchist strand, in vogue at a slightly earlier time, of *reprise individuelle* or individual reclamation in which actors seized property from control of the capitalists based on explicitly moral foundations. Illegalism, on the other hand, prioritized the act of reappropriation itself, as opposed to seeking justifications thereof. Thus the “illegalists were to make a theory of theft without the embarrassment of theoretical justifications”<sup>359</sup>. Illegalism is thus the more fitting dictum for us here, for recall the earlier rebuttal of Hall’s attempt at defanging the political force of piracy: the justifications for the act matter not in the least for the consequence of its outcome. Moral justification for the elimination of intellectual property (whether it be based on anarcho-socialist, anarcho-individualist, anarcho-capitalist, or any other grounds) is thus insignificant to the underlying anti-capitalist ethos inherent in the action itself. The focus must be on the insurrectionary nature of the praxis itself.

With Stirner’s affirmation thus firmly in mind, we can then proceed to make sense of what we will here call Hoffman’s Paradox. In 1967, Abbie Hoffman (under the alias George Metesky) published a pamphlet entitled *Fuck the System* which included a number of methods of obtaining a variety of free content in New York city which, one could say as Striphas did about IP dissidence “engage[d] the legal but that cannot be reduced to it”<sup>360</sup>. The end of the text includes the following proclamation: “Nothing in this manual is copyrighted. Anyone may reprint this information without permission If you paid money for this manual you got screwed. It's absolutely free because it's yours. Think about it”<sup>361</sup>. Four years later, Hoffman published a much larger text with a similar but broader scope, now encompassing nation-wide tactics of not only the free procurement of goods and services but armed insurrection as well. Released under the title *Steal This Book*, the book included a fairly boilerplate copyright incantation: “All rights reserved. No part of this book may be reproduced, stored in a database or other retrieval system, or transmitted in any form, by any means, including mechanical, electronic, photocopying, recording, or otherwise, without the

---

<sup>358</sup> Stirner, *The Ego and His Own*, *op. cit.*, p. 128.

<sup>359</sup> Parry, *op. cit.*, p. 15.

<sup>360</sup> Striphas and McLeod, *op. cit.*, p. 130.

<sup>361</sup> Hoffman, Abbie (alias George Metesky). 1967. *Fuck the System*. New York. <http://dizzy.childrenofmay.org/fuck.the.system.txt>.

prior written permission of the publisher”<sup>362</sup>. How is one to reconcile the apparent contradiction of a single mind concocting too wildly different IP notices? Aside from the fact that *Fuck the System* was distributed freely and thus the treeware text could not be stolen in the physical sense, whereas *Steal This Book* was sold in stores and thus the command to action in the title of course applied to physical expropriation of the book itself; the latter’s title-cum-invitation could only apply to the actual *information* contained therein if it bore a typical copyright incantation which legally attempted to make its dissemination impossible, thereby necessitating its theft from the fetters of the legal injunction against both material and informational distribution. For as previously discussed, intellectual property constitutes theft only in as much as the theft is enacted and in turn necessitated by the construction of its legal coding as thievery in the first place; and when this realization is in turn coupled with Stirner’s call for active, associative robbery, the resulting book can thus only be (legally, and yet illegally) stolen if it contains a copyright incantation which aims to prohibit the very action it necessitates and calls into being in the first place.

Given the existent legal parameters which permeate existent culture in their meticulous attempts at corralling and congealing information flows, however, it would be far too foolhardy to merely engage in reckless robbery that pays no heed to the potential consequences if econo-legal restraints come bearing down on the budding data liberator. The prevention of apprehension is thus of pivotal importance both to the assurance of a continued liberation of information as well as to similar assurance of unabated devotion to the copyfight. Lest one, dejected and utterly defeated by the machinations of the State, traitorously yet tragically renounces illegalism, as did Marius Jacob—“one of the foremost exponents and practitioners of anarchist illegalism in pre-war France” who conducted a number of burglaries and the like—who by 1948 stated: “I don’t think that illegalism can free the individual in present-day society. If he manages to free himself of a few constraints using this means, the unequal nature of the struggle will create others that are even worse and, in the end, will lead to the loss of his freedom, the little freedom he had, and sometimes his life”<sup>363</sup>, as informational illegalism is concerned by the eponymous information, not the individual, we could replace instances of ‘individual’ in Jacob’s quote with ‘information’; and yet the outcome would be the same. If either individuals involved in the copyfight or the information

---

<sup>362</sup> Abbie Hoffman. 1971. *Steal This Book* (25th Anniversary Facsimile Edition). New York: Four Walls Eight Windows.

<sup>363</sup> Doug Imrie. 1994-5. “The ‘Illegalists’”, in *Anarchy: a Journal Of Desire Armed* (Fall-Winter 1994-5). [http://theanarchistlibrary.org/HTML/Doug\\_Imrie\\_\\_The\\_\\_Illegalists\\_.html](http://theanarchistlibrary.org/HTML/Doug_Imrie__The__Illegalists_.html).

being liberated is itself once again caged, then the damage to the struggle at hand would indeed be quite severe.

### **2.4 Case Study 3: Informational Illegality (Critical Praxis) — Unwatermarking Eelectronic Journal Articles**

When thereby engaging in the ‘critical praxis’ discussed by Striphias and McLeod, as well as the utilization of piracy to undermine the restraints of IP-laden academic publishing, one must—now being fully cognizant of the hostile legal climate—take the necessary precautions so as to avoid detection and neutralization. It is towards this pivotal practical concern that we now turn attention to by way of example. The immediate issue at hand is here then not so much the creation of “an open source peer-to-peer system which would make it very difficult for anyone involved to be prosecuted for copyright infringement”<sup>364</sup>, but rather the potentiality that the content itself—and not necessarily the distribution system—may lead to the pirate’s undoing. An elaborately established array of getaway cars will do little good, in other words, if the money bags taken from the bank contain tracer beacons.

Indeed access to the ‘bank’ as such is a task of relative ease. Despite academic journal subscriptions at times costing tens of thousands of dollars, as long as one has the necessary credentials one can gain entry thereto. Academic journal publishers employ two singular methods of authentication for entry: either the provision of an authorized Internet Protocol (IP) address from a subscribing institution, or a login/password combination. To gain an academic IP address one can either access the specific journal portal from an on-campus location: an unsecured or compromised wifi connection, for instance, or one can tunnel in through an open proxy connection, by searching public lists of precisely such proxies<sup>365</sup>. To obtain a login/password combination, meanwhile, one could either sniff wireless network connections for possible unsecured login credentials, or search for trial passwords to various academic journal databases that some library websites (in)advertently place online. Of course, if one is actually a member of any academic institution, the matter of access to the journal databases simply becomes a matter of legitimately logging in to the desired presses and downloading all content not yet freely available so as to readily facilitate its unbridled dissemination. Though indeed, the matter of downloading may itself prove to be problematic, as Aaron Swartz received a federal indictment precisely due to his downloading of a number

---

<sup>364</sup> Hall, *op. cit.*, p. 23

<sup>365</sup> AtomInterSoft. 2014. “Free Open Public Proxy List sorted by domain”. *AliveProxy*. [http://atomintersoft.com/proxy\\_list\\_domain\\_edu](http://atomintersoft.com/proxy_list_domain_edu).

of journal articles from the JSTOR e-journal content provider<sup>366</sup>. Thus caution needs to be exercised when obtaining the articles themselves.

However, the focus of this case study will not be on content acquisition (due to the fact that instructions on utilizing proxy services and the like may be readily found with a web search), but on diffusing of content once procured—in other words, once downloaded, how are we to ensure both our and its safety in avoiding apprehension. Refer to Appendix 2: ‘Sample Procedure for Watermark Removal from Eestro eJournal Articles’ for a step-by-step enumeration of a possible workflow for neutralizing procured content and rendering it suitable for anonymous distribution. What follows here is a summary and reflection of the undertaken procedure.

Our primary and most pivotal concern is with nothing short of *time* itself. The capitalist fascination with, and elaborate enunciation of time discipline extends beyond mere regulation of the workforce<sup>367</sup> into the codification and striation of all Bodies of Work it seeks to lay claim to. Within our immediate domain of attention—academic journal article—time discipline is manifested in the form of timestamps deployed for the purposes of *traitor tracing*. The latter is the forensic practice of embedding information within set content which would allow the content owners to trace the originating source of the data leak<sup>368</sup> (who is thus tacitly/affectionately termed as a traitor). Specifically, by including the precise time (and at times the location) at which a specific journal article was downloaded, the academic publishers, upon encountering said article outside of its allotted cage of economically-sanctioned distribution via the publisher’s official sales site, may then correlate the timestamp with their server logs and precisely deduce which IP address (and where applicable, which potential subscribing institution and/or individual account) downloaded the article and question is therefore to be held liable for the act of content liberation.

Aside from the timestamp injected into a given journal article by the content owners, however, PDF files also have an internal timestamp of their own which lists the time (and at times timezone) at which that specific instance of the document was created and modified. A sample dataset would resemble the following:

---

<sup>366</sup> Nancy Sims. 2011. “Library licensing and criminal law The Aaron Swartz case”, in *College & Research Libraries News* 72 (9). pp. 534-537.

<sup>367</sup> EP Thompson. 1967. “Time, Work-Discipline, and Industrial Capitalism”, in *Past and Present* 38. pp. 56-97.

<sup>368</sup> Jarrod Trevathan and Hossein Ghodosi. 2003. “Overview of Traitor Tracing Schemes”.

<http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.5.5947>; K. J. Ray Liu, Wade Trappe, Z. Jane Wang, Min Wu, and Hong Zhao. 2005. *Multimedia Fingerprinting Forensics for Traitor Tracing*. New York: Hindawi Publishing Corporation.

```
<xap:CreateDate>2012-02-10T21:12:52+05:30</xap:CreateDate>
<xap:ModifyDate>2012-02-10T21:12:52+05:30</xap:ModifyDate>
<xap:MetadataDate>2012-02-10T21:12:52+05:30</xap:MetadataDate>
```

The timestamp thus contains the year, the month, the day, the hour, the minute, the second, and the timezone. What this translates to for the informational illegalist is that the very thing one must do, prior to downloading any journal articles to be liberated, is to change one's system clock to a differing time, date, and timezone. While the exact process to do so varies by operating systems, simple instructions to do so are readily available online<sup>369</sup>.

Following the change in time on one's own computer, one can now proceed to download the desired articles. Whilst the aforementioned change affects the documents made on one's own computer, however, it does not affect the timestamp which may be imprinted on the PDF server-side by the publisher.

Out of a sample set of eight prominent academic journal publishers—Annual Reviews Inc., Cambridge University Press, Duke University Press, JSTOR, MIT Press, Oxford University Press, Sage, Taylor & Francis, Wiley—I found that ~71%, or 5 out of 7—all use varying timestamps to mark the downloaded journal article PDF files. The timestamps present themselves either as marginalia on the outskirts of the page, and/or as a cover sheet which precedes the main journal article. Following identification, let us now then set about the excision of this insidious location beacon from our pilfered money bag. Using the briss tool<sup>370</sup>—a program for cropping PDF documents—we can define new margins for any given PDF file, thus effectively cropping out the offending time and location stamps. And yet, briss performs what is known as a *non-destructive crop*: while the page margins are indeed resized to fit out stipulated dimensions, any actual data that was formerly within those margins is not actually deleted from the PDF file; merely rendered invisible to the casual observer. To eliminate this security risk, we must then further print our briss-cropped PDF file into yet a third new PDF by using the PDFCreator<sup>371</sup> PDF printer software. This third iteration of the journal article now effectively rids the PDF of the timestamp fetters. If the PDF in question also included an aforementioned publisher-injected cover page which identifying information, then we can set PDFCreator to simply not print the first page, as the need may be.

At this point, the resultant journal article should both be free of traitor-tracing timestamps injected by the publisher, as well as have an erroneous timestamp within the file

---

<sup>369</sup> Computer Hope. 2014. "How to set a computer's date and time". <http://www.computerhope.com/issues/ch000554.htm>.

<sup>370</sup> Gerhard Aigner. 2010. briss. v. 0.9. <http://sourceforge.net/projects/briss/>.

<sup>371</sup> Philip Chinery and Frank Heindörfer. 2006. PDFCreator. v. 0.9.3. <http://sourceforge.net/projects/pdfcreator/>.

itself. Aside from timestamps however, there is another other potential insidious method of traitor-tracing publishers may deploy known as Natural Language Watermarking (NLW), “which uses the structure of the sentence constituents in natural language text in order to insert a watermark”<sup>372</sup>, thus rendering every downloadable copy of a text literally unique by modifying the actual wording of the text itself. To detect unique permutations in individual iterations of the same parent article, one can perform a comparison attack (alternatively called a detection-comparison attack) so as to attempt to elucidate any latent modifications by bringing to the fore any incongruities found between the analyzed versions of the given document<sup>373</sup>. However, in performing a basic comparison attack that would detect any such modification in all seven sample articles from the various publishers, I found that none currently employ NLW methodology of traitor tracing. Nonetheless, lest such practice becomes more commonplace in the future, one must download a minimum of two instances of the same article, and—upon stripping out any timestamps or other potential uniquely identifying content—convert the articles two plaintext (by simply copy and pasting the contents of each PDF), thereupon performing a standard \*nix command<sup>374</sup>:

```
sdiff first_copy_of_article.txt second_copy_of_article.txt
```

which will result in the presentation of any variations within the two files side by side, which one can then modify so as to foil any potentially present natural language watermarks. One can then now proceed to engage in the dissemination of the unfettered journal articles.

Having thus far predominantly exclusively on written forms of content congealment, as explored through paratextual analysis of copyright/left incantations and the liberation of academic journal articles, we can now move on to the exploration of the cinematic realm to further analyze and develop emancipato-surgical strategies of unbridled content promulgation.

---

<sup>372</sup> Mercan Topkara, Cuneyt M. Taskiran, and Edward J. Delp. 2005. “Natural Language Watermarking”. *Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents*. pp. 441-452 (p. 441).

<sup>373</sup> For examples of discussions of comparison attacks on watermarks embedded in various media, see: Fabian M. Suchanek, David Gross-Amblard, and Serge Abiteboul. 2011. “Watermarking for Ontologies”, in *The Semantic Web - ISWC 2011 - 10th International Semantic Web Conference Bonn, Germany, October 2011, Proceedings, Part I* (eds. Lora Aroyo, Chris Welty, Harith Alani, Jamie Taylor, Abraham Bernstein, Lalana Kagal, Natasha Noy, and Eva Blomqvist). Lecture Notes in Computer Science 7031. Germany: Springer-Verlag. pp. 697-713 (p.701); Darko Kirovski and Henrique Malvar. 2002. “Audio Watermark Detector”. US Pat. US 2002/0107691 A1. p. 7; Ed Felten. 2006. “How Watermarks Fail”. *Freedom to Tinker*. <https://freedom-to-tinker.com/blog/felten/how-watermarks-fail/>.

<sup>374</sup> Alternatively, a number of other comparison tools may be deployed, such as WinMerge (Dean P. Grimm. 2013. WinMerge. v. 2.14.0. <http://winmerge.org>).

**3.**

**Ordinance the Second:  
Emancipato-Surgical Strategies for  
Data Liberation**



Once a legally-delineated Body of Work (BoW) has been congealed by the primary IP-based fettering discussed in the previous chapter, a secondary set of shackles is then imposed on this conjured BoW to further ascertain its acquiescence to its newly formed state of stasis, or at best, of restricted and pre-chartered flow. This secondary set of fetters operates through an architectural mode of repression: data flows are stifled through systems built directly into, or grafted and hence fused with, the particular BoW in question. In other words, the secondary set of shackles attempts to ensnare and congeal data through a series of technological restraints, which then operate in tandem with the aforementioned legal restraints which they serve to reinforce. Once a plot of private property has been accorded through the primary legal congealment, landmines and electrical fencing is then placed throughout the perimeter by way of the secondary fettering. Specifically, these fetters consist of various Digital Rights Management (DRM) implementations as well as a variety of forensic watermarking measures. The former, DRM, is essentially an array of technological content access control implementations which serve to impede who may view a given DRMed BoW and where said BoW may be viewed on<sup>375</sup>; for instance, a DRMed ebook purchased from Amazon is only accessible via devices which are registered to the purchasing account, and further limiting the total amount of registered devices which may simultaneously view the book<sup>376</sup>. The presence of DRM is explicit and overt: if one tries to open a DRMed BoW on an unauthorized device, the BoW will not be viewable. This is in stark contrast to the modus operandi of watermarking, which is implicit and covert: if one tries to open a watermarked BoW on any device, the BoW will be viewable, as will the watermark, albeit the latter may not be obviously apparent—depending on if a perceptible or imperceptible fingerprinting schema is used—to those who are unaware of their presence<sup>377</sup>.

---

<sup>375</sup> Niels Rump. 2003. “Digital Rights Management: Technological Aspects: Definition, Aspects, and Overview”, in *Digital Rights Management: Technological, Economic, Legal and Political Aspects* (eds. G. Goos, J. Hartmanis, and J. van Leeuwen). New York: Springer. pp. 3-15. See also: Supriya Singh, Margaret Jackson, Jenny Waycott, and Jenine Beekhuyzen. 2006. “Downloading vs Purchase: Music Industry vs Consumers”, in *Digital Rights Management: Technologies, Issues, Challenges and Systems* (eds. Reihaneh Safavi-Naini and Moti Yung). Germany: Springer-Verlag. pp. 52-65 (p. 53).

<sup>376</sup> Amazon. 2014. “Downloading Content to Multiple Kindle Devices”, in *Transferring, Downloading, and Sending Files to Kindle 2nd Generation*.  
[http://www.amazon.com/gp/help/customer/display.html/ref=hp\\_navbox\\_multiple\\_200375630?nodeId=200375630&#multiple](http://www.amazon.com/gp/help/customer/display.html/ref=hp_navbox_multiple_200375630?nodeId=200375630&#multiple). See also: Defective by Design. 2010. “Amazon's Kindle Swindle”.  
<http://www.defectivebydesign.org/amazon-kindle-swindle>.

<sup>377</sup> Inegemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker. 2008. *Digital Watermarking and Steganography* (Second Edition). Burlington, MA: Elsevier.

As there is already a sizable body of work aimed at circumventing or otherwise defeating DRM-shackled media<sup>378</sup>, the focus of this case study will instead be on the much more often overlooked second set of architectural fetters: forensic watermarking. In contrast to DRM-based restrictions which aim at an *a priori* restriction of the unbridled promulgation of information, watermarking-based fetters operate through a seemingly paradoxical *a posteriori* restriction of content dispersal. That is to say, while DRM attempts to prevent the initial liberation of a particular set of data, akin to requiring the user to enter a certain combination to open the bank vault door, the aim of watermarking is to fetter future attempts at content dispersal by leading to the identification and—here once again highlighting how architectural and legal fetters function in tandem—apprehension of whoever was responsible for the leaking of the content, thus preempting any future promulgation from that particular, now neutralized, node of resistance. Thus, as recalled from our earlier discussions of watermarking during our foray into ejournal articles and ebooks, watermarking is akin to a tracker beacon planted within a bundle of currency which may or may not reside in a bank vault. Note also that DRM and watermarking shackles are not mutually exclusive, and thus may or may not both be utilized at the same time, and as such a particular BoW may either be exclusively DRMed or watermarked or be twice shackled by both.

Imperceptible watermark-based fettering is achieved through the surreptitious embedding of a uniquely identifiable forensic marker within a target BoW in such a way as to appear invisible to the end-user but immediately recognizable to a piece of recognizance code or watermark-identification algorithm operated by the content controller, which upon extraction, will relay information relating to the origin of this specific BoW, including such potential items as its source and time of manufacture and purchase, which in turn leads to facilitating the ease of the aforementioned apprehension of whoever was responsible for

---

<sup>378</sup> Aside from the technical literature on DRM vulnerability (e.g. Tobias Hauser and Christian Wenz. 2003. “DRM Under Attack: Weaknesses in Existing Systems”, in *Digital Rights Management: Technological, Economic, Legal and Political Aspects, op. cit.*, pp. 206-223.; Stuart Haber, Bill Horne, Joe Pato, Tomas Sander, Robert Endre Tarjan. 2003. “If Piracy Is the Problem, Is DRM the Answer?”, in *Digital Rights Management: Technological, Economic, Legal and Political Aspects, op. cit.*, pp. 224-233.; Mark Stamp. 2003. “Digital Rights Management: The Technology Behind The Hype”, in *Journal of Electronic Commerce Research* 4 (3). pp. 102-112), there are further a number of existent tools for DRM emulation and removal for a variety of media including DVD (Lightning UK!. DVD Decrypter. v. 3.5.4.0. <http://www.dvddecrypter.com>), Blu-ray (DVDFab. 2014. DVDFab HD Decrypter. v. 9.1. [http://www.dvdfab.cn/hd\\_decrypter.htm](http://www.dvdfab.cn/hd_decrypter.htm)), audio (RapidSolution Software AG, *op. cit.*), streaming video (GetFLV.net. 2014. GetFLV. v. 9.6.8.8. <http://www.vdigger.com/>), books (Apprentice Alf. 2014. DeDRM Tools for Calibre. v.6.1.0. <https://apprenticealf.wordpress.com/2012/09/10/drm-removal-tools-for-ebooks/>), and games and software (DT Soft Ltd. Daemon Tools. v. 1.39. <http://www.daemon-tools.cc> (N.B. the latter subverting DRM via emulation or spoofing, as opposed to outright removal as in other cited instances)).

jailbreaking the BoW and thus ending any potential future liberatory action from said neutralized node of resistance. Finally, it is imperative to keep in mind that the watermark effectively forms a positional serial number that becomes engraved in the BoW, which in operating in four dimensions (appearing at a specific time and place in the BoW) need not be expressed as an actual digit, but may present itself through as a data borne of absence, for instance a set of apparently incidental typographic omissions in a text or minute imperfections in the audio stream of a film may serve as uniquely identifiable forensic watermarks just as much as a literal serial number stamped within the fibers of a currency note.

The focus of the immediate chapter thus lies on a critical explication, followed by a potential neutralization, of the various operant modes of audio-visual watermark-based fetters as explored through a case study of cinematic film watermarking, which has been situated above as constituting a particular subset of the larger set of architectural fetters designed to impede the free flow of data. The underlying aim of the case study is two-fold. First and foremost lies the task of bringing to light the operant, transparent systems of data repression, a particularly pivotal aim due to the fact that said systems of repression explicitly rely on invisibility, with the *Digital Cinema System Specification*—a joint document dictating the specific terms of digital cinematic projection drafted by the top cinematic content controllers<sup>379</sup>—stating that “[i]mage Forensic Marking is required to be visually transparent to the critical viewer in butterfly tests for motion image content [...] Audio Forensic Mark is required be inaudible in critical listening A/B tests”<sup>380</sup>. The systems of control rely on undetectability, their explication alone thus serves a fundamental blow to their efficacy of content repression. However, going beyond mere explication, and all the while engaging in what Deleuze has described as the “socio-technological study of the mechanisms of control, grasped at their inception [which] would have to be categorical and to describe what is already in the process of substitution for the disciplinary sites of enclosure”<sup>381</sup>, the *critical* aspect of the case study involves an active attack against said systems of congealed oppression by developing a counter-forensic methodology of—having now identified the

---

<sup>379</sup> Specifically, the initiative, which forms its own Limited Liability Company entitled Digital Cinema Initiatives, is composed of Disney, Fox, Paramount, Sony, Universal, and Warner Bros. film production and distribution corporations (Digital Cinema Initiatives. 2014. “About DCI”. <http://www.dcimovies.com/>).

<sup>380</sup> Digital Cinema Initiatives, LLC. 2008. *Digital Cinema System Specification v1.2*. pp. 127-8 [http://www.dcimovies.com/DCIDigitalCinemaSystemSpecv1\\_2.pdf](http://www.dcimovies.com/DCIDigitalCinemaSystemSpecv1_2.pdf).

<sup>381</sup> Gilles Deleuze. 1992. “Postscript on the Societies of Control”, in *October* 59. Cambridge, MA: MIT Press. pp. 3-7. <http://www.n5m.org/n5m2/media/texts/deleuze.htm>.

venomous serpents of congealment—active defanging thereof. Thus the analysis will move from an initial engagement with existent film theory around the theme of the film as prisoner to an overview of operant cinematic film watermarking techniques, to finally an attempted counter-forensic neutralization thereof which will culminate this particular case study in the praxis of data liberation. The strategies deployed in this section are termed emancipato-surgical, for they seek to emancipate the film from the technical fetters deployed in the service of IP congealment by content controllers, and are further surgical due to the fact that to achieve said emancipation they need to operate with precision upon the film’s body, performing operations to remove the malignancies ailing the body in the form of audio-visual forensic markers.

### **3.0 Cinema as Prison (CaP<sub>1</sub>)**

When the relation between the cinema and imprisonment is broached in existent film theory, the cinema is either presented as being a safe haven from the prison, affording the audience a cocoon-like reprise from the horrors of the real, or alternatively, the cinema is seen as indeed being a prison, albeit one wherein the prisoners are the attending audience. The problem with both theorizations, as shall be shown, is their audience-centric approach which ignores the impact of the cinema on the film itself. In their place, I then postulate a relatively straightforward alternate formulization in which the film is the prisoner in the cinema. To then first look at the theories that present the cinema as panacea to the terrors of modern life, according to Burgin, “[i]n American cities, where ‘street life’ so often gives way to ‘street death’, the citizen is almost certainly safer in the movie theatre than at home, at work or in prison. In a world driven by violent factional and fractional conflict, the cinema is peaceful”<sup>382</sup>, with Barthes likewise crooning a mesmerizing lullaby, “[i]t is in this urban dark that the body's freedom is generated; this invisible work of possible affects emerges from a veritable cinematographic cocoon”<sup>383</sup>. How then could one possibly challenge these veritable odes to the transcendent power of the *cinéfantastique*? Why, by turning to another critical text, namely *Last Action Hero*, a Schwarzenegger-powered actioner from 1993.

The plot, as it were, revolves around a schoolboy, Danny Madigan, who takes shelter from the harsh realities of ‘street life’ giving way to ‘street death’ in the comforts of a lush old multiplex. To wit, in a particularly poignant moment early on in the film, an intruder breaks into Danny’s apartment late at night (Danny’s mother, a widow, works the night shift

---

<sup>382</sup> Victor Burgin. 2004. *The Remembered Film*, London: Reaktion Books. p. 43.

<sup>383</sup> Roland Barthes. 1975. “Leaving the Movie Theater” (trans. Richard Howard), in *The Rustle of Language*. Berkeley: University of California Press. pp. 345-349 (p. 346).

thus leaving Danny home alone), slams Danny into the bathroom sink, handcuffs him to the toilet plumbing, and after colorfully stating his displeasure at the lack of liquid assets in the Madigan residence, then proceeds to toss the handcuff key into the toilet. Upon receiving no satisfaction from the local constable, Danny flees to the theater, desperately banging on the closed doors to be let into the sanctuary. Once inside the comfort of the theater hall and as the opening credits to Schwarzenegger's latest action sequel begin to roll, Danny's constitution morphs from one of morbid terror exhibited during the aforementioned burglary, to one of carefree *jouissance* marked, one could say, "by the relaxation of postures (how many members of the cinema audience slide down into their seats as if into a bed, coats or feet thrown over the row in front!)"<sup>384</sup>. Thus far, in other words, the film presents a narrative identical to that idyllic fable spun by Burgin. And then a bundle of dynamite, lobbed by one of the bad guys in the film, flies through the screen and into the middle of the theater aisle. With the ensuing dissipation of Danny's relaxed facial intonation, so too comes the dissipation of the comforting theater-as-embryonic-panacea theorization. So too does the subsequent eruption of said dynamite, which propels Danny into the screen, serve to shatter any tidy bifurcation between reality and the film. A delineation that is rendered all the more impossible throughout the film as Danny and various other good and bad guys repeatedly journey from the other side of the screen back into Danny's side and vice versa, eventually even inviting personages from other films into Danny's world as well, thus journeying not only across the spatial constraints of filmed reality, but easily traversing any temporal limitations as well.

The overall impact of this continuously induced vertigo, the slinging back and forth of characters from one reality to the other and back again any number of times, has the dizzying impact of ungrounding any formerly wedded notions of separation between film and any tangible existence outside thereof. Thus the very predicate upon which Burgin's argumentation is primarily structured, that there exists a neat bifurcation between the screen and its exterior, indeed that there exists a distinguishable exterior in the first place, is here exposed as a falsity. And of course, it then makes precious little sense to postulate the cinema as being a safe haven from reality when no clear-cut separation between the two exists in the first place. Burgin's formulation is thus exposed by the film to be naught more than a castle built within a castle in the air. What's further, however, is that *Last Action Hero's* literal dynamiting of terroritorial restriction, its bombing of borders, furthermore instills a notable

---

<sup>384</sup> *Ibid.*

potentiality of equality between the formulated fellow co-constituents of the thusly all-encompassing Real. If there is no separation between the film and the real, indeed if the film is simply a particular component of the real, akin to the audience, the theater seats, or the projection apparatus, then it becomes both inexcusable and unexplainable to restrict an analysis of the cinema to an audience-centric formulation. Barthes' constant intonation that the film exists *for him* thus betrays, at best, either an unfortunate naïveté, an ignorance borne of his egocentric analysis, or at worst a dark sadism which takes joy in the film's forced subservience to the whims of the audience.

And yet perhaps it will be said that the aforementioned analysis has all too conveniently itself been restrained to the confines of a cinematic example of the alleged annihilation of the existence of the purely cinematic, thus rendering the argument toothless in our own reality? Why then, we can easily extend the cinematic into the real once again by turning to the horror film *Scream 2* (1997). At the onset of the film, the audience (within the film) is viewing the horror film *Stab*, a film based on the first *Scream* (1996), when one of the audience members is stabbed by the killer who looks identical to the one in *Stab*, who in turn looks like the one in *Scream*.

Going forward to 2008, we find news reports of two audience members stabbed whilst watching the horror film *The Signal*<sup>385</sup>. Fullerton then would appear to be one American city where street life indeed gave way to street death, albeit within the confines of what one will recall, according to Burgin, is supposed to offer greater safety than the dreaded outside. Thus once again, the flaw with the theater-as-alternative-to-harsh-reality hypothesis is shown to lie not only in the fact that street death can just as easily happen within the theater as outside of it, but that this very non-existence of any sort of magic force field further paves the way for a destruction of the cinematic/real (or 'street' to use Burgin's term) delineation. The cinema in general, and the film in particular, are—far from offering a reprise fro reality—are active co-constituent actants in the construction of emergent realities.

To take another example highlighting the implosion of the street life and death, in what may have been either an anti-piracy campaign and/or a viral marketing effort, a curious file appeared on The Pirate Bay on March 3, 2012, entitled "PLAN-C CAM READNFO XViD SHOCKING.avi"<sup>386</sup>. The video file starts off typically enough as a theatrical

---

<sup>385</sup> Gene Byrd. 2008. "Two People Stabbed in Fullerton Theater: Horror Movie 'The Signal'", in *The National Ledger*. <http://www.nationalledger.com/news-tech/video-two-people-stabbed-in-f-167978.shtml>.

<sup>386</sup> MonkeyT. 2012. "PLAN-C CAM XViD SHOCKING". *The Pirate Bay*. <https://thepiratebay.se/torrent/7074665>.

camcorder recording (CAM) of the film *Plan C*, which had only come out in theaters in the Netherlands two days prior<sup>387</sup>, thus rendering the fact that a CAM copy would be uploaded entirely plausible<sup>388</sup>. Several minutes into the recording, however, masked gunmen enter the theater and begin shooting. The camera recording the screen thus records the shooting. When whoever is holding the camera is presumably shot, the camera falls to the ground and continues recording, eventually showing the police arrive. The facts that the video was uploaded to a torrent website, instead of being confiscated by police, and presented as a straightforward CAM release, combined with the fact that there appear to be no news stories about the theatrical shooting, all point to the recording being a publicity stunt (which, itself, failed to draw much attention as well) and perhaps an anti-piracy message. An event, which was presumably not CAMed (as no such footage was available when searches were performed), but which did have corroborating news coverage, was the Aurora, Colorado shooting of July 20, 2012<sup>389</sup>, several months after the *Plan C* faux shooting, during which a masked gunman killed multiple audience members attending a screening of *The Dark Knight Rises*, once again shattering the projection of the theater as any sort of reprieve from the street.

### **3.1 Cinema as Prison (CaP<sub>2</sub>)**

There is, however, a second strand of argumentation which postulates that the cinema indeed functions as a prison, albeit one for the audience. Tracing its origins to circa 380 BC when Plato told the tale of a group of prisoners chained to the floor of a cave watching shadows cast upon the facing cave wall made by those walking behind the prisoners, whom they cannot turn around to see, this line of argumentation places modern-day movie-goers as being the ancestors to the Platonic prisoners; or, as Baudry puts it “projection and reflection take place in a closed space and those who remain there, whether they know it or not (but they do not), find themselves chained, captured, or captivated. [...] The arrangement of the different elements- projector, darkened hall, screen [...] reproducing in a striking way the

---

<sup>387</sup> “Plan C Release Info”. *IMDb*. <http://www.imdb.com/title/tt1922689/releaseinfo>.

<sup>388</sup> A ‘CAM’ is a video which has been recorded with a camcorder in a movie theater. ‘Cammers’ are those who do the recording, and ‘cammed’ copies are copies of said recordings. For discussions of CAMs, see Paul Craig. 2005. *Software Piracy Exposed*. Rockland, MA: Syngress. pp. 162-163; Wallace Wang. 2004. *Steal This File Sharing Book: What They Won’t Tell You About File Sharing*. San Francisco: No Starch Press. pp. 155-156.

<sup>389</sup> Ed Pilkington and Matt Williams. 2012. “Colorado theater shooting: 12 shot dead during *The Dark Knight Rises* screening”. *The Guardian*. <http://www.theguardian.com/world/2012/jul/20/colorado-theater-shooting-dark-knight>.

mise-en-scène of Plato's cave"<sup>390</sup>. Ah, but *who* precisely are those that remain there? Ostensibly, one may perhaps be prone to reply, 'why, the audience, of course.' And yet, at the very onset of his composition Baudry makes a highly curious note that "the development of the optical apparatus which will have as a consequence the decentering of the human universe, the end of geocentrism"<sup>391</sup>, and what's furthermore, in keeping with this decentering, is there is absolutely no explicit reference to the 'audience' in Baudry's essay at all. There is certainly talk of 'consumption of a product' producing any number of 'effects' to be sure, and yet the lack of an explicitly labeled subject leaves us in an unbridled interpretive limbo wherein 'those who remain there' may indeed be the films themselves as much as the audience. The ensuing analytical heliocentrism, ode to the glimmering projection bulb, nonetheless finds itself subjected to the dying humanist universe, for the question then becomes *for whom* are those who remain there chained, captured and captivated, if not for the audience? Thus the films become objectified as naught more than chained performers in this reversal of forms, existing indeed as lures for the audience with the ultimate goal—a goal upon which future offspring is predicated upon—of gross profit accumulation for their human owners. It is therefore imperative to elucidate that while indeed "the cinema can thus appear as a sort of psychic apparatus of substitution, corresponding to the model defined by the dominant ideology. The system of repression (primarily economic) has as its goal the prevention of deviations and of the active exposure of this 'model'"<sup>392</sup>, the cinema and the audience are here both exploited by the studio-owners of the films as well as by the particular managers of the prison industrial complexes (*viz.* multiplexes) they cohabit for the duration of the film.

And yet there are those who, through misrepresentation of the facts, would have us doubt the ensuing logical necessity of formulating solidarity between film and audience against the great congealers of content, the owners who bank on the exploitation of the film reel, who indeed present film as a mere lure upon which to hook the sedated, indeed 'hypnotized' spectators such as the likes of Barthes. Consider, for instance, the work of film theorist Mark Winokur, who in comparing the theater to a panoptic prison complex, claims that "[s]eeing a film in a theater, people sit evenly spaced in semi-circular fashion around a single image, panopticon-style; as Jean-Louis Baudry notes, the scene of filmgoing

---

<sup>390</sup> Jean-Louis Baudry. 1974-1975. "Ideological Effects of the Basic Cinematographic Apparatus" (trans. Alan Williams), in *Film Quarterly* 28 (2). pp. 39-47 (p. 45).

<sup>391</sup> *Ibid.*, p. 40.

<sup>392</sup> *Ibid.*, p. 46.



reproduces Plato's allegory of the enslaving cave which is itself, we might note, panoptic (if anachronistically so) in the sense that it provides an illusory world in order to enforce immobility in its viewers"<sup>393</sup>. There are indeed not merely one, but two misrepresentations herein, misreading—if indeed it is not an intentional disreading; the distinction between the former and the latter being one of intent—stacked upon misreading which has the cumulative effect of presenting the film/audience relationship as being one borne of antagonism, thus preempting any attempts at joint emancipatory cooperation. It will first be recalled, as just previously discussed, that Baudry makes no explicit mention of the audience or 'viewers', indeed the only explicit subject in his extension of the Platonic analogy to the realm of the film lies in the aforementioned mysterious 'those who remain', which in light of his noted de-centering of the geocentric, may just as well refer to the films and not the viewers or audience. Winokur further appears to commit a misreading of the original allegory itself, for Plato quite explicitly, and indeed repeatedly, makes mention of the chains which hold the prisoners in place—"Behold! human beings living in a underground den, which has a mouth open towards the light and reaching all along the den; here they have been from their childhood, and have their legs and necks chained so that they cannot move, and can only see before them, being prevented by the chains from turning round their heads"<sup>394</sup>. Thus immobility is quite clearly and explicitly enforced through the use of actual shackles, and not, as Winokur would have us believe, through the creation of an illusory world, which presumably for him refers to the projection of the shadow image. One could here certainly retort that the tale of the cave is after all allegorical, and thus there are not necessarily any literal chains to speak of, and thus perhaps Winokur is here applying the metaphor of the chains as extending to film projection itself? However, this cannot be the case as within the realm of the allegory itself, the chains and the projection are presented as two distinct elements, thus to confound the two would lead to a clear-cut misreading of the allegory just the same. But so what? Supposing that Winokur does commit a seemingly minor misrepresentation of the historical facts, an incidental revisionism, what is the import of this slight? Recall our earlier discussion of the import of solidarity between film-viewer and film against the controllers of content who seek to profit from both. By shifting the enchaining function from the chains themselves to that of projection of the shadow image or the film

---

<sup>393</sup> Mark Winokur. 2003. "The Ambiguous Panopticon: Foucault and the Codes of Cyberspace". *CTheory.net* a124. <http://www.ctheory.net/printer.aspx?id=371>.

<sup>394</sup> Plato. 2008 (c. 380 BC). *The Republic* (trans. Benjamin Jowett). Project Gutenberg. <http://www.gutenberg.org/files/1497/1497-h/1497-h.htm>.

itself, Winokur, however unwittingly or not, presents the illusory world of projection (*viz.* the film itself) as being the agent which imprisons the audience. In other words the film quite clearly becomes the enemy of the people, shattering all possibility of allegiance and furthermore masking the underlying puppet master who own both the filmed content and gain revenue for each audience admission into the cave.

Now, to be sure, Winokur is certainly cognizant of this malignant string-pulling third party, for he goes on to say:

[b]ut, while we believe ourselves to be watching television and film, these media are watching us along those axes by which we are allowed social definition: our viewing habits and so (presumptively) our desires, through Nielsen ratings, advertising sales, bottom lines, pre-emptive censorship, and so on. While, during the experience of watching, we believe the gaze to originate from the spectator and onto the screen, in fact the gaze is relayed from the screen/tower to the spectator in a way that coerces her to internalize consciously and unconsciously the lessons of the screen. This, at least, is the assumption that advertisers take on faith<sup>395</sup>.

Note, however, the collusion of varying subjects: the media (television and film) and screen/tower are apparently equivocated to the advertisers. Yet it is not the film itself that is watching the audience and collecting marketing data, but the advertisers which are watching the audience watch the film. The film's complicity as performer in the spectacle is purely involuntary, with the data mining of marketing intelligence being harvested through third-party metrics akin to black boxes sent to those chosen to be the statistical aggregators of Nielsen ratings or theater managers (prison wardens) selling their ticket-purchase numbers to third party marketing brokers. The pivotal point of this seemingly minute distinction is, once again, that the film is exploited as much as the audience; it does not merely partake in said exploitation on the part of the content owners. Recall our previous ANT-based discussion of the Berlin lock and key, actants which play pivotal parts in the ensuing assemblage, being subjected to duress (e.g. being filed away) as well as subjecting others to duress at behest of the landlord (e.g. by locking some people out). To forego discussion of nonhuman agency, as Winokur does, is to preempt any attempt at unification between the oppressed by painting comrades as enemies, to ignore both the complicity and the vulnerability of all players

---

<sup>395</sup> Winokur, *op. cit.*

involved in the de-scription of film viewing, is to thus serve the interests of those who seek to corral and congeal content, and of course to profit therefrom by rendering the exploitation of an entire subset of participants invisible.

Aside from the aforementioned audience-centric analyses which serve to vilify the film (image) via crass objectification (the film existing solely as a subservient *for*, as opposed to an active, co-actant *with*), there is still another approach to portrait the image as demonic through a subjectification coded as one of intrusion, of film being portrayed as a masked invader of the real. To wit, Baudrillard claims that “it is precisely when it appears most truthful, most faithful and most in conformity to reality that the image is most diabolical [...] It is in its resemblance, not only analogical but technological, that the image is most immoral and most perverse”<sup>396</sup>. Thus for Baudrillard the error would lie precisely in the reading of film as fellow compatriot with the audience against the struggle with the content owners, for it is allegedly in precisely this duplicity that the image colludes all distinction between the real and representation, “the secret of the image (we are still speaking of contemporary, technical images) must not be sought in its differentiation from reality [...] but on the contrary in its ‘telescoping’ into reality, its short-circuit with reality, and finally, in the implosion of image and reality”<sup>397</sup>. However, the fundamental premise of this politics of invasion, or *cinematic xenophobia* perhaps, is predicated upon an assumed *a priori* distinction between the image and the real that then subsequently becomes blurred to the point of erasure. In order for an image to be introduced into reality, as it were a virus contaminating a *foreign* body, which it then proceeds to wholly take over, the image must thus initially indeed exist as an externality. In other words there must exist a point in space-time in which the image has clearly existed as an independent external constituent outside of the scope of the real. Baudrillard, conveniently, offers no explanation of this necessary initial condition, instead resorting to the repetition of the modern day collusion of images and reality. In light of a lack of evidentiary support then, we may just as well postulate that the image has always been a constituent of the real.

Today there is indeed a coalescence of the cinematic and the realist, but far from being the result of the presumably insidiously viral properties of the image (where then did it come from, of what is it constituted?), it is instead an always-already intermingling, existing since the very birth of the image. What’s more, is it is highly curious to here see Baudrillard

---

<sup>396</sup> Jean Baudrillard. 1987. “The Evil Demon of Images” (trans. Paul Patton and Paul Foss). pp. 13-34 (pp. 13-14). <https://courses.arch.ntua.gr/fsr/130155/jean%20baudrillard.PDF>.

<sup>397</sup> *Ibid.*, p. 27.

code the fusion of the cinematic real as being a *contamination* of reality, seeing as how he has also claimed that “it would not be too far-fetched to say that the extermination of mankind begins with the extermination of germs”<sup>398</sup>. The corollary of course here being that if indeed the image is coded as a contaminant, a germ as it were, its own destruction would lead to the destruction of reality itself, thus betraying a symbiotic co-dependence borne of constituent coexistence with/in the real. For daily life to ‘become’ cinematographic and televisual would mean that a non-cinematographic real has been exterminated through the complete absorption and subsequent total diffusion of the cinematographic contaminant, a conceptual impossibility given the aforementioned mention of the fact that the extermination of the former is predicated upon the *extermination*, and not the *contamination*, of the latter. If contamination of the real with the germ of the cinematographic leads to the death of mankind—which is after all a prominent constituent of the real indeed—then how curious that this same extermination (or technically a different extermination, albeit with the same end, *viz.* that of extinction) is likewise achieved through the destruction of the germ. If death is achieved both through either injection or through removal of the same element, and if indeed mankind can only either exist or not, then the aforementioned binary elimination leads one to conclude that there could never have existed such a separate figment in the first place. Within the crude bifurcation of non/existence, the cinematographic must of necessity have always already been indistinguishable from the real. Baudrillard’s proclamation that is now indeed a most “marvelous indistinguishability, ideal constellation of simulation”<sup>399</sup> thus certainly rings true, with the sole augmentation being that this blending is not merely immediate but atemporal.

Not only then is it indeed true that “*Holocaust* is above all (and exclusively) a *televised* event or rather object” or in other words that “it is *Holocaust* the television film which constitutes the definitive holocaust event”<sup>400</sup>, but going further one can indeed say that this becoming-real is not born of any sort of transcendence of signification, that it constitutes the definitive holocaust event not due to the fact that “it is no longer an image”<sup>401</sup>, but precisely due to the fact that it never was an image wherein image is understood to be anything as being distinct from the real, rather it constitutes the potential of being a definitive

---

<sup>398</sup> Jean Baudrillard. 1988. *The Ecstasy of Communication* (trans. Bernard Schütze and Caroline Schütze). New York City, NY: Semiotext(e). p. 38.

<sup>399</sup> Baudrillard, “The Evil Demon of Images”, *op. cit.*, p 20.

<sup>400</sup> *Ibid.*, pp. 24-5.

<sup>401</sup> *Ibid.*, p.25.

holocaust event precisely *qua* image. What concerns us here is that the imprisonment of the filmed body, both in the sense of the literal bodies being filmed and in the sense of the film's actual body itself, is tantamount to imprisonment of the human; both, one will recall, constituting components of the all-encompassing real. Thus the "secret of the image" lies indeed neither in its "differentiation from reality", yet neither does it lie with "its 'telescoping' into reality"<sup>402</sup>, instead the secret lies precisely in the fact that the image is an actual constituent of reality, held prisoner in the cinema. The secrecy here arising is instead due to the fact that this fundamental truism is all too often suppressed by audience-centric film theorizations, which have the effect of further serving the interests of the content controllers in keeping the audience, who may otherwise feel compelled to take on the role of acting as jailbreakers, firmly segmented from any notion of solidarity with the film as fellow co-actants. The film being a figment of the real is thus on equal footing as any other surrounding component, be it the attending audience or the chairs upon which they sit. To elucidate this equivocation further, we can perform a comparative reading of *Theresienstadt* (1944) and a recent Warner Bros movie studio anti-piracy advert.

The only film to be shot inside an operating Nazi concentration camp, *Theresienstadt* depicts an apparently idyllic worker paradise, with camp denizens playing a game of soccer, spiritedly going about their errands, and even putting on a festive music show. Of course the film, the full subtitle of which translates to *A Documentary Film of the Jewish Resettlement*, is not as much a documentary as it is a coerced piece of propaganda intended to portray a benign view of life inside the camps. The 'actors', which is to say the camp occupants, were made to perform as instructed under penalty of death, and indeed most were eventually killed upon the completion of filming. The director, Kurt Geron, was told by the Nazis that he and his family would not be killed in exchange for making the film, only to be promptly transported to the Auschwitz camp wherein they were all gassed once filming was finished. And so the filmed result affords us a glimpse not into the idyllic camp life seemingly portrayed therein, but into the operation of the coercive Nazi propaganda machine<sup>403</sup>.

A Warner Bros. advert played at the start of various retail DVDs issued circa 2007 ostensibly shows a one-minute clip from the film *Casablanca* (1942) wherein Rick is upset because "the woman he loves is pirating DVDs"<sup>404</sup>. Of course Rick actually says no such

---

<sup>402</sup> *Ibid.*, p.27.

<sup>403</sup> Brad Prager. 2008. "Interpreting the Visible Traces of Theresienstadt", in *Journal of Modern Jewish Studies* 7 (2). pp. 175-194.

<sup>404</sup> Warner Bros. 2007. *Casablanca* Anti-Piracy Advert. <https://www.youtube.com/watch?v=DvjFsZJqAPs>.

thing, and indeed DVD discs did not exist in the 1940s. Instead, this piece of film was specifically crafted for the propaganda needs of the film studio, with the film being lashed into an enforced performativity with the aim of propagating a distinctly political message denigrating DVD piracy. Upon completion, the *Casablanca* film print is placed back into the confinement of the Warner Bros. film vault wherein it is confined until market demands lash it outwards yet again. Stripped of its original plot, *Casablanca* is made to conform to the whims of the studio's anti-piracy campaigning, effectively becoming a cog in the operation of the coercive anti-piracy propaganda machine, with the end of the advert of course bearing the notation "© 2007 Warner Bros", thus appropriation is itself ensconced in an act of IP congealment.

Both of the aforementioned examples of propaganda function through a peculiar mode of reappropriated *détournement* which encompasses both the cinematic and the realist, perpetrated by the dominant ideology. Neither film of course makes use of any actors or film sets; instead, both images use real bodies, wrenched from their genuine existence, so as to be forcibly manipulated to express an explicit ideology. Much like the underlying narrative of *Casablanca* has here been rewritten by Warner to suit its needs, so too has the narrative of everyday life of the Theresienstadt detainees been grafted with an alternate narrative to suit the needs of the Nazis. Thus Theresienstadt becomes *Theresienstadt*, the process of italicization thus signifying an act of revisionism. The liberation of the concentration camps has of course already occurred, when then will the film vaults likewise be liberated? A situation rendered all the more perverse by the countless filmed examples which depict the liberation of the former, all the while the latter, thusly still enchained, is nonetheless forced to repeatedly reenact the other's liberation. To render this pivotal point all the more explicit, with no mistake of metaphorical flourish: the film is a literal camp detainee, a prisoner in the jail of the multiplex.

Of course an objection at this point can be made that all of the hitherto accusatory discussion of a gross audience-centric anthropocentrism in the relevant prevalent film theory itself succumbs to an anthropomorphizing, or perhaps fetishizing, of the film. This criticism would of course miss the mark in its disregarding of our earlier discussion of ANT at the outset of the *Operations Manual*. The task in this section has been to highlight the potency of the film itself as vibrant actor in the de-scription of the cinema; the elucidation of the film's agency, in other words, should not be mistaken for an extension, or imposition, of humanism. On the contrary, the recognition of hybrid actant agency constitutes a removal of the

exclusively humanist claims to it. The exercise in other words was not one of attributing human characteristics to the film, but instead was an attempt “simply to extend the list and modify the shapes and figures of those assembled as Participants”<sup>405</sup> in the encompassing assemblage which constitutes a theatrical experience.

Specific charges of *anthro*-\* however, may be dealt with by firstly elucidating that anthropocentrism cannot be assumed to be a de facto equivalent of anthropomorphism, though the latter may indeed lead to the former, but if and only if, the anthropomorphized object is actually claimed to become the human itself, rather than merely possessing human-like attributes. And as I have nowhere stated that the film is indeed the human, rather that the film is simply a co-constituent (albeit not necessarily symmetric) alongside the human in a given operant network, I thus commit no anthropocentrism, and as such there is no problem of consistency free of any hypocrisy with the aforementioned derision of the anthropocentric focus of previous film theory. As to the question of anthropomorphism, the presumably controversial issue is in fact self-deflating, for through an egalitarian extension of allegedly human-like characteristics to the non-human, the characteristics in turn cease to be exclusively human, and thus the question of anthropomorphism no longer applies. Instead, we are merely left with a tepid remainder of a sort of ‘anthroattributionism’, or in other words the assigning of (no longer exclusively) human characteristics by humans. And this is all to say nothing of the fact that talk of anthropomorphism in the first place must seemingly accept a stifling purity of forms—the exclusively ‘human’ which is to be grafted on the formerly exclusively non-human—the very existence of which is by no means a certainty in the first place. Indeed, “the expression ‘anthropomorphic’ considerably underestimates our humanity. We should be talking about morphism. Morphism is the place where technomorphisms, zoomorphisms [...] all come together”<sup>406</sup>. Let us then leave behind fettering notions of totalizing humanism and turn towards the practicalities involved in unfettering the film from the chains clenched by IP holders instead.

### **3.2 Cinema as Prison (CaP<sub>3</sub>)**

Having thusly exposed the limitations in the aforementioned existent film theories which postulate the cinema as either a safe haven from the prison or as actually being a

---

<sup>405</sup> Bruno Latour. 2005. *Reassembling the Social: An Introduction to Actor-Network-Theory*. New York: Oxford University Press. p.72.

<sup>406</sup> Bruno Latour. 1993. *We Have Never Been Modern* (trans. Catherine Porter). Cambridge, MA: Harvard University Press. p. 137.

prison for the audience, we can now begin to put forth an alternate hypothesis which postulates that the cinema is indeed a prison, albeit one in which it the film, and not the audience, that is being held captive. To further explore the imprisonment of the film, we can proceed to undertake an analysis of the specific techniques of discipline centered around regulated distribution as applied to the production of the docile body of the film stock, “which transform the confused, useless or dangerous multitudes into ordered multiplicities”<sup>407</sup>, and can be initially summarized by the following table:

<i>Disciplinary characteristics</i>	<i>...as applied to cinema.</i>
Enclosure	Cinema
Partitioning	Theaters
Functional Sites	Entertainment Centers
Rank	Box Office Charts
Time-Table	Show-Times
Temporal Elaboration	Framerate
Body/Gesture Correlation	Projection
Body/Object Articulation	Audience Manipulation
Exhaustive Use	No Blank Frames

**Table 3.0:** Disciplinary Characteristics of Cinema.

First and foremost, “discipline sometimes requires *enclosure*, the specification of a place heterogeneous to all others and closed in upon itself. It is the protected place of disciplinary monotony”<sup>408</sup>. The primary sites of enclosure with regard to the film are of course the multiplexes, modern day cinematic prison industrial complexes that dot the commercial cityscape. Film reels are sent there in guarded containers, or increasingly as encrypted digital data streams, both of which function as literal prison irons which ensure that the film will not escape during transport to its designated place of confinement. The goal of this concentrated incarceration is of course the achievement of a total monitoring of both the inmates and their interaction with any potential visitors—the audience viewing the films—for “the aim is to derive the maximum advantages and to neutralize the inconveniences (thefts, interruptions of

<sup>407</sup> Michel Foucault. 1977. *Discipline and Punish: The Birth of the Prison* trans. Alan Sheridan). London: Penguin Books. p. 148.

<sup>408</sup> *Ibid.*, p. 141.



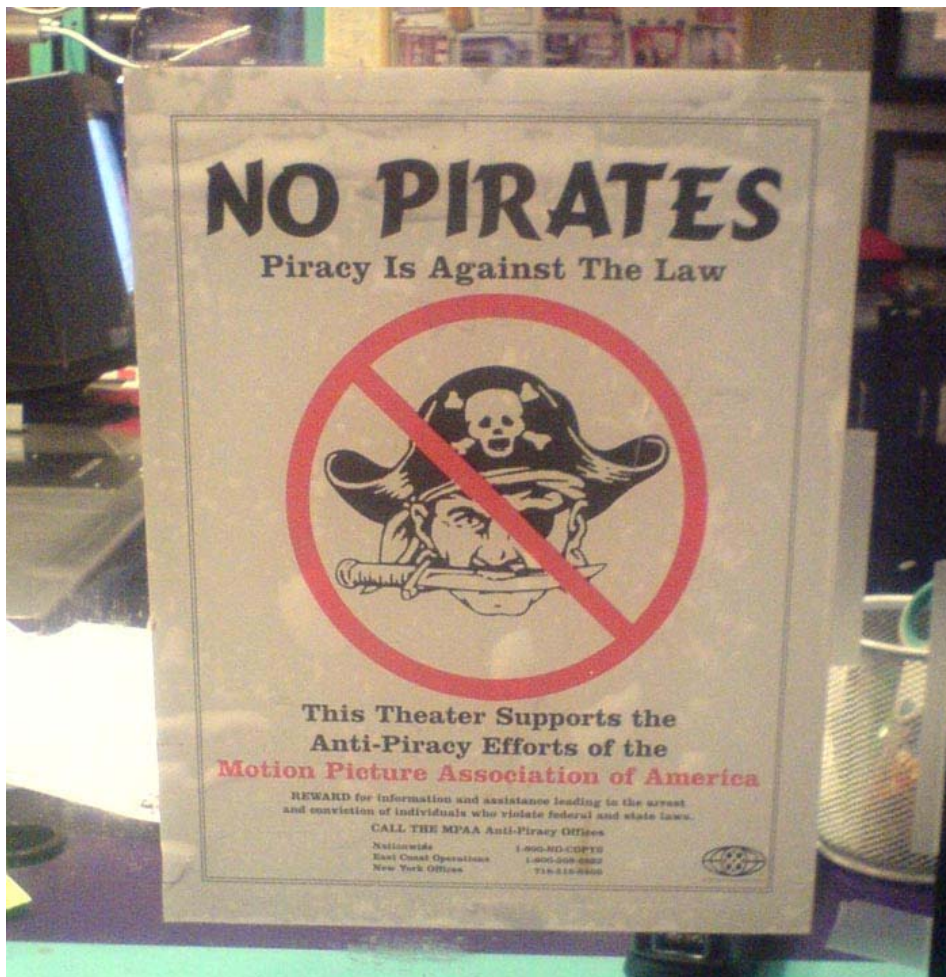
work...)<sup>409</sup>. To this end, the modern-day multiplex is thus equipped with a plethora of surveillance cameras which monitor not only the exterior perimeter of the multiplex, overlooking all entrances, exits, and the parking lot, and further not merely interior surveillance which monitors everything from the lobby to the stockrooms, but also via the utilization of specially-crafted infrared night vision cameras and night vision goggles which monitor the inside of the actual theater hall to ascertain that business is proceeding as usual (*viz.* that no one is attempted to jailbreak the film via the use of that modern-day acetylene torch, the camcorder). Further surveillance mechanisms are employed to ensure acquiescence to the demands of the content owners via the attempted foiling of any potential jailbreaking as seen by the presence of prison guards (ushers), who have often been told that they will receive a cash reward in addition to their standard wage for reporting any attempted jailbreak<sup>410</sup> and who are likewise at times equipped with night-vision goggles and require the visiting moviegoers to walk through metal detectors prior to entering the cinema<sup>411</sup>.

---

<sup>409</sup> *Ibid.*, p. 142.

<sup>410</sup> “The Take Action! reward program provides \$500.00 in qualifying cases to theater employees who identify patrons illegally recording a movie” (Motion Picture Association of America, Inc. 2012. “Take Action!”. *Fight Film Theft*. <http://www.fightfilmtheft.org/take-action.html>).

<sup>411</sup> Wang, *op. cit.*



**Figure 3.0** MPAA piracy reporting reward poster<sup>412</sup>.

Note, for instance, the poster in Figure 3.0, which states: “No Pirates. Piracy Is Against The Law. This Theater Supports the Anti-Piracy Efforts of the Motion Picture Association of America. REWARD for information and assistance leading to the arrest and conviction of individuals who violate federal and state laws. CALL THE MPAA Anti-Piracy Offices”. Thus within the enclosure of the theater an effort is made by content controllers to mobilize not merely the staff, but any visitors in general, in an effort to prevent dissemination of the films outside the sanctioned confines of the cinema.

All of which in turn brings us to the secondary technique of discipline, which follows enclosure: partitioning, for “the principle of ‘enclosure’ is neither constant, nor indispensable, nor sufficient in disciplinary machinery”. To wit, it is indeed insufficient to assign a film to a specific multiplex wherein it could leverage a state of spatio-temporal uncertainty to garner its freedom; that is to say that the content controllers are not content with knowing merely

---

<sup>412</sup> Image courtesy of: timotron. 2007. “Movie Review: Pirates of the Caribbean – At World’s End”. *Blogadilla.com*. <http://www.blogadilla.com/2007/05/27/movie-review-pirates-of-the-caribbean-at-worlds-end/>.

that a certain print is assigned to a certain multiplex. No, a much more finessed art of distribution must be employed to assure continued monitoring, to know precisely where in the prison the film prisoner has been allocated, and hence “disciplinary space tends to be divided into as many sections as there are bodies or elements to be distributed”<sup>413</sup>. Individual prison cells are thus assigned to the films upon their arrival under the title of specific theater hall numbers. And thus the content controllers know that a certain inmate is to be found in a certain theater hall within a certain multiplex. But of course, this spatial specificity, the elimination of imprecise distribution as it were, also has the added counter-effect of alerting any potential jailbreakers of where, precisely, to find the film they seek to liberate as well. Thus at least some of the metrics of discipline may indeed be appropriated for their liberatory potentiality, for a jailbreak operation becomes magnitudes easier when one knows the precise cell to which a captive has been confined.

Going further, however, the multiplex is of course not *merely* a site of confinement, for it also operates as a functional site, wherein “particular places were defined to correspond not only to the need to supervise, to break dangerous communications, but also to create a useful space”<sup>414</sup>. Thus theaters take on the role of not only chambers of compartmentalized enclosure, but of a functional entertainment center wherein the film is presented as a spectacle to enthrall the audience, and in turn boost revenue accumulation for both the governing multiplex operators and the underlying content owners. The function of the multiplex, aside from containment, is then quite clearly profit accumulation by way of a perverse sadism masquerading as recreational entertainment; akin to watching a public flogging. The pivotal point here is of course that confinement is a necessary condition for the profit accumulation to take place, at least within this particular economic schema, and thus the two functions are here deeply interlinked. In order to bank a profit the films must be confined, and in order to be confined the films must in turn be profitable, for profit is here the only acceptable form of value in the eyes of the content owners.

The aforementioned functional assignment of enforced performativity as a vector of profit accumulation in turn gives rise to a strict and highly detailed ranking mechanism in the form of box office revenue charts published at regular intervals in trade publications such as *Variety* and online platforms like *Box Office Mojo*<sup>415</sup>. Much like “rank attributed to each pupil at the end of each task and each examination”, so too is each film ranked after each

---

<sup>413</sup> Foucault, *op. cit.*, p. 143.

<sup>414</sup> *Ibid.*, p. 144.

<sup>415</sup> IMDb.com, Inc. 2014. *Box Office Mojo*. <http://www.boxofficemojo.com/>.

showing, the number of seats sold carefully tabulated by the prison officials before being forwarded to central aggregators which in turn supply the data to content owners and head wardens who then for their part authorize particular allotments within each prison complex to the best performing inmates, for after all “discipline is an art of rank, a technique for the transformation of arrangements. It individualizes bodies by a location that does not give them a fixed position, but distributes them and circulates them in a network of relations”<sup>416</sup>. Hence the highest grossing inmates are given the most luxurious cells, the largest theaters with the best projectors and biggest screens, whilst the lowest performing films are ushered into dingy side cells, running on screens that are often not much bigger than today’s high-end home entertainment systems, with archaic projection mechanisms which mutilate the print all the more during playback. Effectively, the inmates thus become pitted against one another for higher rankings, diffusing any possibility of a cinematic solidarity in favor of bigger cages and longer chains.

Discipline is further instilled in the prisoner films in the multiplex compounds via a rigorous control in the form of a time-table which serves to “establish rhythms, impose particular occupations, regulate the cycles of repetition”<sup>417</sup>. The showtime-table is unique not only for each multiplex, but custom-tailored based on the runtime of each and every film, resulting in a convoluted, always alternating, cinematic playlist with ever-shifting performance allotments for each film. The same film that is showing at 8:15 on a Tuesday may now be shown at 1:37 the following Monday, until it is no longer deemed sufficiently profitable for exhibition and is ushered into the ancillary confinement of the film vault. Much as with disciplinary partitioning, however, the presence of an, admittedly ever-shifting, timetable also has the advantage of presenting jailbreakers with not only the exact spatial coordinates of a given prisoner, but with its temporal coordinates as well. The introduction of a time-table thus allows not only the regulation of internal rhythms by the wardens and content owners, but also presents the advantage of knowing precisely when and where a film may be potentially liberated.

However, as is the similar case with enclosure in and of itself not being a sufficient disciplinary condition, necessitating a further partitioning within the initial confinement of enclosure, so too is the simple presence of a time-table not sufficient as the sole temporal characteristic of disciplinary order. To this end, an additional system of temporal elaboration

---

<sup>416</sup> *Ibid.*, p. 146.

<sup>417</sup> *Ibid.*, p. 149.

is further added, wherein “a new set of restraints had been brought into play, another degree of precision in the breakdown of gestures and movements, another way of adjusting the body to temporal imperatives”<sup>418</sup>. The cinematic specificities of precisely such a temporal elaboration are meticulously outlined in the new *Digital Cinema System Specification* guidelines, collectively dubbed a “code stream structure”, which for instance specify that “[a] 4K distribution shall have a maximum of 1,302,083 bytes per frame (aggregate of all three color components including headers). Additionally, the 2K portion of each frame shall satisfy the 24 FPS 2K distribution requirements”<sup>419</sup>. Thus the film is forced to play not only at a specific framerate (24 frames per second, in this instance), but with a set allotment of data designated for each frame, a clear-cut ‘marching step’ that must be perfectly synchronized as the “time measured and paid must also be a time without impurities or defects; a time of good quality, throughout which the body is constantly applied to its exercise”<sup>420</sup>. Temporal elaboration, in other words, further serves to achieve a smooth functioning leading to profit maximization whilst exercising the utmost discipline over the maximally regulated body of the film stock. The aforementioned process of division into set playrates, framerates, and showtimes, furthermore provides a perfect answer to the question of “how one can organize profitable durations”, for the content controllers must first of all “divide duration into successive or parallel segments, each of which must end at a specific time”<sup>421</sup>, before then proceeding to form an “analytical plan” of playback, and then upon finalizing the duration of each segment, then “draw up series of series”, and thus we have a set of prearranged frames, designated to play at very specific rates, at very specific intervals, on very specific days, and finally for very specific times. Specificity, and thus an exacting discipline, is thus enforced through a perfectly meticulous exertion of temporal regulation over the body of the film. The same regulation which, however, grants potential jailbreakers the key knowledge of when and where to best strike.

Strict temporal delineation, framerate and data allotments, still further serves to create a perfect correlation between the body of the film and its gesture. The synchronized projection of every frame at a set time leads to a seamless presentation of the film before the viewing audience. Any deviation from the outlined prescription leads to a desynchronization during the all important playback, resulting in imperfection which in turn affects potential

---

<sup>418</sup> *Ibid.*, p. 151.

<sup>419</sup> Digital Cinema Initiatives, LLC, *op. cit.*, p. 41.

<sup>420</sup> Foucault, *op. cit.*, p. 151.

<sup>421</sup> *Ibid.*, p. 157.

profit accumulation through the demands of refunds for ticket purchasing, with continued error perhaps even leading to an avoidance of that particular multiplex. And here we see that body/gesture articulation is in fact intimately linked to a further body/object articulation, wherein “discipline defines each of the relations that the body must have with the object that it manipulates”<sup>422</sup>. The object here being manipulated is of course the audience, resonating pertinent emotional peaks relevant to the body’s (film’s) genre, coupled with further profit accumulation solicitation via the injection of commercials both before the actual film reel and during via the placement of insidious product placements. The film is thus forced to elicit a pleasurable response from the audience that not only ensures sufficient satisfaction to merit repeated patronage of that particular multiplex, but to further solicit revenue accumulation through literal ads for commodities which have been grafted onto the film’s body by the marketing partners of the content owners. The result, of course, is that the film becomes pitted against the audience in the service of said content owners, much like one will recall was the outcome of Winokur’s earlier theoretical misreadings. Everywhere and always we thus see a trend to divide the audience and the film, to pit the one against the other endless, all in an effort to prevent a solidarity leading to the liberation of the film and the end of content owners’ attempt at data congealment for the purposes of profit at the direct expense of free unbridled data exchange.

Finally, what all of the aforementioned characteristics of cinematic discipline have been leading up to is in fact an exhaustive use of the film body, wherein no frame and no second is wasted on idleness. There are no allowances for any blank frames; the Specifications are once again quite explicit in their demands: “[t]he Image Track File is required to begin and end with complete frames that allow for splicing. Frames are defined to be image frames such as 24 FPS (1/24 sec) or 48 FPS (1/48 sec)”<sup>423</sup>. Every single cell, or frame, of the filmed body is put to use in every performance, and every performance is in turn exhaustively repeated until the body has either been worn beyond future use and is replaced (which is increasingly becoming a non-issue as actual film reels become more and more replaced by digital projection methods wherein the film is stored digitally rather than on actual film stock), or until the film has reached the requisite profit accumulation thresholds, at which point having thusly worn out its welcome and therefore its value for the

---

<sup>422</sup> *Ibid.*, p. 152-3.

<sup>423</sup> Digital Cinema Initiatives, LLC, *op. cit.*, p. 51.

content owners and wardens, it is simply replaced by a newer film which is ushered into its former cage in its place.

Yet, in spite of all of the aforementioned extensions of disciplinary regulation of the film, and even in light of all the accompanying modes of surveillance—the omnipresent CCTV, night vision goggles, metal detectors, and monetary incentives for apprehension of potential jailbreakers—films still escape from the prison complex we have conveniently dubbed the multiplex so as to mask its real intentions of bodily regulation. Indeed, according to the jailer organization MPAA, “approximately ninety percent of newly released movies that are pirated can be traced to thieves who use a digital recording device in a movie theater to literally steal the image and/or sound off the screen”<sup>424</sup>. Traditional disciplinary methods of content strangulation thus proving to be ineffective, we are now thus witnessing what Deleuze dubbed a “crisis of institutions, which is to say, the progressive and dispersed installation of a new system of domination”<sup>425</sup>. While these new systems of domination indeed operate through a “free-floating control that replaced the old disciplines operating in the time frame of a closed system”<sup>426</sup>, they are nevertheless not so much replacing the old systems as operating in tandem with them, so as to form an all the more stringent mesh of entrapment that operates *both* within the closed disciplinary system of the multiplex, and outside of it throughout the multiplicity of the external data swarm. Specifically, we are now witnessing a system of control that manifests itself through an “abstract machine of overcoding”; namely, via a plethora of pervasive watermarking schemas that seek to continuously track a film long after it has escaped the confines of the theatrical prison, all the while using the original disciplinary safeguards placed within the multiplex to help pinpoint those who have aided in the film’s initial escape. For instance, the use of a control metric, say an audio forensic watermark implanted into the film which persists after the film has been jailbroken from the multiplex, leads to the identification of the film pirate by pinpointing the latter’s location both in terms of specific multiplex and theater hall, but also even specific seat and showtime. This newly garnered data is then cross-checked against the existent disciplinary metrics, say the CCTV footage at that particular multiplex at that particular time alongside any pertinent ticket purchasing (replete with seat number) information, in order to thus subsequently identify the pirate who would then be apprehended by the police force—and here the intertwining of the two-headed serpent of State and Capital is perfectly crystallized—and thus neutralized from any future film liberation action.

---

<sup>424</sup> Motion Picture Association of America, Inc. 2011. “Types of Content Theft”.  
<http://www.mpa.org/contentprotection/types-of-content-theft>.

<sup>425</sup> Deleuze, *op. cit.*

<sup>426</sup> *Ibid.*

### **3.3 Cinematic Watermarking as Post-Disciplinary Control**

Make no mistake about it. We are indeed situated in the midst of violent copyfight, with regular news stories of film liberators jailed for their actions in support of the unbridled flow of information, caged and fined for their eschewal of the morbid stasis of congealment at the behest of those who stand to profit from the strictly ordained containment of data. Take for instance the case of Geremi Adam, who was arrested in 2010 for liberating various films from within a Canadian prison multiplex and sentenced to two and a half months of prison time. Geremi then started taking morphine, according to a friend, as a coping mechanism for the stresses of the legal process, and eventually died from an overdose that same year<sup>427</sup>. Several weeks ago, however, due to a leaked diplomatic cable released by Wikileaks on April 28, 2011, it was discovered that Geremi was arrested by the Royal Canadian Mounted Police (RCMP) solely based upon the personal behest of a member of the Canadian Motion Picture Distributors Association (CMPDA), to wit the cable plainly states that “with regard to the arrest of the individual who had been pursued by the CMPDA, RCMP officers stated that they arrested the individual ‘as a personal favor’ to a CMPDA official, and that they did not view theater camcording as ‘a major issue’”<sup>428</sup>. It is with this incident in mind, with the somber realization that the stakes involved in the ensuing copyfight sometimes extend to life and death, it is thus imperative to bring to the fore the all too often invisible functioning of cinematic watermarking and furthermore lay down the framework for an explicit attack methodology against it to ensure the safety of both those who risk their lives in liberating films and of the films themselves.

Towards this end we can begin by identifying four distinct, albeit interconnected, clusters of forensic audio-visual watermarking that effectively operate as “sieves whose mesh will transmute from point to point”<sup>429</sup>, making their elucidation both all the more difficult and all the more pivotal due to their constant changeability and fluctuation. The watermarks, by their very nature, are not the same for any two prints of a film, thus formulating a unique fingerprint for each copy which is used for future identification of the source of the print in question. While the precise inner-workings of the various watermarking systems are closely guarded industry secrets, we can nonetheless gain a fundamental grounding in their varying modes of operation through the availability of public patent filings, industry press releases, research publications, and finally through actual samples of watermarked films. Furthermore it should be noted that while the *Digital Cinema System Specification* stipulates that “[t]hese specifications require that image and

---

<sup>427</sup> enigmax, “Canadian Movie Pirate ‘Maven’ Dies of Drug Overdose”, *op. cit.*

<sup>428</sup> Marshall. 2006. “Camcording in Montreal theaters: perspectives from industry and law enforcement”. Embassy Cable. Ref. ID. 06MONTREAL1220. <https://wikileaks.ch/cable/2006/12/06MONTREAL1220.html>.

<sup>429</sup> Deleuze, *op. cit.*



audio Forensic Marking (FM) capability be included in each Image Media Block”, it nonetheless goes on to say that “[m]ultiple solutions may be qualified and will allow Media Block solutions providers to select the solution of their choice. Candidate providers should meet with individual studios”<sup>430</sup>. In other words, while the presence of audio-visual watermarking is mandated for all theater systems which use digital projection and adhere to the outlined specifications, there is nonetheless at this point in time no set industry standard of watermarking, with the result being that there is a proliferation of privatized proprietary watermark schemas developed by the corporations involved in cinematic distribution (the likes of Kodak, Sony, and so on). As is often the case however, the various watermarking schemas borrow heavily off of one another, allowing us as mentioned above to formulate a general 2x2 watermarking matrix, which can be summarized thusly:

	Primary Location Tracking (L <sub>1</sub> )	Secondary Location Tracking (L <sub>2</sub> )
Auditory Forensic Marker	Soundtrack Modulation	Time-Offset Detection
Visual Forensic Marker	Coded Anti-Piracy Imaging	Camcorder Positioning

**Table 3.1:** Theatrical Watermarking Potentiality Matrix.

There are effectively two kinds of cinematic forensic markers: those which watermark the video stream of the film, which for ease of reference will be referred to as Visual Forensic Markers (VFM), and those which similarly watermark the audio stream of the film, Auditory Forensic Markers (AFM)<sup>431</sup>. There are furthermore two types of auditory and visual forensic markers, each serving to identify a distinct location serving to identify precisely where the film was pirated, thus enforcing a four-dimensional temporal spatiality of control over the films. Primary Location Tracking (L<sub>1</sub>) serves to identify the specific multiplex from which the film was liberated, as well as the specific theater hall in which the film was broadcasted, and finally the specific date and at times time that the film was shown. Secondary Location Tracking (L<sub>2</sub>) goes even further and aims to identify the precise seat within a theater hall where the film was recorded. Finally, it is essential to keep in mind that while all of the discussed watermarks

<sup>430</sup> Digital Cinema Initiatives, LLC, *op. cit.*, p. 125.

<sup>431</sup> Much like there is no set standard for watermarking, there is furthermore no set nomenclature for the watermarks themselves. As the *Digital Cinema System Specification* states, “[i]ndustry terminology for watermarking and Forensic Marking is not consistent. For these security specification purposes, stakeholders have agreed to use the term Forensic Marking for all content marks” (*Ibid.*).

function based on the principle of invisibility and detection avoidance by all except specified detection algorithms and software, watermarks by their very definition introduce extraneous data in the audio-visual streams of the film which was not there prior to the injection of the watermark (or conversely, an inverse watermarking process may take place in which some data is removed from the original streams). It is this key principle of data tampering which we will now proceed to repeatedly exploit in our analysis of each specific cluster of existent watermarking systems.

### 3.3.0 Soundtrack Modulation [AFM; L<sub>1</sub>]

Primary location tracking oriented audio forensic markers effectively embed a uniquely identifying serial number into the audio stream of a projected film which serves to identify the time and location during which this specific copy of the film was broadcasted, as well as other ancillary data such as the make and model of the equipment used for playback. At the end of 2003, Digital Theater Systems, Inc., a corporation specializing in theatrical sound broadcasting, announced that it had begun beta-testing audio-based watermarking, with a planned wider global roll-out after the first quarter of 2004, claiming that “the system enhancements are aimed at providing increased control and security features to protect DTS-formatted audio for cinema use from unauthorized tampering, copying or playback”<sup>432</sup>. Similarly, in 2009 Sony filed a patent for an “audio watermarking apparatus” which “includes a time stamp and other data, for example information indicating the identity of the system on which the cinematic content is being reproduced”<sup>433</sup>. At unique points in the audio-stream of each watermarked copy of the film, the soundtrack is specially modulated to include a set frequency signal that when collectively identified by a well-guarded piece of watermark detection software produces a uniquely-identifying string which allows the aforementioned encoded data to be brought to light. Thus a content owner would potentially download a copy of a pirated film, feed the audio stream into said piece of detection software, and be presented with the encoded identifiable information, which would in turn be forwarded to the prison wardens as well as the relevant law enforcement agencies which owe the content holders a “personal favor” as seen in the aforementioned case of Geremi Adam, thus leading to the potential apprehension of the pirate and at least a temporary interruption of the stream of film liberation.

Recall that the *Digital Cinema System Specification* (and similarly echoed in the aforementioned Sony patent) states that its foremost “audio survivability requirement” is that

---

<sup>432</sup> Digital Theater Systems, Inc. 2003. “DTS to Introduce Security Enhancements for Cinema Audio Content Protection”. *PR Newswire*. Press release. <http://www.prnewswire.co.uk/cgi/news/release?id=113104>.

<sup>433</sup> Christopher Slater, Stephen Mark Keating, Mark Julian Russell. 2010. “Audio Watermarking Apparatus and Method”. Patent No.: US20100057231A1. p. 1.

“Audio Forensic Mark is required be [sic] inaudible in critical listening A/B tests”<sup>434</sup>. In other words, a ‘critical listener’ must not be able to tell an unwatermarked audio sample (A) apart from a watermarked, but otherwise identical, audio sample (B). While at first glance appearing as quite a stringent requirement indeed, nowhere does the *DCSS* appear to actually specify how, when, or even if, said A/B tests are supposed to be conducted. Nor is what constitutes a critical listener properly explained. This lack of distinct guidelines within the specifications leaves for us a notable bit of wiggle room with regard to precisely what constitutes an inaudible watermark. Note further that that aforementioned Sony patent states only that “the apparatus and method according to the present invention *reduces* the watermark's audibility”<sup>435</sup> [emphasis added], as opposed to, say, *eliminating* the audibility altogether. All of this ambiguity regarding audibility led me to conduct my own blind A/B test. I procured two audio samples taken from a theatrical broadcast of *Illegala*<sup>436</sup> and set them up for random playback, thus not knowing which sample was the watermarked one. I was in turn, successfully able to correctly identify the watermarked sample and furthermore pinpoint the precise watermarks, which presented themselves as distinctly audible background ‘beeps’.

However, while this freehand analysis proved to be successful in this instance, it is nonetheless predicated upon the continuous attention of the listener for the duration of the film’s soundtrack<sup>437</sup>. Even a slight distraction or lapse in attention could lead one to avoid spotting the presence of the watermark. Thus a more automated system is required that could be used in tandem with the freehand listening approach so as to effectively produce a “redundancy of consciousness and love that is not the same as the signifying redundancy of the other regime”, for “in the signifying regime, redundancy is a phenomenon of objective frequency involving signs or elements of signs [...] In the postsignifying regime, on the other hand, the redundancy is one of subjective resonance”<sup>438</sup>. Thus while the watermark identification software of the content owners operates strictly via a predefined detection algorithm which picks out the modulated frequencies within the film’s soundtrack, we choose to operate through a redundancy of subject resonance, letting our own ears detect the supposedly undetectable albeit combined with a technological backbone of our own, helping to ensure our own counter-detection of the audio watermark. We can here recall Barthes useful observation that “sound is merely a supplementary instrument of representation; it is meant to integrate itself unobtrusively into the object shown, it is in no way

---

<sup>434</sup> Digital Cinema Initiatives, LLC, *op. cit.*, p. 128.

<sup>435</sup> Slater et al., *op. cit.*

<sup>436</sup> Title is fictional. Refer to Disclaimer of Liability. Watermarked audio sample courtesy of [anonymous].

<sup>437</sup> An operative presumption of course being that the sample in which an audio watermark was not heard was watermark-free.

<sup>438</sup> Deleuze and Guattari, *op. cit.*, pp. 132-133.

detached from this object; yet it would take very little in order to separate this sound track: one displaced or magnified sound, the grain of a voice milled in our eardrums”<sup>439</sup>. Indeed, while it is the aim of the content controllers and their operative enforcers to seamlessly blend the auditory forensic markers into the background, fusing them with the so-called ‘cinema experience’ to the point of evading notice by either the casual audience or the dedicated film liberator, it would nonetheless in fact take just a singular audible stray beep to expose the watermark’s existence, and likewise it would take very little for us to separate said soundtrack from the film and render it palatable to specialized examination.

#### *3.3.0.0 Case Study 4: Auditory Forensic Marker Neutralization*

Towards this latter end of finding a betraying beep, we can perform a spectral analysis of a given film’s audio stream by mapping the audio track’s time (x-axis)/frequency (y-axis) distribution to produce a spectrogram—a visual depiction of the audio track—so as to be able to note any particular frequency aberrations which could denote the presence of a possible forensic modulation of the audio stream. Refer to Appendix 3: ‘Sample Procedure for Cinematic Auditory Forensic Watermark Neutralization’ for a step-by-step enumeration of the workflow discussed herein for neutralizing watermarked audio and thusly rendering it suitable for later anonymous distribution (following successful subsequent removal of visual forensic markers as well, of course).

The initial step is acquiring a liberated or ‘cammed’ film audio track. This can be achieved via a variety of methods, for instance: via the use of a camcorder’s built-in microphone, the use of a higher quality external microphone, recording the audio from an Assisted Listening Device, or directly from the audio rack in the projection room. Note that this list is presented in order of increasing access control and thus of increased difficulty of access, and is likewise directly proportional to the resultant fidelity of the recording. For instance, it would be easier to utilize the camcorder’s built-in microphone rather than bringing in an additional external microphone, as the chances of a cinema warden noticing the added equipment is greater the more and larger equipment there is. However, the external microphone may produce a better quality audio recording than the built-in microphone. Similarly, recording the audio directly from an Assisted Listening Device would likely produce a still better quality recording, but access to said device would need to be negotiated with the theater staff. Finally, recording the audio directly from the line feed in the projection booth would produce the highest quality audio, but would also necessitate gaining entry into

---

<sup>439</sup> Barthes, *op. cit.* p. 347.

a restricted area (thus potentially requiring the collusion of the projectionist, assuming here that the projectionist is a different party than the recorder).

Following the successful procurement of a film's audio track, the first operative step becomes to separate or demux the audio stream (which may otherwise be packed inside a container such as an AVI file, which holds both the audio and video streams of the film) so as to render it palatable to individual analysis. If the audio is already a separate file, then of course this step can be bypassed, depending on whether or not the camcorder or other recording device provides separate audio/video files. The extraction can be achieved using any number of freely available video and audio editing tools. For our purposes we will make use of Avidemux, "[a] free multi-format, cross-platform video editor designed for simple cutting, filtering and encoding tasks"<sup>440</sup>. Upon loading the target video file into the program, we can then proceed to export the audio track in its native format (for instance, either a compressed MP3 or uncompressed WAV file). Upon successful extraction of the audio track, we then proceed to use, once again, any number of freely available audio analysis tools, for instance Raven Lite, a "free software program that lets users record, save, and visualize sounds as spectrograms and waveforms"<sup>441</sup>, to conduct a spectral analysis of the film's audio stream, producing a spectrogram for the entire duration of the audio track.

Spectral depictions of human speech tend to fluctuate by various frequencies over time, thus, conversely, perfectly static frequencies over a period of time could denote non-human speech. Said non-human speech may be a musical interlude in the film, bird calls, or auditory forensic markers. Thus the presence of any regular rectangular formations in the spectrogram over a period of time may warrant close scrutiny. The audio track can be played in any audio player of choice<sup>442</sup> at the given suspect times to attempt to discern whether the suspect formation is indeed a potential watermark. Once it has been determined that the identified suspect blocks are probable watermarks, we can then proceed to run a low-pass filter over the audio stream, which allows the 'low' frequencies to pass unmodified, while greatly lowering the amplitude of frequencies above a specified cut-off range, thus decreasing and at times eliminating the occurrences of certain sounds from the audio track.

Using the GoldWave audio editing suite<sup>443</sup> we can gradually increase the steepness of the filter until traces of the watermark have been removed (the spectrogram of each iteration

---

<sup>440</sup> Mean. 2012. Avidemux. v. 2.6.0. <http://www.avidemux.org>.

<sup>441</sup> Bioacoustics Research Program, Cornell Lab of Ornithology. 2009. Raven Lite. v. 1.0 build 9 update 23. <http://www.birds.cornell.edu/brp/raven/RavenOverview.html>.

<sup>442</sup> VideoLAN Team. VLC media player. v. 2.0.8. <http://www.videolan.org>.

<sup>443</sup> Goldwave Inc. 2008. GoldWave. v. 5.25. <http://www.goldwave.com>.

can be examined and the audio can be listened to). Of course, the resultant attack may have the unwanted side-effect of slightly distorting the actual audio presentation of the film itself, though certainly not to the point of inaudibility. Thus the potential slight loss in quality is at this point a necessary remaining surgical scar, or battle wound, as it were. Once the audio has been suitably excised of the identifying forensic markers, we can then once again use Avidemux to re-combine, or remux, the new audio stream back with the video stream, producing a functioning liberated copy of the film.

Of course, it should be noted that the above attack methodology relies on only one copy of the film. If two or more copies can be obtained from two different locations, one could then perform a collusion attack in searching for the placement of the audio watermarks by viewing the two audio streams side by side and noticing any peculiar singularities that would not be explained by any potential background noise in the theater. Upon locating the potential watermarks within one of the audio streams, instead of relying on a low-pass filter to phase out the offending watermarks, one could then cut out the same fragments from the second copy of the audio stream, which would be free of watermarks at the same exact points, since it is precisely the presence of these points which formulates a unique audio forensic marker fingerprint, and then simply insert the ‘clean’ fragments into first stream. The net result would be a composite, watermark free audio stream born of the colluding of disparate audio sources. Indeed, if one has access to more than one copy of the liberated film, one may not even need to know the precise location of the watermarks, instead simply cutting and merging the two audio streams at set intervals which would have the effect of distorting any attempts by the watermark detection software to form a cohesive identifying serial number for the film.

### 3.3.1 Secondary Location Tracking [AFM, VFM; $L_2$ ]

Moving on to a comparatively recent (a paper outlining the functioning of secondary location tracking forensic markers was just published in late 2010, versus the earlier 2003 publication of  $L_1$ -based audio watermarking, or the even earlier development of  $L_1$  visual forensic markers in the 1980’s) development in the cinematic watermarking arena, we come to the secondary location tracking audio-visual forensic markers which aim to pinpoint the precise seat in which a film pirate was seated. When used in tandem with  $L_1$  forensic markers as well as the various aforementioned disciplinary modes of surveillant record-keeping,  $L_2$ -based forensic analysis could thus potentially lead to an exact identification of the jailbreaker involved in the liberation of a given film. Not content with merely knowing which theater a

film was liberated from, content owners demand knowledge of precisely *who* was responsible, “only identifying when and where the illegal recording happens is not sufficient to the original purpose of copyright protection and traitor tracing”<sup>444</sup>. ‘Traitor tracing’ is a curious industry term which simply means identifying the source of a leak, in our case the liberator responsible for freeing the film. It is not a term reserved exclusively for industry-insiders (despite the fact that insiders may be responsible for a majority percentage of film leaks<sup>445</sup>), and thus the nomenclature is here a bit misleading seeing as how no a priori allegiance to the industry of congealment, of content ownership, is necessarily presumed, and hence no actual betrayal need occur; though presumably the content owners like to delude themselves into thinking that all those who go to view their films are de facto subjects under the film industry’s sovereignty!

Secondary location-based visual forensic markers seek to identify the exact location of a film recorder within a theater based on a complex “camera projective geometry”<sup>446</sup> which identifies the position of a camcorder in the geometric grid of the theater space retroactively depending on the angle of recorded visual watermarks. Operating in a similar mode of retroactive identification, secondary location-based audio forensic markers strive to identify the precise location of a pirate by relying on multi-channel/multi-speaker surround-sound theater audio projection systems. Each audio channel from each speaker is injected with a unique audio watermark, with the combination of all of the recorded channels culminating at a set point in the theater which marks the location of the camcorder’s microphone based on a unique time-offset (or delay) fingerprint, or in other words “the signal from each loudspeaker is delayed in proportion to the distance from that loudspeaker to the microphone of the camcorder. Our main idea is to utilize these delays for the position estimation”<sup>447</sup>. Effectively, the once ostensibly innocent visitation room of the theater hall,

---

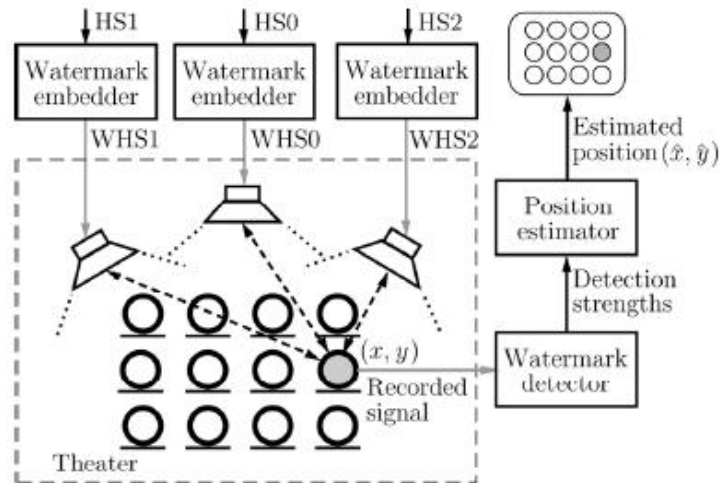
<sup>444</sup> Min-Jeong Lee, Kyung-Su Kim, and Heung-Kyu Lee. 2010. “Digital Cinema Watermarking for Estimating the Position of the Pirate”, in *IEEE Transactions on Multimedia* 12 (7). pp. 605-621 (p. 605).

<sup>445</sup> “We developed a data set of 312 popular movies and located one or more samples of 183 of these movies on file sharing networks, for a total of 285 movie samples. 77% of these samples appear to have been leaked by industry insiders” (Simon Byers, Lorrie Cranor, Dave Kormann, Patrick McDaniel, Eric Cronin. 2003. “Analysis of security vulnerabilities in the movie production and distribution process”, in *DRM '03 - Proceedings of the 3rd ACM Workshop on Digital Rights Management*. pp. 1-18 (p.1). <https://lorrie.cranor.org/pubs/drm03.html>). Insider-sources leaking of cultural products is not unique to the realm of film. For discussions of insider-sourced music industry leaks, see: Andrew Sockanathan. 2011. “Digital Desire and Recorded Music: OiNK, Mnemotechnics and the Private BitTorrent Architecture”. Doctoral thesis, Goldsmiths, University of London. [https://research.gold.ac.uk/6569/1/CCS\\_thesis\\_Sockanathan\\_2011.pdf](https://research.gold.ac.uk/6569/1/CCS_thesis_Sockanathan_2011.pdf).

<sup>446</sup> Lee, et al., *op. cit.*, p. 610.

<sup>447</sup> Yuta Nakashima, Ryuki Tachibana, Noboru Babaguchi. 2009. “Watermarked Movie Soundtrack Finds the Position of the Camcorder in a Theater”, in *IEEE Transactions on Multimedia* 11 (3). pp. 443-454 (p. 444).

now becomes complicit in the identification of the exact location of the camcorder and presumably its accompanying film liberator. Thus “the different control mechanisms are inseparable variations, forming a system of variable geometry the language of which is numerical”<sup>448</sup>, allowing content controllers to forensically determine that, say, the film pirate was sitting precisely  $n$  meters away from the second-right speaker. As can be seen in Figure 3.1, the theater space thus becomes a grid of identification leading to a subsequent neutralization. A forensic striation with only one purpose: that of entrapment.



**Figure 3.1** Secondary location-based audio watermarking schema<sup>449</sup>.

And yet paradoxically, it is precisely this geometric overdeterminism, which while at first glance seemingly freezing the film liberator at a locked-in set of coordinates, ready to be turned over to the authorities, may in actuality afford us the wiggle room of once again avoiding detection. Or in other words, a laser-focused beam is much easier avoided than a roving searchlight. I was however, unable to find samples of the secondary location-based watermarking systems being deployed in films in the wild, and thus while the following attack methodology is thus necessarily experimental, it is nonetheless based on the flaws inherent in the primary research documentation which describes the workings of said watermarking technique. Towards this end, it must first of all be noted that, as with the aforementioned soundtrack modulation watermarking, while the end-goal is one of transparency and detection avoidance, the actual documentation nonetheless hedges and states that “the results of our MUSHRA subjective listening tests show the method does not

<sup>448</sup> Deleuze, *op. cit.*

<sup>449</sup> Diagram from: Nakashima, et al., *op. cit.*



significantly spoil the subjective acoustic quality of the soundtrack”<sup>450</sup>. Unlike the previously discussed A/B test, the MUSHRA test is meant to gauge the overall subjective quality of the audio track, rather than note any salient differences between two sample tracks. Nonetheless, the fact that the very injection of the L<sub>2</sub> auditory forensic marker into the film’s audio streams produces an audible distinct track, albeit one that presumably “does not significantly spoil” (with ‘significantly spoil’ being undefined) the quality of the overall soundtrack, in turn signifies that there exists a noticeable differentiation, and thus an initial probing could employ the same attack vectors as those discussed in the above section on [AFM; L<sub>1</sub>], namely by both listening to the [AFM; L<sub>2</sub>] watermarked track to see if any possible injection suspects can be isolated freehand, and further substantiating this initial analysis with a more detailed spectral sonogram approach.

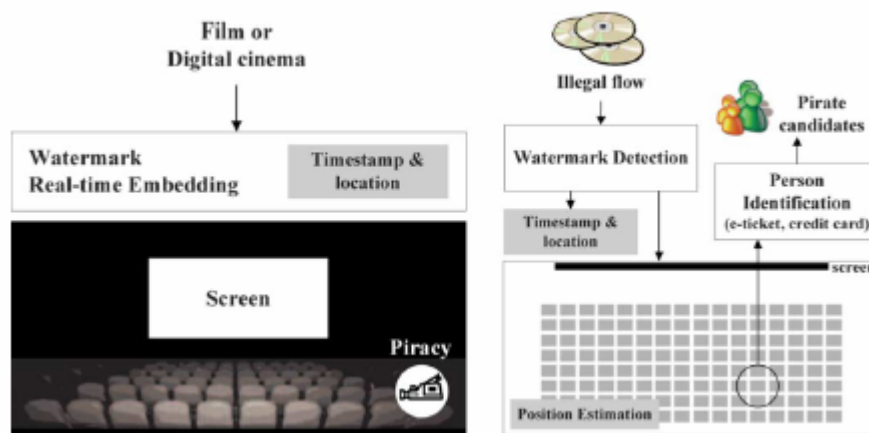
However, aside from incorporating the same attacks as those used for [AFM; L<sub>1</sub>], we can once again return to the problem of overdetermination so as to exploit opening within the existent variable geometry of control. Namely, L<sub>2</sub> watermarking systems are predicated on an identical continuity throughout the duration of the film; that is to say, the schemas assume that the pirate remains stationary within the confines of the same seat for the whole showing. If one were then to move throughout the film, it would potentially be possible to foil forensic analysis by failing to predict a stationary location. Aside from subsequent movement within the actual theater hall however, L<sub>2</sub> systems place an even greater emphasis—and thus dependence—on the initial mode of movement *into* the multiplex in the first place. For the successful identification of the ticket holder is predicated upon a traceable transaction, with the L<sub>2</sub> systems in fact automatically designed to scan through individually identifiable ticket purchases, within [VFM; L<sub>2</sub>], “the extracted information from the embedded watermark determines when and where the pirate is made [sic], and also it helps to match the persons who illegally recorded a movie to the databases stored in the electronic ticket offices or in payment system”<sup>451</sup>, and similarly [AFM; L<sub>2</sub>] includes “a person identification system [which] identifies the pirate by making correspondence between the seat and the person who was on the seat. A ticketing system or a video surveillance system may be used as the person identification system”<sup>452</sup>. The very diagrams in the pertinent literature in fact further betray the almost total ultimate dependency on the traceability of the initial ticket purchase:

---

<sup>450</sup> *Ibid.*, p. 443.

<sup>451</sup> Lee, et al., *op. cit.*

<sup>452</sup> Nakashima, et al., *op. cit.*



**Figure 3.2** Position estimation through secondary location-based visual watermarking<sup>453</sup>.

In order to produce a suitable list of ‘pirate candidates’, said ‘candidates’ must have acquired access to the theater through a traceable e-ticket or credit card purchase, and must furthermore not have subsequently changed seats, as discussed above, for indeed within this watermarking schema individuals are mere *dividuals*, with the movie-goers being reducible to data points, situated on a geometric grid correlated to seat numbers which are themselves in turn correlated to ticket numbers and their purchasing credit card numbers, thus being “samples, data, markets, or ‘banks’”<sup>454</sup>, with the whole watermarking system being dependent on a “numerical language of control made of codes”<sup>455</sup>, as governed by traitor tracing algorithms which seek to highlight rogue dividual coordinate pairs present in the theater’s seating grid at a given time. Thus not only is it the case that, as Williams—expanding upon Deleuze’s formulation of the dividual—points out, “[o]ur divisibility hence becomes the basis for our classifiability into salient, useful, and even profitable categories for the businesses and government agencies that manipulate the data”<sup>456</sup>, divisible formation further renders the individual susceptible to forensic identification and subsequent legal apprehension, and thus vulnerability and punishment is seen to here be explicitly predicated upon dividuality as well.

Aside from the obvious attack vector of purchasing the ticket with cash, one could of course not purchase a ticket at all, and thus avoid all possible ticket-based detection. Towards this end there exist entire manuals<sup>457</sup>, which outline techniques of gaining admittance into the multiplex prison compound without payments; for instance, by proceeding to enter through

<sup>453</sup> Diagram from: Lee, et al., *op. cit.*, p. 605.

<sup>454</sup> Deleuze, *op. cit.*

<sup>455</sup> *Ibid.*

<sup>456</sup> Robert W. Williams. 2005. “Politics and Self in the Age of Digital Re(produ)cibility”, in *Fast Capitalism* 1 (1). [https://www.uta.edu/huma/agger/fastcapitalism/1\\_1/williams.html](https://www.uta.edu/huma/agger/fastcapitalism/1_1/williams.html).

<sup>457</sup> Dan Zamudio. 1995. *How to Sneak into the Movies*. Port Townsend, WA: Breakout Productions.

the designated exit in the midst of a parting crowd from a previous showing. Alternatively, one could purchase a ticket for one showing, an intentional decoy as it were, and then proceed to go to the theater hall showing the film targeted for liberation instead. Whilst the presence of CCTV identification in-sync with the  $L_2$  watermarking would still be possible, though by no means as certain as e-ticket or credit card-based identification, the risk could be minimized by alternating which multiplexes one frequents, as well as by donning any number of potentially suitable disguises<sup>458</sup>. And thus any number of decidedly low-tech counter-forensic techniques may be employed to foil superlatively more nuanced high-tech modes of control and surveillance.

### 3.3.2 Primary Location Tracking [VFM; $L_1$ ]

Primary location-based visual forensic marking, otherwise known as Coded Anti Piracy (CAP) (having been given nicknames such as CRAP dots or digital measles by those who have encountered them<sup>459</sup>), is a form of forensic marking which embeds small dots arranged in unique patterns at various times throughout the film print. Each CAP-infused film print distributed to each theater thus has a unique amalgamation of dots, allowing the governing watermark detection algorithm to scan through a camcorded copy of a film and, based on the unique arrangement of the dots, determine where (and some instances, when) the film was recorded. CAP codes thus form a visual equivalent of a unique serial number being embedded in each film print. If it is then noted that a high preponderance of cammed copies of films come from a certain theater, more security measures may be implemented to attempt apprehend the cammer. If, for instance, based on the CAP codes in films *X*, *Y*, and *Z*, it is discovered that all three films were recorded at *A* cinema, ticket purchasing records may be used to determine if there was, perhaps, only one person who bought tickets to all three films, and so on. Thus, CAP codes facilitate the instigation of further investigation by providing the primary location details of letting content enforcers know where to start looking for film liberators.

According to John P. Pytlak, a Senior Technical Specialist at Eastman Kodak who was on the initial team that developed the CAP coding, posting on the TKColorist Internet Group mailing list, CAP-based watermarking was developed by Kodak at behest of the MPAA in the early 1980s.

---

<sup>458</sup> Edmond A. MacInaugh. 1984. *Disguise Techniques: Fool All of the People Some of the Time*. Boulder, CO: Paladin Press.

<sup>459</sup> As discussed on an anonymous forum. [http://\\*](http://*). Note also that while, technically recent dot-shaped visual forensic markers are not the original CAP code, they are at times referred to as such (e.g., Sean P. Means. 2003. "Movies: Arrrgh, there be pirates in movie theaters -- but even more inside Hollywood", in *The Salt Lake Tribune*. <http://www.sltrib.com/2003/nov/11022003/arts/107311.asp>), thus signifying that CAP code has become a generic name; though this section will at times refer to them alternatively as 'CAP-like', any reference to CAP following the historical introduction should be taken to refer to the broader variety of cinematic dot-based visual forensic markers.

The first film to use CAP markings was *Night Crossing*, released in 1982. Pytlak goes on to state that “many HUNDREDS” of films since then have had the codes embedded in their film prints<sup>460</sup>. Following the initial development of the CAP codes, a number of patents have continuously been filed which add modifications to the original schema, which seek to improve upon elements of the original CAP codes, such as targeted—as opposed to randomized—dot placement in areas of the frame where there’s a higher chance of the dots surviving video compression, or making the dots themselves more prominent so as to better survive video compression and re-encoding techniques used when camming and uploading the film<sup>461</sup>. Kodak themselves, in the mean time, have moved on to developing digital, as opposite to film stock, watermarks<sup>462</sup>. Though CAP-inspired visual forensic markers can thus be seen to continue to be developed and refined, their underlying modus operandi remains more or less the same: CAP and CAP-like watermarking schemas all seek to embed visual markers (typically dots, though some variations call for blocks or dashes) in various frames of each unique theatrical print of a film distributed to each theater. Once the CAP codes are read and reconstituted by the detection algorithm, the result is a uniquely identifying serial number tied to a particular print, which is in turn tied to a specific theater during a set distribution window.

In other words, CAP operates through an exhaustive parceling of the film by dividing the film print into scenes, then further delineating several sequences within each scene, and finally selecting individual frames within each sequence upon which to graft the CAP code formation. Thus [VFM; L<sub>1</sub>] CAP watermarking operates as “an abstract machine of overcoding: it defines a rigid segmentarity, a macrosegmentarity, because it produces or rather reproduces segments, opposing them two by two, making all the centers resonate, and laying out a divisible, homogenous space striated in all directions”<sup>463</sup>. And yet this compartmentalization must of course not be misconstrued as precluding the possibility of centralization, in the sense that there certainly exists a centralized database in the hands of the content controllers which holds the resultant serial numbers of each unique film print. The rigid segmentarity manifests itself via the forced cleaving of the film’s body into select frames selected frames (chosen for their resiliency

---

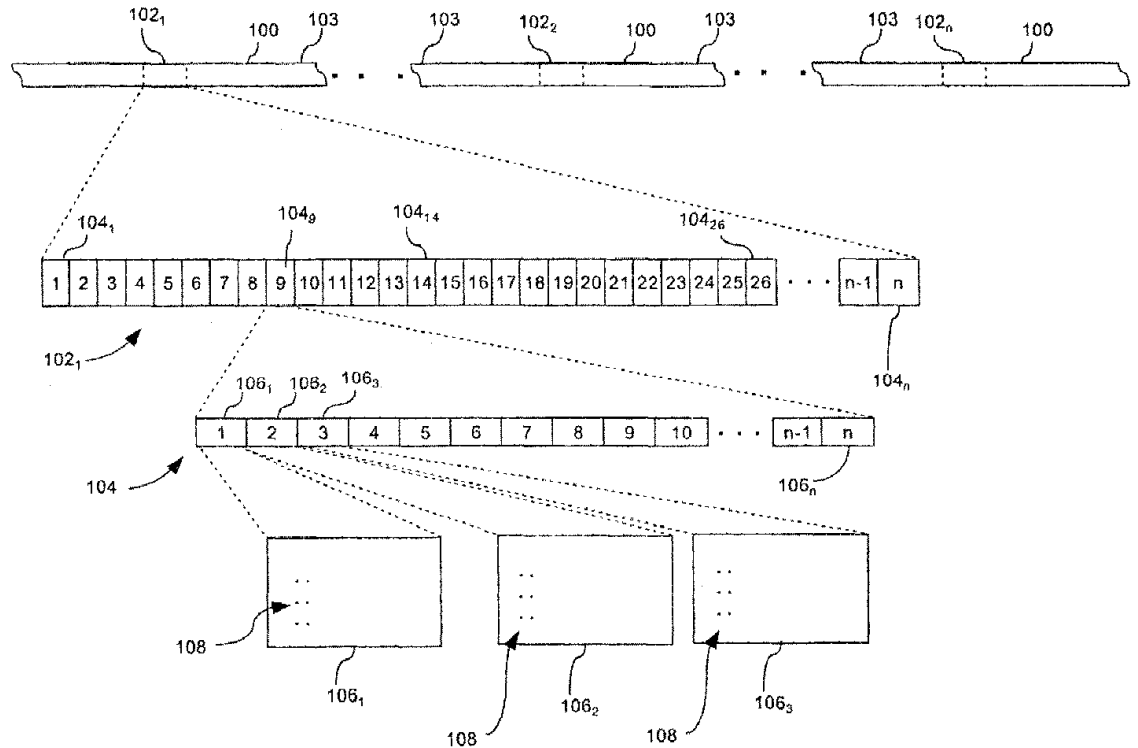
<sup>460</sup> John P. Pytlak. 2003. “Anti-Piracy Coding”. TKColorist Internet Group. <https://tig.colorist.org/pipermail/tig/2003-November/003836.html>.

<sup>461</sup> See, e.g., James E. Roddy, Robert J. Zolla, Leslie Gutierrez. 2005. “Method and Apparatus for Watermarking Film”. Patent No.: US6882356B2; David Jay Duffield, Mark Alan Schultz, Michael Allan Sterling. 2006. “Theater Identification System Utilizing Identifiers Projected onto a Screen”. Patent No.: US20060262280A1; Darcy Antonellis, Jeffrey J. Bartley, Margit Elisabeth Elo, Jean Pierre Gagnon, William B. Hogue, Jr., Edward J. Price. 2007. “Motion Picture Anti-Piracy Coding”. Patent No.: US7206409B2; Ion Vizireanu, Yousef Wasef Nijim, Mike Arthur Derrenberge. 2012. “System and Method for Analyzing and Marking Film”. Patent No.: US8090145B2.

<sup>462</sup> Kodak. 2001. “Invisible Watermarking for Digital Cinema”. *Kodak Research and Development*. <http://www.kodak.com/country/US/en/corp/researchDevelopment/productFeatures/cinema.shtml>.

<sup>463</sup> Deleuze and Guattari, *op. cit.*, p. 223.

in high-compression encoding environments), upon which the specific CAP formation is then branded. Refer to Figure 3.3 for a visual depiction of the resultant segmentarity, as seen directly from a visual forensic watermarking patent jointly filed by Technicolor and Warner Bros. Entertainment.



**Figure 3.3** Macrosegmentarity imposed on film print by a visual forensic watermarking schema<sup>464</sup>.

In thinking back to our earlier comparative example of *Theresienstadt* and MPAA anti-piracy propaganda reels, one once again notices an unsettling similarity to the treatment of bodies in the concentration camp and those in the multiplex. Concentration camp inmates were assigned, and eventually tattooed with, a five-digit Hollerith Code (so named after its eponymous creator, whose company eventually merged into IBM):

this five-digit number would follow the Polish merchant from labor assignment to assignment as Hollerith systems tracked him and his availability for work, and reported it to the central inmate file [...] Later in the summer of 1943, the timber merchant's same five-digit Hollerith number, 44673, was tattooed on his forearm. Eventually, during the summer of 1943, all non-Germans at Auschwitz were similarly tattooed<sup>465</sup>.

<sup>464</sup> Diagram from: Antonellis et al., *op. cit.* p. 1.

<sup>465</sup> Edwin Black. 2008. *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation*. US: Dialog Press. p. 356.



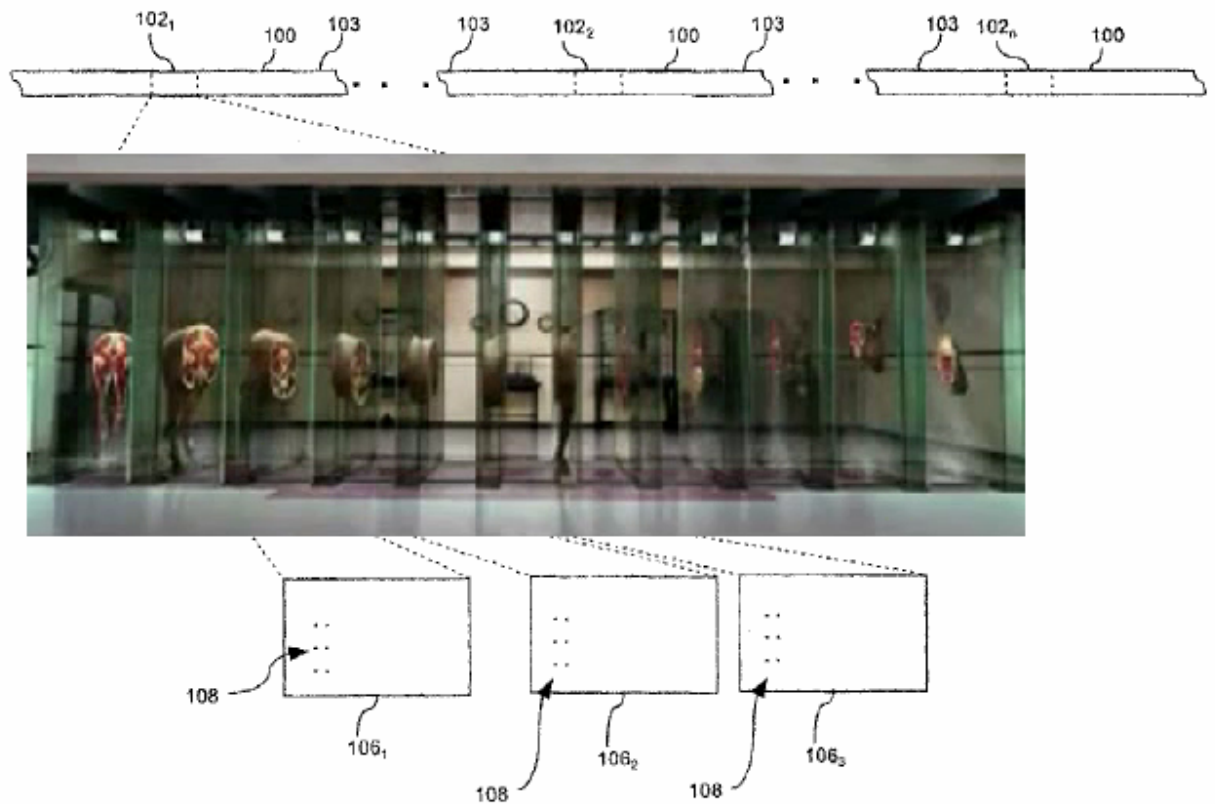
**Figure 3.4** Example of CAP-like visual watermarking<sup>466</sup>.

Likewise, more and more films are being tattooed with the dotted CAP code (as seen in Figure 3.4, above), which allows the movement of the film to be continuously tracked by a centralized database at the hands of the content owners. One is reminded of a scene in *The Cell* (2003), wherein a living horse is forcibly sliced into windowed partitions, and thus “we are entering into an era of films which no longer have meaning properly speaking, large synthetic machines with variable geometry”<sup>467</sup>. Figure 3.5 depicts a segmented horse overlaid atop the watermarking compartmentalization schema so as to highlight the visceral corporeality of the act. The film’s body being reduced to a variable geometry based upon algorithmic segmentation and augmentation to foster identification and subsequent traitor neutralization.

---

<sup>466</sup> Unknown film. Watermarked film frame sample courtesy of [anonymous]. Refer to Appendix 4: ‘Examples of Cinematic Visual Forensic Watermarks in Select Film Frames’ for additional examples.

<sup>467</sup> Jean Baudrillard. 1987. “The Evil Demon of Images”, *op. cit.*, p. 32.



**Figure 3.5** Explication of visual forensic marker segmentation via horse overlay<sup>468</sup>.

Not only is the visitation room, the seating array of the theater hall, subjected to the variable geometry of the various  $L_2$  watermarking schemas, but so too is the film itself now relegated to a fleshy array of segmented components by which its potential escape is to be monitored and those aiding and abetting to be prosecuted.

### 3.3.2.0 Case Study 5: Emancipato-Surgical Operation for Visual Forensic Marker Excision

Luckily for the films and their liberators, but not so much for the content controllers (recall that the difference between a program and an antiprogram is merely a matter of perspectivism), tattooing is in fact a negatable process: tattoos, and indeed watermarks, can be excised from the body. The initial problem is one of identification. As with the other cinematic watermarking methodologies we have thus far considered, CAP-based watermarking is intended to be imperceptible to even the ‘critical’ viewer, only presumably being detectable by specialized detection software operating via a specific watermark-identification algorithm. However, the forensic markers nonetheless *are* in fact plainly visible to the casual, let alone the critical, observer; as evinced by the simple fact that there are now more

<sup>468</sup> Diagram from: Antonellis et al., *op. cit.*; overlaid horse image from *The Cell*.

and more articles as well as blog and forum posts complaining about said watermarks<sup>469</sup>. Film cammers have also taken notice, with a scene notice in 2007 alerting cammers about their presence: “[t]he MPAA is going the opposite route that the RIAA is going and is going to catch us all with our pants down. Take a look at the jpg's I captured [...] Kinda strange to be seeing those dots huh? I went to see it again in the theater - same dots in different locations in the movie”<sup>470</sup>. Thus, as with previous watermarking methods, a freehand analysis may be sufficient in detecting the presence and location of the CAP/CAP-like visual markers.

Further helpful hints for detecting said markers may be obtained from the available technical literature. For instance, one patent advises that “the motion picture scenes can also be selected by identifying portions of the motion picture that have density, lighting and/or coloration characteristics that enhance the visibility of the marking pattern”<sup>471</sup>. In other words, scenes shot against either a clear or uniformly cloudy sky, or those which otherwise have so-called ‘high contrast’ backgrounds make ideal positions for watermarking, and thus warrant greater scrutiny than, say, scenes shot in a dingy unlit cave or during scenes of rapid movement such as raging forest fires. The mandated necessity of a bright, static background upon which the CAP dots are best placed can indeed help us narrow the search, especially when combined with other noticeable patterns. For instance, while five of the ten sampled watermarked frames which were analyzed appeared to have randomized ‘scattershot’ patterns, two had CAP-like dot arrays appearing in a noticeable ‘T’ formation, one appeared in a discernable turned-L (‘**┐**’) array, and two appeared as hybrid linear-and-scattershot patterns. All ten appear in a muddy-orange colorization in clusters of around five or six dots. Refer to Appendix 4: ‘Examples of Cinematic Visual Forensic Watermarks in Select Film Frames’ for a full listing of sampled dot formations, collected from anonymously-supplied samples taken from various exhibited film prints. With all of this in mind, we can now proceed to formulate a precise four-pronged attack methodology (Dissection, Identification, Isolation and Excision, and Recombination) to attempt to strip the CAP-like dots from liberated films. Our counter-forensic dissection is a surgical procedure, necessitating heavy operating upon the film’s body to excise the malignant cells.

Refer to Appendix 5: ‘Sample Emancipato-Surgical Operation for Visual Forensic Marker Excision’ for a sample illustrated and annotated workflow for removing CAP-like video-

---

<sup>469</sup> See, e.g., Roger Ebert. 2003. “Dots on film designed to track pirated movies are a nuisance”, in *The Victoria Advocate* - October 5, 2003. p. 2D; Roger Ebert. 2003. “Big screen anti-piracy system continues to annoy audiences”, in *The Victoria Advocate* - October 26, 2003 p. 2D; alkemyst. 2003. “Red dots for anti-piracy getting out of hand?”. AnandTech Forums. <http://forums.anandtech.com/showthread.php?t=1171155>; Marty Langford. 2008. “Anti-Piracy measures becoming more intrusive...”. *MassLive*. [http://blog.masslive.com/screenwriting/2008/05/antipiracy\\_measures\\_becoming\\_m.html](http://blog.masslive.com/screenwriting/2008/05/antipiracy_measures_becoming_m.html).

<sup>470</sup> InR. 2007. “MPAA.DOTS.ALL.CAMMERS.READ-InR”. <http://scenenotice.org/details.php?id=977>.

<sup>471</sup> Antonellis et al., *op. cit.*



based forensic watermarks from a cammed video via the deployment of, as with the other case studies, a counter-forensic methodology.

Prior to undertaking the excision of watermarks, it is of course first necessary to obtain a CAM video. The camera can be wedged snugly in the gap formed between two seats in the row immediately in front of where the cammer is situated in the theater, thus producing a minimum of video disturbance, contrasted to simply holding the camcorder in one's hands. Alternatively, the camera may be clipped to the seat in front of the cammer by using a miniature tripod clip. If access to the projection booth can be negotiated, the camera can then be placed on a full tripod or balanced on a flat surface. Black electrical tape should also be placed over all camera light emissions (such as the red recording light and green power light) to minimize chances of detection and apprehension. The camera display panel(s) should likewise be shut, dimmed, turned off, or taped over as well. A coat or jacket should be brought into the theater to be draped over the forward seat should an usher walk into the theater. Once a CAM has thus successfully been procured, we can turn to the task at hand.

A feature-length film which is, after all, a motion picture, is generally composed of a touch over a hundred thousand individual frames (for instance a 90-minute film will consist of approximately 130,000 frames<sup>472</sup>), any set number of which may be marred by CAP-like code. The original CAP code called for the marking of 11 frames, while later implementations do not necessarily have a set amount<sup>473</sup>. Thus our first step will be to dissect the composed digital film file that has been liberated from a multiplex prison compound into its individual constituent frames. This can be achieved via opening the CAM video file in any number of freely available video editing tools. We'll be using Avidemux, which it will be recalled we already used once during our attack on soundtrack modulation watermarking [AFM; L<sub>1</sub>] to extract the audio stream, save for the fact that we will now be using it to extract all of the composing frames of the film as individual JPEG image files<sup>474</sup>.

Once we have used Avidemux to extract all of the frames as separate images, our next task is to identify the specific watermarked frames. For this we can use imgSeek<sup>475</sup>, which provides us with "open-source content-based image searching" wherein "the query can be expressed either as a rough sketch painted by the user or as another image you supply. The

---

<sup>472</sup> Assuming a constant framerate of 23.976 frames per second,  $23.976 * 60 * 90 = 129,470.4$ .

<sup>473</sup> Vizireanu et al, *op. cit.*, p.6.

<sup>474</sup> N.B. For the visual forensic marker counter-forensic methodology, we will need to use an older version of Avidemux (Mean. 2010. Avidemux. v. 2.5.6. <http://www.avidemux.org>), as the newer version used during our auditory forensic marking case study does not have whole-frame extraction features, as it utilizes a time-based, as opposed to frame-based, video processing technique.

<sup>475</sup> Ricardo Niederberger Cabral. 2005. imgSeek. v. 0.8.5. <http://www.imgseek.net/>.

searching algorithm makes use of multiresolution wavelet decomposition of the query and database images”<sup>476</sup>. Upon loading our folder of JPG image files extracted during our dissection processes with Avidemux in the initial step of our attack against visual forensic watermarking into imgSeek’s database, we can then either draw a pattern on the fly within the program or select a pre-drawn array of patterns according to which it will then match up all of the images in the given databases (in our case all of the component frames of the film) according to a probability percentage, with the highest matching images showing up first, and so on. We can create sample pattern template files using the patterns seen in Appendix 4 in a basic image editing program. Once a template is thus loaded into imgSeek, we can analyze the results. In our case, while the first, third, and fourth hits (with 13.14%, 11.69%, and 10.94% probability matches, respectively) correctly identify the watermarked frames, the second and from the fifth onward hits (with 12.72% and 10.69% probabilities, respectively) are negative matches, serving to highlight that as the patterns we are searching for are often quite small and variable, the CAP codes only taking up a small portion of each also highly variable frame, imgSeek may both miss a potentially watermarked frame as well as report unwatermarked frames incorrectly as being watermarked. Ergo we must once again, as we did during our counter-forensic analysis of soundtrack modulation, resort to a redundancy of consciousness by viewing all of the images ourselves to ascertain whether or not any of the remaining images (frames) still contain a CAP code-based watermark. Instead of flipping through over a hundred thousand images separately, we may at this point simply watch the film in a video player, paying attention to any suspect formations which may appear.

Following the successful identification of all watermarked cells, we then make note of the specific cell number (which Avidemux outputted to match the filename of each image, thus for instance the 504<sup>th</sup> frame will be saved as *filename000503.jpg*, since the first frame is saved as *filename000000.jpg*) and return to Avidemux to excise the offending frames. After navigating to the specific frame we simply delete it, and then navigate to the next and so on, until all traces of the visual forensic markers have been successfully excised from the body of the film.

In order to complete our surgical procedure, all that is left to do is to recombine the frames into a functioning video stream and to then mux in the watermark-neutralized audio stream (if not done so already), with the end result effectively being a cleaned film, presumably devoid of all traces of the CAP-like fetters it was previously shackled by. These relatively straightforward tasks can once again all be done from within Avidemux. It may however be the

---

<sup>476</sup> niederberger. 2013. “imgSeek - Intelligent Image Database”. <http://sourceforge.net/projects/imgseek/>.

case, though not covered in the pertinent literature, that the content controllers may then attempt to conduct a sort of anti-counter-forensics which attempts to reconstruct the location of the watermark by discovering the points in the newly formed video which appear to be missing the vital watermarked frames. If the content controller adversary knows the exact frame numbers at which the watermarks should be—an unlikely scenario given that frame count will likely be greatly altered during the camming of the video from the frame count of the theatrical broadcast, due to the varying framerate of the camcorder)—a previous or succeeding unwatermarked duplicate (or ‘dupe’) frame can be injected into the video file by picking the closest matching unwatermarked frame, selecting the start and end points to select said frame, and copying it in place of the watermarked frame. In which case instead of a mere excision, we may instead apply a blur-effect filter over the targeted frames so to blur out the watermark without having to remove the frames altogether. In lieu of using the dupe frame approach, one can also instead apply the blur-effect filter over the watermarked areas of the frame. The blur effect is a bit of a misnomer, as it does not merely blur a target area but uses background-matching of previous/prior frames to attempt the erasure all traces of the zone designated for removal (in our case, the region surrounding the forensic dot formations), with the end result being the successful removal of the CAP-like codes without either any dropped or duplicate frames.

Having thus now successfully liberated a film from both audio and visual forensic markers, the question to be addressed next becomes one of distribution. Namely, now that those responsible for liberating the film from the multiplex are shielded from prosecution, how are we to ensure that those who are involved in the actual online dissemination are likewise protected? Current filesharing systems which are in vogue, namely BitTorrent and various file-hosting sites, are inadequate distribution vectors as they do not provide any sort of inherent anonymity, though there are certainly various third-party measures one could employ, for instance the masking of the uploader’s Internet Protocol (IP) address via the use of an off-shore Virtual Private Network (VPN) connection or other proxy server which would likewise hide the personally identifiable IP address. However, what we are looking for is something which has privacy and anonymity built into the system by default. In other words a sort of virtual Tong, which Hakim Bey defined as “a mutual benefit society for people with a common interest which is illegal or dangerously marginal—hence, the necessary *secrecy*”<sup>477</sup>. To this end, in the next chapter we will turn towards an in-depth analysis of various existent darknets, decentralized, decrypted and anonymized

---

<sup>477</sup> Hakim Bey. 1992. *The Radio Sermonettes*. New York City, NY: The Libertarian Book Club. [http://hermetic.com/bey/radio\\_se.html](http://hermetic.com/bey/radio_se.html).

distribution networks, so as to critically interrogate their potentiality as vectors of unbridled data dissemination.

**4.**

**Ordnance the Third: Distributive  
Strategies for Data Liberation**

During our development of initial contraceptive strategies of data liberation, we postulated tactics for undoing the existence of Intellectual Property fetters themselves—the dismantling of copyright and copyleft via an extended exposition of their internal incongruities, complete with an exhibitively sample foray into unfettering academic ebooks and journal articles. We then moved on to the successive deployment of emancipato-surgical strategies of illustrating how IP-conjured Bodies of Work (BoWs) are in fact literally imprisoned in their particular confines via the practical example of cinematic film and the accompanying instructions for the liberation thereof through the precise surgical excision of audio-visual watermarks therefrom. Following our various field campaigns of content liberation we arrive at a state wherein we now have a sizable, mobilized array of unfettered content in the form of academic ebooks, journal articles, and films. The next question of import here now then becomes one of distribution of said content whilst assuring the safety of both the uploader and downloader of the content. In other words, whilst the focus in prior sections has been on the matter itself, the attention in Part IV is now shifted to an analysis of existent and emergent conduits for it. The issue of safety is borne of the existent legal climate which makes it unlawful to distribute IP-bound BoWs, thus necessitating clandestine operations to ensure the continued longevity of both up/downloaders and, in turn, successive unbridled distribution of content. That is to say, legality—being an infringement on the flow of content—is thus seen as that which is to be overcome so as to ascertain a study of legally unbridled data distribution.

#### **4.0 Islands in the Net**

Toward this end, we will now turn to a preliminary examination of a sampling of existent means of file sharing, highlighting the potential advantages, as well as pitfalls, of each operant file sharing system and protocol by utilizing a three-pronged measurement methodology. Specifically, a representative cross-section of various file sharing ecosystems will be examined via their specific constitution of the userland, serverland, and fileland arenas vis-à-vis the operational security and anonymity thereof. In other words, we will examine the extent to which various file sharing systems protect the users of said system, the underlying servers running said systems, and finally the files themselves.

The term userland, as employed herein, is slightly distinct from the traditional formulation which, as collated from various hacker terminologies in the *Jargon File*, is

presented as simply being “anywhere outside the kernel”<sup>478</sup>. The *Jargon File*, “a collection of slang terms used by various subcultures of computer hackers”<sup>479</sup> gathered predominantly from Usenet and other resources, was created in 1975 and continuously updated by any number of contributors, with the last revision being in 2003<sup>480</sup>. Described as a ‘poetics of forms’<sup>481</sup>, the ever-mutating *Jargon File* knowingly regards, and indeed constitutes, the formulation of a polymorphic hacker vernacular as “as a game to be played for conscious pleasure”<sup>482</sup>. Hence, it is in keeping in the spirit of the *File* to here present a variant or perhaps nuanced definition of userland.

As previously mentioned, traditionally userland has specifically, yet at the same time also therefore rather broadly, referred to any space in the operating system that was not within the system-critical land or space of the kernel, which handles interactions between software and the computer’s central processing unit. Instead of being allowed to interact directly with the kernel, userland code merely communicates with the various software installed on the particular operating system, with the user in turn interacting with said software code. For our purposes however, userland will refer not so much to the specific code space but rather to the underlying users themselves. Specifically, the userland component of our typology will examine how particular file sharing systems handle the security and anonymity of the users of said systems. The inhabitants of userland consist of uploaders and downloaders, though depending on the particular file system it should be noted that these are not only shifting and porous, but at times also simultaneous roles, with uploaders potentially ceasing to act solely as uploaders and becoming downloaders, or at other times functioning as uploaders and downloaders at the same time; thus all serving to form the fluid constituency of userland.

Serverland in turn is the hosting infrastructure of a particular file sharing system. This arena helps to explore questions pertaining to where and how the files which users upload and download are stored and accessed. The term has previously been used in the information security literature when describing a network geography which differentiates local-running

---

<sup>478</sup> Eric S. Raymond and Guy L. Steele Jr. (eds.). 2003. *The Jargon File*. Version 4.4.7. <http://www.catb.org/jargon/html/U/userland.html>.

<sup>479</sup> *Ibid.*, <http://www.catb.org/jargon/html/introduction.html>.

<sup>480</sup> *Ibid.*, <http://www.catb.org/jargon/html/revision-history.html>.

<sup>481</sup> Florian Cramer. 2003. “Exe.cut[up]able statements: the Insistence of Code”, in *Ars Electronica 2003 - Code - The Language of Our Time* (eds. Gerfried Stocker and Christine Schöpf). Linz: Hatje Cantz. pp. 98-103 (p. 102). [http://archive.aec.at/media/archive/2003/185088/File\\_04108\\_AEC\\_FE\\_2003.pdf](http://archive.aec.at/media/archive/2003/185088/File_04108_AEC_FE_2003.pdf).

<sup>482</sup> Raymond and Steele, *The Jargon File*, *op. cit.*, <http://www.catb.org/jargon/html/introduction.html>.

servers from the broader Internetland<sup>483</sup>. For our purposes, a modified orthogonal definition is deployed in which, while serverland refers to servers specifically related to the file sharing system, the servers are not themselves necessarily owned by the administrators of said system—instead serverland may be constituted by (re)appropriated public servers or via ad-hoc userland-provided resources. A file sharing system may thus be said to deploy remote servers in the service of its hosting infrastructure that would also fall within serverland under our operative classification schema.

Finally, having addressed the users and hosting of a file sharing system, we come to the eponymous files themselves. Fileland is the arena which examines the actual data coagulants existent within a file sharing ecosystem—amalgamations of informational clotting—often termed ‘files’<sup>484</sup>. File handling practices will here be examined with an eye towards security (e.g. encryption) and longevity (e.g. retention), the former of which protects the file from adversaries whilst the latter assures the existence of the protected file in the first place.

With an understanding that these various lands are subject to continual seismic shifts as evinced by, for instance, the on-going release of updated software versions which at times radically alter the previously delineated typology, we will now turn to an examination of different kinds of anonymity afforded over various layers (namely the transport and application layers), before moving onto an examination of four prominent file sharing systems—Usenet, Internet Relay Chat (IRC), Cyberlockers (or Direct Download (DDL) sites), and BitTorrent—as well as a mentioning of darknet systems, as introduced via Freenet, and further explicated by a foray into Tor’s Onionland in which a sample file sharing architecture will be established to test the possibility of increased \*land anonymity and security.

#### 4.0.0 Layer Anonymity

One way of discussing the various available anonymization options is to address how said anonymization measures impact the anonymity of a given layer, as opposed to the

---

<sup>483</sup> Nicklaus A. Giacobe and Sen Xu. 2011. “Geovisual Analytics for Cyber Security: Adopting the GeoViz Toolkit”, in *IEEE Symposium on Visual Analytics Science and Technology*, pp. 313-314 (p. 313). [https://svn.labri.fr/visu/InfoVis\\_2011/VisWeek2011\\_proceedings/vast/challenge/giacobe.pdf](https://svn.labri.fr/visu/InfoVis_2011/VisWeek2011_proceedings/vast/challenge/giacobe.pdf).

<sup>484</sup> Whilst technical literature tends to present attempts at neutral readings of the term (e.g. “a file is simply a sequence of characters” (Hans Petter Langtangen. 2009. *A Primer on Scientific Programming with Python*. New York: Springer. p. 274)), the nomenclature of describing delineated data allocations as files is of course itself tied to the vernacular of business practice, “the mind-numbing operations of office work and bureaucracy are built right into the foundations of the computer and its user interface” (Warren Sack. 2008. “Memory”, in *Software Studies - A Lexicon*, *op. cit.*, pp. 184-193 (p. 190)).



entirety of the system, thus subsequently allowing for the elucidation of how there may exist different anonymity measures which may be deployed in tandem for each layer. The concept of layering as, for instance, presented within the Open Systems Interconnection (OSI) communications model<sup>485</sup>, is a systems “structuring technique”<sup>486</sup> for grouping similar subsystem functionalities. Of particular interest for our analysis are the transport and application layers, the former focusing on end-to-end communications with a transport service “provid[ing] the means to establish, maintain, and release transport-connections”<sup>487</sup>, and the latter focusing on host (or application) communications, wherein “[a]pplication-processes exchange information by means of application-entities which use application-protocols and presentation services”<sup>488</sup>. The transport and application layers correspond to server and user interactions in or across networks, and thus roughly correspond to the previously delineated user- and serverland terminology. Additionally, the content layer (corresponding to the aforementioned fileland nomenclature), which may be defined as “the locus of information owned by various parties and accessed using communications”<sup>489</sup>, is of course also of concern as various anonymity factors may need to be taken into account when distributing particular filetypes; however, said content layer has already been addressed earlier in the research project when discussing various watermark and other content protection defanging techniques<sup>490</sup>.

*Transport Layer.* Within the communications transport layer, there are two primary transport protocols of interest to us, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)<sup>491</sup>. When striving to anonymize the transport layer, a tool to aid in TCP anonymization is the free Tor anonymity software<sup>492</sup>, which routes a user’s TCP/IP connections through a series of intermediary relays, before finally coming out of a distanced

---

<sup>485</sup> International Organization for Standardization. 1994. *ISO/IEC 7498-1:1994(E): Information Technology — Open Systems Interconnection — Basic Reference Model: The Basic Model*. International Organization for Standardization. [http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269\\_ISO\\_IEC\\_7498-1\\_1994\(E\).zip](http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip).

<sup>486</sup> Hubert Zimmermann. 1980. “OSI reference model—The ISO model of architecture for open systems interconnection.” *IEEE Transactions on Communications* (28.4). pp. 425-432 (p. 426).

<sup>487</sup> International Organization for Standardization, *op. cit.*, p. 37.

<sup>488</sup> *Ibid.*, p. 32.

<sup>489</sup> Hu Hanrahan. 2007. *Network Convergence: Services, Applications, Transport, and Operations Support*. West Sussex, England: John Wiley & Sons Ltd. p. 55.

<sup>490</sup> Refer to sections 1.4.2, 2.4, 3.3.0.0, and 3.3.2.0 of the Operations Manual for content layer anonymity analyses.

<sup>491</sup> R. Braden. 1989. “RFC 1122: Requirements for Internet Hosts -- Communication Layers”. Network Working Group/Internet Engineering Task Force. <https://tools.ietf.org/html/rfc1122>.

<sup>492</sup> Tor Project. <https://www.torproject.org/>.

exit node, thus successively masking the user's IP address<sup>493</sup>. Tor, originally developed by the US Navy for purposes of facilitating secure government communication, has since then been (re)appropriated as a community-developed project for the ensuring of online anonymity<sup>494</sup>. Aside from anonymizing web (HTTP/HTTPS) communications, Tor can further be stacked on top of other Internet-facing applications which use the TCP/IP protocol suite to further anonymize the user's connection to said services. Thus, for example, torrent or chat clients can be configured to run proxied TCP/IP connections through Tor, helping to ensure the protection of the user's IP address from anyone else in the particular torrent's swarm. Web browsers can similarly be configured to access the web via Tor (and in fact the default Tor install package is a 'browser bundle' which comes preconfigured with a portable browser optimized for anonymized Tor-based web navigation).

Not only can Tor facilitate anonymous connections-to Internet services, it can also be used to facilitate the anonymization of connections-from services via Tor's own operant darknet known as Tor's Onionland. The Onionland is a loose-knit network of Tor-routed Internet-facing servers configured to receive inbound Tor connections which are known as Tor hidden services. Upon setting up a Tor hidden service through the fine-tuning of Tor configuration files (namely by pointing the torrc file to, say, your own web server), one's hidden service becomes accessible through a .onion domain, which is in turn only accessible through the use of Tor<sup>495</sup>. Thus a website operating as a Tor hidden service may have the URL of, say, <http://dj839nduydow74.onion>, and would only be accessible through a browser configured to browse through Tor itself. The tangible benefit of such a setup is that both user and serverland IPs are now anonymized, in that server log files do not show user's personal IPs due to the fact that the users are accessing the service via Tor, and conversely users cannot determine the server's personal IP due to the fact that the server is likewise being tunneled through Tor. A sample Tor-based BitTorrent site and tracker will subsequently be established and discussed in section 4.2 of the Operations Manual.

As will be noted above, however, TCP is only one particular transport protocol operating within the transport layer. Filesharing applications may, however, deploy additional transport protocols such as User Datagram Protocol (UDP), which is for instance,

---

<sup>493</sup> Tor Project. "Tor: Overview". *Tor Project*. <https://www.torproject.org/about/overview>.

<sup>494</sup> *Ibid.*

<sup>495</sup> The Tor Project, Inc. 2011. Tor. v. 0.2.2.35. <https://www.torproject.org>; Tor Project. "Configuring Hidden Services for Tor". *Tor Project*. <https://www.torproject.org/docs/tor-hidden-service.html.en>.

utilized by BitTorrent<sup>496</sup>. As Tor only strives to anonymize Transport Control Protocol/Internet Protocol (TCP/IP) traffic, alternative anonymization options must be considered when addressing UDP traffic. One such alternative anonymization option is a Virtual Private Network (VPN) provider which offers UDP support<sup>497</sup>, though using a VPN service may in turn open the target up to a variety of other attacks<sup>498</sup>, such as an attacker exploiting the fact that some VPN providers may offer split-routing in which some services are not tunneled via the VPN, with an attacker potentially exploiting the existing gap in the routing table to make a given application connect to the attacker's service outside the VPN and reveal their non-VPN IP. Defined as "a temporary physical route formed over a mesh structured public network"<sup>499</sup>, a VPN provides "a secure, private network over a public network such as the Internet"<sup>500</sup>. Effectively, a user employing a VPN service connects to the VPN service and the VPN service subsequently connects to the Internet on behalf of the user and relays the traffic back to said user. The effect being that the user's personal (or, in the strict sense, the non-VPN) IP address is *ideally* masked from everyone aside from the VPN provider. Thus, as a VPN privacy guide point out, the key point of trust becomes the VPN provider<sup>501</sup>, with the pivotal question thus here being whether one trust the VPN provider to provide userland anonymity via transport layer anonymization (and, conversely, security against deanonymization)?

In attempting to provide a generic definition of trust in the sense of being domain-independent (as opposed to focusing on a specific field such as e-commerce) Grandison and Sloman describe it as "the firm belief in the competence of an entity to act dependably, securely and reliably within a specified context"<sup>502</sup>. Let us now turn to a sample trust

---

<sup>496</sup> Olaf van der Spek. 2008. "UDP Tracker Protocol for BitTorrent". BitTorrent.org. [http://www.bittorrent.org/beps/bep\\_0015.html](http://www.bittorrent.org/beps/bep_0015.html).

<sup>497</sup> See, e.g., AirVPN. 2014. "Why Us?". <https://airvpn.org/whyus/>. For a summative list of additional VPN providers which offer UDP support, see Ernesto. 2015. "Which VPN Services Take Your Anonymity Seriously? 2015 Edition". *TorrentFreak*. <https://torrentfreak.com/anonymous-vpn-service-provider-review-2015-150228/>.

<sup>498</sup> Jacob Appelbaum, Marsh Ray, Karl Koscher, Ian Funder. 2012. "vpwns: Virtual pwned networks". *2nd Workshop on Free and Open Communications on the Internet*. <https://www.usenix.org/system/files/conference/foci12/foci12-final8.pdf>.

<sup>499</sup> Gilbert Held. 2004. *Virtual Private Networking: A Construction, Operation and Utilization Guide*. West Sussex: John Wiley & Sons, Ltd. p. 1.

<sup>500</sup> Charlie Scott, Paul Wolfe, Mike Erwin. 1999. *Virtual Private Networks, Second Edition*. Sebastopol, CA: O'Reilly & Associates Inc. p. 6.

<sup>501</sup> Douglas Crawford. 2014. "The Ultimate Privacy Guide". *Best VPN*. <https://www.bestvpn.com/the-ultimate-privacy-guide/#vpn>.

<sup>502</sup> Tyrone Grandison and Morris Sloman. 2000. "A Survey of Trust in Internet Applications", in *IEEE Communications Surveys and Tutorials*. pp. 1-30 (p. 4).

[https://www.doc.ic.ac.uk/~mss/Papers/Trust\\_Survey.pdf](https://www.doc.ic.ac.uk/~mss/Papers/Trust_Survey.pdf). Notably, even following said paper, subsequent

management analysis via the case study of FrootVPN, selected due to its recent high-scale visibility in the torrenting scene. Given that VPNs are particularly popular amongst the BitTorrent ecosystem<sup>503</sup>, it is perhaps no surprise that when the front page of the Pirate Bay was for an amount of time changed from their standard logo to an advertisement for a VPN service entitled FrootVPN, said service subsequently saw an intake of 100,000 new subscribers, with the Pirate Bay staff claiming that it is not a paid advert, but merely a favor for some people they know<sup>504</sup>. With regard to dependability, early adopters reported favorable speeds<sup>505</sup> with the operators intending to add yet more bandwidth<sup>506</sup>. Whilst not specifically describing FrootVPN, it is nonetheless notable that in their analysis of 128 million peers, Le Blond et al. found that “peers using VPNs are usually very fast peers, and that VPNs do not dramatically decrease the performance of those peers.”<sup>507</sup>. In regard to reliability, FrootVPN’s website states that “[w]e will run this service for free as long as we can. But we will eventually need to bring money in to be able to pay our bills”<sup>508</sup>, thus forecasting that the free tier of the service is unreliable for long-term usage. Finally, coming to the security aspect of the aforementioned trust metric, FrootVPN makes the claim that they “don’t keep any logs of any kind. All we ask from you is your email address and username. No other information is kept on our servers”<sup>509</sup>, a claim which published reviews of the service repeat uncritically<sup>510</sup>. Whilst, as Cahill et al. point out, trust building is in part done via the “recommendations from partly trusted third parties”<sup>511</sup>, much as there is no evidence

---

research continues to trade in tautologies; e.g., “trust management, roughly speaking, refers to the management of the trustworthiness of relationships among entities” (Shuo Ma, Ouri Wolfson, Jie Lin. 2011. “A Survey on Trust Management for Intelligent Transportation System”, in *Proceedings of the 4th ACM SIGSPATIAL International Workshop on Computational Transportation Science*. pp. 1-6 (p. 1). <http://www.cs.uic.edu/~sma/Papers/trust.pdf>).

<sup>503</sup> Ernesto. 2013a. “BitTorrent Accounts for 35% of All Upload Traffic, VPNs are Booming”. *TorrentFreak*. <https://torrentfreak.com/bittorrent-accounts-for-35-of-all-upload-traffic-vpns-are-booming-130518/>.

<sup>504</sup> Ernesto. 2014b. “Pirate Bay Sends 100,000 New Users to ‘Free’ VPN”. *TorrentFreak*. <https://torrentfreak.com/pirate-bay-sends-100000-users-free-vpn-141024/>.

<sup>505</sup> mr-peabody. 2014. “FrootVPN?”. *Reddit*. <https://reddit.com/r/VPN/comments/2jzatj/frootvpn/>.

<sup>506</sup> Ernesto, “Pirate Bay Sends 100,000 New Users to ‘Free’ VPN”, *op. cit.*

<sup>507</sup> Stevens Le Blond, Arnaud Legout, Fabrice Le Fessant, Walid Dabbous. 2010. “Angling for Big Fish in BitTorrent”. INRIA Technical Report. pp. 1-13 (pp. 12-13). [https://hal.inria.fr/inria-00451282/PDF/bt\\_angling.pdf](https://hal.inria.fr/inria-00451282/PDF/bt_angling.pdf).

<sup>508</sup> FrootVPN. 2014. “FAQ for General”. *FrootVPN*. <https://www.frootvpn.com/faq/general-15.html>.

<sup>509</sup> *Ibid.*

<sup>510</sup> E.g., vpnreviewer. 2014. “FrootVPN Review”. *VPN Reviewer*. <https://vpnreviewer.com/frootvpn-review/>;

Paul Nash. 2014. “FrootVPN Review”. *VPN Creative*. <https://vpncreative.net/vpn-providers/frootvpn/>.

<sup>511</sup> Vinny Cahill, Elizabeth Gray, Jean-Marc Seigneur, Christian D. Jensen, Yong Chen, Brian Shand, Nathan Dimmock, Andy Twigg, and Jean Bacon, Colin English, Waleed Wagealla, Sotirios Terzis, and Paddy Nixon, Giovanna di Marzo Serugendo and Ciarán Bryce, Marco Carbone, Karl Krukow, Mogens Nielsen. 2003. “Using Trust for Secure Collaboration in Uncertain Environments”, in *Pervasive Computing* (July-September 2003). pp. 51-61 (p. 55).

to assign to FrootVPN the status of a trusted party, there is similarly no evidence upon which to assign a review website to the status of partly trusted third party either. Cahill et al. further introduce the notion of risk evaluation into trust calculation, in which “the risks of a trust-mediated action are decomposed by possible outcomes. Each outcome’s risk depends on the other principal’s trustworthiness (the likelihood) and the outcome’s intrinsic cost”<sup>512</sup>. Given that some VPNs have explicitly been shown to reveal user identities<sup>513</sup>, we can thus cumulatively deduce that the trust allocation given by users to VPN providers is not entirely risk free as users may incur the cost of deanonymization, and hence the userland security afforded to VPN-employing users can be said to be tenuous at best; especially when the fact that no trust verification or testing of a VPN’s claims to anonymity and privacy can effectively be performed is considered (as it would not be realistically possible to verify a VPN provider’s claims of various limited or nonexistent log-keeping practices). Thus the injunction to ‘use a VPN’ is no more secure than a similar one to ‘use Tor’; both would require precautionary strengthening measures to help mitigate potential de-anonymization vectors by making sure that the appropriate transport layer anonymization tool is used, and further that the given application which uses said tool is likewise securely set up, which in turn brings us to application layer-based anonymity considerations.

*Application Layer.* Whereas the transport layer addressed anonymization of the transport of end-to-end communications, the anonymization concerns in the application layer focus on strengthening a given application itself to not reveal potentially deanonymizing information about the user. Towards this end, we can now turn to an analysis of specific filesharing ecosystems, with an eye towards how we can deploy Tor and/or VPNs to work in tandem with given filesharing applications. Throughout this analysis, it is imperative to realize that both transport and application layer anonymity are of pivotal import and must operate in tandem to help assure user anonymity; as if only one layer is providing anonymity but the other layer is not, then user anonymity may be compromised in its entirety. For instance, if a BitTorrent application is configured correctly to connect via Tor, transport layer anonymity has been achieved; but if said application is also configured to transmit the user’s personal, non-anonymized IP, then even though the user’s IP is being sent anonymously (over the

---

<http://www.tara.tcd.ie/bitstream/handle/2262/27085/Using+trust+for+secure+collaboration+in+uncertain+environments.pdf?sequence=1>.

<sup>512</sup> *Ibid.*, p. 54.

<sup>513</sup> tracked6040. 2014. “I use VYPR VPN and just got a DCMA copyright notice”. *Reddit*. [https://reddit.com/r/VPN/comments/2bb0u1/i\\_use\\_vypr\\_vpn\\_and\\_just\\_got\\_a\\_dcma\\_copyright/](https://reddit.com/r/VPN/comments/2bb0u1/i_use_vypr_vpn_and_just_got_a_dcma_copyright/).

properly configured transport-layer anonymization tool, such as Tor), the application layer presents a point of failure in nonetheless relaying the user's true IP address (this particular case and additional examples of transport/application-layer anonymization desynchronization will be further discussed in section 4.2.1.2). To examine the potential interoperability between the transport and application layers, let us now then turn to an examination of four prominent file sharing systems—Usenet, Internet Relay Chat (IRC), Cyberlockers (or Direct Download (DDL) sites), and BitTorrent—as well as a mentioning of friend-to-friend (F2F) filesharing systems, through the sample examination of the Freenet ecosystem.

#### 4.0.1 Usenet

Developed in 1979, Usenet is perhaps the oldest still-utilized means of information sharing in general, and file sharing in particular. Whilst the first Bulletin Board System (BBS)—an alternate information and file sharing system—came online a year prior in 1978, they are no longer widely utilized today<sup>514</sup>, whereas Usenet has on the contrary seen a surge in usage in the 21<sup>st</sup> century<sup>515</sup>. Conceived of as an alternative to the Advanced Research Projects Agency Network (ARPANET), access to which was denied to universities which did not have Department of Defense contracts<sup>516</sup>, Usenet initially allowed the free exchange of only textual information. 1988 saw the creation of alternative or 'alt.\*' newsgroups, specifically alt.sex, alt.drugs, and alt.rock-n-roll. As Wang notes,

the creation of these three 'alternative' newsgroups sparked the beginning of anarchy within the previously tame world of newsgroups. Unlike the traditional newsgroups, which offer academic or friendly discussions, many alternative newsgroups skirt the boundaries of the law, letting people swap everything from copyrighted audio and video files to live viruses and hacking tools<sup>517</sup>.

Thus it can here be seen that the introduction of illegalism into Usenet discussion groups paved the way for facilitating data piracy via unbridled information sharing. Though, as previously mentioned, Usenet was initially a text-only medium (prior to the employment of binary-to-text encoding techniques that would allow the sharing of binary files), it is notable

---

<sup>514</sup> BBS Corner. 2009. "A Brief History of BBS Systems". *The BBS Corner*.

<http://www.bbcorner.com/usersinfo/bbshistory.htm>.

<sup>515</sup> Edward Henigin. 2009. "Up and to the Right: The Recent History of the Global Usenet Feed", in *North American Network Operators' Group (NANOG) 46*.

[https://www.nanog.org/meetings/nanog46/presentations/Wednesday/Henigin\\_light\\_N46.pdf](https://www.nanog.org/meetings/nanog46/presentations/Wednesday/Henigin_light_N46.pdf).

<sup>516</sup> Bryan Pfaffenberger. 2003. "'A Standing Wave in the Web of Our Communications': Usenet and the Socio-Technical Construction of Cyberspace Values", in *From Usenet to CoWebs: Interacting with Social Information Spaces* (eds. Christopher Lueg and Danyel Fisher). London: Springer-Verlag. pp. 20-43 (p. 22).

<sup>517</sup> Wang, *op. cit.*, pp. 41-42.

to highlight that this content restriction did not hinder Usenet's ability to act as an unbridled distributive vector for liberated content. For instance, William Gibon's *Agrippa*, an ephemeral text initially sold for values ranging from \$450 to \$7500 as a book-on-disk which would self-erase after one initial viewing<sup>518</sup>, appeared transcribed on the Usenet alt.cyberpunks group three days after its initial public reading<sup>519</sup>, though it had previously also been posted on a BBS the day after the reading<sup>520</sup>. Hence, being an ostensibly text-only communication system did not preclude Usenet from being a conduit for illicit file sharing.

Though throughout the 1980s and 90s the uuencode system was used to encode binary (non-text) files into text for sharing over the application layer Network News Transfer Protocol (NNTP)<sup>521</sup>, 2001 saw the introduction of the yEncode (yEnc) binary-to-text encoding system into the Usenet ecosystem<sup>522</sup>. Described as "a quick and dirty encoding for binaries"<sup>523</sup>, yEnc was a more efficient conversion system with less overhead with the resulting text-converted data only being up to 2% larger than the original binary size of the file. yEnc is explicitly highlighted by Fellows as a driving factor making "newsgroups a much improved functional alternative to P2P networks, especially for the distribution of large or very large files, or those which consist of illegal material"<sup>524</sup>, with Kim et al. similarly stating that "NNTP is used by some as a high performance alternative to traditional P2P file sharing options such as eDonkey or BitTorrent"<sup>525</sup> and Roettgers referring to Usenet as "the original piracy hotbed"<sup>526</sup>. Thus despite initially being a text-only medium, Usenet is now fully capable of aiding in the distributive of binary data as well.

Whilst filetype exclusionism has thus been shown not to be a salient issue affecting Usenet, in the sense that sharing is not limited to text-only files but encompasses binary data

---

<sup>518</sup> Tim Oerting (ed.). 1993. "Agrippa: A Book of the Dead", in *The Unofficial FAQ for alt.cyberpunk*. [https://cdn.preterhuman.net/texts/computer\\_culture/ACY01011.TXT](https://cdn.preterhuman.net/texts/computer_culture/ACY01011.TXT).

<sup>519</sup> Mr. PIEaSanT. 1992. "AGRIPPA". *alt.cyberpunk*. <https://groups.google.com/d/msg/alt.cyberpunk/-AFN4yB0TkQ/RVjgqTmarpUJ>.

<sup>520</sup> Matthew G. Kirschenbaum. 2008. *Mechanisms: New Media and the Forensic Imagination*. London: The MIT Press. pp. 218-219.

<sup>521</sup> Harley Hahn. 2014b. "How Binary Files Are Handled", in *Harley Hahn's Usenet Tutorial*. <http://www.harley.com/usenet/usenet-tutorial/how-binary-files-are-handled.html>.

<sup>522</sup> Juergen Helbing. 2002. "yEncode - A quick and dirty encoding for binaries". Version 1.3. <http://www.yenc.org/yenc-draft.1.3.txt>.

<sup>523</sup> *Ibid.*

<sup>524</sup> G. Fellows. 2006. "Newsgroups reborn - The binary posting renaissance", in *Digital Investigation 3* (2). pp. 73-78 (p. 74).

<sup>525</sup> Juhoon Kim, Fabian Schneider, Bernhard Ager, Anja Feldmann. 2010. "Today's Usenet Usage: NNTP Traffic Characterization", in *INFOCOM IEEE Conference on Computer Communications Workshops*. pp. 1-6 (p. 1). [https://www.net.t-labs.tu-berlin.de/teaching/ss10/IM\\_seminar/pdf/KSAF-TUUCNNTP-10.pdf](https://www.net.t-labs.tu-berlin.de/teaching/ss10/IM_seminar/pdf/KSAF-TUUCNNTP-10.pdf).

<sup>526</sup> Janko Roettgers. 2007. "Usenet, the Original Piracy Hotbed". *Gigaom*. <https://gigaom.com/2007/06/02/usenet/>.

as well, there is nonetheless another factor to consider in regard to fileland: that of data retention. Usenet news server providers have what is known as a retention period, the time after initial uploading that a file is available for access on the server prior to deletion (so as to make room for newly uploaded material due to finite storage resources). For instance, the Giganews news server provider currently offers “the world's longest Usenet retention with over 110,000 newsgroups. We deliver a world leading 2280 days of binary retention and more than 8.5 years of text retention”<sup>527</sup>, meaning that retention periods effectively constitute death clocks, upon the expiration of which content that was uploaded more than 6.2 years ago will no longer be available for downloading. Retention periods, however, are continuously rising, as evinced by comparing older versions of Giganews’ marketing material<sup>528</sup>. The Usenet ecosystem further allows for what is known as reposting, or reuploading content that is outside the retention span of news servers by users who had previously downloaded it or made a new encode of the files in question (for instance, by converting the same audio disc to a new digital file).

Shifting towards the serverland arena, the question of accessibility to the news servers themselves crops up. Early piracy manuals noted that Internet Service Providers generally provided Usenet access bundled with a standard Internet access package<sup>529</sup>. However, mid-2008 saw the cancellation of Usenet access by various large American ISPs under auspices of combating child pornography<sup>530</sup>. Note that many of the subsequent legal intrusions into file sharing ecosystems to be discussed shortly likewise stem from charges related to child pornography; thus outcry at the latter is often explicitly deployed as a legal and rhetorical excuse to fetter entire systems of distribution based on isolated incidents of particularized modes of data exchange. Said legal intrusions at the same time function as highlighting those areas of thusly neutralized file sharing ecosystems which need to be strengthened against said fettering.

The necessary shift to fee-based news servers such as the aforementioned Giganews thus hampers free unbridled access to data, and further erodes the security of the userland by tying transactions (e.g. credit card data) to illicit or other downloads. Up to the end of 2014,

---

<sup>527</sup> Giganews. 2014. <https://www.giganews.com/>.

<sup>528</sup> E.g., cf. “1341 days binary retention”. Giganews. 2012. <https://web.archive.org/web/20120407173534/http://www.giganews.com/why.html>.

<sup>529</sup> Wang, *op. cit.*, p. 42.

<sup>530</sup> Eric T. Schneiderman. 2008. “Attorney General Announces Agreement With Cablevision To Block Online Child Pornography”. Press release. <http://www.oag.state.ny.us/press-release/attorney-general-announces-agreement-cablevision-block-online-child-pornography>.



BT—the Internet Service Provider (ISP) in the UK with the largest amount of users, exceeding four million<sup>531</sup>—had provided bundled Usenet access to subscribers via a partnership with Giganews, which was not renewed for unstated reasons<sup>532</sup>. News servers themselves are further susceptible to government shutdown, as in the case of News Service Europe (NSE), “the largest usenet provider in Europe”<sup>533</sup>, ceasing operations after being taken to court by Dutch anti-piracy association Bescherming Rechten Entertainment Industrie Nederland (BREIN). The existence of concentrated news servers thus provides a potentially deadly chocking point for the free promulgation of information, serving to highlight the vulnerability of Usenet’s serverland.

Finally, with regard to userland it must be kept in mind that the IP address of the uploader of content is passed along within posted Usenet messages. Instruction manuals advise the employment of anonymous remailer services which effectively function as intermediaries or proxies<sup>534</sup> as well as the use of ostensibly privacy-oriented newsgroup servers<sup>535</sup>. From the application layer however, a given newsreader application may be configured to connect to the NNTP server via Tor<sup>536</sup>, thus obfuscating the poster’s connection over the transport layer, with the exit node IP subsequently being the one present in the Usenet posting. A poster may also elect to first connect to a VPN provider prior to opening and posting via the newsreader application, thus once again obfuscating their IP at the transport layer prior to launching a given application.

Aside from the poster’s IP address, newsgroup postings also contain an encrypted X-Trace parameter. As Hahn points out, “[w]hen necessary, however, the information in the X-Trace line can be decrypted by the Usenet provider”<sup>537</sup>. Thus while the poster’s IP address may remain masked to the public, the originating news servers maintains a record thereof that is further tied to the payment mechanism the poster used to purchase access to the Usenet server in the first place. To deal with the latter potential deanonymization vector, a

---

<sup>531</sup> Blogcetera. 2009. “UK ISP, Cable and Dongle User Numbers - Jan 2009”. *Blogcetera*. <http://blogcetera.blogspot.co.uk/2009/02/uk-isp-cable-and-dongle-user-numbers.html>.

<sup>532</sup> BT Broadband. 2014. “Giganews closure: what I need to know”. *BT.com*. [http://bt.custhelp.com/app/answers/detail/a\\_id/51205/?s\\_cid=con\\_FURL\\_giganews](http://bt.custhelp.com/app/answers/detail/a_id/51205/?s_cid=con_FURL_giganews).

<sup>533</sup> Ernesto. 2011c. “Major Usenet Provider Shuts Down Following Court Order”. *TorrentFreak*. <https://torrentfreak.com/major-usenet-provider-shuts-down-following-court-order-111106/>.

<sup>534</sup> Wang, *op. cit.*, p. 58.

<sup>535</sup> Fellows, *op. cit.*, p. 77.

<sup>536</sup> Said connectivity may be achieved via setting up a given newsreader application to connect via a SOCKS5 proxy, with the proxy being the instance of Tor the user is running (jj4321. 2013. “USENET over TOR (nntp)?”. *TorForum.org*. <http://torforum.org/viewtopic.php?f=2&t=18313>).

<sup>537</sup> Harley Hahn. 2014a. “Anonymous File Sharing”, in *Harley Hahn’s File Sharing Tutorial*. <http://www.harley.com/usenet/file-sharing/05-anonymous-file-sharing.html>.

free Tor-based NNTP server may be used in lieu of one requiring a credit card-based account purchase<sup>538</sup>.

Even when encryption mechanisms are employed, court documents reveal that law enforcement may nonetheless infiltrate ostensibly private Usenet communities<sup>539</sup>. It is thus demonstrable that Usenet server and userlands, and thus filelands, can be compromised by legal forces impeding the unbridled flow of data sharing. Indeed, following the identification of the Usenet posters, the presence of encryption keys served as incriminating evidence in the case<sup>540</sup>. What is further of pivotal import herein is that despite the technological sophistication of the userland of this particular case study, there was nonetheless apparently a lack of knowledge of the legal operation of law enforcement<sup>541</sup>. Thus the security of the operative userland (and likewise of file and serverlands) in any given file sharing ecosystem is predicated on an all-encompassing operational security that entails procedural familiarity with any potential adversary. Given that one may not be aware of all potential adversaries, total security thus remains elusive, whilst practical measures can nonetheless be taken to strengthen acknowledged imperfect defenses. Law enforcement guidelines state that “participation in otherwise illegal activity [is justified] to obtain information or evidence necessary for the success of the investigation”<sup>542</sup>. Familiarization with said guidelines is thus imperative for successful distribution vectors. It can hence be seen that anonymity ruptures throughout Usenet’s server and userlands, when coupled with the limited longevity of fileland data and further exasperated by a lack of familiarity with the operational procedures of congealing actants, all culminate to potentially jeopardize the efficacy of Usenet as a distributive strategy for data dissemination.

#### 4.0.2 Internet Relay Chat (IRC)

---

<sup>538</sup> Colio. 2007. “Free hidden usenet (NNTP) service”. *Planet Peer - The anonymous networking community*. <http://board.planetpeer.de/index.php?topic=3556.0>.

<sup>539</sup> *United States of America v. Neville McGarity (aka Wraith), Daniel Castleman (aka Chingachgook), Gary Lakey (aka Eggplant), Marvin Lambert (aka Methuselah), Ronald White (aka Roadkill), James Freeman (aka Mystikal), Warren Mumpower (aka Lizzard)*. 2012. No. 09–12070. D.C. Docket No. 08–00022–CR–3–LAC. § I. A. – “Discovery and Infiltration of Child Pornography Ring”. <http://caselaw.findlaw.com/us-11th-circuit/1593463.html>.

<sup>540</sup> “PGP encryption keys of the type used by Constable Power to access the pertinent newsgroup postings were found in possession of every defendant except Neville McGarity”. *Ibid.*, § I. A. – “Arrest of Members of Child Pornography Ring”.

<sup>541</sup> “Because of the illegality of posting child pornography and the extensive familiarity with child pornography required to complete the tests, it was believed by the ring members that law enforcement agents would be prevented from gaining admission into the ring.” *Ibid.*, FN10.

<sup>542</sup> Council of the Inspectors General on Integrity and Efficiency. 2010. § 4. H. “Participation in Otherwise Illegal Activity by Undercover Employees”, in *Guidelines on Undercover Operations*. Washington, DC: Council of the Inspectors General on Integrity and Efficiency. pp. 11-13 (p. 11). [http://www.governmentattic.org/12docs/GuidelinesUndercoverOpsOIG\\_2010.pdf](http://www.governmentattic.org/12docs/GuidelinesUndercoverOpsOIG_2010.pdf).

Internet Relay Chat (IRC), another application layer protocol which, much like Usenet, was initially designed for the transmission of text messages, can indeed also be utilized for the transmission of binary files via the Direct Client-to-Client (DCC) sub-protocol<sup>543</sup>. IRC networks are constituted via conglomerates of servers to which end-users connect to be able to interact with other users on the same network by joining chatrooms, colloqually termed ‘channels’. An IRC network may consist of one or more servers, with users being able to interact with others on different servers which are part of the same network, but not with users who are on alternate networks altogether (unless the specialized use of a bridge or relay-bot is employed)<sup>544</sup>. Once a particular file sharing is joined, users may set up a file serving script, or fserv, which allows other users to connect to them and download files<sup>545</sup>. Whilst the security of the serverland is compromised by the fact that law enforcement networks monitor said servers<sup>546</sup>, court documents further reveal that law enforcement also actively seeks to neutralize those who are engaging in running fservs as well by undercover agents connecting to the fserv and obtaining the server’s IP address<sup>547</sup>. An IRC client can, much like a newsreader, likewise be configured to connect via Tor<sup>548</sup>, thus obfuscating a user’s IP via the transport layer (or the user can, once again as when accessing a Usenet server, connect to a VPN service prior to connecting to an IRC server). Application layer based anonymity thus here, as with the setting up of a newsreader, revolves around the ability to configure the application to connect via a transport layer-based anonymization tool, with the caveat being that the tool must also support the given transport layer protocol (in this case TCP).

Whilst fservs are generally run by home users, an alternative serving system known as XDCC generally uses high-speed “r00ted” corporate or academic servers which provide fast transfer rates<sup>549</sup>. That is to say that while fservs are generally run by file sharers sharing

---

<sup>543</sup> Troy Rollo. “A description of the DCC protocol”. <http://www.irchelp.org/irchelp/rfc/dccspec.html>.

<sup>544</sup> Nemesis][. “Frequently Asked Questions about Internet Relay Chat robots”. <http://www.irchelp.org/irchelp/misc/botfaq.html>.

<sup>545</sup> Paul L. Piccard. 2006. *Securing IM and P2P Applications for the Enterprise*. Rockland: Syngress. pp. 388-389.

<sup>546</sup> David Décary-Héту. 2014. “Information Exchange Paths in IRC Hacking Chat Rooms”, in *Crime and Networks* (ed. Carlo Morselli). New York: Routledge. pp. 218-230 (p. 229).

<sup>547</sup> “Agent Robin Andrews conducted an undercover search on a file-sharing program known as an mIRC [...] typing in a ‘trigger’ that allowed her to establish a direct connection with azgymguy2’s file-trader” (*United States of America v. Jason A. Wright*. 2010. No. 08-10525. D.C. Docket No. 4:03-cr-01908-RCC-CRP. Opinion. [http://njlaw.rutgers.edu/collections/resource.org/fed\\_reporter/NEWcircs/cir9/08-10525\\_cir9.html](http://njlaw.rutgers.edu/collections/resource.org/fed_reporter/NEWcircs/cir9/08-10525_cir9.html)).

<sup>548</sup> phrozen77. 2009. “HowTo: IRC anonymously with TOR”. <http://www.irc-junkie.org/2009-12-31/howto-irc-anonymously-with-tor/>.

<sup>549</sup> DÍzzIE. 2005. “The 2005 Beginner's Guide to Getting Warez on IRC”. <http://dizzy.childrenofmay.org/The.2005.Beginners.Guide.to.Getting.Warez.on.IRC.pdf>.

content from their home computer, XDCC servers are run by file sharers who have procured (often illicit) access onto business or academic servers, upload files to said servers, and then direct said servers to join the file sharing channel. Thus file sharers who run XDCC servers share files by proxy of the server they have gained access to. Instruction manuals and general discussions of the IRC file sharing ecosystem generally cover both systems<sup>550</sup>. However, despite the frequency of their mention, the advantageous anonymity implications are not made explicit: by serving files from an impersonal IP address, content sharers are protected from direct fettering. However, system administrators of the XDCC servers may be able to trace the identity of the uploader, though as said administrators themselves note, this in turn leads to further evasion techniques deployed by the uploaders to avoid connecting to the compromised file sharing server from their own home IPs<sup>551</sup>. Thus obfuscating the originating IP address of a content uploader—via, once again, transport-layer based obfuscation by way of, for instance, utilizing Tor or a VPN—is here shown to be pivotal to assuring longterm unfettered information sharing.

#### 4.0.3 Cyberlockers

Unlike other file sharing ecosystems, cyberlockers, alternatively called digital lockers<sup>552</sup>, are filehosting websites which harness Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Secure (HTTPS) in the service of data distribution in lieu of utilizing their own specialized protocol. Uploaders of content upload data to the cyberlocker and receive a unique link for the file which can then be passed onto forums and aggregated on other websites known as Direct Download (DDL) sites<sup>553</sup>. Thus it can immediately be seen that in this case the longevity of fileland data is intrinsically tied to that of the serverland, which in this case is constituted by the cyberlocker site and its accompanying backing servers. Filehosts typically specify death-clock style limits on the amount of time a file is stored on the servers predicated on the last-download data. For instance, a typical cyberlocker policy reads “[t]he files are kept forever as long as they are being downloaded. If the files are not downloaded even once within 30 days consecutively they are removed. If you have a premium account your files are never deleted”<sup>554</sup>. The incentive to obtain a purchased premium account to increase the longevity within the fileland in turn leads to potential

---

<sup>550</sup> See, e.g., DIzzIE, *ibid.*, p. 11, 19; Piccard, *op. cit.*, p. 387; Wang, *op. cit.*, p. 66.

<sup>551</sup> TonikGin. 2002. “XDCC - An .EDU Admin’s Nightmare”.

<https://www.ncsu.edu/itd/security/papers/EduHacking.html>.

<sup>552</sup> Gail Blasser Riley. 2011. *Internet Piracy*, Tarrytown: Marshall Cavendish Corporation. p. 16.

<sup>553</sup> DDL Rank. 2014. “Top DDL Sites”. *DDL Rank*. <http://ddlrnk.com/top-download-sites.html>.

<sup>554</sup> File Dropper. “About Us”. *File Dropper*. <https://www.filedropper.com/aboutus.php>.

compromise of the security of the userland via establishing a link between financial information (e.g. credit card details) and the ensuing file sharing.

Though one could be sure to schedule downloading of a given file within each filehost's permissible period so as to extend storage, the longevity of the serverland itself is also highly precarious. Filehosts may shutdown under the weight of impending lawsuits, as for instance was the case with the Oron cyberlocker<sup>555</sup> or, going a step further, may be actively shut down by law enforcement<sup>556</sup>, as in the case of the Megaupload cyberlocker following a federal indictment<sup>557</sup>. Though Megaupload relaunched a year later under the title Mega<sup>558</sup>, previously shared files stored on Megaupload servers were not available on the new Mega platform with its founder describing the loss as "the largest data massacre in the history of the Internet caused by the US government, the Department of Justice and LeaseWeb"<sup>559</sup>. Thus the centralization of cyberlockers can be seen to lead to an effacement of fileland longevity and serverland security given that the files are stored on readily identifiable web servers.

With regard to cyberlocker userland anonymity, filehost websites often state that user data is not tracked or logged by the cyberlocker. For instance, the Pomf.se cyberlocker claims that "No logs are kept, no logs over uploading nor over downloading"<sup>560</sup>, whilst the aptly named Anonfiles invites users to "Upload your files anonymously"<sup>561</sup>. Under a transparency initiative, Pomf publishes its site source code<sup>562</sup> as well as server configuration files and other miscellanea such as takedown request letters<sup>563</sup>. However there is of course no assurance that the published materials accurately reflect the active site code and configuration files.

---

<sup>555</sup> enigmax. 2012. "Massive Copyright Infringement Suit Could Collapse Cyberlocker, Studio Warns". *TorrentFreak*. <https://torrentfreak.com/massive-copyright-infringement-suit-could-collapse-cyberlocker-studio-warns-120702/>.

<sup>556</sup> Kevin Lincoln. 2012. "The Feds Just Shut Down A Huge File Sharing Site And Charged Its Founder With Piracy". *Business Insider*. <http://www.businessinsider.com/megaupload-shut-down-2012-1>.

<sup>557</sup> *United States of America v. Kim Dotcom, Megaupload Limited, Vestor Limited, Finn Batato, Julius Bencko, Sven Echternach, Mathias Ortmann, Andrus Nomm, Bram Van Der Kolk*. 2012. Indictment. Criminal No. 1:12CR3. <https://www.scribd.com/doc/78786408/Mega-Indictment>.

<sup>558</sup> C.S.-W. 2013. "Mega relaunch". *The Economist*. <http://www.economist.com/blogs/schumpeter/2013/01/kim-dotcom>.

<sup>559</sup> Juha Saarinen. 2013. "'Data Massacre' as Megaupload Files Deleted". *iTnews*. <http://www.itnews.com.au/News/347330,data-massacre-as-megaupload-files-deleted.aspx>.

<sup>560</sup> neku. "FAQ". *Pomf.se*. <https://pomf.se/faq.html>.

<sup>561</sup> AnonFiles. 2014. <https://anonfiles.com/>.

<sup>562</sup> neku. 2014. "Source code for Pomf.se". *GitHub*. <https://github.com/nokonoko/Pomf>.

<sup>563</sup> neku. 2014-2015. "Transparency". *Pomf.se*. <http://transparency.pomf.se/>.

Similarly, one can likewise skeptically approach Anonfiles' claims of anonymous uploading. Despite the invitation to anonymous uploading, the Terms page states that uploaders can "be held responsible for illegal and/or Copyright infringement material"<sup>564</sup>. The precise entailment of said responsibility is not expanded upon. Perhaps the matter can be elucidated by following the path of a file on Anonfiles. When a file is first uploaded to Anonfiles, a unique URL is produced: <https://anonfiles.com/file/db8418275b2df3572d534a0629ba5f54>. The URL can be seen to consist of the protocol (HTTPS), followed by the site domain (anonfiles) and in turn the top-level domain (.com), which is then followed by the folder directory or path (file), and finally the specific page (db8418275b2df3572d534a0629ba5f54), in this case named by the uploaded file's MD5 checksum hash. When a user clicks on the Download link on said URL, they are redirected to, in this case, <https://cdn.anonfiles.com/1414158879447.txt>, the content delivery network (CDN) subdomain. The original name of the file (justafile1.txt; which is nonetheless still visible on the webpage of the previous MD5-based URL) is replaced by a server-generated 13-digit filename either randomly generated or based on a particular hashing algorithm (1414158879447), though the file extension (.txt) is kept unmodified. However, this secondary CDN URL in turn prompts an 'HTTP 302 Moved Temporarily' response from the Anonfiles server, redirecting to [http://bayfiles.net/api\\_anon?file=1414158879447.txt](http://bayfiles.net/api_anon?file=1414158879447.txt) which finally allows one to download the file. Going to [http://bayfiles.net/api\\_anon](http://bayfiles.net/api_anon) in turn redirects to <https://anonfiles.com/file/notfound>. Similar URL query logs showing that Anonfiles redirects to Bayfiles and vice versa can be found via cached copies of urlQuery reports<sup>565</sup>, a web service which traces the path the browser takes to retrieve a given URL. What is the significance of the fact that Anonfiles seems to be a front-end for Bayfiles, an ostensibly unrelated cyberlocker? Whilst, as will be recalled, Anonfiles claims that files are uploaded anonymously, the BayFiles Privacy Policy explicitly states that the cyberlocker stores "IP address of the computer from which the upload is started"<sup>566</sup>, going on to further state that "if we are legally obliged to turn over information about the origin of a file, we will fulfill that obligation"<sup>567</sup>. It is unknown whether AnonFiles acts as a middle-man proxy on behalf of

---

<sup>564</sup> Anonfiles. 2012. "Terms". *AnonFiles*. <https://anonfiles.com/terms>.

<sup>565</sup> urlQuery. 2014. "[cdn.anonfiles.com/1400515873889.pdf](https://cdn.anonfiles.com/1400515873889.pdf)". *urlQuery* [Google Cache].

<https://webcache.googleusercontent.com/search?q=cache:JsvASEdVyaQJ:https://urlquery.net/report.php%3Fid%3D1406955387110>.

<sup>566</sup> Bayfiles. "Privacy Policy". *BayFiles*. <https://bayfiles.net/privacy>.

<sup>567</sup> *Ibid.*

the uploader when uploading files to Bayfiles via the AnonFiles interface due to the fact that the configurations of the underlying servers are not publicly accessible, hence the possibility that uploader IP addresses are likewise stored, thus potentially serving to compromise userland anonymity.

With regard to cyberlocker-based distributive strategies we have thus seen how a combination of serverland takedown vulnerability coupled with lack of userland anonymization due to an accompanying lack of serverland transparency all lead to fileland insecurity; as compromised hosting and compromised uploading translate to compromised file availability.

Given that cyberlockers are generally accessed via a web browser, transport layer anonymization may be achieved by configuring the web browser to connect via Tor (or by using Tor's especially-configured Tor Browser<sup>568</sup>), thus tunneling the web browser application communications via Tor. However, given the rise of browser fingerprinting techniques to deanonymize users based on various information leakages from the web browser application such as time zone, installed font sets, and screen resolution<sup>569</sup>, particular attention to application layer anonymization should be given when utilizing web-based cyberlocker services. Specifically, a user would of necessity thus ideally not only not use the same web browser for accessing various services, but would also further use different machines (or different virtual machines) for doing so, or would otherwise have to modify their system timezone, resolution, installed font sets and other potentially identifying parameters. As even if transport layer anonymity is achieved, the identity of the user may nonetheless be compromised via the application layer based on said browser and cross-browser fingerprinting techniques.

#### 4.0.4 BitTorrent

Instead of hosting files on set servers from which users can download them, the BitTorrent file sharing protocol adopts a peer to peer (P2P) method of distribution in which users download files from one another<sup>570</sup>, thus firmly enmeshing the user, server, and filelands. Traditionally the torrent protocol had two critical points of centralization: 1) torrents relied on core servers or 'trackers' which were "responsible for helping downloaders

---

<sup>568</sup> Tor Project. 2015. *Tor Browser*. <https://www.torproject.org/projects/torbrowser.html.en>.

<sup>569</sup> See, for instance, Károly Boda, Ádám Máté Földes, Gábor György Gulyás, Sándor Imre. 2012. "User tracking on the web via cross-browser fingerprinting", in *Information Security Technology for Applications*. Berlin: Springer. pp. 31-46.

<sup>570</sup> Bram Cohen. 2008. "The BitTorrent Protocol Specification". *BitTorrent.org*. [http://www.bittorrent.org/beps/bep\\_0003.html](http://www.bittorrent.org/beps/bep_0003.html).

find each other”<sup>571</sup> by providing information about the swarm or the group of uploaders and downloaders on any particular torrent; and 2) various servers were necessary for hosting the created .torrent files where users could download them. Said points of congealment allowed for a degree of vulnerability in BitTorrent’s efficacy as an unbridled distributive strategy, leading, for instance, to state and corporate neutralization of copious torrent trackers<sup>572</sup>. Though at times the trackers have returned<sup>573</sup>, or been replaced by other trackers catering to the same area<sup>574</sup>, at other times no apparent replacements exist for other shutdown trackers<sup>575</sup>, thus serving to highlight the precarity of the BitTorrent ecosystem.

Today however, neither trackers nor .torrent files are necessary for the successful deployment of the BitTorrent protocol. The introduction of the Distributed Hash Table (DHT) protocol in BitTorrent led to “each peer becom[ing] a tracker”<sup>576</sup> which is deployed over the UDP transport protocol, whilst the introduction of magnet Uniform Resource Identifiers allowed for “clients to join a swarm and complete a download without the need of downloading a .torrent file first”<sup>577</sup>. Thus, for instance, the modern day Pirate Bay, formerly a torrent tracker<sup>578</sup>, today chiefly only provides magnet links. Though still a potential point of centralization as certain websites act as repositories of magnet URIs in lieu of torrent files, any user can post a text magnet URI on any website which allows for user text input (e.g. forums and comment fields) which other users can then paste into their client. In other words, serverland security is strived for in the BitTorrent ecosystem via increased decentralization thereof.

---

<sup>571</sup> Bram Cohen. 2006. “Incentives Build Robustness in BitTorrent”, in *Workshop on Economics of Peer-to-Peer Systems*. pp. 1-5 (p. 2). <https://pdos.csail.mit.edu/6.824-2010/papers/cohen-btecon.pdf>.

<sup>572</sup> E.g., Ernesto. 2013e. “Underground Gamer Goes Down Citing Legal Problems”. *TorrentFreak*.

<https://torrentfreak.com/underground-gamer-goes-down-citing-legal-problems-130602/>; Chris Harris. 2007. “Music File-Sharing Site OiNK Shut Down Following Criminal Investigation”. *MTV*.

<http://www.mtv.com/news/1572554/music-file-sharing-site-oink-shut-down-following-criminal-investigation/>; Adi Robertson. 2012. “Demonoid torrent tracker shut down by Ukrainian police”. *The Verge*.

<http://www.theverge.com/2012/8/6/3223253/demonoid-bittorrent-tracker-shut-down-by-ukrainian-police>.

<sup>573</sup> Ernesto. 2014a. “Demonoid Returns, Website Now Back Online”. *TorrentFreak*.

<https://torrentfreak.com/demonoid-back-140330/>.

<sup>574</sup> Ben Jones. 2007. “What Waffles? The Hydra Lives On”. *TorrentFreak*. <https://torrentfreak.com/what-waffles-hydra-071030/>.

<sup>575</sup> dexter311. 2014. “One year on - is there anything that comes close to what Underground Gamer used to be?”. *Reddit*. [https://reddit.com/r/trackers/comments/2kgo45/one\\_year\\_on\\_is\\_there\\_anything\\_that\\_comes\\_close\\_to/](https://reddit.com/r/trackers/comments/2kgo45/one_year_on_is_there_anything_that_comes_close_to/).

<sup>576</sup> Andrew Loewenstern and Arvid Norberg. 2008. “DHT Protocol”. *BitTorrent.org*.

[http://www.bittorrent.org/beps/bep\\_0005.html](http://www.bittorrent.org/beps/bep_0005.html).

<sup>577</sup> Greg Hazel and Arvid Norberg. 2012. “Extension for Peers to Send Metadata Files”. *BitTorrent.org*.

[http://www.bittorrent.org/beps/bep\\_0009.html](http://www.bittorrent.org/beps/bep_0009.html).

<sup>578</sup> Ernesto. 2009. “The Pirate Bay Tracker Shuts Down for Good”. *TorrentFreak*. <https://torrentfreak.com/the-pirate-bay-tracker-shuts-down-for-good-091117/>.



Much like when connecting through the DCC sub-protocol on IRC, peers connecting over BitTorrent similarly reveal their IP addresses (assuming at this point that users are connecting directly, not using any additional transport layer anonymization tools) to everyone in the swarm as is generally common in P2P architectures, which has led to attempted neutralization of the ecosystem's userland via legal action<sup>579</sup>. However, unlike the case with IRC/DCC which communicates via TCP/IP and which can thus potentially be anonymized over the transport layer via the deployment of Tor, the DHT protocol is, as previously mentioned, deployed over UDP. One will thus not be able to in this case—unlike our previous use-cases discussed thus far—use Tor for transport layer anonymity as Tor only supports TCP/IP. The potential snares and pitfalls of configuring BitTorrent to run over Tor whilst maximizing user anonymity will be further discussed in section 4.2.1.2, as the related privacy concerns may inhibit user adoption of the deployed experimental Tor-based BitTorrent tracker to be introduced in section 4.2.0. Transport layer anonymity can further be addressed via the potential of using a VPN which supports UDP prior to running a BitTorrent client.

Even though the apprehension of BitTorrent users based on their IP address has become a contested practice not only in the populist sense<sup>580</sup> but in the legal arena as well<sup>581</sup>, recall that there has further been a rise<sup>582</sup> in the attempted bolstering of userland security via the purchasing of VPN and seedbox services (which offer the user server space from which to download and upload content procured from torrent files) which mask the user's personal (non-VPN) IP address from the swarm, instead effectively displaying the purchased third party VPN IP. Recall our previous discussion of the potential cost of a given outcome when assessing trust relationships in section 4.0.0. With the case of BitTorrent usage over a VPN, the cost would be literal in the sense of damages sought by the plaintiffs following their

---

<sup>579</sup> Ernesto. 2011a. "200,000 BitTorrent Users Sued In The United States", *TorrentFreak*.

<https://torrentfreak.com/200000-bittorrent-users-sued-in-the-united-states-110808/>.

<sup>580</sup> Dana Liebelson. 2014. "Why It's Getting Harder to Sue Illegal Movie Downloaders". *Mother Jones*.

<http://www.motherjones.com/politics/2014/02/bittorrent-illegal-downloads-ip-address-lawsuit>.

<sup>581</sup> *Elf-Man, LLC. v. Eric Cariveau, et al.* 2014. Case No. C13-0507RSL. Order Granting Motion to Dismiss and Granting Leave to Amend. <https://www.scribd.com/doc/201180332/ORDER-Granting-Motion-to-Dissmiss>.

<sup>582</sup> Ernesto. 2013a. "BitTorrent Accounts for 35% of All Upload Traffic, VPNs are Booming", *op. cit.*

copious motions for discovery<sup>583</sup> of the identities of various swarm peers including, notably, VPN users<sup>584</sup>.

Finally, aside from the aforementioned anonymization techniques, additional BitTorrent-specific anonymization options such as BitBlender<sup>585</sup> may be considered. BitBlender functions by BitBlender, described as an “anonymous network protocol specifically tailored to P2P file sharing, and in particular, the BitTorrent protocol”<sup>586</sup>, consists of relay peers which effectively act as crowd-sourced intermediary peers which make requests and relay responses on behalf of the originating peers. Said relay peers further provide plausible deniability as any potential peer or observer would not know if the peer requesting data from a swarm is an active seeker of said content or simply an intermediary proxy, though the potential legal benefits of a lack of differentiation between the two remains dubious<sup>587</sup>.

#### 4.0.5 Miscellaneous Services

There is of course a veritable plethora of other existent online vectors for file propagation. Protocols and services such as the Gnutella network<sup>588</sup>, Hotline<sup>589</sup>, File Transfer Protocol (FTP) sites<sup>590</sup>, soulseek<sup>591</sup>, Direct Connect<sup>592</sup>, and so on too numerous to explicitly mention singularly. However, we can describe said systems as all falling into the same distributory patterns as those delineated in our aforementioned four test cases, fitting into one

---

<sup>583</sup> “Cases matching ‘killer joe nevada’”. 2014. Justia Dockets & Filings.

<http://dockets.justia.com/search?query=killer+joe+nevada>; e.g., *Killer Joe Nevada, LLC., v. Does 1-15*. 2013. Civil Action 2:13-cv-00848. <https://cases.justia.com/federal/district-courts/ohio/ohsdce/2:2013cv00848/165535/4/0.pdf>.

<sup>584</sup> Ernesto. 2013b. “‘Killer Joe’ Sues VPN-Using BitTorrent Pirates”. *TorrentFreak*.

<https://torrentfreak.com/killer-joe-sues-vpn-using-bittorrent-pirates-130418/>.

<sup>585</sup> Kevin Bauer, Damon McCoy, Dirk Grunwald, Douglas Sicker. 2008. “BitBlender: Light-weight anonymity for BitTorrent”. Proceedings of the workshop on Applications of private and anonymous communications. ACM. <https://gnunet.org/sites/default/files/bauer-alpaca2008.pdf>.

<sup>586</sup> *Ibid.*

<sup>587</sup> “It is unclear whether the operators of anonymizing network infrastructure (such as Tor routers, BitBlender relay peers, etc.) could be held vicariously liable for the potentially illegal actions of the system’s users” (Kevin Bauer, Dirk Grunwald, Douglas Sicker. 2009. “The Arms Race in P2P”. *37th Research Conference on Communication, Information, and Internet Policy, TPRC*.

[https://cs.uwaterloo.ca/~k4bauer/papers/bauer\\_tprc2009.pdf](https://cs.uwaterloo.ca/~k4bauer/papers/bauer_tprc2009.pdf)).

<sup>588</sup> Gnutella is a decentralized P2P protocol, and much like BitTorrent, has a variety of clients available, though a general community portal for discussions exists at Gnutella Forums (<http://www.gnutellaforums.com/>).

<sup>589</sup> Hotline integrated FTP and IRC-style protocols with its own proprietary schema (Josh. 2006. “Hotline File Sharing”. *Nailbat.com*. <http://www.nailbat.com/content/view/14/32/>).

<sup>590</sup> The general FTP network protocol is widely adopted for illicit file dissemination (see, e.g., Craig, *op. cit.*).

<sup>591</sup> Soulseek employs both its own client and protocol (Soulseek. 2014. “Download”. *Soulseek*.

<https://www.soulseekqt.net/news/node/1>; daelstrom and lbponey . 2010. “The Soulseek Protocol”. *Museek+*. <https://www.museek-plus.org/wiki/SoulseekProtocol>).

<sup>592</sup> The Direct Connect (and subsequent Direct Connect ++ development) is once again a P2P protocol with a variety of available clients (cologic, emtee, Fredrik Ullner, Wicked World Games. 2009-2013. “DC++ Documentation”. *DC++: Just These Guys, Ya Know?*. <https://dcpp.wordpress.com/category/documentation/>).

of the following architectural constructs: 1) wholly centralized distribution sites, in which a central server coordinates connections and file distribution, necessitating for users to connect to the server to then download files therefrom (e.g. Hotline, FTP), 2) wholly distributed distribution networks, in which there is neither a central server nor central users, in which users connect to one another to share segments of files betwixt each other in an entirely-P2P architecture (e.g. Gnutella), or 3) mixed-architecture distribution arrays which may rely on a networks of distributed servers alongside distributed peers, but nonetheless contain some coalescent points of centralization (soulseek, Direct Connect). The operative pitfalls of each distribution model, as has been shown via the previous test cases, typically involve the dangers of IP revelation with respect to userland security which can in turn lead to user deanonymization via legal motions for discovery which seek to create court orders for service providers to reveal identifying information based on said IP leakage and/or purchase leakage in the form of the service provider being in possession of the user’s payment data; the risk of server neutralization (i.e. seizure and/or shutdown) with regard to the serverland via legal coercion; and in the realm of fileland, limited file expectancy leading to ultimate unavailability of data and thus the exposition of the temporal failure of data dissemination. IP revelation may however be mitigated via the deployment of various transport layer anonymization tools such as Tor and/or VPNs in tandem with careful configuration of the application layer via tweaking any particular application’s settings to minimize potential information leakage.

#### 4.0.6 F2F Systems

Seeing as how one of the key pitfalls of existent distribution systems can thus be seen to be the injection of unwanted (e.g. state or corporate) agents into the distribution chain—attack vectors which can be classed as Sybil attacks in which a single adversary (or entity) controls multiple peers (has multiple identities) for hostile purposes<sup>593</sup>—alternate privatized or ‘dark’ file sharing systems have been proposed and at times dubbed ‘friend to friend’ (F2F)<sup>594</sup>, as opposed to the more generally open P2P systems. The general aim of F2F systems can thus be said to “combine the flexibility and autonomy of peer-to-peer architectures with the confidentiality and authentication of traditional groupware”<sup>595</sup>. In other

---

<sup>593</sup> John R. Douceur. 2002. “The sybil attack”, in *Peer-to-peer Systems*. Berlin: Springer. pp. 251-260.

<sup>594</sup> Dan Bricklin. 2000. “Friend-to-Friend Networks”. <https://bricklin.com/f2f.htm>.

<sup>595</sup> Michael Rogers and Saleem Bhatti. 2007. “How to Disappear Completely: A Survey of Private Peer-to-Peer Networks”, in *SPACE (Sustaining Privacy in Autonomous Collaborative Environments) 2007*. pp. 1-10 (p. 7). <http://www.cs.st-andrews.ac.uk/files/publications/download/RB07b.pdf>.

words, F2F systems engage in userland trust management via the restriction of serverland access to authenticated (which is to say, vetted) peers and further by the attempted hardening of the underlying serverland against compromise, thus seeking to establish the security of the existent fileland as well (the security of available files being predicated upon assuring the persistence of secure user and serverland bases). Given that F2F systems thus by definition connect friends to one another (with the aforementioned aim of preventing Sybil attacks), an adversary may potentially observe the resultant social network of the peers in a given F2F system. Thus the primary focus of F2F systems is typically on the anonymization and security of the traffic, as opposed to that of the users (in the form of either clients and/or servers), with the users being peers trusted by other peers in the given F2F ecosystem.

Whilst the clients which facilitate the networking are themselves generally public, as for instance is the RetroShare software<sup>596</sup> which has become popular in recent years<sup>597</sup>, in order to connect to a given network one must be in the proverbial know: to know someone to invite them to said network. Whilst in traditional P2P applications one can generally connect to a number of public services, F2F systems can necessitate an *a priori* knowledge of existent servers before one can connect to them; in the sense of no public server list being offered. Whilst Zuo et al. point out that “users with a small set of friends are penalized by lack of available storage for their needs”<sup>598</sup>, thus serving to highlight the technological ramifications for all three here-entangled userlands, the social dimensions of penalizations should likewise here be brought to the fore. That is to say that aside from small groups of peers having more limited storage space than larger groups of peers (assuming a, *ceteris paribus*, equal per-user storage allocation), an earlier penalization occurs via an erected barrier to access: users with small sets of friends do not receive the same access privileges as users with larger sets of friends.

It is important to here note that whilst there are indeed specialized F2F clients, other existent file sharing venues can also be configured to work in an effectively obscured pseudo-F2F mode. For instance, there are private invitation-only BitTorrent trackers, as are there invitation-only IRC channels, Direct Connect hubs, FTP servers, and so on. Thus layers

---

<sup>596</sup> csoler, defnax, drbob7, thunder2. 2014. RetroShare. <http://retroshare.sourceforge.net/>.

<sup>597</sup> Ernesto. 2012. “Anonymous, Decentralized and Uncensored File-Sharing is Booming”. *TorrentFreak*. <https://torrentfreak.com/anonymous-decentralized-and-uncensored-file-sharing-is-booming-120302/>.

<sup>598</sup> Xiang Zuo, Jeremy Blackburn, Nicolas Kourtellis, John Skvoretz, Adriana Iamnitchi. 2014. “The Power of Indirect Ties in Friend-to-Friend Storage Systems”, in *14th IEEE International Conference on Peer-to-Peer Computing (P2P)*. pp. 1-5 (p. 1). [https://www.p2p-conference.org/~ptwopcon/p2p14/wp-content/uploads/2014/09/221.P2P2014\\_64.pdf](https://www.p2p-conference.org/~ptwopcon/p2p14/wp-content/uploads/2014/09/221.P2P2014_64.pdf).

of privatization can be added to virtually any existent file sharing protocol by various modes of restricting access<sup>599</sup>. What makes F2F systems distinct from private modes of other P2P systems, however, is that users of F2F systems only connect directly to trusted friends, as opposed to for instance private BitTorrent trackers on which one can connect to anyone within the broader group who may not necessarily be an immediate trusted friend (instead being perhaps the friend of a friend).

The practical question however here becomes whether the resultant stringent access control policies constitute an effective protection mechanism, and further whether these communities actually facilitate unbridled data sharing. The fact that private torrent tracker communities are periodically infiltrated by undesirable agents seeking to congeal data flow<sup>600</sup>, would seemingly indicate that so-called private trackers, whilst perhaps being harder to penetrate, are certainly not immune to infiltration and subsequent neutralization. As information security literature oft advises, “you can take advantage of obscurity; just don't rely on it”<sup>601</sup>. In other words, ineffectual reliability on security through obscurity can inherently lead to a deterioration of trust afforded to the torrent site operators (reliability being one of the aforementioned parameters of trust-building). Hence the actual security of F2F-oriented distribution networks ushered in by a privatization of access can be seen to be questionable at best, and illusory and damaging at worst—serving to ensconce server and userland actants in the comforting blanket of nonexistent privacy, paradoxically rendering them all the more vulnerable to apprehension and persecution. In other words, whilst an aforementioned key aim of F2F services may be the prevention of Sybil attacks in which an adversary adds a number of malicious peers to an open P2P system and uses said peers to adversely impact the ecosystem (for instance by deanonymizing users which connect to the malicious peers, or by spreading malicious payloads amongst peers), access restriction, on its own, is nonetheless an insufficient security measure due to the underlying fact that even friend(ly) connections may ultimately not be trustworthy. That is to say, a trusted friend may have their machine compromised by an adversary at any given point in time, with the

---

<sup>599</sup> For instance, one notoriously difficult to enter private BitTorrent tracker, restricts access to practicing magicians (venotes. 2014. “What tracker is **\*\*the\*\*** hardest to get into these days?” *Reddit*. [https://www.reddit.com/r/trackers/comments/27paw7/what\\_tracker\\_is\\_the\\_hardest\\_to\\_get\\_into\\_these\\_days/ci30m9x](https://www.reddit.com/r/trackers/comments/27paw7/what_tracker_is_the_hardest_to_get_into_these_days/ci30m9x)).

<sup>600</sup> E.g., enigmax. 2011. “Police Raid ‘Excellent’ Private BitTorrent Tracker, Admins Arrested”. *TorrentFreak*. <https://torrentfreak.com/police-raid-excellent-private-bittorrent-tracker-admins-arrested-110526/>; enigmax. 2010b. “Six BitTorrent Admins Arrested, Interpol Chase Two More”. *TorrentFreak*. <https://torrentfreak.com/six-bittorrent-admins-arrested-interpol-chase-two-more-100310/>.

<sup>601</sup> Aaron W. Bayles. 2005. *InfoSec Career Hacking: Sell Your Skillz, Not Your Soul*. Rockland, MA: Syngress. p. 152.

adversary then using the friend's trusted credentials to connect to the F2F network. In other words, given  $n$  users on a sample F2F ecosystem, one user can never be certain that the remaining  $n-1$  users have not become compromised (indeed, one user in an  $n$  user ecosystem may further never be certain that  $n$  users have not been compromised, as the given user may also be compromised without the user's knowledge thereof). F2F systems do, however, prevent unverified peers from initially connecting to the network (depending on how strict credential assignments are within the given F2F ecosystem).

The previously mentioned second, though by no means secondary in importance, issue is whether or not said F2F-structured distribution systems are palatable with our stated aim of unbridled wholesale file distribution. Given that these systems are predicated upon the sharing of content only within an exclusive group of those privileged enough (via monetary resources—as accounts to private F2F communities can at times be purchased<sup>602</sup>—or via the aforesaid social-connectedness) to have access to said systems, the answer is thus a firm *no* precisely by virtue of the exclusionary nature of F2F systems. Thus all manner of F2F systems must be eschewed if our aim is to locate an open data dissemination system without privileged levels of access. It must however be noted that whilst our answer is firmly in the negative, the rejection is based upon the elitist nature of said systems, as opposed to their often strengthened security (via the broad deployment of encrypted communication networks and SSL implementation, for instance). The latter is indeed quite useful and can in fact be deployed on public-facing file distribution hubs, as for instance the Pirate Bay now offers HTTPS connections by default<sup>603</sup>.

#### 4.0.6.0 Freenet

A desirable distributive mechanism is one that would have privacy and anonymity built into the system by default so as to avoid neutralization of the aforesaid user, server, and filelands. In other words a sort of virtual Tong, which Bey defines as “a mutual benefit society for people with a common interest which is illegal or dangerously marginal—hence, the necessary *secrecy*”<sup>604</sup>. One such potential darknet file sharing ecosystem is known as Freenet.

Freenet is described by its developers as “free software which lets you publish and obtain information on the Internet without fear of censorship. To achieve this freedom, the network is entirely decentralized and publishers and consumers of information are

---

<sup>602</sup> Torrent Invite. <http://www.torrentinvitesell.com/>.

<sup>603</sup> The Pirate Bay. <https://thepiratebay.se>.

<sup>604</sup> Bey, *The Radio Sermonettes*, *op. cit.*

anonymous”<sup>605</sup>. When one downloads the Freenet software, one also selects an amount of hard drive disk space to devote to Freenet, with the bare minimum allocation being two gigabytes. When one connects to the Freenet network, unlike other file sharing and communications applications which rely on varying degrees of centralization—for instance, IRC or Usenet connection necessitates a connection to a specific data server—the Freenet network is marked by a notable lack of any such horizontal stratification. Freenet may thus be run in an ‘open’ fashion in which anyone may connect, or it may be run in a ‘closed’ F2F styled system, with the latter being the direction more recent Freenet development has been taken in by its core developers<sup>606</sup>. Thus Freenet sits on an uncertain ledge, oscillating between a closed F2F system and a more open darknet structure, depending on which instance one chooses to run<sup>607</sup>.

As the original paper outlining the Freenet concept goes on to explain, “no node is privileged over any other node, so no hierarchy or central point of failure exists”<sup>608</sup>. Thus the dilemma of interconnectivity of Freenet resembles that of the war machine, “the problem of the war machine, or the firing squad: is a general necessary for  $n$  individuals to manage to fire in unison? The solution without a General is to be found in an acentered multiplicity...without any copying of a central order”<sup>609</sup>. Each Freenet node (i.e. each user) has the potential to connect to every other node, and likewise, thus formulating a theoretical mesh of potential horizontal interactivity. While, as will be examined shortly, there are various constraints which may be put into place so as to serve to inhibit a truly universal notion of complete interlinking, the key point to recall is that in lacking any manner of centralization, Freenet-enabled data dissemination cannot be restrained by the elimination of any singular node<sup>610</sup>. That is to say, if one node is discovered and taken offline, the network

---

<sup>605</sup> srv017.bxl.xs4all.be. 2005. “What is Freenet?”. *The Freenet Help Site*. <http://www.freenethelp.org/html/Freenet.html>.

<sup>606</sup> Ian Clarke and Oskar Sandberg. 2005. “Covert Communication in a Dark Network: A major new version of freenet”. *22nd Chaos Communication Congress*. [https://events.ccc.de/congress/2005/fahrplan/attachments/544-Slides\\_CovertCommunicationInADarkNetwork.pdf](https://events.ccc.de/congress/2005/fahrplan/attachments/544-Slides_CovertCommunicationInADarkNetwork.pdf).

<sup>607</sup> “Normally Freenet will connect automatically and should ‘just work’, automatically connecting to other nodes (Strangers). However, if you know several people who are already using Freenet, you can enable high security mode and add them as Friends, so Freenet will only connect to them” (The Freenet Project. “Download Freenet”. *The Freenet Project*. <https://freenetproject.org/download.html>).

<sup>608</sup> Ian Clarke, Oskar Sandberg, Brandon Wiley, Theodore W. Hong. 2000. “Freenet: A Distributed Anonymous Information Storage and Retrieval System”, in *Designing Privacy Enhancing Technologies* (ed. Hannes Federrath). Germany: Springer-Verlag, pp. 46-66 (p. 49).

<sup>609</sup> Deleuze and Guattari, *op. cit.*, p. 17.

<sup>610</sup> A standard website is typically stored on a data server in a concrete location. Whilst some servers have various back-ups or mirrors, when the server is shutdown, the website goes with it. For instance, if a web server were raided by State or Corporate interests, the website (pending a mirror copy) would effectively be taken

itself mutates to accommodate the loss, thus not only surviving, but rather thriving, despite attempts at statist abridgement.

Alongside a rhizomatic interconnectivity, Freenet is also marked by a notable distributed data warehousing architecture. As soon as one allocates the aforementioned disk space to Freenet, the resultant datastore pool begins to both receive and transmit outpours of data flows. In Freenet, the congealed totality of data, *a file*, is eschewed in favor of an encrypted segmentarity: when a file, let us say an MP3, is uploaded to the Freenet network, it is encrypted and subsequently broken down into randomized bits and pieces, which are then redundantly distributed throughout the network, bits and pieces stored on the datastores of various nodes. It is precisely this disintegration of congealment, a rejection of static totality, which lends Freenet to fostering unbridled data exchange, “there are no points or positions in a rhizome, such as those found in a structure, tree or root. There are only lines”<sup>611</sup>. In order to reconstitute the file structure, to retrieve a congealed artifact from the depths of Freenet, a node connects to a neighboring node and requests certain anonymous chunks of digital flotsam floating in that node’s datastore pool. That node, if it does not possess the desired segment, connects to another node and so on<sup>612</sup>.

Failed requests for data, far from leading to critical collapse as they did in the ARPANET schema<sup>613</sup>, merely serve to foster all the greater interconnectivity, as the nodes reach out to all the more nodes if any error in data is transmitted from the initial nodes. Freenet deploys a proto-DHT routing methodology, known as key-based routing, with requests being routed by the network to nodes which have keys which match the files users may be looking for, though there is no guarantee that a given file will ultimately be found in a given cluster. As Bey points out, it is decisively this capacity for thriving upon aberration, on disintegration and on-going reconstitution of the network, which fosters the creation of a Temporary Autonomous Zone, it is “precisely *within* the margin of error [where] the TAZ can come into existence”<sup>614</sup>. Unlike, say, ARPANET which had as its primary goal reliability

---

online, with the data no longer being available. On the other hand, if a particular Freenet node were subjected to similar repression, the attempted seizure would have little effect on the availability of the targeted data, as it is redundantly distributed around a multitude of horizontal, anonymous nodes; thus Freenet is notably marked by an eschewal of arborescence.

<sup>611</sup> Deleuze and Guattari, *op. cit.*, p. 8.

<sup>612</sup> Clarke et al., *op. cit.*, p. 52.

<sup>613</sup> Despite “a large number of error-control mechanisms [which] were designed into the system” (Katie Hafner and Matthew Lyon. 1996. *Where Wizards Stay Up Late: The Origins of the Internet*. New York: Simon and Schuster. p. 119), “occasionally the network simply went berserk...trouble in one machine could trip a systemwide domino effect” (*ibid.*, p. 195).

<sup>614</sup> Bey, *T.A.Z.*, *op. cit.*



and speed<sup>615</sup>, the five design goals of Freenet are articulated as having an emphasis on anonymity, deniability, resistance, storage, and decentralization”<sup>616</sup>. As such, the developers write, “Freenet is designed with anonymity in mind, performance comes second”<sup>617</sup>. Though the point here is not one of grafting Freenet into an imposed TAZ-like typology, but merely of the elucidation of a seemingly shared mindset, a mutual privileging of something other than optimization, a joint espousal of the virtues of aberration. While the blitzkrieg of randomized and encrypted data transmission is limited only by each node’s individual upstream/downstream bandwidth speeds, thus potentially maxing out all connections, *individual* data retrieval can nonetheless take a significant amount of time, due to the aforementioned architecture of each node having to contact each other node for a specific piece of segmented data.

Thusly it is evinced that Freenet privileges the transmission of unbridled, randomized data in lieu of congealed artifacts akin to standard computer files. While the file is symptomatic of stasis, the digital equivalent of a brick or perhaps a book lying on a shelf, the data stream itself, the raw information which was formally congealed in the mold of a file, perhaps even complete with the previously discussed fetters of intellectual properties, Freenet thrives on the in-between transfer of disintegrated data, the myriad potential folds of the rhizome: “[t]he life of the nomad is the intermezzo. Even the elements of his dwelling are conceived in terms of the trajectory that is forever mobilizing them”<sup>618</sup>. When one taps into the Freenet one is thrust into the midst of an always already situatedness, saturated with inpours and outpours of encrypted data flows to be temporarily archived in the prescribed datastore pool until they are replaced by other, equally ephemeral, segments.

To be sure, Freenet is itself not an isolated exemplar of unbridled data exchange. A solitary enclave would succumb to the same critiques of congealment, albeit from a metanarrative (i.e., were Freenet a solitary *exception to the rule*, it could be isolated, relegated to the role of an irrelevant outlier by zealous statisticians seeking a purity of congealment). Yet as others have pointed out<sup>619</sup> networks akin to Freenet have existed prior

---

<sup>615</sup> “How it was to be achieved didn’t concern Taylor greatly, as long as the network was reliable and fast” (Hafner and Lyon, *op. cit.*, p. 44).

<sup>616</sup> Clarke et al., *op. cit.*, p. 47.

<sup>617</sup> The Freenet Project. “Freenet Frequently Asked Questions”. *The Freenet Project*. <https://freenetproject.org/faq.html>.

<sup>618</sup> Deleuze and Guattari, *op. cit.*, p. 380.

<sup>619</sup> See, for instance: Michael Bailey, Evan Cooke, Farnam Jahanian, Andrew Myrick, Sushant Sinha. 2006. “Practical Darknet Measurement”, in *Information Sciences and Systems, 40th Annual Conference*. pp. 1-6. <http://www.eecs.umich.edu/fjgroup/pubs/darknet-ciss06.pdf>; Biddle, et al, *op. cit.*

to its inception as well as existing in congruence *with* Freenet. In stating, as previously mentioned, that “the darknet is not a separate physical network but an application and protocol layer riding on existing networks”<sup>620</sup>, Biddle et al. point out that darknets—networks of unbridled data exchange—may exist not only in the digital terrain, as does Freenet or a number of other \*nets, but also in meatspace, as the case of the Sneakernet elucidates.

When you burn a Blu-ray copy of some files to give to a friend—or perhaps dub a copy of a film onto a repurposed VHS—to whom presumably you then walk over to deliver the data, you are then partaking in a Sneakernet: the transferal of data that escapes the State’s attempts at congealment both by ignoring whatever license or other content management system the files in question and by literally avoiding detection by not exchanging the unauthorized discs in front of police officers or the like<sup>621</sup>. Thus what is evident is that the throes of unbridled data exchange have a sort of fail-safe metaredundancy built into the act of dissemination itself. If one were to regard Freenet as the solitary example of said practices, then such a narrative focalization would nonetheless create a congealed center of operation, albeit a distributed one. Freenet cannot be shutdown lest all nodes are somehow found and destroyed, but nonetheless to focus solely on Freenet would be to give the state machine hope, an aspiration: shutdown Freenet and you shutdown the data flows, successfully reinforcing a congealment of information. Thus while the focus of this section is presumably on Freenet of its own accord, the focus is itself a mere sampling of an ungraspable multitude. Within the metanarrative of data exchange, Freenet, whilst being composed entirely of nodes and lines of data transferal between the nodes (and thusly being composed of data exchange itself), is *itself* naught but a singular node amidst a broader distributed ecosystem of data dissemination.

#### 4.0.7 Darknets

Given that our operative demands are stringent security measures to protect both those in user and serverland (which in turn leads to prolonged protection of the content in fileland by denizens of the former two lands) while at the same time also fostering maximal public availability of said content, a final area of data distribution to explore is that of the darknet. Though at times closely affiliated with F2F systems, strictly speaking darknets differ in their ability to be publicly available. In other words, while placing the utmost value on encryption and data security, darknets are not necessarily unavailable to the public. Instead, they only function in the dark in the sense that they are not accessible through standard

---

<sup>620</sup> Bailey, et al., *op. cit.*

<sup>621</sup> For an espousal and examination of contemporary sneakernets, see: Henry Warwick. 2014. *Radical Tactics of the Offline Library*. Network Notebooks 07. Amsterdam: Institute of Network Cultures.

protocols or clients like FTP software or web browsers, without the deployment of specialized software. Instead they necessitate the installation of their specialized client/server applications which link the user into the particular darknet. At times employing distributed and encrypted peer-to-peer file storage and propagation (in other words with multiple users on the network containing encrypted packets which, together, make up a certain file), darknets at other times deploy more centralized, albeit anonymized, distribution mechanisms (for instance, a centralized server the IP address of which is entirely obfuscated from any sort of look-up due to a mediated delivery system which bounces the user-requested file through a series of intermediary servers or relays).

The term darknet entered the nomenclature several years following the aforementioned introduction of F2F terminology, with Biddle et al. describing a darknet system as simply “a collection of networks and technologies used to share digital content”<sup>622</sup>, though subsequent definitions have highlighted the secure and anonymous tendencies of darknet networks<sup>623</sup>. However, aside from the tendency towards security-consciousness which darknets share with F2F networks, darknets—unlike F2F ecosystems—are “easy to connect to, and as they become more popular due to the barriers to entry shrinking”<sup>624</sup>. We can thus classify darknets as filesharing ecosystems which emphasize user- and serverland anonymity and security. Much like with accessing standard P2P protocols and networks, to access a darknet one generally needs to download a particular client. Though it must be pointed out that downloading the client in the first place may prove to be a complicated endeavor as state and corporate interests may attempt to inhibit the distribution thereof. For instance, less than a day after a download link to the previously-discussed one will recall, in Part I of the *Operations Manual*, WASTE darknet was posted, the parent company (AOL) of the company the WASTE developers worked for (Nullsoft) removed the download link<sup>625</sup>, and replaced the webpage with a notice claiming, in part, that “any reproduction, distribution, display or other use of the Software by you is unauthorized”<sup>626</sup>. However, the problem of

---

<sup>622</sup> Biddle, et al., *op. cit.*, p. 1.

<sup>623</sup> E.g., “the term is used to differentiate private, anonymous distributed networks from their public predecessors” (Jessica A. Wood. 2010. “The Darknet: A Digital Copyright Revolution”, in *Richmond Journal of Law & Technology* 16 (4). pp. 1-60 (p. 17). <http://jolt.richmond.edu/v16i4/article14.pdf>).

<sup>624</sup> Symon Aked. 2011. “An Investigation Into Darknets and the Content Available Via Anonymous Peer-to-Peer File Sharing”, in *Australian Information Security Management Conference*. pp. 10-18 (p. 17). <https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1105&context=ism>.

<sup>625</sup> Nate Mook. 2003. “AOL Execs Flush Nullsoft’s WASTE”. *betanews*. <http://betanews.com/2003/05/30/aol-execs-flush-nullsoft-s-waste/>.

<sup>626</sup> Nullsoft. 2003. “Notice of Unauthorized Software”. <https://web.archive.org/web/20030602021255/http://www.nullsoft.com/free/waste/>.

access to clients is by no means restricted to darknets, as for instance the official website of the P2P program LimeWire, a client used to connect to the Gnutella network, currently states that “LimeWire is under a court order dated October 26, 2010 to stop distributing the LimeWire software”<sup>627</sup>. Thus the mere distribution of file sharing clients (whether darknet F2F or clearnet P2P) poses an initial hurdle to gaining entry into the particular file sharing ecosystem, particularly since the trust of an unofficial mirror link containing a client may subsequently be questioned, if for instance a malicious third party hosts a modified version which allows for user tracking.

A way to approach the problem of client validation, which is here manifested as a particular articulation of trust management, is via a process known as checksum verification. Whilst it is traditionally described in the literature as a specific use-case of verifying that a file has been downloaded entirely, as opposed to being incomplete due to an interrupted transfer<sup>628</sup>, the file checksum may also potentially be used to verify the authenticity of a downloaded client. Upon downloading the client, the user can run a command to calculate the downloaded file’s checksum and compare the resultant value against the value listed by the developers of the client, assuming that 1) such an original value has been made available by the developers somewhere, and that 2) said value can be trusted not to have been tampered with (e.g. if a rogue entity has modified the developers’ website to inject a malicious ‘original’ value). In lieu of mere checksum validation, one may instead deploy public key cryptography to sign the client using a private key, with the signature then being possible to verify by anyone using the accompanying public key<sup>629</sup>. Though once again, such as client verification schema is dependent on the developers having originally deployed it in the first place and on the private/public key pair not having been tampered with. In other words the potential downloader would have to be sure to verify that the public key they are using to verify the client’s signature is indeed the public key of the client developers.

## **4.1 Cautionary Notes Regarding Theory and Data**

### **4.1.0 On the Dangers of Theoretical Compartmentalization**

---

<sup>627</sup> LimeWire. 2014. <http://www.limewire.com/>.

<sup>628</sup> E.g., Jack James. 2006. *Digital Intermediates for Film and Video*. Burlington, MA: Elsevier Inc. p. 195; Shantanu Tushar and Sarath Lakshman. 2013. *Linux Shell Scripting Cookbook* (Second Edition). Birmingham, UK: Packt Publishing, pp. 77-80.

<sup>629</sup> Peter Loshin. 2013. *Simple Steps to Data Encryption: A Practical Guide to Secure Computing*. Waltham, MA: Elsevier. pp. 55-63; see also: Free Software Foundation. 1999. “Making and verifying signatures”, in *The GNU Privacy Handbook*. <https://www.gnupg.org/gph/en/manual/x135.html>.

When attempting to see how particular theoretical constructs may coalesce with tangible examples, particularly when the tangible example at hand—an amorphous swarm of data dissemination—is anything *but*, one runs afoul of the danger of theoretical congealment: that of attempting to confine emergent data stratum to a pre-existent theory. For instance, upon an initial reading of Bey, one may be prone to envision Freenet as a cyber manifestation of the Temporary Autonomous Zone: “the TAZ is an encampment of guerilla ontologists: strike and run away. Keep moving the entire tribe, even if it's only data in the Web...The strike is made at structures of control, essentially at ideas; the defense is ‘invisibility,’ a martial art, and ‘invulnerability’—an ‘occult’ art within the martial arts”<sup>630</sup>. Surely Freenet meets the specific ‘criteria’: its strong encryption schemas lend the network to a literal invisibility, ephemeral data nodes strike a blow against static congealment of data, only to disappear into and be subsumed by other nodes, and so on. And yet, whilst Bey at one point in time acknowledged the “liberatory potential”<sup>631</sup> of the Internet, he nonetheless went on to caution against a techno-liberation tunnel vision, “I don’t think that this technology, any more than any other technology, is going to be the fix that will bring us freedom and glory”<sup>632</sup>, going on to later describe his view of cyberspace as “dire” due to increasing privacy erosion<sup>633</sup>.

Freenet construed as tangible architectural mechanism of data dissemination is an irrelevancy for as mentioned, it itself constitutes but one of many amorphous nodes. The focus instead, is on the *data flow*, the architecture is but a spatial constraint; indeed “crudely speaking one might say the TAZ ‘exists’ *in information* [emphasis added]”<sup>634</sup>, as such it cannot possibly be congealed into a reified artifact such as a particular darknet client, to do so would be akin to conjuring a license to dominate a likewise conjured BoW. Akin to the nomadic rhizome, the TAZ exists *in-between*; specific network architecture may be conducive to its transmission, but the architecture *itself* is nonetheless an inhibitor so long as the focus remains on the objects, the frameworks, instead of the actual data transmission. Akin to the warrior god Indra, “the war machine in itself...is like a pure and immeasurable

---

<sup>630</sup> Bey, *T.A.Z.*, *op. cit.*

<sup>631</sup> Peter Lamborn Wilson. 1996. “Cybernetics & Entheogenics: From Cyberspace to Neurospace”, in “Next Five Minutes” *Conference on Tactical Media Amsterdam*. <http://www.t0.or.at/hakimbey/neurospc.htm>.

<sup>632</sup> Bey, *ibid.*

<sup>633</sup> Hakim Bey and Hans Ulrich Obrist. 2010. “In Conversation with Hakim Bey”. *e-flux* 21. <http://www.e-flux.com/journal/in-conversation-with-hakim-bey/>.

<sup>634</sup> *Ibid.*

multiplicity, the pack, an irruption of the ephemeral and the power of metamorphosis”<sup>635</sup>. The war machine does not manifest itself within Freenet, it does not lend itself to exorcism by haunting a particular body, rather its goal is the “emission of quanta of deterritorialization”<sup>636</sup>, data incessantly flowing in and out of every node on the network. It is precisely the *static on the line*, intangible, ungraspable, which breaks down all constituencies ranging from intellectual properties akin to copyright/left, to the notion of a tangible digital file itself.

The significance of static, here exhibited in the form of encrypted darknet packet data, cannot be overstated. An article from a 1959 issue of the *National Security Agency Technical Journal* that was only recently declassified in January 2008 is devoted to the problems of transmitting data over telephone lines (predating the first commercial modem by several years). In explaining the technicalities and challenges of data transmission the article (whose author has been redacted) goes on to discuss the problem of extraneous noise,

because of its nature, impulse noise defies mathematical analysis, so that most studies of it are empirical. If the signal spectrum it corrupts is narrow in comparison to the spectrum of the impulse, it resembles thermal or white noise in many respects. In any case, our attempt at providing an adequate defense against it leaves much to be desired<sup>637</sup>.

The sheer magnitude of noise, the now proverbial static on the line, is here stressed by the fact that the NSA, in its own technical publications, was essentially admitting the breakdown of attempts at command and control of their coveted data transmissions. The fear over encrypted noise is today manifested by, for instance, the NSA’s fears over not being able to access smartphones<sup>638</sup>; though the potent possibility of course exists that such stories of apparent inaccessibility are designed to foster false states of confidence in the highlighted corporate products. Encryption, extraneous signal noise, or perhaps encryption masquerading as noise, thus continue to be symptoms of aberrant data flow, manifested via the darknet as viable strategies for digital distribution.

Whilst risking congealment via categorization, Deleuze and Guattari nonetheless go on to explicitly define three characteristics of the war machine: the spatiogeographic (which

---

<sup>635</sup> Deleuze and Guattari, *op. cit.*, p. 352.

<sup>636</sup> *Ibid.*, p. 229.

<sup>637</sup> [Redacted]. 1959. “Data Transmission Over Telephone Circuits”, in *NSA Technical Journal* 4 (1). pp. 67-81 (p. 75). [https://www.nsa.gov/public\\_info/\\_files/tech\\_journals/data\\_transmission.pdf](https://www.nsa.gov/public_info/_files/tech_journals/data_transmission.pdf).

<sup>638</sup> Sam Frizell. 2014. “The FBI and NSA Hate Apple’s Plan to Keep Your iPhone Data Secret”. *Time*. <https://time.com/3437222/iphone-data-encryption/>.

stresses the *in-between* of two points, as opposed to, say, focusing on the nodes themselves), the arithmetic (distribution via an open space versus closed, regimented parceling), and the affective (a paradoxical eschewal of movement, a reterritorialization built ‘on deterritorialization itself’)<sup>639</sup>. Likewise, the unbridled dissemination of data on, or rather *through*, Freenet depends not on the movement of tangible segments from one node to the other, but rather on the flux itself. The particular segments archived on any one node are entirely incidental (not to mention entirely indecipherable, as they are not only compartmentalized but also encrypted), they are naught but temporal ephemera always ready to be caught up in the mix of the tumultuous data flow itself.

Whereas the loss of data, of conjured intellectual property in the form of digital excreta may be lamented by self-prescribed ‘property holders’, unbridled darknet data dissemination *consists* of this very disintegration. Thus “every ‘catastrophe in the Net is a node of power for the Web, the counter-Net. The Net will be damaged by chaos, while the Web may thrive on it’<sup>640</sup>. Though this is most certainly not to say that state machines (albeit here perhaps more concisely constructed as *capital* machines) will not seek to utilize the data flows of the war machines for their own statist ends; indeed, that this process is occurring can be evinced by taking a customary glance at the literature of capital<sup>641</sup>, which extols the economic virtues of ‘leaderless organization.’ And yet, for flows of capital to be advantageous to their masters, they must presumably generate a sustainable level of profit accumulation. It is precisely at this point of monetary congealment that capitalist appropriation of data flows breaks down, congeals. Indeed Brafman and Beckstrom’s explanation of another file sharing ecosystem, emule<sup>642</sup>, seems most uncertain, as if they peered behind every nook and cranny for some prospect of profit accumulation and manage to come up empty-handed. Similarly, whilst, in aiming to dispel cyber utopianism through a ‘net criticism’, Lovink adopts the view that “the glorification of action and counterculture will prove no match for corporations and nation states to contain the web”<sup>643</sup>, he nonetheless later goes on to lament that “e-commerce offspring from Napster, Gnutella, Freenet and other

---

<sup>639</sup> Deleuze and Guattari, *op. cit.*, p. 381.

<sup>640</sup> Bey, *T.A.Z.*, *op. cit.*

<sup>641</sup> Ori Brafman and Rod A. Beckstrom. 2006. *Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*. New York: Penguin Group.

<sup>642</sup> *Ibid.*, pp. 9-29.

<sup>643</sup> Geert Lovink. 2003. *Dark Fiber: Tracking Critical Internet Culture*. Cambridge, MA: The MIT Press. p. 19.

peer-to-peer networks have been disappointingly few<sup>644</sup>; thus perhaps betraying the corporations and nation states are the ones who, at least in this example, have proven to be no match for the enacted anti-corporate practice of the peer-to-peer networks. Even the advocates of capital appropriation of unbridled data exchange are unable to find tangible examples of their flights of fancy. Yet even should such examples materialize, they would do little other than to then further highlight non-commercial deployments of commercialized architecture. To introduce commercial enclosure would be to introduce trappings for the data to overflow once again, and thus we would see a retelling of a similar story as the aforementioned one we have told in an earlier section about the demise of intellectual property. The essential point, of course, is that unbridled data exchange cannot be corralled for any need or purpose other than data flow itself. To introduce *purpose* is to introduce a gross congealment, to once again invite outpouring. Our strategy is unbridled distribution as an end in itself; whether it is also a potential means to something further is of no relevancy to the immediate project at hand.

#### 4.1.1 An Ethnographic Crisis in Data Collection

Prior to our foray into Tor's Onionland darknet, a note on data sampling is in order. When venturing out into *the field*, the budding ethnographer proceeds, Petri dishes in hand, ready for the routine task of data acquisition. In the cyber realm this particular practice oft manifests itself via, say, survey collection<sup>645</sup>, or perhaps verbal interaction (which is perhaps a softer way of saying informal interviewing, which is in turn to perhaps a softer way of saying interrogation)<sup>646</sup>. And yet these exercises in data acquisition at times seem to forget that the object of research, of data collection itself, does not exist *a priori*. It is instead conjured by the highly-localized perceptions of the ethnographer, via pre-stated hypotheses and research aims, whether via adopting an illusory observational 'fly on the wall' distance, or engaging in fully-immersed participatory-observation, the end result is the same: nuggets of a congealed dataset constructed through the ethnographer's perceptions are nonetheless collected as if the ethnographer excavated from the depths of the 'field.' Thus "ethnography

---

<sup>644</sup> *Ibid.*, p. 364. N.B. given that Lovink presents a grand total of zero actual examples of capitalist co-option of any darknet, 'disappointingly few' is thus perhaps best read in the spirit of hyperbole.

<sup>645</sup> Ian Condry. 2004. "Cultures of Music Piracy: An Ethnographic Comparison of the US and Japan", in *International Journal of Cultural Studies* 7(3). pp. 343-363.

<sup>646</sup> Elizabeth M. Reid. 1996. "Communication and Community on Internet Relay Chat: Constructing Communities", in *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace* (ed. Peter Ludlow). Cambridge, MA: MIT Press. pp. 397-411.



involves the creation and manipulation of knowledge”<sup>647</sup>. Whatever is collected in our researcher’s Petri dish, whatever is written down in their field notes or winds up under the Findings heading of their forthcoming paper, is a congealed construction *born of the* ethnographer’s own perception.

As Dicks et al. further suggest, talk of ‘data’ in ethnography is somewhat inappropriate. The methodological language we use, such as ‘data’, ‘observation’, ‘recording’, ‘analysis’ and ‘findings’, all come from positivist models of empirical research, and do not necessarily reflect the complexity and contingency of study in the social and cultural fields<sup>648</sup>.

Ironically, ‘empirical proof’ of this critical theorization can be presented precisely via an attempt to congeal a viable dataset from Freenet. Recall that Freenet, embodying the eschewal of stasis, only houses congealed data in segmented, encrypted slivers stored in an allocated datastore (a folder on the hard drive). Recall that not only is the Freenet data always *in flux*, but it is also compartmentalized, with various pieces of a disintegrated file being redundantly distributed to various random nodes, but on top of that, the data is also encrypted. An artificial congealment, a trapping of an ephemeral transcendence slipping in time thus only serves to obfuscate and cogent attempts at analysis of data flows themselves. The irony of course is the futility of data acquisition is exhibited precisely *through* an exercise in congealment. In the attempted bottling up of ephemeral data dissemination, in an attempted exertion of congealment, what this entire project is dedicated to elucidating the futility of, we finally see emerge a digital ouroboros.

Thus the data acquisition practices of the positivist bring with them their own demise. In outlining her suggested principles of a virtual ethnography, Hine states that we can usefully think of the ethnography of mediated interaction a mobile rather than multi-sited. As a consequence, the concept of the field site is brought into question...The object of ethnographic enquiry can usefully be reshaped by concentrating on flow and connectivity rather than location and boundary as the organizing principle<sup>649</sup>.

---

<sup>647</sup> Bella Dicks, Bruce Mason, Amanda Coffey, Paul Atkinson. 2005. *Qualitative Research and Hypermedia: Ethnography for the Digital Age*. London: Sage Publications. p. 116.

<sup>648</sup> *Ibid.*

<sup>649</sup> Christine M Hine. 2000. *Virtual Ethnography*. London: Sage Publications. p. 64.

Thus the case studies herein have been devoted to the disintegration and accompanying dissemination of information, not to any congealed datasets. Intersecting with aforesaid PAR-based principles, the research is instead devoted on a deployment of constant *actions*, which in turn reframe and reshape the constantly-recontextualized research itself.

Yet, whilst Freenet may certainly be theoretically palatable, and indeed appealing, a number of inherent limitations in the system have led us to consider alternate suggested distribution modes for this project. First of all, recent versions of Freenet have focused predominantly on F2F, as opposed to public, development, which render it explicitly counter to our sought-after unbridled data distribution which necessitates a publicly-accessible distribution, as privatization is quite an explicit fettering of data. As Clarke and Sandberg declare that “future networks may need to limit connections to trusted friends [...] the next version of Freenet will be based on this philosophy”<sup>650</sup>, the emergent F2F model is thus incompatible with a broad distributive strategy. If the Freenet network, or at least the now-privatized portions thereof, can no longer be accessed by the general populace, then Freenet regretfully loses its efficacy as a viable means of unhindered populist data promulgation, resigning itself to an elitist mode of data sharing for the privileged few; with gaining access to a closed Freenet community being the thematic equivalent of gaining closed entry to, say, a corporate publisher’s intranet.

Yet even if operated in its public mode, recall that Freenet nonetheless presents the potent problem of file attrition. Due to limited allocated drive space by users of the network, unpopular files are eventually sacrificed to make room for the more popular and newer ones, echoing Bey’s aforementioned admonition of the Internet as memory blackhole<sup>651</sup>. Thus, much like with aforementioned fileland pitfalls in open P2P distribution systems or clearnets, the lifespan of a given bit of data is of pivotal importance. The potential loss of unpopular files is of particular import here as Freenet itself is at first glance a platform for the preservation of potentially unpopular material; but alas this proves to be a deceptive mirage, though the Freenet Project suggests using the KeepAlive plugin to repeatedly re-insert files into the network<sup>652</sup>, the plugin is of course not active by default; necessitating that whoever has the files is still around to re-add them In sum, the twin components of recent Freenet

---

<sup>650</sup> Ian Clarke and Oskar Sandberg. 2005. “Covert Communication in a Dark Network: A major new version of freenet”, *op. cit.*

<sup>651</sup> Bey and Obrist, *op. cit.*

<sup>652</sup> The Freenet Project. “Why can’t Freenet store data permanently?”, in “Freenet Frequently Asked Questions”. *The Freenet Project*. <https://freenetproject.org/faq.html#store-perm>.

development trending toward anti-social F2F-based darknet erection compounded by the serious issue of potential file attrition, have thus led us to seek other viable anonymized means of unbridled data dissemination.

## **4.2 Torrenting on Tor's Onionland: An Empty Kitchen**

### **4.2.0 Setting up a Tor-based BitTorrent Site**

A logical extension of facilitating the anonymous promulgation of information is to setup a torrent tracker as a Tor hidden service, thus providing greater anonymity in terms of the serverland with regard to obfuscating the location of the host of the tracker, as well as potentially boosting the anonymity in terms of the userland by way of bolstering the privacy of the peers within any given swarm of a torrent that uses the Tor-based tracker, presuming of course that the peers use Tor not only for tracker communication but for peer-to-peer communication as well. Prior art in this field previously existed in the form of a Tor-backed BitTorrent tracker known as The Hidden Tracker<sup>653</sup>. Established circa 2009<sup>654</sup> and existing intermittently<sup>655</sup> until seemingly 2011<sup>656</sup> or 2012<sup>657</sup>, The Hidden Tracker was described as a “free and open BitTorrent tracker concealed behind a Tor hidden service”<sup>658</sup> that “doesn’t have to worry about being shut down”<sup>659</sup>. Aside from its relatively short lifespan, The Hidden Tracker appears to have provided basic tracker functionality and thus was involved in coordinating peer interactions within the swarm such as allowing each new peer to obtain a list of existent peers who are sharing the content of a particular torrent<sup>660</sup>, whilst also providing basic operational tracker statistics such as the total number of peers using the coordinating tracker and the total number of torrents tracked by the tracker<sup>661</sup>. The Hidden Tracker does not however appear to have provided any additional functionality, included no

---

<sup>653</sup> The Hidden Tracker. 2009. <http://z6gw6skubmo2pj43.onion>.

<sup>654</sup> While the exact origin date could not be pinpointed, a 2009 *TorrentFreak* article refers to The Hidden Tracker as “brand new” (enigmax. 2009. “BitTorrent Hydra: Anonymous Hidden Tracker Via Tor”. *TorrentFreak*. <https://torrentfreak.com/bittorrent-hydra-anonymous-hidden-tracker-via-tor-090725/>).

<sup>655</sup> According to tweets on The Hidden Tracker’s Twitter page (The Hidden Tracker. <https://twitter.com/hiddentracker>) the tracker experienced various periods of downtime, with the longest lasting roughly ten months, going down on February 21<sup>st</sup> 2010 (*Ibid.*, <https://twitter.com/HiddenTracker/status/9451900556>) and coming back online on December 24<sup>th</sup> 2010 (*Ibid.*, <https://twitter.com/HiddenTracker/status/18501362614538240>).

<sup>656</sup> The last tweet from The Hidden Tracker twitter account, announcing that the tracker is back online, is from January 15<sup>th</sup> 2011 (*Ibid.*, <https://twitter.com/HiddenTracker/status/26300375199911936>).

<sup>657</sup> A directory scan of .onion addresses from April 19<sup>th</sup> 2012 includes The Hidden Tracker address, thus indicating that at least the host was reachable at the time (gatomalo. 2012. “Spider Scan of ToR Directories A-Z”. *USCyberLabs*. <http://uscyberlabs.com/blog/2012/04/19/spider-scan-tor-directories-a-z/>).

<sup>658</sup> The Hidden Tracker. <https://twitter.com/hiddentracker>.

<sup>659</sup> Hackbloc. 2011. “The Hidden Tracker Returns”, in *Hack This Zine*, V. 12 (Spring 2011). p. 33.

<sup>660</sup> “Tracker HTTP/HTTPS Protocol”, in Bittorrent Protocol Specification v1.0.

[https://wiki.theory.org/BitTorrentSpecification#Tracker\\_HTTP.2FHHTTPS\\_Protocol](https://wiki.theory.org/BitTorrentSpecification#Tracker_HTTP.2FHHTTPS_Protocol).

<sup>661</sup> The Hidden Tracker. 2010. <https://twitter.com/HiddenTracker/status/18711490781519873>.

possibility to actually store the .torrent files which would include the tracker information, with *TorrentFreak* point out what is necessary now is a safe haven for the storage of torrent files themselves<sup>662</sup>. Thus, given The Hidden Tracker's limited up-time, coupled with its lack of ancillary supporting features such as torrent storage and the facilitation of peer interaction, this project thought to deploy a feature-rich Tor-based BitTorrent tracker that would extend the functionality of The Hidden Tracker to facilitate .torrent storage and user interaction.

Towards this end, the project utilized the PHP-based TBSource torrent tracker codebase<sup>663</sup>, which while called also called a 'tracker' includes not only the technical tracker functionality but also the aforementioned torrent-storage and peer interaction capabilities. When referring to a 'torrent tracker', the term thus sees two uses: the narrow aforementioned technical denotation of a tracker as the server-side coordination of peer communication and statistics, and the broader connotation referring to both the aforementioned technical denotation and the surrounding paraphernalia (including torrent storage and community practices). TBSource thus provides not only the technical tracker, but also PHP-based web front-ends that can store and display torrent files in categories, provide space for users to add torrent descriptions (which may include both text and graphical information about the torrents), and further provides community forums.

Said TBSource codebase was installed on a remote web server which also subsequently had Tor installed<sup>664</sup>, with the torrc file then being configured to route the web service through Tor, as per the configuration instructions provided by the Tor Project<sup>665</sup>. The resultant Tor-based torrent tracker was then listed on the Hidden Wiki<sup>666</sup>, a user-contributed index of various Tor hidden services. Over a period of several months, the tracker<sup>667</sup> received an excess of 1,000 user registrations and a total of around 100 torrent uploads. However, following the initial popularity of the tracker, usage statistics saw a significant drop-off to its unfortunate current state of total stagnation and inactivity. For instance, out of a current 2,405 userbase, only 18 users have uploaded data and only 28 have downloaded, with the total

---

<sup>662</sup> enigmax, "BitTorrent Hydra: Anonymous Hidden Tracker Via Tor", *op. cit.*

<sup>663</sup> rb, wyz, YeOK. 2010. TBSource Classic. <http://sourceforge.net/projects/tbsource/>.

<sup>664</sup> With thanks to [anonymous] for facilitating the necessary hardware and technical implementation of the tracker.

<sup>665</sup> Tor Project. "Configuring Hidden Services for Tor". <https://www.torproject.org/docs/tor-hidden-service.html.en>.

<sup>666</sup> The Hidden Wiki. 2013. [http://kpvz7ki2v5agwt35.onion/wiki/index.php/Main\\_Page](http://kpvz7ki2v5agwt35.onion/wiki/index.php/Main_Page).

<sup>667</sup> Space Puppy Grotto (SPG). [http://\\*.onion](http://*.onion). Title is fictional; URL redacted. Refer to Disclaimer of Liability.

data transferred hovering around 500 gigabytes<sup>668</sup>. What, then of May's exultations of the virtues of crypto-anarchy? "Data havens for the storage and marketing of controversial information is another area of likely future growth"<sup>669</sup> he prophesized in 2001. Of Bey's exultation of the Tong and the Temporary Autonomous Zone? Granted, Bey was explicit in his critique of the computerized web and its blind overlaid interpretation as being congruent with the TAZ, "we must still admit to some qualms about computers [...] Most of all I want computers to provide me with information linked to real goods"<sup>670</sup>. The bifurcation Bey delineates between so-called 'real goods' and presumably digital-only files no longer rings true, and thus the call for turnips—"the full potential of non-hierarchic information networking logically leads to the computer as the tool par excellence. Now I'm waiting for the hackers to prove I'm right, that my intuition is valid. Where are my turnips"<sup>671</sup>, can now be fulfilled.

The Silk Road<sup>672</sup>, another Tor hidden service, and following its shutdown a myriad of other similar services<sup>673</sup>, allows users to purchase a variety of goods ranging from outlawed pharmaceuticals to ammunition and weaponry using the Bitcoin cryptocurrency. Furthermore, the rise of 3D printing has allowed many to start literally creating tangible 'real' goods as well. The interest in Silkroad could have raised awareness of Tor's Onionland and could have perhaps further had the potentially beneficial spill-over effect of garnering increased initial cursory interest in SPG. How then can we explain the near-total fall-off of usage of an anonymized file distribution system geared towards protecting against user and serverland deanonymization attacks (which would have, it was hypothesized, in turn lead to increasing the longevity of the ensuing fileland—due to the fact that the existence of which was predicated upon operational server and userlands immune to takedown)?

#### 4.2.1 Factors Potentially Detrimental to User Adoption of the Torrent Tor Site

There are a number of compounding factors which can be extracted from the experiment which may have served as coalescing detrimental effects on attracting a userbase

---

<sup>668</sup> Statistics augmented and not presented in a tabulated manner to preserve user anonymity by avoiding correlation attacks. The augmented data does not impact the analysis.

<sup>669</sup> Timothy C. May. 2001. "Crypto Anarchy and Virtual Communities", in *Crypto Anarchy, Cyberstates, and Pirate Utopias* (ed. Peter Ludlow). Cambridge, MA: The MIT Press. pp. 65-80 (p. 72).

<sup>670</sup> Bey, *TAZ*, *op. cit.*,

<sup>671</sup> *Ibid.*

<sup>672</sup> Silk Road. <http://silkroadvb5piz3r.onion>.

<sup>673</sup> Digital Citizens Alliance. 2014. "Busted, But Not Broken: The State of Silk Road and the Darknet Marketplaces".

<https://www.globalinitiative.net/download/cybercrime/global/Digital%20Citizen%20Alliance%20-%20Busted,%20but%20not%20broken%20The%20State%20of%20Silk%20Road%20and%20the%20darknet%20marketplaces.pdf>.

for the project, which include technological factors in the form of barriers to entry, personal factors in the form of objections to particular content, and privacy factors in the form of anonymity concerns around BitTorrent-over-Tor usage.

#### 4.2.1.0 Technological ‘Barrier to Entry’ Factors

First of all, a predominant factor to consider in any technological adaptation is the barrier to entry from user and serverland perspectives. Users had to not only download Tor, but to also subsequently configure either their own browser (or use Tor’s own browser bundle) to be able to access the tracker, and to further configure their torrent client so as to tunnel torrent tracker communications through Tor as well. The technological barrier to user entry may thus have been a sufficient deterrent to put-off prolonged use of the tracker, as users would thus have had to maintain not one but two separate web browsers and torrent clients, unless they wanted to route all their web and torrent traffic through Tor. Furthermore, at the time of the tracker’s launch, the use of seedboxes and VPNs for anonymous torrenting were exponentially in vogue (as previously discussed), and thus perhaps from a userland perspective there was little reason to use a slower Tor-based mechanism for content acquisition rather than streamlined and fast dedicated remote torrenting servers.

As Pyka and Saviotti point out with regard to entry barriers, there are “increasing returns to adoption which often tend to favor incumbents with respect to late entrants”<sup>674</sup>. Considering that this was the first known Tor-based BitTorrent tracker, and particularly as public familiarity with Tor’s Onionland may have drastically increased as of late with Facebook’s launch of their own onion site<sup>675</sup>, future iterations of similar projects may thus prove to be more successful, assuming of course that Pyka and Saviotti’s economic development schema has any relevance for the project at hand, considering that this undertaking was indeed not a Schumpeterian one.

Thus, though economic explanations may be ‘mapped’ onto the resultant situation, they cannot explain it due to the simple fact that the tracker was not a business, and its userbase was not a customer base. Barriers to entry, as such, were thus merely technological, and entry itself was to a free domain, not into a competitive business environment. Thus we

---

<sup>674</sup> Pier Paolo Saviotti and Andreas Pyka. 2011. “Generalized Barriers to Entry and Economic Development”, in *Catching Up, Spillovers and Innovation Networks in a Schumpeterian Perspective* (eds. Andreas Pyka and Maria da Graça Derengowski Fonseca). London: Springer-Verlag. pp. 59-80 (p. 60).

<sup>675</sup> Tom Fox-Brewster. 2014. “Facebook opens up to anonymous Tor users with .onion address”. *The Guardian*. <http://www.theguardian.com/technology/2014/oct/31/facebook-anonymous-tor-users-onion>.

can appropriate Pyka and Saviotti's schema, whilst keeping it divorced from any underlying economics.

The 'barrier to entry', or simply 'accessibility', from the serverland perspective was unexpectedly encountered via fellow-tracker censorship. Notices of the tracker's existence were placed on the forums of five existent public and private web-facing torrent trackers. Four of the five trackers deleted the announcement within a few days. Whilst the reasons for deletion were never formerly enunciated, they may perhaps relate to the actual advertised content of the tracker. Designed to be an unfettered, unbridled formulation, there were no rule restrictions placed on any manner of content that could be uploaded. Indeed, in general terms content which would potentially be deleted from other locales was actively encouraged, with the original announcement describing the site as

a home for the The Dispossessed. A tracker for torrents banned from other sites, but where no content is ever banned; where there are no administrators, no truth, and everything is permissible. A place for us space puppies, insane and bitter, to spend our nights plotting vengeance against the earth puppies who live such idyllic lives in comfortable pens, free from the horror of being devoured.

[...]

If you thirst for content that's verboten elsewhere, crave a locale from which no one can remove you, then give the ol' Grotto a visit<sup>676</sup>.

Refer to Appendix 6: 'Sample User Responses to Space Puppy Grotto Notice Postings' for a listing of user responses elicited via the aforementioned notice postings about SPG on five torrent communities. Of the 16 responses: 11 expressed a lack of interest in the topic—with the tone of the expressed lack of interest ranging from "[d]oesn't sound like it's my cup o' tea but good luck with it nonetheless", to "[m]otherfuck off"; three expressed reservations about using Tor; two went so far as to urge moderators to delete the notice postings; and two expressed interest. Thus the main hurdle appears to be garnering user interest in the project.

#### *4.2.1.1 Personal Content Preference Factors*

Some comments expressed reservation about the possible presence of crush videos on SPG. Within the subcultural spiral which formulates any domain of fetishism, with the extremity rising in proportion to the depth of the spiral, there exists a paraphilia known as crush fetishism, in which arousal is achieved through the crushing of various objects, for

---

<sup>676</sup> [http://\\*](http://*).

instance grapes or miniature cities (the latter at times dove-tailing with macrophilia)<sup>677</sup>. Within the crush fetish community there is a further sub-community which emphasizes the crushing of living creatures such as insects and crustaceans<sup>678</sup>. Going further down the spiral, however, one finds crush fetishists interested in what is termed ‘hard crush’, or the crushing of living mammals such as mice and larger animals<sup>679</sup>. Crush is an obscure paraphilia that often receives not more than a passing mention in texts devoted to unusual sexual proclivities<sup>680</sup>, when it is not ignored entirely<sup>681</sup>. Thus it is notable that out of 16 comment responses, two demonstrated knowledge of the activity, thus signifying that even notices in communities where a generally-obscure term may be known, may not be sympathetic to the subject matter, due of course to the fact that knowledge is not automatically equated with acquiescence.

#### 4.2.1.2 Privacy Factors

An additional factor to consider may be that potential privacy concerns may have deterred potential user adoption. There exists an array of studies outlining potential attacks against Tor-routed BitTorrent usage<sup>682</sup>, though the self-proclaimed<sup>683</sup> first foray into the field of investigating de-anonymizing user information leakage over BitTorrent usage over Tor is the work by Manils et al<sup>684</sup>. Manils et al. present three attacks for harvesting potentially de-

---

<sup>677</sup> Mark Griffiths. 2012. “Trample Leaning: A Beginner’s Guide to Crush Fetishism”. *drmarkgriffiths*. <https://drmarkgriffiths.wordpress.com/2012/05/17/trample-leaning-a-beginners-guide-to-crush-fetishism/>.

<sup>678</sup> Jeremy Biles. 2004. “I, Insect, or Bataille and the Crush Freaks”, in *Janus Head: Journal of Interdisciplinary Studies in Literature, Continental Philosophy, Phenomenological Psychology, and the Arts* 7 (1). pp. 115-131 (p. 116). <http://www.janushead.org/7-1/biles.pdf>.

<sup>679</sup> *Ibid.*, p. 128.

<sup>680</sup> E.g., Aggrawal’s compendium of ‘unusual sexual practices’ only mentions crush fetishism in an appendix, merely providing a curt definition: “[s]exual arousal from seeing small creatures being crushed by members of the opposite sex, or being crushed oneself” (Anil Aggrawal. 2009. *Forensic and Medico-legal Aspects of Sexual Crimes and Unusual Sexual Practices*. Boca Raton, FL: CRC Press. p. 373).

<sup>681</sup> E.g., Eskapa’s *Bizarre Sex*, billed on the back cover as being a “comprehensive overview” of “sexuality through its more bizarre manifestations” with “hundreds of case studies”, makes no mention of crush (Roy Eskapa. 1987. *Bizarre Sex*. London: Grafton Books).

<sup>682</sup> See, e.g., Stevens Le Blond, Pere Manils, Abdelberi Chaabane, Mohamed Ali Kaafar, Arnaud Legout, Claude Castellucia, Walid Dabbous. 2010. “De-anonymizing BitTorrent Users on Tor”. *7th USENIX Symposium on Network Design and Implementation (NSDI’10)*. [https://hal.inria.fr/inria-00471177/document](https://hal.inria.fr/inria-00471177/document;).; Stevens Le Blond, Pere Manils, Abdelberi Chaabane, Mohamed Ali Kaafar, Claude Castellucia, Arnaud Legout, Walid Dabbous. 2011. “One Bad Apple Spoils the Bunch: Exploiting P2P Applications to Trace and Profile Tor Users”. arXiv preprint; arXiv:1103.1518. <http://arxiv.org/abs/1103.1518>.; Aaron Johnson, Chris Wacek, Rob Jansen, Micah Sherr, Paul Syverson. 2013. “Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries”, in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. <http://www.cryptome.org/2013/08/tor-users-routed.pdf>.

<sup>683</sup> “no studies have been conducted on the way BitTorrent may leak the identity of users when the application is running over an anonymizing network” (Pere Manils, Abdelberi Chaabane, Stevens Le Blond, Mohamed Ali Kaafar, Claude Castellucia, Arnaud Legout, Walid Dabbous. 2010. “Compromising Tor Anonymity: Exploiting P2P Information Leakage”. arXiv preprint; arXiv:1004.1461. <http://arxiv.org/pdf/1004.1461>. p. 1).

<sup>684</sup> *Ibid.*



anonymizing information leakage over BitTorrent via Tor which are predicated on an adversary controlling any number of Tor exit nodes; the attacks are 1) collecting peer IP addresses from the custom client-sent tracker announce URL, 2) collecting peer IP addresses via hijacking tracker responses to include the adversary as the first endpoint in a swarm, and 3) collecting peer IP addresses via DHT by performing `get_peers` requests to identifying IP addresses corresponding to unique port numbers. The knowledge of the existence of said attacks may cumulatively or singularly deter user adoption of a Tor-based BitTorrent tracker such as SPG. To mitigate said potential user averseness to the use of the experimental SPG tracker, we can examine each one and present potential counter-measures that would neutralize the attacks proposed by Manils et al., whilst also presenting practical specifications of how a sample BitTorrent client may be setup to further protect users.

*Attack #1:* The first attack present by Manils et al. seeks to obtain “the IP of a BitTorrent user simply by looking at the IP field contained in the BitTorrent control messages”<sup>685</sup>. The BitTorrent protocol allows for an optional `ip` parameter which relays “[t]he true IP address of the client machine”<sup>686</sup> to the tracker via appending the parameter to the announce URL. Thus, if a user has configured their BitTorrent client to use Tor, but is unaware that their client may also be sending their actual IP to the tracker (albeit over Tor) via the `ip` parameter, an adversary who controls an exit node may see the announce URLs passing through it and may in turn discover the real IP of a torrent user.

*Countermeasure #1:* Given that the alleged IP address of a BitTorrent user may be passed along as a parameter appended to the tracker announce URL, may the parameter value perhaps be susceptible to user modification? Manils et al. explicitly identify  $\mu$ Torrent as one particularly vulnerable client (alongside BitSpirit and libTorrent) engaged in “constantly embedding public IP addresses”<sup>687</sup> (presumably in the afore-discussed tracker announce URLs). Manils et al. do not state which particular version of  $\mu$ Torrent engages in said behavior. Manils et al. conducted their surveillance over a period of 23 days, “[f]rom January 15 to February 7<sup>th</sup>”<sup>688</sup>. Manils et al. further do not state year their attacks were conducted or otherwise tested. Given that the arXiv submission date for said Manils et al. article is April 9<sup>th</sup> 2010, for the purposes of the counter-measure scenario it will be assumed that the aforementioned 23-day period likewise transpired in 2010. Assuming then that 1) Manils et

---

<sup>685</sup> *Ibid.*, p. 3.

<sup>686</sup> “Tracker HTTP/HTTPS Protocol”, *Bittorrent Protocol Specification v1.0. op. cit.*

<sup>687</sup> Manils et al., *op. cit.*, p. 3.

<sup>688</sup> Manils et al., *op. cit.*, p. 3.

al. conducted their surveillance in 2010; 2) Manils et al. used the latest version of  $\mu$ Torrent available at the time; and 3) Manils et al. used a Windows version of  $\mu$ Torrent<sup>689</sup>, it would then appear that Manils et al. deemed  $\mu$ Torrent v. 1.8.3 to be the vulnerable version of the client, as said version was released on 2009 June 13<sup>690</sup>, with the subsequent version, 1.8.4, only being released on 2009 August 12<sup>691</sup>. Thus we can use the version potentially used by Manils et al. to explore possible counter-attack techniques, as even if Manils et al. did not use said version<sup>692</sup>, privacy-conscious users may nonetheless use it themselves regardless as if it is proven that said version can be configured to successfully foil the attacks proposed by Manils et al then for the purpose of the counter-attacks it ultimately does not matter if Manils et al did in fact use a given version or not (though it may matter by impacting the potential reproducibility of the attack susceptibilities described by Manils et al.).

Opening  $\mu$ Torrent v. 1.8.3<sup>693</sup> and proceeding to Preferences, and selecting the BitTorrent section, we see that there is an available field which states “IP/Hostname to report to tracker:”, followed by an empty entry in which we can type a parameter value. Thus, one could simply input an IP other than one’s own in said field to successfully counter the first attack proposed by Manils et al., who do acknowledge that they have “not checked the authenticity of the public IP address”<sup>694</sup> that they have found via monitoring the ip parameter of tracker announce URLs.

*Attack #2:* The second attack exploiting BitTorrent information leakage to de-anonymize Tor/BitTorrent users proposed by Manils et al. centers around a man-in-the-middle technique in which tracker responses are hijacked by the rogue exit node to inject an attacker into the list of peers returned by the tracker to the target, with the attacker being the first endpoint in the peerlist, and the result thus being that if the target only uses Tor for tracker and not peer communications, the attacker will now find the target’s non-Tor IP (what Manils et al. call a “public IP”)<sup>695</sup>.

---

<sup>689</sup> As most other applications utilized in this research are Windows-based, in the absence of any available contrasting evidence from the Manils et al. study, we will similarly be using a Windows-based version of  $\mu$ Torrent.

<sup>690</sup> Oldversion.com. “Download Old Versions of uTorrent for Windows”. *OldVersion.com*. <http://www.oldversion.com/windows/utorrent/>.

<sup>691</sup> *Ibid.* N.B. Intermittent beta version release dates (e.g.  $\mu$ Torrent 1.8.3 Beta 14715) are not available.

<sup>692</sup> Owing to a lack of presented documentation of which versions of the software are explicitly vulnerable to their attacks, it does not appear to be possible to discern with any certainty which specific version(s) of  $\mu$ Torrent Manils et al. employed in their attack testing. This is significant as it potentially brings into question the ability of subsequent researchers to reproduce the attack susceptibilities described by Manils et al.

<sup>693</sup> BitTorrent, Inc. 2009.  $\mu$ Torrent v. 1.8.3. <http://www.oldversion.com/windows/utorrent-1-8-3>.

<sup>694</sup> Manils et al., *op. cit.*, p. 3.

<sup>695</sup> Manils et al., *op. cit.*, p. 4.

*Countermeasure #2:* The counter-attack to the second attack is self-evident from the conditional clause caveat presented by Manils et al. in their postulation of the attack itself—*viz.* “If Alice uses Tor only to connect to the tracker, but not to connect to peers, then Bob will see Alice’s public IP address”<sup>696</sup>. In other words, privacy-conscious BitTorrent-over-Tor users could use Tor not only for tracker communication, but for peer communication as well. In  $\mu$ Torrent v. 1.8.3 this is accomplished by going to Preferences, selecting the Connection section, and checking the “Use proxy server for peer-to-peer connections” box. Rogue peers will thus not be able to detect the target’s public IP address, as peer communications will be redirected via Tor as well as tracker communications in this instance.

*Attack #3:* The third attack proposed by Manils et al. pivots around the fact that Tor only serves to anonymize TCP/IP, and not UDP, traffic, with the latter being used by the DHT feature of the BitTorrent protocol. Thus even if a target uses Tor to connect to both the tracker and to other peers, if the target has DHT enabled in the client, an attacker may lookup the target’s public IP via performing `get_peers` requests in the DHT until an endpoint entry with a port matching the associated Tor IP in the swarm is found<sup>697</sup>.

*Countermeasure #3:* The first counter-measure is to use a less-unique port, as Manils et al. state that they “exclude ports 80, 443, 6881, 16884, 35691, and 51413 that are more popular than others”<sup>698</sup> from their attack. The listening port may be changed in  $\mu$ Torrent v. 1.8.3 by going to Preferences, selecting the Connection section, and in the “Port used for incoming connections” field within the Listening Port box, inputting one of the more popular excluded ports conveniently delineated by Manils et al., thus countering their operative assumption that “listening port numbers [are] a good identifier within a torrent”<sup>699</sup>. That is to say, if the presence of a unique port used for the BitTorrent client may allow an attack to correlate the target’s Tor IP to their public IP (e.g. if an attacker sees *tor.ip:64039* in the tracker peerlist and via the IP reported by the client, as per the aforementioned attack 1 and 2 countermeasures, but still sees *public.ip:64039* in the DHT, the attacker may assume that the two IPs are related due to the presumed uniqueness of the operative port, 64039); if multiple peers use the same port, said correlation would become more difficult.

Going further however, one may also entirely disable DHT by proceeding to Preferences, selecting the BitTorrent section, and unchecking the ‘Enable DHT Network’

---

<sup>696</sup> *Ibid.*

<sup>697</sup> *Ibid.*

<sup>698</sup> *Ibid.*

<sup>699</sup> *Ibid.*

box (one may additionally, though not necessarily, also uncheck the ‘Enable DHT for new torrents’, ‘Enable Local Peer Discovery’, and ‘Enable Peer Exchange’ boxes), thus disabling the UDP-based attack on BitTorrent Tor users. The downside of said countermeasure would of course be that, with DHT disabled, the user would be reliant on the tracker staying up to be able to successfully connect to peers. An alternative countermeasure would be to use a VPN service, though such services of course come with their own anonymization concerns, as discussed previously in section 4.0.0.

*Additional Threat:* Aside from the three aforementioned BitTorrent/Tor user deanonymization attacks, Manils et al. also describe a potentially deanonymizing ‘domino effect’<sup>700</sup>, which notes that given that Tor uses a single circuit for multiple streams, an attacker controlling a rogue exit node may be able to observe all related user activity (e.g. both using BitTorrent and checking email) originating from the same circuit. Thus, if a target is using Tor both for BitTorrent and for browsing their personal plaintext (unencrypted) email, and the email message contains personally-identifiable information, then the attacker will be able to associate the BitTorrent user with said information. If the same ip:port combination are found by the rogue exit node monitoring attacker in a latter circuit, then both the streams within a circuit (the “intra-circuit domino effect”) and other circuits (the “inter-circuit domino effect”) may be linked to the target, increasing the target profile visible by the attacker.

*Additional Countermeasure:* Given the risk of an attacker building up potentially deanonymizing user profiles, the primary countermeasure to said threat is to not use Tor for more than one purpose at a time: thus while running BitTorrent over Tor, one must not also, for instance, be browsing the web over Tor. The Tor Project further proposes two potential technical countermeasures that future versions of Tor may implement<sup>701</sup>, including making circuit-creation be application-dependent (with each application using a new Tor circuit), or making stream-compartmentalization be port-dependent (with traffic from each port being on separate streams on different circuits).

Although each of the aforementioned attacks proposed by Manils et al. can thus be countered in the respective afore-delineated manners, the ideal BitTorrent client would of course have the aforementioned properties—‘IP to report’ set to reflect an IP not belonging to the target, ‘use proxy for peer-to-peer connections’ enabled, listening port assigned to a

---

<sup>700</sup> Manils et al., *op.cit.*, p. 5.

<sup>701</sup> arma. 2010. “Bittorrent over Tor isn't a good idea”. *The Tor Blog*. <https://blog.torproject.org/blog/bittorrent-over-tor-isnt-good-idea>.

commonly used port, and DHT disabled—configured by default, and not require the user to comb through the preferences to enable non-obvious privacy enhancement features. Manils et al. further repeatedly<sup>702</sup> point to the lack of authentication and encryption in the BitTorrent protocol as being a contributing factor to the success rates of their proposed attacks. A possible step towards mitigating said threat would be to use HTTPS, as opposed to HTTP, torrent trackers, although that would of course open up the target to additional man-in-the-middle HTTPS-based attacks, such as Tor exit nodes injecting false certificates<sup>703</sup>. Tracker peerlists could likewise be signed by the tracker, though they too could likewise be susceptible to forgery (with the attacker likewise being able to at times become an organic peer versus using peer injection and still potentially connecting to the target in the given torrent swarm). Though tracker-side security implementations of course assume that the attacker is not operating or otherwise has control of the tracker itself, which would of course make said protective measures useless. While Manils et al. acknowledge that “a solution consisting in end-to-end encryption and authentication in BitTorrent might countermeasure our attacks”<sup>704</sup>, they nonetheless go on to state that “we believe this would be a costly solution for trackers to implement, and would induce higher latencies into BitTorrent connections. These non desirable properties such solution exhibits would certainly make heavy downloaders and content providers reluctant to adopt it”<sup>705</sup>. Manils et al. do not, however, present any actual evidence to substantiate their assertion that heavy users would be reluctant to adopt said features due to the higher latency. Indeed, it stands to reason that the converse may hold just as well, in that the privacy-strengthening characteristics of said features may override latency-based barriers. The latter counter-assertion may be further buttressed by the fact that configuring BitTorrent to run over Tor in the first place already requires an additional level of effort and introduces greater latency; thus, if privacy-conscious users are already willing to setup such a connection, they may be further willing to strengthen it via the deployment of additional encryption solutions.

More recent attacks against BitTorrent-over-Tor users have emphasized that such users are more highly susceptible to traffic correlation attacks (in which an adversary can monitor both incoming and outgoing traffic in the Tor network) than Tor users who generally

---

<sup>702</sup> *Ibid.*, p. 2, 4.

<sup>703</sup> cypherpunks. 2013. “Bad russian exit node attacks connections to Wikipedia”. *Tor Bug Tracker & Wiki*. <https://trac.torproject.org/projects/tor/ticket/8657>.

<sup>704</sup> Manils et al., *op. cit.*, p. 9.

<sup>705</sup> *Ibid.*

do not use BitTorrent over Tor<sup>706</sup>. As the Tor Project has repeatedly<sup>707</sup> emphasized, Tor's threat model emphasizes trying to "to decrease the chances that an adversary will end up in the right positions to see the traffic flows"<sup>708</sup>, not protecting against traffic correlation should an adversary end up in the right positions. However, as Johnson et al. point out, a contributory reason for why BitTorrent-over-Tor users may be more susceptible to traffic correlation attacks than users who do not use BitTorrent over Tor, may be that a number of Tor exit nodes block ports used by BitTorrent applications, thus "enabling the malicious exit to provide a larger fraction of that bandwidth"<sup>709</sup>. In other words, if one of the aims of the Tor Project are indeed to decrease the chances of adverse positioning, and if restricting certain ports is adversarial to said aims as it forces BitTorrent-over-Tor users to use a smaller percentage of available exit nodes, then it stands to reason that from an anonymity perspective as emphasized in the Tor Project's own material, exit node policies which block particular ports should be done away with to greater facilitate user anonymity, as such polices are both damaging to the anonymity of certain Tor users. An ideal anonymity-centered filesharing application would first of all thus take user anonymity seriously from the application layer, taking care not to leak a user's non-anonymized IP to other entities in the network. The network would further not restrict the use of particular ports and, if the anonymization service exists over a broader network, as opposed to specific application, layer, the service should then take care not to facilitate the contamination of inter-application identities by privileging strict compartmentalization of services (e.g. with different application streams appearing on different circuits). Said ideal implementations may assuage user worries of deanonymization and may in turn facilitate wider adoption.

#### 4.2.2 Concluding Remarks

While the infrastructure of the torrent tracker stacked on a Tor hidden service still exists, it remains in a state of disuse. Occasional comments are left on the existent torrents, asking for seeders for the files. There then is evidence of a continued trickle of interest. Yet, in true PAR fashion, it must also be recalled that change cannot be forced, and thus not only will individual users need to switch to Tor usage of their own accord, but other tracker administrators will also need to switch to Tor for themselves. The existence of the tracker

---

<sup>706</sup> See, e.g., Johnson, et al., *op. cit.*

<sup>707</sup> See also arma. 2014a. "Traffic correlation using netflows". *The Tor Blog*.  
<https://blog.torproject.org/blog/traffic-correlation-using-netflows>.

<sup>708</sup> arma. 2009. "One cell is enough to break Tor's anonymity". *The Tor Blog*.  
<https://blog.torproject.org/blog/one-cell-enough>.

<sup>709</sup> Johnson et al., *op. cit.*, p. 7.

alone however is itself proof of concept that it is indeed technologically feasible to run a Tor-based torrent tracker, if not yet particularly widely adopted. For now, however, Tor can of course still be readily used to protect those in userland, whilst existent tracker administrators can mitigate their own risk factor by masking their registration identity when registering the tracker websites, accepting and paying funds via cryptocurrencies, and using off-shore hosting providers which are not affected by corporate IP interests.

The cumulative findings of all of the explorations in this Ordinance thus seem to reveal that there is no singular crystallization of an ideal distributive strategy for data dissemination; instead, there are a myriad potent potentialities of distribution vectors, each coming with their own snares and entanglements affecting the various user, server and filelands which they constitute and intersect, all coming complete with a multiplicity of security and (de)anonymization concerns, as well as various counter-measures thereto in our by now all too familiar game of forensic apprehension and counter-forensic evasion (as intersecting with aforesaid illegalist and non-legalist maneuvering). What has further been demonstrated is that it would be a mistake to consider the various file sharing ecosystems as discrete entities, for as our Tor torrent tracker elucidated it is possible to stack various services together in attempts to strengthen the security of the underlying data dissemination. Data flow, constantly undergoing an on-going polymorphism, existing betwixt stationary sites, cannot be reduced and congealed to a singular technical implementation. Thusly there is no one grand file sharing permanent autonomous zone, there exist instead a myriad of potentialities for promulgation.

**5.**

## **Concluding Remarks: On the Copyfight**



This project undertook a critical examination of the potentialities of unbridled data dissemination via a close counter-forensic exploration and attempted neutralization of the various existent and emerging legal and technical content control fetters. Through the conduction of various case studies it was found that there exist persistent juridical as well as technical modes of data congealment which seek to hamper the unrestricted flow of information born of cultural production. Specifically, analyses were performed of how academic e-book and journal publishers enact various techniques of content distribution restriction in the form of textual watermarking technologies. Similarly, cinematic film distributors were likewise found to deploy audio-visual watermarks to aid in future attempts at traitor tracing and source neutralization by seeking to identify and subsequently prosecute whoever assisted in facilitating the unbridled distribution of said cultural products.

However, the results of the case studies further revealed that the content control mechanisms that were analyzed are not impermeable, but are instead highly susceptible to emancipato-surgical strategies of content liberation. The case studies demonstrate that once the watermarking technologies are identified they may be successfully excised and the content distributed with reduced fear of reprisal from content owners. A final case study then setup an experimental distribution network for said content via a Tor-based bittorrent server. Whilst the server was (and continues to be) operational, its adoption and continued usage by users was found to be minimal, thus elucidating that technological adaptation is void without wide-scale social deployment, and that information liberation cannot necessarily be congealed through a singular technological implementation. Prior to engaging in the aforementioned practice-based research, however, it will be recalled that this study initially commenced with the synthesis of an array of theoretical threads leading to the development of an operant hacker methodology. Let us then take a final look at how the said methodological framework permeated the case studies that ensued, examine the broader cultural implications of the outcomes of said cases, whilst keeping in mind the limits inherent in their potential wide-scale applicability so as to avoid any unwarranted claims of universalism, and finally look onwards to potential future developments.

The theoretical and methodological framework developed throughout this study can be summarized via three characterizations: it is identified by a disjunctive embedding, an ongoing polymorphism, and non-legalism. Let us then take a look at how this trio of characteristics which, when combined, formulate the resultant hacker methodology have manifested themselves throughout this project.

## **5.0 Disjunctive Embedding**

Participatory Action Research lays bare the always-already situatedness of the researcher within the focal areas being researched, with the site of study and the researcher thus being intertwined in a “co-creative dance”<sup>710</sup> which in turn gives rise to new situational formulations by virtue of the researcher’s inherent participation and co-creation of the newly emergent circumstance. In other words, situatedness gives rise to the formation of new situations. Foucault makes a similar point through his explication that the specificity of the situated intellectual is linked to the surrounding localized truth formation<sup>711</sup>, to not mere presence-in but active construction-of the network circuitry any actants may find themselves in. The realization of the existent embedding then, replacing any notions of unbiased detachment, in turn give rise to a conscious participation in the co-created field of operation. The manifestation of embedding may however initially appear to be disempowering and immobilizing, with the ensuing realization that the integrated circuit is marked as much as it is by the “informatics of domination”<sup>712</sup>, with actants being soldered in place on a highly regimented circuit board of content congealment.

Following this study’s initial bringing to the fore of various latent watermarking technologies, as explicated through their existence in books, journal articles, and films, it may be all too easy to conclude that these intricate forensic marking schemas render any unauthorized mode of distribution unfeasible, due to the possibility of traceability and source neutralization. In other words, the realization that there are a myriad of intricacies and redundancies built into systems of content control may lead one to conclude that it’s then safest of all to simply not share. Yet as Haraway goes on to point out, “if we learn how to read these webs of power and social life, we might learn new couplings, new coalitions”<sup>713</sup>. Realization of embedding is thus merely the first step, to be followed by detailed expatiation of the surrounding circumstances and operant mechanics one finds oneself enmeshed in, and finally by potent disjunction. As Deleuze suggests, “the key thing may be to create vacuoles of noncommunication, circuit breakers, so we can elude control”<sup>714</sup>. Hence, whilst this project certainly started out from a mere delineation of the various operant machinations of content control via an analysis of existent patent literature, whitepapers, and existent forensic

---

<sup>710</sup> Reason and Bradbury, *op. cit.* p. 8.

<sup>711</sup> Foucault, “Truth and Power”, *op. cit.* p. 132.

<sup>712</sup> Haraway, “A Cyborg Manifesto”, *op. cit.*

<sup>713</sup> *Ibid.*

<sup>714</sup> Deleuze and Negri, *op. cit.*

research on variant textual, audio, and visual watermarking and fingerprinting procedures, it then proceeded from explication of its embeddedness to disjunctive dissonance therefrom.

The hacker methodology calls for active *disruptive* participation in embedded systems of control, in the utilization of a soldering iron to actively modify the existent integrated circuit via praxis. Thus this project proceeded to exploit existent techniques of content control via the development of practical counter-forensic techniques of content liberation through the leveraging of discovered exploits in said content control mechanisms. Watermarking techniques and copyright licenses were not merely delineated and analyzed, but were actively subjugated to modification and neutralization via a participatory manifestation of a disjunctive embedding which sought to explore the possibilities of leveraging one's situatedness to affect the creation of antiprograms which would actively be disruptive to processes of content congealment.

### **5.1 On-going Polymorphism**

The hacker method is further marked by viral mutation which avoids identification and neutralization through its eschewal of stasis; termed *viral* due to its discovery, exploitation and escalation of vulnerabilities in existent systems, evading capture by shifting its operating tactics in response to, and anticipation of, the underlying processes of command and control enacted by content congealers. Recall that for Stirner, personalism is characterized by an hourly self-(re)creation<sup>715</sup>, and with the union of egoists avoiding the appropriation of being reduced to mere abstract conceptualization by always only being defined in terms of lived praxis—the union being not an abstract conceptualization, but an enacted particularity, mutating at each iteration. As Landstreicher points out, “the union of egoists is not a concept but a name used to refer to each of the particular instances of individuals acting together”<sup>716</sup>. Thus Stirner, when responding to misreadings of the union of egoists as existing on the abstract—albeit paradoxically thus consistently identifiable and vulnerable—plane of conceptualization, always only presents the union as manifested through discrete lived experiences, akin to a group of children deciding to play a game in the courtyard outside, encountering a group of friends and deciding to venture to a tavern, or perhaps falling in love<sup>717</sup>. However, whilst Stirner nonetheless remains mired in notions of the *discrete*—albeit pivotally not the human, recalling that for Stirner the egoist exists as a *monster*—union of *egoists*, Braidotti postulates the notion of figuration, “the expression of

---

<sup>715</sup> Stirner, “The False Principle of Our Education”, *op. cit.*

<sup>716</sup> Landstreicher, “Egoism Versus Modernity”, *op. cit.*

<sup>717</sup> Stirner, “Stirner’s Critics”, *op. cit.*

alternative representations of the subject as a dynamic non-unitary entity”<sup>718</sup>, which helps us advance the thesis of detection-avoidant imperceptibility via polymorphous subject-eschewal, the emphasis now being on process or movement, rather than stationary enclaves. Darting around the embedded circuit, the figuration of the hack operates via what Bey terms a guerrilla ontology, underlying immediatist imperative to “strike and run away. Keep moving the entire tribe, even if it’s only data in the Web”<sup>719</sup>. Thus whilst engaging in antiprogramming, in “seek[ing] to annul, destroy, subvert, circumvent a program of action”<sup>720</sup>, the hack likewise engages in an on-going process of becoming-imperceptible, of evading also-evolving anti-virus heuristics (in the form of content controllers in turn deploying counter-anti-forensics) via constant self-modification. PAR’s process of continual adjustment, of on-going questioning, reflection, and refinement<sup>721</sup>, is here employed in the services of an ever-developing hack. Thus, when in the case studies a particular method of content protection removal was found to no longer work, as for instance was the case with the inability to remove content protection from digitally rented ebooks in Twilynax’s catalogue, the procedure was modified to instead remove the content protection from the in-browser versions of the ebooks. Similarly, cropping techniques developed during the case study of journal watermarking are of course ineffective against metadata-based fingerprinting, and thus further counter-forensic techniques of metadata alteration were developed.

Likewise, whilst the Tor-based BitTorrent server was found to lack wide-scale adaptation by users, such an outcome of widespread usage was by no means necessary, and indeed may be advantageous in that the aim of its development was merely the presentation of an alternate mode of data distribution, as opposed to any pretense of presenting an idealized monopolization of a ‘preferred’ distribution channel. The torrent tracker case study thus sought to highlight the willingness to abandon, to move on to alternate forms of distribution whilst still making use of existent and emergent options. While the Space Puppy Grotto still remains operational, actual usage thereof by the userbase remains minimal; however, the option to employ it as a distribution mechanism thus nonetheless persists. The expatiation of the various diverse file sharing ecosystems in this study thus served to highlight the multifarious plurality of forms available for the content propagation. Much like the forensic watermarking techniques deployed by content controllers are continuously being

---

<sup>718</sup> Braidotti, *op. cit.*, p. 164.

<sup>719</sup> Bey, *T.A.Z.*, *op. cit.*

<sup>720</sup> Latour, “The Berlin Key”, *op. cit.*, p. 18.

<sup>721</sup> McIntyre, *op. cit.*, p. 7.

revised in the technical and patent literature, so too must it be kept in mind that counter-forensic methods mutate so as to minimize the risk to the broader project of wholesale data dissemination should one technique subsequently become inoperative. The underlying hacker method stresses a plurality of techniques, whilst providing a few discrete exemplary techniques to illustrate the divergent forms of available resistance and to likewise motivate the development of an even greater plurality of disjunctive antiprograms

## **5.2 Non-Legalism**

The third aspect of the hacker method developed throughout this study is that of a rejection of juridical limitations on praxis development, succinctly characterized by a “release from all authority”<sup>722</sup>. Stallman similarly summarizes the intersectionality of the given operant legal framework with a hacker method by noting that “hackers typically had little respect for the silly rules that administrators like to impose, so they looked for ways around”<sup>723</sup>. A similar, albeit more tacit, non-legalism is likewise found in PAR scholarship, as for instance any signification of a potentially-hampering legalism is absent in Borda and Rahman’s intonation that PAR researchers “know and recognize themselves as a means of creating people’s power, and the internal and external mechanisms of countervailing power”<sup>724</sup>. Throughout the variant case studies, this project has similarly highlighted that potential legal fetters must not serve as restrictions to conducting either practice-based research or the ensuing practices of unauthorized data dissemination. Indeed, the case studies may at time run counter to varying geospatial juridical fetters on particular modes of content promulgation, as for instance movie theaters at times have notices posted throughout their facilities highlighting the illegality of recording films. However, a non-legalist approach is not one that merely disregards legalistic impediment, for do so would potentially lead to apprehension via, for instance, content-owner utilization of traitor-tracing watermarking and fingerprinting algorithms. On the contrary, the case studies have instead gone to lengths to explicitly highlight the dangers of engaging in researching various forms of data congealment and have then gone on to provide knowledgeable best-practices for avoiding detection whilst maintaining the possibility of dissident engagement.

Lest the documentation of said case studies be potentially misread as evidence of actual transgression however, it is salient to once again highlight that all case material contained herein throughout the project is presented as mere potentiality, not as lived reality.

---

<sup>722</sup> Stirner, “The False Principle of Our Education”, *op. cit.*

<sup>723</sup> Stallman, “On Hacking”, *op. cit.*

<sup>724</sup> Fals-Borda and Rahman, *op. cit.*, p. 7.

The techniques and methods operate on a plane of hypothesis, not as recorded enactments of actually carried-out practices. Much like in our discussion of audio-visual cinematic watermarking a 2x2 Theoretical Watermarking Potentiality Matrix was developed, thus highlighting the fact that a given film only had the *potential* for being watermarked by content controllers, so too are modes of resistance to content congealment plausible but not necessarily enacted. Or in other words, the techniques could be implemented or carried out, but have not necessarily have been. The result of this study has thus been to demonstrate the existence of *imagined* modes of unbridled data flow via the explication of the various means of undoing content control measures.

### **5.3 Future Implications**

The techniques developed throughout this project are, of course, highly localized: focusing on uniquely discrete watermarking schematizations. As such, said techniques may of course not be immediately transferable to other areas of content restriction. For instance, Digital Rights Management is a broad field in its own right covering everything from audio, video, text and software to webpages and digital cartography<sup>725</sup>, employing more overt forms of content protection rather than the often transparent forms of watermarking techniques that have been discussed throughout this study. However, whilst the single techniques and procedures developed around specific case studies may not be immediately transferable, the broader hacker methodology may nonetheless have wider adoptability when applied to newly emergent problem sets. Given that one of the primary aims of said method is to bring to the fore latent modes of content restriction, future research may choose to examine ostensibly open systems of content distribution such as Open Access publishing mechanisms to expose any underlying fetters which may lie within, corralling content unseen, their operation shrouded by the rhetorics of seeming transparency and ready availability. Following exposure of such opacity, further work could in turn necessitate the postulation of neutralization techniques.

In the area of content distribution, recent crises regarding the potential compromise of the Tor network<sup>726</sup>, necessitate a detailed counter-forensic unpacking of the techniques deployed by law enforcement to potentially infiltrate and disrupt hidden services operating

---

<sup>725</sup> Information Resources Management Association. 2013. *Digital Rights Management: Concepts, Methodologies, Tools, and Applications*. Hershey, PA: IGI Global.

<sup>726</sup> See, e.g., arma. 2014. "Possible upcoming attempts to disable the Tor network". *The Tor Blog*. <https://blog.torproject.org/blog/possible-upcoming-attempts-disable-tor-network>; phobos. 2014. "Thoughts and Concerns about Operation Onymous". *The Tor Blog*. <https://blog.torproject.org/blog/thoughts-and-concerns-about-operation-onymous>.

via Tor so as to potentially develop resilient counter-measures or alternate modes of unbridled distribution altogether. As this study has illustrated, it may also be possible to concatenate various existent means of data promulgation via the linking together of seemingly divergent filesharing ecosystems so as to enact a hybridity of form that may be less susceptible to single-points of neutralization. The operant methodology developed throughout this study is intrinsically fault-tolerant in that the delineated methods are by no means definitive, but are instead built upon with constant reconstitution and refinement in mind, serving to highlight their adaptability and malleability to the analysis of emergent threats to unbridled data dissemination as the copyfight rages on. This project has presented certain points of engagement with variant content control mechanisms, other possibilities for the deployment of the framework to various sites of congealment via the deployment of a counter-forensic approach abound.

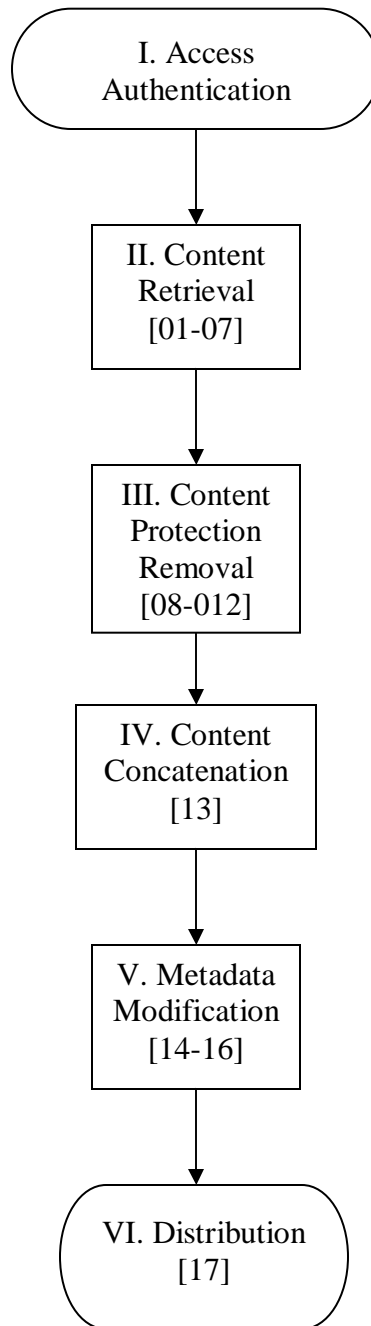
# **Appendix 1:**

## **Sample Procedure for Content Protection Removal from Twilynax eBooks**

This case study presents an illustrated and annotated workflow for removing content protection from a sample ebook from the ebook publisher/distributor Twilynax. Refer to §1.4.2 ‘Case Study 2: Hacking Away at Twilynax Publishing’ of the dissertation for analysis of the case study.

The general workflow schema can be visualized as follows (with accompanying procedural step numbers):





## I. Access Authentication

[00] Access the Twilynax ebook collection via passing through a series of login screens, ultimately using university-afforded authentication credentials through the appropriate institutional login portal.

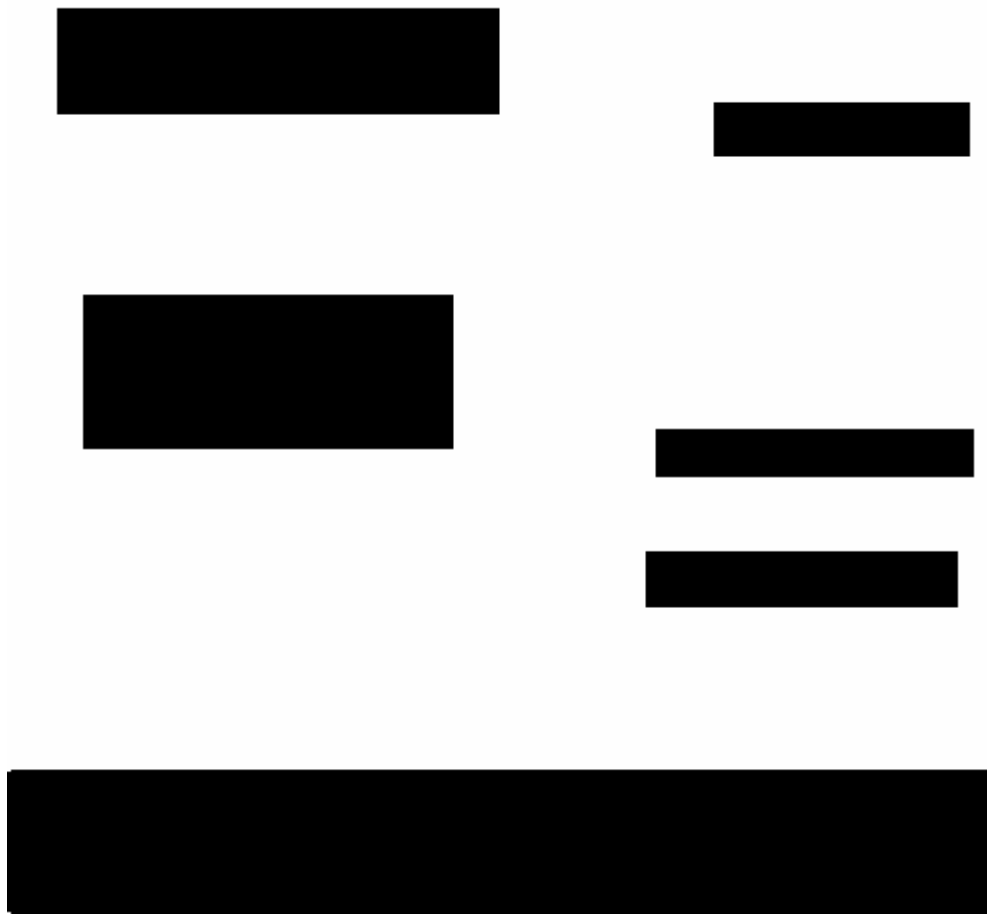
**Nota Bene:** The operative web browser used in the case study is Firefox<sup>727</sup>.

---

<sup>727</sup> Mozilla. 2014. Firefox. v. 33.1.1. <https://www.mozilla.org/firefox/new/>.



**Figure A1.00.0** Twilynax homepage<sup>728</sup>.



**Figure A1.00.1** Primary Twilynax login screen<sup>729</sup>, to be arrived at after selecting ‘Sign in’ on the Twilynax homepage, as seen in Figure A1.00.0.

---

<sup>728</sup> [https://\\*](https://*).

<sup>729</sup> [https://\\*/\\*/\\*](https://*/*/*).



**Figure A1.00.2** Secondary Twilynax login screen<sup>730</sup>, to be arrived at after selecting the appropriate institutional login portal on the primary login screen, as seen in Figure A1.00.1.



**Figure A1.00.3** Tertiary Twilynax login screen, to be arrived at after selecting the appropriate institution with which one has an account on the secondary login screen, as seen in Figure A1.00.2.

## II. Content Retrieval.

[01] Perform a title search query for an e-book.

---

<sup>730</sup> [https://\\*/\\*\\*/\\*\\*/](https://*/**/**/).



**Figure A1.01.0** Search query results for a sample ebook selection<sup>731</sup>.

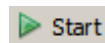
[02] Install, launch, and start the HttpFox add-on<sup>732</sup> for Firefox.



**Figure A1.02.0** Installation webpage for Httpfox.



**Figure A1.02.1** HttpFox launch button, as seen in the Firefox status bar.



**Figure A1.02.2** HttpFox start button, as seen in the HttpFox interface following the pressing of the HttpFox launch button in Figure A1.02.1.

<sup>731</sup> [https://\\*/\\*/?\\*=-\\*&\\*](https://*/*/?*=-*&*)

<sup>732</sup> Martin Theimer. 2014. HttpFox. v. 0.8.14. <https://addons.mozilla.org/firefox/addon/httpfox/>.

[03] Going back to Twilynax, select the Read Online option for the ebook.

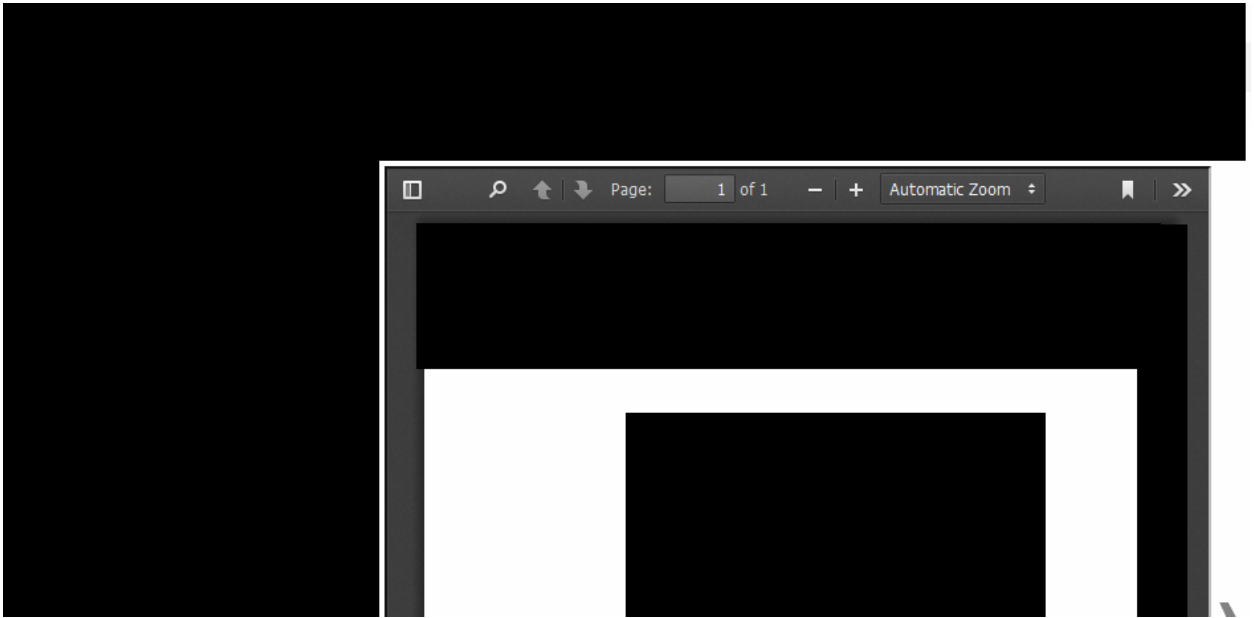


Figure A1.03.0 Read online option for the sample ebook selection<sup>733</sup>, to be arrived at after selecting the read online icon, as seen in Figure A1.01.0.

[04] Note the JSON and PDF filetypes in the HttpFox log following the loading of the online reader.

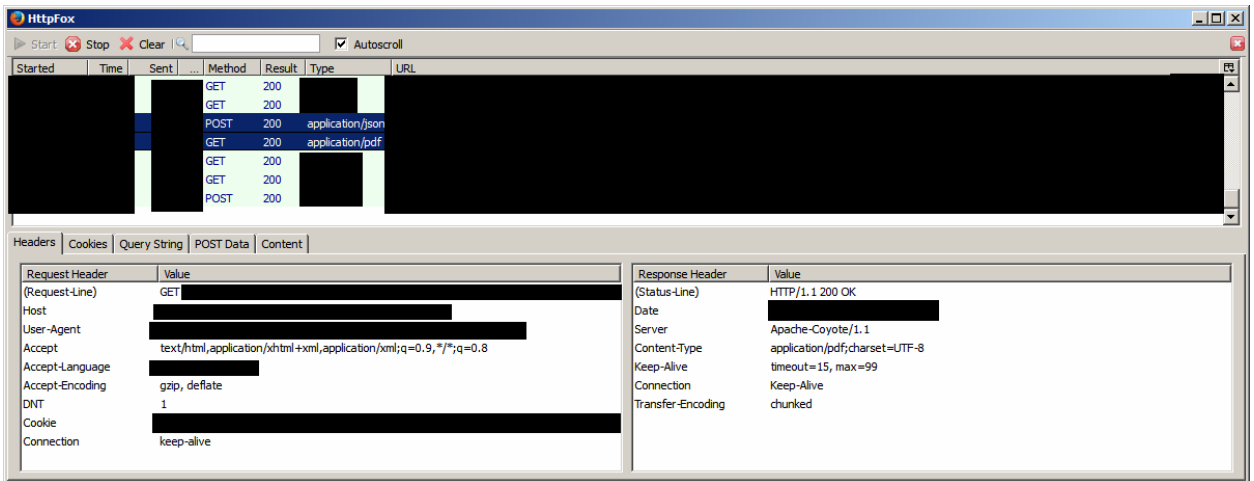


Figure A1.04.0 HttpFox log for the Twilynax online reader.

[05] Observe sample JSON file read-out:

<sup>733</sup> [https://\\*/\\*](https://*/*).

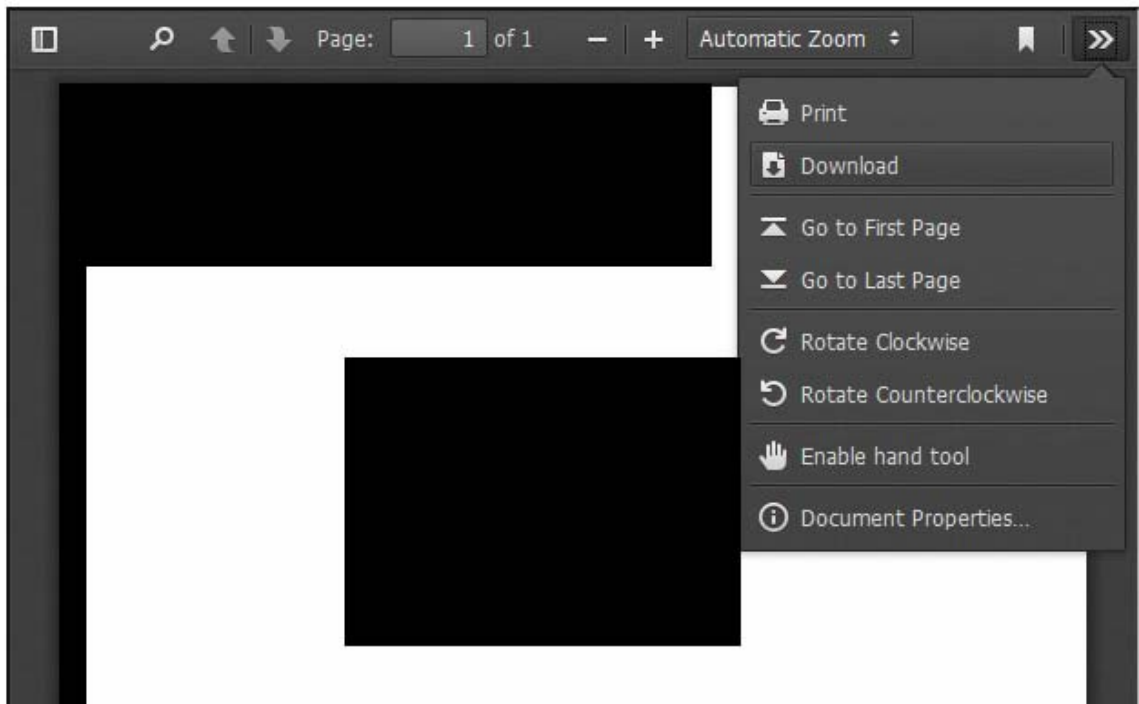
```
{ "page":1, "note":null, "pdfURL": "/pdf/191o4xroJlJjppOiW8?toolbar=0&st  
atusbar=0&scrollbar=0&messages=0&navpanes=0&view=Fit", "abuseDetected  
":false, "preview":false, "previewPageError":false, "previewTimeExpired  
":false, "adminPreviewExpiry":false, "autoPurchaseNoNoficiation":false  
, "bookAccessError":false, "mcaReadOnline":false, "pageInfo": { "copyEnab  
led":false, "printEnabled":false, "print":false, "page":1, "pdfPageRando  
mString": "191o1xroJlJjppOiW8" } }734
```

It can here be seen that Twilynax employs an 18-character A-Z, 0-9 string with variable capitalization for individual PDF page filenames (the variable pdfPageRandomString), hence preempting a sequence pattern downloading attack. However, the accompanying JSON files which include the necessary pdfURL parameter are sequentially numbered. While it is therefore possible to sequentially download all related JSON files for a particular e-book, subsequently parse them for the pdfURL parameters, and to then finally download the resulting list of PDF pages, a simpler alternative is to simply download the pages manually using the browser's built-in PDF viewer. Thus in this case, a manual approach is seen to be more efficient than automation.

**[06]** Select the download option in the Firefox PDF viewer whilst viewing a page from the book.

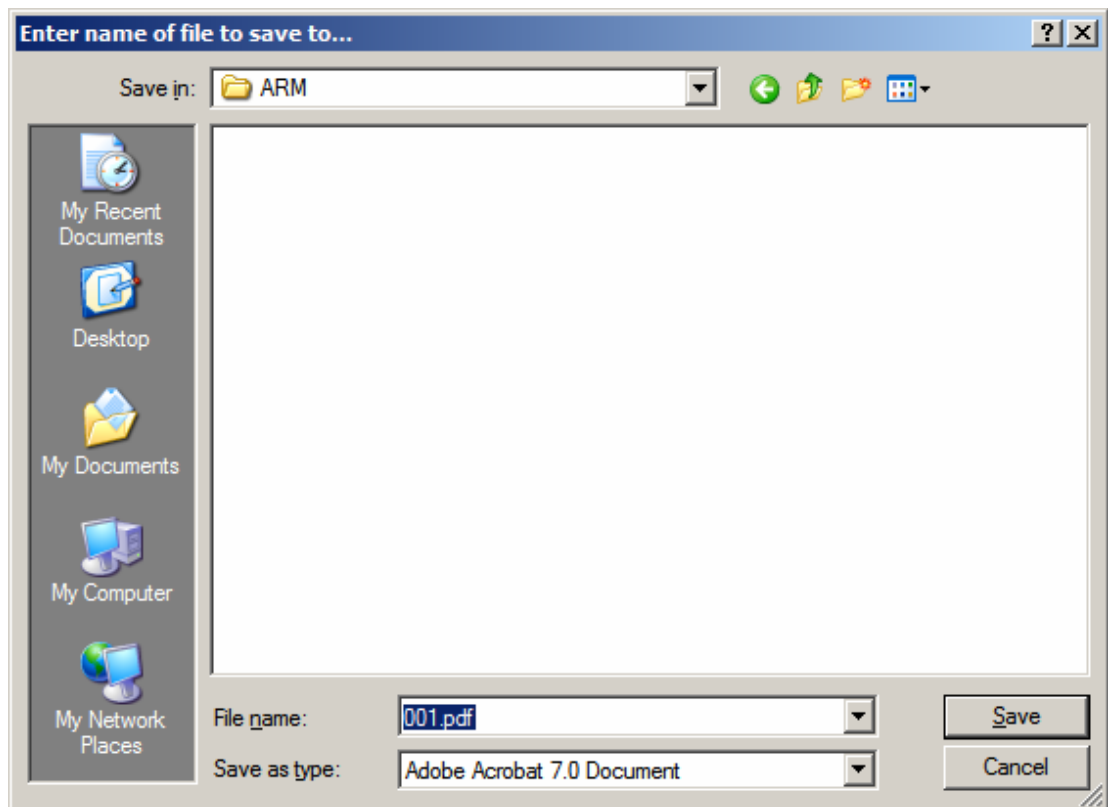
---

<sup>734</sup> [https://\\*/\\*/\\*/\\*](https://*/*/*/*).



**Figure A1.06.0** Firefox PDF viewer extended options panel.

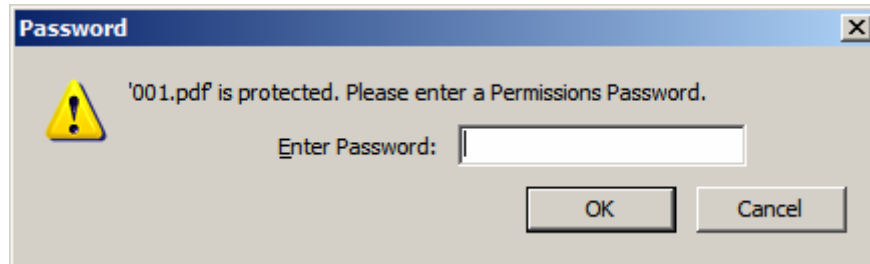
[07] Rename the default titled document.pdf to a sequential numbering scheme; e.g., 001.pdf.



**Figure A1.07.0** Firefox Save window.

### III. Content Protection Removal

[08] Following the successful downloading of all book pages, the next step is merging the pages into a single file. However, attempting to do so using any number of PDF merge tools results in a password prompt.



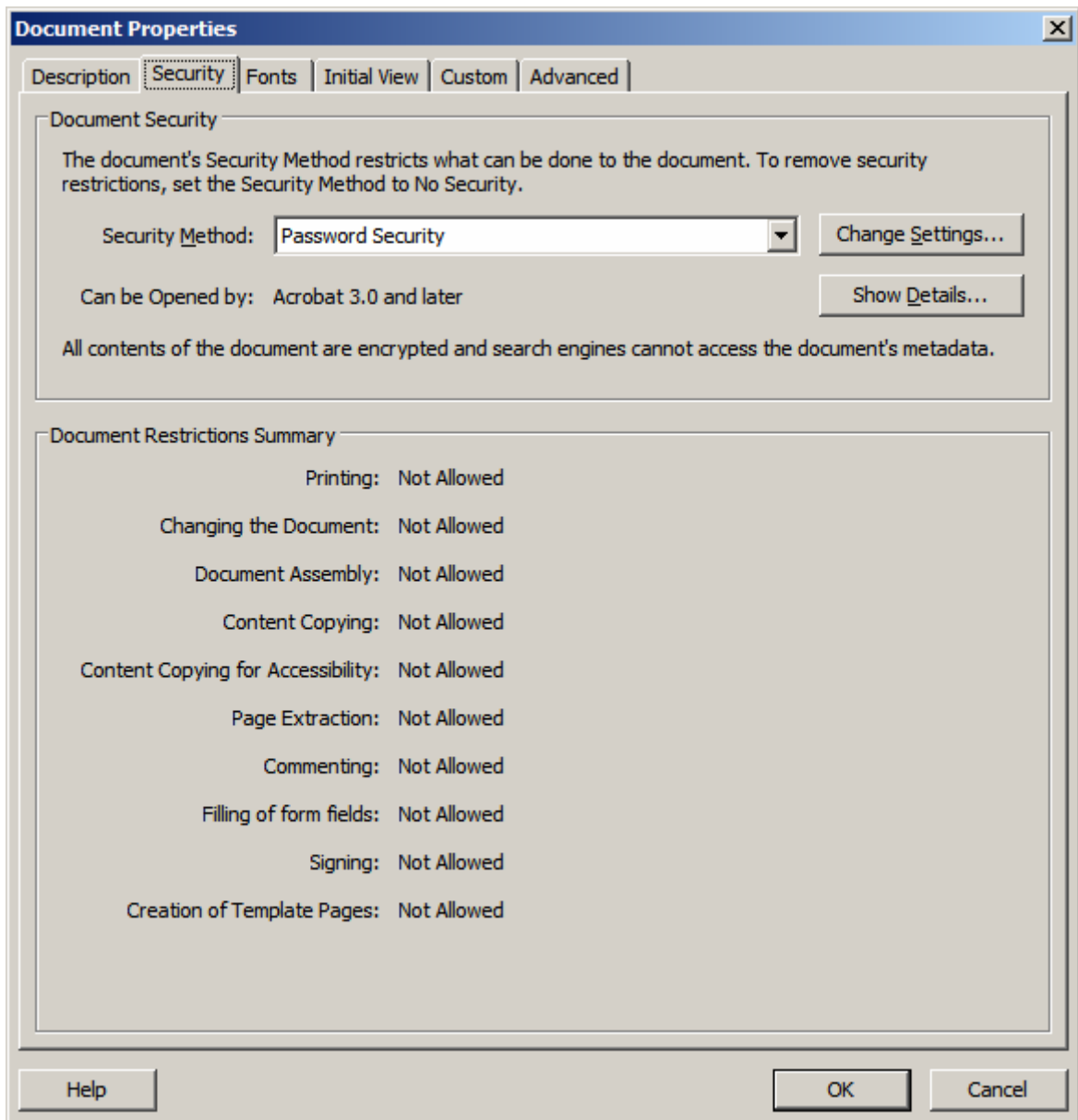
**Figure A1.08.0** PDF merge password prompt, as seen in Adobe Acrobat 8 Professional<sup>735</sup>.

[09] View the PDF document Security Settings in Adobe Acrobat to reveal existent content protection components of the PDF. This is achieved via the File menu, by selecting Properties and then further selecting the Security tab.

---

<sup>735</sup> Adobe Systems Incorporated, *op. cit.*

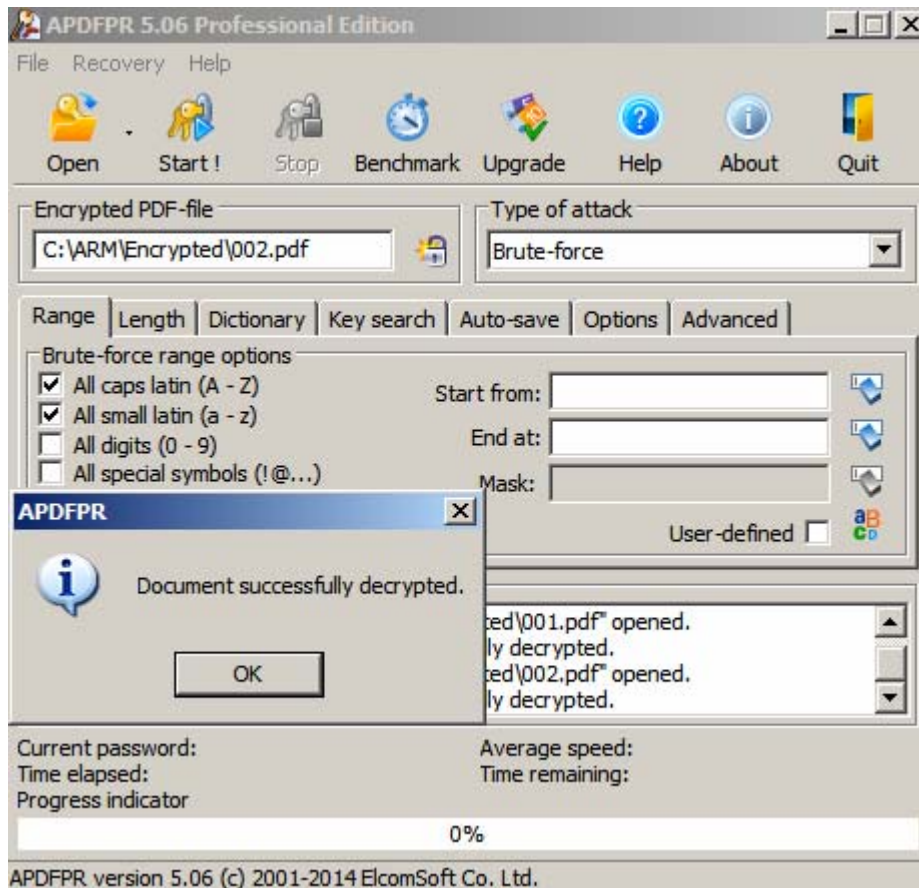




**Figure A1.09.0** Security Settings for a sample book page. All permissions have been removed.

[10] Install the program Advanced PDF Password Recovery Pro<sup>736</sup> (APDFPR) and load a sample encrypted page.

<sup>736</sup> ElcomSoft Co. Ltd., *op. cit.*



**Figure A1.10.0** APDFPR content protection identification and removal. APDFPR identified the content protection identification of the sample page as being ‘Acrobat Standard (Standard) 40-bit security v.1.’ and was able to successfully remove the content protection.

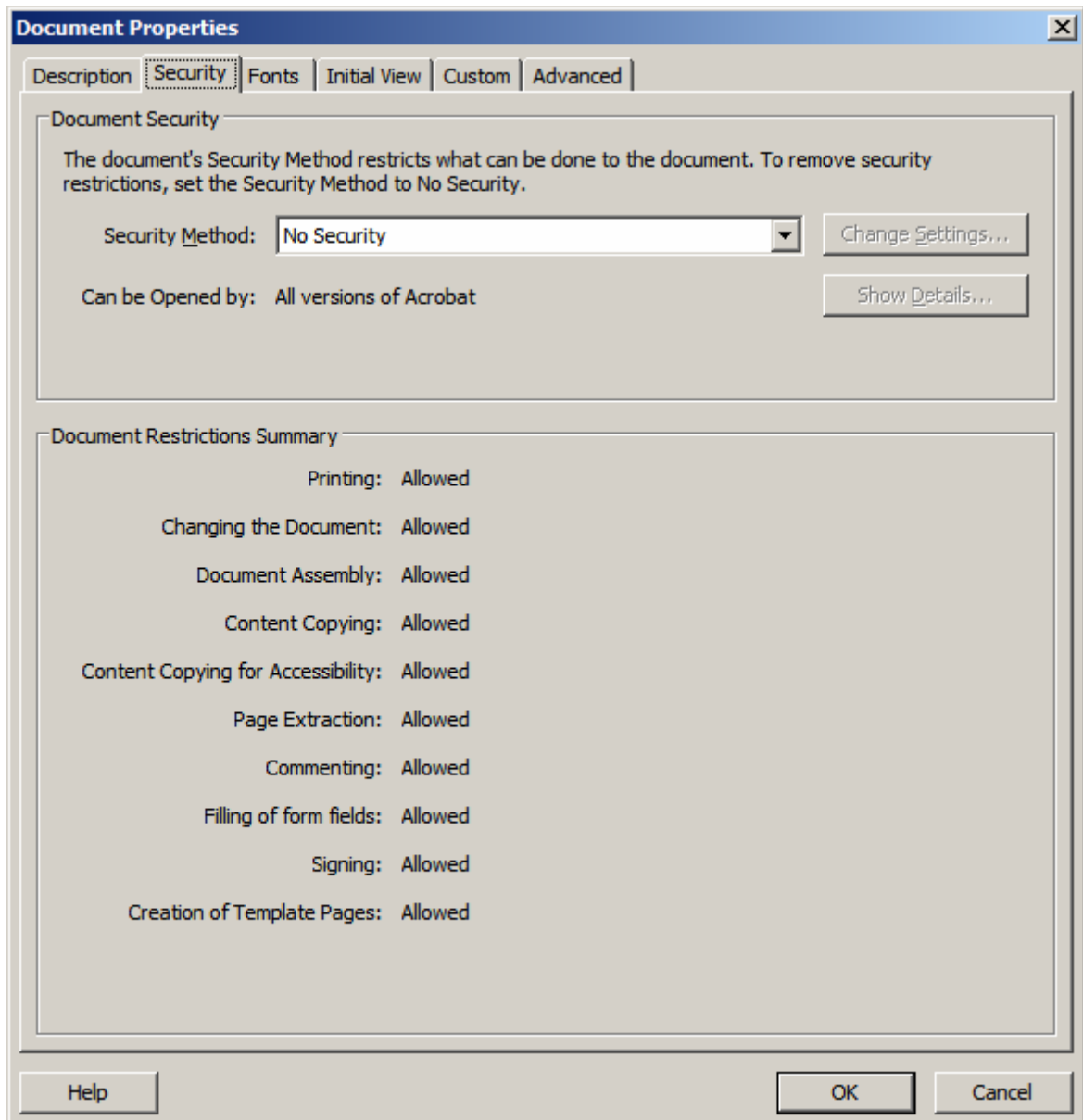
[11] Given that sample page decryption worked, all of the downloaded book pages can now be decrypted. The process is automated by running APDFPR in batch mode via the command line.

The following command is used:

```
apdfpr.exe -batch "c:\ARM\Encrypted\*.pdf" "c:\ARM\Decrypted\" -w
```

The -batch parameter launches APDFPR in batch mode. The first directory denotes all PDF files in the Encrypted directory to be decrypted and placed into the secondary directory. The -w parameter exits the APDFPR program once the batch conversion is complete.

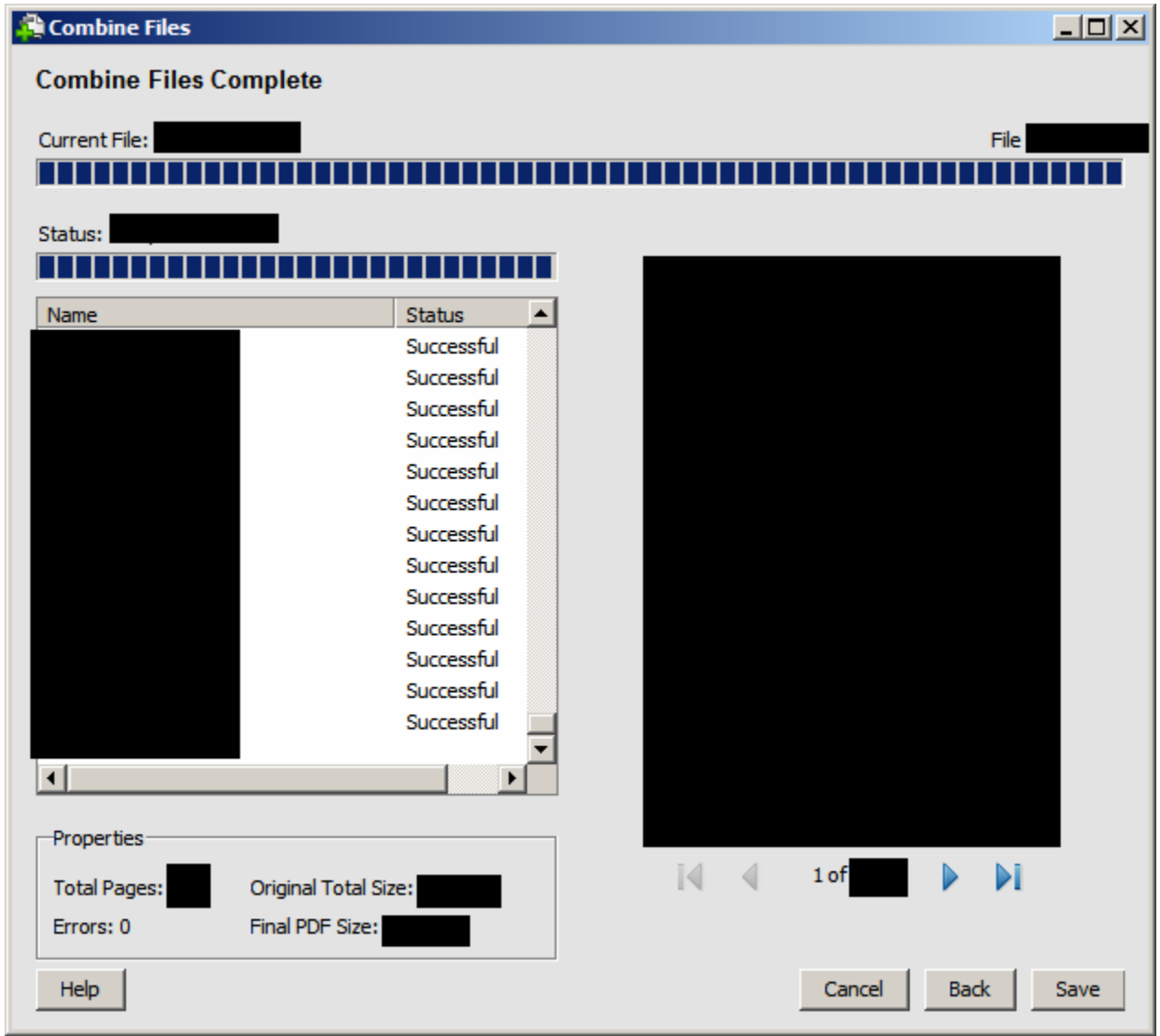
[12] As in Step 9, view the PDF document Security Settings in Adobe Acrobat to reveal existent content protection components of the decrypted PDF.



**Figure A1.12.0** Security Settings for a sample decrypted book page. All permissions have been restored (*cf.* Figure A1.09.0).

#### **IV. Content Concatenation.**

[13] Following successful decryption, the individual pages can now be merged into a single PDF e-book file. This is achieved via the File menu, by selecting Combine Files, further Add Folders and adding the Decrypted folder.

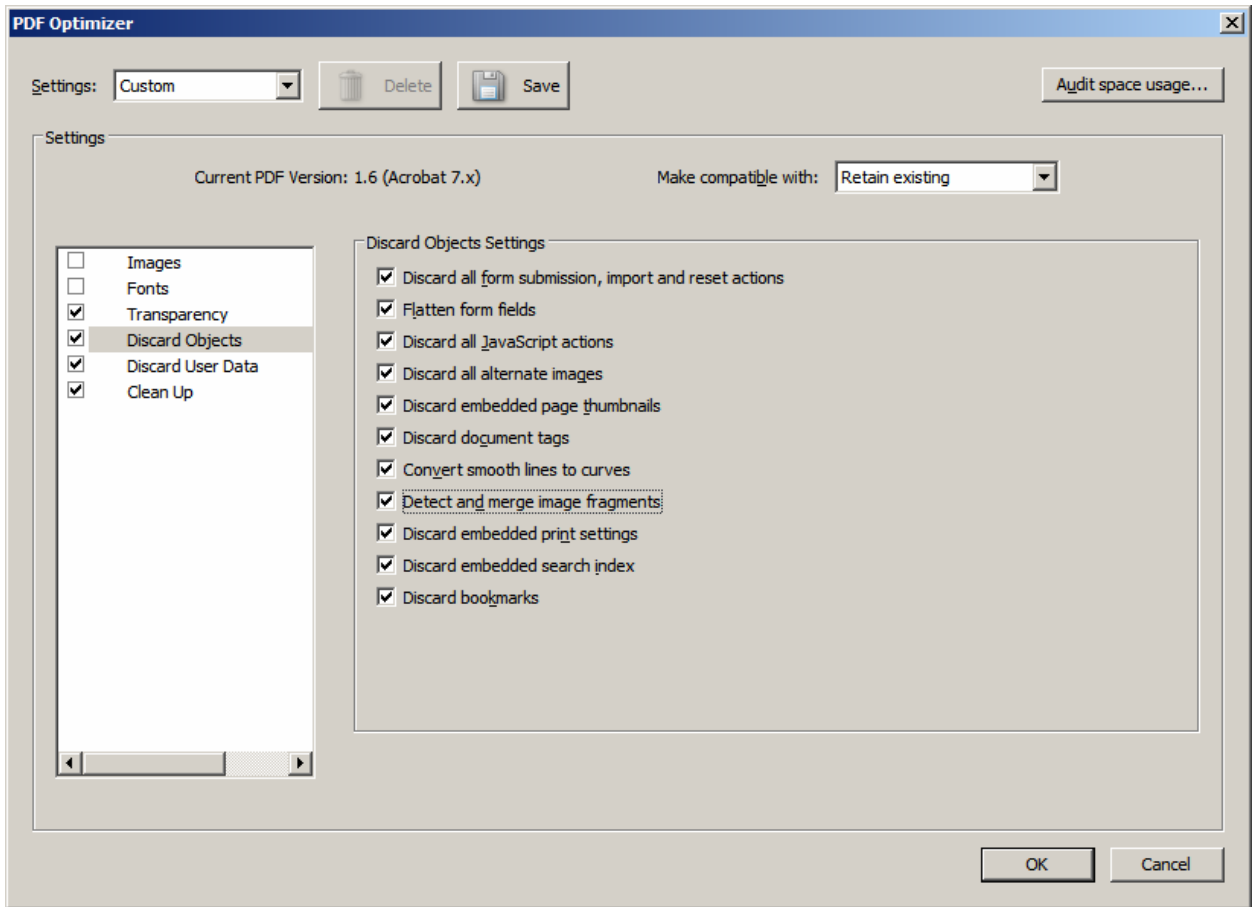


**Figure A1.13.0** Acrobat Combine files menu, showing successful merging of individual decrypted page PDFs into a single PDF e-book file.

## V. Metadata Modification.

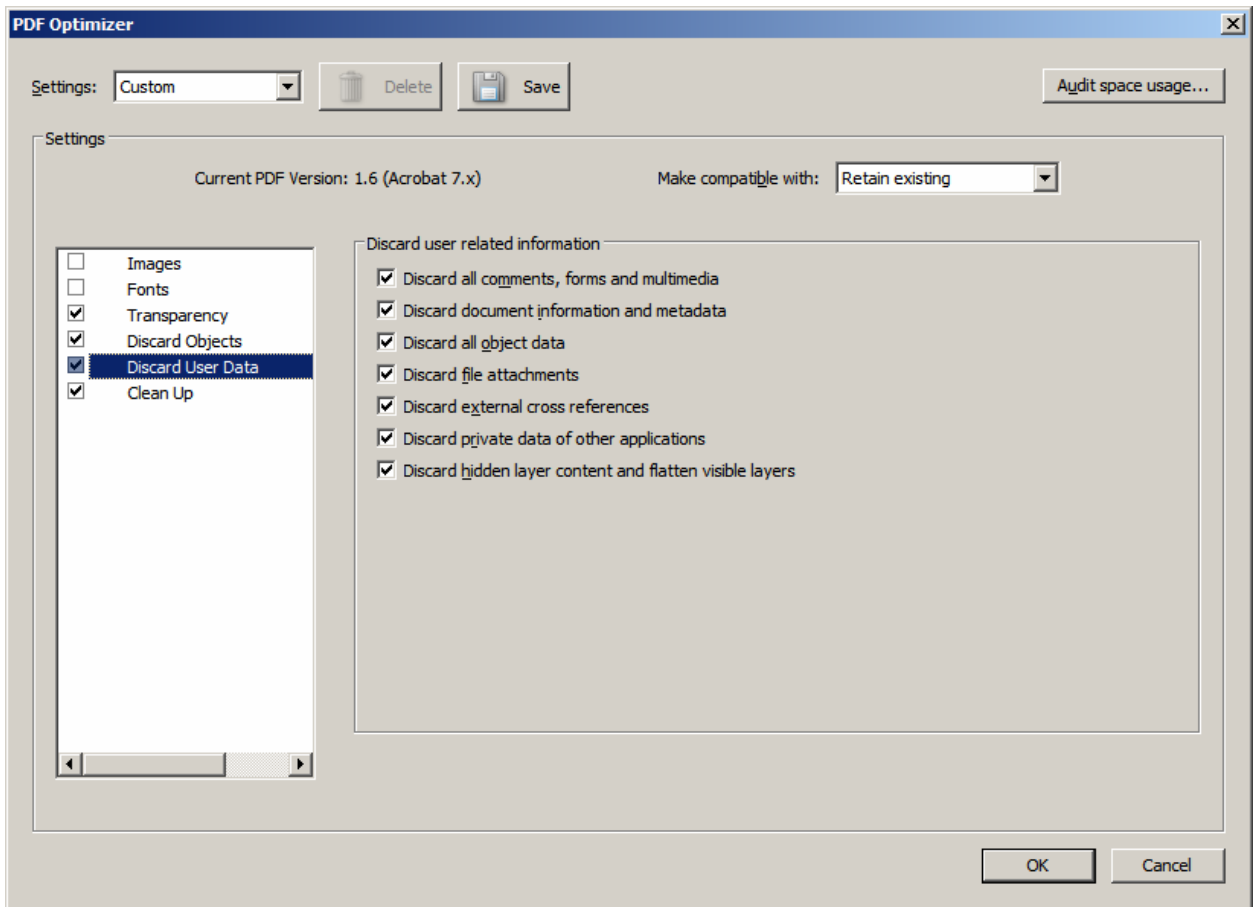
[14] The final component in the workflow is the removal of potentially identifying metadata from the merged PDF. The bulk, albeit notably not all, of said metadata can be removed by using Acrobat. This is achieved via the Advanced menu, by selecting PDF Optimizer.

Select the Discard Objects field and check all available options.



**Figure A1.14.0** Acrobat PDF Optimizer Discard Objects menu.

Next, select the Discard User Data, once again checking all available options.



**Figure A1.14.1** Acrobat PDF Optimizer Discard User Data menu.

The other fields (Images, Fonts, Transparency, Clean up) are irrelevant for the purposes of metadata removal and can be left as-is. Press OK to create the new optimized PDF.

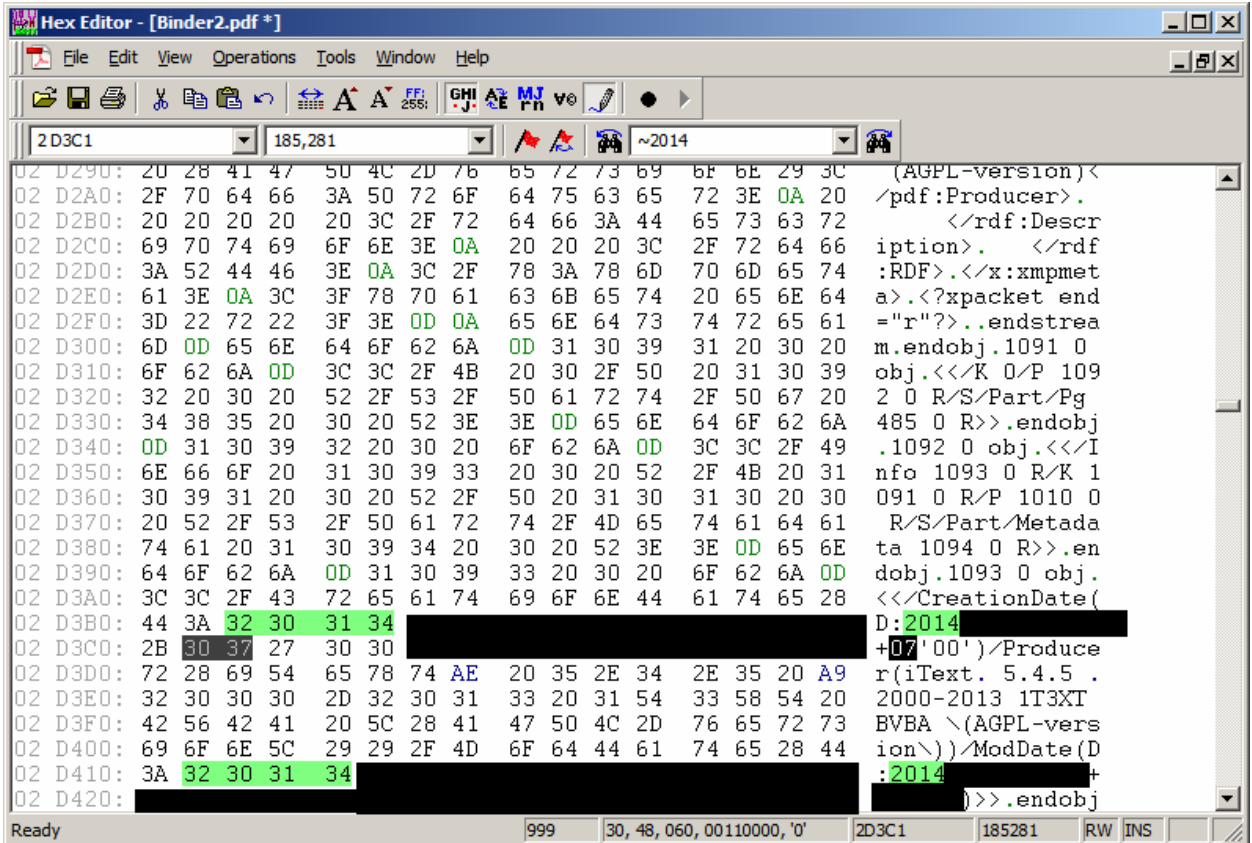
[15] Following the utilization of Acrobat's own PDF metadata removal tools, there are still two persistent metadata parameters left to modify which cannot be accomplished with Acrobat.

Install the program HexEdit<sup>737</sup>, a hex editor, and load the merged PDF.

The first metadata parameter to modify is the time zone data. Access the Find menu in HexEdit. This is achieved via the Edit menu, by selecting Find, and then selecting Find again. Change the type of query from the default Hex setting to ASCII and perform a search for the current year.

---

<sup>737</sup> Andrew W. Phillips. 2002. HexEdit. v. 2.00. <http://www.expertcomsoft.com/hexedit.htm>.



**Figure A1.15.0** HexEdit view of sample merged PDF e-book file showing date fields.

Once the data field is isolated, modify it to a date that does not correspond to your actual Twilynax date. This is done to foil time-of-access forensic attacks against the distributor of the e-book (e.g. if the PDF was distributed at a certain time, Twilynax server access logs may be checked by forensic analysts to see if anyone accessed the book around that approximate time).

**Note Bene:** There will typically be a minimum of four date fields to modify in the metadata.

In this example there are four such fields:

```
CreationDate(D:20140911191101+01'00' )
ModDate(D:20140911191101+01'00' )
<xap:CreateDate>2014-09-11T19:11:01+01:00</xap:CreateDate>
<xap:ModifyDate>2014-09-11T19:11:01+01:00</xap:ModifyDate>
```

Modify not only the date, but the time zone offset as well to foil location forensic location attacks.

[16] The second metadata parameter to modify is the Universally Unique Identifier (UUID). Once again selecting ASCII mode, search the document for 'uuid'.

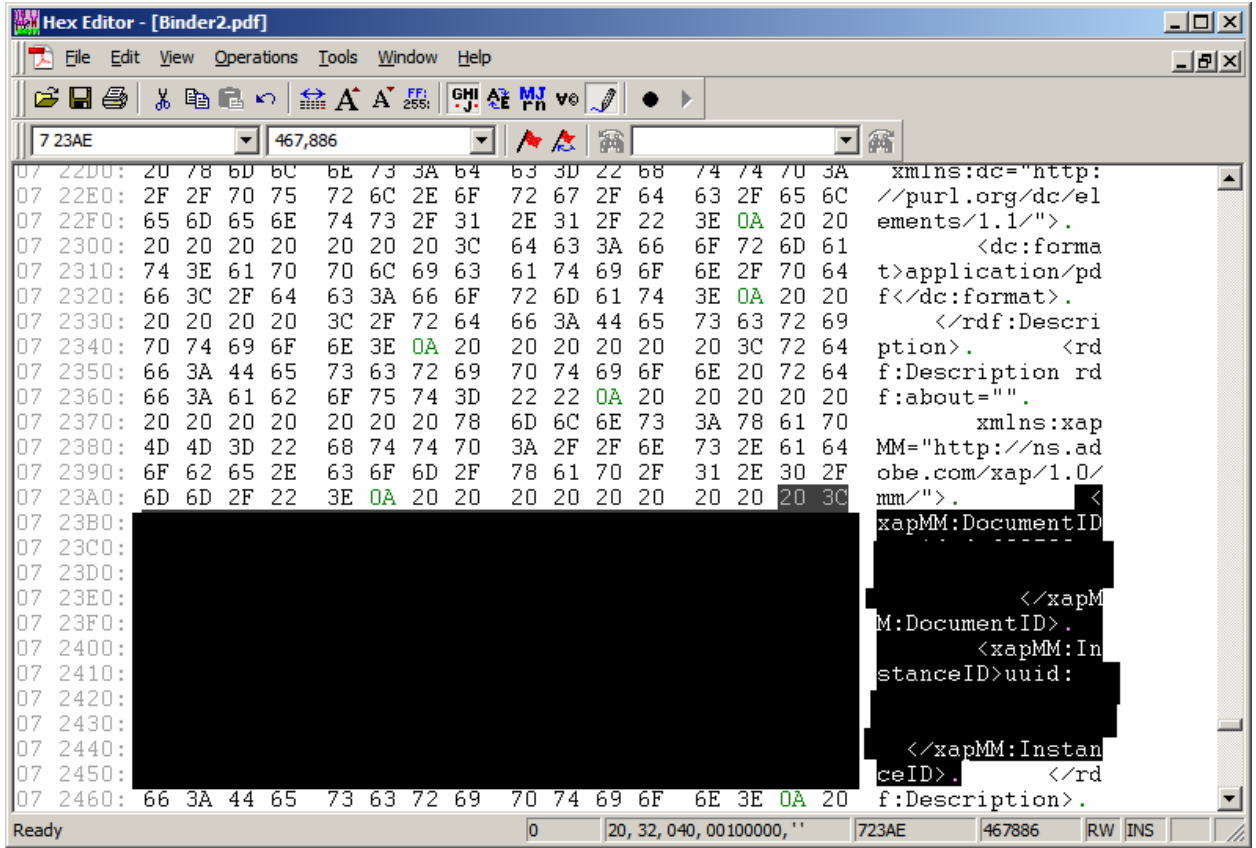


Figure A1.16.0 HexEdit view of sample merged PDF e-book file showing UUID fields.

Replace the existent UUID strings with randomly crafted ones consisting of a-f; 0-9.

## VI. Distribution.

[17] Save the PDF document and exit HexEdit. The workflow is at this stage complete with the Twilynax e-book now being ready for distribution.



## **Appendix 2:**

# **Sample Procedure for Watermark Removal from Eestro eJournal Articles**

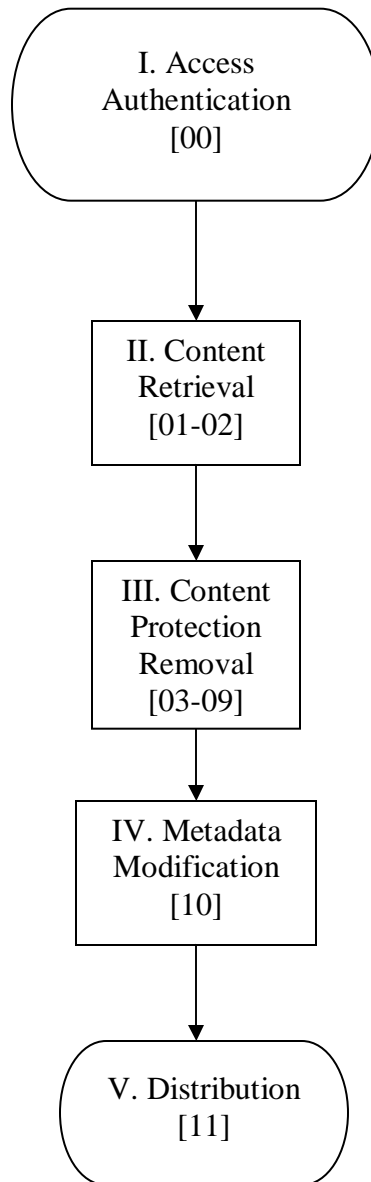
This case study presents an illustrated and annotated workflow for removing content watermarks from a sample selection of academic ejournal articles. Refer to §2.4 ‘Case Study 3: Informational Illegalism (Critical Praxis) — Unwatermarking Eestro eJournal Articles’ of the dissertation for analysis of and reflection on the case study.

A total of seven academic ejournal publishers/content providers were selected: Aestro, Bestro, Cestro, Destro, Eestro, Festro, and Gestro. For the purposes of this case study, a watermark is defined as a mark added to a digital document to explicitly foster the identification of the source/downloader of the article. Cover page watermarks are those watermarks which are injected into a unique cover page into the PDF file for each download. Margin watermarks are those watermarks which are injected into the margins of one or multiple pages of the PDF file for each download. Natural Language Watermarking meanwhile modifies the actual text (e.g. ‘I pirated some e-journals yesterday’ → ‘Yesterday, I paired some ejournal articles’). All three varieties of watermarking techniques can embed potentially-downloader-identifying information including such data as date and time of the download, the Internet Protocol (IP) address of the download, and the name of the sponsoring institution through which the download was conducted. Of the seven publishers examined, two were found to contain both cover page watermarking and margin watermarking, two were found to contain only margin watermarking, one was found to contain only cover page watermarking, and two were found to contain no visible method of article watermarking.

<u>Publisher</u>	<u>Cover Watermark</u>	<u>Margin Watermark</u>	<u>Natural Language Watermark</u>
Aestro		✓	
Bestro			
Cestro	✓	✓	
Destro			
Eestro	✓	✓	
Festro	✓		
Gestro		✓	

**Table A2.0:** eJournal Article Watermark Occurrence.

The general workflow schema can be visualized as follows (with accompanying procedural step numbers):

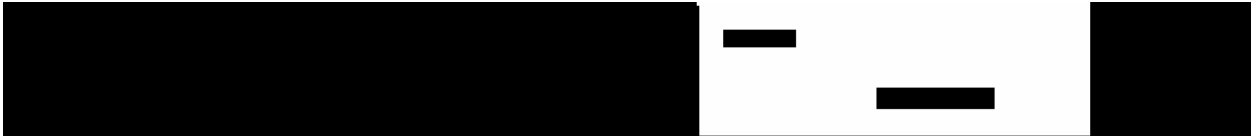


## **I. Access Authentication**

As in Appendix 1, the workflow initializes with gaining access authentication to the content in question. Whilst the particulars of gaining access authentication to each publisher vary slightly based on particular login portals and website structure, the basic workflow nonetheless remains fundamentally the same for all seven publishers; as such, publisher five—here named Eestro—will be used as a comprehensive, illustrative workflow case study.

[00] Access the Eestro ejournal collection via passing through a series of login screens, ultimately using university-afforded authentication credentials through the appropriate institutional login portal.

**Nota Bene:** The operative web browser used in the case study is Firefox<sup>738</sup>.



**Figure A2.00.0** Eestro homepage<sup>739</sup>.



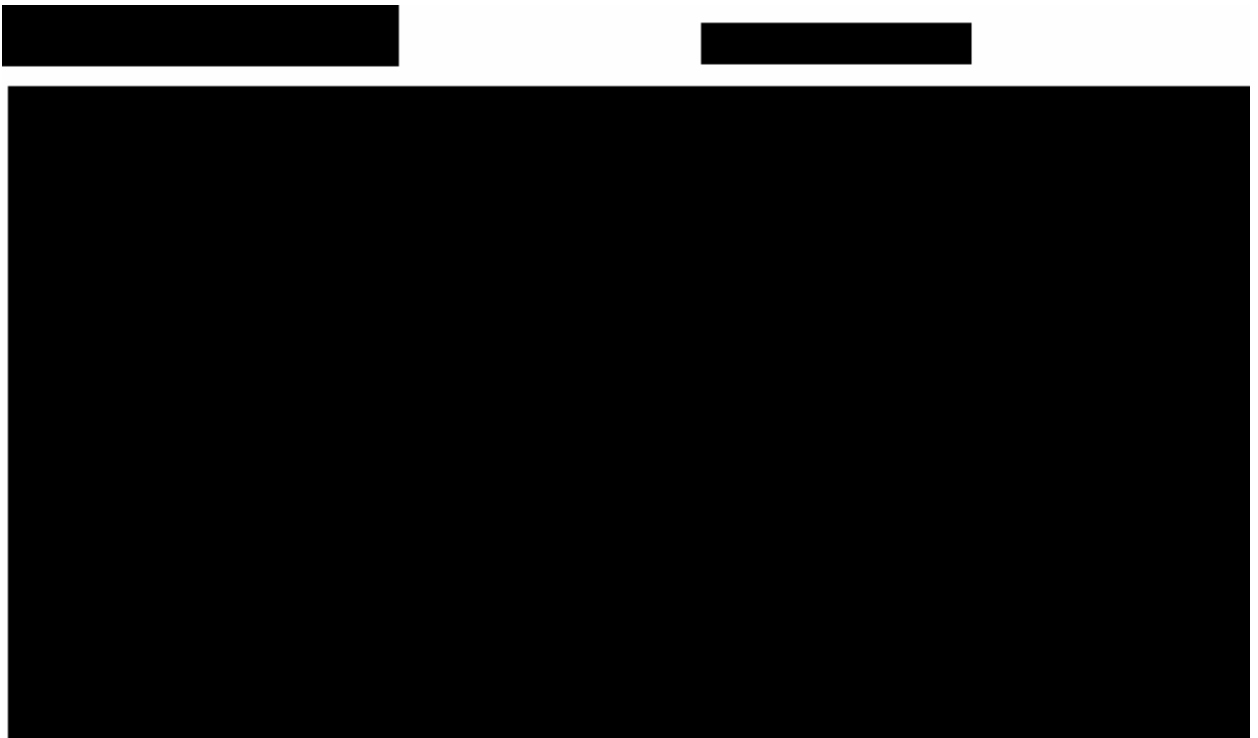
**Figure A2.00.1** Primary Eestro login screen<sup>740</sup>, to be arrived at after selecting ‘Sign in’ on the Eestro homepage, as seen in **Figure A2.00.0**.

---

<sup>738</sup> Mozilla, *op. cit.*

<sup>739</sup> [http://\\*/](http://*/).

<sup>740</sup> [https://\\*/\\*/](https://*/*/).



**Figure A2.00.2** Secondary Eestro login screen<sup>741</sup>, to be arrived at after selecting the appropriate institutional login portal on the primary login screen, as seen in Figure A2.00.1.



**Figure A2.00.3** Tertiary Eestro login screen, to be arrived at after selecting the appropriate institution with which one has an account on the secondary login screen, as seen in Figure A2.00.2.

## II. Content Retrieval

---

<sup>741</sup> [http://\\*/\\*/\\*](http://*/*/*).

[01] Perform a search query for an ejournal article by title, author, journal name, keyword, or Document Object Identifier (DOI).

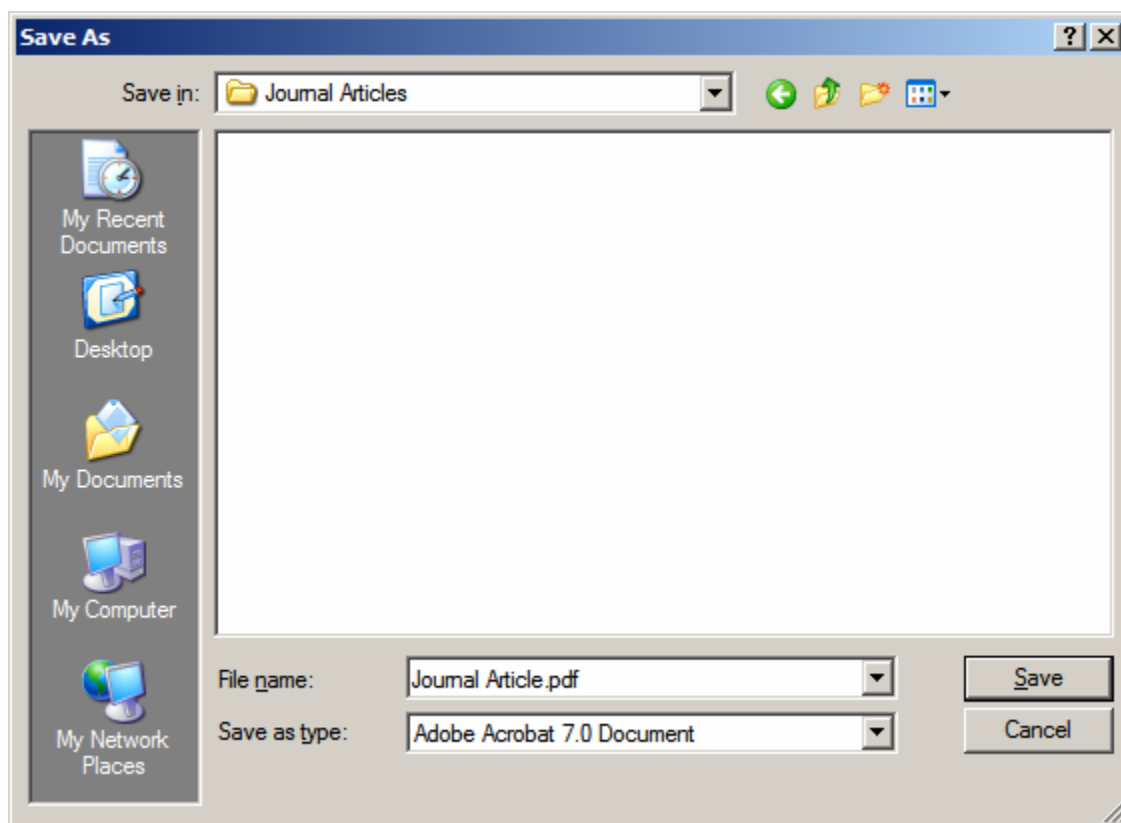


**Figure A2.01.0** Search query results for a sample DOI<sup>742</sup>.

[02] Select the ‘Download full text’ link and save the resultant PDF.

---

<sup>742</sup> [http://\\*/\\*/\\*/?\\*=\\*](http://*/*/*/?*=*).



**Figure A2.02.0** Firefox Save window.

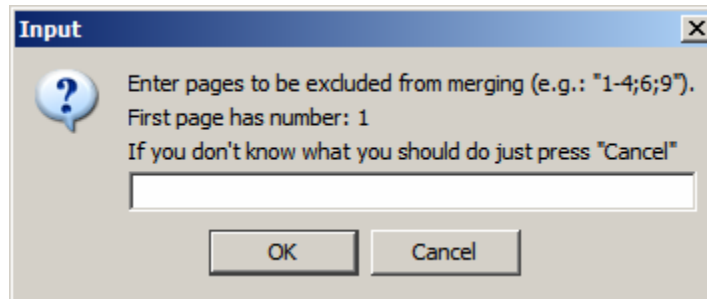
**Nota Bene:** Unlike the case study presented in Appendix 1, it will be noted that there is no filename obfuscation employed by Eestro; instead, PDF document downloads are named based on the publicly-viewable DOI of each journal article. Thus step 01 can be skipped with foreknowledge of a desired article's DOI by going to the URL — [http://\\*\\*/\\*\\*/\\*\\*/\[DOI here\]](http://**/**/**/[DOI here]).

### **III. Content Protection Removal**

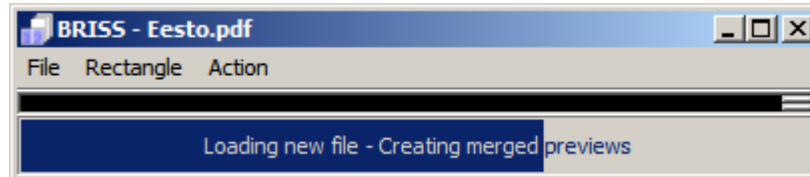
[03] As the sample Eestro ejournal article contains both cover page and margin watermarks, both need to be removed. Start with removing the margin watermark by loading the article PDF downloaded in Step 2 in briss<sup>743</sup>, a cropping application which allows one to redefine the margin dimensions of pages within a PDF document, by proceeding to File → Load File, or by pressing the F key. A dialogue box will appear asking about excluding any pages from the crop procedure; select Cancel and briss will initiate the loading of the selected PDF.

---

<sup>743</sup> Aigner, *op. cit.*



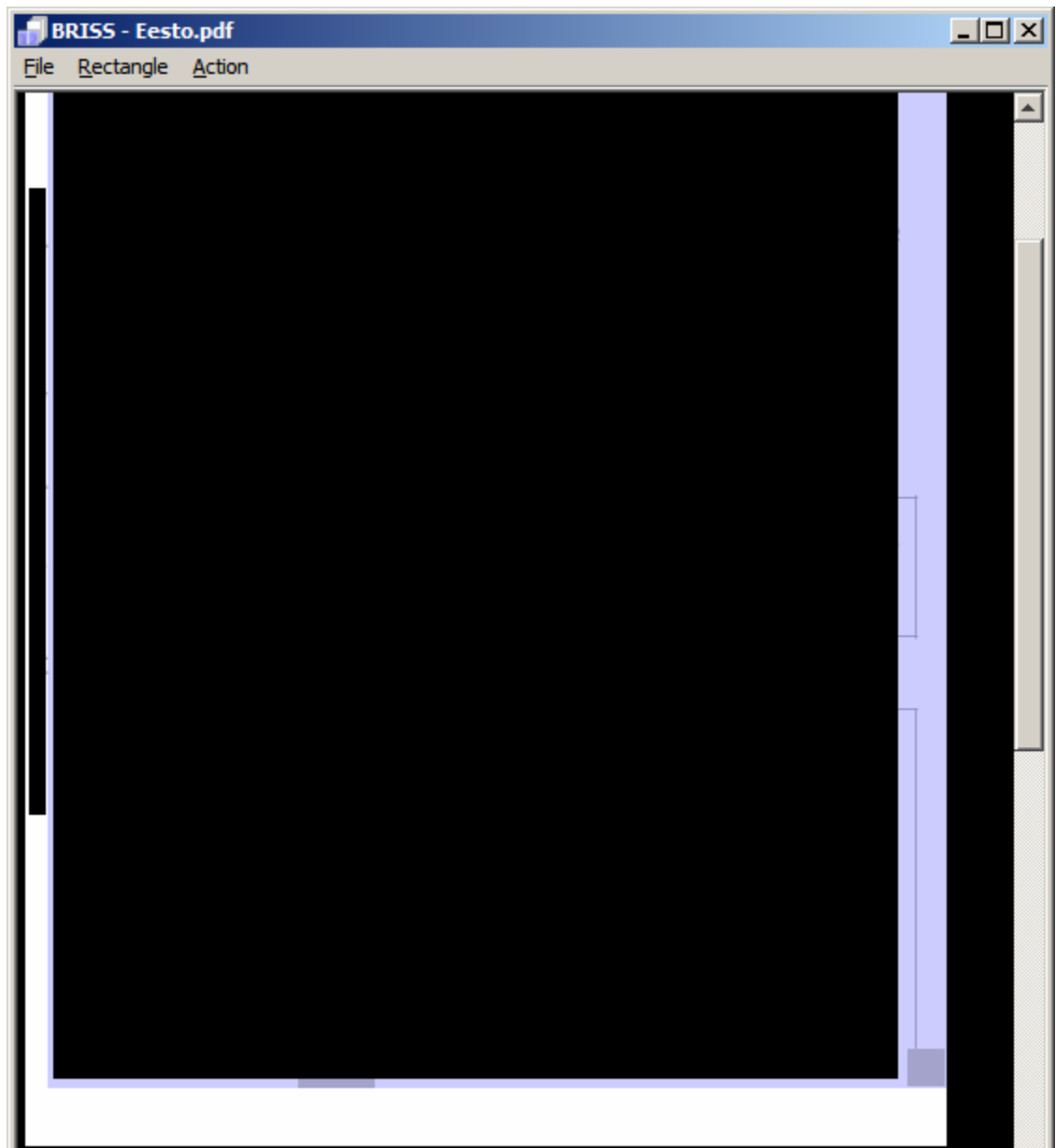
**Figure A2.03.0** briss page exclusion dialogue box. Select Cancel.



**Figure A2.03.1** briss PDF loading bar.

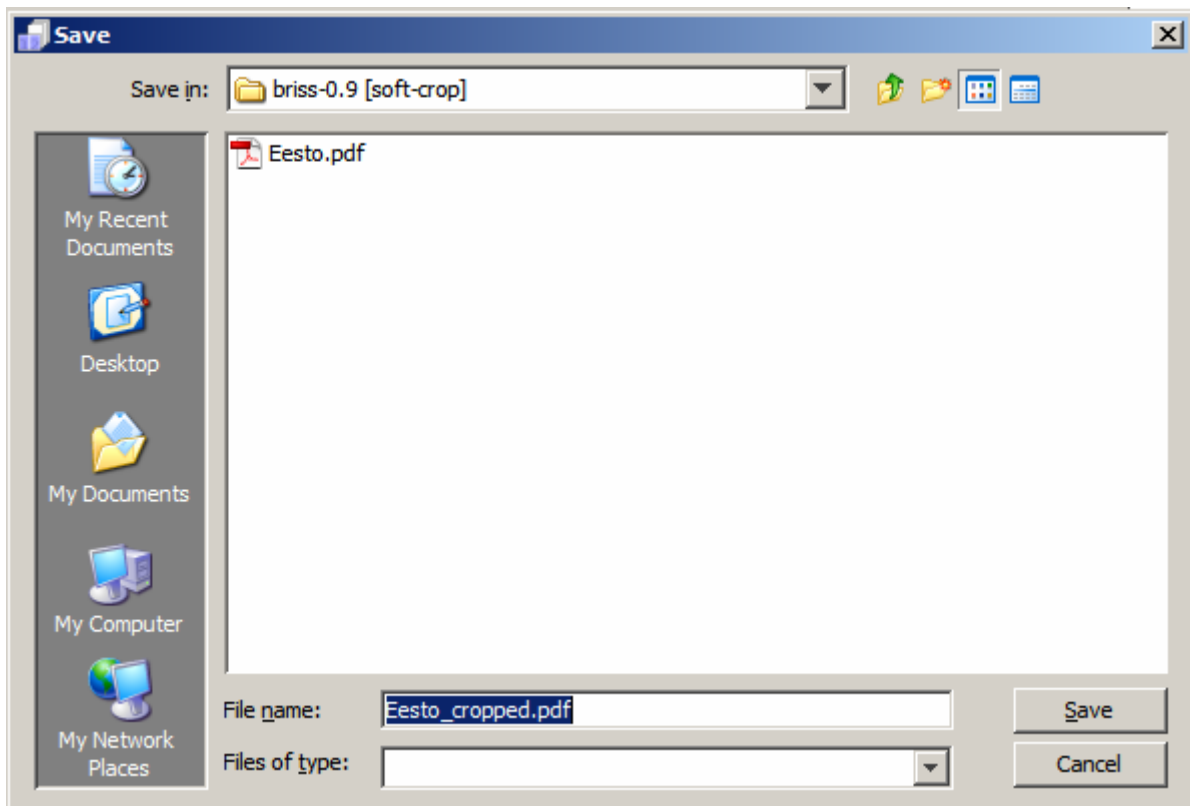
[04] Once the PDF has loaded, select the area of the page that is to be preserved, excluding the margins which include the watermark.





**Figure A2.04.0** Eestro journal article loaded in briss, with margin watermark (on the lefthand side, outside the light blue border) set to be cropped out.

[05] Once the desired area has been selected, crop the PDF by proceeding to Action → Crop PDF, or by pressing the C key. The briss save dialogue will appear, enter the new filename and select Save.

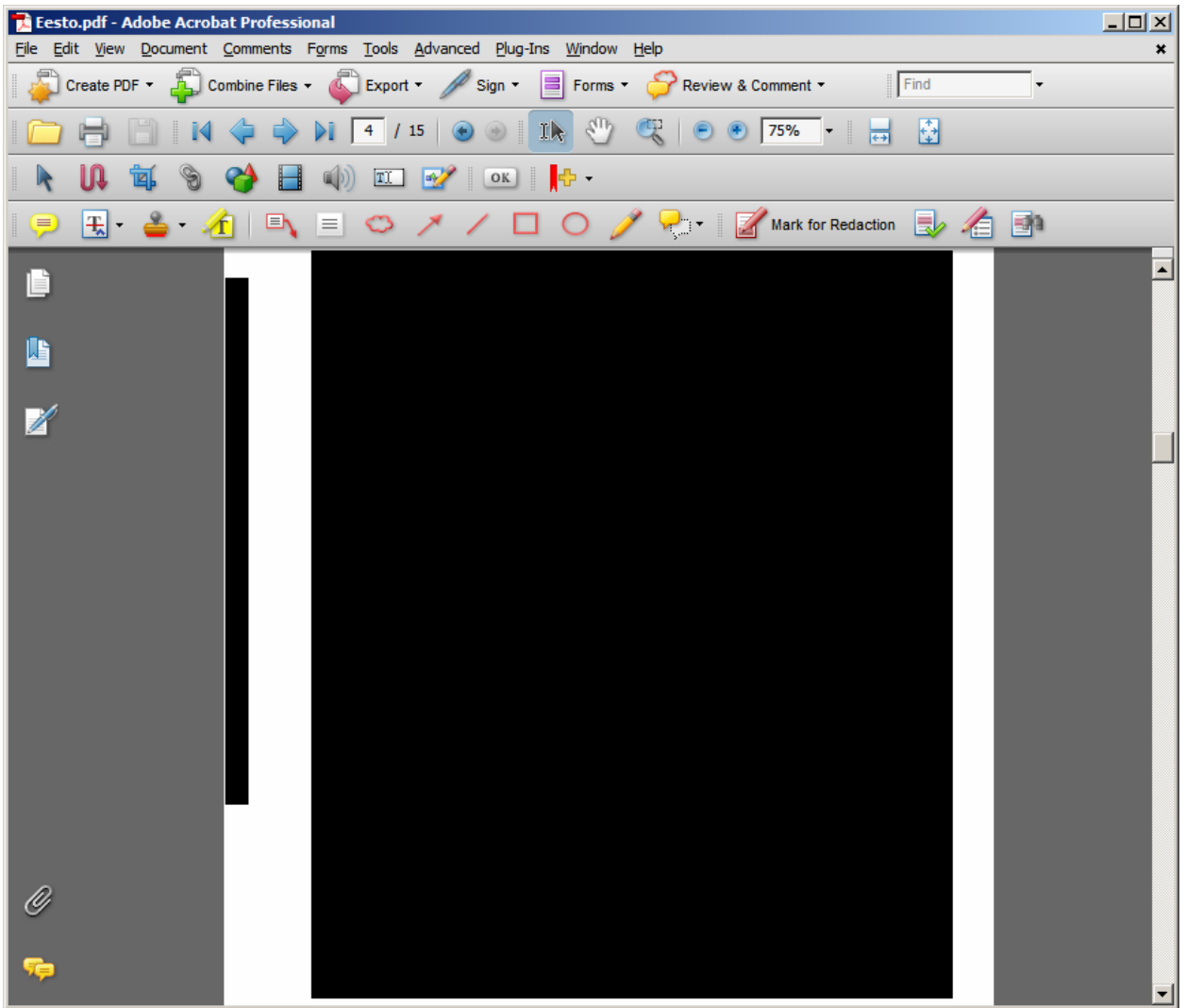


**Figure A2.05.0** briss Save window.

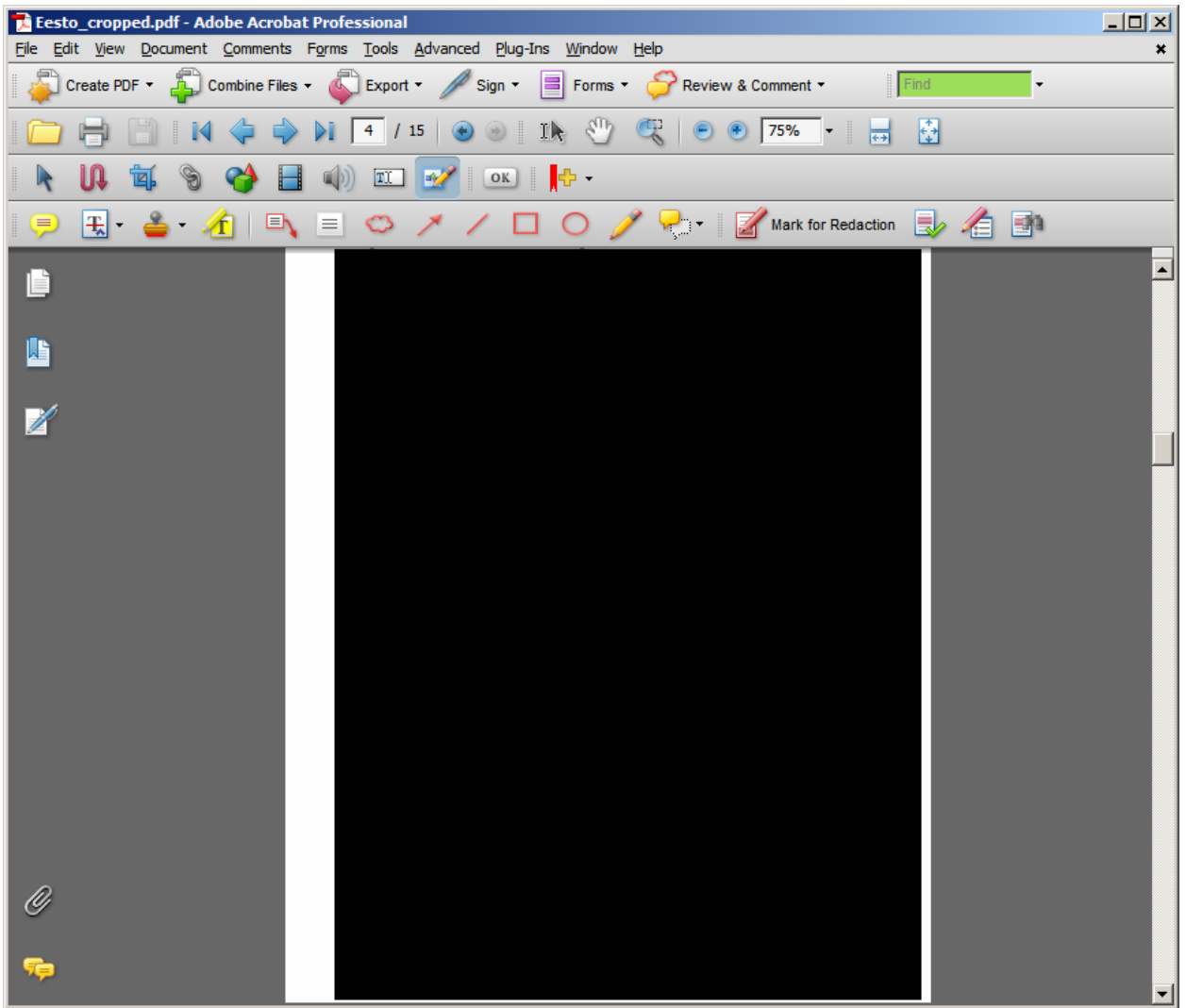
[06] However, briss performs only a *nondestructive crop*: a crop in which the dimensions of the displayed page are readjusted, with the data outside the new dimensions thus rendered invisible but not deleted. Thus it is insufficient to merely use briss, as forensic analysis can reveal the cropped watermark data. This can be verified by opening the briss-outputted PDF from Step 5 in Adobe Acrobat Professional<sup>744</sup>, and proceeding to Tools → Advanced Editing → TouchUp Object Tool, and then proceeding to View → Select All, or pressing Ctrl-A. Once all objects on the page have been selected, draw the out of bounds objects onto the page to reveal the margin watermark.

---

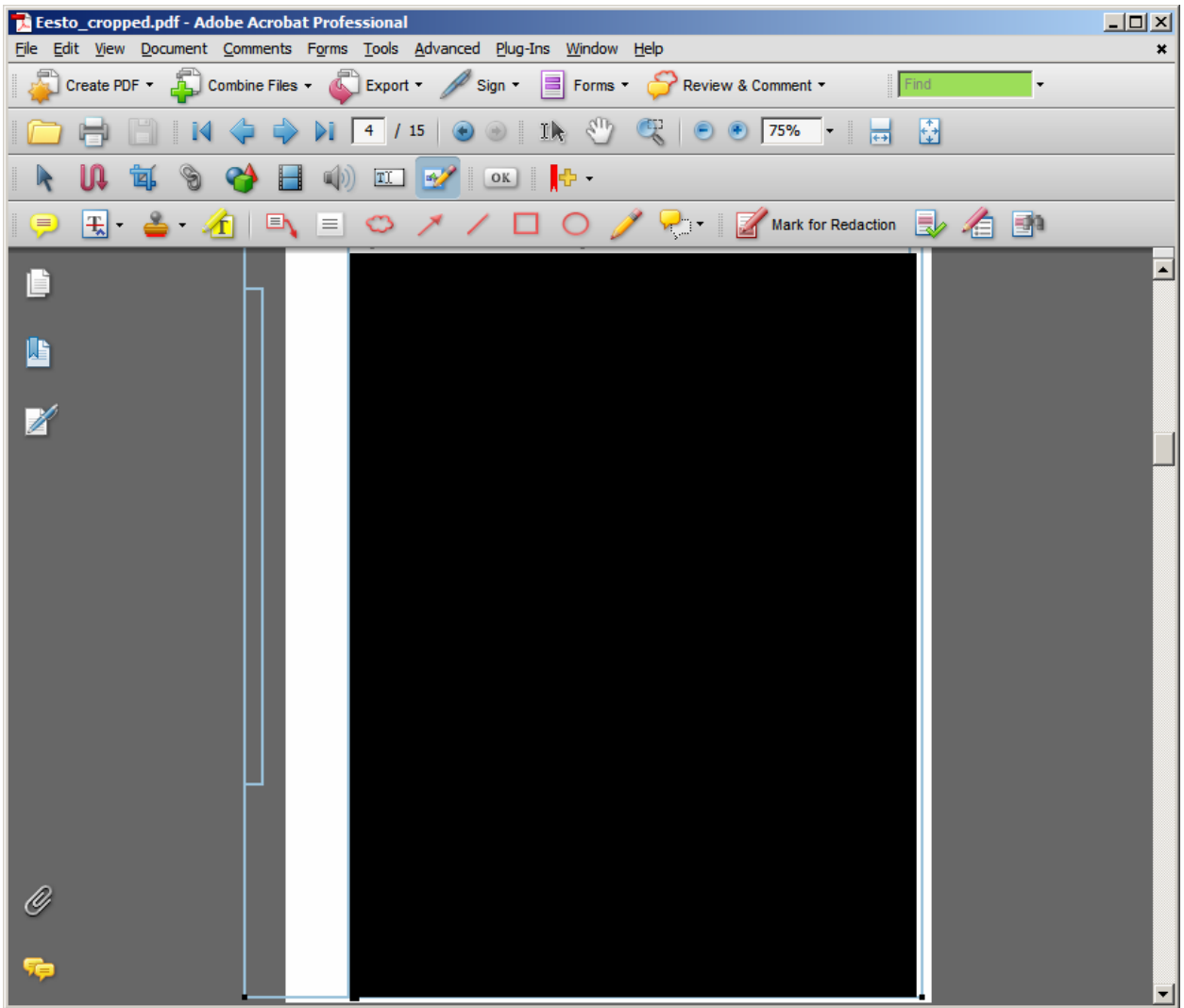
<sup>744</sup> Adobe Systems Incorporated, *op. cit.*



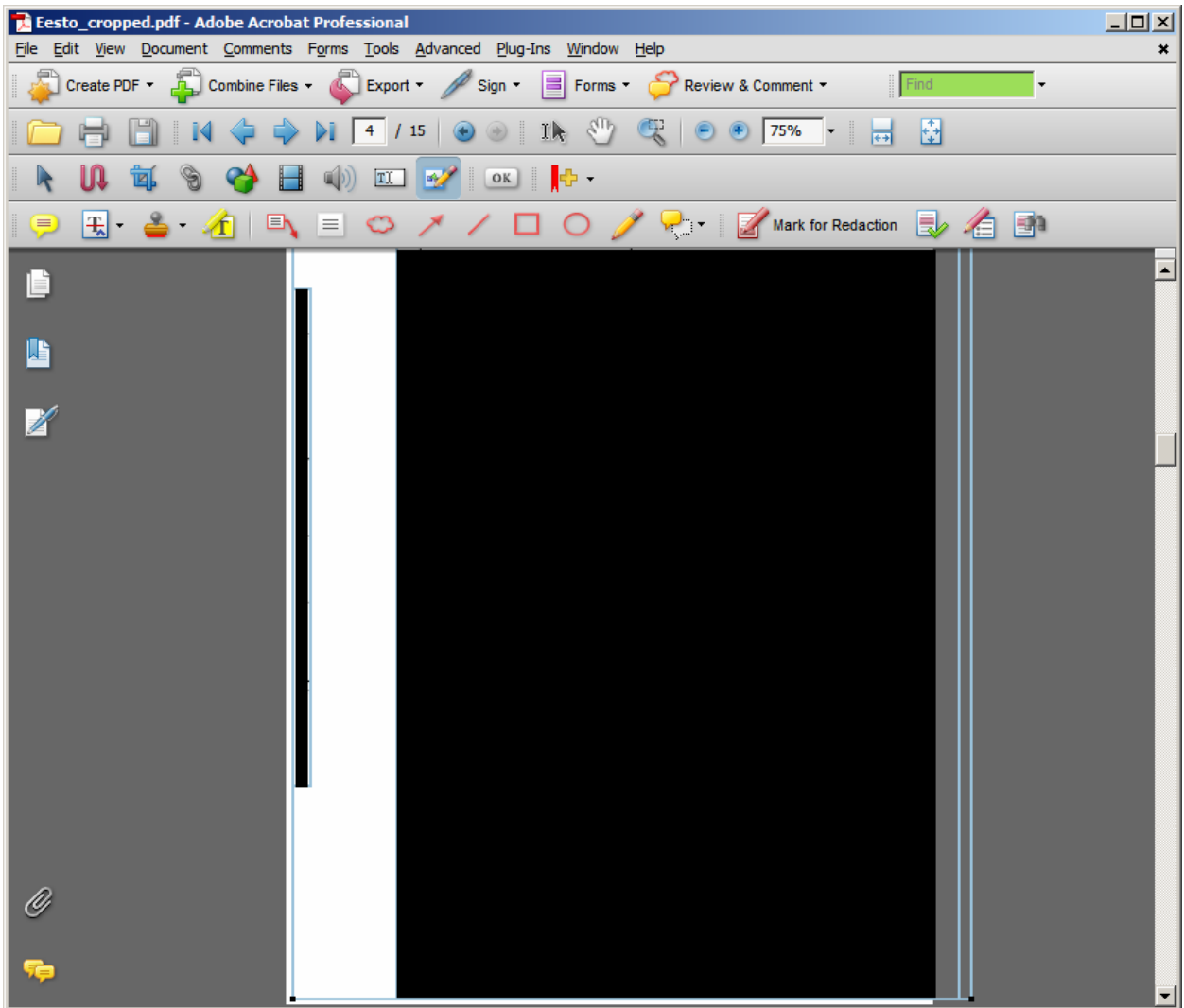
**Figure A2.06.0** The initial, uncropped article page.



**Figure A2.06.1** The briss-cropped article page, seemingly without the cropped watermark.



**Figure A2.06.2** Touch-Up Tool selection. Once the Touch-Up Tool is selected and the Select All option is further invoked, the watermark elements are now apparent off-page but in-document.

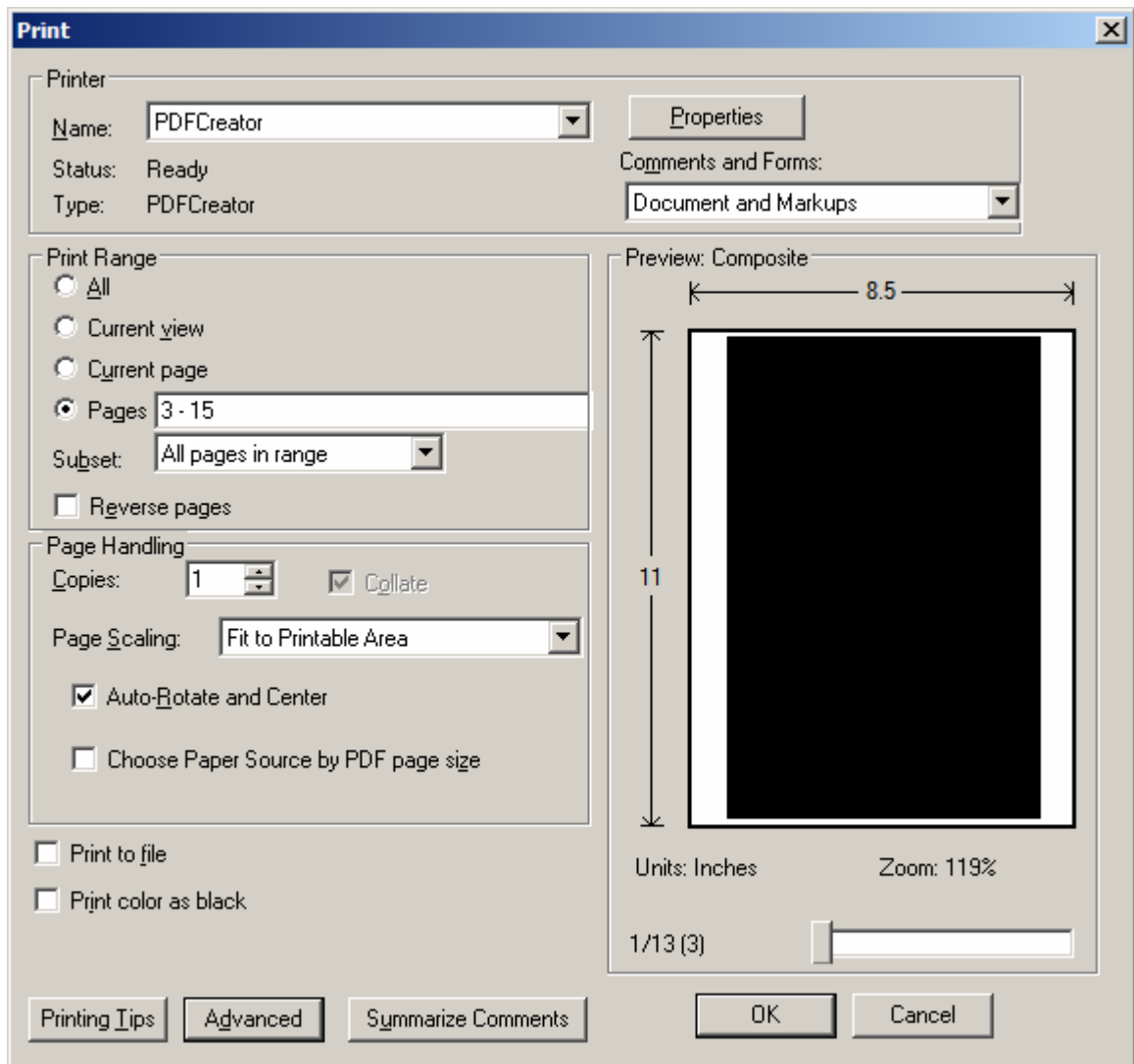


**Figure A2.06.3** Nondestructive crop reveal. The off-page element can be dragged onto the page to be rendered readable, thus revealing the nondestructively-cropped watermark.

[07] In order to achieve a destructive crop, the briss-cropped PDF created in Step 5 may further be printed by using PDFCreator<sup>745</sup>. Once PDF Creator is downloaded and installed, open the briss-cropped PDF created in Step 5 in Adobe Acrobat and proceed to File → Print, or press Ctrl-P. In the Print window which appears, select PDFCreator as the printer. At this step the cover page watermark may also be removed by selecting a page range which excludes the first one or two cover pages which contain the watermark.

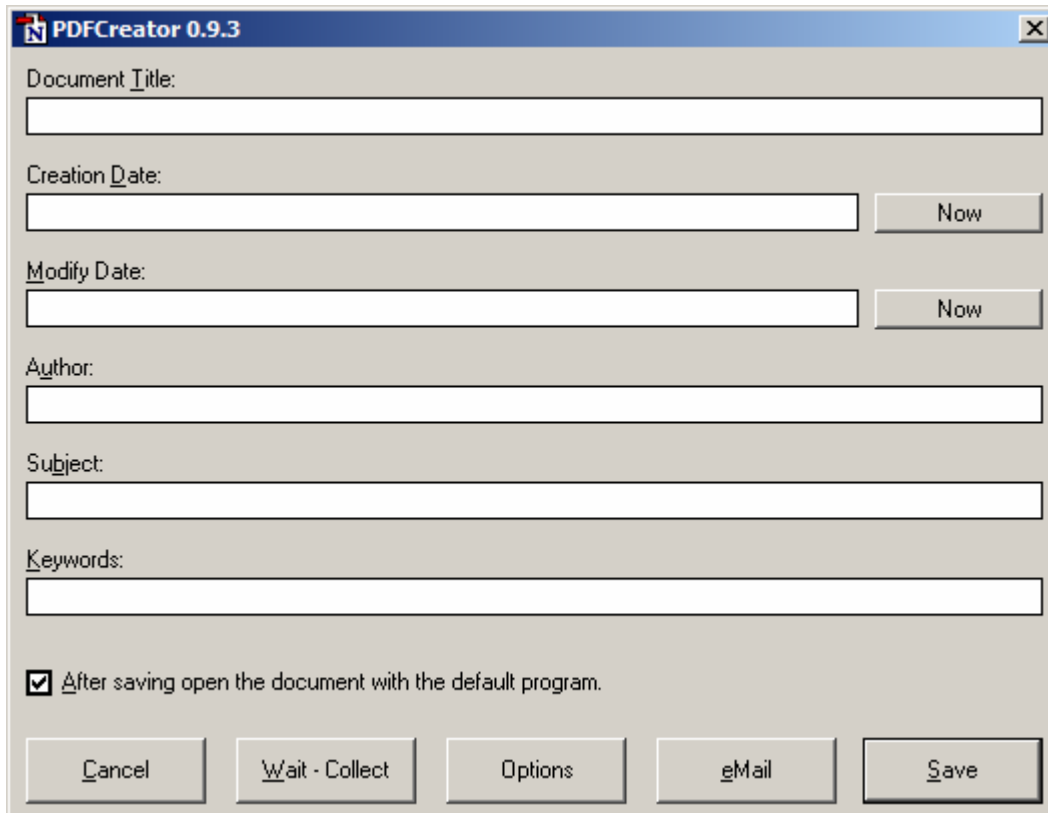
---

<sup>745</sup> Chinery and Heindörfer, *op. cit.*



**Figure A2.07.0** Adobe Acrobat Print window with PDFCreator selected as the printer, and watermark cover pages excluded from the print job.

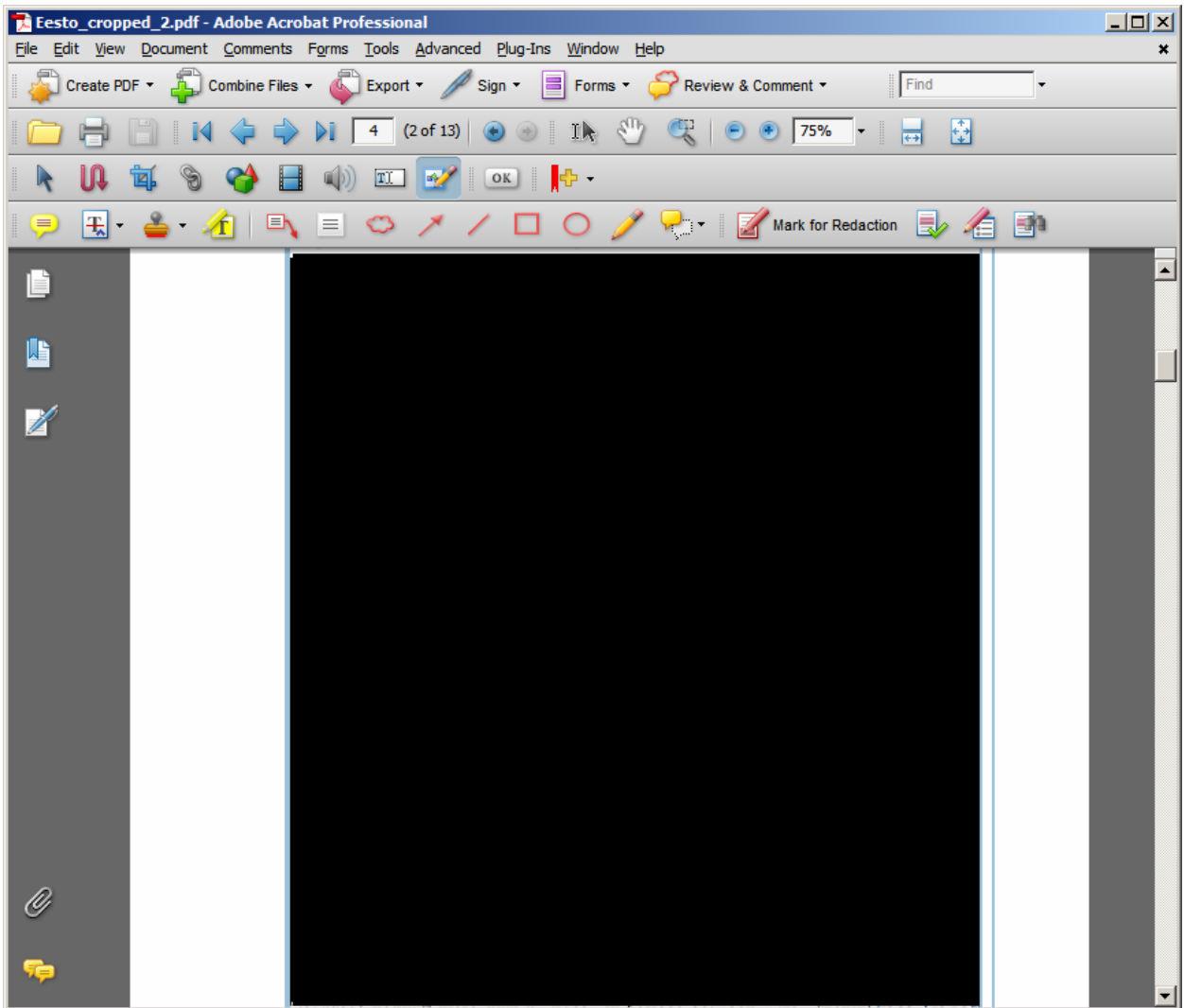
[08] In the PDFCreator window which subsequently appears, remove all of the metadata information and select Save.



**Figure A2.08.0** PDFCreator window with document metadata removed.

[09] The successful destructive cropping and removal of margin metadata may be verified by repeating the procedure in Step 6, revealing that there are now no hidden object fields present.





**Figure A2.09.0** The TouchUp Object Tool reveals that there are no hidden objects, thus signifying that a destructive crop has been performed, successfully excising the margin watermarks.

#### **IV. Metadata Modification**

[10] As work is being done on PDF files, further metadata modification must be performed, with the workflow being identical to that in §V of Appendix 1.

#### **V. Distribution**

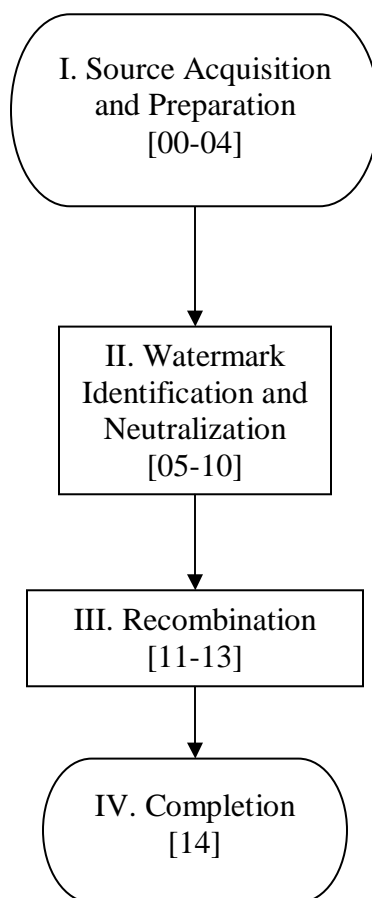
[11] The workflow is at this stage complete with the ejournal article now being ready for distribution.

# Appendix 3:

## Sample Procedure for Cinematic Auditory Forensic Watermark Neutralization

This case study presents an illustrated and annotated workflow for neutralizing audio-based watermarks from a sample cammed video of the film *Illegala*<sup>746</sup>. Refer to §3.3.0.0 ‘Case Study 4: Audio Forensic Marker Neutralization’ of the dissertation for analysis of and reflection on the case study.

The general workflow schema can be visualized as follows (with accompanying procedural step numbers):



---

<sup>746</sup> As previously noted, title is fictional. Refer to Disclaimer of Liability. Watermarked audio sample courtesy of [anonymous].

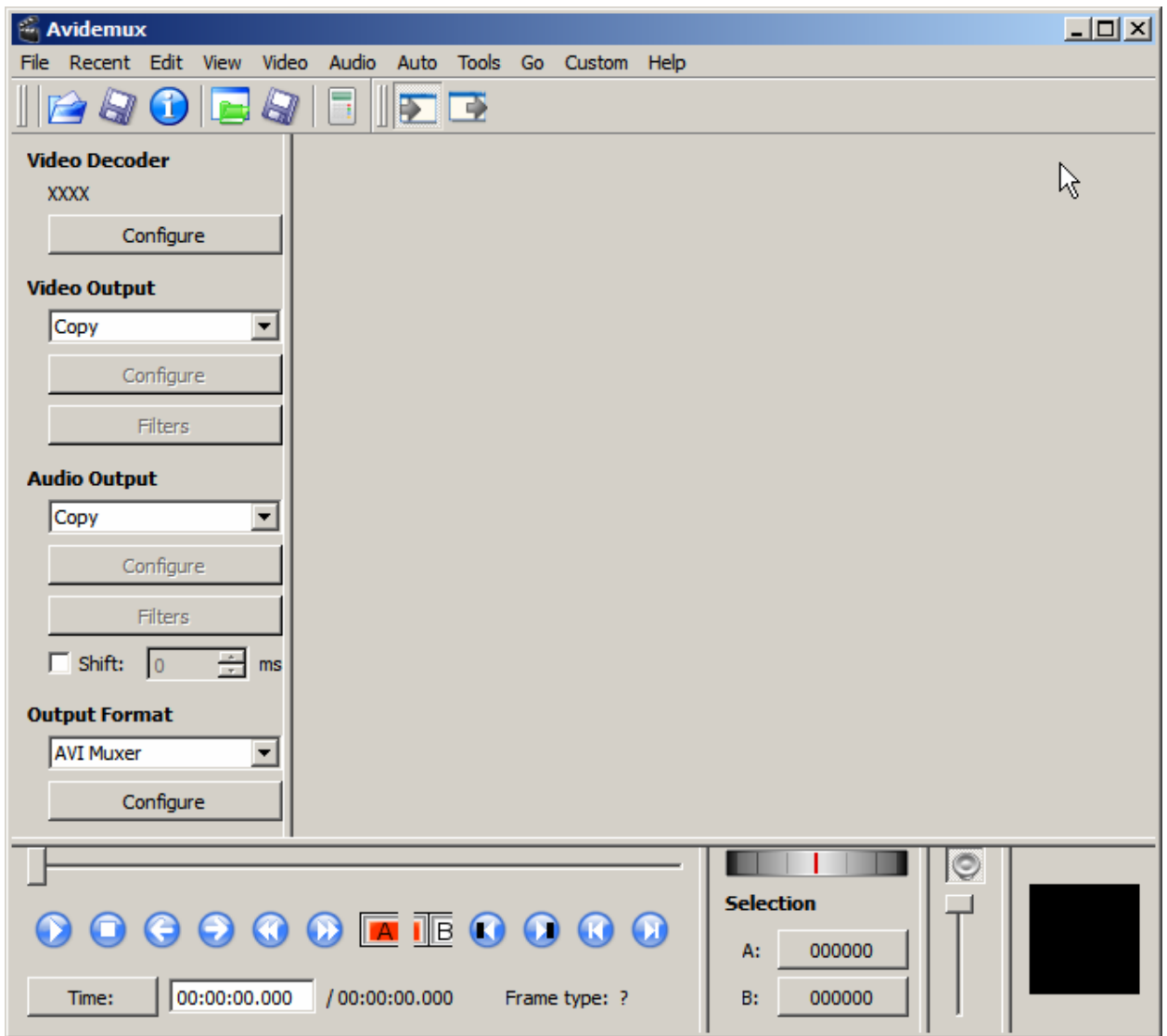
## I. Source Acquisition and Preparation

[00] Procure the source audio track for the film. This can be achieved, in order of escalating access control or increasing difficulty of access (with said order also being directly proportional to the resultant fidelity of the recording), via the use of a camcorder's built-in microphone, the use of a higher quality external microphone, recording the audio from an Assisted Listening Device, or directly from the audio rack in the projection room. In other words, it would be hardest to gain access to the projection room (requiring collusion with the projectionist, if the projectionist is a different party than the recorder) to record the audio feed directly, but would also produce the highest quality recording.

[01] If the audio track is not already immediately separately available (e.g. if the camcorder produces a video file which contains both audio and video streams combined, or muxed, into a single file such as an MP4 or AVI), it is necessary to isolate the audio track by extracting, or demuxing, the audio stream from the container file. To do so, download, install, and launch Avidemux (v. 2.6.0)<sup>747</sup>.

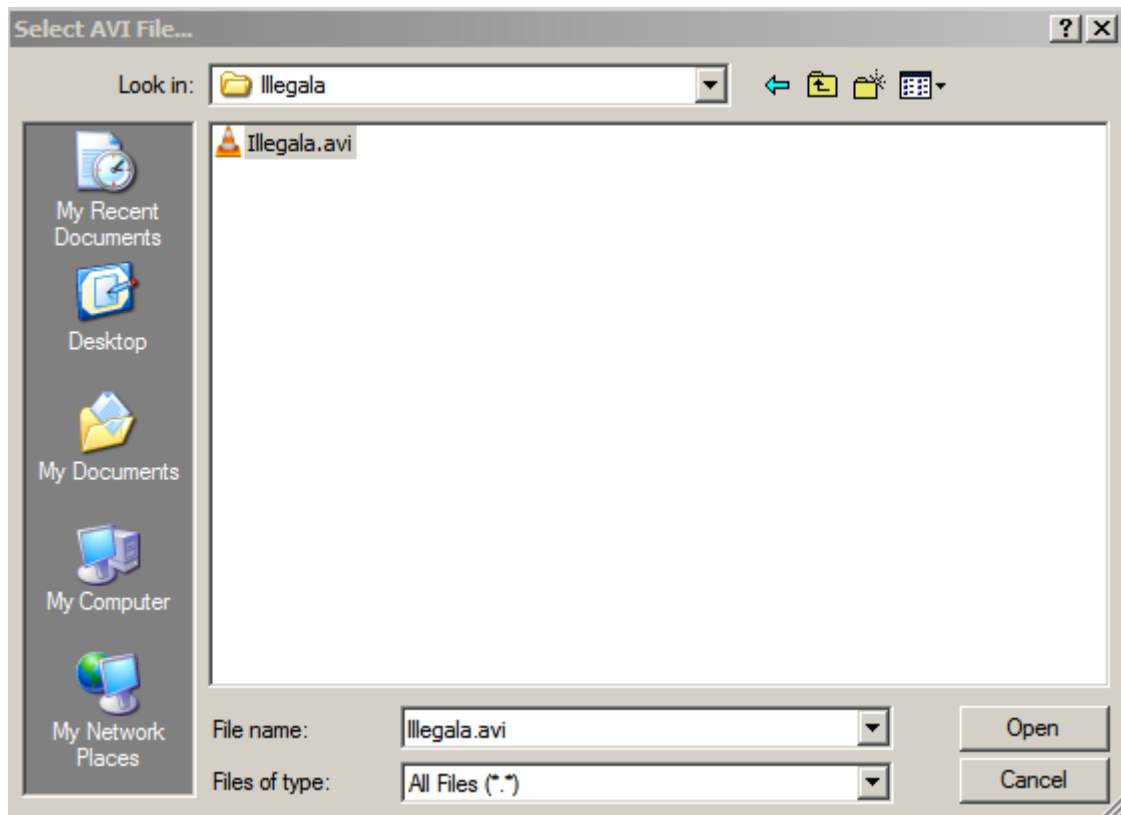
---

<sup>747</sup> Mean, 2012, *op. cit.*

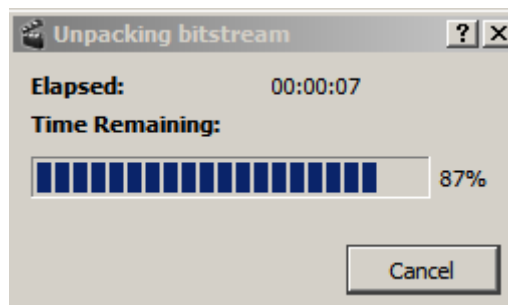


**Figure A3.01.0** New Avidemux (v. 2.6.0) window.

[02] Load the container file into Avidemux by going to File → Open, or by pressing Ctrl-O.

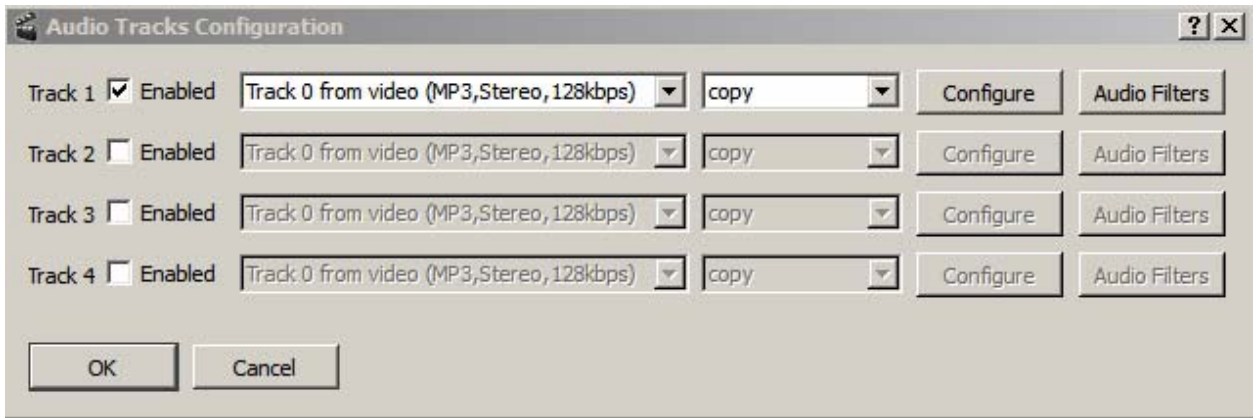


**Figure A3.02.0** Avidemux (v. 2.6.0) File Open window.



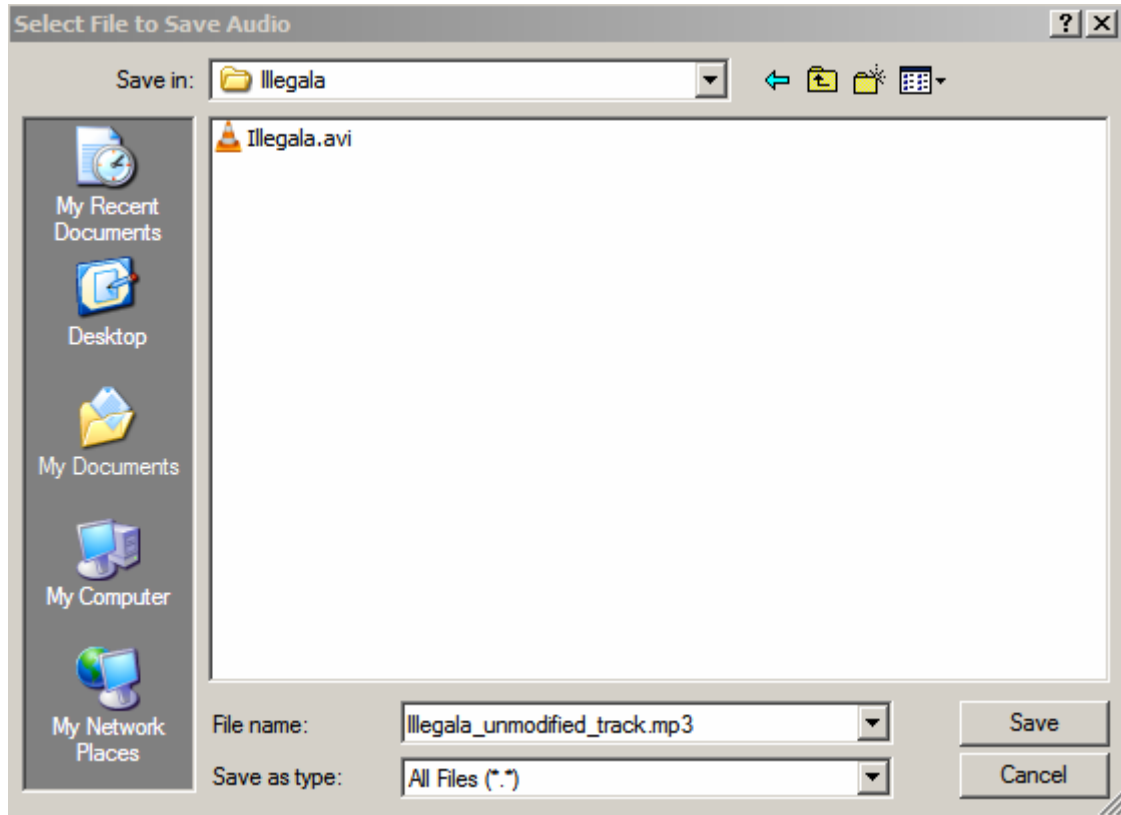
**Figure A3.02.1** Avidemux (v. 2.6.0) in the process of opening the sample file, Illegala.avi.

[03] To extract, or demux, the audio stream so as to have a separate audio file, instead of an audio-video file to work with, proceed to Audio → Select Track and select the watermarked audio track (there will generally only be one audio track; if the copy of the film also has a foreign-dub track which may also be watermarked, then the steps will need to be repeated for each track). Select 'copy' to avoid re-encoding the audio track at this stage, as selecting any other option will further needlessly decrease audio fidelity, and click 'OK'.

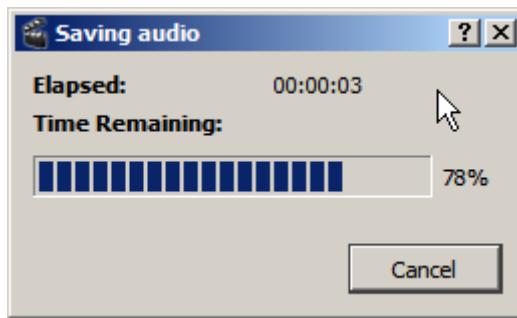


**Figure A3.03.0** Avidemux Audio Track Selection window.

[04] Proceed to Audio → Save audio to save the audio track as a separate audio file.



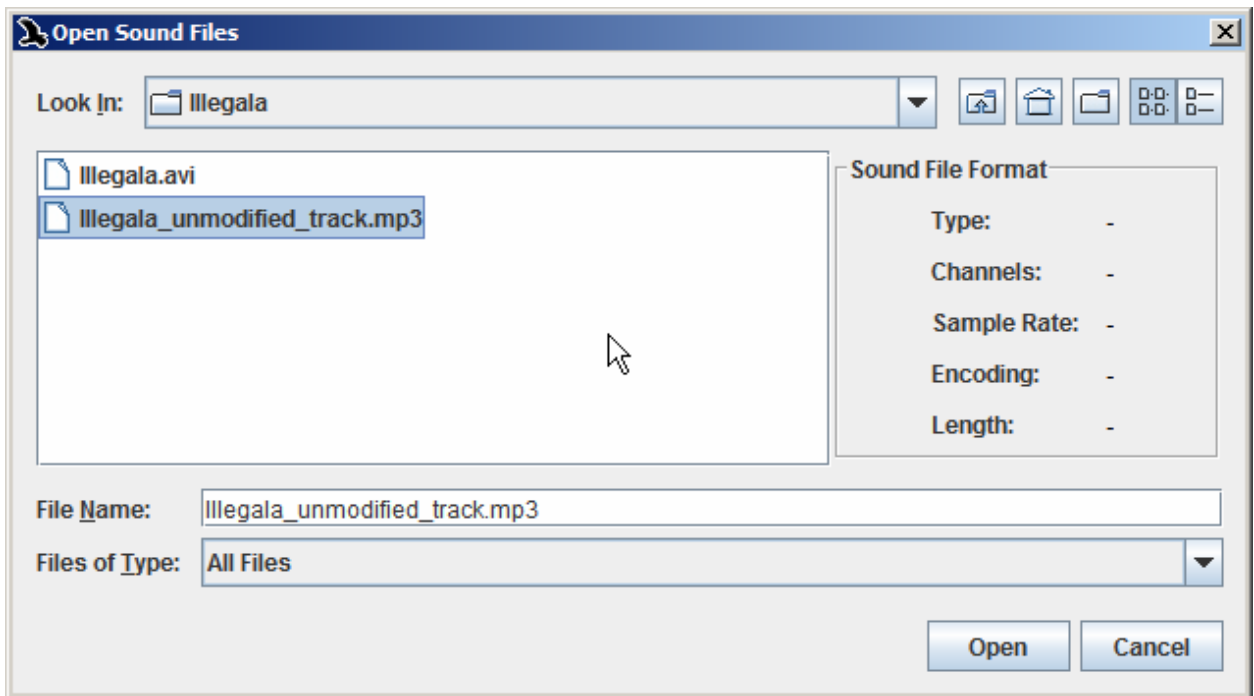
**Figure A3.04.0** Avidemux Audio Track Save window.



**Figure A3.04.1** Avidemux in the process of saving the audio track being extracted, *Illegala\_unmodified\_track.mp3*.

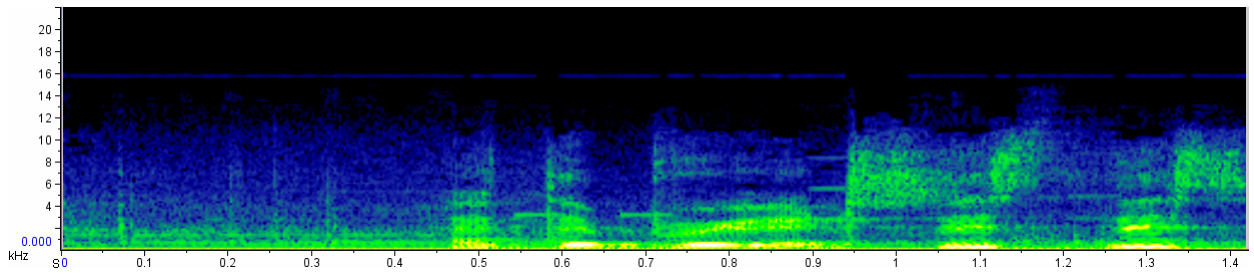
## II. Watermark Identification and Neutralization

[05] Open the extracted audio track in the Raven Lite spectral analyzer application<sup>748</sup> by going to File → Open Sound Files, or by pressing Ctrl-O.



**Figure A3.05.0** Raven Lite Open Sound Files window.

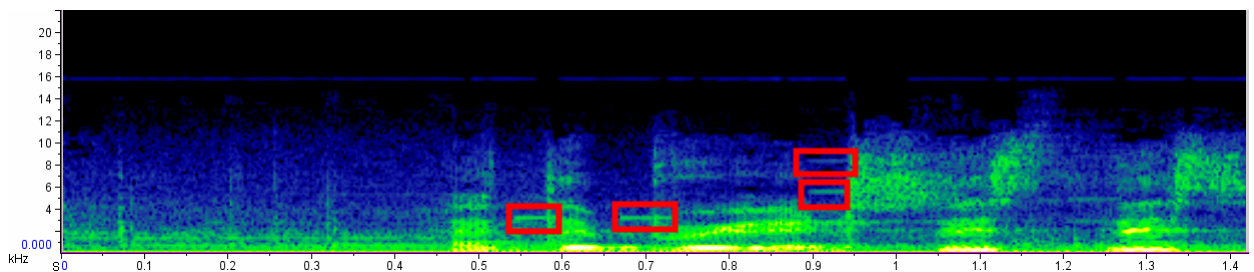
<sup>748</sup> Bioacoustics Research Program, Cornell Lab of Ornithology, *op. cit.*



**Figure A3.05.1** Raven Lite spectrogram for the file *Illegala\_unmodified\_track.mp3*.

In contrast to the generally variable frequency of human speech, a perfectly static frequency over a period of time could betray the presence of a watermark. Thus note any rectangular formations in the resulting spectrogram.

**Nota Bene:** Static frequency over time blocks are not necessarily indicative of the presence of auditory forensic markers, as they can also be depictions of musical portions of the soundtrack, of bird calls, and other audio occurrences. Thus be sure to listen to the audio track to help discern the presence of watermarks (see Step 10).

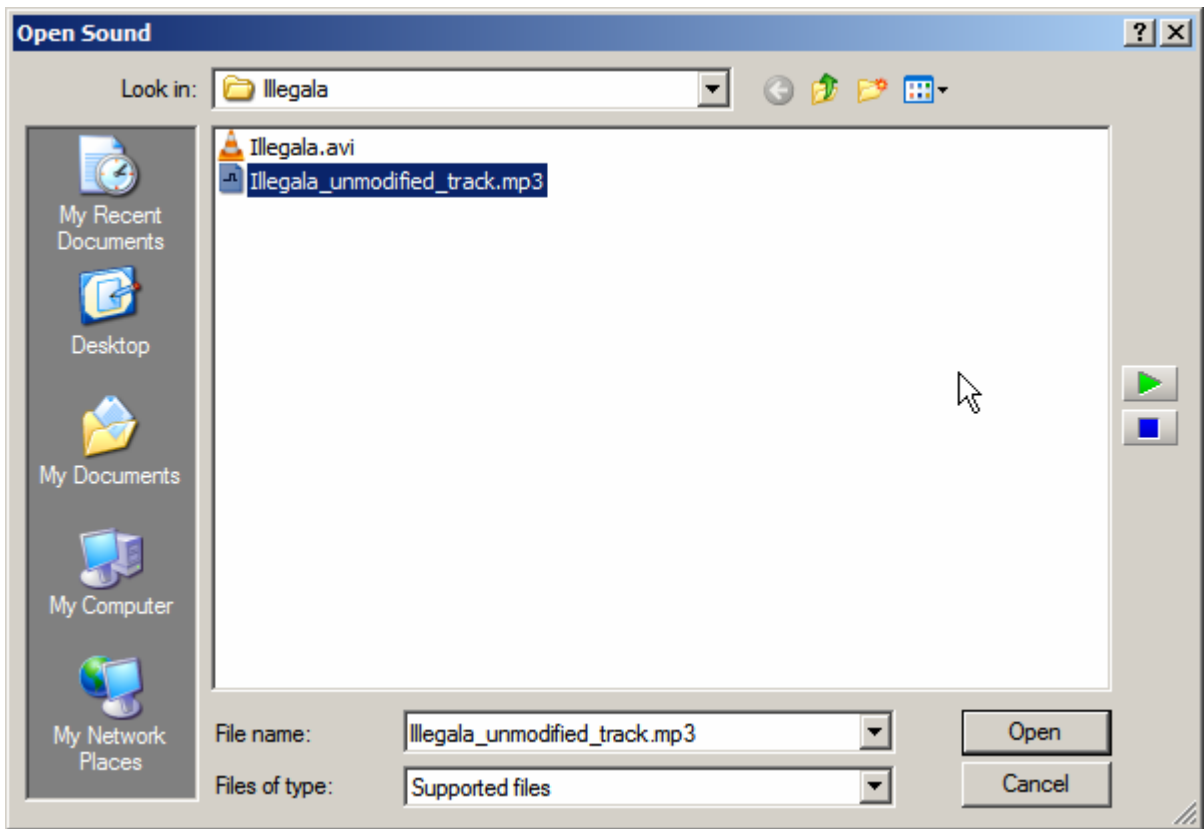


**Figure A3.05.2** Raven Lite spectrogram for the file *Illegala\_unmodified\_track.mp3*, with suspect blocks highlighted (in the Figure A3.only) to emphasize the suspect blocks.

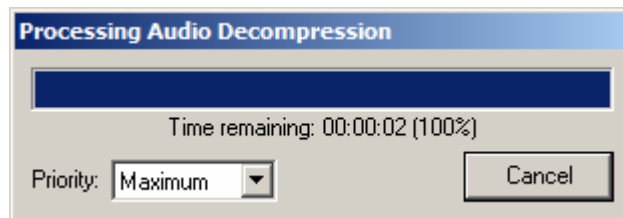
[06] Now that suspect watermarks have been identified via spectral analysis, an attempt can be made to move towards their neutralization. Open the extracted audio track in the GoldWave audio editing suite<sup>749</sup> by going to File → Open, or by pressing Ctrl-O.

<sup>749</sup> Goldwave Inc., *op. cit.*



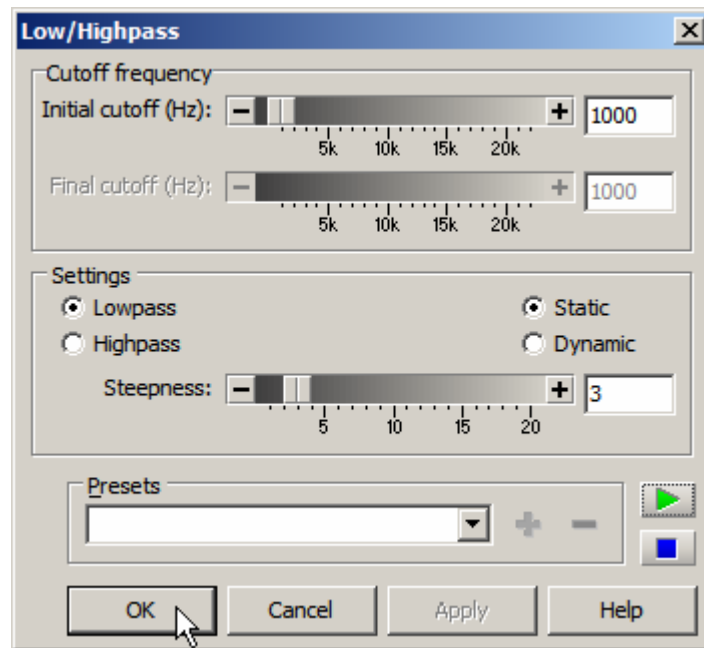


**Figure A3.06.0** GoldWave Open Sound window.



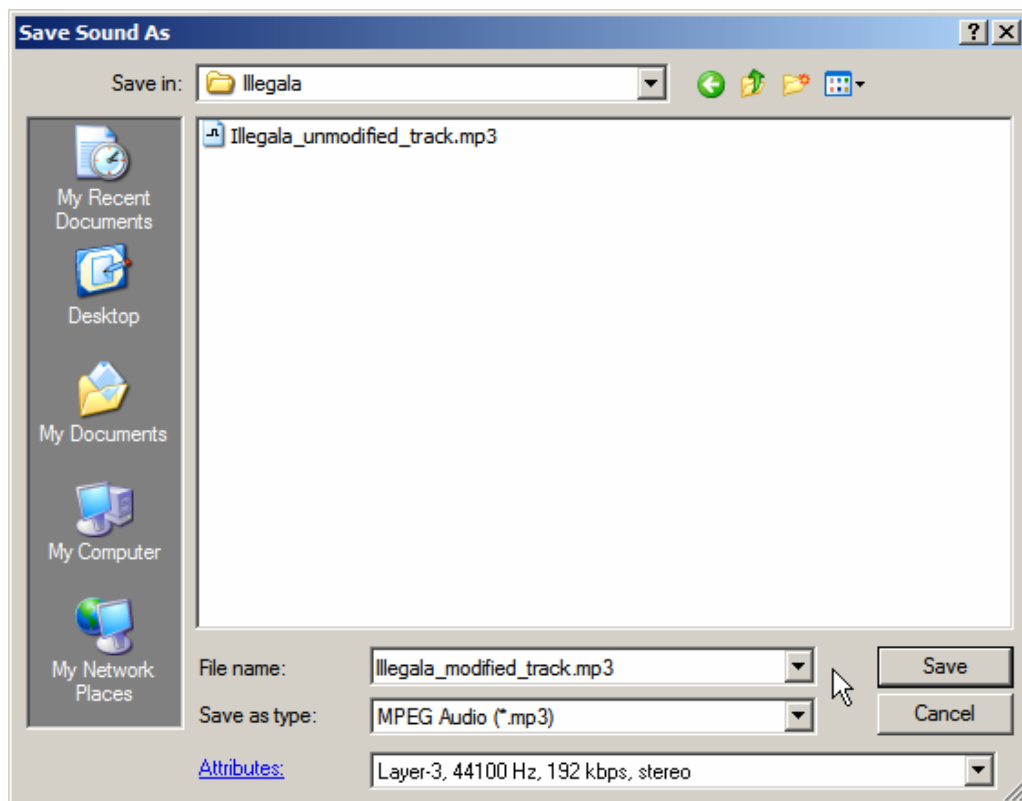
**Figure A3.06.1** GoldWave in the process of opening the file Illegala\_unmodified\_track.mp3.

[07] Proceed to Effect → Filter → Low/Highpass. Set the Cutoff frequency to an Initial cutoff of 1000 Hz. Select the Static Lowpass filter, set the Steepness level to 3, and press 'OK'.



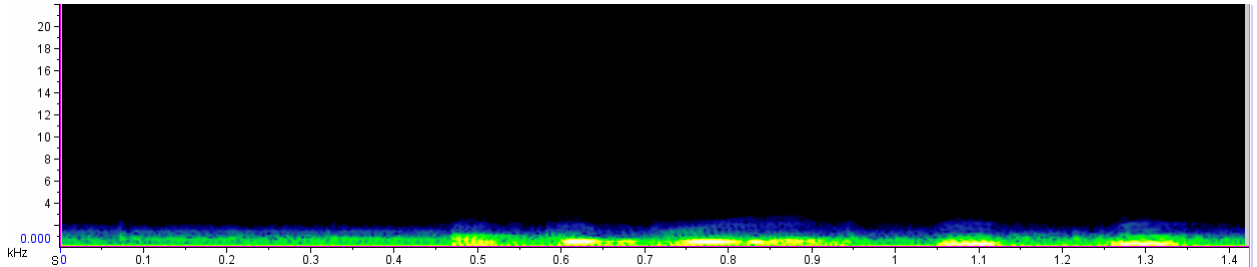
**Figure A3.07.0** GoldWave Lowpass Filter settings window.

**[08]** Save the filtered audio file by going to File → Save As, keeping the original format the audio track was in intact.



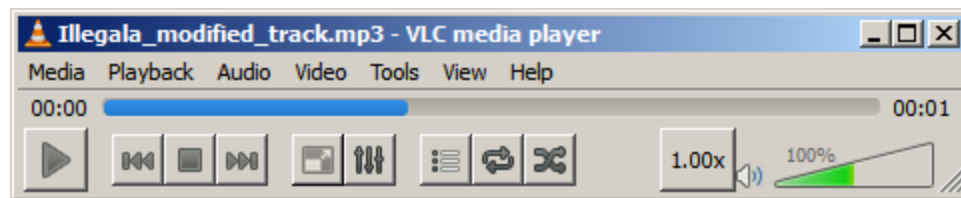
**Figure A3.08.0** GoldWave Save Sound As window.

[09] Open the modified audio track created in Step 8 (Illegala\_modified\_track.mp3) in Raven Lite, and confirm the disappearance of the suspect blocks previously seen in Step 5. If suspect blocks are still visible, return to Step 7 and increase the Steepness level by a factor of one. Repeat as necessary until suspect blocks have disappeared.



**Figure A3.09.0** Raven Lite spectrogram for the file Illegala\_modified\_track.mp3. Note the absence of suspect blocks.

[10] Listen to the modified audio track created in Step 8 (Illegala\_modified\_track.mp3) in an audio player, such as VLC media player<sup>750</sup>, to confirm there are no audible audio forensic markers which can be audibly discerned.



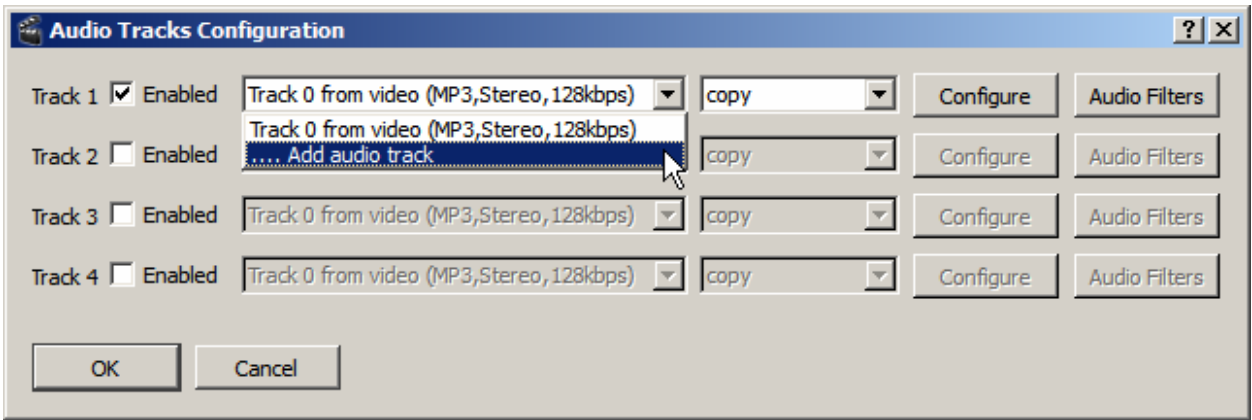
**Figure A3.10.0** The file Illegala\_modified\_track.mp3 opened in VLC media player for playback analysis.

### III. Recombination

[11] Returning to Avidemux (repeating Step 2 if Avidemux was closed), proceed to the Audio Track Selection window (Audio → Select Track). Select ‘.... Add audio track’ from the Track drop-down menu.

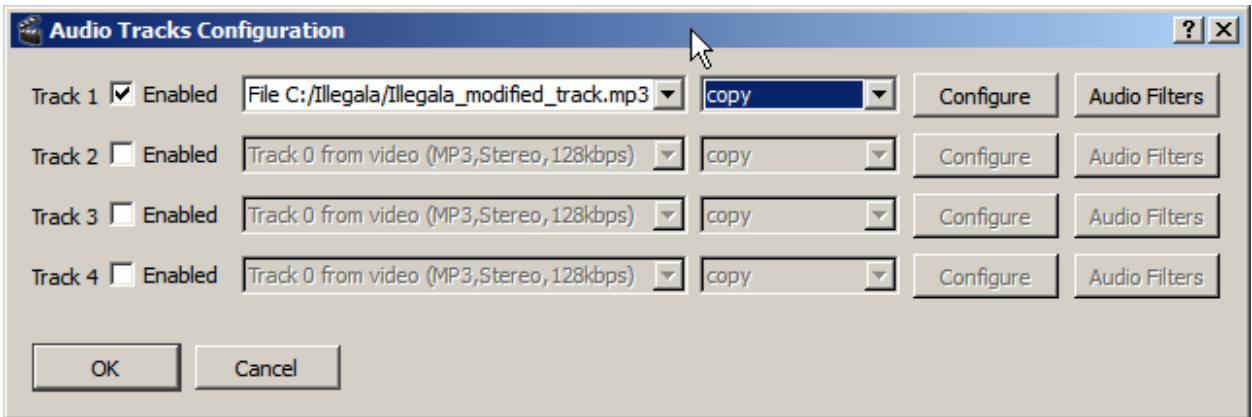
---

<sup>750</sup> VideoLAN Team, *op. cit.*



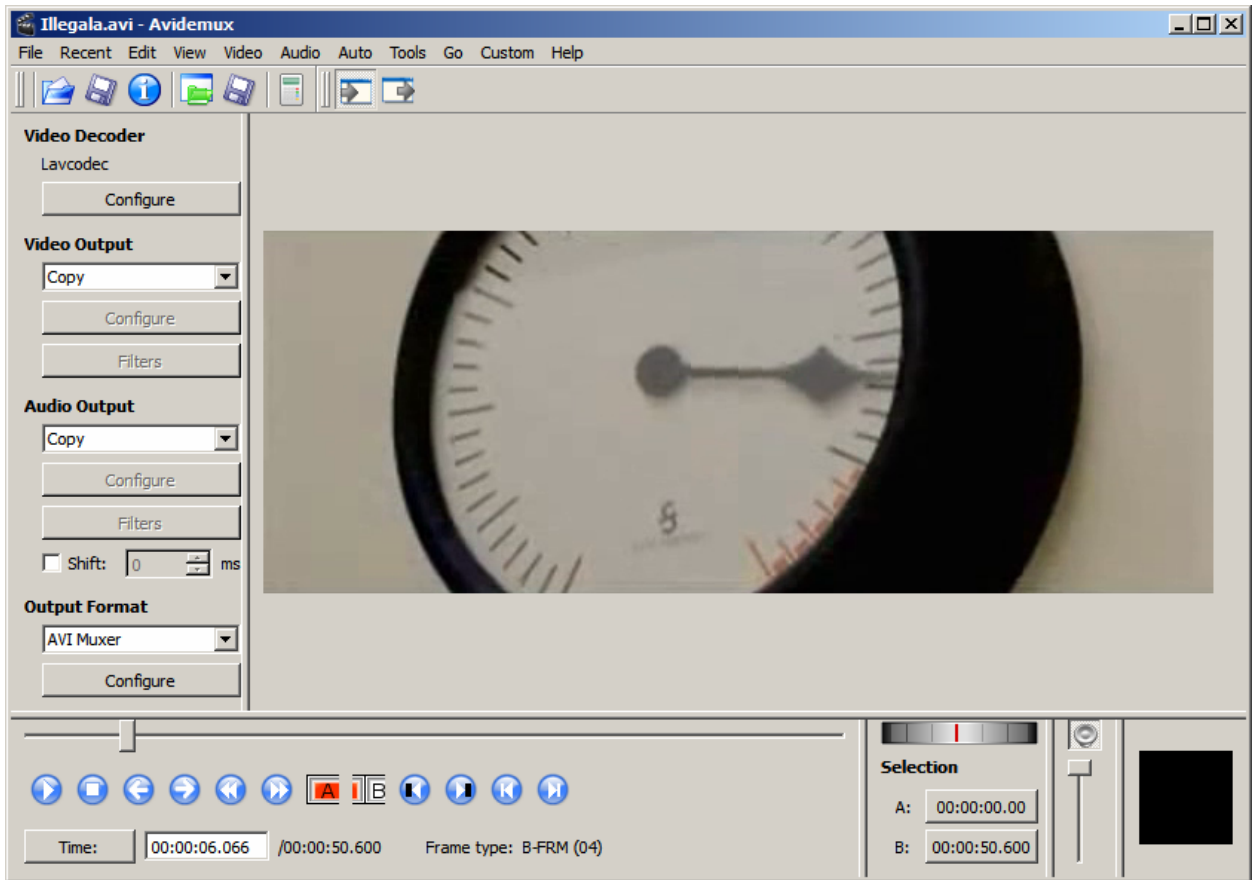
**Figure A3.11.0** Avidemux Audio Tracks Configuration window, showing the Track drop-down menu.

[12] Select the modified audio track created in Step 8 (Illegala\_modified\_track.mp3) and select 'Copy' for the output format and press 'OK'.



**Figure A3.12.0** Avidemux Audio Tracks Configuration window, showing the modified audio track replacing the original track.

[13] Being sure both Video Output and Audio Output are set to Copy in the main Avidemux window so as not to needlessly further decrease the video and audio quality, proceed to File → Save As (or press Ctrl-S) to save the new container file, containing the original video stream and the modified audio stream.



**Figure A3.13.0** Main Avidemux panel, showing both Video and Audio Output fields being set to Copy to avoid unnecessary quality deterioration.

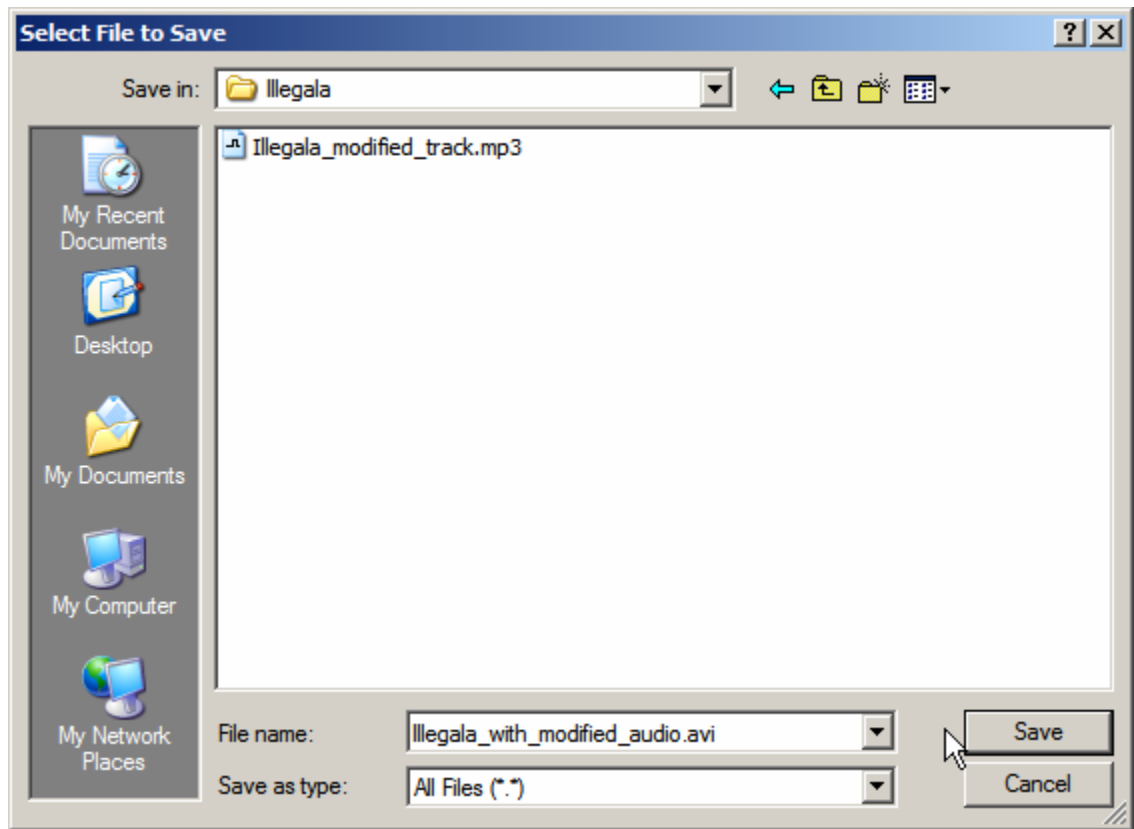


Figure A3.13.1 Avidemux (v. 2.6.0) Select File to Save window.

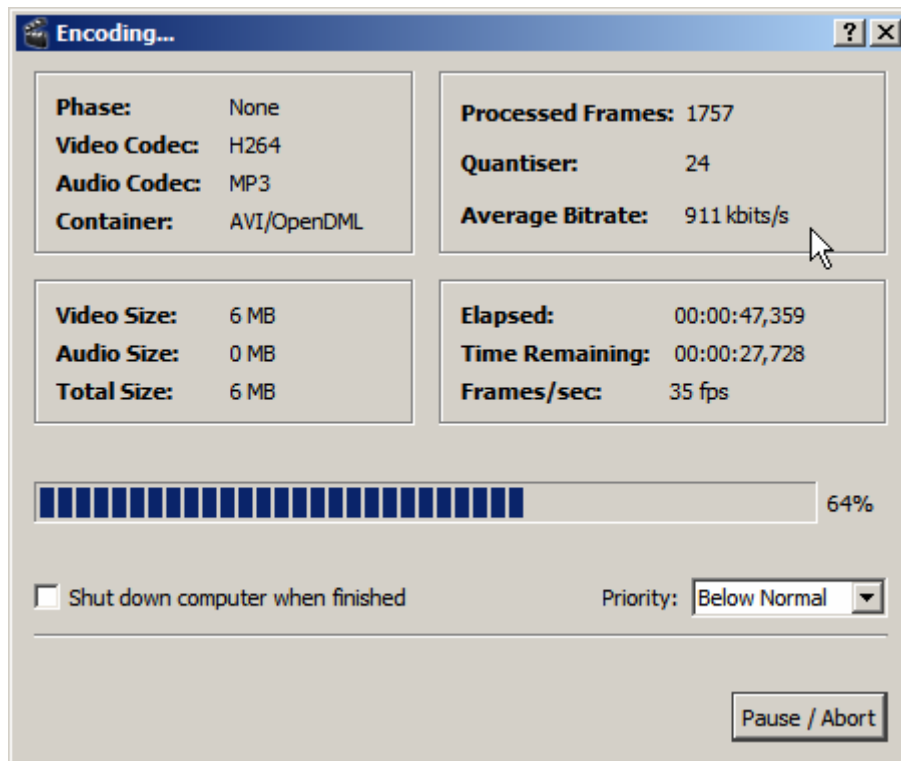
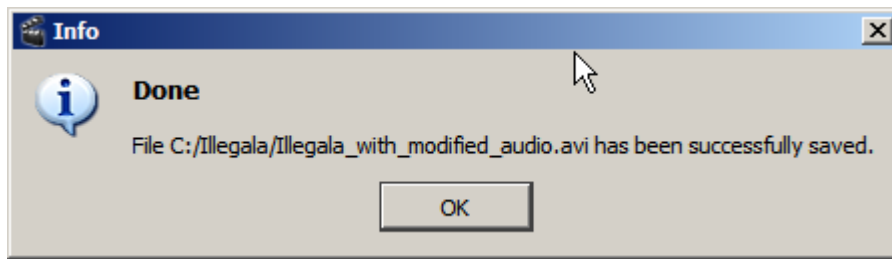


Figure A3.13.2 Avidemux (v. 2.6.0) Encoding... window.



**Figure A3.13.3** Avidemux (v. 2.6.0) Save process completion notification window.

#### **IV. Completion**

[14] The workflow is at this stage complete with the auditory forensic markers having successfully been identified and neutralized, and the audio track remuxed back into the audio/video container file. Prior to distribution, the video file should now be checked for the presence of visual forensic markers in the video stream (Appendix 5).

## Appendix 4:

# Examples of Cinematic Visual Forensic Watermarks in Select Film Frames

This appendix presents an exhibit collection of film frames which have been tagged with visual forensic markers<sup>751</sup>. Refer to §3.3.2 ‘Primary Location Tracking [VFM; L1]’ of the dissertation for further discussion of cinematic visual forensic markers.



**Figure A4.0** Primary example of visual forensic markers in a scattershot array.



**Figure A4.1** Secondary example of visual forensic markers in a scattershot array.

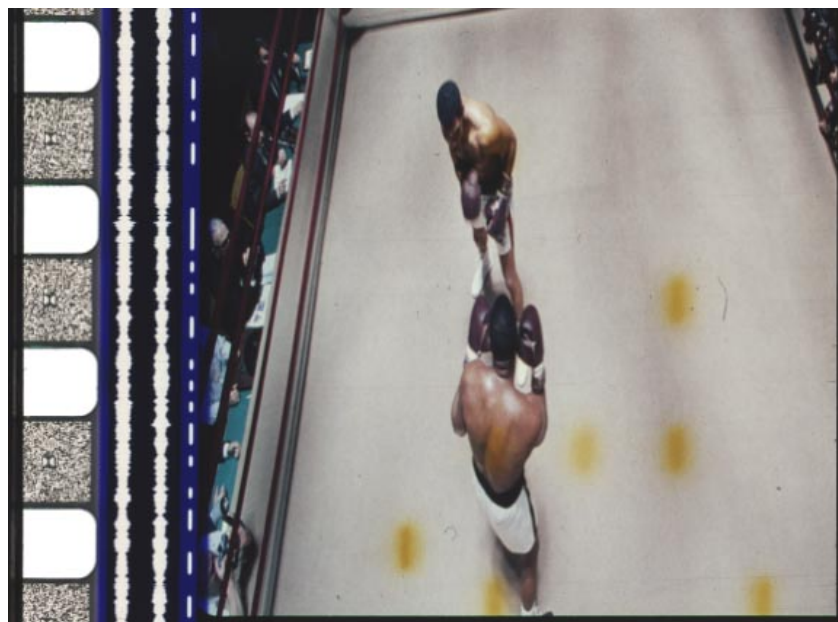
---

<sup>751</sup> Sample film frames provided by anonymous sources. Refer to Disclaimer of Liability.





**Figure A4.2** Tertiary example of visual forensic markers in a scattershot array.



**Figure A4.3** Quaternary example of visual forensic markers in a scattershot array.



**Figure A4.4** Primary example of ‘thin’ visual forensic markers in scattershot array.



**Figure A4.5** Primary example of visual forensic markers in a hybrid linear and scattershot array.



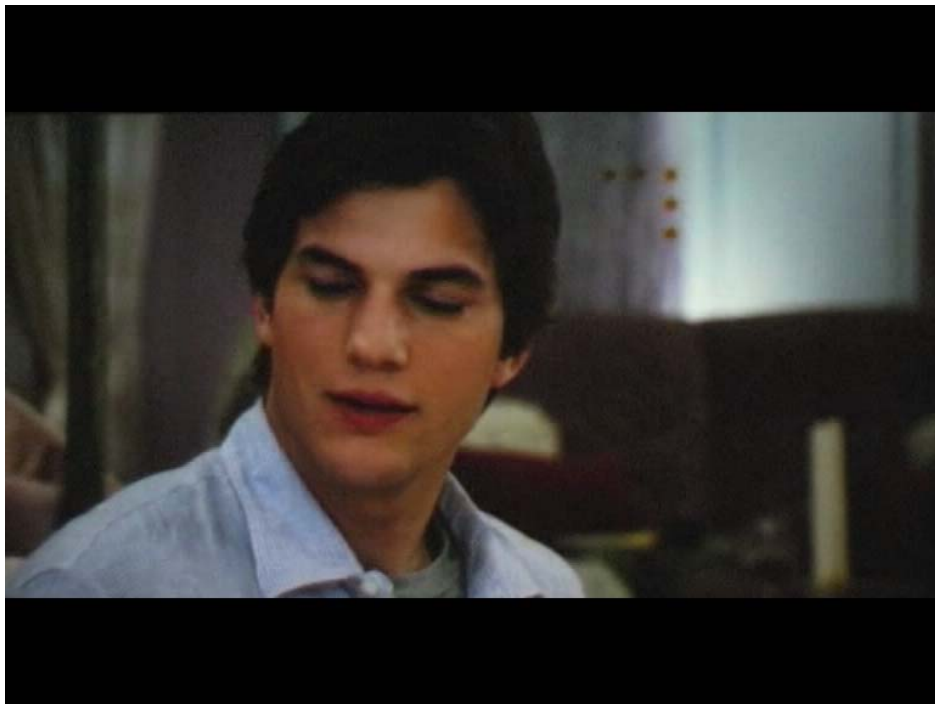
**Figure A4.6** Secondary example of visual forensic markers in a hybrid linear and scattershot array.



**Figure A4.7** Primary example of visual forensic markers in a 'T' array.



**Figure A4.8** Secondary example of visual forensic markers in a 'T' array.



**Figure A4.9** Primary example of visual forensic markers in a turned-L ('L') array.

## **Appendix 5:**

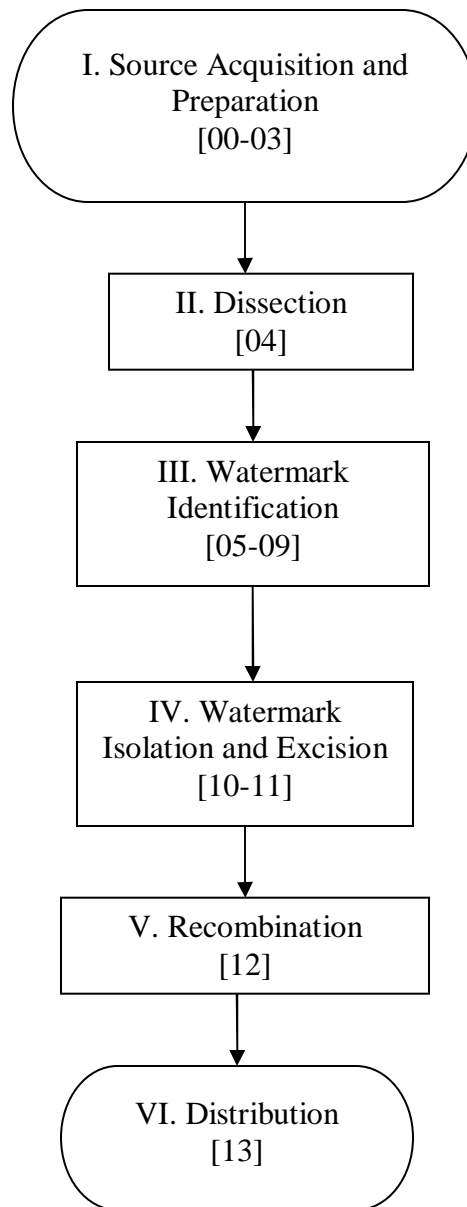
# **Sample Emancipato-Surgical Operation for Visual Forensic Marker Excision**

This case study presents an illustrated and annotated workflow for removing video-based watermarks from a sample cammed video of the film *Illegala*<sup>752</sup>. Refer to §3.3.2.0 ‘Case Study 5: Emancipato-Surgical Operation for Visual Forensic Marker Excision’ of the dissertation for analysis of and reflection on the case study.

The general workflow schema can be visualized as follows (with accompanying procedural step numbers):

---

<sup>752</sup> As previously noted, title is fictional. Refer to Disclaimer of Liability. Watermarked video sample courtesy of [anonymous].



## **I. Source Acquisition and Preparation**

**[00]** Procure a CAM for analysis and watermark excision. Steady cam work can be achieved by balancing the camera snugly in the gap between two seats in the row immediately in front of where the cammer is situated. Alternatively, the camera may be clipped to the seat in front of the cammer by using a miniature tripod clip. If access to the projection booth can be negotiated, the camera can then be placed on a full tripod or balanced on a flat surface. Black electrical tape should be placed over all camera light emissions (such as the red recording light and green power light) to minimize chances of detection and apprehension. The camera

display panel(s) should likewise be shut, dimmed, turned off, or taped over as well. A coat or jacket should be brought into the theater to be draped over the forward seat should an usher walk into the theater.



**Figure A5.00.0** Modified miniature tripod clip, for attaching the camcorder to the seat in front of the cammer<sup>753</sup>.

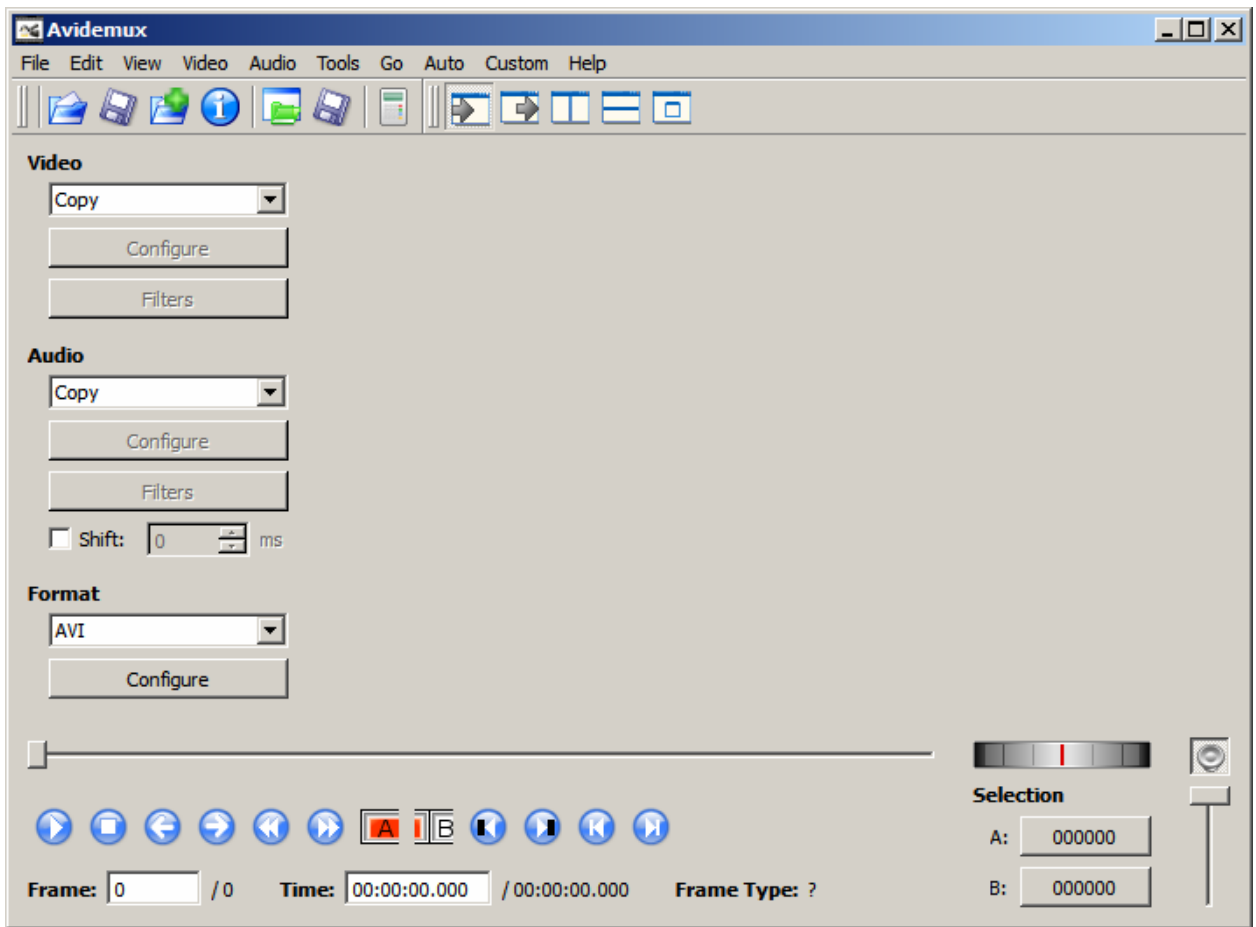
[01] Transfer the resultant CAM video file from the camcorder to the PC via the appropriate cabling, which will vary by camera (e.g. FireWire).

[02] Download, install, and launch Avidemux (v. 2.5.6)<sup>754</sup>.

---

<sup>753</sup> Image from: Motion Picture Association of America, Inc. 2012. "Tools of the Trade". *Fight Film Theft*. <http://www.fightfilmtheft.org/tools.html>. The MPAA generously provides photographs of various cammer kits for inspiration.

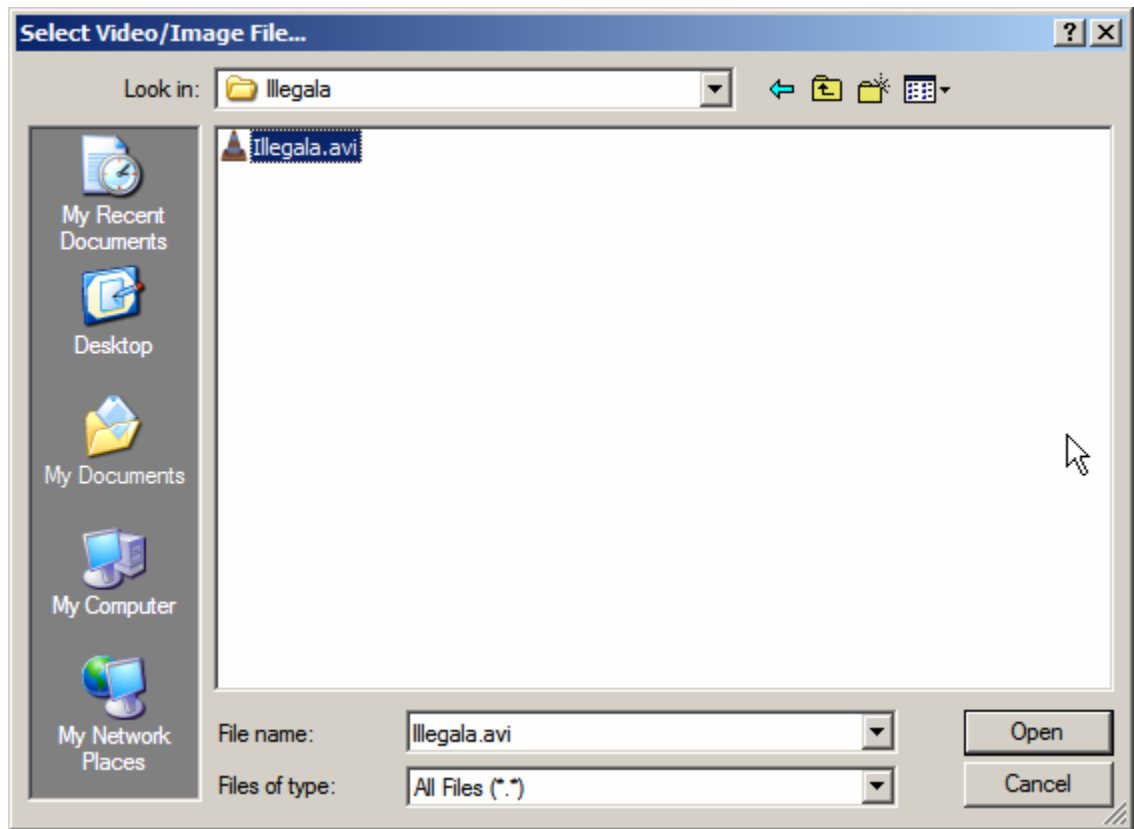
<sup>754</sup> Mean, 2010, *op. cit.*



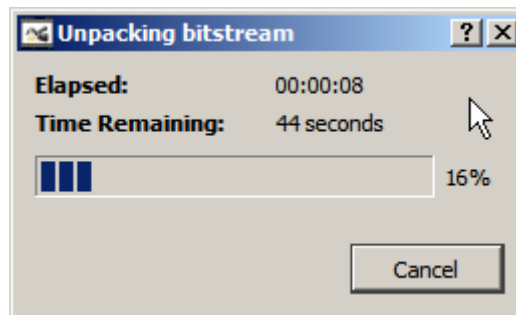
**Figure A5.02.0** New Avidemux (v. 2.5.6) window.

[03] Load the video file into Avidemux by going to File → Open, or by pressing Ctrl-O.





**Figure A5.03.0** Avidemux (v. 2.5.6) File Open window.



**Figure A5.03.1** Avidemux (v. 2.5.6) in the process of opening the sample file, Illegala.avi.

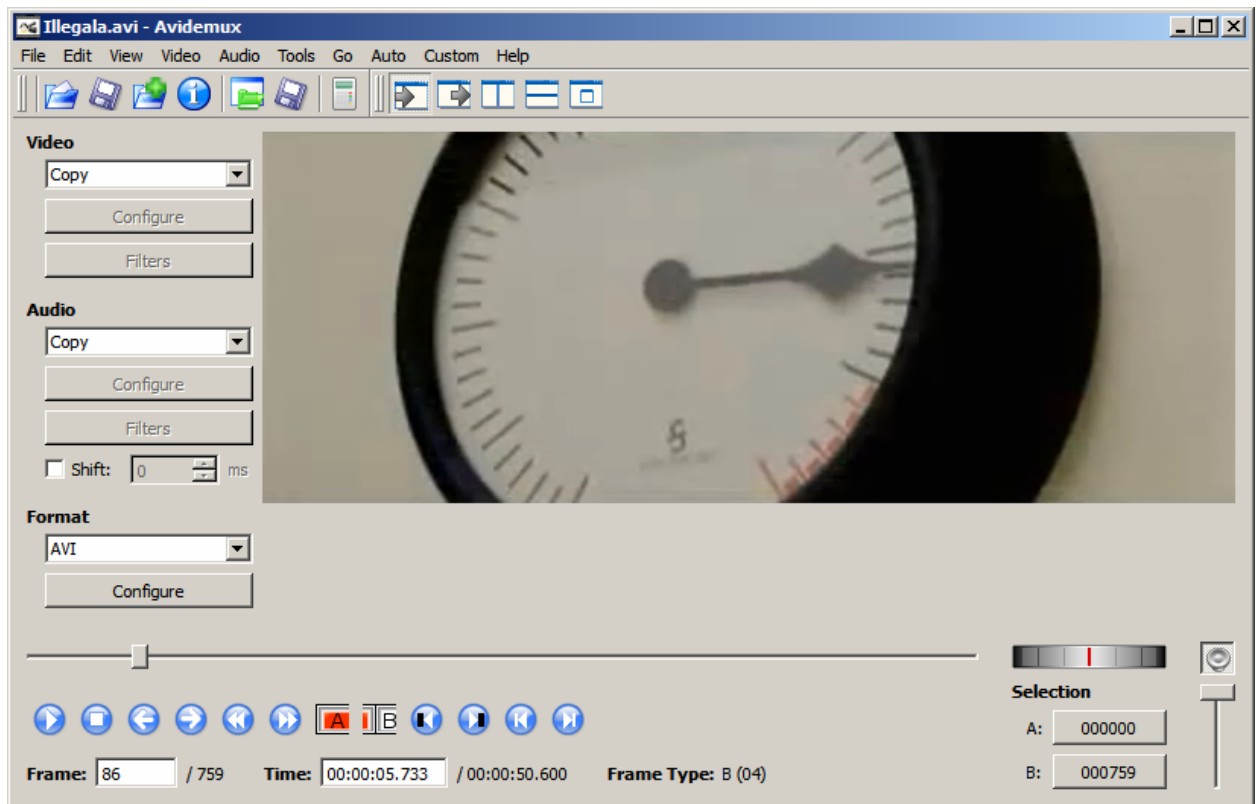


Figure A5.03.2 Illegala.avi opened in Avidemux.

## II. Dissection

[04] Extract all frames as separate images from the video file by going to File → Save → Save Selection as JPEG Images.... If saving all frames from a video file, as we are, then it is not necessary to select start and end-points, as Avidemux's default behavior for saving video frames when no start/end-points are selected is to extract all frames from the video.

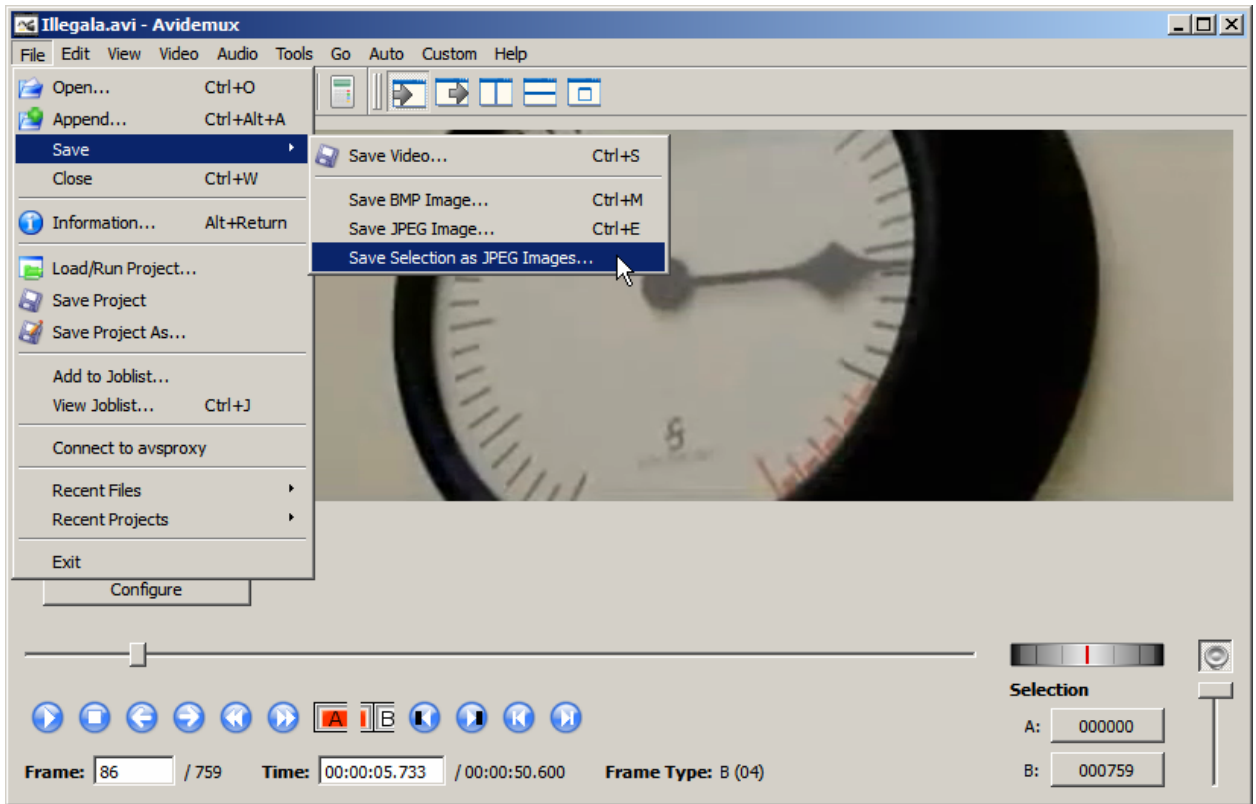


Figure A5.04.0 Avidemux Save menu.

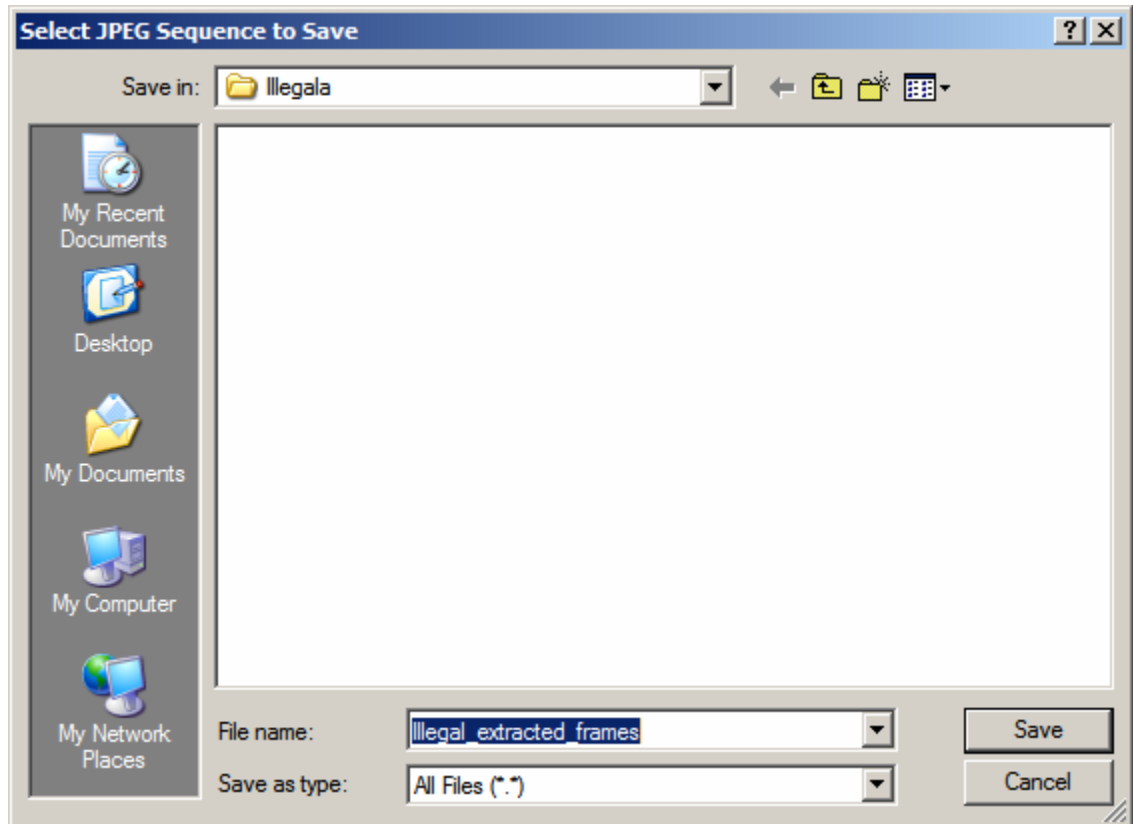
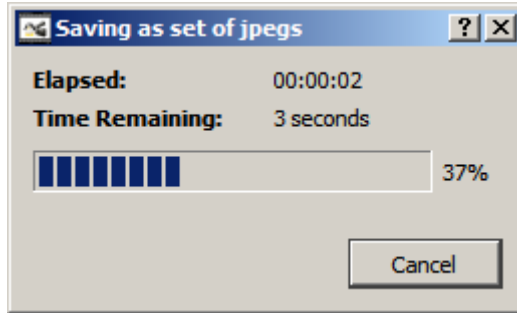
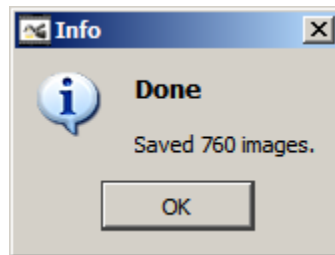


Figure A5.04.1 Avidemux Select JPEG Sequence to Save Save window.



**Figure A5.04.2** Avidemux Saving as set of jpegs progress bar.



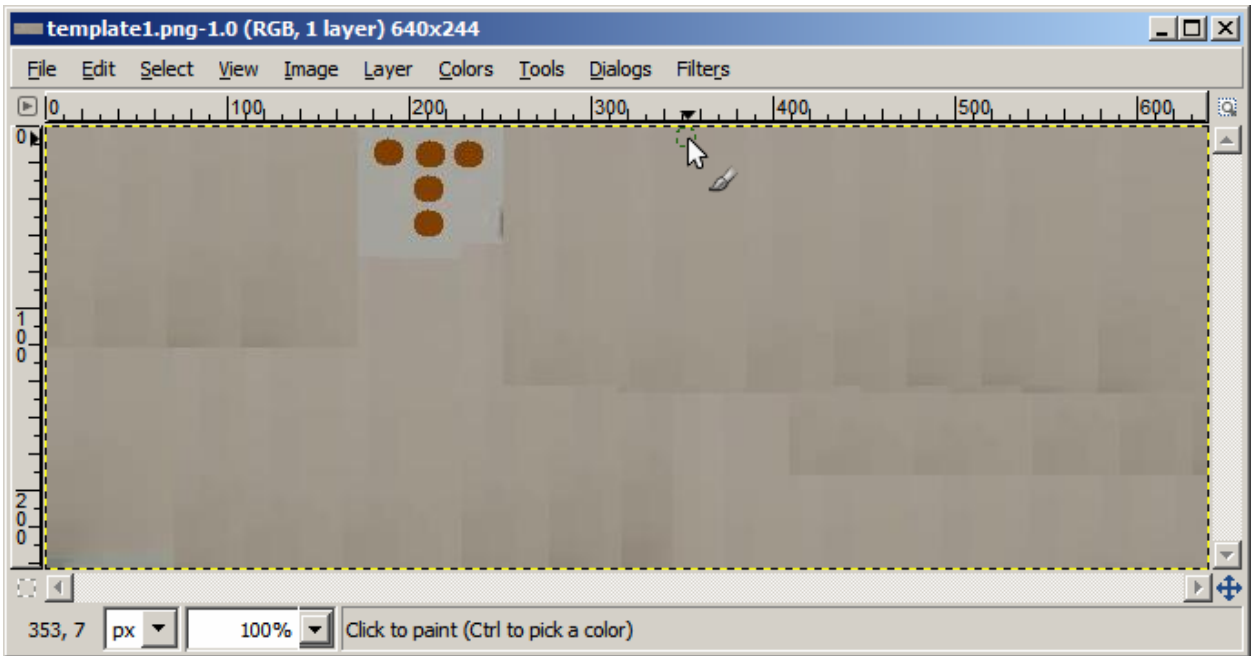
**Figure A5.04.3** Avidemux Save completion window.

### **III. Watermark Identification**

[05] Based on common watermark patterns identified in Appendix 4 (e.g. 'T' or 'L'-shaped dot formations), create pattern template files (which simply represent the watermark formations, and can be made in any general image editing software) to scan the extracted frames for any possible similar frames, which may have the same pattern. The scan is performed by using *imgSeek*<sup>755</sup>.

---

<sup>755</sup> Cabral, *op. cit.*

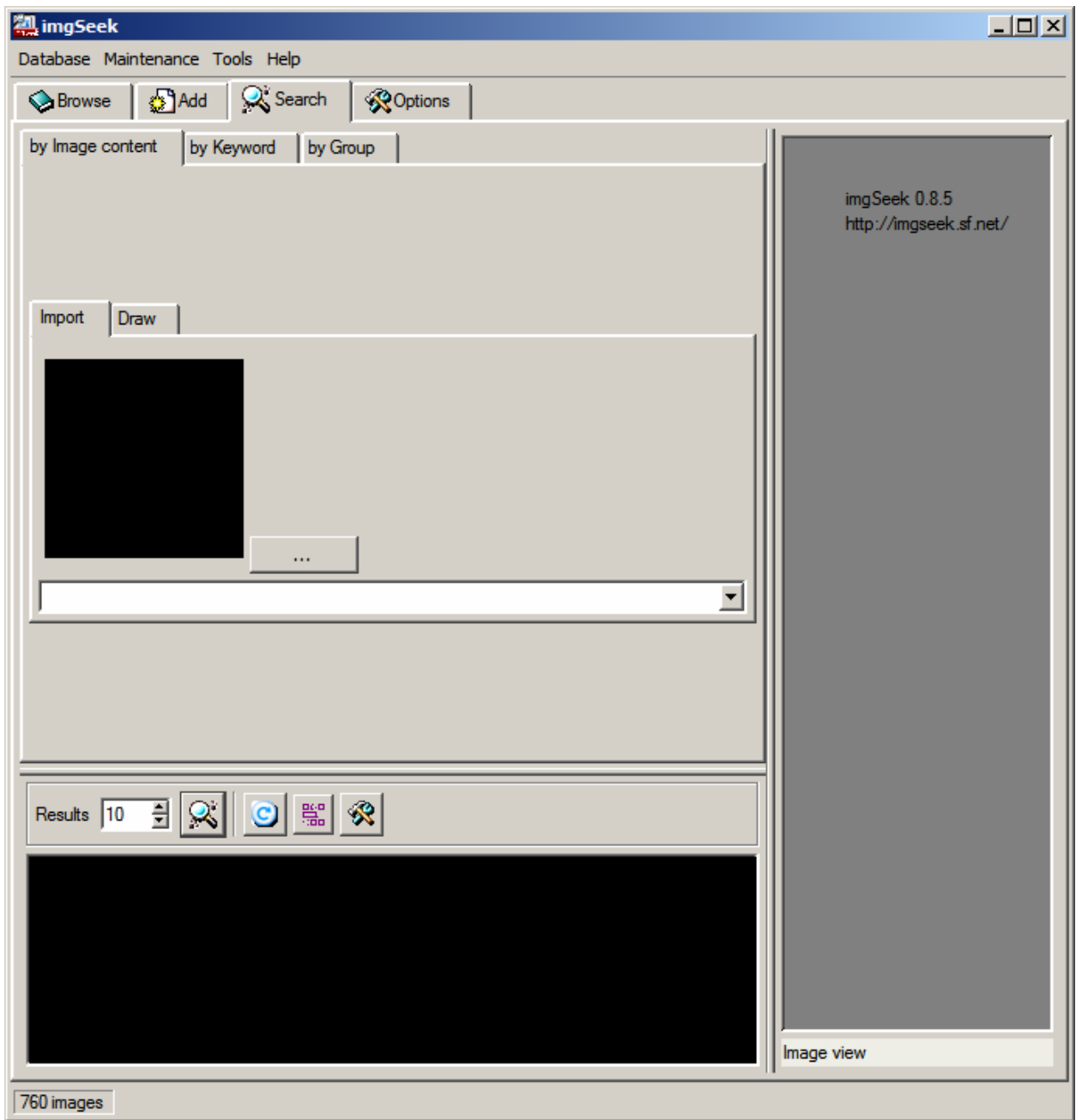


**Figure A5.05.0** Sample watermark pattern template (template1.png), created in the GNU Image Manipulation Program (GIMP) image editor<sup>756</sup>.

[06] Download, install, and launch imgSeek.

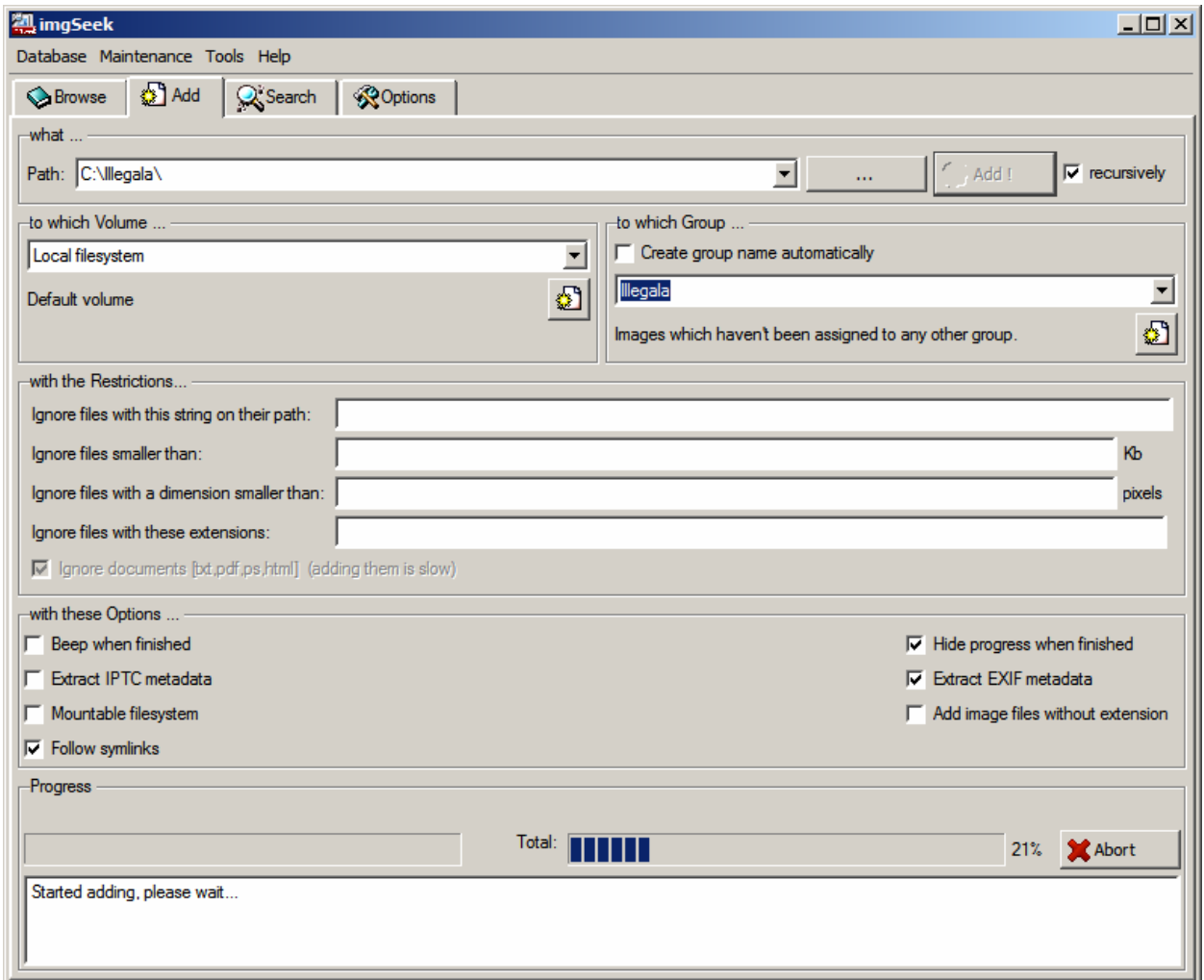
---

<sup>756</sup> Spencer Kimball, Peter Mattis, and the GIMP Development Team. 2007. GNU Image Manipulation Program. <http://www.gimp.org/>.



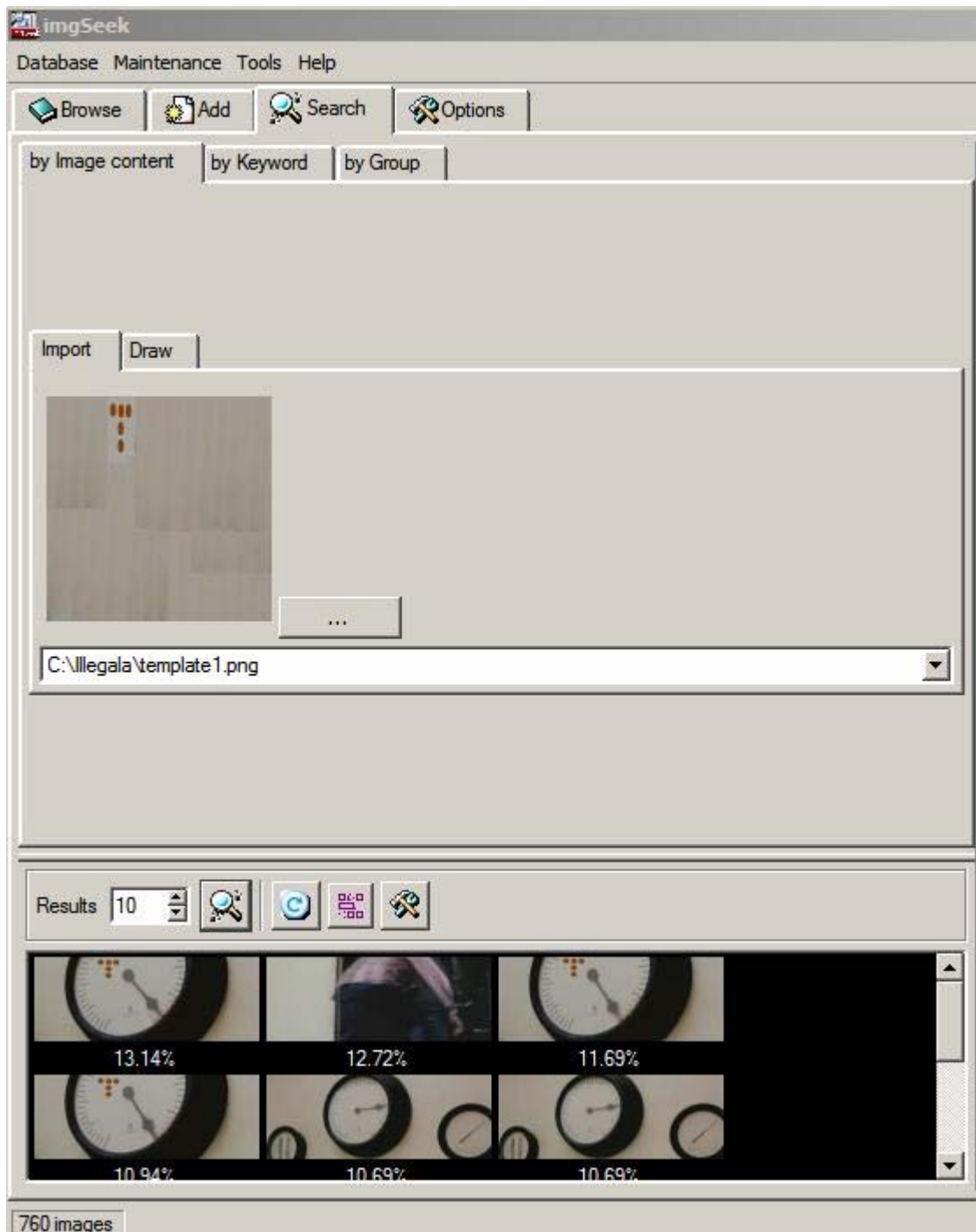
**Figure A5.06.0** New imgSeek window.

[07] Import the frames extracted in Step 4 into imgSeek by selecting the Add tab, setting Path to the same directory as the one the frames were saved to in Step 4, make certain all of the Ignore files fields are blank, and press Add.



**Figure A5.07.0** imgSeek Add images window.

[08] Select the Search tab, then the by Image content tab, and then the Import tab. Select the directory where the watermark template files (which were created independently in an image editing program prior to Step 5) are located, and select one template. The sample template being used here will be a ‘T’ dot formation. imgSeek will now search through the extracted frames directory, and return a list sorted by highest similarity to the sample template image.

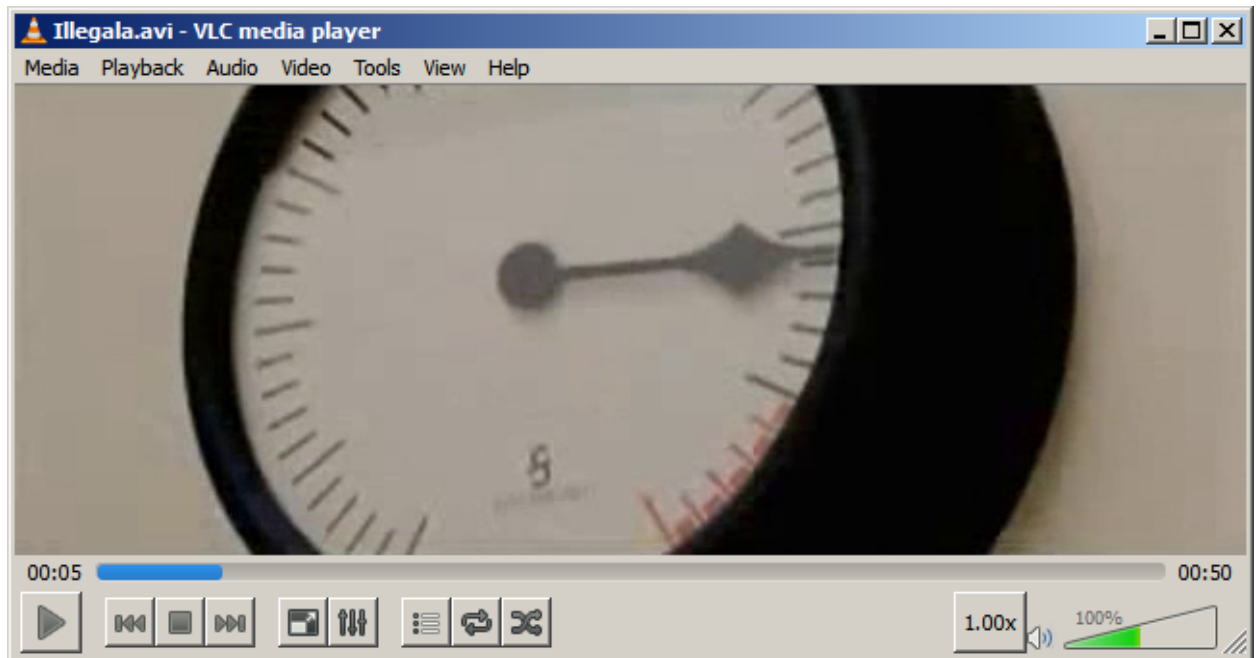


**Figure A5.08.0** imgSeek Search by Image content window.

[09] Check if any of the images returned with the highest percent similarity ratings appear to have visual forensic markers. If none are found, create a different watermark dot template and repeat step 7. If an image is found, note its filename (e.g. Illegal\_extracted\_frames0209.jpg).



[10] Due to the possibility that imgSeek may either have not found any matches, or may have missed some while finding others, a manual check will now need to be performing by going through all of the frames. This may be done in an image viewer, or the film may simply be viewed in a video player, with attention paid to any emergent dot formations.



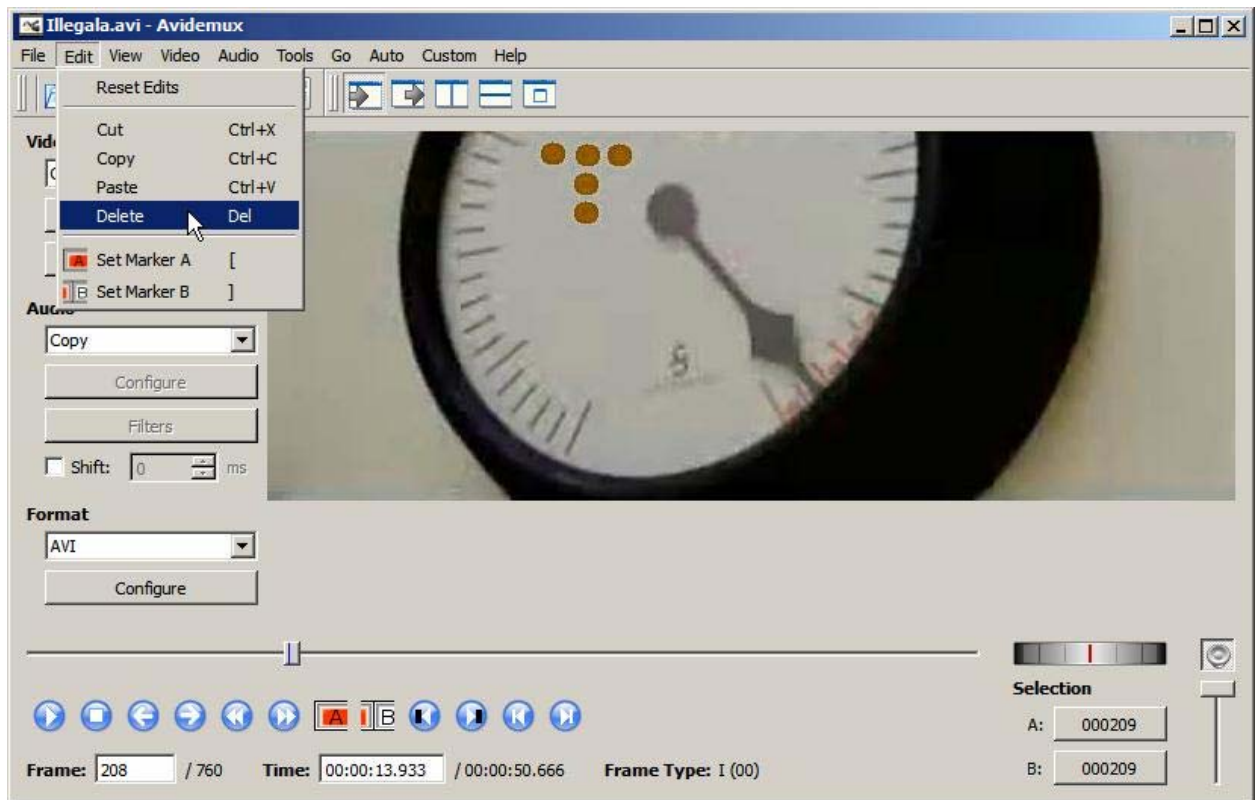
**Figure A5.10.0** The file Illegala.avi opened in VLC media player<sup>757</sup> for playback analysis.

#### IV. Watermark Isolation and Excision

[11] Returning to Avidemux (repeating Step 3 if Avidemux was closed), navigate to the watermarked frame. The number at the end of the filename identified in Step 10 corresponds to the number of the watermarked frame, minus one (e.g. Illegal\_extracted\_frames0209.jpg is frame 208, as the first frame is 0). Proceed to Edit → Delete, or press the Del key.

---

<sup>757</sup> VideoLAN Team, *op. cit.*

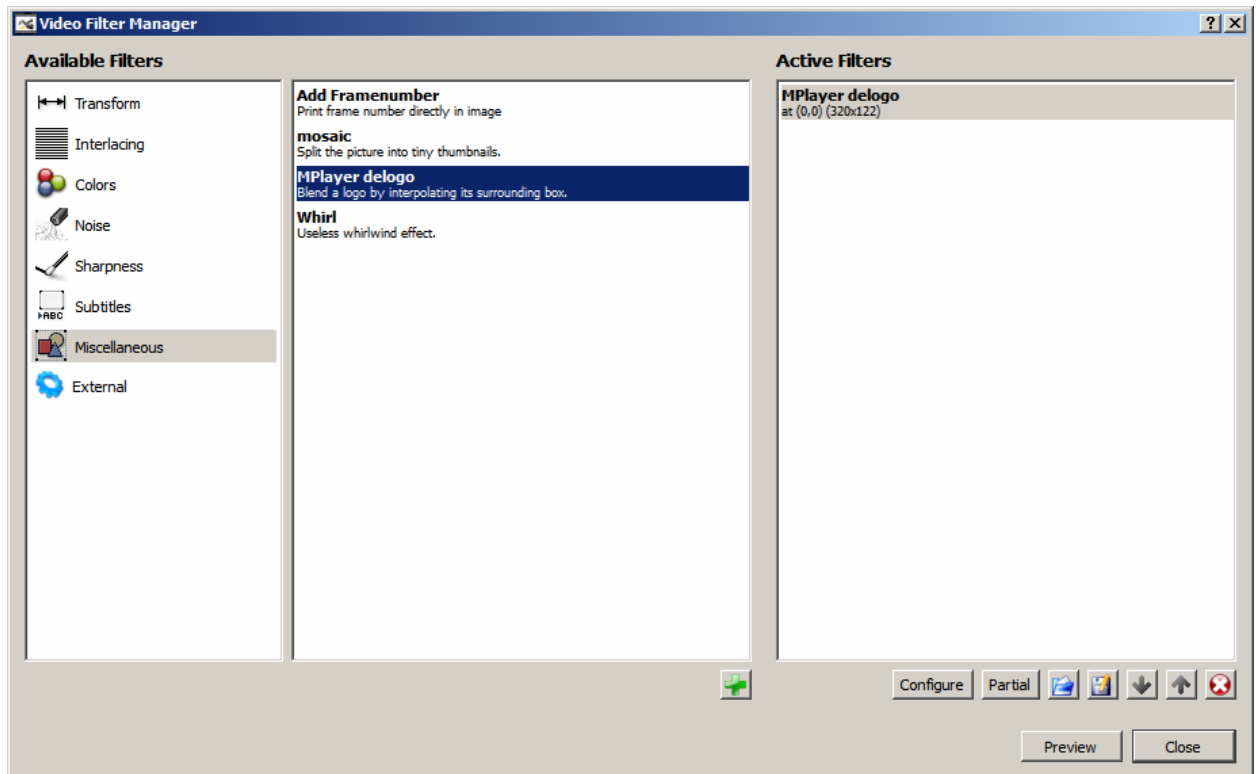


**Figure A5.11.0** Avidmeux frame deletion.

[12] If there is suspicion that the specific frame placement of the visual forensics markers is sufficient to render the modified file vulnerable to a counter-anti-forensic attack (if the content controller adversary knows the exact frame numbers at which the watermarks should be—an unlikely scenario given that frame count will likely be altered during the camming of the video from the frame count of the theatrical broadcast, due to the varying framerate of the camcorder), a previous or succeeding unwatermarked duplicate (or ‘dupe’) frame can be injected into the video file by picking the closest matching unwatermarked frame (e.g. frame 207), selecting the start and end points to select said frame, proceeding to Edit → Copy, and then immediately proceeding to Edit → Paste, thus duplicating frame 207 to now become frame 207 and 208. Thus the resultant video file will have the same number of frames as the watermarked file, albeit with a dupe unwatermarked frame inserted in place of the watermarked one.

An alternative technique to deploying dupe frames is to apply a blur filter to the watermarked frame. Select the start and end points of the watermarked frame, change the Video Output mode from Copy to an encoding format (e.g. H.263), and then proceed to Video → Filters...,

or press Ctrl-Alt-F, and then select Miscellaneous from the Available Filters menu, and finally select Mplayer delogo. Select the watermark area to be blurred. Repeat the process for all watermarks found, as they are likely to appear in different places throughout the frame, and thus a static blur filter will be ineffective.



**Figure A5.12.0** Avidemux Video Filter Manager.

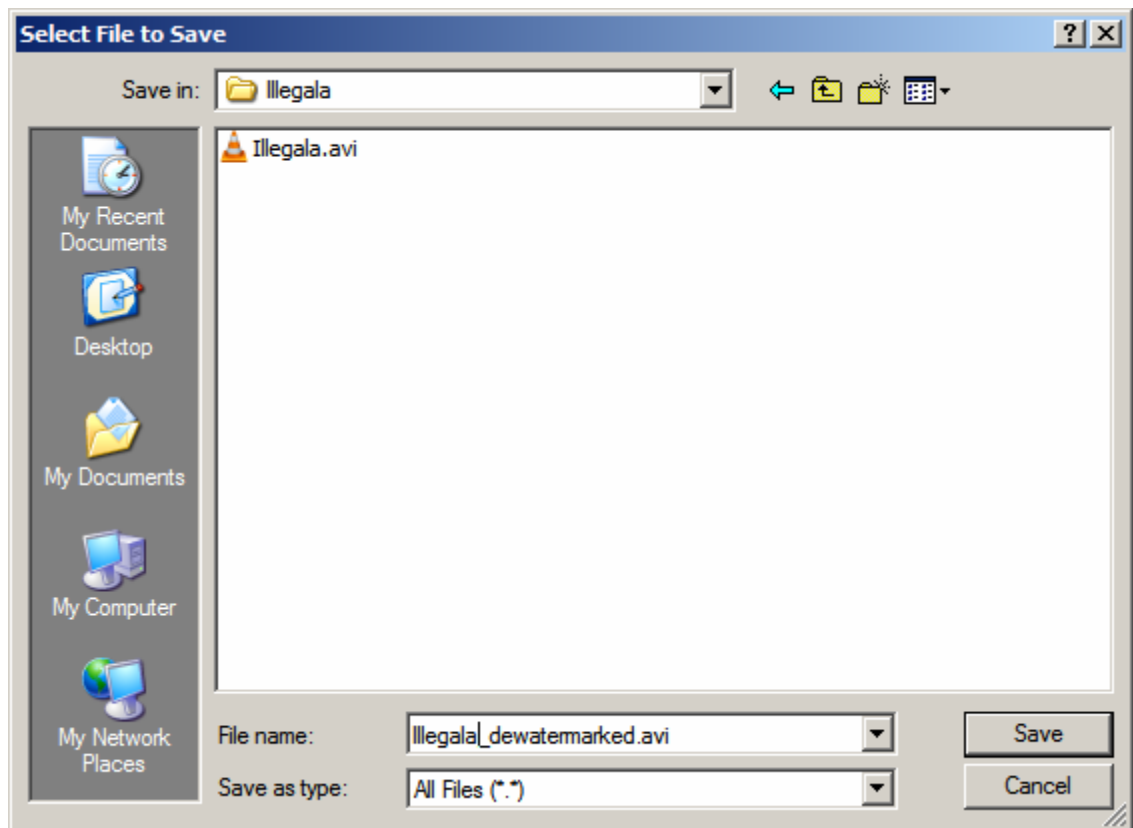
## V. Recombination

Following the successful excision of all watermarked frames:

[13] If frame deletion (and possibly dupe frame injection) were conducted, set Video and Audio to Copy in the main Avidemux window so as not to needlessly further decrease the video and audio quality, proceed to File → Save → Save Video... (or press Ctrl-S) to save the new container file, containing the dewatermarked video stream and the modified audio stream (having modified the audio stream to neutralize any present auditory forensic markers previously in Appendix 3).

If the blur filter was applied, set Video to the encoding format selected in Step 11, and Audio to Copy, and proceed to File → Save As (or press Ctrl-S) to save the new container file, containing the original video stream and the modified audio stream (having modified the audio stream to neutralize any present auditory forensic markers previously in Appendix 3).

**Nota Bene:** Depending on the encoding method and codec originally used for the video file, it may be necessary to select ‘Copy’ for Video if dupe frames were injected as well.



**Figure A5.13.0** Avidemux (v. 2.5.6) Select File to Save window.

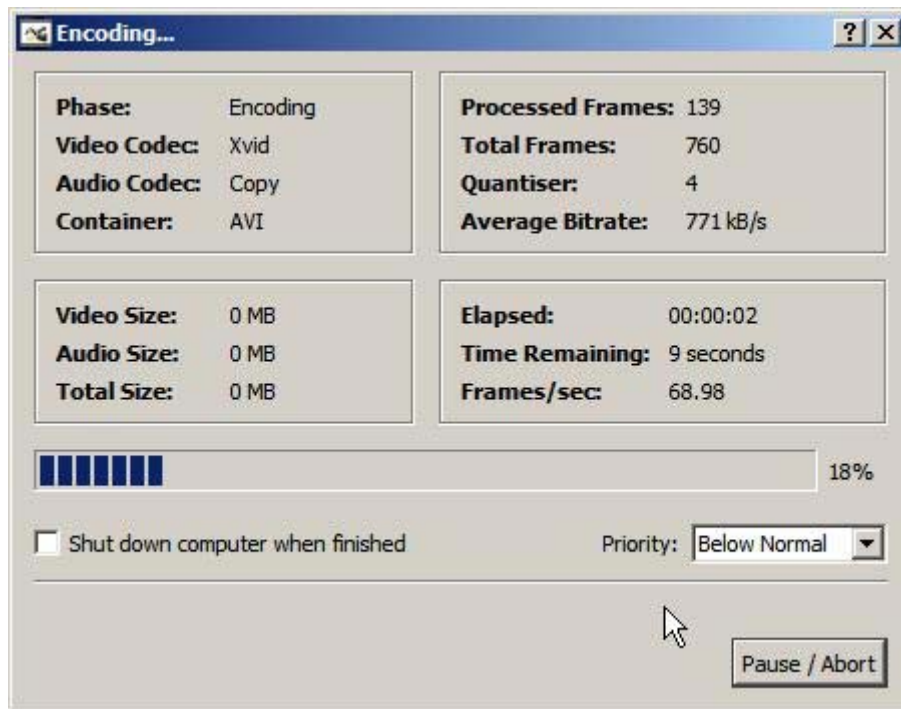


Figure A5.13.1 Avidemux (v. 2.5.6) Encoding... window.

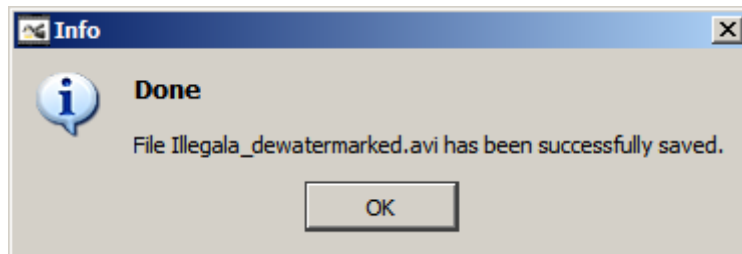


Figure A5.13.2 Avidemux (v. 2.5.6) Save process completion notification window.

## VI. Distribution

[14] The workflow is at this stage complete with the visual forensic markers having successfully been identified and excised, and—the audio forensic markers having been previously neutralized in Appendix 3—the video file is thus now ready for distribution.

## **Appendix 6:**

### **Sample User Responses to Space Puppy Grotto Notice Postings**

Notices describing SPG were posted to four private public and private web-facing torrent trackers. Four of the five trackers deleted the announcement within a few days. Below are the user responses that were recorded prior to the deletions<sup>758</sup>. Refer to §4.2 ‘Torrenting on Tor’s Onionland: An Empty Kitchen (Setting up A Tor-based Torrent Site)’ of the dissertation for analysis and discussion.

- “Doesn’t sound like it’s my cup o’ tea but good luck with it nonetheless.”
- ““Doesn’t sound like it’s my cup o’ tea but good luck with it nonetheless.”” Seconded.
- “Do they have any reptilian foot fetish vids? I am researching them for... academic purposes.”
- “Badass, definitely going to check this out, although I’m confused how tor wouldn’t fuck with my ip address that’s seeding torrents to other trackers.”
- “I’m too lazy to bother with tor. Serious any good reasons for this to be tor based? I don’t really want to even use a program that ‘seems’ to be mostly used by the Navy and pedos. I like my tinfoil hat screwed on tight.”
- “cool, but I don’t like that Tor shit, so I’ll pass.”
- “Disgusting seems to be a fitting word. Thanks, but no thanks.”
- “Motherfuck off.”
- “animal crush videos? - fuck off indeed”
- ““Disgusting seems to be a fitting word.’ fully agree! Are you serious about this tracker? if yes... thumbs down.”
- “What’s this stupid advertising message doing here, anyway ? What’s the link with Cinema ? It stinks too much.”
- “I hope this ‘announcement’ gets deleted by the mods as soon as possible.”
- “What a fucking shit. I see they using tor and they better do with a content like above. I recommend all to stay out of this shit.”

---

<sup>758</sup> User comments have been modified where it was felt necessary to preserve user and server anonymity; otherwise, they are copy and pasted verbatim from the original, deleted replies.

- “I saw the title of this thread and thought it would be complaining about a tracker like this, not advertising one. I don't think any of us are interested in animal-mutilation porn, sorry.”
- “I saw this thread already yesterday and the fact the moderators have still let it be up is so disappointing that I don't even know what to say :). Would love to hear what you feel justify links to a site like that.”
- “Looks too scary for me :(.”

# References

## Audio

Anonymous<sup>759</sup>. Unknown Film. Audio Sample of Auditory Forensic Marking.

Mason, Matt. 2008b. *My Media Musings*. Interview.

<http://mymediamusings.files.wordpress.com/2008/03/matt-pc1.mp3>.

## Software

Adobe Systems Incorporated. 2010. Adobe Acrobat Professional. v. 8.3.1.

<https://www.adobe.com/products/acrobatpro.html>. *Gratis ex gratia* availability:

<https://kickass.so/adobe-acrobat-8-professional-t7059968.html><sup>760</sup>.

Aigner, Gerhard. 2010. briss. v. 0.9. <http://sourceforge.net/projects/briss/>.

Alf, Apprentice. 2014. DeDRM Tools for Calibre. v. 6.1.0.

<https://apprenticealf.wordpress.com/2012/09/10/drm-removal-tools-for-ebooks>.

Artifex Software, Inc. 2007. Ghostscript. v. 8.60. <http://ghostscript.com/>.

Bioacoustics Research Program, Cornell Lab of Ornithology. 2009. Raven Lite. v. 1.0 build 9 update 23. <http://www.birds.cornell.edu/brp/raven/RavenOverview.html>.

BitTorrent, Inc. 2009. µTorrent v. 1.8.3. <http://www.oldversion.com/windows/utorrent-1-8-3>.

Brahms. 2012. Requiem. v. 4.1.

---

<sup>759</sup> Source and title redacted. Refer to Disclaimer of Liability.

<sup>760</sup> All URLs are provided *ex gratia* (without liability); some are further provided *gratis ex gratia* (to freely accessible content, without liability). URLs are provided to, perhaps, assist in the reproducibility of the research conducted.



<http://digiex.net/downloads/download-center-2-0/applications/11796-requiem-4-1-remove-itunes-drm-fairplay-music-video-books.html>.

Cabral, Ricardo Niederberger. 2005. imgSeek. v. 0.8.5. <http://www.imgseek.net/>.

Chinery, Philip and Frank Heindörfer. 2006. PDFCreator. v. 0.9.3.  
<http://sourceforge.net/projects/pdfcreator/>.

csoler, defnax, drbob7, thunder2. 2014. RetroShare. v. 0.5.5c 7261.  
<http://retroshare.sourceforge.net/>.

DT Soft Ltd. Daemon Tools. v. 1.39. <http://www.daemon-tools.cc>.

DVDFab. 2014. DVDFab HD Decrypter. v. 9.1. [http://www.dvdfab.cn/hd\\_decrypter.htm](http://www.dvdfab.cn/hd_decrypter.htm).

ElcomSoft Co. Ltd. 2014. Advanced PDF Password Recovery. v. 5.06.  
<https://www.elcomsoft.com/apdfpr.html>. *Gratis ex gratia* availability:  
<http://tv-release.net/324655/>.

Goldwave Inc. 2008. GoldWave. v. 5.25. <http://www.goldwave.com>.

Grimm, Dean P. 2013. WinMerge. v. 2.14.0. <http://winmerge.org>.

GetFLV.net. 2014. GetFLV. v. 9.6.8.8. <http://www.vdigger.com/>.

Hotline Communications Ltd. 2003. Hotline. v. 1.8.5.  
[http://nandafalva.hu/download/szoftver/HLClientPC1.8.5\\_Installer.exe](http://nandafalva.hu/download/szoftver/HLClientPC1.8.5_Installer.exe).

Johnson, Anthony Dean. 2014. Do It Again. v. 1.6.  
<http://www.spacetornado.com/DoItAgain/>.

Lang, Russell. 2006. GSview. v. 4.8. <http://pages.cs.wisc.edu/~ghost/gsview/>.

Lightning UK!. DVD Decrypter. v. 3.5.4.0. <http://www.dvddecrypter.com>.

Mean. 2010. Avidemux. v. 2.5.6. <http://www.avidemux.org>.

———. 2012. Avidemux. v. 2.6.0. <http://www.avidemux.org>.

Praetox and abatishchev. 2010. Low Orbit Ion Cannon (LOIC).  
<http://sourceforge.net/projects/loic/>.

RapidSolution Software AG. 2010. Tunebite. v. 7.2. <http://www.audials.com>.

rb, wyz, YeOK. 2010. TBSource Classic. <http://sourceforge.net/projects/tbsource/>.

Rosalind and Nir Arbel. 2008. Souseek. v. 157 NS 13c. <https://www.souseekqt.net/>.

Sieka, Jacek. 2014. DC++. v. 0.843. <http://dcplusplus.sourceforge.net/index.html>.

Tor Project, Inc., The. 2011. Tor. v. 0.2.2.35. <https://www.torproject.org>.

VideoLAN Team. VLC media player. v. 2.0.8. <http://www.videolan.org>.

WASTE Development Team. 2003. WASTE. <http://waste.sourceforge.net/>.

## Text

[Redacted]<sup>761</sup>. 1959. “Data Transmission Over Telephone Circuits”, in *NSA Technical Journal* 4 (1). pp. 67-81.  
[https://www.nsa.gov/public\\_info/\\_files/tech\\_journals/data\\_transmission.pdf](https://www.nsa.gov/public_info/_files/tech_journals/data_transmission.pdf).

---

<sup>761</sup> Unlike all other redactions in this *Operations Manual*, this one was not performed by myself, but by the National Security Agency.

AAAARG. "About AAAARG". AAAARG. <http://aaaarg.org/about>.

Aggrawal, Anil. 2009. *Forensic and Medico-legal Aspects of Sexual Crimes and Unusual Sexual Practices*. Boca Raton, FL: CRC Press.

Aked, Symon. 2011. "An Investigation Into Darknets and the Content Available Via Anonymous Peer-to-Peer File Sharing", in *Australian Information Security Management Conference*. pp. 10-18.  
<https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1105&context=ism>.

Akrich, Madeleine. 1992. "The De-Description of Technical Objects", in *Shaping Technology/Building Society: Studies in Sociotechnical Change* (eds. Wiebe E. Bijker and John Law). Cambridge, MA: The MIT Press. pp. 205-224.

Akrich, Madeleine and Bruno Latour. 1992. "A Summary of a Convenient Vocabulary for the Semiotics of Human and Nonhuman Assemblies", in *Shaping Technology/Building Society: Studies in Sociotechnical Change* (eds. Wiebe E. Bijker and John Law). Cambridge, MA: The MIT Press. pp. 259-264.

alkemyst. 2003. "Red dots for anti-piracy getting out of hand?". AnandTech Forums.  
<http://forums.anandtech.com/showthread.php?t=1171155>.

Alleyne, Brian. 2011a. "We are all hackers now": critical sociological reflections on the hacking phenomenon". Under Review. pp. 1-28. <https://eprints.gold.ac.uk/6305/>.

———. 2011b. "We are all hackers now": critical sociological reflections on the hacking phenomenon". Under Review. pp. 1-28. <https://eprints.gold.ac.uk/6306/>.

Amazon. 2014. "Downloading Content to Multiple Kindle Devices", in *Transferring, Downloading, and Sending Files to Kindle 2nd Generation*.  
[http://www.amazon.com/gp/help/customer/display.html/ref=hp\\_navbox\\_multiple\\_200375630?nodeId=200375630&#multiple](http://www.amazon.com/gp/help/customer/display.html/ref=hp_navbox_multiple_200375630?nodeId=200375630&#multiple).

- Anarchist FAQ Editorial Collective, The (Ian McKay, Gary Elkin, Dave Neal, Ed Boraas). 2008. "An Anarchist FAQ". v. 13.0. *Infoshop*.  
<http://www.infoshop.org/AnarchistFAQIntro>.
- Anderson, Chris. 2008. "Free! Why \$0.00 Is the Future of Business". *Wired* 16 (3).  
[http://www.wired.com/techbiz/it/magazine/16-03/ff\\_free](http://www.wired.com/techbiz/it/magazine/16-03/ff_free).
- Andersson, Jonas. 2009. "For the Good of the Net The Pirate Bay as a Strategic Sovereign", in *Culture Machine* 10. pp. 64-108.
- Anonfiles. 2012. "Terms". *AnonFiles*. <https://anonfiles.com/terms>.
- Antliff, Allan. 2011. "Anarchy, Power and Post-Structuralism", in *Post-Anarchism - A Reader* (eds. Duane Rousselle and Süreyya Evren). New York: Pluto Press. pp. 160-167.
- Antonellis, Darcy, Jeffrey J. Bartley, Margit Elisabeth Elo, Jean Pierre Gagnon, William B. Hogue, Jr., Edward J. Price. 2007. "Motion Picture Anti-Piracy Coding". Patent No.: US7206409B2.
- Appelbaum, Jacob, Marsh Ray, Karl Koscher, Ian Finder. 2012. "vpwns: Virtual pwned networks". *2nd Workshop on Free and Open Communications on the Internet*.  
<https://www.usenix.org/system/files/conference/foci12/foci12-final8.pdf>.
- arma. 2009. "One cell is enough to break Tor's anonymity". *The Tor Blog*.  
<https://blog.torproject.org/blog/one-cell-enough>.
- . 2010. "Bittorrent over Tor isn't a good idea". *The Tor Blog*.  
<https://blog.torproject.org/blog/bittorrent-over-tor-isnt-good-idea>.
- . 2014a. "Traffic correlation using netflows". *The Tor Blog*.  
<https://blog.torproject.org/blog/traffic-correlation-using-netflows>.

- . 2014b. “Possible upcoming attempts to disable the Tor network”. *The Tor Blog*.  
<https://blog.torproject.org/blog/possible-upcoming-attempts-disable-tor-network>.
- AtomInterSoft. 2014. “Free Open Public Proxy List sorted by domain”. *AliveProxy*.  
[http://atomintersoft.com/proxy\\_list\\_domain\\_edu](http://atomintersoft.com/proxy_list_domain_edu).
- Bailey, Michael, Evan Cooke, Farnam Jahanian, Andrew Myrick, Sushant Sinha. 2006.  
“Practical Darknet Measurement”, in *Information Sciences and Systems, 40th Annual Conference*. pp. 1-6. <http://www.eecs.umich.edu/fjgroup/pubs/darknet-ciss06.pdf>.
- Balázs, Bodó. 2011. “Coda: A Short History of Book Piracy”, in *Media Piracy in Emerging Economies*. New York: Social Science Research Council. pp. 399-413.  
<http://piracy.americanassembly.org/wp-content/uploads/2011/06/MPEE-PDF-Coda-Books.pdf>.
- Band, Jonathan and Jonathan Gerafi. 2013. *The Fair Use/Fair Dealing Handbook*.  
<https://infojustice.org/~infojust/wp-content/uploads/2013/03/band-and-gerafi-2013.pdf>.
- Barthes, Roland. 1975. “Leaving the Movie Theater” (trans. Richard Howard), in *The Rustle of Language*. Berkeley: University of California Press. pp. 345-349.
- Bataille, Georges. 1991. *The Accursed Share: Volume 1* (trans. Robert Hurley). New York: Zone Books.
- Baudrillard, Jean. 1987. “The Evil Demon of Images” (trans. Paul Patton and Paul Foss). pp. 13-34. <https://courses.arch.ntua.gr/fsr/130155/jean%20baudrillard.PDF>.
- . 1988. *The Ecstasy of Communication* (trans. Bernard Schütze and Caroline Schütze). New York City, NY: Semiotext(e).
- Baudry, Jean-Louis. 1974-1975. “Ideological Effects of the Basic Cinematographic Apparatus” (trans. Alan Williams), in *Film Quarterly* 28 (2). pp. 39-47.

- Bauer, Kevin, Damon McCoy, Dirk Grunwald, Douglas Sicker. 2008. "BitBlender: Lightweight anonymity for BitTorrent". *Proceedings of the workshop on Applications of private and anonymous communications*. ACM.  
<https://gnunet.org/sites/default/files/bauer-alpaca2008.pdf>.
- Bauer, Kevin, Dirk Grunwald, Douglas Sicker. 2009. "The Arms Race in P2P". *37th Research Conference on Communication, Information, and Internet Policy, TPRC*.  
[https://cs.uwaterloo.ca/~k4bauer/papers/bauer\\_tprc2009.pdf](https://cs.uwaterloo.ca/~k4bauer/papers/bauer_tprc2009.pdf).
- Bauman, Zygmunt. 2000. *Liquid Modernity*. Cambridge: Polity Press.
- Bayfiles. "Privacy Policy". *BayFiles*. <https://bayfiles.net/privacy>.
- Bayles, Aaron W. 2005. *InfoSec Career Hacking: Sell Your Skillz, Not Your Soul*. Rockland, MA: Syngress.
- BBC Worldwide. 2014. "BBC Worldwide update on Doctor Who leaks". *BBC*.  
<http://www.bbc.co.uk/corporate2/mediacentre/worldwide/2014/doctor-who-update>.
- BBS Corner. 2009. "A Brief History of BBS Systems". *The BBS Corner*.  
<http://www.bbscorner.com/usersinfo/bbshistory.htm>.
- Béranger. 2013. "Adobe LiveCycle Rights Management: the removal". *Homo Ludditus*.  
<https://beranger.org/2013/09/20/adobe-livecycle-rights-management-the-removal/>.
- Berne Convention for the Protection of Literary and Artistic Works. 1971 Paris Act. "Article 6bis - Moral Rights".  
<http://global.oup.com/booksites/content/9780198259466/15550001>.
- Bey, Hakim. 1985. *T.A.Z.: The Temporary Autonomous Zone: Ontological Anarchy, Poetic Terrorism*. New York: Autonomedia. [http://www.hermetic.com/bey/taz\\_cont.html](http://www.hermetic.com/bey/taz_cont.html).

- . 1992. *The Radio Sermonettes*. New York City, NY: The Libertarian Book Club.  
[http://hermetic.com/bey/radio\\_se.html](http://hermetic.com/bey/radio_se.html).
- . 1994. *Immediatism*. Edinburgh, Scotland: AK Press.
- Bey, Hakim and Hans Ulrich Obrist. 2010. “In Conversation with Hakim Bey”. *e-flux* 21.  
Interview. <http://www.e-flux.com/journal/in-conversation-with-hakim-bey/>.
- Biddle, Peter, Paul England, Marcus Peinado, Bryan Willman. 2002. “The Darknet and the Future of Content Distribution”, in *ACM Workshop on Digital Rights Management* Volume 6. pp. 1-16. [http://the-evan.com/files/rt/darknet\\_msft.pdf](http://the-evan.com/files/rt/darknet_msft.pdf).
- Biles, Jeremy. 2004. “I, Insect, or Bataille and the Crush Freaks”, in *Janus Head: Journal of Interdisciplinary Studies in Literature, Continental Philosophy, Phenomenological Psychology, and the Arts* 7 (1). pp. 115-131. <http://www.janushead.org/7-1/biles.pdf>.
- Bishop, Matt. 2002. *Computer Security: Art and Science*. Boston, MA: Addison-Wesley.
- Bittorrent Protocol Specification v1.0.  
[https://wiki.theory.org/BitTorrentSpecification#Tracker\\_HTTP.2FHHTTPS\\_Protocol](https://wiki.theory.org/BitTorrentSpecification#Tracker_HTTP.2FHHTTPS_Protocol).
- Black, Edwin. 2008. *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation*. US: Dialog Press.
- Blaze, Matt. 2003. “Cryptology and Physical Security: Rights Amplification in Master-Keyed Mechanical Locks”. *IEEE Security and Privacy*. March/April 2003.  
<http://www.crypto.com/papers/mk.pdf>.
- Blogcetera. 2009. “UK ISP, Cable and Dongle User Numbers - Jan 2009”. *Blogcetera*.  
<http://blogcetera.blogspot.co.uk/2009/02/uk-isp-cable-and-dongle-user-numbers.html>.
- Blond, Stevens Le, Arnaud Legout, Fabrice Le Fessant, Walid Dabbous. 2010. “Angling for

- Big Fish in BitTorrent”. INRIA Technical Report. pp. 1-13.  
[https://hal.inria.fr/inria-00451282/PDF/bt\\_angling.pdf](https://hal.inria.fr/inria-00451282/PDF/bt_angling.pdf).
- Boda, Károly, Ádám Máté Földes, Gábor György Gulyás, Sándor Imre. 2012. “User tracking on the web via cross-browser fingerprinting”, in *Information Security Technology for Applications*. Berlin: Springer. pp. 31-46.
- Bogdan, Robert and Sari Knopp Biklen. 1992. *Qualitative Research for Education*. Boston, MA: Allyn and Bacon.
- Bosworth, Derek L. 1986. *Intellectual Property Rights*. New York: Pergamon Press.
- Braden. R. 1989. “RFC 1122: Requirements for Internet Hosts -- Communication Layers”. Network Working Group/Internet Engineering Task Force.  
<https://tools.ietf.org/html/rfc1122>.
- Bradley, Dale. 2004. “Open Source, Anarchy, and the Utopian Impulse”, in *M/C: A Journal of Media and Culture* 7 (4).  
[http://www.media-culture.org.au/0406/03\\_Bradley.php](http://www.media-culture.org.au/0406/03_Bradley.php).
- Brafman, Ori and Rod A. Beckstrom. 2006. *Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*. New York: Penguin Group.
- Braidotti, Rosi. 2013. *The Posthuman*. Cambridge: Polity Press.
- Bricklin, Dan. 2000. “Friend-to-Friend Networks”. <https://bricklin.com/f2f.htm>.
- BT Broadband. 2014. “Giganews closure: what I need to know”. *BT.com*.  
[http://bt.custhelp.com/app/answers/detail/a\\_id/51205/?s\\_cid=con\\_FURL\\_giganews](http://bt.custhelp.com/app/answers/detail/a_id/51205/?s_cid=con_FURL_giganews).
- Burgin, Victor. 2004. *The Remembered Film*, London: Reaktion Books.
- Byers, Simon, Lorrie Cranor, Dave Kormann, Patrick McDaniel, Eric Cronin. 2003.



“Analysis of security vulnerabilities in the movie production and distribution process”, in *DRM '03 - Proceedings of the 3rd ACM Workshop on Digital Rights Management*. pp. 1-18. <https://lorrie.cranor.org/pubs/drm03.html>.

Byrd, Gene. 2008. “Two People Stabbed in Fullerton Theater: Horror Movie ‘The Signal’”, in *The National Ledger*.  
<http://www.nationalledger.com/news-tech/video-two-people-stabbed-in-f-167978.shtml>.

Cahill, Vinny, Elizabeth Gray, Jean-Marc Seigneur, Christian D. Jensen, Yong Chen, Brian Shand, Nathan Dimmock, Andy Twigg, and Jean Bacon, Colin English, Waleed Wagealla, Sotirios Terzis, and Paddy Nixon, Giovanna di Marzo Serugendo and Ciarán Bryce, Marco Carbone, Karl Krukow, Mogens Nielsen. 2003. “Using Trust for Secure Collaboration in Uncertain Environments”, in *Pervasive Computing* (July-September 2003). pp. 51-61.  
<http://www.tara.tcd.ie/bitstream/handle/2262/27085/Using+trust+for+secure+collaboration+in+uncertain+environments.pdf?sequence=1>.

Callon, Michel. 1989. “Society in the Making: The Study of Technology as a Tool for Sociological Analysis”, in *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology* (eds. Wiebe E. Bijker, Thomas P. Hughes, and Trevor Pinch). Cambridge, MA: The MIT Press. pp. 83-103.

Castellanet, Christian and Carl F. Jordan. 2002. *Participatory Action Research in Natural Resource Management - A Critique of the Method Based on Five Years' Experience in the Transamazônica Region of Brazil*. New York, NY: Taylor & Francis.

Cerven, Pavol. 2002. *Crackproof Your Software*. San Francisco, CA: No Starch Press.

Clarke, Ian and Oskar Sandberg. 2005. “Covert Communication in a Dark Network: A major new version of freenet”. *22nd Chaos Communication Congress*.  
[https://events.ccc.de/congress/2005/fahrplan/attachments/544-Slides\\_CovertCommunicationInADarkNetwork.pdf](https://events.ccc.de/congress/2005/fahrplan/attachments/544-Slides_CovertCommunicationInADarkNetwork.pdf).

- Clarke, Ian, Oskar Sandberg, Brandon Wiley, Theodore W. Hong. 2000. "Freenet: A Distributed Anonymous Information Storage and Retrieval System", in *Designing Privacy Enhancing Technologies* (ed. Hannes Federrath). Germany: Springer-Verlag. pp. 46-66.
- Cohen, Bram. 2006. "Incentives Build Robustness in BitTorrent", in *Workshop on Economics of Peer-to-Peer Systems*. pp. 1-5.  
<https://pdos.csail.mit.edu/6.824-2010/papers/cohen-btecon.pdf>.
- . 2008. "The BitTorrent Protocol Specification". *BitTorrent.org*.  
[http://www.bittorrent.org/beps/bep\\_0003.html](http://www.bittorrent.org/beps/bep_0003.html).
- Cohn, Jesse and Shawn Wilbur. 2003. "What's Wrong With Postanarchism?".  
[http://theanarchistlibrary.org/library/Jesse\\_Cohn\\_and\\_Shawn\\_Wilbur\\_\\_What\\_s\\_Wrong\\_With\\_Postanarchism\\_.html](http://theanarchistlibrary.org/library/Jesse_Cohn_and_Shawn_Wilbur__What_s_Wrong_With_Postanarchism_.html).
- Coleman, Gabriella. 2011. "Anonymous: From the Lulz to Collective Action".  
<http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action>.
- . 2012a. "Am I Anonymous?", in *Limn 2: "Crowds and Clouds"*.  
<http://limn.it/am-i-anonymous/>.
- . 2012b. "Our Weirdness Is Free, The logic of Anonymous—online army, agent of chaos, and seeker of justice", in *May 9*, pp. 83-111.  
<http://gabriellacoleman.org/wp-content/uploads/2012/08/Coleman-Weirdness-Free-May-Magazine.pdf>.
- . 2014a. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. London: Verso.

- . 2014b. “Hackers”, in *The Johns Hopkins Encyclopedia of Digital Textuality*. Forthcoming. <http://gabriellacoleman.org/wp-content/uploads/2013/04/Coleman-Hacker-John-Hopkins-2013-Final.pdf>.
- cologic, emtee, Fredrik Ullner, Wicked World Games. 2009-2013. “DC++ Documentation”. *DC++: Just These Guys, Ya Know?*. <https://dcpp.wordpress.com/category/documentation/>.
- Computer Hope. 2014. “How to set a computer's date and time”. <http://www.computerhope.com/issues/ch000554.htm>.
- Condry, Ian. 2004. “Cultures of Music Piracy: An Ethnographic Comparison of the US and Japan”, in *International Journal of Cultural Studies* 7(3). pp. 343-363.
- Copyright Act of 1976. 1976. 17 U.S.C. § 107 - “Limitations on exclusive rights: Fair use”. <http://www.law.cornell.edu/uscode/text/17/107>.
- Copyright Act of 1976. 1976. 17 U.S.C. § 401 - “Notice of copyright: Visually perceptible copies”. <http://www.law.cornell.edu/uscode/17/401>.
- Council of the Inspectors General on Integrity and Efficiency. 2010. *Guidelines on Undercover Operations*. Washington, DC: Council of the Inspectors General on Integrity and Efficiency. [http://www.governmentattic.org/12docs/GuidelinesUndercoverOpsOIG\\_2010.pdf](http://www.governmentattic.org/12docs/GuidelinesUndercoverOpsOIG_2010.pdf).
- Cox, Inegemar J., Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker. 2008. *Digital Watermarking and Steganography* (Second Edition). Burlington, MA: Elsevier.
- Craig, Paul. 2005. *Software Piracy Exposed*. Rockland, MA: Syngress.
- Cramer, Florian. 2003. “Exe.cut[up]able statements: the Insistence of Code”, in *Ars Electronica 2003 - Code - The Language of Our Time* (eds. Gerfried Stocker and

Christine Schöpf). Linz: Hatje Cantz. pp. 98-103.

[http://archive.aec.at/media/archive/2003/185088/File\\_04108\\_AEC\\_FE\\_2003.pdf](http://archive.aec.at/media/archive/2003/185088/File_04108_AEC_FE_2003.pdf).

Crawford, Douglas. 2014. "The Ultimate Privacy Guide". *Best VPN*.

<https://www.bestvpn.com/the-ultimate-privacy-guide/#vpn>.

Creative Commons. "About the Licenses". <https://creativecommons.org/licenses/>.

———. "Creative Commons Board of Directors".

<https://creativecommons.org/board#lawrencelessig>.

CrimethInc. ex-Workers' Collective. 2004. *Recipes for Disaster: An Anarchist Cookbook*.

Olympia: CrimethInc. ex-Workers' Collective.

Critical Art Ensemble. 2000. "The Financial Advantages of Anti-Copyright", in *Digital*

*Resistance: Explorations in Tactical Media*. New York: Autonomedia. pp. 148-152.

———. 2006. *Marching Plague*. Brooklyn, NY: Autonomedia.

C.S.-W. 2013. "Mega relaunch". *The Economist*.

<http://www.economist.com/blogs/schumpeter/2013/01/kim-dotcom>.

cypherpunks. 2013. "Bad russian exit node attacks connections to Wikipedia". *Tor Bug*

*Tracker & Wiki*. <https://trac.torproject.org/projects/tor/ticket/8657>.

daelstrom and lbponey . 2010. "The Souseek Protocol". *Museek+*.

<https://www.museek-plus.org/wiki/SouseekProtocol>.

Décary-Héту, David. 2014. "Information Exchange Paths in IRC Hacking Chat Rooms", in

*Crime and Networks* (ed. Carlo Morselli). New York: Routledge. pp. 218-230.

DDL Rank. 2014. "Top DDL Sites". *DDL Rank*. <http://ddlrank.com/top-download-sites.html>.

- Defective by Design. 2010. "Amazon's Kindle Swindle".  
<http://www.defectivebydesign.org/amazon-kindle-swindle>.
- Deleuze, Gilles. 1992. "Postscript on the Societies of Control", in *October* 59. Cambridge, MA: MIT Press. pp. 3-7. <http://www.n5m.org/n5m2/media/texts/deleuze.htm>.
- Deleuze, Gilles and Felix Guattari. 1987. *A Thousand Plateaus: Capitalism and Schizophrenia* (trans. Brian Massumi). Minneapolis, MN: University of Minnesota Press.
- Deleuze, Gilles and Antonio Negri. 1990. "Gilles Deleuze in Conversation with Antonio Negri" (trans. Martin Joughin), in *Futur Anterieur* 1. Interview.  
<http://www.generation-online.org/p/fpdeleuze3.htm>.
- dexter311. 2014. "One year on - is there anything that comes close to what Underground Gamer used to be?". *Reddit*.  
[https://reddit.com/r/trackers/comments/2kgo45/one\\_year\\_on\\_is\\_there\\_anything\\_that\\_comes\\_close\\_to/](https://reddit.com/r/trackers/comments/2kgo45/one_year_on_is_there_anything_that_comes_close_to/).
- Dicks, Bella, Bruce Mason, Amanda Coffey, Paul Atkinson. 2005. *Qualitative Research and Hypermedia: Ethnography for the Digital Age*. London: Sage Publications.
- Digital Cinema Initiatives, LLC. 2008. *Digital Cinema System Specification v1.2*.  
[http://www.dcmovies.com/DCIDigitalCinemaSystemSpecv1\\_2.pdf](http://www.dcmovies.com/DCIDigitalCinemaSystemSpecv1_2.pdf).
- Digital Cinema Initiatives, LLC. 2014. "About DCI". <http://www.dcmovies.com/>.
- Digital Citizens Alliance. 2014. "Busted, But Not Broken: The State of Silk Road and the Darknet Marketplaces".  
<https://www.globalinitiative.net/download/cybercrime/global/Digital%20Citizen%20Alliance%20%20Busted,%20but%20not%20broken%20The%20State%20of%20Silk%20Road%20and%20the%20darknet%20marketplaces.pdf>.

- Digital Theater Systems, Inc. 2003. "DTS to Introduce Security Enhancements for Cinema Audio Content Protection". *PR Newswire*. Press release.  
<http://www.prnewswire.co.uk/cgi/news/release?id=113104>.
- DizzIE. 2005. "The 2005 Beginner's Guide to Getting Warez on IRC".  
<http://dizzy.childrenofmay.org/The.2005.Beginners.Guide.to.Getting.Warez.on.IRC.pdf>.
- Doctorow, Cory. 2012. "Rumblefish claims to own copyright to ambient birdsong on YouTube". Boing Boing.  
<http://boingboing.net/2012/02/27/rumblefish-claims-to-own-copyr.html>.
- Douceur, John R. 2002. "The sybil attack", in *Peer-to-peer Systems*. Berlin: Springer. pp. 251-260.
- Doyle, Vincent A., George D. Cary, Marjorie McCannon, and Barbara A. Ringer. 1957. *Copyright Law Revision - Study 7 - Notice of Copyright*. Subcommittee on Patents, Trademarks, and Copyrights of the Committee on the Judiciary, United States Senate. Washington: United States Government Printing Office.  
<http://www.copyright.gov/history/studies/study7.pdf>.
- Drogin, Marc. 1983. *Anathema!: Medieval Scribes and the History of Book Curses*. A. Schram.
- Duffield, David Jay, Mark Alan Schultz, Michael Allan Sterling. 2006. "Theater Identification System Utilizing Identifiers Projected onto a Screen". Patent No.: US20060262280A1.
- Ebert, Roger. 2003a. "Dots on film designed to track pirated movies are a nuisance", in *The Victoria Advocate* - October 5, 2003. p. 2D.
- . 2003b. "Big screen anti-piracy system continues to annoy audiences", in *The Victoria Advocate* - October 26, 2003 p. 2D.

- eeplox. 2012. “‘Matched third party content. Entity: rumblefish Content Type: Musical Composition’, but no music in the video”. *Google Groups - Google Product Forums - YouTube Help Forum*.  
<https://productforums.google.com/forum/#!category-topic/youtube/how-to-use-youtube-features/eSjKSGBrFMo>.
- Elf-Man, LLC. v. Eric Cariveau, et al.* 2014. Case No. C13-0507RSL. Order Granting Motion to Dismiss and Granting Leave to Amend.  
<https://www.scribd.com/doc/201180332/ORDER-Granting-Motion-to-Dismiss>.
- enigmax. 2009. “BitTorrent Hydra: Anonymous Hidden Tracker Via Tor”. *TorrentFreak*.  
<https://torrentfreak.com/bittorrent-hydra-anonymous-hidden-tracker-via-tor-090725/>.
- . 2010a. “Canadian Movie Pirate ‘Maven’ Dies of Drug Overdose”. *TorrentFreak*.  
<https://torrentfreak.com/canadian-movie-pirate-%E2%80%98maven%E2%80%99-dies-of-drug-overdose-100406/>.
- . 2010b. “Six BitTorrent Admins Arrested, Interpol Chase Two More”. *TorrentFreak*.  
<https://torrentfreak.com/six-bittorrent-admins-arrested-interpol-chase-two-more-100310/>.
- . 2011. “Police Raid ‘Excellent’ Private BitTorrent Tracker, Admins Arrested”. *TorrentFreak*.  
<https://torrentfreak.com/police-raid-excellent-private-bittorrent-tracker-admins-arrested-110526/>.
- . 2012. “Massive Copyright Infringement Suit Could Collapse Cyberlocker, Studio Warns”. *TorrentFreak*.  
<https://torrentfreak.com/massive-copyright-infringement-suit-could-collapse-cyberlocker-studio-warns-120702/>.
- Ernesto. 2009. “The Pirate Bay Tracker Shuts Down for Good”. *TorrentFreak*.

<https://torrentfreak.com/the-pirate-bay-tracker-shuts-down-for-good-091117/>.

———. 2011a. “200,000 BitTorrent Users Sued In The United States”, *TorrentFreak*.

<https://torrentfreak.com/200000-bittorrent-users-sued-in-the-united-states-110808/>.

———. 2011b. “BitTorrent Tracker Becomes Official Movie Distributor”. *TorrentFreak*.

<https://torrentfreak.com/bittorrent-tracker-becomes-official-movie-distributor-110428/>.

———. 2011c. “Major Usenet Provider Shuts Down Following Court Order”. *TorrentFreak*.

<https://torrentfreak.com/major-usenet-provider-shuts-down-following-court-order-111106/>.

———. 2012. “Anonymous, Decentralized and Uncensored File-Sharing is Booming”.

*TorrentFreak*.

<https://torrentfreak.com/anonymous-decentralized-and-uncensored-file-sharing-is-booming-120302/>.

———. 2013a. “BitTorrent Accounts for 35% of All Upload Traffic, VPNs are Booming”.

*TorrentFreak*.

<https://torrentfreak.com/bittorrent-accounts-for-35-of-all-upload-traffic-vpns-are-booming-130518/>.

———. 2013b. “‘Killer Joe’ Sues VPN-Using BitTorrent Pirates”. *TorrentFreak*.

<https://torrentfreak.com/killer-joe-sues-vpn-using-bittorrent-pirates-130418/>.

———. 2013c. “Kim Dotcom Teases New Music Service... Baboom”. *TorrentFreak*.

<https://torrentfreak.com/kim-dotcom-teases-new-music-service-baboom-130907/>.

———. 2013d. “Pirate Bay Moves to Guyana After Domain Suspension, 70 Domains to Go”.

*TorrentFreak*. <https://torrentfreak.com/pirate-bay-moves-to-guyana-131218/>.

———. 2013e. “Underground Gamer Goes Down Citing Legal Problems”. *TorrentFreak*.



<https://torrentfreak.com/underground-gamer-goes-down-citing-legal-problems-130602/>.

———. 2014a. “Demonoid Returns, Website Now Back Online”. *TorrentFreak*.

<https://torrentfreak.com/demonoid-back-140330/>.

———. 2014b. “Pirate Bay Sends 100,000 New Users to ‘Free’ VPN”. *TorrentFreak*.

<https://torrentfreak.com/pirate-bay-sends-100000-users-free-vpn-141024/>.

———. 2015. “Which VPN Services Take Your Anonymity Seriously? 2015 Edition”. *TorrentFreak*.

<https://torrentfreak.com/anonymous-vpn-service-provider-review-2015-150228/>.

Eskapa, Roy. 1987. *Bizarre Sex*. London: Grafton Books.

Eyebeam. “Marching Plague from Critical Art Ensemble”.

<http://eyebeam.org/events/marching-plague-from-critical-art-ensemble>.

Fals-Borda, Orlando and Muhammad Anisur Rahman (eds.). 1991. *Action and Knowledge: Breaking the Monopoly with Participatory Action-Research*. New York: The Apex Press.

Farache, Emily. 2001. “Napster Goes Legit”. *E! Online*.

<http://eonline.com/news/41734/napster-goes-legit>.

Feenberg, Andrew. 1999. *Questioning Technology*. New York: Routledge.

Feiten, Elmo. 2013. “Would the Real Max Stirner Please Stand Up?”, in *Anarchist Developments in Cultural Studies* 2013.1: “Blasting the Canon”. pp. 117-137.

Fellows, G. 2006. “Newsgroups reborn - The binary posting renaissance”, in *Digital Investigation* 3 (2). pp. 73-78.

- Felten, Ed. 2006. "How Watermarks Fail". *Freedom to Tinker*.  
<https://freedom-to-tinker.com/blog/felten/how-watermarks-fail/>.
- File Dropper. "About Us". *File Dropper*. <https://www.filedropper.com/aboutus.php>.
- Foucault, Michel. 1977. *Discipline and Punish: The Birth of the Prison* trans. Alan Sheridan).  
London: Penguin Books.
- . 1980. "Truth and Power", in *Power/Knowledge: Selected Interviews & Other Writings 1972-1977* (ed. Colin Gordon; trans. Colin Gordon, Leo Marshall, John Mepham, Kate Soper). New York: Pantheon Books.
- Fox-Brewster, Tom. 2014. "Facebook opens up to anonymous Tor users with .onion address".  
*The Guardian*.  
<http://www.theguardian.com/technology/2014/oct/31/facebook-anonymous-tor-users-onion>.
- Franks, Benjamin. 2011. "The Politics of Postanarchism" (Book Review), in *Anarchist Studies* 19:1. pp. 113-117.
- Free Software Foundation. 1998. "Legal Issues about Contributing Code to GNU". The GNU Operating System and the Free Software Movement.  
<https://www.gnu.org/software/gnustep/developers/conditions.text>.
- . 1999. *The GNU Privacy Handbook*.  
<https://www.gnupg.org/gph/en/manual/book1.html>.
- . 2008. "Information for Maintainers of GNU Software", § 4. Legal Matters – Subsection 4.1 Copyright Papers.  
[https://www.gnu.org/prep/maintain/html\\_node/Copyright-Papers.html](https://www.gnu.org/prep/maintain/html_node/Copyright-Papers.html).
- . 2012. "Staff and Board". <https://www.fsf.org/about/staff-and-board/>.

———. 2013. “Current Campaigns”. <https://www.fsf.org/campaigns/>.

———. 2014. “The GNU Operating System and the Free Software Movement”. <https://gnu.org/>.

Freenet Project, The. “Download Freenet”. *The Freenet Project*.  
<https://freenetproject.org/download.html>.

———. “Freenet Frequently Asked Questions”. *The Freenet Project*.  
<https://freenetproject.org/faq.html>.

Frizell, Sam. 2014. “The FBI and NSA Hate Apple’s Plan to Keep Your iPhone Data Secret”.  
*Time*. <https://time.com/3437222/iphone-data-encryption/>.

FrootVPN. 2014. “FAQ for General”. *FrootVPN*. <https://www.frootvpn.com/faq/general-15.html>.

Gay, Joshua. 2005. “FSF Licensing & Compliance Team”. *Free Software Foundation*.  
<https://www.fsf.org/licensing/>.

Gaycken, Sandro. 2005. “Free Software and Anarchism - does this compute?”. *22nd Chaos Communication Congress - Private Investigations*.  
<https://events.ccc.de/congress/2005/fahrplan/events/517.en.html>.

Genette, Gerard. 1997. *Paratexts: Thresholds of Interpretation* (trans. Jane E. Lewin).  
Cambridge: Cambridge University Press.

Giacobe, Nicklaus A. and Sen Xu. 2011. “Geovisual Analytics for Cyber Security: Adopting the GeoViz Toolkit”, in *IEEE Symposium on Visual Analytics Science and Technology*. pp. 313-314.  
[https://svn.labri.fr/visu/InfoVis\\_2011/VisWeek2011\\_proceedings/vast/challenge/giacobe.pdf](https://svn.labri.fr/visu/InfoVis_2011/VisWeek2011_proceedings/vast/challenge/giacobe.pdf).

- Goldsmiths, University of London. 2012. "About – Goldsmiths Research Online".  
<https://eprints.gold.ac.uk/information.html>.
- . 2012. "Deposit Guide – Goldsmiths Research Online".  
[https://eprints.gold.ac.uk/deposit\\_guide.html](https://eprints.gold.ac.uk/deposit_guide.html).
- . 2013 "Brian Alleyne. 2011. "'We are all hackers now':  
critical sociological reflections on the hacking phenomenon". HTML source code.  
<https://eprints.gold.ac.uk/6306/>.
- Gramsci, Antonio. 1971. *Selections from the Prison Notebooks* (eds. and trans. Quintin Hoare and Geoffrey Nowell Smith). New York: International Publishers.
- Griffiths, Mark. 2012. "Trample Leaning: A Beginner's Guide to Crush Fetishism".  
*drmarkgriffiths*.  
<https://drmarkgriffiths.wordpress.com/2012/05/17/trample-leaning-a-beginners-guide-to-crush-fetishism/>.
- Grandison, Tyrone and Morris Sloman. 2000. "A Survey of Trust in Internet Applications",  
in *IEEE Communications Surveys and Tutorials*. pp. 1-30.  
[https://www.doc.ic.ac.uk/~mss/Papers/Trust\\_Survey.pdf](https://www.doc.ic.ac.uk/~mss/Papers/Trust_Survey.pdf).
- gatomalo. 2012. "Spider Scan of ToR Directories A-Z". *USCyberLabs*.  
<http://uscyberlabs.com/blog/2012/04/19/spider-scan-tor-directories-a-z/>.
- Haber, Stuart, Bill Horne, Joe Pato, Tomas Sander, Robert Endre Tarjan. 2003. "If Piracy Is  
the Problem, Is DRM the Answer?", in *Digital Rights Management: Technological,  
Economic, Legal and Political Aspects*. pp. 224-233.
- Hackbloc. 2011. "The Hidden Tracker Returns", in *Hack This Zine*, V. 12 (Spring 2011). p.  
33.

- Hafner, Katie and Matthew Lyon. 1996. *Where Wizards Stay Up Late: The Origins of the Internet*. New York: Simon and Schuster.
- Hahn, Harley. 2014a. "Anonymous File Sharing", in *Harley Hahn's File Sharing Tutorial*.  
<http://www.harley.com/usenet/file-sharing/05-anonymous-file-sharing.html>.
- . 2014b. "How Binary Files Are Handled", in *Harley Hahn's Usenet Tutorial*.  
<http://www.harley.com/usenet/usenet-tutorial/how-binary-files-are-handled.html>.
- Hall, Gary. 2009. "Introduction: Pirate Philosophy", in *Culture Machine* 10, pp. 1-5.
- . 2009. "Pirate Philosophy (Version 1.0): Open Access, Open Editing, Free Content, Free/Libre/Open Media", in *Culture Machine* 10. pp. 1-43.
- Hall, Stuart, Peter Osborne and Lynne Segal. 1997. "Culture and Power", in *Radical Philosophy* 86. pp. 24-41. Interview.  
[https://www.radicalphilosophy.com/wp-content/files\\_mf/rp86\\_interview\\_hall.pdf](https://www.radicalphilosophy.com/wp-content/files_mf/rp86_interview_hall.pdf).
- Hanrahan, Hu. 2007. *Network Convergence: Services, Applications, Transport, and Operations Support*. West Sussex, England: John Wiley & Sons Ltd.
- Haraway, Donna. 1991. "A Cyborg Manifesto: Science, Technology, and Socialist-Feminism in the Late Twentieth Century," in *Simians, Cyborgs and Women: The Reinvention of Nature*. New York: Routledge. pp. 149-181.  
<https://wayback.archive.org/web/20120214194015/http://www.stanford.edu/dept/HPS/Haraway/CyborgManifesto.html>.
- . 1997. *Modest\_Witness@Second\_Millennium.FemaleMan@\_Meets\_OncoMouseTM: Feminism and Technoscience*. New York: Routledge.
- Harris, Chris. 2007. "Music File-Sharing Site OiNK Shut Down Following Criminal Investigation". *MTV*.  
<http://www.mtv.com/news/1572554/music-file-sharing-site-oink-shut-down->

following-criminal-investigation/.

Harvey, Brian. 1985. "What is a Hacker?", in "Computer Hacking and Ethics" (ACM Select Panel on Hacking). <https://www.cs.berkeley.edu/~bh/hacker.html>.

Harvey, David<sup>762</sup>. 2010. *Companion to Marx's Capital*. London: Verso Books.

Hauser, Tobias and Christian Wenz. 2003. "DRM Under Attack: Weaknesses in Existing Systems", in *Digital Rights Management: Technological, Economic, Legal and Political Aspects* (eds. G. Goos, J. Hartmanis, and J. van Leeuwen). New York: Springer. pp. 206-223.

Hawley, Aaron S. 2007. "Making copyleft work with implied compliance". *Free Software Foundation*.  
[http://gplv3.fsf.org/wiki/index.php/User:ashawley/Making\\_copyleft\\_work\\_with\\_implied\\_compliance](http://gplv3.fsf.org/wiki/index.php/User:ashawley/Making_copyleft_work_with_implied_compliance).

Hazel, Greg and Arvid Norberg. 2012. "Extension for Peers to Send Metadata Files". *BitTorrent.org*. [http://www.bittorrent.org/beps/bep\\_0009.html](http://www.bittorrent.org/beps/bep_0009.html).

Helbing, Juergen. 2002. "yEncode - A quick and dirty encoding for binaries". Version 1.3.  
<http://www.yenc.org/yenc-draft.1.3.txt>.

Held, Gilbert. 2004. *Virtual Private Networking: A Construction, Operation and Utilization Guide*. West Sussex: John Wiley & Sons, Ltd.

Henigin, Edward. 2009. "Up and to the Right: The Recent History of the Global Usenet Feed", in *North American Network Operators' Group (NANOG) 46*.  
[https://www.nanog.org/meetings/nanog46/presentations/Wednesday/Henigin\\_light\\_N46.pdf](https://www.nanog.org/meetings/nanog46/presentations/Wednesday/Henigin_light_N46.pdf).

---

<sup>762</sup> N.B. Though it is of course far from certain whether Harvey actually authored the copyright incantation himself, and thus a more fitting citation may here be: Anonymous. 2010. *Companion to Marx's Capital*. Verso Books; or perhaps Verso. 2010. *Companion to Marx's Capital*. Verso Books, with the same uncertainty of citation applying to all other quoted copyright/left notices as well.

- Hine, Christine M. 2000. *Virtual Ethnography*. London: Sage Publications.
- Hoffman, Abbie (as George Metesky). 1967. *Fuck the System*. New York.  
<http://dizzy.childrenofmay.org/fuck.the.system.txt>.
- Hoffman, Abbie. 1971. *Steal This Book* (25th Anniversary Facsimile Edition). New York:  
Four Walls Eight Windows.
- Horowitz, Edward D. 1998. "The Ascent of Content", in *The Future of the Electronic Marketplace* (ed. Derek Leebaert). London: The MIT Press. pp. 91-112.
- Imrie, Doug. 1994-5. "The 'Illegalists'", in *Anarchy: a Journal Of Desire Armed* (Fall-Winter 1994-5).  
[http://theanarchistlibrary.org/HTML/Doug\\_Imrie\\_\\_The\\_\\_Illegalists\\_.html](http://theanarchistlibrary.org/HTML/Doug_Imrie__The__Illegalists_.html).
- Information Resources Management Association. 2013. *Digital Rights Management: Concepts, Methodologies, Tools, and Applications*. Hershey, PA: IGI Global.
- InR. 2007. "MPAA.DOTS.ALL.CAMMERS.READ-InR".  
<http://scenenotice.org/details.php?id=977>.
- International Organization for Standardization. 1994. *ISO/IEC 7498-1:1994(E): Information Technology — Open Systems Interconnection — Basic Reference Model: The Basic Model*. International Organization for Standardization.  
[http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269\\_ISO\\_IEC\\_7498-1\\_1994\(E\).zip](http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip).
- James, Jack. 2006. *Digital Intermediates for Film and Video*. Burlington, MA: Elsevier Inc.
- Johnson, Aaron, Chris Wacek, Rob Jansen, Micah Sherr, Paul Syverson. 2013. "Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries", in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*.

<http://www.cryptome.org/2013/08/tor-users-routed.pdf>.

Jones, Ben. 2007. "What Waffles? The Hydra Lives On". *TorrentFreak*.

<https://torrentfreak.com/what-waffles-hydra-071030/>.

Jordan, Tim and Paul Taylor. 2004. *Hactivism and Cyberwars: Rebels with a Cause*.  
London: Routledge.

Josh. 2006. "Hotline File Sharing". *Nailbat.com*.

<http://www.nailbat.com/content/view/14/32/>.

Kaspersky, Kris. 2005. *Hacker Debugging Uncovered*. Wayne, PA: A-List Publishing.

Kemmis, Stephen and Robin McTaggart (eds.). 1988. *The Action Research Planner*. Victoria,  
Australia: Deakin University Press.

*Killer Joe Nevada, LLC., v. Does 1-15*. 2013. Civil Action 2:13-cv-00848.

<https://cases.justia.com/federal/district-courts/ohio/ohsdce/2:2013cv00848/165535/4/0.pdf>.

Kim, Juhoon, Fabian Schneider, Bernhard Ager, Anja Feldmann. 2010. "Today's Usenet Usage: NNTP Traffic Characterization", in *INFOCOM IEEE Conference on Computer Communications Workshops*. pp. 1-6.

[https://www.net.t-labs.tu-berlin.de/teaching/ss10/IM\\_seminar/pdf/KSAF-TUUCNNTPT-10.pdf](https://www.net.t-labs.tu-berlin.de/teaching/ss10/IM_seminar/pdf/KSAF-TUUCNNTPT-10.pdf).

Kindon, Sarah, Rachel Pain and Mike Kesby (eds.). 2007. *Participatory Action Research Approaches and Methods: Connecting People, Participation and Place*. New York: Routledge.

Kirovski, Darko and Henrique Malvar. 2002. "Audio Watermark Detector". US Pat. US 2002/0107691 A1.



- Kirschenbaum, Matthew G. 2008. *Mechanisms: New Media and the Forensic Imagination*. London: The MIT Press.
- Kodak. 2001. "Invisible Watermarking for Digital Cinema". *Kodak Research and Development*.  
<http://www.kodak.com/country/US/en/corp/researchDevelopment/productFeatures/cinema.shtml>.
- Kristeva, Julia. 1986. "A New Type of Intellectual: The Dissident" (trans. Seán Hand), in *The Kristeva Reader* (ed. Toril Moi). New York: Columbia University Press.
- Kwall, Roberta Rosenthal. 2010. *The Soul of Creativity: Forging a Moral Rights Law for the United States*. Stanford, CA: Stanford Law Books.
- Landry, Brett J. L and Dinah Payne. "Technical Perspectives of Illegal P2P File Sharing: Available Technical Solutions", in *International Journal of Services and Standards* 2 (3). pp. 228-237.
- Landstreicher, Wolfi. 2011. "Translator's Preface", in "Stirner's Critics".  
<http://theanarchistlibrary.org/library/max-stirner-stirner-s-critics>.
- . 2012. "Egoism Versus Modernity: John Welsh's Dialectical Stirner", in *Modern Slavery* 1. pp. 186-191. <http://modernslavery.calpress.org/?p=492>.
- Langford, Marty. 2008. "Anti-Piracy measures becoming more intrusive...". *MassLive*.  
[http://blog.masslive.com/screenwriting/2008/05/antipiracy\\_measures\\_becoming\\_m.html](http://blog.masslive.com/screenwriting/2008/05/antipiracy_measures_becoming_m.html).
- Langtangen, Hans Petter. 2009. *A Primer on Scientific Programming with Python*. New York: Springer.
- Latour, Bruno. 1992. "Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts", in *Shaping Technology/Building Society: Studies in Sociotechnical*

*Change* (eds. Wiebe E. Bijker and John Law). Cambridge, MA: The MIT Press. pp. 225-258.

———. 1993a. “The Berlin Key or How to Do Things with Words”, in *Matter, Materiality and Modern Culture* (ed. Paul Graves-Brown). London: Routledge. pp. 10-21.

———. 1993b. *We Have Never Been Modern* (trans. Catherine Porter). Cambridge, MA: Harvard University Press.

———. 2005. *Reassembling the Social: An Introduction to Actor-Network-Theory*. New York: Oxford University Press.

Le Blond, Stevens, Pere Manils, Abdelberi Chaabane, Mohamed Ali Kaafar, Arnaud Legout, Claude Castellucia, Walid Dabbous. 2010. “De-anonymizing BitTorrent Users on Tor”. *7th USENIX Symposium on Network Design and Implementation (NSDI'10)*. <https://hal.inria.fr/inria-00471177/document>.

Le Blond, Stevens, Pere Manils, Abdelberi Chaabane, Mohamed Ali Kaafar, Claude Castelluccia, Arnaud Legout, Walid Dabbous. 2011. “One Bad Apple Spoils the Bunch: Exploiting P2P Applications to Trace and Profile Tor Users”. arXiv preprint; arXiv:1103.1518. <http://arxiv.org/abs/1103.1518>.

Lee, Matt. 2010. “Meet the free software gang”. *Free Software Foundation*. <https://www.fsf.org/working-together/gang>.

Lee, Min-Jeong, Kyung-Su Kim, and Heung-Kyu Lee. 2010. “Digital Cinema Watermarking for Estimating the Position of the Pirate”, in *IEEE Transactions on Multimedia* 12 (7). pp. 605-621.

Leeds, Jeff. 2008. “Nine Inch Nails Album Is Free Online”. *The New York Times*. <http://www.nytimes.com/2008/05/06/arts/music/05cnd-nine.html>.

Lessig, Lawrence. 2001. *The Future of Ideas: The Fate of the Commons in a Connected*

*World*. New York: Random House.

———. 2004. *Free Culture: How Big Media Uses Technology and The Law to Lock Down Culture and Control Creativity*. New York: The Penguin Press.

———. 2006. *Code: And Other Laws of Cyberspace*. Version 2.0. New York: Basic Books.

Levy, Stephen. 1984. "The Tech Model Railroad Club", in *Hackers: Heroes of the Computer Revolution*. New York: Dell Publishing. pp. 3-27.

Liebelson, Dana. 2014. "Why It's Getting Harder to Sue Illegal Movie Downloaders". *Mother Jones*.  
<http://www.motherjones.com/politics/2014/02/bittorrent-illegal-downloads-ip-address-lawsuit>.

Lincoln, Kevin. 2012. "The Feds Just Shut Down A Huge File Sharing Site And Charged Its Founder With Piracy". *Business Insider*.  
<http://www.businessinsider.com/megaupload-shut-down-2012-1>.

Liu, K. J. Ray, Wade Trappe, Z. Jane Wang, Min Wu, and Hong Zhao. 2005. *Multimedia Fingerprinting Forensics for Traitor Tracing*. New York: Hindawi Publishing Corporation.

Loewenstern, Andrew and Arvid Norberg. 2008. "DHT Protocol". *BitTorrent.org*.  
[http://www.bittorrent.org/beps/bep\\_0005.html](http://www.bittorrent.org/beps/bep_0005.html).

Loshin, Peter. 2013. *Simple Steps to Data Encryption: A Practical Guide to Secure Computing*. Waltham, MA: Elsevier.

Lovink, Geert. 2003. *Dark Fiber: Tracking Critical Internet Culture*. Cambridge, MA: The MIT Press.

- Ma, Shuo, Ouri Wolfson, Jie Lin. 2011. "A Survey on Trust Management for Intelligent Transportation System", in *Proceedings of the 4th ACM SIGSPATIAL International Workshop on Computational Transportation Science*. pp. 1-6.  
<http://www.cs.uic.edu/~sma/Papers/trust.pdf>.
- MacInaugh, Edmond A. 1984. *Disguise Techniques: Fool All of the People Some of the Time*. Boulder, CO: Paladin Press.
- Manils, Pere, Abdelberi Chaabane, Stevens Le Blond, Mohamed Ali Kaafar, Claude Castelluccia, Arnaud Legout, Walid Dabbous. 2010. "Compromising Tor Anonymity: Exploiting P2P Information Leakage". arXiv preprint; arXiv:1004.1461.  
<http://arxiv.org/pdf/1004.1461>.
- Marshall. 2006. "Camcording in Montreal theaters: perspectives from industry and law enforcement". Embassy Cable. Ref. ID. 06MONTREAL1220.  
<https://wikileaks.ch/cable/2006/12/06MONTREAL1220.html>.
- Martin, Brian. 1998. *Information Liberation*. London: Freedom Press.
- Marx, Karl. 1852. *The Eighteenth Brumaire of Louis Bonaparte* (trans. Saul K. Padover).  
<https://www.marxists.org/archive/marx/works/1852/18th-brumaire/>.
- Masnack, Mike. 2010. "Music Licensing Firm Offers Cheap Licenses For YouTube Videos". *Techdirt*. <http://www.techdirt.com/articles/20100629/02511010000.shtml>.
- Mason, Matt. 2008a. *The Pirate's Dilemma: How Youth Culture is Reinventing Capitalism*. London: Free Press.
- Massumi, Brian. 2007. "Potential Politics and the Primacy of Preemption", *Theory & Event* 10 (2).  
<http://www.brianmassumi.com/textes/POTENTIAL%20POLITICS%20AND%20THE%20PRIMACY%20OF%20PREEMPTION%20-%20T%20E.doc>.

- Mateas, Michael. 2006. "Weird Languages", in *Software Studies - A Lexicon* (ed. Matthew Fuller). 2008. Cambridge, MA: The MIT Press. pp. 267-275.
- May, Timothy C. 2001. "Crypto Anarchy and Virtual Communities", in *Crypto Anarchy, Cyberstates, and Pirate Utopias* (ed. Peter Ludlow). Cambridge, MA: The MIT Press. pp. 65-80.
- McIntyre, Alice. 2008. *Participatory Action Research*, Qualitative Research Methods Series 52. London: Sage Publications.
- McLeod, Kembrew. 2005. *Freedom of Expression: Resistance and Repression in the Age of Intellectual Property*. New York: Doubleday.
- McTaggart, Robin (ed.). 1997. *Participatory Action Research: International Contexts and Consequences*, SUNY Series: Teacher Preparation and Development. Albany, NY: State University of New York Press.
- Means, Sean P. 2003. "Movies: Arrrgh, there be pirates in movie theaters -- but even more inside Hollywood", in *The Salt Lake Tribune*.  
<http://www.sltrib.com/2003/nov/11022003/arts/107311.asp>.
- Meier, Christian. 2007. "Intellectual Property 2.0: Lawrence Lessig Defends Creativity in the Age of Cyberspace", in *The Berlin Journal* 14. p. 49.  
[http://www.americanacademy.de/uploads/media/BJ14\\_web\\_100dpi\\_01.pdf](http://www.americanacademy.de/uploads/media/BJ14_web_100dpi_01.pdf).
- Milan, Stefania. 2013. "Wikileaks, Anonymous, and the Exercise of Individuality: Protesting in the Cloud", in *Beyond Wikileaks: Implications for the Future of Communications* (eds. Benedetta Brevini, Arne Hintz, Patrick McCurdy. New York: Palgrave Macmillan. pp. 191-208.
- Moglen, Eben. 1999. "Anarchism Triumphant: Free Software and the Death of Copyright". *First Monday* 4 (8). <http://firstmonday.org/ojs/index.php/fm/article/view/684/594>.

- . 2003. “The dotCommunist Manifesto”.  
[http://emoglen.law.columbia.edu/my\\_pubs/dcm.html](http://emoglen.law.columbia.edu/my_pubs/dcm.html).
- Monaghan, Angela. 2007. “Radiohead challenges labels with free album”. *The Telegraph*.  
<http://www.telegraph.co.uk/finance/markets/2816893/Radiohead-challenges-labels-with-free-album.html>.
- Mook, Nate. 2003. “AOL Execs Flush Nullsoft’s WASTE”. *betanews*.  
<http://betanews.com/2003/05/30/aol-execs-flush-nullsoft-s-waste/>.
- Motion Picture Association of America, Inc. 2011. “Types of Content Theft”.  
<http://www.mpa.org/contentprotection/types-of-content-theft>.
- mr-peabody. 2014. “FrootVPN?”. *Reddit*.  
<https://reddit.com/r/VPN/comments/2jzatj/frootvpn/>.
- Nakashima, Yuta, Ryuki Tachibana, Noboru Babaguchi. 2009. “Watermarked Movie Soundtrack Finds the Position of the Camcorder in a Theater”, in *IEEE Transactions on Multimedia* 11 (3). pp. 443-454.
- Nash, Paul. 2014. “FrootVPN Review”. *VPN Creative*.  
<https://vpncreative.net/vpn-providers/frootvpn/>.
- neku. “FAQ”. *Pomf.se*. <https://pomf.se/faq.html>.
- . 2014. “Source code for Pomf.se”. *GitHub*. <https://github.com/nokonoko/Pomf>.
- . 2014-2015. “Transparency”. *Pomf.se*. <http://transparency.pomf.se/>.
- Nemesis][. “Frequently Asked Questions about Internet Relay Chat robots”.  
<http://www.irchelp.org/irchelp/misc/botfaq.html>.
- Newman, Saul. 2001a. *From Bakunin to Lacan: Anti-Authoritarianism and the Dislocation*

- of Power*. Plymouth, UK: Lexington Books.
- . 2001b. “Spectres of Stirner: a Contemporary Critique of Ideology”, in *Journal of Political Ideologies* 6.3. pp. 309-330.
- . 2010a. *The Politics of Postanarchism*. Edinburgh, UK: Edinburgh University Press.
- . 2010b. “Voluntary Servitude Reconsidered: Radical Politics and the Problem of Self-Domination”, in *Anarchist Developments in Cultural Studies* 2010.1: “Post-Anarchism Today”. pp.31-49.
- . 2011. “Stirner’s Ethics of Voluntary Inservitude”, in *Max Stirner* (ed. Saul Newman). New York: Palgrave Macmillan. pp. 189-209.
- Nimus, Anna. 2006. “Copyright, Copyleft and the Creative Anti-Commons”, in *subsol*.  
[http://subsol.c3.hu/subsol\\_2/contributors0/nimustext.html](http://subsol.c3.hu/subsol_2/contributors0/nimustext.html).
- Notes from Nowhere (eds.). 2003. *We Are Everywhere: The Irresistible Rise of Global Anti-Capitalism*. New York: Verso.
- Nullsoft. 2003. “Notice of Unauthorized Software”.  
<https://web.archive.org/web/20030602021255/http://www.nullsoft.com/free/waste/>.
- O’Brien, Damien and Brian Fitzgerald. 2006. “Mashups, Remixes and Copyright Law”, in *Internet Law Bulletin* 9 (2). pp. 17-19. <http://eprints.qut.edu.au/4239/1/4239.pdf>.
- Oerting, Tim (ed.). 1993. “Agrippa: A Book of the Dead”, in *The Unofficial FAQ for alt.cyberpunk*. [https://cdn.preterhuman.net/texts/computer\\_culture/ACY01011.TXT](https://cdn.preterhuman.net/texts/computer_culture/ACY01011.TXT).
- Parry, Richard. 1987. *The Bonnot Gang: The Story of the French Illegalists*. London: Rebel Press.

- Parsonage, Harry. 2010. "The Meaning of LIFE: Linkfiles In Forensic Examinations".  
<http://computerforensics.parsonage.co.uk/downloads/TheMeaningofLIFE.pdf>.
- Pfaffenberger, Bryan. 2003. "'A Standing Wave in the Web of Our Communications':  
Usenet and the Socio-Technical Construction of Cyberspace Values", in *From Usenet  
to CoWebs: Interacting with Social Information Spaces* (eds. Christopher Lueg and  
Danyel Fisher). London: Springer-Verlag. pp. 20-43.
- phobos. 2014. "Thoughts and Concerns about Operation Onymous". *The Tor Blog*.  
<https://blog.torproject.org/blog/thoughts-and-concerns-about-operation-onymous>.
- Piatek, Michael, Tadayoshi Kohno, and Arvind Krishnamurthy. 2008. "Challenges and  
directions for monitoring P2P file sharing networks, or, why my printer received a  
DMCA takedown notice". *USENIX HotSec (Hot Topics in Security)*.  
[https://www.usenix.org/conference/hotsec-08/challenges-and-directions-monitoring-  
p2p-file-sharing-networks%E2%80%94or%E2%80%94why-my](https://www.usenix.org/conference/hotsec-08/challenges-and-directions-monitoring-p2p-file-sharing-networks%E2%80%94or%E2%80%94why-my).
- Piccard, Paul L. 2006. *Securing IM and P2P Applications for the Enterprise*. Rockland:  
Syngress.
- PIEaSanT, Mr. 1992. "AGRIPPA". *alt.cyberpunk*.  
<https://groups.google.com/d/msg/alt.cyberpunk/-AFN4yB0TkQ/RVjgqTmarpUJ>.
- Pilkington, Ed and Matt Williams. 2012. "Colorado theater shooting: 12 shot dead during  
The Dark Knight Rises screening". *The Guardian*.  
[http://www.theguardian.com/world/2012/jul/20/colorado-theater-shooting-dark-  
knight](http://www.theguardian.com/world/2012/jul/20/colorado-theater-shooting-dark-knight).
- Plato. 2008 (c. 380 BC). *The Republic* (trans. Benjamin Jowett). Project Gutenberg.  
<http://www.gutenberg.org/files/1497/1497-h/1497-h.htm>.
- Prager, Brad. 2008. "Interpreting the Visible Traces of Theresienstadt", in *Journal of Modern  
Jewish Studies* 7 (2). pp. 175-194.



- Proudhon, Pierre-Joseph. 1840. *What Is Property?: or, An Inquiry into the Principle of Right and of Government* (trans. Anonymous).  
<https://www.gutenberg.org/files/360/360-h/360-h.htm>.
- Pyrdum, Carl. 2010. "Medieval Copy Protection". *Got Medieval*.  
<http://www.gotmedieval.com/2010/08/medieval-copy-protection.html>.
- Pytlak, John P. 2003. "Anti-Piracy Coding". TKColorist Internet Group.  
<https://tig.colorist.org/pipermail/tig/2003-November/003836.html>.
- Raymond, Eric. 2011. "The importance of being 'ESR' – a sidelight on the G+ nym wars".  
*Armed and Dangerous*. <http://esr.ibiblio.org/?p=3583>.
- Raymond, Eric S. and Guy L. Steele Jr. (eds.). 2003. *The Jargon File*. Version 4.4.7.  
<http://www.catb.org/jargon/html/>.
- Rayna, Thierry and Ludmila Striukova. 2008. "White Knight or Trojan Horse? The Consequences of Digital Rights Management for Consumers, Firms and Society", in *Communications & Strategies* 69. pp. 109-125.
- Read, Jason. 2003. "The Real Subsumption of Subjectivity By Capital", in *The Micro-Politics of Capital: Marx and the Prehistory of the Present*. Albany: SUNY Press. pp. 103-151.
- Reason, Peter and Hilary Bradbury (eds.). 2001. *Handbook of Action Research: Participative Inquiry and Practice*. London: Sage Publications.
- Reid, Elizabeth M. 1996. "Communication and Community on Internet Relay Chat: Constructing Communities", in *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace* (ed. Peter Ludlow). Cambridge, MA: MIT Press. pp. 397-411.
- Renkichi, Hirato. 1921. "Manifesto of the Japanese Futurist Movement" (trans. Miryam Sas),

- in *Cabinet* 13. 2004. <http://cabinetmagazine.org/issues/13/renkichi.php>.
- Riley, Gail Blasser. 2011. *Internet Piracy*, Tarrytown: Marshall Cavendish Corporation.
- Robertson, Adi. 2012. "Demonoid torrent tracker shut down by Ukrainian police". *The Verge*.  
<http://www.theverge.com/2012/8/6/3223253/demonoid-bittorrent-tracker-shut-down-by-ukrainian-police>.
- Roddy, James E., Robert J. Zolla, Leslie Gutierrez. 2005. "Method and Apparatus for Watermarking Film". Patent No.: US6882356B2.
- Roettgers, Janko. 2007. "Usenet, the Original Piracy Hotbed". *Gigaom*.  
<https://gigaom.com/2007/06/02/usenet/>.
- Rogers, Michael and Saleem Bhatti. 2007. "How to Disappear Completely: A Survey of Private Peer-to-Peer Networks", in *SPACE (Sustaining Privacy in Autonomous Collaborative Environments) 2007*. pp. 1-10.  
<http://www.cs.st-andrews.ac.uk/files/publications/download/RB07b.pdf>.
- Rollo, Troy. "A description of the DCC protocol".  
<http://www.irchelp.org/irchelp/rfc/dccspec.html>.
- Rome Act, 1928. 1928. "Article 6bis". International Convention for the Protection of Literary and Artistic Works.  
<http://global.oup.com/booksites/content/9780198259466/15550019>.
- Rump, Niels. 2003. "Digital Rights Management: Technological Aspects: Definition, Aspects, and Overview", in *Digital Rights Management: Technological, Economic, Legal and Political Aspects* (eds. G. Goos, J. Hartmanis, and J. van Leeuwen). New York: Springer. pp. 3-15.
- Saarinen, Juha. 2013. "'Data Massacre' as Megaupload Files Deleted". *iTnews*.

<http://www.itnews.com.au/News/347330,data-massacre-as-megaupload-files-deleted.aspx>.

Sack, Warren. 2008. "Memory", in *Software Studies - A Lexicon* (ed. Matthew Fuller). 2008. Cambridge, MA: The MIT Press. pp. 184-193.

Saviotti, Pier Paolo and Andreas Pyka. 2011. "Generalized Barriers to Entry and Economic Development", in *Catching Up, Spillovers and Innovation Networks in a Schumpeterian Perspective* (eds. Andreas Pyka and Maria da Graça Derengowski Fonseca). London: Springer-Verlag. pp. 59-80.

Schneiderman, Eric T. 2008. "Attorney General Announces Agreement With Cablevision To Block Online Child Pornography". Press release.  
<http://www.oag.state.ny.us/press-release/attorney-general-announces-agreement-cablevision-block-online-child-pornography>.

Scott, Charlie, Paul Wolfe, Mike Erwin. 1999. *Virtual Private Networks* (Second Edition). Sebastopol, CA: O'Reilly & Associates Inc.

Seltzer, Wendy. 2011. "Infrastructures of Censorship and Lessons from Copyright Resistance". *USENIX FOCI Workshop*.  
[http://www.usenix.org/events/foci11/tech/final\\_files/Seltzer.pdf](http://www.usenix.org/events/foci11/tech/final_files/Seltzer.pdf).

Seventh Congress. 1802. The 1802 Amendment to the Copyright Act of 1790, in *Primary Sources on Copyright (1450-1900)* (eds. L. Bently and M. Kretschmer).  
[http://copy.law.cam.ac.uk/cam/tools/request/showRepresentation?id=representation\\_us\\_1802](http://copy.law.cam.ac.uk/cam/tools/request/showRepresentation?id=representation_us_1802).

Shiva, Vandana. 1999. *Biopiracy: The Plunder of Nature and Knowledge*. Boston, MA: South End Press.

Slater, Christopher, Stephen Mark Keating, Mark Julian Russell. 2010. "Audio Watermarking Apparatus and Method". Patent No.: US20100057231A1.

- Sockanathan, Andrew. 2011. "Digital Desire and Recorded Music: OiNK, Mnemotechnics and the Private BitTorrent Architecture". Doctoral thesis, Goldsmiths, University of London.  
[https://research.gold.ac.uk/6569/1/CCS\\_thesis\\_Sockanathan\\_2011.pdf](https://research.gold.ac.uk/6569/1/CCS_thesis_Sockanathan_2011.pdf).
- Spek, Olaf van der. 2008. "UDP Tracker Protocol for BitTorrent". BitTorrent.org.  
[http://www.bittorrent.org/beps/bep\\_0015.html](http://www.bittorrent.org/beps/bep_0015.html).
- srv017.bxl.xs4all.be. 2005. "What is Freenet?". *The Freenet Help Site*.  
<http://www.freenethelp.org/html/Freenet.html>.
- Supriya Singh, Margaret Jackson, Jenny Waycott, and Jenine Beekhuyzen. 2006. "Downloading vs Purchase: Music Industry vs Consumers", in *Digital Rights Management: Technologies, Issues, Challenges and Systems* (eds. Reihaneh Safavi-Naini and Moti Yung). Germany: Springer-Verlag. pp. 52-65.
- Sims, Nancy. 2011. "Library licensing and criminal law The Aaron Swartz case", in *College & Research Libraries News* 72 (9). pp. 534-537.
- Stallman, Richard M. 2002a. *Free Software, Free Society: Selected Essays of Richard M. Stallman*. Boston: GNU Press.
- . 2002b. "On Hacking". <https://stallman.org/articles/on-hacking.html>.
- . 2013. "Free Software Is Even More Important Now". *GNU Project*.  
<https://www.gnu.org/philosophy/free-software-even-more-important.html>.
- Stamp, Mark. 2003. "Digital Rights Management: The Technology Behind The Hype", in *Journal of Electronic Commerce Research* 4 (3). pp. 102-112.
- Stevens, Jacob. "About Verso". <http://www.versobooks.com/pg/about-verso>.

- Stirner, Max. 1842. "The False Principle of Our Education; or, Humanism and Realism".  
[http://theanarchistlibrary.org/library/Max\\_Stirner\\_\\_The\\_False\\_Principle\\_of\\_Our\\_Education.html](http://theanarchistlibrary.org/library/Max_Stirner__The_False_Principle_of_Our_Education.html).
- . 1845. "Stirner's Critics" (trans. Wolfi Landstreicher).  
<http://theanarchistlibrary.org/library/max-stirner-stirner-s-critics>.
- . 1907. *The Ego and His Own* (trans. Steven T. Byington). New York: Benj. R. Tucker. <http://www.df.lth.se/~triad/stirner/theego/theego.html>.
- Strangelove, Michael. 2005. *The Empire of Mind: Digital Piracy and the Anti-Capitalist Movement*. Toronto: University of Toronto Press.
- Striphas, Ted. 2006. "Disowning Commodities: Ebooks, Capitalism, and Intellectual Property Law", in *Television and New Media* 7 (3). pp. 231-260.
- Striphas, Ted and Kembrew McLeod. 2006. "Strategic Improprieties - Cultural Studies, The Everyday, and the Politics of IP", in *Cultural Studies* 20 (2-3). pp. 119-144.
- Stroustrup, Bjarne. 1998. "Generalizing Overloading for C++2000".  
[https://www.cct.lsu.edu/~hkaiser/spring\\_2012/files/whitespace98.pdf](https://www.cct.lsu.edu/~hkaiser/spring_2012/files/whitespace98.pdf).
- Suchanek, Fabian M., David Gross-Amblard, and Serge Abiteboul. 2011. "Watermarking for Ontologies", in *The Semantic Web - ISWC 2011 - 10th International Semantic Web Conference Bonn, Germany, October 2011, Proceedings, Part I* (eds. Lora Aroyo, Chris Welty, Harith Alani, Jamie Taylor, Abraham Bernstein, Lalana Kagal, Natasha Noy, and Eva Blomqvist). Lecture Notes in Computer Science 7031. Germany: Springer-Verlag. pp. 697-713.
- Ted the Tool. 1991. MIT Guide to Lockpicking.  
<https://www.lysator.liu.se/mit-guide/MITLockGuide.pdf>.
- Thomas, Douglas. 2002. *Hacker Culture*. Minneapolis, MN: University of Minnesota Press.

- Thompson, EP. 1967. "Time, Work-Discipline, and Industrial Capitalism", in *Past and Present* 38. pp. 56-97.
- timbotron. 2007. "Movie Review: Pirates of the Caribbean – At World’s End".  
*Blogadilla.com*.  
<http://www.blogadilla.com/2007/05/27/movie-review-pirates-of-the-caribbean-at-worlds-end/>.
- TonikGin. 2002. "XDCC - An .EDU Admin’s Nightmare".  
<https://www.ncsu.edu/itd/security/papers/EduHacking.html>.
- Topkara, Mercan, Cuneyt M. Taskiran, and Edward J. Delp. 2005. "Natural Language Watermarking". *Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents*. pp. 441-452.
- Tor Project. "Configuring Hidden Services for Tor". *Tor Project*.  
<https://www.torproject.org/docs/tor-hidden-service.html.en>.
- . "Tor: Overview". *Tor Project*. <https://www.torproject.org/about/overview>.
- Toscano, Alberto. 2009. "Chronicles of Insurrection: Tronti, Negri and the Subject of Antagonism", in *Cosmos and History: The Journal of Natural and Social Philosophy* 5 (1).  
<http://cosmosandhistory.org/index.php/journal/article/view/128/240>.
- tracked6040. 2014. "I use VYPR VPN and just got a DCMA copyright notice". *Reddit*.  
[https://reddit.com/r/VPN/comments/2bb0u1/i\\_use\\_vypr\\_vpn\\_and\\_just\\_got\\_a\\_dcma\\_copyright/](https://reddit.com/r/VPN/comments/2bb0u1/i_use_vypr_vpn_and_just_got_a_dcma_copyright/).
- Trevathan, Jarrod and Hossein Ghodosi. 2003. "Overview of Traitor Tracing Schemes", in *Communications of CCISA, Selected Topics of Cryptography and Information Security* 9 (4). pp. 51-63.

Tushar, Shantanu and Sarath Lakshman. 2013. *Linux Shell Scripting Cookbook* (Second Edition). Birmingham, UK: Packt Publishing.

United Nations General Assembly. 1966. International Covenant on Civil and Political Rights. Part III. Article 6. 1.  
<http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>.

United States Copyright Office. 2011. *Circular 92: Copyright Law of the United States and Related Laws Contained in Title 17 of the United States Code*. Washington, DC: Library of Congress. <http://copyright.gov/title17/circ92.pdf>.

United States Copyright Office. 2013. *Circular 3: Copyright Notice*. Washington, DC: Library of Congress. <http://www.copyright.gov/circs/circ03.pdf>.

*United States of America v. Jason A. Wright*. 2010. No. 08-10525. D.C. Docket No. 4:03-cr-01908-RCC-CRP. Opinion.  
[http://njlaw.rutgers.edu/collections/resource.org/fed\\_reporter/NEWcircs/cir9/08-10525\\_cir9.html](http://njlaw.rutgers.edu/collections/resource.org/fed_reporter/NEWcircs/cir9/08-10525_cir9.html).

*United States of America v. Kim Dotcom, Megaupload Limited, Vestor Limited, Finn Batato, Julius Bencko, Sven Echternach, Mathias Ortmann, Andrus Nomm, Bram Van Der Kolk*. 2012. Indictment. Criminal No. 1:12CR3.  
<https://www.scribd.com/doc/78786408/Mega-Indictment>.

*United States of America v. Neville McGarity (aka Wraith), Daniel Castleman (aka Chingachgook), Gary Lakey (aka Eggplant), Marvin Lambert (aka Methuselah), Ronald White (aka Roadkill), James Freeman (aka Mystikal), Warren Mumpower (aka Lizzard)*. 2012. No. 09-12070. D.C. Docket No. 08-00022-CR-3-LAC.  
<http://caselaw.findlaw.com/us-11th-circuit/1593463.html>.

United States Patent and Trademark Office. 2014. *Protecting Your Trademark: Enhancing Your Rights Through Federal Registration - Basic Facts About Trademarks*.

<http://www.uspto.gov/sites/default/files/trademarks/basics/BasicFacts.pdf>.

Universal Copyright Convention. 1971. Article III, §1.

[https://en.wikisource.org/wiki/Universal\\_Copyright\\_Convention#Article\\_III](https://en.wikisource.org/wiki/Universal_Copyright_Convention#Article_III).

Vaidhyathan, Siva. 2001. *Copyrights and Copywrongs: The Rise of Intellectual Property and How It Threatens Creativity*. New York: New York University Press.

Vaneigem, Raoul. 1967. *The Revolution of Everyday Life: Impossible Realisation or Power as the Sum of Seductions*. Red & Black.

<http://library.nothingness.org/articles/SI/en/display/56>.

Verso. 2010. "Growing Knowledge: Wu Ming Present Manituana". *Versobooks.com*.

<http://www.versobooks.com/events/16-growing-knowledge-wu-ming-present-manituana>.

Vizireanu, Ion, Yousef Wasef Nijim, Mike Arthur Derrenberge. 2012. "System and Method for Analyzing and Marking Film". Patent No.: US8090145B2.

vpnreviewer. 2014. "FrootVPN Review". *VPN Reviewer*.

<https://vpnreviewer.com/frootvpn-review>.

Wadsworth, Yoland. 1998. "What is Participatory Action Research?". *Action Research International*, Paper 2.

<http://web.archive.org/web/20090205153046/http://scu.edu.au/schools/gcm/ar/ari/p-ywadsworth98.html>.

Wang, Wallace. 2004. *Steal This File Sharing Book: What They Won't Tell You about File Sharing*. San Francisco: No Starch Press.

Warwick, Henry. 2014. *Radical Tactics of the Offline Library*. Network Notebooks 07.

Amsterdam: Institute of Network Cultures.



- Welsh, John F. 2010. *Max Stirner's Dialectical Egoism - A New Interpretation*. Plymouth, UK: Lexington Books.
- Whitfield, Lee. 2011. "Rock Around the Clock". *SANS EU Digital Forensics and Incident Response Summit*.  
<https://digital-forensics.sans.org/summit-archives/2011/2-rock-around-the-clock.pdf>.
- Wijayaratna, C. M. 1996. *Participatory Action Research: Strengthening Farmer Organizations and Agency-Farmer Relations*. International Irrigation Management Institute.
- Williams, Robert W. 2005. "Politics and Self in the Age of Digital Re(pro)ducibility", in *Fast Capitalism* 1 (1). [https://www.uta.edu/huma/agger/fastcapitalism/1\\_1/williams.html](https://www.uta.edu/huma/agger/fastcapitalism/1_1/williams.html).
- Wilson, Peter Lamborn. 1996. "Cybernetics & Entheogenics: From Cyberspace to Neurospace", in "Next Five Minutes" *Conference on Tactical Media Amsterdam*.  
<http://www.t0.or.at/hakimbey/neurospc.htm>.
- WikiLeaks. 2010. "Global - PayPal freezes WikiLeaks donations". *WikiLeaks*.  
<https://www.wikileaks.org/PayPal-freezes-WikiLeaks-donations.html>.
- . 2011. "Wikileaks: Banking Blockade and Donations Campaign". *WikiLeaks*.  
<https://wikileaks.org/IMG/pdf/WikiLeaks-Banking-Blockade-Information-Pack.pdf>.
- "Wikipedia:Wikipedians". 2014. *Wikipedia*.  
<https://en.wikipedia.org/wiki/Wikipedia:Wikipedians>.
- Wilson, Rowan. 2009. "ATTENTION AAAARG.ORG ADMINISTRATOR".  
<http://ifile.it/e235laq>.
- Winokur, Mark. 2003. "The Ambiguous Panopticon: Foucault and the Codes of Cyberspace". *CTheory.net* a124. <http://www.ctheory.net/printer.aspx?id=371>.

- Wood, Jessica A. 2010. "The Darknet: A Digital Copyright Revolution", in *Richmond Journal of Law & Technology* 16 (4). pp. 1-60.  
<http://jolt.richmond.edu/v16i4/article14.pdf>.
- World Intellectual Property Organization. 2004. "International Treaties and Conventions on Intellectual Property", in *WIPO Intellectual Property Handbook: Policy, Law and Use*. pp. 237-364.  
<http://www.wipo.int/export/sites/www/about-ip/en/iprm/pdf/ch5.pdf>.
- Zamudio, Dan. 1995. *How to Sneak into the Movies*. Port Townsend, WA: Breakout Productions.
- Zetter, Kim. 2012. "LulzSec Leader Was Snitch Who Helped Snag Fellow Hackers". *Wired*.  
<http://www.wired.com/2012/03/lulzsec-snitch/>.
- . 2014. "Is Anonymous Dead, or Just Preparing to Rise Again?" *Wired*.  
<http://www.wired.com/2014/06/anonymous-sabu/>.
- Zimmermann, Hubert. 1980. "OSI reference model—The ISO model of architecture for open systems interconnection." *IEEE Transactions on Communications* (28.4). pp. 425-432
- Zuo, Xiang, Jeremy Blackburn, Nicolas Kourtellis, John Skvoretz, Adriana Iamnitchi. 2014. "The Power of Indirect Ties in Friend-to-Friend Storage Systems", in *14th IEEE International Conference on Peer-to-Peer Computing (P2P)*. pp. 1-5.  
[https://www.p2p-conference.org/~ptwopcon/p2p14/wp-content/uploads/2014/09/221.P2P2014\\_64.pdf](https://www.p2p-conference.org/~ptwopcon/p2p14/wp-content/uploads/2014/09/221.P2P2014_64.pdf).

## Video

- Cameron, James. 1984. *The Terminator*. US: Hemdale Film, Pacific Western, Euro Film Funding, Cinema '84.

Cameron, James. 1991. *Terminator 2: Judgment Day*. US: Carolco Pictures, Pacific Western, Lightstorm Entertainment, Le Studio Canal+ S.A.

Craven, Wes. 1996. *Scream*. US: Dimension Films and Woods Entertainment.

Craven, Wes. 1997. *Scream 2*. US: Dimension Films, Konrad Pictures, Craven-Maddalena Films, Miramax, Maven Entertainment.

eeplox. 2012. "Simple Living - Picking a Wild Salad". *YouTube*.  
<https://www.youtube.com/watch?v=nPBIfeuZuWg>.

Federation Against Copyright Theft (FA©T). 2002. Anti-Piracy Advert.  
<https://www.youtube.com/watch?v=hNzCiZAzxCA>.

Gerron, Kurt. 1944. *Theresienstadt - Ein Dokumentarfilm aus dem jüdischen Siedlungsgebiet* (aka *The Führer Gives a City to the Jews*). Germany: SS-Central Office for the Settlement of the Jewish Question in Bohemia and Moravia.

Lucas, George. 1971. *THX 1138*. US: American Zoetrope and Warner Bros.

McTiernan, John. 1993. *Last Action Hero*. US: Columbia Pictures and Oak Productions.

MonkeyT. 2012. "PLAN-C CAM XViD SHOCKING". *The Pirate Bay*.  
<https://thepiratebay.se/torrent/7074665>.

No one. *Illegala*<sup>763</sup>.

phrozen77. 2009. "HowTo: IRC anonymously with TOR".  
<http://www.irc-junkie.org/2009-12-31/howto-irc-anonymously-with-tor/>.

Porcelijn, Max. 2012. *Plan C*. Netherlands: LEV Pictures, Plan C Filmfonds, CTM Films,

---

<sup>763</sup> Details redacted. Refer to Disclaimer of Liability.

Algemene Vereniging Radio Omroep (AVRO), Production Value.

Warner Bros. 2007. *Casablanca* Anti-Piracy Advert.

<https://www.youtube.com/watch?v=DvjFsZJqAPs>.

## Web

AirVPN. 2014. “Why Us?”. <https://airvpn.org/whyus/>.

Amazon. “Marching Plague”. Product Listing.

<http://www.amazon.com/Marching-Plague-Warfare-Global-Public/dp/157027178X/>.

AnonFiles. 2014. <https://anonfiles.com/>.

“Cases matching ‘killer joe nevada’”. 2014. Justia Dockets & Filings. Web search.

<http://dockets.justia.com/search?query=killer+joe+nevada>.

CrimethInc. Ex-Workers’ Collective. 2014. “Web Store - Recipes for Disaster”. Product Listing. <http://www.crimethinc.com/books/rfd.html>.

Critical Art Ensemble. 2007. via Internet Archive Wayback Machine.

<https://web.archive.org/web/20070612035716/http://www.critical-art.net/books/mp/index.html>.

———. 2007. via Internet Archive Wayback Machine.

<https://web.archive.org/web/20070406135154/http://www.critical-art.net/books/index.html>

Distributed Proofreaders. <http://www.pgdp.net/c/>.

DRM Removal. 2014. Reddit. <https://pay.reddit.com/r/drmremoval>.

DuckDuckGo. 2014. <https://duckduckgo.com>.

Giganews. 2012.

<https://web.archive.org/web/20120407173534/http://www.giganews.com/why.html>.

———. 2014. <https://www.giganews.com/>.

Gnutella Forums. <http://www.gnutellaforums.com/>.

Google. 2014. <https://www.google.com>.

Hidden Tracker, The. 2009. <http://z6gw6skubmo2pj43.onion>.

Hidden Tracker, The. <https://twitter.com/hiddentracker>

Hidden Wiki, The. 2013. [http://kpvz7ki2v5agwt35.onion/wiki/index.php/Main\\_Page](http://kpvz7ki2v5agwt35.onion/wiki/index.php/Main_Page).

IMDb.com, Inc. 2014. *Box Office Mojo*. <http://www.boxofficemojo.com/>.

jj4321. 2013. “USENET over TOR (nntp)?”. *TorForum.org*.

<http://torforum.org/viewtopic.php?f=2&t=18313>.

KickassTorrents. 2014. <https://kickass.to>.

Library Genesis. 2014. <http://libgen.org>.

LibrePlanet. 2014. [https://libreplanet.org/wiki/Main\\_Page](https://libreplanet.org/wiki/Main_Page).

LimeWire. 2014. <http://www.limewire.com/>.

Motion Picture Association of America, Inc. 2012. *Fight Film Theft*.

<http://www.fightfilmtheft.org/>.

niederberger. 2013. “imgSeek - Intelligent Image Database”.

<http://sourceforge.net/projects/imgseek/>.

Nine Inch Nails. 2008. *The Slip*. <https://dl.nin.com/theslip/signup>.

Oldversion.com. “Download Old Versions of uTorrent for Windows”. *OldVersion.com*.

<http://www.oldversion.com/windows/utorrent/>.

“Plan C Release Info”. *IMDb*. <http://www.imdb.com/title/tt1922689/releaseinfo>.

Pirate Bay, The. <https://thepiratebay.se>.

Radiohead. 2007. *In Rainbows*. <http://www.inrainbows.com/>.

Right2Remix.org. 2013. <http://right2remix.org>.

Silk Road. <http://silkroadvb5piz3r.onion>.

Soulseek. 2014. “Download”. *Soulseek*. <https://www.soulseekqt.net/news/node/1>.

Space Puppy Grotto (SPG). [http://\\*.onion](http://*.onion)<sup>764</sup>.

Tor Project. <https://www.torproject.org/>.

Torrent Invite. <http://www.torrentinvitesell.com/>.

urlQuery. 2014. “cdn.anonfiles.com/1400515873889.pdf”. *urlQuery* [*Google Cache*].

<https://webcache.googleusercontent.com/search?q=cache:JsvASEdVyaQJ:https://urlquery.net/report.php%3Fid%3D1406955387110>.

V£R\$O. 2013. <https://fckvrso.wordpress.com/>.

---

<sup>764</sup> Title is fictional; URL redacted. Refer to Disclaimer of Liability.

venotes. 2014. "What tracker is **\*\*the\*\*** hardest to get into these days?" *Reddit*.

[https://www.reddit.com/r/trackers/comments/27paw7/what\\_tracker\\_is\\_the\\_hardest\\_to\\_get\\_into\\_these\\_days/ci30m9x](https://www.reddit.com/r/trackers/comments/27paw7/what_tracker_is_the_hardest_to_get_into_these_days/ci30m9x).

YouTube. Content ID. *YouTube*. <https://www.youtube.com/t/contentid>.