

Sub-Versions: Investigating Videogame Hacking Practices and Subcultures

Michael Iantorno

A Thesis

In

The Department

Of

Communication Studies

Presented in Partial Fulfillment of the Requirements

For the Degree of Master of Arts (Media Studies) at

Concordia University

Montreal, Quebec, Canada

June 2019

© Michael Iantorno, 2019

Concordia University: Signature Page

School of Graduate Studies

This is to certify that the thesis prepared

By: **Michael Iantorno**

Entitled: **Sub-Versions: Investigating Videogame Hacking Practices and Subcultures**

and submitted in partial fulfillment of the requirements for the degree of

Masters of Arts (Media Studies)

complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

Dr. Owen Chapman Chair

Dr. Mia Consalvo Examiner

Dr. Darren Wershler Examiner

Dr. Matt Soar Thesis Supervisor

Approved by _____
Chair of Department, *Charles Acland*

_____ 2019 _____
Dean of Faculty, *André G. Roy*

Abstract

Sub-Versions: Investigating Videogame Hacking Practices and Subcultures

Michael Iantorno

“Hacking” is an evocative term — one that is mired in tropes that reduce a diverse range of practices into a few stereotypically malicious activities. This thesis aims to explore one hacking practice, videogame hacking, whose practitioners make unauthorized alterations to videogames after their release. Through interviews, game analysis, and reflective writing, this thesis investigates videogame hacking subcultures of production — communities of creative labour that exist in the margins of mediamaking and the fringes of the law.

This thesis begins by reviewing popular media and existing accounts of computer hacker culture, primarily Steven Levy’s *Hackers: Heroes of the Computer Revolution* and Gabriella Coleman’s *Coding Freedom*, in order to contextualize videogame hacking in broader histories of computer culture. Using this analysis as a starting point, the author then proposes a reflexive methodological framework for studying videogame hacking subcultures, designed to accommodate the ephemerality of virtual communities and the apprehensions of participants.

The following two chapters refer to participant interviews to pursue two avenues of research. First, drawing upon Michel de Certeau’s writing on strategies versus tactics and Henry Jenkins chronicling of prohibitionist and collaborationist models, this study explores how intellectual property law serves as a site of tension between media companies and videogame fans. Second, the author explores the diverse motivations of videogame hackers who create works that are undistributable through commercial markets and may face the risk of legal action.

Dedication

I would like to dedicate this work to my partner Brooke, who wisely warned me of the challenges associated with a master's degree, but whose advice fell on deaf ears (at least at first). I am truly lucky to have your continued love, support, and patience.

Acknowledgements

There are too many people to acknowledge in this very limited space, but I will try my best. I would like to sincerely thank...

- Matt Soar, for supporting my research despite countless unforeseen changes in direction over the past two years.
- Mia Consalvo, for warmly inviting me into the mLab and introducing me to one of the kindest collections of grad students I have ever met.
- Darren Wershler, for helping shape and enrich my PhD research aspirations.
- Owen Chapman, for empowering me to teach creatively and (hopefully) competently.
- The entire Media Studies 2017-2019 cohort, whose brilliance inspired me to read more, study harder, and write fervently.
- All the folks at TAG and the mLab, for showing me that game studies can include everything from homemade tricorders to sprawling essays about Eastern Europe.
- My brothers: Matt, for encouraging me to pursue extremely niche game design interests; Mark, for (perhaps unintentionally) getting me hooked on role-playing games; and Alex, for giving me an excuse to revisit all my favourite games in an older-brother capacity.
- My parents, for lovingly raising and supporting four giants nerds.

Table of Contents

List of Images	vii
Introduction: A Decade of EarthBound Hacking	1
Investigating Videogame Hacking	4
Chapter 1: What Is Videogame Hacking?	8
A Short Excerpt From <i>Hackers</i> (1995)	9
Computer Hacker Tropes and Stereotypes	10
Levy, Coleman, and the Principles of Hacking	12
Bailey and Finding a Working Definition for Videogame Hacking	16
Narrowing the Field	21
Assembling a Methodological Framework	23
Interviews	25
Videogame Hack Analysis	27
Reflective Writing	29
Chapter 2: Technical & Legal Barriers	31
Chrono Trigger: Crimson Echoes	31
Disclaimer: This Is Not A Legal Study	35
de Certeau, Strategies, and Tactics	37
Applying Strategy and Tactics to Videogame Hacking	39
Prohibitionist and Collaborationist Models	41
Pokémon Prism	44
Patch Files and Decentralization	46
Anonymity, Dispersal, and Persistence	49
The <i>A Link to the Past Randomizer</i> and Online Patching	53
Pass-Through Modification and Nintendo vs Galoob	56
Chapter 3: Hacking Motivations	60
A Typology of Motivations	61
Love for the Game - Fans of the Code	63
Community and Collective Intelligence	68
Improvement, Creativity, and Media Archaeology	74
Hacking for Fun and Profit	80
Conclusion	86
A Review of Common Themes	89

Research Limitations and Considerations	92
Hack to the Future	95
References	98
Works Cited	98
Mediography	102
Hackography	104
Appendix I: Participant Profiles	105
Adam	105
Pokémon Prism	105
Axel Hellström	106
Chris Owen	106
Veetorp	107
A Link to the Past Randomizer	107
David Shayne	108
Project M	109
Kaze Emanuar	109
SM64: Last Impact	110
SM64 Online	110
Max Ponoroff	111
Edwin & Jones	111
Starstruck: A Music Adventure Game	112
ZeaLity	112
Chrono Trigger: Crimson Echoes	113
Appendix II: Glossary of Terms	114
Appendix III: Glossary of Websites	118

List of Images

Introduction

- 0.1 Screenshot from: *HyperBound*. 2
- 0.2 Screenshot from: *HyperBound*. 2

Chapter 1

- 1.1 Screenshot from: *Space Invaders*. 19
- 1.2 Screenshot from: *Space Invaders Arcade*. 19
- 1.3 Excerpt from game logs for *Sub-Versions* 28

Chapter 2

- 2.1 Cease and Desist Order for *Chrono Trigger: Crimson Echoes*. 33
- 2.2 *Calvin and Hobbes*, 25 February, 1995. 50
- 2.3 Screenshot of the *A Link to the Past Randomizer*'s online patching application. 55
- 2.4 Game Genie, Front. 58
- 2.5 Game Genie, Box. 58

Chapter 3

- 3.1 Screenshot from: *A Link to the Past Randomizer*. 67
- 3.2 Screenshot from: *The Legend of Zelda: Mystery of Solarus DX*. 67
- 3.3 Puzzle Race #8 72
- 3.4 Screenshot of *Icons: Combat Arena*. 83
- 3.5 Concept Art for *The Wu Xing*. 83

Conclusion

- 4.1 Work-in-progress screenshot of *Edwin & Jones* 86
- 4.2 *Starstruck: A Music Adventure Game* – Trailer. 86

Introduction: A Decade of EarthBound Hacking

In the spring of 2007, as part of my senior project in Ryerson University's New Media program, I created the simple videogame hack *HyperBound*. Built entirely within the framework of the 1994 Super NES title *EarthBound* — one of my all-time favourite videogames — *HyperBound* follows the trials and tribulations of an unnamed amnesiac who is thrust into a world that is completely unknown to them. While sharing innumerable similarities with its predecessor, I heavily altered *EarthBound*'s assets in order to rearrange the game world, introduce an original narrative, and remove all the game's combat elements. Instead of leveling up and defeating enemies, players instead explore a peaceful game world while attempting to piece together their lost memories. Failing at this task causes the entire game to crumble in a stereotypically glitchy manner: garbage blocks muck up the screen, dialogue becomes scrambled, and some of the hack's content may become completely inaccessible. Despite diverging from *EarthBound*'s themes and mechanics, *HyperBound* gained a surprising amount of popularity online, appearing in various blogs and even finding its way into Anna Anthropy's book *Rise of the Video Game Zinesters*:

Throughout the hack, Iantorno repurposes assets from EarthBound to fit his new story. The bearded, sunglasses-wearing criminal the player encounters in EarthBound becomes the radio DJ whose show the protagonist of HyperBound used to call in to before he lost his memory. The boarding school that appears in EarthBound, with its classrooms and lockers, becomes the university that HyperBound's protagonist attended, where he meets former teachers and finds valuable information on his previous life. All of EarthBound's graphics are sampled and give new purposes in the hacked game. (Anthropy 78)

Published five years after *HyperBound*'s completion and exhibition, Anthropy's framing of videogame hacking as a type of sampling seemed curious to me at the time. Sampling drew my mind toward other types of media practice — particularly electronic music composition and remix — and was certainly not a term that was utilized by the online hacking communities that I frequented. Reflecting on that moment, I now realize that my confusion was likely sparked by my own narrow understanding of the practice. My perspective on videogame hacking was rooted in a specific time, on a single title, and was centered almost completely around the Starmen.net *EarthBound* fan community. Thus, my comprehension of the practice was very limited, defined by the tacit knowledge I had acquired through the creation of *HyperBound* and my continued involvement with a very small corner of the internet.



Fig 1. Screenshot from: *HyperBound*.
michaeliantorno.com/portfolio/hyperbound.
 Accessed 6 June 2018.



Fig 2. Screenshot from: *HyperBound*.
michaeliantorno.com/portfolio/hyperbound.
 Accessed 6 June 2018.

Opening my thesis with a recollection of my past work may seem a touch indulgent, but this short stretch of autobiographical writing is important for two key reasons. First, I felt it was essential to establish how I am situated in relation to my research, which aims to explore a practice that I have been engaged with for over a decade. Henry Jenkins notes that when he

writes about fan cultures, he does so as “an academic (who has access to certain theories of popular culture, certain bodies of critical and ethnographic literature) and as a fan (who has access to the particular knowledge and traditions of that community)” (Jenkins, *Textual Poachers* 5). I consider myself similarly positioned, as my history with videogame hacking provides me with a certain level of insider knowledge, while also saddling me with biases and presumptions about its practices and communities. This brings me to a second reason for this preamble, which became clear to me as I set out on my research: even for someone entrenched in the activity, videogame hacking can be a difficult topic to pin down. Across gaming websites, the practice is consistently framed as pirating or cheating within digital games, popping up in the news cycle during particularly scandalous (Gach) incidents or in reaction to developer-focused efforts to ban cheaters (Horti). Popular depictions of hacking often fail to move past the persistent trope of the hacker as a rogue computer programmer, using their computer prowess for good (*Hackers*) or evil (*Live Free or Die Hard*). Even among its practitioners, there is much debate on what exactly constitutes videogame hacking. Whereas Cory Arcangel may refer to *Super Mario Clouds* as a modification in his portfolio (Arcangel), the Whitney Museum of Art classifies it as a “hacked” game (*Super Mario Clouds* 2002), and recent critiques by Patrick Lemieux attempt to position it as a sampling of elements from *Super Mario Bros.* rather than either hacking or modding (LeMieux).

Despite the limits of both my personal experiences with the practice and these popular definitions, they still serve as a useful starting point for my research on videogame hacking subcultures — communities of creative labour that exist in the margins of mediamaking and the fringes of the law. This study intends to engage with various videogame hackers and hacking communities in an attempt to answer two core research questions: 1) What motivates game

developers to create tools and hacks that are undistributable through commercial markets and are at constant risk of legal action?; and 2) What novel gameplay experiences and narratives can emerge through the editing, remixing, and subversion of existing video game content? As my research progressed, these two questions prompted a pair of additional queries: “what is videogame hacking?” and “how does one go about studying it?” These latter questions compelled me to revisit the historical and methodological aspects of my work, and proved useful in laying the foundation for my core research questions.

Investigating Videogame Hacking

This thesis is interested in locating videogame hacking in broader contexts of hacking culture and history while also exploring how and why certain individuals and communities engage in a practice that often lies in opposition to the contemporary regimes of capitalism. I combined interviews with various videogame hackers with textual analysis of their creative outputs — primarily consisting of completed hack projects and development tools — to form the basis of my thesis, while utilizing reflexive writing to synthesize my research and position myself in relation to it. I will further elaborate upon my methodology in later chapters, but I would like to establish that I did not intend to provide a thorough history of videogame hacking nor an absolute definition of what it is. I instead chose to focus on a few key individuals and projects that were prominent within videogame hacking communities and were accessible enough to facilitate my research methods, resulting in a partial study that aims to productively generate knowledge about the motivations and works of videogame hackers.

Chapter 1 of my thesis interrogates two practical concerns associated with my research: “what is videogame hacking?” and “how does one go about studying it?” I begin with a short reflection on the 1995 movie *Hackers* which, due to both its popularity and inaccuracies, serves

as an excellent site for discussing the hacker tropes that I have grappled with throughout my research. Seeking a working definition of both “hacking” and “videogame hacking,” I turn toward three important documents about hacker culture: Loyd Blankenship’s *The Conscience of the Hacker*, Stephen Levy’s *Hackers: Heroes of the Computer Revolution*, and Gabriella Coleman’s *Coding Freedom: The Ethics and Aesthetics of Hacking*. Using these as historical and theoretical grounding, I then refer to William Ruffin Bailey’s *Hacks, Mods, Easter Eggs, and Fossils* in an attempt to locate videogame and modding practices in broader computer hacking histories. Having formulated a working — but certainly not authoritative — definition of videogame hacking, I close the chapter by detailing the methods used to undertake my research: interviews, qualitative game analysis, and reflective writing.

Chapter 2 focuses primarily on the work of ROM hackers — those who enact changes to digital copies of cartridge-based videogames — documenting the technical and legal concerns that inform and complicate their work. Citing high-profile cease and desist orders leveled at *Chrono Trigger: Crimson Echoes* and *Pokémon Prism* as examples of direct developer intervention, I craft a theoretical framework for understanding the tension between media companies and videogame hackers. Rooted in the theories of Michel de Certeau and Henry Jenkins, I consider how developers establish strategies to protect their published works, and how videogame hackers tactically seek out cracks in these strategies in order to continue their practice and distribute their cultural outputs. I then document and analyze three sets of tactics adopted by my participants: patch files and decentralization; anonymity, dispersal, and persistence; and online patching applications. I conclude the chapter with a short reflection on *Lewis Galoob Toys, Inc. v. Nintendo of America, Inc.*, a lawsuit that several of my participants believe vindicates their production and distribution methods.

In Chapter 3, I move on from the “how” of videogame hacking and instead explore what motivates players to edit a game’s code in unsanctioned and unexpected ways. I open with a brief summary of Jeroen Jansz and Jørgen Haug Theodorsen’s list of potential modding motivations, using their typology as a guide while also adding context and categories of my own. I then compare these motivations with those expressed by both my participants and other scholars, beginning with Hector Postigo’s account of PC game modders in which he analyzes how videogame fandom can extend to both its text and its code. Extending upon this idea, I consider how speedruns and puzzle races tie into the formation of videogame hacking knowledge communities as well as Boluk and LeMieux’s concept of the metagame — as both require in-depth knowledge of a game’s code, logic, and mechanics. Returning to Henry Jenkins, I then discuss how virtual communities leverage their collective intelligence to map out the inner-workings of videogames, facilitating both amateur media archaeology and the development of new tools, techniques, and applications. Finally, I close the chapter by outlining the financial and professional applications of videogame hacking, ranging from meagre transactions within fan communities to professional hacking operations.

In my conclusion, I revisit my personal experiences in videogame hacking and summarize some of the themes, limitations, and future considerations of my research. I begin with a short discussion with fellow *EarthBound* hacker (and current game designer) Max Ponoroff, who recounts his history with the practice while providing another perspective on the hacking definitions I laid out in Chapter 1. I then outline some of the core themes of my research, identifying key connections and dissonances present in my work, before summarizing some of the recurring motivations of my participants. I next consider the limitations of my thesis, including those caused by a relatively small pool of participants, as well as the potential

historical gaps in the knowledge communities that I documented. Finally, I close my thesis by posing one last question to myself — “where can this research go next?” — and contemplate how this type of study could be expanded upon in future academic contexts.

Chapter 1: What Is Videogame Hacking?

The first chapter of my thesis interrogates two fundamental questions: “what is videogame hacking?” and “how does one go about studying it?” My goal through this writing was not to come to some sort of exhaustive and unambiguous answer to either of these queries, but rather to recount how I grappled with them throughout my research. I begin the chapter with a short reflection on the 1995 movie *Hackers*. This is not because the film is a particularly realistic account of computer hacking culture, but rather an acknowledgement of its role in popularizing hacker tropes and stereotypes that still persist across film, television, and videogames. After dissecting some of the non-fictional elements of the film — such as excerpts from Loyd Blankenship’s *The Conscience of the Hacker* — I shift my attention toward a pair of works that meticulously document various aspects of hacker culture: Stephen Levy’s *Hackers: Heroes of the Computer Revolution* and Gabriella Coleman’s *Coding Freedom: The Ethics and Aesthetics of Hacking*. Using these documents as historical and theoretical grounding, I then contemplate how videogame and modding practices could potentially fit into broader conversations of computer hacking. Acknowledging the impossibilities of positioning videogame hacking neatly into the canon of hacker culture, I shift my focus toward creating a tentative definition of the practice and a tangible set of research methods. Referring to William Ruffin Bailey’s *Hacks, Mods, Easter Eggs, and Fossils*, and acknowledging some of the logistical issues facing my study, I craft a working definition of videogame hacking designed to guide me toward individual participants and projects. To close the chapter, I review the methods used to undertake my research: interviews, qualitative game analysis, and reflective writing.

A Short Excerpt From *Hackers* (1995)

EXT. OUTSIDE JOEY'S PLACE.

Joey's apartment building is an L-shaped skyscraper about 30 storeys high, unimpressive by New York City standards. Two Secret Service agents are staking Joey out in a car outside.

SECRET SERVICE AGENT BOB
Unit 3 outside suspect Joey Pardella's
apartment. Nothing to report. Suspect still
grounded... by his mother.

His radio crackles.

AGENT BOB
Listen to this bullshit.
(he reads)
"This is our world now. The world of the
electron and the switch, the beauty of the
baud. We exist without nationality, skin
color, or religious bias. You wage wars,
murder, cheat, lie to us and try to make us
believe it's for our own good, yet we're the
criminals. Yes, I am a criminal. My crime is
that of curiosity. I am a hacker and this is
my manifesto." Huh, right, manifesto? "You
may stop me, but you can't stop us all."

AGENT RAY
Now that's cool.

AGENT BOB
Cool?

AGENT RAY
Yeah, cool.

AGENT BOB
You think it's cool?

AGENT RAY
(not caring for where Bob is going
with this)
It's cool!

AGENT BOB
It's not cool. It's commie bullshit!

Computer Hacker Tropes and Stereotypes

While attempting to trace a line through the popular, academic, and historical descriptions of “the hacker,” it would be easy for me to dismiss the portrayals found within the 1995 film *Hackers* as outdated, comical, and completely irrelevant to academic research. Even at the time of its release, the significantly less computer saturated world of the mid-nineties, the film faced a great deal of criticism for its haphazard interpretation of hacker subcultures and practice. Roger Ebert blithely described *Hackers* as “smart and entertaining... as long as you don't take the computer stuff very seriously. I didn't. I took it approximately as seriously as the archeology in *Indiana Jones*” (Ebert) and *Entertainment Weekly*'s Owen Gleiberman lambasted the movie for buying into the “computer-kid-as-elite-rebel mystique currently being peddled by magazines like *Wired*” (Gleiberman). Despite playing it a bit fast-and-loose with the realities of the technological landscape, its continued popularity as a cult classic makes it a useful starting point for unpacking some of the presuppositions associated with computer hacking.

Simultaneously depicting the hacker as a rebel, computer geek, social outcast, anarchist, criminal, and naive teenager out to test the limits of their world, *Hackers* helped crystallize a series of tropes which have persisted throughout the ensuing decades in film (*Swordfish*, *Live Free or Die Hard*), television (*CSI: Cyber*, *Mr Robot*), and videogames (*Hackmud*, *Watch Dogs*). In the context of my own research, which focuses more narrowly on the subcultures and practice of videogame hackers, I have found it useful to seek out the truths embedded in these depictions. By sifting through the broad stereotypes presented in popular media, I can simultaneously steer myself away from the perception of a cliché-riddled homogenous hacker culture, while working my way toward more nuanced views grounded by empirical and historical research.

So what truths can be extracted from *Hackers*? In the scene transcribed above — a short vignette that unfolds during a stake-out of teenage computer hacker Joey Pardella’s apartment — two secret service agents debate the contents of *The Conscience of a Hacker*, a real manifesto penned by the computer hacker Loyd Blankenship (who worked under the pseudonym of “The Mentor”). Oftentimes referred to as the *Hacker Manifesto*, the short essay was originally published in the underground hacker ezine *Phrack* in 1986. Ironically, considering the *Manifesto*’s prominence in the film, Blankenship was frustrated with popular depictions of hackers and wanted to distill “the essence of what we were doing and why we were doing it.” The conversation between the agents, despite its comical nature, is one of many recurring representations of hacking as an antithesis to established authority. Bob, the older and more cynical of the two, regards the document with open disgust. He reads excerpts from it in a mocking tone, rolling his eyes and dismissing its message as “commie bullshit.” Ray, the younger and more sympathetic agent, plays the role of the slightly out-of-touch (but intrigued) adult and reluctantly admits that he finds the *Manifesto* to be “cool.” Through the agents’ conversation, as well as their surveillance methods, *Hackers* evokes several classic conflicts commonly associated with the practice of computer hacking: young versus old, freedom versus authority, privacy versus surveillance, and change versus the status quo. Bearing these contentions in mind, I found the choice of excerpt to be particularly noteworthy:

“You wage wars, murder, cheat, lie to us and try to make us believe it's for our own good, yet we're the criminals. Yes, I am a criminal. My crime is that of curiosity. I am a hacker and this is my manifesto. You may stop me, but you can't stop us all.” (Blankenship)

The quote (which, in actuality, is cobbled together from two later sections of the *Manifesto*) is indicative of Blankenship’s outlook at the time of the publication, having authored the document

shortly after his arrest in 1986 (Marsh) for being “in a computer [he] shouldn’t have been in” (K2K2 2002). While ostensibly admitting his own guilt, Blankenship’s writing is unapologetic and incisive. He frames the actions of hackers as both a harmless curiosity and a potent antithesis to sins committed by an ambiguously defined “you,” presumably referring to large corporations and government structures. While Blankenship is certainly not the first voice to distill the motivations of computer hackers, nor is he the definitive one, he does lay out some principles that appear in past and future academic and historical accounts. He reflects on how computers, modems, and other technologies set him on a path of discovery — “a door opened to a world” (Blankenship) that allowed him to connect with like-minded individuals from around the globe. He justifies the action of hacking as necessary to oppose corruption and greed — “we make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons” (Blankenship). And he acknowledges that this opposition will generally be judged to be illicit — “We explore... and you call us criminals. We seek after knowledge... and you call us criminals” (Blankenship). Although his evasiveness regarding the details of his own hacking practice and his failure to acknowledge his own position of privilege — possessing ready access to both a university computer lab and a personal computer in the late 1970s and early 1980s (Capello) — in a purportedly meritocratic practice does detract some credence from *The Conscience of the Hacker*, the longevity of the document is telling of the sway it holds in some hacker circles, and how many of its ideals still circulate in *Hackers* and other popular depictions of the practice.

Levy, Coleman, and the Principles of Hacking

Blankenship is quick to pontificate on many of the ideals associated with hacker culture, but he was certainly not the first to inscribe them. Steven Levy, journalist and writer for *Wired*

magazine, is often considered a pioneer in this regard, famously documented the pillars of “Hacker Ethic” in *Hackers: Heroes of the Computer Revolution* in 1984. Much like Blankenship, Levy was unsatisfied with many of the broad stereotypes of hacker culture, and attempted to paint a fuller picture by tracing its history from its beginnings within the MIT computer labs of the 1950s to the software development scene of the 1980s. Noting that the word “hack,” as conceived by MIT students, was used to describe “a project undertaken or a product built not solely to fulfill some constructive goal, but with some wild pleasure taken in mere involvement” (Levy, 10), Levy centered the idea of hacking around an extreme proficiency with computers while also emphasizing the importance of certain political ideals and working habits. By speaking with dozens of participants involved with hacking culture, Levy fleshed out the unspoken precepts from the early years of the computer revolution, eventually consolidating what he believed to be the six core tenets of hacker ethic:

“Access to computers — and anything that might teach you something about the way the world works — should be unlimited and total. Always yield to the Hands-On Imperative!” (Levy 28). Important lessons can be learned about systems by disassembling and scrutinizing them, and any barrier that stands in the way of this knowledge is viewed with contempt.

“All information should be free” (Levy 28). A free exchange and flow of information, especially in regards to computer programs, is necessary to enable creativity and collaboration.

“Mistrust authority and promote decentralization” (Levy 29). The only way to enable this free exchange of information is to have systems without boundaries, and any forces that attempt to limit this access should be mistrusted.

“Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position” (Levy 31). No credential, qualification, or superficial characteristic is more important than a person’s practical computer skills.

“You can create art and beauty on a computer” (Levy 31). The code of a computer holds beauty unto itself, and there is an art to working within the constraints of systems.

“Computers can change your life for the better” (Levy 34). Since computers had enriched the lives of hackers, it is logical to assume that the rest of the world could also benefit from hacker ethic

Written two years before Blankenship’s *The Conscience of the Hacker*, which focuses more on the emergence and online hackers in the early Internet age, Levy speaks more broadly of the mainframe, hardware, and game hackers that flourished in the middle of the twentieth century. Despite this difference in temporality, there are many commonalities between these two documents: an emphasis on the free exchange of information, an opposition to authority and bureaucracy, and a belief that computers can offer freedom and power to a portion of the population who previously had no means to acquire it. I found it tempting to simply take Levy’s six tenets and cross-reference them with Blankenship’s manifesto, to frame my research as just another facet of computer hacking practice. However, this approach would have been notably incomplete. In addition to overlooking recent developments in hacking culture, and side-stepping a direct connection to videogame hacking, these six tenets are somewhat presumptuous about the homogeneity of hacking culture.

Gabriella Coleman elaborates on two of the aforementioned points (I will touch on the videogame connection later in this chapter) in her book *Coding Freedom: The Ethics and Aesthetics of Hacking*. Currently the Wolfe Chair in Scientific and Technological Literacy in the

Department of Art History and Communication Studies at McGill University, Coleman's research begins with the simple question — “what is a computer hacker?” — but encompasses various aspects of hacker production, politics, and identity. Profiling the so-called “modern” hacker, Coleman explores issues surrounding copyright, free speech, and intellectual property while documenting the Free and Open Source Software (F/OSS) movement throughout the nineties and the turn of the twenty-first century. Importantly, she interrogates the notion of a singular hacker ethic or identity. Referring to Levy's six tenets, she laments that “...almost *all* academic and journalistic work on hackers commonly whitewashes these differences, and defines all hackers as sharing a singular ‘hacker ethic’” (Coleman 17). While acknowledging Levy's work as foundational, Coleman expresses that there is great diversity to be found within the idea of hacker ethic which can be exposed through ethnographic inquiry: “although hacker ethical principles may have a common core... similar to any cultural sphere, we can easily identify great variance, ambiguity, and even serious points of contention” (Coleman 18). Further complicating the idea of hacker ethic, Coleman notes that many modern hacker ideals are generated reflexively, creating a sort of feedback loop between existing documentation (and perhaps even pop culture portrayals) of the hacker ethic and a hacker's formation of their own identity. Whereas Levy describes that “the precepts of this revolutionary Hacker Ethic were not so much debated and discussed as silently agreed upon. No manifestos were issued. No missionaries tried to gather converts” (Levy 27), Coleman notes that, in the decades following the publication of *Hackers: Heroes of the Computer Revolution*, debate, discussion, and written manifestos all became commonplace (18). Once requiring access to isolated and privileged communities, such as the MIT computer labs, hackers began to form their identities by joining online communities, reading books about the history of the practice, and attending various

conventions and conferences. Even a cursory Google search for a “hacker manifesto” — which Levy purports did not exist at the time of his writing — brings forth a bevy of documents that highlight various aspects of hacker culture. In addition to Blankenship’s *The Conscience of a Hacker*, one might find inspiration from Richard Stallman’s *GNU Manifesto*, which trumpets the importance of free and open source software, or Mackenzie Wark’s *A Hacker Manifesto*, a critique of the commodification of information in the digital age. Although many key themes do appear across these documents, individual hackers seem free to form their identities by embracing or rejecting any number of these values. The result is a heterogeneous collection of hacking subcultures.

Bailey and Finding a Working Definition for Videogame Hacking

When I first proposed this research project, I imagined that videogame hacking would be easily located in the broader history of computer hacking. However, my interaction with Levy’s historical writing, Blankenship’s manifesto, and Coleman’s ethnographic research dispelled any notion that I could (or should) create a static definition of a videogame hacker. Although there are certain themes and tenets that resurface throughout the history of hacking, the identity of any hacking subculture is contingent on specific configurations of technologies, policies, and values. Levy’s hackers embraced computer technologies as they emerged in both institutions and homes, valuing the free exchange of information and idealizing a sort of self-actualization through technology. Blankenship’s manifesto valorizes the early Internet and how it enabled hackers to push back against ostensibly greedy and corrupt organizations. Coleman turned her attention toward online collaboration, documenting the F/OSS movement and how hacker ideals were formalized through ongoing software projects. These accounts make it clear that there is no single type of hacker and, as a result, videogaming hacking should not be framed as an easily

defined subset of hacking culture. Despite this acknowledgement, however, I did require some parameters in order to identify and recruit participants for my research. Creating a definition for videogame hacking thus became an important first step, despite my intent to interrogate and fragment that very definition throughout my research.

One of the challenges I faced while crafting this preliminary interpretation of videogame hacking was that much of the existing game studies literature on the practice downplayed its connection to computer hacking history or used the term “hacking” interchangeably with cheating and modding. Despite my acknowledgement that videogame hacking may not fit perfectly in the history of hacking, I still felt it was important to make a connection with it before moving ahead with my research. One article that I came across that specifically compared videogame hacking to hacker ideals was *Hacks, Mods, Easter Eggs, and Fossils*, penned by William Ruffin Bailey, in which he states that a hack occurs “when an unsanctioned third-party or independent programmer changes a program’s code to function in non-standard but not necessarily unintended ways” (74). Bailey specifically highlights the practice of hacking Atari 2600 ROM images and how programmers are able to modify code in-place to tweak various aspects of a game, such as the amount of damage a player takes or their avatar’s ability to interact with game terrain and obstacles. Bringing in the example of Robert Kudla, who altered a ROM image of *Space Invaders* for the Atari 2600 in attempt to create a “truer to the arcade” (Atari 2600 Hacks) version titled *Space Invaders Arcade*, Bailey expresses three reasons why Kudla’s work fits under his definition of videogame hacking as an unsanctioned activity. First, Kudla utilized a ROM image from a cartridge which, by intent, was never meant to be copied or distributed by a third party. Second, *Space Invaders* is still under copyright, ostensibly forbidding alteration and modification. Finally, the original programmers did not provide

documentation, instructions, or tools to facilitate this sort of game alteration (Bailey 78). Under these parameters, Bailey seems to consider the role of videogame hacker as that of an outsider (a third-party or independent programmer), who makes unauthorized changes to a videogame after its commercial release.

Bailey also attempts to draw a line between videogame hacking and other types of game alteration — such as modding and skinning — which he sees as further separated from the game engine and oftentimes “anticipated and encouraged by the games’ designers” (Bailey 78). One of the keys to his separation of these two concepts lies in a seemingly straightforward portion of his definition: “[changing] a program’s code” (Bailey 74). Pushing back against the idea of a videogame as a singular system, Bailey attempts to separate engine from content and, by extension, hacking from modification. Noting that game engines “enforce the rules of their virtual worlds, but they are not worlds themselves” (Bailey 75), he emphasizes how a single game engine can be reusable and often supports various types of content. For example, in addition to the first-person shooter *Unreal*, the Unreal game engine has been used to create a deluge of stylistically disparate titles such as *Duke Nukem Forever*, *The Wheel of Time*, *TNN Outdoor Pro Hunter*, *Deus Ex*, and *Nerf Arena Blast* (Herz). However, Bailey admits that this distinction is difficult to maintain in older console games, as they often contain “engines that were not designed for reuse and seem inextricably wedded to their content” (Bailey 75). As evident in his example of *Space Invaders* for the Atari 2600, a ROM image is essentially a single file that requires careful disassembly and dissection to make even the simplest changes, aesthetic or otherwise. Recognizing this point, Bailey points out that hacking and modding should not be defined exclusively by *what* is being changed but rather *the process* behind the changes. He notes that if a user can simply drop content — such as a new map or player model — into a game

using a standardized memory address or a specified location in a file structure, then the practice should be considered modding. If a user has to find “a memory address through subversive code disassembly” (Bailey 78) in order to enact a change, then the practice is hacking. Thus, Bailey’s assertion that hacking involves “[changing] a program’s code” specifies that the code is not designed to be swapped out easily, and requires some sort of discovery process by the hacker.



Fig 1. Screenshot from: *Space Invaders*.
Atari 2600, 1980.



Fig 2. Screenshot from: *Space Invaders Arcade*.
atariage.com/hack_page.php?SystemID=2600&SoftwareHackID=6. Accessed 15 May 2019.

Although Gabriella Coleman does not delve deeply into videogame hacking practice in *Coding Freedom*, the process of acquiring, dissecting, and modifying videogames has many parallels to her review of hacker craft and craftiness. In addition to cultivating technical mastery (i.e. the craft), Coleman indicates that hackers find a certain pleasure in discovering and then outwitting software and hardware constraints (i.e. craftiness). To a hacker, “constraints are constant and are of nearly infinite variety” (Coleman 98), and can include hardware limitations, bureaucratic barriers, technical specifications, and legal obstacles such as copyright and intellectual property law. While these factors certainly complicate the work of hackers, Coleman notes that working with and against the limitations of systems is an intrinsic part of the hacking practice: “the very nature of hacking — turning a system against itself — is the process of using existing code, comments, and technology for more than what the original authors intended” (98).

Returning to Bailey's definition, the implication could be that if the process is too straightforward or simple then it is simply not crafty enough to be considered hacking. In his analysis of the *Space Invaders Arcade* hack, Bailey argues that Robert Kudla outwits constraint in many ways: sourcing a ROM image from a cartridge based videogame, altering the game without documentation or guidance, and eventually making his hack available online despite potential copyright complications (Bailey 77). The result is both an impressive technical achievement and a playful one. Kudla, who was never granted permission to alter *Space Invaders*, had to expend a great deal of energy overcoming technical barriers inherent to the project. Although Bailey does not provide a personal account from Kudla describing his motivations, it is reasonable to presume that he found some joy in both pushing the Atari 2600 to his limits and one-upping the work of professional videogame designers.

Akin to Levy's six principles, Bailey interpretation of videogame hacking is both neatly contained and incomplete. He fails to acknowledge that developer intents are not always transparent, making it difficult to determine whether or not a user's changes are unintended, unsanctioned, or even unwelcome. His tendency to silo hacking and modding into separate activities is also problematic, particularly his desire to separate game engine alteration from the manipulation of assets such as maps, graphics, and music. In both old and new games — and even in his example of *Space Invaders* for the Atari 2600 — the divide between these elements is fluid and can be difficult to discern. Despite these shortcomings, however, I leaned quite heavily on Bailey's definition throughout the early stages of my research. The definition served as a malleable framework as I began assembling my research methods and searching for projects and hackers to engage with.

Narrowing the Field

Much of the reason I embraced Bailey's definition of videogame hacking was because it was neither complete nor authoritative and I felt a certain freedom to interrogate it (perhaps, hack it?) throughout my research, reinterpreting it as I completed my literature review and considered potential research subjects. Part of this interrogation meant acknowledging that the subjects of my research — videogame hacks, hackers, and online communities — would essentially be non-fixed entities. Although I still intended to use Bailey's codification of videogame hacking (i.e. unsanctioned projects that edited a game's code in unexpected ways) as a sort of makeshift search parameters, a pair of complications came to light as I began my research: Bailey's definition was entirely too broad and encompassed literally thousands of potential projects and; hackers were somewhat elusive, hiding behind pseudonyms or within closed online communities. Out of necessity, I adopted three additional criteria to help me narrow the field and guide me toward potential participants. First, I decided to reach out to those who self-identified as hackers rather than modders. Although Bailey's definition provided me with guidelines to make this distinction on my own, I felt it was important to speak with participants who identified with the practice by name and could elaborate on what it meant to them. Secondly, I was interested in utilizing the moniker of "classic" games as a sort of divining rod to guide me toward potential videogame hacking projects. Although some scholars are quick to deride the prevalence of the term "classic" because of the "vagueness, nostalgia, or hyperbole with which it is frequently associated" (Swalwell 45), I felt the label still held some merit. Videogames are often referred to as classic not just because they are presumed to be cultural touchstones, but also because they have been deemed worthy of revisiting. Titles that have been branded as classic seem to hold a sustained popularity, making it easier for me to find information regarding the

original release and, by extension, the hacks that have been derived from it. Finally, and perhaps most pragmatically, I decided to only pursue videogame hacks that had at least one participant with freely available contact information, taking the form of either a real name or an Internet handle, and some documentation of their work. Although taking the time to unearth “lost hacking projects” does sound like an appealing endeavour, I did not think it would be feasible within the scope of a master’s thesis to locate hackers who had intentionally hidden their projects or had absconded from the online world entirely. As an extension of the above points on accessibility, I also came to the realization that my research was very much limited by language. Presumably, there are a large number of non-English language videogame hacks and subcultures that are completely indiscernible to both myself and my participants.

Although not strictly one of my search parameters, I also found myself gravitating toward videogame hacks that had attained some sort of notability among the myriad of projects made available on the Internet. Notability is, admittedly, a slippery term, but includes projects that have been made widely available online and had cultivated some sort of audience (or perhaps even notoriety). This notability commonly took the form of an active and visible presence on social media, a central archive or depository of information, or simply a forum or website where hackers gathered. This aspect is perhaps best demonstrated by the *Link to the Past Randomizer* hacking community — whose members are featured heavily throughout my research — who run massive online tournaments, maintain a strong presence on online video streaming services such as Twitch and Discord, and make regular appearances at speedrunning conventions such as Awesome Games Done Quick. Media coverage also played a role in directing me toward hacking projects, as the archives of online publications such as Kotaku, Polygon, and Gamasutra are valuable resources for discovering discontinued projects and identifying their associated

members. By sifting through old news articles and short features, I was provided a means to identify canceled projects, as well as their members, such as the popular *Super Smash Bros Brawl* hack *Project M*. Finally, since videogame hacking is inextricably intertwined with copyright law, it made sense to seek out works that have been affected by copyright strikes, cease-and-desist orders, or other legal action at some point during their history. *Chrono Trigger: Crimson Echoes*, *SM64 Online*, and *Pokémon Prism* all fall under this category, being rare examples of direct developer intervention upon a videogame hacking community. Although these litigious examples should be considered somewhat exceptional, their interactions with the law enable an examination of the unsanctioned and potentially illicit aspects of videogame hacking. This focus on notability, alongside Bailey's definition and my three additional criteria (self-identification, classic games, and accessibility), allowed me to shrink my pool of potential participants and scale down my research to something that was both feasible and focused.

Assembling a Methodological Framework

However confident I may have been with my growing collection of definitions and typologies, I still only had only a vague idea of which hackers, videogame hacks, and communities would become my research subjects. Despite targeting videogame hackers who had made their contact information accessible — and having a handful of potential targets in my sights — it was impossible to predict which participants would respond to my interview requests and, by extension, which videogame hacking communities I would be engaging with. Therefore, I felt it was important to develop a flexible methodological framework that would allow me to constantly re-evaluate the breadth and depth of my research. Would I focus on a smaller number of interviews, engaging with multiple hackers from the same community to gain a more in-depth understanding of their efforts? Or would it become necessary to scale back my interviews, and

instead direct my efforts toward analyzing the cultural outputs of these subcultures - the innumerable videogame hacks I could access online without going through community gatekeepers? I felt it was impossible to truly know which approach would be best suited for my research until I was in the thick of things. I found Clifford Geertz's reflections on ethnography to be valuable in solidifying my approach, and even a bit comforting in acknowledging the potential productivity of fluidity. Geertz challenges the perceived linearity of research, academic or otherwise, by taking note of its fragmentary, experimental, and almost cyclical nature. He notes that "studies do build on other studies, not in the sense that they take up where the others leave off, but in the sense that, better informed and better conceptualized, they plunge more deeply into the same things" (Geertz 25). In the early phases of my research, I had imagined that videogame hacking would fit cleanly into a broader history of hacking and that my research would essentially consist of a series of neatly contained case studies. Although developing a historical grounding for my research was certainly important, I began to realize that it would be impossible to simply trace a line from Levy's mainframe and hardware hackers, through Coleman's F/OSS hackers and Bailey's videogame hackers, and conveniently resolving with my own research. Therefore, the goal for my thesis was not to create something that fit perfectly into the canon of hacker research and history, nor to have a well manicured selection of participants, but to instead slowly develop research that "less stands on the shoulders [of previous studies] than, challenged and challenging, runs by their side" (Geertz 25). Acknowledging that my research approach would need to be flexible and reflexive, I decided to adopt a three-pronged methodology that centered around interviews, qualitative game analysis, and iterative writing.

Interviews

The early stages of my research were guided by my working definition of videogame hacking and primarily involved securing and conducting interviews with members from various online videogame hacking subcultures. Completed over the course of four months, I spoke to eight individuals about their videogame hacking projects, which I have outlined in **Appendix I: Participant Profiles**. The purpose of these interviews was twofold: first, I intended to learn about the values, processes, and objectives behind their hacking work and their affiliated communities; second, I wished to gain access to their hacking projects and related ephemera. I had originally expected this ephemera to consist almost entirely of videogame hacks, but my collection of materials turned out to be incredibly varied. Participants were quick to provide me with work-in-progress, documentation videos, images and diagrams, editors and hacking tools, patching systems, game logs, and even legal documents such as cease-and-desist orders. To better analyse these interviews, and organize these additional assets, I decided to adopt grounded theory analysis. The method provided by grounded theory seemed ideal for my research due its emphasis on flexible strategies, its acknowledgement that research is both cyclical and emergent, and the tangible guidelines it provides for both conducting and coding interviews. Grounded theory describes interviewing as a “flexible, emergent technique; ideas and issues emerge during the interview, and the interviewer can then immediately pursue these leads” (Charmaz 677). In the context of my research, these leads were not just topics or ideas, but also videogame hacks and other ephemera provided by my participants.

I conducted my interviews almost exclusively through Discord — an online text, image, video, and audio communication service — using video or audio chat, as determined by the preference each individual participant. On the onset of my research, I had not considered using

Discord as a communication tool but, as most of the videogame hacking subcultures I engaged with used the platform to mobilize their activities it was by far the easiest way to get in touch with my participants. As suggested by grounded theory, my interview questions were open-ended and I encouraged participants to talk about their personal history with videogame hacking by recounting their own experiences through linear narrative (Charmaz 680). During these discussions, I found it vitally important to be aware of what topics my participants may not be comfortable touching on — especially in regard to potential legal complications associated with their work — and to use “in-depth interviewing to explore, not to interrogate” (Charmaz 680). This meant allowing participants to opt-out of certain lines of questioning and even completely redact answers that contained details which they felt were too sensitive to share. Although this may seem as if it would result in less forthcoming participants, I found that it actually inspired the opposite response. This approach created a comfort level during interviews that encouraged participants to be more open and allowed them to explore tangents without the fear of saying something they would regret. This openness extended beyond the confines of the formal interview, as one of the unforeseen benefits of utilizing Discord was the sustained engagement it enabled through text chat. Following interviews, I often received messages, files, and links from participants who wished to provide additional context to topics that had been discussed. After an interview was completed, I transcribed the recorded audio and coded the text using a two-step grounded theory method (Charmaz 686). The first step consisted of reviewing the key points of an interview, briefly summarizing what was stated by my participant, and then inscribing the resulting synopsis alongside the original transcription. The second step involved a more selective coding process in which I identified broader themes in an interview, extracted quotes, and sorted these excerpts in a secondary document. The intent behind this coding was to group my findings

thematically, identifying similarities and points of contention across various interviews, before considering how these themes could eventually be sorted into chapters.

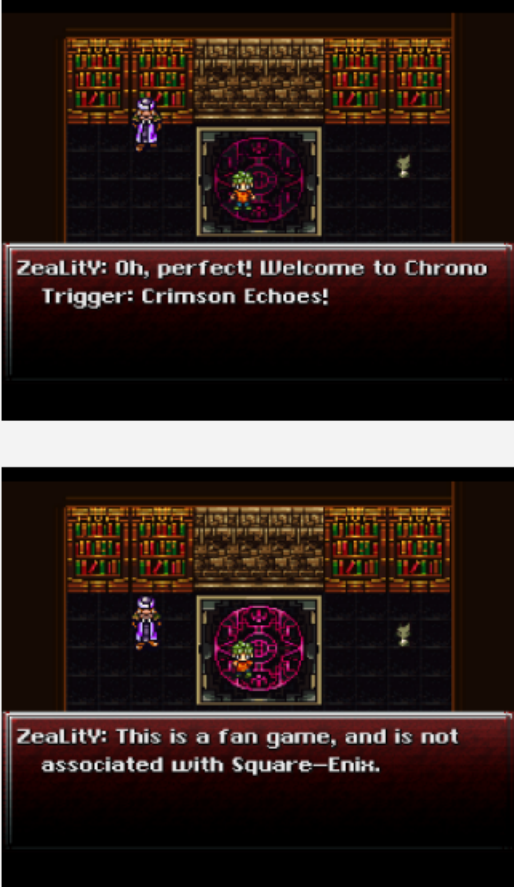
Videogame Hack Analysis

The qualitative analysis of videogame hacks also played an important role in my research, as it allowed me to better prepare questions for my interviews and gain familiarity with the projects that had been completed by my participants. My analysis was guided by the principles laid out in Mia Consalvo and Nathan Dutton's article *Game Analysis: Developing a Methodological Toolkit for the Qualitative Study of Games*. Outlining four key research methods for game studies (object inventories, interface studies, interaction maps, and gameplay logs), Consalvo and Dutton present a framework for scrutinizing games as "cultural artefacts that can reveal social, political, and other insights about contemporary life." For the purposes of my research, I selected two of these methods: interface studies and gameplay logs. I found interface studies to be useful, not for analyzing videogame hacks themselves, but rather for examining the various patching applications that have been developed to alter videogame ROM images. For example, the *Link to the Past Randomizer* uses a web-based patching application that provides users with dozens of options for customizing a *The Legend of Zelda: A Link to the Past* ROM image. Examining the patching application's interface allowed me to determine how much freedom players were granted to customize their experience, what aspects of the videogame hack were deemed important by the development team, and even how legal responsibilities (such as providing a copy of a *Link to the Past* ROM image) were allocated.

Summary

Chrono Trigger: Crimson Echoes is a fangame developed by the international team Kajar Laboratories as a ROM hack of Square's role-playing video game Chrono Trigger for the Super Nintendo Entertainment System. It was conceived as an unofficial installment in the Chrono series, set between the events of Chrono Trigger and its sequel Chrono Cross.

Gameplay Log



ZeaLitV: Oh, perfect! Welcome to Chrono Trigger: Crimson Echoes!

ZeaLitV: This is a fan game, and is not associated with Square-Enix.

When you start the game for the first time, you are immediately greeted by avatars created by the hacks' developers.

“This is a fan game, and is not associated with Square-Enix. In fact, the characters and world you see belong to Square Enix! We just gave them a new story as an interquel to Chrono Trigger and Chrono Cross. Crimson Echoes was created by fans of the game in their spare time. It's not canon, nor should it be.”

Fig 3. Excerpt from game logs for *Sub-Versions*.

Consalvo and Dutton note that gameplay logs allow the researcher to focus on “emergent behaviour or situations, the larger game world or system, and intertextuality as it is constituted with the game,” and I used gameplay logs as a way to document how hackers modified these game elements in various ways. In comparison to interface studies, my approach towards

gameplay logs was markedly more experimental. One of the complications facing this analysis was the fact I was essentially analyzing two games simultaneously: the original videogame, as made by the developer, and the hack that had been constructed within it. Thus, instead of trying to chronicle each of my chosen game hacks exhaustively — which I felt was beyond the scope of my research — I decided to complete targeted playthroughs in the hopes of documenting hacker intervention within a given title. Practically, this took the form of a text document that contained gameplay observations, transcriptions of game text, and screenshots gathered using the video/image capture software FRAPS. The exact length of these playthroughs varied wildly, but with the exception of a few small-scale hacks, my analysis rarely involved finishing or fully completing all of a title's objectives. To help fill in some of the gaps in my gameplay logs, I cross-referenced my findings with hacker-created patch notes. Mirroring the patch notes commonly released by commercial videogame developers, these documents provided comprehensive accounts of the changes enacted upon a videogame, with a focus on code improvements and newly crafted features.

Reflective Writing

The final method I adopted for my research was reflective writing, which I used to formulate tentative propositions and identify trends within my work. My approach was inspired by Laurel Richardson's *Writing as a Method of Inquiry* and *Writing Strategies: Reaching Diverse Audiences*, in which she poses two notions that she believes are vital to qualitative writers. Richardson encourages sociological researchers to both "understand ourselves reflexively as persons writing from particular positions at specific times" and to free ourselves from "trying to write a single text in which everything is said to everyone" (Richardson and St

Pierre 821). Regarding research data as somewhat malleable, she encourages researchers to inscribe diverse interpretations and presentations of their knowledge. In the context of my research, this writing took the form of a WordPress blog that was updated once or twice a month as I conducted interviews and completed my qualitative game analysis. My blog posts included reflections on my personal experiences with hacking, documentation of videogame hacks and their related tools, typologies designed to interrogate my literature review, complications that had arisen during research, and scraps of information that simply did not seem to fit anywhere else. Crafting this diverse collection of content allowed me to rethink my research as it was unfolding, leading toward an understanding of videogame hacking that was “deepened, complex, and thoroughly partial” (Richardson and St Pierre 823). This style of writing allowed me to transform tacit knowledge — garnered from my personal history with videogame hacking and my interviews — into rough ideas and propositions. It also served as a mechanism to return to grounded theory, which encourages researchers to write short memos to help them fracture and then reassemble their data (Charmaz 690). Each post brought forth new hypotheses, explications, and documentation, allowing me to bring additional insights to my interviews and my research on the whole.

Chapter 2: Technical & Legal Barriers

This chapter explores how videogame hackers, particularly ROM hackers, engage with the technical and legal barriers that complicate their work. I begin with a summary of the cease and desist order that was leveled against the *Chrono Trigger: Crimson Echoes* videogame hack, as an example of direct developer intervention upon videogame hacking practice. I then craft a theoretical framework for understanding the tension between media companies and videogame hackers, rooted primarily in the viewpoints of Michel de Certeau and Henry Jenkins. I consider how videogame developers and publishers establish strategies — often leveraging existing legal policies and their own vast resources — to protect their copyrighted works, and how videogame hackers tactically seek out cracks in these strategies continue their practice and distribute their cultural outputs. Extending de Certeau's theories to Jenkin's work on convergence culture, I discuss how videogame developers establish collaborationist and prohibitionist models for their titles that dictate what types of fan works are authorized or unauthorized. I then analyze three distinct tactics adopted by my participants to push back against prohibitionist models: patch files and decentralization; anonymity, dispersal, and persistence; and online patching systems. I conclude by reflecting upon *Lewis Galoob Toys, Inc. v. Nintendo of America, Inc.*, a lawsuit cited by some of my participants as a justification for the legality of their activities.

Chrono Trigger: Crimson Echoes

On May 8th 2009, two members of the *Chrono Compendium* fan community — known on the website's messageboards as ZeaLity and Agent 12 — discovered a distressing message in their email inboxes. The legal department from Square Enix, one of the world's largest videogame developers and publishers, had sent them a cease and desist order demanding that they halt their work on *Chrono Trigger: Crimson Echoes*. An in-progress ROM hack of the

popular 1995 Super NES title *Chrono Trigger*, *Crimson Echoes* had been developed for roughly half a decade by a small team of *Compendium* members that referred to themselves as Kajar Laboratories. Led by ZeaLity, Agent 12, and fellow community member Chrono'99, the team's goal was to construct an entirely new entry in the *Chrono* series built within the framework of the original release. Advertising *Crimson Echoes* as an unofficial interquel (taking place after *Chrono Trigger* but before its official Playstation sequel *Chrono Cross*), the hack boasted 35 hours of new gameplay alongside a bevy of graphics, maps, and music that were not present in the original title. Set to debut on May 31st of the same year, mere weeks after the cease and desist order arrived, the hack's release plans were promptly halted. The Square Enix legal department minced no words in their cease and desist order, claiming that by altering *Chrono Trigger* Kajar Laboratories had engaged in an "act of copyright infringement" that was "deliberate and willful." Prominently citing the Digital Millennium Copyright Act (DMCA), they threatened that "statutory damages for willful copyright infringement are up to \$150,000 per work" and that the team must "immediately remove, take down, delete and destroy all work product on CT:CE" including related projects, such as Kajar Laboratories' previously completed ROM hack *Prophet's Guile*.

SQUARE ENIX®

May 8, 2009

Personal information removed.

Re: Cease and Desist: Chrono Compendium, Crimson Echoes

Dear Messrs. [REDACTED]

It has come to our attention that you, along with other members of Kajar Laboratories, have been developing a ROM hack game called *Chrono Trigger: Crimson Echoes* ("CT:CE") based on Square Enix's copyrighted intellectual property. We understand that you claim a copyright to CT:CE and intend to distribute it online imminently.

Your act of copyright infringement is deliberate and willful, as demonstrated by the "readme" file to the CT:CE demo, which states:

ROM altering and modification is illegal, and the demo has been made without the consent of Square Enix... Should Square Enix perceive the project as a threat... Kajar Laboratories will immediately cease operation on the project and comply with Square Enix's orders.

The statutory damages for willful copyright infringement are up to \$150,000 per work. (See 17 U.S.C. § 504(c)(2).)

We hereby request and demand that you immediately remove, take down, delete and destroy all work product on CT:CE, as well as all other Square Enix-related ROM hacks currently on your sites (including, but not limited to, *Prophet's Guile*).

We understand that you intend to instruct others how to circumvent our copy protection using Temporal Flux in violation of the Digital Millennium Copyright Act, 17 U.S.C. § 1201. We demand that you cease and desist any and all efforts to rip, hack or circumvent our copyright protection measures or to teach others to do so.

If any of these unlawful products are ever distributed, or if you fail to remove all infringing material immediately, then we will have no choice but to turn this matter over to our litigation counsel and appropriate authorities.

Please contact us by May 13th to confirm that you have complied with all of our demands.

Sincerely,

SQUARE ENIX LEGAL DEPARTMENT

SQUARE ENIX, INC. 999 N. Sepulveda Blvd. 3rd Floor, El Segundo CA 90245 t: 310.846.0400 f: 310.321.6095

Fig 1. *Cease and Desist Order for Chrono Trigger: Crimson Echoes* from: "Cease & Desist Letter." *Chrono Compendium*, 10 May 2009, chronocompendium.com/Forums/index.php?topic=7396.0.

Interestingly, the cease and desist order also encompassed Temporal Flux, a popular hacking tool that had been developed by *Chrono Compendium* members. Designed to enable easy editing of a *Chrono Trigger* ROM image, the custom software facilitated “whole-scale editing of scenarios, field maps, the script, and many other areas of the game” (“Modification: Kajar Laboratories”). Noting that Kajar Laboratories had the intent to “instruct others how to circumvent [Square Enix] copy protection using Temporal Flux in violation of the Digital Millennium Copyright Act” the legal department demanded that the team “cease and desist any and all efforts to rip, hack, or circumvent our copyright protection measures or to teach others to do so.” In essence, it was not enough to simply stop production on *Crimson Echoes*. It appeared that Square Enix wanted to cut off *Chrono Trigger* hacking at its source.

Perhaps the most incriminating aspect of Square Enix’s cease and desist order was extracted from a readme file that circulated alongside demo releases of *Crimson Echoes*. Penned by members of Kajar Laboratories, the statement appeared to be a preemptive admission of guilt which acknowledged that, although the intent behind *Crimson Echoes* was not malicious, the practice of ROM alteration and modification was both illicit and unauthorized:

ROM altering and modification is illegal, and the demo has been made without the consent of Square Enix. However, Kajar Laboratories wishes that Square Enix view it as a piece of fanfiction or other fan-related work, falling in the general body of fan community proceedings that are too numerous to prosecute and summarily have a positive effect on the popularity of its games. Should Square Enix perceive the project as a threat to its sales or intellectual property, Kajar Laboratories will immediately cease operation on the project and comply with Square Enix's orders. (“C&D: Director’s Response”)

Square Enix was quick to pounce on this perceived admission of guilt, providing it as evidence to support their cease and desist order — “Your act of copyright infringement is deliberate and willful, as demonstrated by the ‘readme’ file to the CT:CE demo.” Having somewhat backed themselves into a corner, and unwilling to test the waters against the vast resources of Square Enix, Kajar Laboratories acquiesced to the legal department’s demands. Without protest, ZeaLity, Agent 12, and Chrono’99 discontinued production on the project they had spent four and a half years labouring over.

Disclaimer: This Is Not A Legal Study

Despite beginning this chapter with a cease and desist order, it is not my intent to provide a deep legal analysis of videogame hacking in North America. Rather, by referring to interviews conducted with my participants, I will instead discuss how intellectual property law and the methods by which corporations enforce it, affect development and distribution within videogame hacking subcultures. Many of the attitudes that circulate in these communities about legal matters are either: speculative, working under an assumption of what is legal or illegal (or at least what can be gotten away with) rather than directly engaging with policy; or reactionary, informed by a few well publicized incidents such as Square Enix’s cease and desist order. Thus, instead of attempting to analyze which aspects of videogame hacking may or may not be legal, I choose to consider how the interplay between copyright holders (primarily game developers and publishers) and videogame hackers shapes the practice. In this regard, I have found both Michel de Certeau’s writing on strategies and tactics and Henry Jenkins’s overview of collaborationist and prohibitionist models to be especially useful. As the *Crimson Echoes* cease and desist order exemplifies, videogame hacking occupies a place of tension between videogame developers and videogame hackers. Over the past decades, video game developers have created many strategies

of control for their intellectual properties while hackers have adopted tactics to work with and against these political, economic, and corporate structures.

Although I am reluctant to position this thesis as a legal study, I do feel it is important to briefly summarize copyright law in order to better understand how it intersects with the practice of videogame hacking. Even though my research participants hail from across North America and Europe, I will use Canadian law as a starting point, as its principles are quite similar to intellectual property law in the United States and parts of Europe. Laura Murray and Samuel Trosow provide an excellent summary of this legal landscape in their book *Canadian Copyright: A Citizen's Guide*, in which they highlight copyright's importance as one of four of the key intellectual property devices in Canada — the others being patent, trademark, and confidential information, such as trade secrets (55). The stated purpose of copyright is to protect forms of expression — such as literature, artistic works, and computer programs — by giving the original creator certain exclusive rights to their original work for their entire lifetime, plus 50 years. During this time frame, “the owner of the right not only can do the thing specified, but also can exclude others from doing it” (Murray and Trosow 77), with these “things” including acts such as reproduction, translation, and exhibition. Reproduction is particularly pertinent to videogame hacking which, as demonstrated by Robert Kudlha's *Space Invaders* ROM hacking, often relies on the duplication, alteration, and sharing of videogames. The Canadian Copyright Act states that a creator has “the sole right to produce or reproduce the work or any substantial part thereof in any material form whatever” (Copyright Act), meaning that a hacker's copying and alteration of a copyrighted work could be viewed as a violation of copyright law. However, Lawrence Lessig has complicated this seemingly cut-and-dry distinction, noting that in our current digital landscape almost any interaction with media can be considered a violation of copyright law:

“Because if copyright law at its core regulates something called copies, then in the digital world the one fact we can't escape is that every single use of culture produces a copy.

Every single use therefore requires permission; without permission, you are a trespasser”

(“Lawrence Lessig: Laws That Choke Creativity”)

As the enforcement of copyright law is not uniform — relying heavily on the original creator’s resources and their desire to protect their original work — there is often some confusion over what actions are permitted and which are not. Lessig explains that much of this confusion emerges from the amateur appropriation of digital media, noting that “what before was both impossible and illegal is now just illegal” (38). In the context of my research, media companies and videogame hackers are essentially contesting the meaning of copyright — or, perhaps, simply the limits of its efficacy — in a world where acquiring and altering videogames has never been more accessible.

de Certeau, Strategies, and Tactics

In *The Practice of Everyday Life*, Michel de Certeau defines a typology of power that involves two opposing forces: strategy and tactics. de Certeau notes that strategy is the purview of power, primarily facilitated through the occupation of space and becoming “possible as soon as a subject with will or power (a business, a city, a scientific institution) can be isolated” (36). Strategy is a concerted effort “to delimit one’s own place in a world” (36) and a capitalization on previously acquired advantages, relying on the mastery of space through vision and generating types of knowledge that can only be gained through this establishment of control. Where a strategy is dependent on the aggregation of power, in contrast, a tactic is determined by the absence of power. Tactics must “play on and with a terrain imposed on it and organized by the law of a foreign power” (Certeau 37) and must do so under surveillance and “within enemy

territory” (37). Capitalizing on mobility and seizing upon opportunities that offer themselves up at any given moment, tactics are both nomadic and ephemeral. While a strategy has the option of orchestrating a plan within a defined space, tactics instead operate opportunistically through isolated actions and must make use of:

“...cracks that particular conjunctions open in the surveillance of proprietary powers. It poaches them. It creates surprises in them. It can be where it is least expected. It is a guileful ruse” (Certeau 37).

Speaking more broadly, de Certeau elaborates that tactics can encompass a variety of concepts such as “victories of the ‘weak’ over the ‘strong’” within an imposed order, “clever tricks,” or even just “knowing how to get away with things” (Certeau xix). Although it is tempting to hearken these concepts back to their military origins, de Certeau notes that tactics can apply to many mundane everyday practices such as shopping, cooking, and even simply moving about a space (xix). To cite a well-known example, de Certeau outlines how the planning and development of a city can be considered a strategy while the navigation of its streets by its citizens is tactical in nature. Planners may invest numerous resources to predict and control the flow of people, but the citizens of the city will create their own paths — using shortcuts and other opportunities presented by the terrain — that can work with and against those plans (Certeau 99).

Although the city metaphor is evocative, much of what de Certeau discusses in *The Practice of Everyday Life* focuses upon how people transform, re-use, or appropriate media. Pushing back against the perception of media consumers as sheep, de Certeau discusses the practice of reading and challenges its perception as a purely consumptive practice (167).

Working against the presumption that “to write is to produce the text; to read is to receive it from

someone else without putting one's own mark on it, without remaking it" (169), de Certeau outlines how ordinary people (as opposed to professionals, intellectuals, and the ilk) can transform and reinvent the function of the media that they consume. de Certeau frames popular reading as a type of textual poaching, where instead of taking only the author's intended position, a reader "invents in texts something different from what was 'intended'" (169), much like how urban-dwellers travel their own paths in the aforementioned analogy of the city. Invoking the concept of bricolage — a French word that literally refers to "fiddling" or "tinkering" — de Certeau applies and transforms the concept to include everyday activities, noting that readers "fragment texts and reassemble the broken shards according to their own blueprints, salvaging bits and pieces of the found material in making sense of their own social experience" (175). Despite granting readers more agency over their interaction with media, de Certeau frames them as isolated travellers and nomads who "[poach] their way across fields they did not write" (37). They are capable of creating a multitude of meanings from a single text, but are thoroughly unable to keep whatever is gained (Certeau 37).

Applying Strategy and Tactics to Videogame Hacking

Throughout this chapter, I employ de Certeau's theories in two ways to better understand the practice of videogame hacking. First, strategy and tactics are a useful framework to consider the legal and technical landscape that complicates the alteration of videogames. Intellectual property law, as a collection of laws and policies, can be utilized by corporations as part of a broader strategy to control how people interact with and reproduce their creative works. It is the purview of power, in the sense that it generally requires enormous resources to enforce, a very particular type of legal knowledge to engage with, and relies on a mastery of space through vision — companies can only police what they can perceive and isolate, both in physical spaces

and across the Internet. In contrast, videogame hacking can be considered a tactic that is utilized by consumers and fans to engage with videogames that they have purchased or otherwise acquired. Whereas media companies lobby governments and employ their legal might to dictate where, when, and how consumers can interact with games, videogame hackers exploit cracks, ambiguities, and blind spots in both policies and vision to play, remake, and redistribute games in the ways that best suit them. These tactics are often forced to rely on amateur interpretations of legal and technical matters and can be quite reactionary in nature, often changing in response to major enforcement incidents, such as the aforementioned *Crimson Echoes* cease and desist order. They also have motivations rooted in the tenets of computer hacking, specifically the common hacker ideal of free information exchange and a generally distrust toward authority. In keeping tight control of the circulation and reproduction of creative works such as videogames, companies could be viewed as limiting “the deployment of copyrighted material in other expressive activity, and consequently [censoring] the public use of certain forms of expressive content” (Coleman 9).

Secondly, the idea of textual poaching is an intriguing way to consider how fans interact with videogames, from simply playing a commercial title to hacking it apart and reassembling it into something new. Primarily focusing on fans of television programs, Henry Jenkins built upon de Certeau’s idea of textual poaching in his 1992 book *Textual Poachers*. Jenkins summarizes the poaching analogy as a way to “characterize the relationship between readers and writers as an ongoing struggle for possession of the text and for control over its meanings” (24) and re-introduces the metaphor of bricolage to describe how “consumers are selective users of a vast media culture whose treasures, though corrupt, hold wealth that can be mined and refined for alternative uses” (27). Despite co-opting de Certeau’s metaphor, Jenkins questions de Certeau’s

claim that poaching can leave no traces, as well as the notion that the activity is primarily an individual one. Expanding on the idea of active reading, Jenkin notes that tactical reading can create more than just personal interpretations — it can also result in the propagation of fan culture generated texts that can be “shared and exchanged and created in a social infrastructure that supported such exchanges” (Jenkins, *Textual Poachers* xxiv). Jenkins touches on fanfiction (literary fan works), filk (science-fiction folk music), songvids (amateur music videos), and other ways that fans engage with the images presented to them via their television sets, examining the tension that is found between media producers and fans who interact with their texts in ways that are not always fully embraced or authorized (Jenkins, *Textual Poachers* xxii). In a sense, videogame hackers use tactics from both a hacker’s perspective, who desires to tinker with games despite legal barriers designed to prevent them from doing so, and a player’s perspective, who craves to play and share their games freely.

Prohibitionist and Collaborationist Models

I will further explore the various motivations of videogame hackers in Chapter 3. However, I would first like to explore how the interplay between strategy and tactics ties into videogame hacking and copyright law, while touching upon the hacking versus modding distinction I outlined in Chapter 1. With copyright and intellectual property law existing as more-or-less a blanket set of policies that relies heavily on a company’s willingness to enforce it, the difference between hacking and modding is often established through developer intent (i.e. whether or not a fan created alteration or addition to a game is authorized by the original creator). In a sense, each videogame developer sets their own strategy for controlling fan interaction with their titles, based on their own desires and the resources they have at hand. Writing with Joshua Green in 2009, Jenkins notes that this intent is often defined by a company’s

attitude toward its intellectual property and can be split into collaborationist and prohibitionist models. Under a collaborationist model, consumers and fans are viewed as allies and potential creators of value for a product. When considering videogames, this model can range from open file structures that allow users to easily add new content, something that has been well documented through studies such as Tanja Sihvonen's research on *The Sims* series, to moderated platforms in which players can create, upload, and sometimes even sell content, such as with Valve's *Skyrim* mod marketplace on their online distribution platform Steam ("Introducing New Ways to Support Workshop Creators"). Although this collaborationist model is not without its tensions — Valve, for example, eventually removed mod monetization from Steam due to pushback from its player base (Joseph) — it does represent a more flexible relationship between developers and their audience. In contrast, the prohibitionist model views this same group of consumers and fans as a potential threat to the circulation and meaning of their product, whose "acts of repurposing and recirculation constitute theft" (Green and Jenkins 220). *Chrono Trigger: Crimson Echoes*' cease and desist order can be considered part of this prohibitionist mindset, as despite the hack's lack of monetization and its framing as fan-generated content, it was still targeted by Square Enix's legal department as "deliberate and willful" copyright infringement. Hector Postigo recounts a similar situation in 2003, chronicling a group of fans who created *GI Joe* mod for the PC title *Battlefield 1942* that introduced vehicles and characters from the popular military franchise to the game (Postigo, "Video Game Appropriation through Modifications" 63). Similarly framed as a fan activity designed to sustain interest in both *Battlefield 1942* and the *GI Joe* franchise, the mod eventually received a cease and desist order from Hasbro that halted development (Postigo, "Video Game Appropriation through Modifications" 64). Struggling with Hasbro's motivations for shutting down the mod, fans

attempted to negotiate a licensing agreement with the developer to legitimize continued development. However, similar to *Crimson Echoes*, the game's developer had no interest in embracing the *GI Joe* mod or fostering a relationship with the fans who had created it. True to the prohibitionist model, they simply wanted to eliminate the unauthorized usage of their brand.

The prohibitionist and collaborationist models are firmly rooted in the concept of participatory culture, which Jenkins outlined in his 2006 book *Convergence Culture*. Referencing both de Certeau and his own writing in *Textual Poachers*, Jenkins describes participatory culture as a broad concept in which people are viewed not simply as consumers of media, but also active contributors. Although this viewpoint grants a certain amount of agency to the individual consumer (in the purview of my research, the player) it still acknowledges that corporations wield considerably more power than any individual consumer could. As I described in my own example of *Crimson Echoes* and Hector Postigo's analysis of the *GI Joe* mod for *Battlefield 1942*, this imbalance of power often results in conflict. Jenkins is quick to highlight this tension, acknowledging that "the key debates of our times will be over who gets to define the terms of our participation" and that these debates will only become more diverse and ambiguous "as more groups assert control over the processes of cultural production and circulation" (Jenkins, *Textual Poachers* xxii). In a sense, participatory culture and the prohibitionist and collaborationist models can be viewed as an extension of de Certeau's theories — they can be used to scrutinize how media industries have chosen to interact with their consumers, as well as how consumers have accepted or resisted this engagement. Jenkins encourages scholars to adopt this lens to question "who is participating (and who is excluded from participation)" and "what factors limit or enable participation," such as the resources and competencies necessary to dispute copyright claims.

It is important to note that corporate strategies in regard to media content are rarely consistent or homogenous. Collaborationist and prohibitionist approaches, for example, are not always adopted universally throughout a given company, as individual strategies are often created for different projects. As an example, Nintendo encourages players to create their own levels within the Nintendo Wii U game *Super Mario Maker*, publishing their creations in a free marketplace of user-generated content. At the same time, Nintendo's legal department has leveled copyright strikes and other legal action against videogame hackers who create their own levels within older entries in the *Mario Series* (Schreier, "Nintendo Files Copyright Strikes Against Super Mario 64 Online") — something I will explore later when discussing Kaze Emanuel's long history of *Super Mario 64* hacking. Where and when the collaborationist and prohibitionist models are implemented are part of a company's overarching corporate strategy, leaving their fans to navigate a varied landscape with inconsistent and oftentimes unclear rules of engagement. As such, many videogame hacker tactics involve testing the waters to see what sort of projects are allowed or, at the very least, what can be gotten away with. Throughout the remainder of this chapter, I will discuss some specific tactics that emerged during my discussions with videogame hackers, how they were developed, and how they fit into broader contexts of media creation and distribution online.

Pokémon Prism

Seven years after Square Enix ordered Kajar Laboratories to halt production on their fan hack *Chrono Trigger: Crimson Echoes*, another videogame ROM hack found itself facing a nearly identical legal situation. Adam, a *Pokémon* hacker from California, received a cease and desist order on December 21st 2016 from Nintendo of Australia that claimed he was making "unauthorised use of Nintendo intellectual property." The order specifically targeted *Pokémon*

Prism, a fan-made entry in the *Pokémon* series that Adam constructed using a *Pokémon Crystal* ROM image as its base. Adam had spent roughly eight years developing the project and had plans to release it to the public in the following months. Nintendo's demands were straightforward and extensive: Adam was to abstain from releasing the (nearly completed) videogame hack, remove all related content from his website, and refrain from using any of Nintendo's intellectual property in the future. Much like the Kajar Laboratories team at the *Chrono Compendium*, Adam felt like he had little means to dispute the order. He quickly complied to Nintendo's demands.

I spoke with Adam in 2018, almost exactly two years after he walked away from his project, and he recounted the development of *Pokémon Prism* from its beginnings as a relatively unknown fan project to something that was prominent enough to catch Nintendo's attention. By the time that Adam received the cease and desist order for *Prism*, he had been hacking videogames for over a decade. His first major project was *Pokémon Brown*, an unofficial entry in the *Pokémon* series released in 2004, which he created by hacking a ROM image of *Pokémon Red* for the Game Boy. *Prism* was essentially a follow-up effort to *Brown*, and Adam describes the beginnings of the ROM hack as a solo, hobbyist effort — “I would get help with like small things like music or graphics, but like 95-96% of the game was me doing stuff in my free time.” Although the *Pokémon* fan community was always supportive of his work, Adam noted that the project maintained a pretty low profile until the final year of development where “things got kinda crazy.” Worrying about his ability to finish development on *Pokémon Prism*, Adam connected with the Twitch Plays *Pokémon* team — a group of Twitch streamers and videogame hackers that he had previously assisted with their *Pokémon Crystal* playthroughs — and they came to agreement. If the Twitch Plays *Pokémon* team would help Adam bring *Prism* to

completion, then Adam would allow them to premiere the finished videogame hack on their Twitch stream. Adam noted that he was quite grateful for the assistance, claiming that he had begun to hold the creeping suspicion that “the project had been going on way too long; it’s never going to get done.” However, he never anticipated how much attention *Prism* would receive as it neared completion. A trailer for the game, authorized but not created by Adam, quickly racked up over 1.4 million views on YouTube and *Pokémon Prism* began popping up on gaming news websites such as Kotaku, IGN, and Gamespot. Adam notes that this uptick in publicity began to raise concerns about legality, especially in the wake of previously litigation aimed at fangames such as *Pokémon Uranium* (Good). “I was worrying about that ever since the trailer got released and news sites were reporting on it,” he noted, while emphasizing that any doubts he had were overshadowed by a strong desire to complete the game. “I’ve been working on this for a long time and I’m not going to let fear stop me from doing this... and if it happens, it happens, and that’s that. And it did happen.”

Patch Files and Decentralization

At first glance, it may seem that both Adam and Kajar Laboratories were somewhat careless with their handling of intellectual property that belonged to industry juggernauts such as Nintendo and Square Enix. However, their distribution methods were, are still are, considered the standard for many videogame hackers. I connected with ZeaLity, one of the lead designers from Kajar Laboratories and a current staff member at the Chrono Compendium, in November of 2018 and he emphasized that the community had been very diligent in releasing *Chrono Trigger* videogame hacks exclusively as IPS patches. Patches are computer files that contain sets of instructions that can be applied to a videogame ROM image to enact changes, altering anything from graphics, to music, to the underlying code of a game. When combined with the ROM image

of a game — *Chrono Trigger* for *Crimson Echoes* and *Pokémon Crystal* for *Pokémon Prism* — using a piece of free-to-download software, the patch file creates an updated ROM image that includes all of the hacker’s intended changes. ZeaLity noted that the Kajar Laboratories team felt comfortable distributing these files, since the IPS patch did not actually contain any copyrighted content and instead “just [decided] what to overwrite to turn *their* game into *your* game.”

Commonly used by large videogame hacking websites such as ROMHacking.net, patch files shift the onus for sourcing copyrighted material to the individual user, allowing hacking repositories to avoid hosting potentially illicit content on their servers. As an added note, ZeaLity mentioned that in addition to the insulation that IPS patches provided the development team felt that Square Enix was no longer keeping tabs on the *Chrono* series, which had not seen a new release for nearly a decade. The IPS file for the community’s previously released ROM hack, *Prophet’s Guile*, had been downloaded over 25,000 times without incident and there was “a general feeling that things had died so much that Square doesn’t care about the series — none of these characters are going to be in *Smash Bros*!”

If the decentralization of ROM ownership sounds familiar, it is because the tactic is not unique to videogame hackers. Offloading the responsibility of hosting copyrighted content to individual users is something that peer-to-peer file sharing technologies have been doing for decades with varying degrees of success. BitTorrent, an extremely popular communication protocol for peer-to-peer file sharing, has gained notoriety since its creation in 2001 for its ability to share large media files such as movies, TV shows, and digital audio. To send or receive such files, a user must install a BitTorrent client on their computer, such as BitComet or μ Torrent, which then implements the BitTorrent protocol for them. Once they have the software up and running they can then consult a BitTorrent tracker, a website that tracks which files are available

for users to download, to essentially browse a menu of files that they can download. Instead of taking responsibility for hosting copyrighted files on a central computer, these trackers instead rely on files that live on the machines of individual Internet-connected users. Although lawsuits have been leveled against various BitTorrent trackers — perhaps most famously against The Pirate Bay, which keeps extensive records of this legal action on their website (“Legal threats against The Pirate Bay”) — corporations have generally found it difficult and time consuming to control this sort of decentralized exchange. In contrast, game developers and publishers often find little resistance when targeting legal action directly at individual users or websites that directly host illicit copies of games, perhaps best exemplified through Nintendo’s 2018 lawsuits against LoveROMs and LoveRetro (Onanuga). Run by Jacob and Cristian Mathias, LoveROMs and LoveRetro were two popular ROM sharing websites that hosted enormous selections of videogame ROM images for download. Unwilling to face Nintendo directly in court, the couple decided to accept the charge of copyright infringement and eventually agreed to pay a settlement figure of \$12.23 million while abstaining from ever working with emulators, ROMs, and their related technologies again (Wajeeh). Looking to limit their own risk, but still interested in sharing their work, many videogame hackers leverage BitTorrent and file patches in tandem to facilitate the distribution of their hacks. Peer-to-peer technologies afford access to digital copies of videogames, oftentimes in bundles containing thousands of ROM images, while patches provide an ostensibly legal method to enact a hacker’s changes onto a ROM. Decentralization benefits hackers as it provides them with the games they use as raw materials and ensures that their audience will have access to games that, when combined with their patch files, will be transformed into their completed projects.

Anonymity, Dispersal, and Persistence

While patches are certainly a popular tactic for videogame hackers, some prefer a more direct approach. Kaze Emanuar — a *Super Mario 64* hacker and student from Germany — describes the attitude of many of his fellow *Super Mario 64* hackers as being a touch more cavalier. Although the distribution of patch files remains a popular option, Kaze notes that “people just upload [hacked ROMs] to MediaFire or Megaupload or whatever.” These free file hosting services provide links to uploaded content that can be embedded almost anywhere, from fan websites to YouTube channels, and do not conduct automatic review processes to block copyrighted material. Kaze notes that even when Nintendo does step in to remove a file that contains its intellectual property, “if you take anything down [the Mario 64 community] just re-uploads it and then everything is fine!” Since the community is active enough to re-upload ROM hacks as quickly as they are removed, eliminating copyrighted content from services such as MediaFire and Megaupload proves to be a Sisyphean task. This difficulty is heightened by the fact it is almost impossible to determine who is actually uploading a given file and where they are uploading it from, making directed legal strikes is somewhat arduous. As I discovered when attempting to track down videogame hackers for my research, using a pseudonym is almost ubiquitous, and is often viewed as a way to shield oneself from potential legal scrutiny.

Returning to Postigo’s account of the *GI Joe* mod for *Battlefield 1942*, the use of anonymity was one of the tactics eventually adopted by those who wished to continue work on the project following the cease and desist order. Postigo notes that the mod’s developers had started to “[anonymize] their postings in an attempt to make their identities untraceable” and had even looked into hosting content “somewhere where copyright law could be interpreted in their favour” (Postigo, “Video Game Appropriation through Modifications” 67). In absence of an

official collaboration with Hasbro, the project's developers instead contemplated an approach that relied on anonymity and obfuscation. How would Hasbro stop what they could not keep track of, and would it even be worth the resources required for them to do so? Although the *GI Joe* mod project was ultimately disbanded, this approach does question the efficacy and limits of copyright enforcement.

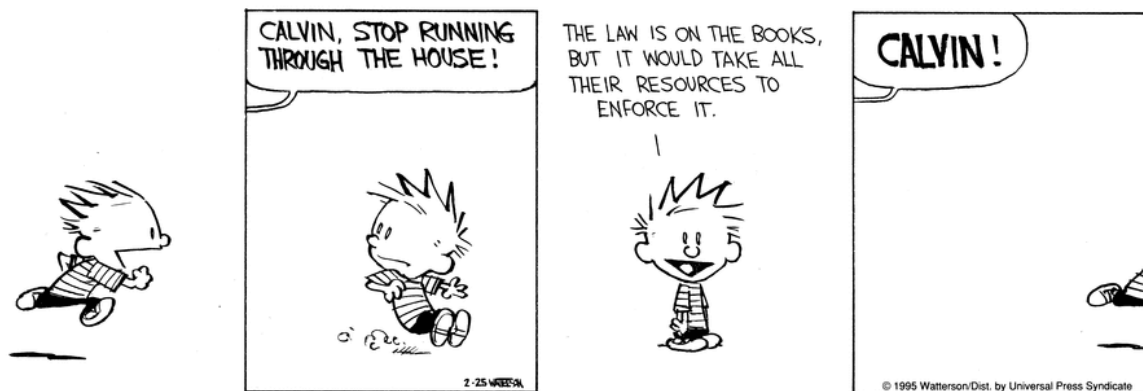


Fig 2. Watterson, Bill. *Calvin and Hobbes*, 25 February, 1995.

In addition to keeping a videogame hacker's identity anonymous, ZeaLity notes that a certain level of caution should be taken when sharing the hacking projects themselves. Looking back on the fate of *Chrono Trigger: Crimson Echoes*, ZeaLity echoed Adam's sentiments that the pre-release publicity of the hack was one of the key factors contributing to its downfall:

I think we just screwed ourselves because, in either February or March 2009, I officially, on the sidebar [of the Compendium], pretty front and center, put a link to a page on our media wiki specifically for the ROM Hack. It was full blast, "coming this year"... I think that our attempt to increase publicity ahead of the launch sorta did it in on that one.

Reflecting upon the decade-old cease and desist order, ZeaLity offered forth a set of revised tactics that he believed that videogame hackers should follow in order to avoid sharing *Crimson Echoes*' fate. Despite his own acknowledgement that "there is no centralized guild of ROM

hackers” and that when videogame hackers “have brushes with IP and copyright, they usually just walk right into it and get blindsided,” ZeaLity’s recommendations are representative of some broader attitudes and trends expressed by my participants. First, he suggested that the best practice for making a hack of a popular franchise game is to “go underground until the day before [release] and just drop it out” into the world. ZeaLity mentioned that game developers simply do not have the resources to monitor “random forums and boards” in search of what could be the next threat to their intellectual property — in a way, you have to let yourself get discovered through promotion and publicity. Building on this point, ZeaLity noted that once a hack has been released on the Internet it is almost impossible to stop its circulation. Patches and most ROM images are very small files by today’s standards, making their distribution easy through a variety of methods. ZeaLity emphasized that with “a file that small and the curiosity of playing a third Chrono game - it’s just too darn easy,” explaining that many ROM hacking communities thrive because of this easy circulation. Reiterating the points that Kaze described in his summary of *Super Mario 64* hackers (who constantly re-upload content to file sharing services), ZeaLity pointed out that “it’s almost as if the ROM hacking community continues to thrive specifically because it would be too cost prohibitive to squash all of it.” As Calvin glibly calls attention to in the above comic strip, “the law is on the books but it would take all of their resources to enforce it.”

However, successes for both videogame developer strategy and hacker tactics are often short-lived and the distinction between winners and losers is generally not cut and dried. Following Nintendo’s cease and desist order against *Pokémon Prism*, for example, the in-progress hack was leaked onto the Internet and can now be found on any number of ROM hacking websites. Fans of *Pokémon Prism* have even gone as far as to form an anonymized

collective titled RainbowDevs to continue development on the hack, creating a homepage to document their efforts and crafting an online patching application that allow fans easy access to the project (“Pokémon Prism File Patcher”). Although Adam notes that this was all completed without his consent or involvement, the fact remains that *Pokémon Prism* is now complete and accessible in the aftermath of direct legal pressure from Nintendo. In contrast, while Nintendo may find themselves somewhat helpless to stop the distribution of Kaze Emanuel’s videogame hacks, they have found other ways to push back against his work. Following the release of *SM64 Online*, a multiplayer hack of *Super Mario 64* for the Nintendo 64, Nintendo leveled copyright strikes against Kaze’s YouTube channel and shuttered his Patreon. “I’m not sure why they did it,” admitted Kaze. “Maybe it was because Odyssey was releasing and the [hack] was getting too popular, so they feared they might lose money there.” Whether the goal was to reduce the profile of Kaze’s work, disrupt his attempts to monetize it, or simply to protect their own brand, Nintendo’s victory was only effective for a short period of time. Kaze’s YouTube channel was quickly restocked with videos documenting his hacking efforts and his Patreon has returned with only a handful of aesthetic changes — “I had to remove any references to anything that was Nintendo related; I used to have a banner that had Mario sitting on Yoshi in Mario 64 and I had to take that out.” As both *Pokémon Prism* and Kaze’s hacking practice demonstrate, there is a tension between media companies and hackers under the prohibitionist model that is rarely resolved neatly. Even when working from a position of power, corporate entities may struggle to create a strategy that can predict and control the distribution of their games, and despite the common belief that their practice is too decentralized to shut down, hackers often feel powerless when faced with legal action from a large media company.

The *A Link to the Past Randomizer* and Online Patching

When exploring the website for the *A Link to the Past Randomizer*, a popular hack of the Super NES game *The Legend of Zelda: A Link to the Past*, I found it remarkable how much its landing page mimicked the style of a professional website. Featuring a sleekly designed logo, a YouTube trailer for the community’s online tournaments, and links to a variety of supporting resources, many would mistake this videogame hack for a commercially released title. The website even greets visitors with an elevator pitch for the hack, summarizing its gameplay and inviting people to join the community:

ALtTP: Randomizer is a new take on the classic game *The Legend of Zelda: A Link to the Past*. Each playthrough shuffles the location of all the important items in the game.

Will you find the Bow atop Death Mountain, the Fire Rod resting silently in the library, or even the Master Sword itself waiting in a chicken coop?

Challenge your friends to get the fastest time on a particular shuffle or take part in the weekly speedrun competition. Hone your skills enough and maybe you’ll take home the crown in our twice-yearly invitational tournament. See you in Hyrule! (“Start Playing”)

I will summarize the *Randomizer*’s development more fully in Chapter 3 — discussing its roots in speedrunning, puzzle races, and *Zelda* series fandom — but for now I would like to provide an overview of the tactics the *Randomizer* development team adopted to allow the project to thrive where other similar hacking projects have not. Whereas ZeaLity preached the importance of anonymity and quick dispersal, the *Randomizer* development team is only partially anonymous and has built a sustained online presence since its inception in 2016. I had the opportunity to speak with three members of the *Randomizer* team: Chris Owen, the *Randomizer*’s British community manager; Axel Hellström, a Massachusetts based software engineer who contributes

to the code and design of the project; and Veetorp, an American computer programmer who maintains the *Randomizer*'s online application and randomization algorithm. Despite the publicity of their efforts — the project has been featured on popular gaming websites such as Kotaku (Schreier, “People Are Doing Remarkable Things With Zelda: A Link to the Past”) and its Twitch tournaments draw hundreds of participants — the development team shares an optimism regarding both the hack's legal standing and the continued viability of the project. Their confidence seemed to be rooted in one of the central elements of their website: the *Randomizer*'s online patching tool.

Most videogame patching tools, such as the popular multi-platform patcher Lunar IPS, are standalone computer programs that must be downloaded and installed on an individual's computer. Despite being relatively straightforward to use, the *Randomizer* team noted that these types of programs do pose some accessibility issues. First, some users may be reluctant to install an unknown application on their computers, or may be unable to do so because of their operating system. Veetorp, the main developer of the *Randomizer*'s online application, noted that one of the reasons he wanted to pursue a web-based patching system was because he was tired of having to emulate Windows on his Mac OS in order to run a patcher — “it has to work quickly, it has to be more efficient, it has to work on every system.” Second, since patching applications are often meant to encompass a large array of videogame and patch types, they may not be tremendously adept at troubleshooting issues for a specific single title. Users may find themselves at a dead end if there is a small issue with either the ROM image or patch file used in the patching process. Finally, using a standalone patcher requires a user to juggle three files — the original game, the patch file provided by the hacker, and the patching software itself. This issue is exacerbated by the fact that many popular videogame hacks release updates on a semi-

regular basis, requiring users to consistently check to see if they have the most up-to-date version. Seeing these issues, and wanting to make their work more available while still leveraging the legal advantages of a patch file, the *Randomizer* team decided to craft a web-based patching application. Instead of managing multiple files, Owen noted “you just visit a website, click a few buttons, and all of a sudden you’ve got a randomized version of your game.”

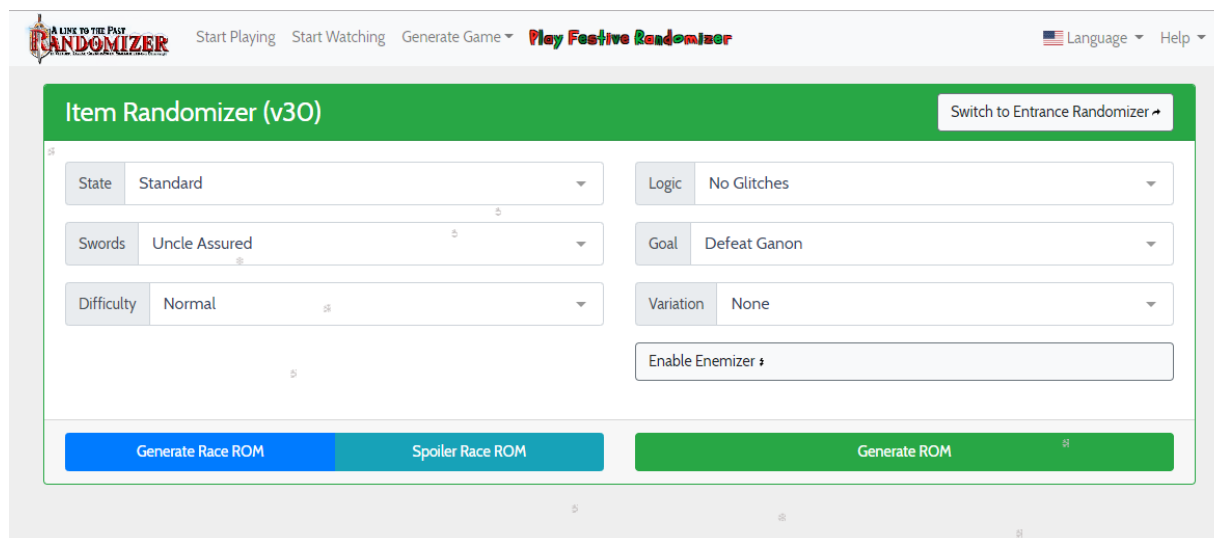


Fig 3. Screenshot of the *A Link to the Past Randomizer*’s online patching application taken by Michael Iantorno from: *A Link to the Past Randomizer*, alttpr.com/en. Accessed 08 Jan. 2019.

In addition to ease of access, the online patching system also facilitates many features that are unique to the *Randomizer*. Unlike most patches, which impose a static set of changes onto a ROM image (such as the sprawling narrative of *Crimson Echoes*), the *Randomizer* reshuffles the location of key items within *The Legend of Zelda: A Link to the Past* differently every time the ROM image is patched. Although based on an algorithm — one that prevents a player from getting stuck and unable to complete the game — this randomization will always create a unique ROM image for a player with a unique set of changes. This algorithm (commonly referred to by the team as “the logic”) is designed to diffuse game mastery, turning each generated ROM into a standalone puzzle that can be solved through experimental play. In a

sense, it takes a familiar game and allows players to unfamiliarize themselves with it for the purpose of replayability. “This is our childhood game... but you can only play the same game so many times,” explained Hellström. “But if it’s your favourite childhood game you can keep playing forever!” Adding to the variety of the core randomization algorithm, the web-based patching software also lets players customize their ROM by toggling features within the application’s interface. This includes options such as difficulty, goal structure, and the location of enemies with the game. Once players have acquired a copy of a *The Legend of Zelda: A Link to the Past* ROM image, they are free to generate as many unique randomized copies as they wish. By using the online patcher, they will always have access to the newest version of the *Randomizer* and can constantly tweak the experience based on their preferences.

Pass-Through Modification and Nintendo vs Galoob

Accessibility and customizability are certainly important aspects of the *Randomizer*’s online patching application, but solidifying the project’s legal status is also a central consideration. Chris Owen emphasized that, under no circumstances, does anyone from the *Randomizer* team provide ROM images to players — “that’s absolutely illegal to do and we don’t do that” — and that the development team “essentially just combined the patch and the person providing the ROM into one step.” Speaking on the possibility of a cease and desist order, particularly one that would invoke the Digital Millennium Copyright Act (DMCA), Hellström outlined his belief that the *Randomizer* team could not be targeted under current laws. Crediting his experience as a software engineer and his strong familiarity with “DMCAs,” Hellström described to me the many difficulties that Nintendo could face if they decided to contest the project:

When you do a DMCA, you have to indicate “what thing,” what piece of your property is being transmitted. So, the idea here was that we look at the network communication between the site and the browser. This is a system set up so we can say: “this is all the traffic between the client and the server. Please point to where in this information in this stream anything that belongs to you... and we’ll remove it. We’ll be happy to.” But the thing is, there is no data of theirs for them to point to, for them to remove. No matter where in the file they point we could say “oh no, that’s our intellectual property. You can see our original source material for it here.”

In essence, the *Randomizer* team set up a system that allows anyone to modify a *The Legend of Zelda: A Link to the Past* ROM within a web browser, without the development team ever having to host a copy of the game. Although arguments could be made about how a *Zelda* ROM image is required for both the initial hacking of the game (how are the hackers making changes in the first place?) and its continued distribution, being able to avoid hosting copyrighted media has proven to be a successful tactic for the *Randomizer* team thus far. Hellström believes that if they were going to be targeted with a cease and desist order, it would have happened already: “We’re a high enough profile project — if they thought they had any chance they would have pulled the trigger months, if not years ago.”



Fig 4. Game Genie, Front from: Johnson, Eric E. “Innovative Add-on Device for Video Game Console Not Copyright Infringement.” Museum of Intellectual Property, museumofintellectualproperty.org/features/game_genie.html. Accessed 15 May 2019.



Fig 5. Game Genie, Box from: Johnson, Eric E. “Innovative Add-on Device for Video Game Console Not Copyright Infringement.” Museum of Intellectual Property, museumofintellectualproperty.org/features/game_genie.html. Accessed 15 May 2019.

Hellström’s viewpoint is not purely a speculative one. As we chatted about the possible legal implications of the online patching system, he mentioned that he views the *Randomizer* as paralleling the functionality and legality of the Game Genie. When questioned about what the development team would do if some sort of legal challenge came forward from Nintendo, Hellström boasted:

They don’t have a pot to piss in or a leg to stand on so, to them, I would say “bring it the fuck on.” I’m not worried about Nintendo because it’s going to be Nintendo versus Galoob part two, I promise you.

The court case that Hellström references is *Lewis Galoob Toys, Inc. v. Nintendo of America, Inc.* (*Ninth Circuit Court of Appeals, 1992*), in which Nintendo sued the toymaker for copyright infringement, focusing on their Game Genie device. Created as a “videogame enhancer” and first released in 1990, the Game Genie was designed to be a plug-and-play solution for cheating in Nintendo games, one that could “selectively block and replace data from the cartridge” (Johnson)

to tilt gameplay to a player's advantage. Although containing no data from the videogame it was modifying, the add-on device allowed players to change aspects of the game upon booting it up. By inserting the Game Genie between a game cartridge and an NES and entering one of many predefined codes, players could grant themselves infinite lives, invulnerability, or any number of other beneficial effects. Claiming that Galoob "infringed upon its copyrights by creating 'derivative works' based on its copyrighted games" (Johnson), Nintendo attempted to stop the manufacturing and distribution of the device. However, in 1992, the Ninth Circuit affirmed the decision made by a federal district court, siding with Galoob and noting that a derivative work "must incorporate the original work in some 'concrete or permanent form'" (Johnson). Judge Fern M. Smith noted in her ruling that "having paid Nintendo a fair return, the consumer may experiment with the product and create new variations of play, for personal enjoyment, without creating a derivative work" (Smith 1292), likening the practice to skipping past pages in a book or fast-forwarding through a movie. Although the parallels with the *Randomizer*'s online patching application are not perfect, Hellström noted his confidence in their legal standing — "It was ruled in no uncertain terms that passive, pass-through modification is protected speech and that is to the dime, what it is." As no online ROM patching system has faced legal action thus far, the tactic could be considered a successful one... at least for the moment. The *Randomizer* maintains a strong public profile, runs constant activities on Twitch, and has even become a part of many speedrunning conventions, all without receiving a single notice from Nintendo's legal team.

Chapter 3: Hacking Motivations

In the previous chapter, I discussed some of the ways in which videogame hackers interact with the technical and legal barriers that challenge their work. In this chapter, I am less concerned with the “how” of videogame hacking and more interested in exploring the “why.” That is, what motivates players to edit a game’s code in unsanctioned and unexpected ways? I open this chapter by briefly summarizing an article by Jeroen Jansz and Jørgen Haug Theodorsen, which contains a list of potential motivations for videogame modders. Using this typology as a guide, while adding additional context and categories of my own, I then compare and contrast these motivations with those of my participants and other scholars. I begin by referring to Hector Postigo’s writing on PC game modders, in which he discusses how a fan’s love for a particular videogame can extend to both its text (such as the narrative or setting) and its code. This admiration for code can focus on a game’s technical parameters or simply how it feels — often characterized as gameplay, movement, and physics — and may motivate a player to stick with an older title despite the release of newer entries in a series. Extending upon this idea, I then outline how speedrunning and puzzle races tie into the formation of videogame hacking knowledge communities, serving as an entry point for fans who may obsess over the code or the logic of a given title. Returning once more to Henry Jenkins, I discuss how these virtual communities leverage their collective intelligence to map out the inner-workings of videogames, in turn allowing members to engage in amateur media archaeology to seek out hidden content within their favourite titles. To close the chapter, I briefly touch upon the financial and professional motivations of videogame hacking, ranging from meagre transactions within fan communities to corporate entities that have adopted the practice.

A Typology of Motivations

In their 2009 conference paper *Modifying Video Games on Web2.0*, Jeroen Jansz and Jørgen Haug Theodorsen elaborated on a series of qualitative interviews and quantitative surveys they conducted in order to determine the motivations behind videogame modding. After speaking with 15 self-described videogame modders, the pair assembled a short list that described the various desires that push people toward the practice. Finding parallels with Henry Jenkins research — particularly his notions of participatory culture and his accounts of media fandom — Jansz and Theodorsen noted that a desire to alter videogames quite often extends beyond the (oft-presumed) career-oriented or commercial motivations (5). Combining previous categorization work completed by Behr and Sotamaa with their own ethnographic research, Jansz and Theodorsen present a set of six motivations:

1. **Improving:** Modders are motivated to develop game content of a higher quality for example by acquiring detailed information about a game and its technical aspects.
2. **Creativity:** Modders feel an urge to produce creative work, which may be experienced as a challenge.
3. **Self-marketing:** Creating mods contributes to one's portfolio.
4. **Community:** Creating mods is done because the modder likes to become part of the modding community or a dedicated modding team.
5. **Entertainment:** Modders create mods because it is in itself experienced as an enjoyable activity.
6. **Love for the game:** Modders engage with mods because they like to spend time with their favourite game. (Jansz and Theodorsen 9)

Although Jansz and Theodorsen describe their participants as modders, these categories also serve as an excellent starting point when considering why videogame hackers choose to engage with their favourite videogames. I will refer to these six criteria as I analyse the accounts of my participants throughout the remainder of this chapter, in an attempt to understand their motivations and contextualize their histories with videogame hacking. I also offer forth an additional entry to the list, based on the accounts of my participants: amateur archival practice and media archaeology. In their article, Jansz and Theodorsen note that “the participatory culture of modding enables individual modders to freely create their own content, but this freedom is limited by the tools provided by the industry” (5). Unlike modders, many videogame hackers are not beholden to the limitations imposed by industry tools, and will access and alter any aspect of a videogame that they have the technical proficiency to facilitate. As videogames — especially older cartridge-based titles — are typically designed as closed systems by developers and publishers, this unauthorized alteration requires the hacker to push into areas of the game which are typically not accessible. Thus, this penetrative work often results in the discovery of unused or hidden assets that have been secreted away in the game, out of the reach of casual users. Unearthing these game assets can be considered another motivation for videogame hackers, allowing them to learn more about the history of a title by speculating on these materials.

As an additional note, one that ties into Jansz and Theodorsen’s entertainment category, a core theme that underlies all of the aforementioned motivations is a general interest in computers and technology. A popular videogame title may inspire a bevy of fan activities — including the widespread practices of fanfiction, fanart, and fan videos — but only a small percentage of players will ever attempt to alter a videogame directly. Those who choose to engage in videogame hacking or modding, at least among my participants, usually hold an

existing interest in computers, code, and software development, or at least a desire to cultivate one. In her study of *The Sims* modders, *Players Unleashed!*, Tanya Sihvonen corroborates this viewpoint (or rather, I corroborate hers) when she outlines how “the practices that we would now consider modding, that is, enhancing, extending, or tweaking the code of computer programmes, especially games, can be traced back to the early days of software development and online networking” (72). As I discussed in my first chapter, videogame hacking finds many of its roots in the diverse history of computer hacking, ranging from mainframe hackers who experimented with early computers to Internet hackers who connected with each other using early iterations of the web. Many of the core tenets of hacker culture (working within constraints, a desire for free information exchange, etc.) are important aspects of videogame hacking, and Sihvonen notes that hacking and modding serve as a connection “between practices that are considered either as programming/working on code or playing games” (72). In essence, videogame hacking lives somewhere in the territory between fan activities and computer programming/hacking culture, making it an intriguing locale to observe the workings of participatory culture that stem from the interactions between player and game.

Love for the Game - Fans of the Code

A “love for the game” may seem like a simple enough statement when considering the motivation of a videogame modder or hacker but, in many ways, the sentiment is too broad. A love for a videogame does not always result in the creation of a fan work and, when it does, it can encompass any number of fan activities. In *Video Game Appropriation through Modifications*, Hector Postigo touches on some of the reasons that a fan may gravitate toward hacking or modding in favour of other fan practices. Referencing projects where players endeavoured to take a franchise that they were a fan of (*GI Joe* and *Duke Nukem*) and graft them

onto existing PC titles (*Battlefield 1942* and *Quake 3*, respectively), Postigo identifies two layers in the fandom of his participants. First, the modders were clearly avid fans of the existing franchises, having meticulously scoured their favourite cartoons, comic books, and games for content. Secondly, Postigo notes that these are “not only fans of the text but also fans of the code” (69) who appreciate the technical aspects of both the *Battlefield 1942* and *Quake 3* game engines. Their choice to interact with a given title was not always based on the text of the game, but also on “the source code of a game, the software development kit or SDK, the textures, and other design elements and tools” (Postigo, “Video Game Appropriation through Modifications” 68). Postigo lists off many of the technical features present in a videogame, but it is important to acknowledge that this admiration for code often begins with a qualitative observation rather than a survey of software features. As I will discuss throughout this chapter, many of my participants were attracted to the “feel” of a game — captivated by the way a character moves, the manner in which the game’s camera follows them, or how they are able to cut their way through a swath of enemies. This love for the code, both at the more ambiguous level of feel and as a list of tangible software features, is an important aspect of videogame fandom, one that helps explain why videogame hackers may go to great lengths to acquire, understand, and alter their favourite titles.

This love for code is also vital for understanding why videogame hackers often focus on older games, despite the existence of newer titles in the same series or franchise. Kaze Emanuar, whom I spoke with about his extensive *Super Mario 64* hacking work, was quick to push back against the idea that entries in Nintendo’s *Mario* series were seeing linear improvement, especially in regard to the movement of its eponymous protagonist. He specifically mentioned that he feels the way in which Mario moves in *Super Mario 64* is superior to what is featured in “new” games in the series (which he considers anything released after 1996’s *Super Mario 64*):

I think that in the new *Mario* games the movement feels a lot slower... Mario doesn't really like have, how do you put that? He doesn't really have inertia anymore.

Kaze noted that this love for the movement — which he refers to interchangeably as “physics,” “inertia,” or “gameplay” — is something that leads people to both videogame hacking and speedrunning, the practice of playing through a videogame with the intention of completing it as quickly as possible. “The people who speedrun the games, they speedrun it because they find the movement fun,” explained Kaze, elaborating that *Super Mario 64* hackers generally avoid tweaking many of the game's core mechanics for the same reason. As demonstrated in Kaze's own hacks, such as *SM64: Last Impact* and *Super Donkey Kong 64*, the emphasis is often placed on creating new content around the core mechanics of the game rather than altering them directly. Playing *SM64: Last Impact* feels much like playing an add-on or expansion to *Super Mario 64*, as most of Kaze's efforts were focused on the creation of new levels, enemies, music, and power-ups.

Members of the *Link to the Past Randomizer* development team corroborated many of Kaze's points, noting that their shared love for *The Legend of Zelda: A Link to the Past*'s core mechanics is central to both their own hacking motivations and the popularity of the *Randomizer* online. Chris Owen, the *Randomizer*'s community manager, describes how fans desire to have more content added to their favourite games, rather than embracing new sequels or fangames that reference only the aesthetic of the original title:

Sure, you can use tools to create new games and you can execute very similar concepts to what hacking an existing game would allow you to do. You could create similar game worlds and have similar puzzle designs. You might even have more creativity in what you can do because there's better tools.... But what you can't recapture is the original

game mechanics. The fluidity of just how you control Link and the items there are and the depth it has. And I think that's why people want to recreate and replay these hacks – they have the nostalgia for the original game and they enjoyed it so much and they want more of it.

Owen goes on to discuss how this loyalty towards *A Link to the Past*'s gameplay is one of the reasons that videogame hacks of the title seem to gain more traction than fangames. He recounted to me the development of *Mystery of Solarus DX*, an impressive *Zelda* fangame that carefully mimicked the overall experience of *A Link to the Past* using a custom-built game engine (“The Legend of Zelda: Mystery of Solarus DX”). Despite its high production values, Owen claimed that *Solarus* failed to reach the same audience of many “objectively worse” *A Link to the Past* hacks. “People enjoyed them more because they’re replaying *A Link to the Past* in a new way that they wanted,” Owen explained. “They don’t want different, they want more of the same.” Interestingly, this love for the code also extends to glitches — a fault or mistake in a videogame’s code that makes its way into a title’s final release. Veetorp, another member of the *Randomizer* team, mentioned that the team based their hacking work around the Japanese 1.0 version of *A Link of the Past* specifically because “there’s certain glitches that allow speedrunners to move faster, such as item dashing, spin speed, and fake flipping” that were patched out in the North American releases and re-releases. In essence, the *Randomizer* community is not only altering *A Link to the Past* in unintended ways, but is also embracing aspects of the game’s code that were never intended to be included in the game in the first place.



Fig 1. Screenshot from: *A Link to the Past Randomizer*. alltpr.com/en. Accessed 15 May 2019.

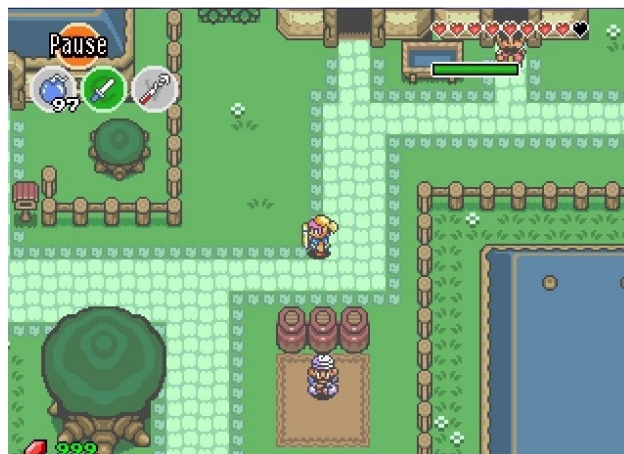


Fig 2. Screenshot from: *The Legend of Zelda: Mystery of Solarus DX*. “The Legend of Zelda: Mystery of Solarus DX.” Solarus Wiki, wiki.solarus-games.org/doku.php?id=zelda_mystery_of_solarus_dx. Accessed 15 May 2019.

This love for a game’s movement is perhaps best exemplified in *Project M*. A modification of the 2008 fighting game *Super Smash Bros Brawl* for the Nintendo Wii — the third entry in Nintendo’s popular *Smash Bros* franchise — *Project M* was developed by a community of *Smash Bros* fans known as the Project M Development Team (PMDev) between 2010 and 2015. I spoke with one of the core members of the PMDev, David Shayne, and he described how many of the project’s contributors shared a dislike for how the series had progressed from the 2001 Nintendo GameCube title *Super Smash Bros Melee* to its direct sequel *Brawl*. Shayne was critical of the slower-paced gameplay of *Brawl*, as well as its inclusion of chance-based elements, noting that these changes had made the game less attractive to its vibrant competitive community:

Melee was very popular, and it had all of the mechanics that people fell in love with.

Then *Brawl* came out and it completely shattered the competitive scene because it flipped *Melee* on its head. It said “no you can’t really be competitive anymore, there’s tripping”

and it just ruined a lot of people's taste in the upcoming *Smash Bros* games. So, we wanted to take what it had and bring *Melee* into it.

In a sense, Shayne and the rest of the PMDev team desired to alter the sequel of one of their favourite games to better match the gameplay and mechanics of its predecessor. These changes included everything from the removal of randomized elements, to single-frame adjustments in the timing of character attacks, resulting in a *Smash Bros* game that played like *Melee* while embracing carefully curated aspects of *Brawl*. Although the scope of the game eventually expanded beyond this mandate — Shayne noted that “as we went on, we realized that *Melee* is not this sacred cow” — *Project M* helped fill a void for players who felt let down by the direction in which Nintendo had taken the franchise. The final iteration of the mod was downloaded over 60,000 times (“Download Project M”), and *Project M* was (and still is) featured at many of the biggest *Smash Bros* tournaments, despite its status as an unofficial installment. “We kinda just got accepted into tournaments,” noted Shayne. “*Smash* is grassroots and we don't have sponsors, so it didn't really matter that we were playing a hacked version of the game because we didn't have sponsors anyways.” Much like with the aforementioned examples of *Super Mario 64* and *A Link to the Past*, a love for the code provided a strong motivation for fans to alter a videogame to better suit their desires as players.

Community and Collective Intelligence

A common thread that runs through the *Link to the Past Randomizer*, *Project M*, and several other videogame fan communities is a rejection of certain corporate philosophies in which older games are pushed aside in favour of newer, ostensibly better releases. The *Zelda* series is an excellent example of this pattern, featuring once-a-console-generation entries that are typically advertised as being bigger, better, and more advanced than their predecessors. I would

consider this release pattern as part of Green's and Jenkin's prohibitionist model, in which engagement with older games is dissuaded through a lack of continued developer support and various legal protections that limit how games can be shared and archived. However, as Henry Jenkins points out in *Convergence Culture*, fans are often quick to "reject the idea of a definitive version produced, authorized, and regulated by some media conglomerate" (261) and may gravitate towards particular entries or aspects of a franchise that resonate with them, regardless of what a corporation directs them to consume. In the case of videogame hacking, this often manifests as a desire to "stay with" a game long after its commercial shelf life has lapsed, or finding new ways to interact with a title that may not entirely align with the intent of the original developers. Although this effort can certainly be a solo endeavour, Jenkins notes that the Internet has facilitated the formation of innumerable knowledge communities centered around popular media franchises. In addition to allowing fans to share their general enthusiasm for a franchise — which could range from a single film to an enormous transmedia property — these virtual communities have the ability to "leverage the combined expertise of their members" (Jenkins, *Convergence Culture* 27) to various ends. Jenkins emphasizes that this expertise often manifests as a pooling of knowledge about a media property, sourced from both official releases as well as fan discoveries, theories, and interpretations. Generally non-corporate ventures, these fan communities are "free of the commercial restraints that surround the source texts, they gain new freedom to explore themes or experiment with structures and styles that could not be part of the 'mainstream' versions of these worlds" (Jenkins, *Convergence Culture* 180). In a sense, these collective intelligence communities connect fans with one another and allow them to change and build-upon their favourite media properties.

I found it tempting to simplify the formation of such videogame hacking knowledge communities as a two-step process in which: 1) computer savvy videogame fans find each other online, and 2) these fans pool their knowledge to begin hacking videogames. However, several of my participants noted that their experiences were far more complex and often began with fan activities other than hacking. Chris Owen from the *Link to the Past Randomizer* development team, for example, noted that before he became an active videogame hacker he was a speedrunner and a puzzle racer for *The Legend of Zelda: A Link to the Past*. Having been a fan of the game when he was younger, he eventually picked up a copy of the Game Boy Advance remake and began playing it through it over and over again. “After I completed it a couple of times, one time I decided - I wonder how fast I can beat this?” Owen recounted, eventually becoming aware of like-minded individuals through the SpeedDemosArchive (SDA) in 2010. After spending six months watching speedruns online, he established his own streaming setup in order to improve and share his experiences with the community:

Since that day I’ve kinda grown to be one of the community leaders of *Link to the Past* speedrunning. I’ve driven my time down, learned so much about the game, been involved in marathon/relay races, created a lot of different puzzle challenges that people have raced and then, when the Randomizer came around (I think it was March 2016), I was just so ready for that!

In addition to connecting him with a community of *Zelda* speedrunners, Owen’s involvement with various *Zelda* fan activities allowed him to accumulate a great deal of gaming capital. Mia Consalvo proposes the concept of gaming capital in her 2007 book *Cheating: Gaining Advantage in Videogames*, likening it to Pierre Bourdieu’s cultural capital and describing it as a fluid type of currency that is gained through knowledge and experience with a game (4).

Consalvo notes that “game players possessed of the proper kinds of gaming capital — for their own gaming circle — are powerful in the sense that they can often dispense advice with confidence, are looked to as experts in some way, and can, through their behavior in game, enhance or reduce opportunities for others” (Consalvo, *Cheating* 123) In Owen’s case, his vast pool of knowledge for *A Link to the Past* allowed him to become a leader in the *Zelda* fan community, the speedrunning community, and eventually the *Randomizer* community. Reflecting on this accumulation of knowledge, Owen noted that “rather than hacking the game itself, I was building up this huge knowledge of what is possible in the game itself and the game mechanics.”

Both Chris Owen’s personal experiences and the history of the *Link to the Past Randomizer* are entangled with speedruns and other types of alternate play — activities that Stephanie Boluk and Patrick LeMieux would likely consider types of metagaming. In their 2017 book, *Metagaming: Playing, Competing, Spectating, Cheating, Trading, Making, and Breaking Videogames*, Boluk and LeMieux define metagames as unprecedented experiences and effects that emerge in, on, and around videogames, and discuss their ability to “reveal the alternate histories of play that always exist outside the dates, dollars, and demographic data that so often define videogames in industry magazines and encyclopedia entries” (9). Specifically referencing the original *Mario Bros* for the NES, the pair detail how the famous plumber has been “manipulated, duplicated, generated, appropriated, and aggregated across dozens of unique practices and diverse material platforms as players grow bored with the standard challenges and begin to game the limits of the software itself” (Boluk and LeMieux 182). In the case of *A Link to the Past*, the game’s knowledge communities both explore the technical limits of the *A Link to*

the Past and the Super NES through hacking, while pushing the limits of game mastery through speedruns and puzzle races.

The Legend of Zelda: A Link to the Past by ChrisOwen #8

Defeat Agahnim 1 with the Master Sword equipped

Open 11 Big Chests Obtain 11 Compasses Open Mysterious Chest

YOU MAY NOT USE ANY ITEMS/WEAPONS ON MORE THAN ONE BOSS
YOU MAY NOT ENTER THE WITCH'S POTION SHOP
YOU MAY NOT OBTAIN MORE THAN ONE BOTTLE

You may only obtain the following items/weapons when the listed criteria is met

Crystals: 2 Pendants	Ether Medallion: 3 Crystals	Ice Rod: 6 Crystals
Super Bomb: 3 Pendants	Lanmolos' Pendant: 4 Crystals	Bug Net: 7 Crystals
Tempered Sword: 2 Crystals	Fire Rod: Visited Fat Faerie	Magic Cape: 20 Hearts

You may only use the following items on bosses when the listed criteria is met

Fighter's Sword: 1 Crystal	Regular Bow: 3 Medallions	Bombs: 5 Crystals
----------------------------	---------------------------	-------------------

NO EXPLORATION GLITCH OR JAPANESE 1.0 GLITCHES

Fig 3. Puzzle Race #8 from: Chris Owen. *Puzzle History*, pastebin.com/UYHrG032. Accessed 15 May 2019.

Puzzle races are a particularly intriguing set of metagames for the *Link to the Past* community, as they serve as a predecessor to the *Randomizer* itself. Whereas the *Randomizer* imposes a series of challenges by manipulating the game's code to rearrange key items and objectives, a puzzle race instead focuses on an unaltered version of *The Legend of Zelda: A Link to the Past* and asks the player to impose restrictions upon themselves as they play. In the puzzle race featured above, created by Chris Owen in 2012, players are directed to avoid several key items until much later than the game intends, and may only use certain weapons (the fighter's sword, the bow, and bombs) when specific criteria are met. "It's a challenge that requires you to not necessarily beat the game but complete other objectives with limitations on what you can do or what can't you

do,” Owen noted, further elaborating that he created “over 50 puzzle races” for the game which gradually grew in creativity and complexity as he became more familiar with the title.

In *The Well-Played Game*, Bernard De Koven describes these sorts of these community-oriented changes as sometimes being necessary to maintain interest in a particular game (52). He notes that if a game is no longer being “played well” by its community — and if a shared desire for change has been openly expressed its members — then modifying its rules can help reinvigorate the play community:

The [game] you’re playing is no longer giving you enough of a challenge for you to feel you want to play it well. You can play it well, but you’re losing interest. Your gaming mind is bored. You’re not playing the way you want to be playing. Or, vice versa, you can’t play it well, the challenge is too big, your playing mind is overwhelmed, the game is too hard. The general purpose for changing a game, therefore, is to restore equilibrium. (de Koven, 53)

Puzzle race communities follow a similar philosophy to what De Koven proposes, looking for ways to change their approach to *The Legend of Zelda: A Link to the Past* to counter a potential stagnation of play. De Koven mentions that this does not simply manifest as adding new features or rules to game, and may mean letting go of certain elements — “In order to maintain the play community as well as the game, we have to give up a little of our commitment to the game” (33). For puzzle races, this can mean shirking the linear structure of a title and even skipping parts of the game entirely. The *Randomizer* builds upon this set of self-imposed rules by enacting tangible changes upon the game itself, meaning the play community must also accept that the game will be altered at the code level to facilitate this new type of metagame. In either case, these changes provide an avenue for experienced players to re-engage with a decades old title

that they have extensive knowledge about but may no longer challenge or intrigue them.

Elaborating on this idea, Chris Owen explained how these activities require “knowledge of the game and some creative puzzle solving solution – that’s the essence of *Randomizer*, that every time you play it through it’s a different experience and you’re tackling the game in a different way, solving the game in a different way, with different items.” Both puzzle races and the *Randomizer* provide a method for players to simultaneously diffuse their game mastery and build upon their vast knowledge of *A Link to the Past*, facilitating endless replays and creating an avenue for the generation of gaming capital.

Improvement, Creativity, and Media Archaeology

As I mentioned earlier in this chapter, one of the motivations commonly expressed by my participants was a desire to engage in amateur media archaeology and archival practice. Many videogames, especially those that exist on cartridges and other difficult-to-scrutinize formats, contain content that was either explicitly cut from the official release or simply leftover from early iterations of the game. This content exists in a sort of purgatory — present on almost every game but generally inaccessible due to its separation from the game’s playable content. Thus, after gaining access to an editable version of a videogame (such as a ROM image or an accessible file structure), the first step for many hackers is evaluating what is housed within a given game, how it is laid out, and if there is any content that was not accessible in the commercial release. Before talking directly about media archaeology, I would like to return to Jansz and Theodorsen for a moment to discuss how this discovery process ties into their definitions of improvement and creativity. The pair describe how “acquiring detailed information about a game and its technical aspects” is an integral part of modding, and documenting a game’s ROM image or file structure also facilitates further hacking practice. Using ROM

hacking as an example, this often involves the creation of a ROM map — essentially, a linear breakdown of a data stored within a ROM image that points to where certain assets (such as text, animation, and music) are stored, based on hexadecimal addresses. Although it is quite rare for a ROM map to be fully comprehensive, this mapping allows a hacker to change various aspects of a game by locating and editing sections of code. Veetorp, one of the developers of the *Link to the Past* randomizer, notes that despite the game’s popularity it “still has some blind and mystery spots” and that a lot of experimental work is needed to make complex changes. Despite this incompleteness, this documentation process lays the groundwork for future technical work.

As elaborated by my participants, this future work usually falls along two lines: the enhancement of a game itself, by tweaking or adding features, and the creation of new tools that allow users to edit various parts of a game. For the *A Link to the Past* hacking community, one of the key ways in which they tried to improve upon the title was by expanding the size of the ROM image. An enormous hurdle facing ROM hackers is that there is little-to-no space in a ROM image for adding new graphics, music, text, or other assets. The simplest hacks usually involve an in-line tweak (such as changing a single value in a hex editor) or an equivalent exchange (such as swapping out one graphic for another of the same size). Simply inserting new content into the ROM, without making space for it, will push existing content out and may even irreparably corrupt the title. Axel Hellström, one of the *Randomizer*’s developers, mentioned that “basically the very first thing I did was to expand the ROM from one megabyte to two,” allowing much greater flexibility during the hacking process. Instead of being limited to replacing or re-arranging elements with *A Link to the Past*, hackers were free to add to the existing game with whatever new content they wished, such as new graphics and text. Hellström also explained that this improvement extended beyond the alteration of a single ROM file and to the tools that

videogame hackers had created to edit them. Reflecting on the popular hybrid emulator/debugger bSNES, he speculated that the hackers had created a tool that was more robust than anything even the original development team had access to:

It's better than anything Nintendo had when they made the game. So I feel like for a Super NES title, I don't need anything more complicated than that. I already have a tool that is substantially better than anything the original dev team could have ever imagined.

This desire to push the limits of a system hearkens back to aspects of Gabriella Coleman's overview of hacker ethic: "the very nature of hacking — turning a system against itself — is the process of using existing code, comments, and technology for more than what the original authors intended" (98). When I spoke with ZeaLity, staff member at the *Chrono Compendium* and one of the lead developers of the *Chrono Trigger: Crimson Echoes* ROM hack, he detailed that there is a certain joy and creativity attached to pushing the limits of decades old hardware. "When you do clever things that technically would have been possible on the Super Nintendo console, that the developers themselves didn't do, it's just this eureka moment," he explained, specifically mentioning how Kajar Laboratories had grafted features onto *Chrono Trigger* sourced from the title's Playstation sequel *Chrono Cross*. By co-opting elements from a game that, by most technical evaluations, would be considered far more advanced than its predecessor, ZeaLity felt they had "pushed the Super Nintendo hardware and this game's programming past what it was intended to do!" Through developing new tools and enhancements to their respective games, both Hellström and ZeaLity felt that they had improved upon their prospective titles at a technical and creative level.

Sifting through a game's content is not entirely focused upon these future technical exercises, however, and may take on some archaeological traits. For many videogame hackers,

there is a certain joy to simply unearthing and documenting previously inaccessible content within a given title. Reminiscing about his first forays into the Internet in the late nineties, ZeaLity described his time at the Inside The Web *Goldeneye 007* forums and the amount of speculation that circulated amongst the forum-goers about the N64 game's content, cheat codes, and development history. "People could make any outlandish claims they wanted to and you couldn't effectively dispute them," ZeaLity recounted, noting that there simply was no way to delve into the game's code back then to verify the truth behind theories. As an example, there was much fan speculation about the inclusion of a hidden "All Bonds" mode in *Goldeneye 007* that allowed players to select Sean Connery, Roger Moore, and Timothy Dalton as their in-game avatars. It was not until 2005, when a *Goldeneye 007* ROM editor was created and released, that hackers were able to verify that "the All Bonds faces and suits are still in the game; Rare had only removed the ability to use them" ("All Bonds Cheat"). Presumably the casualty of a prohibitively expensive licensing agreement, the hackers had finally settled a nearly decade-long debate about the existence of the cheat. Of course, this amateur archaeology is not entirely focused on dispelling Internet rumours. ZeaLity noted that in the late 90s and early 2000s there was a growing interest in finding and dissecting unreleased versions of games to better learn about their development history. He specifically mentioned stumbling upon a *Sonic the Hedgehog 2* fan community that was hacking a beta version of the game in search of previously unseen content:

Their process of exploring was exhilarating: "Oh my goodness, this was never intended for release!" We might find different graphics, we might find a different level like the Hidden Palace zone.... people should actually dig into these games!

For many hackers, this discovery of new content leads them toward documentation and archival

practices. ZeaLity described the creation of the Chrono Compendium as a way to provide a home for both fan works and the content unearthed from videogame hacking, “just to keep found things found.” The Compendium is not alone in its efforts, with like-minded communities such as The Cutting Room Floor serving as repositories for “content never meant to be seen by anybody but the developers” (“Welcome to the Cutting Room Floor”). These amateur archives are places where videogame hackers can leverage their collective intelligence to learn and share information about the inner workings and development histories of their favourite games.

Despite originating in a different medium, there are many parallels between the communities formed by these amateur videogame archaeologists and those created by particularly dedicated fans of the television program *Survivor*, as documented by Henry Jenkins in *Convergence Culture*. *Survivor* pits sixteen strangers against each other in a competitive “stranded on an island” scenario, with one member getting voted off each week until only a “sole survivor” remains, who wins a large cash prize. Speculating about who will get voted off each week is common activity amongst viewers, but some fervent fans have formed virtual “spoiler” communities — going to “extraordinary lengths to ferret out the answers” (Jenkins, *Convergence Culture* 25) to who will get voted off and in what order. Like the videogame hackers described above, these fans carefully scrutinize their favourite media in search of information that may have been accidentally or incidentally left behind by the program’s producers:

They use satellite photographs to locate the base camp. They watch the taped episodes, frame by frame, looking for hidden information. They know *Survivor* inside out, and they are determined to figure it out — together — before the producers reveal what happened. (Jenkins, *Convergence Culture* 25)

Jenkins notes that these spoiler-seekers are engaged in “an adversarial process — a contest

between the fans and the producers, one group trying to get their hands on the knowledge the other is trying to protect” (43). With *Survivor*, the producers of the program have engaged in everything from “disinformation campaigns trying to throw smoke in viewers’ eyes” (Jenkins, *Convergence Culture* 25) to enormous fines directed at “cast and crew members if they get caught leaking the results” (Jenkins, *Convergence Culture* 25). With videogame hacking, this type of control often manifests as a “tight controlled system of technological and licensing constraints” (Consalvo, *Atari to Zelda* 41) that limit when, where, and how players gain access to a game. In *Atari to Zelda*, Consalvo notes players are usually at the mercy of such decisions and are “able to influence design or production only through the basic act of purchase” (41). In both *Survivor* spoiling and amateur videogame archaeology, fans push back against creator control by forming virtual knowledge-sharing communities. Members of these communities leverage their combined expertise and make “voluntary, temporary, and tactical affiliations” (Jenkins, *Convergence Culture* 27) in order to acquire knowledge that producers, developers, and other media creators have secreted away — whether that information is spoilers about the outcome of a television series, or development materials that were never meant to be unearthed.

In the second chapter of *Atari to Zelda*, Consalvo discusses another way that ROM hackers acquire videogame content that was never meant to be available to them: translation projects. It is fairly common practice in the Japanese videogame industry to refrain from releasing particular titles in North America due to either economic or localization concerns, and translating these titles is a long-standing videogame hacking practice. A commonly-cited example of this sort of work is *Mother 3* — the third entry in the *Mother* series (known as *EarthBound* in the West) — which was released for the Game Boy Advance in 2006 in Japan, but never made its way overseas (Consalvo, *Atari to Zelda* 58). Similar in fashion to how the

Goldeneye 007 fan community pooled their resources to discover unused content within the game's ROM image, the *EarthBound* fan community Starmen.net acquired a Japanese ROM image of *Mother 3* and, over the course of two years, translated the entire game into English. Team members were responsible for creating new hacking tools to access ROM data, reworking the game's fonts to accommodate English characters, and translating over 1000 pages of text ("Mother 3 Fan Translation Patch Notes"). Although Jenkins may describe this as an adversarial struggle with the game's original creators (i.e. making unauthorized changes to a videogame and translating it into unintended languages), Consalvo notes that the *Mother 3* translators felt their practice was a benevolent one. Claiming that the project was only made necessary by the absence of an official translation, the team hoped that their efforts would open up a dialogue about the legitimacy of fan translation while allowing fans to play a game that would otherwise be unavailable to them (Consalvo, *Atari to Zelda* 59). Regardless of how Nintendo may feel about the translation project or the possibility of an eventual official *Mother 3* localization — something they have been notoriously evasive about — the possibility space that these sorts of hacks open up is intriguing. Consalvo notes that "translation hackers transform particular Japanese games into hybrids — somewhat Western and somewhat eastern in their expression" (Consalvo, *Atari to Zelda* 64), while also laying the foundation for future hacking work. These translation projects are vital in building knowledge communities, creating new tools and raw materials for hackers to engage with, and challenging geographical strategies of control laid out by media companies.

Hacking for Fun and Profit

Jenkins speculates that an additional motivation that *Survivor* spoiler-seekers have for participating in these knowledge communities is that "it allows them to exercise their growing

competencies in a space where there are not yet prescribed experts and well-mapped disciplines” (Jenkins, *Convergence Culture* 52). Noting the experiences of one of his interviewees, Shawn, Jenkins recounts how he was able to apply the investigative and fact-checking skills he developed during his undergraduate history degree to the spoiling process (53). Since the growth of videogame archival standards has not matched pace with the boom of the videogame industry, many hackers have utilized websites such as The Cutting Room Floor and the Chrono Compendium as platforms to experiment with amateur archival and archaeological practice while developing skills that simply cannot be learned elsewhere. Hector Postigo expands this idea to commercial contexts in *Debugging Game History*, noting that many of the earliest hackers leveraged an interest in games and coding to alter existing videogames, learning game design fundamentals at a time (the late 90s and early 2000s) where there simply were not schools or programs that catered to the practice (Postigo, “Modification” 319). He goes on to explain how modification and hacking can be considered an entry-point practice, serving as a “testing ground for burgeoning designers, who may have little or no institutional training in design or computer programming but who, through their communities of practice, learn the craft of their possible profession” (Postigo, “Modification” 325). Tied into Jansz and Theodorsen’s motivation of self-marketing, the creation of mods and games in order to contribute to one’s portfolio (9), both hacking and modding can be viewed as ways to learn about game design and find alternative pathways into the videogame industry. Although the potentially illicit nature of hacking imposes certain barriers — would a videogame hacker, for example, be comfortable showing a finished project to a potential employer? — many of my participants listed their aspirations to work in or around the videogame industry. It seemed natural for them to transition from fan, to hacker, to professional developer.

Adam, the creator of the *Pokémon Prism*, recounted that the videogame hack was “mostly made for game development practice” and that he saw it as a potential portfolio piece for job applications. Even after receiving a cease and desist order that halted completion of the hack — one that gave the title a certain level of notoriety — he noted that the project still granted him some cachet in the games industry:

A lot of people I know in the videogame industry were actually impressed by [*Pokémon Prism*]. Originally, I was not going to put it on my resume but people, actually from the industry working on AAA games, said it was a good idea and it would only help my resume. So, I did just that. It’s gotten me a lot of connections, contract work, and possibly the job I have right now.

David Shayne from the PMDev team expressed similar motivations for involving himself in videogame hacking and modding — “I always wanted to work in videogames, so this was a perfect break for me because I love *Smash Bros.*” Shayne noted that he would often include *Project M* on his resume when applying for game design jobs, but lamented that “after *Project M* ended I got a very sour taste in my mouth and I really didn’t want to continue with game dev anymore.” He was quick to point out, however, that other *Project M* contributors had made their way into the industry in some fashion: “A lot of our team has actually gone on and worked on their own games,” he explained, specifically pointing out that the indie studio Wavedash Games was formed by former PMDev team members. The studio’s first game, *Icons: Battle Arena*, shares more than a few similarities with *Project M*, particularly in terms of the game’s physics and how the characters move (Boyd). Following the dissolution of *Pokémon Prism*, Adam followed a similar path, focusing his efforts on creating *The Wu Xing* — an original title that shares thematic and mechanical elements with *Pokémon* while shedding any trace of Nintendo’s

intellectual property:

I'm working on a new game right now. It's a monster game — not Pokemon — so it'll be my own IP so I can do whatever I want with it. I don't have to develop Prism anymore (laughs) and I can move on with my life and develop my own original monster project.

In both these cases, videogame hacking served as a stepping stone into professional ventures by allowing hackers to practice game design skills outside of academic or professional environments. Despite the legal complications brought forth by the unauthorized nature of this work, it provided the hackers a level of freedom in development. They could alter whatever game they like, in any way they like, providing they had the required resources, skills, and free time to make the changes.



Fig 4: Screenshot of *Icons: Combat Arena* from: Pascu, Blaine. “EVO Hilight - Icons: Combat Arena by Wavedash Games.” *Unity Blog*, 16 July 2017.



Fig 5. Concept Art for *The Wu Xing* from: @TheWuXing1. “Here's the first finished monster design! It was done by @RacieBeep and she will continue as the lead monster artist & designer for The Wu Xing!” *Twitter*, 2 Jan. 2019, 8:34 p.m., twitter.com/TheWuXing1.

However, framing videogame hacking as merely a training ground or portfolio builder for future employment would not be entirely accurate. Videogame hackers are already profiting through the practice itself, ranging from meagre transactions within fan communities to full-time employment. Kaze Emanuar elaborated on the former, explaining how *Super Mario 64* hackers would often commission other community members to complete specialized tasks:

There are many people who offer to transcribe songs to the Mario 64 format for money, which is interesting... but the pay is absolutely miserable! Like, sometimes for three hours of work the people will take only like three dollars.

Lamenting the low wages of this fan labour, Kaze noted that social media channels can be a more viable method for monetizing videogame hacking. Despite a short interruption at the hands of Nintendo, Kaze's Patreon now pulls in roughly \$300 a month ("Kaze Emanuar is creating YouTube videos") and his YouTube videos receive hundreds of thousands of views. "I'm not starving or anything and I'm doing fine with a bit of ad revenue," Kaze explained, stating that he considers hacking to be his full time job (despite also being a college student). Axel Hellström, one of the lead developers for the *Link to the Past Randomizer*, mentioned that his Twitch broadcasts have seen similar levels of support. During his development streams, in which he experiments with various types of game hardware and software, viewers have gifted him Everdrives and other types of gaming technology. Despite this generosity, Hellström noted that streaming is more of a hobbyist pursuit, and that he "already [makes] money hacking *A Link to the Past*" as a developer for Crowd Control, a Twitch extension created by Warp World. Crowd Control allows viewers to exchange Bits — a virtual good that can be bought through Twitch — for Crowd Control Coins, which can be spent to help or hinder a streamer's progress through a title ("Crowd Control: Frequently Asked Questions"). For example, a benevolent viewer may

grant Mario a few seconds of invulnerability when fighting a boss monster in *Super Mario Bros 3*, while a sadistic one may choose to spawn additional enemies to hinder his progress.

Regardless of a viewer's intentions, the Crowd Control team makes the entire process possible by moderating the interaction between a ROM image (supplied by the streamer), their own custom designed intermediary software, an emulator, and Twitch itself. "We're actually the number one Bits extension on Twitch," Hellström noted, with the company turning a profit by taking a 20% commission on Bits that are spent during each stream. In essence, Warp World has found a way to monetize videogame hacking by reworking a variety of popular videogames and embracing the enthusiasm that Twitch streamers and viewers hold for them. Much like with the *A Link to the Past Randomizer* and many of the other hacks discussed in this chapter, many fans wish to see their favourite games tinkered with and iterated upon in perpetuity — something that Crowd Control is more than happy to accommodate.

Conclusion

As my field research approached its conclusion, I decided to reach out to an online acquaintance of mine: independent game developer and *EarthBound* hacker Max Ponoroff. A fellow member of Starmen.net's hacking community, Ponoroff created the popular *EarthBound* hacking tool CoilSnake and has contributed to numerous projects since he first came to the practice in the late nineties. After spending nearly two decades engaged in videogame hacking, while simultaneously pursuing a career as a professional software engineer, Ponoroff decided to form Createdelic Inc in order to develop the independent videogame *Starstruck: A Music Adventure Game*. Although much of his hacking has fallen to the wayside in the wake of his entry into professional game development, many traces of his former work can be gleaned from *Starstruck*. The game draws much inspiration from *Edwin & Jones*, an incomplete *EarthBound* hack that Ponoroff created with many of the same themes in mind. As someone who has hacked videogames, created development tools, and transitioned into professional game development, I felt Ponoroff could provide a unique perspective on the practice.



Fig 1. Work-in-progress screenshot of *Edwin & Jones* from: Edwin & Jones. web.archive.org/web/20170323092021/http://edwinandjones.com. Accessed 15 May 2019.

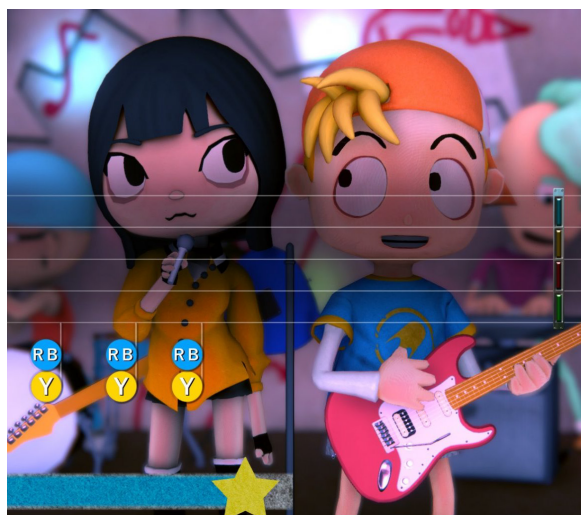


Fig 2. "Starstruck: A Music Adventure Game - Trailer." *YouTube*, uploaded by Starstruck, 17 Dec. 2018, [youtube.com/watch?v=TmIWH2E675M](https://www.youtube.com/watch?v=TmIWH2E675M).

Although this was certainly the case, our conversation quickly transformed into a shared recounting of Starmen.net's history. "It feels weird that I'm telling you this when you're part of the community," laughed Ponoroff, as we began chatting about how he first stumbled upon the fansite while he was in middle school. I found myself chuckling as well, as many of his anecdotes about his early introductions to videogame hacking mirrored my own. Upon discovering Starmen.net, we had both sought out ways in which we could prove ourselves to the established community members. "You want to impress these people doing cool stuff, right?" explained Ponoroff, detailing how he integrated himself by learning the practice inside-out. Much of his early focus was centered around the cultivation of programming skills — learning Java, developing hacking tools, and discovering what was possible within *EarthBound*'s ROM image — and filling areas of need within the hacking community. Due to my lack of programming skills, and a general reluctance to develop them, I found myself taking a slightly different path. Where Ponoroff focused on improving his technical skills, I instead relied upon existing tools and expertise to facilitate my various hacking projects. Regardless of how our approaches differed, as we became established members of the community we eventually found ourselves working toward very similar goals. Both of us became leaders on ambitious *EarthBound* hacking projects — *Edwin & Jones* and *HyperBound*, respectively — with the hopes that we could construct something truly unique within the framework of an existing videogame, and perhaps even translate that success to work in the games industry.

However, this closing interview does serve a purpose beyond just reminiscing with an old online friend. My conversation with Ponoroff allowed me to reflect on the research questions that lay at the heart of my thesis while exploring my own presuppositions about videogame

hacking. I found Ponoroff's perspective on the labeling of the practice particularly illuminating, as much of my early research grappled with the various words — such as modding, hacking, and sampling — that have been used to describe the alteration of videogames. In addition to acknowledging the heterogeneity of the practice, Ponoroff suggested that many of these labels are rooted in a specific time or place rather than an absolute set of values. He compared them to weather phenomena and how they may be classified in different regions of the world:

A typhoon and a hurricane may be the same thing, right? But they call it a hurricane if it is in the west, and they call it a typhoon if it is in the east. That's why you never hear about hurricanes in Japan, you only hear about typhoons... So, for me, stuff that started around the 2000s would be called ROM hacking, because that's just what we called it back then. But stuff you do nowadays is called modding because that's what people call it now.

Ponoroff's meteorological metaphor recalled one of the earliest realizations of my research — that videogame hacking is not a singular activity with a precise set of rules. Many of my participants would switch between terms such as modding, hacking, and remixing freely as they spoke about their latest project, showing little care for the popular or academic connotations that each word held. Others tactically adopted terms in an attempt to frame their practice in a better light, with Ponoroff himself admitting that he referred to his own work as modding on his website “because of the negative implications around the word hacking.” Even those whose goals and techniques seemed to line up perfectly, such as Adam's and ZeaLity's attempts to develop new entries in existing videogame franchises, held conflicting viewpoints on how their practice should be described. As expected, my initial working definition of videogame hacking

(i.e. unsanctioned projects that edited a game's code in unexpected ways) was continuously challenged by those who engaged in the practice themselves.

The creation of an authoritative definition of videogame hacking makes for an interesting thought exercise — and is certainly something that I toyed with during the reflective writing portions of my research — but it was never the ultimate goal of this project. As I expressed in my methodological framework, my expectation was that this study would offer forth a fragmentary, experimental, and thoroughly partial perspective on videogame hacking practices and subcultures. Ien Ang notes in *Living Room Wars: Rethinking Media Audiences for a Postmodern World* that “ethnographic work, in the sense of drawing on what we can perceive and experience in everyday settings, acquires its critical mark when it functions as a reminder that reality is always more complicated and diversified than our theories can represent, and that there is no such thing as 'audience' whose characteristics can be set once and for all” (110). Thus, my broad preconceptions about hacking practices and communities slowly made way for an diverse array of (sometimes conflicting) knowledge generated through my methods: interviews, textual analysis, and reflective writing. The landscape of videogame hacking is far too complex for me to fully summarize or encapsulate, but my hope is that this research has successfully identified some common threads that weave their way through practice.

A Review of Common Themes

Despite my hesitance to neatly place videogame hacking in the broader history of computer hacking, it was hard to ignore how many of my participant's experiences hearkened back to accounts written by both Steven Levy and Gabriella Coleman. When asked about his own introduction to videogame hacking, Ponoroff mentioned that entering into Starmen.net's hacking community came with a bit of an initiation process. Community members were friendly

and shared information readily, but only after he had “put in the effort” by scrounging through documentation and acquiring a certain level of proficiency with both *EarthBound* and its established hacking tools. Ponoroff felt pressured to prove his skills and show he was serious about hacking, mirroring the meritocratic tendencies of many computer hacking subcultures in which “no credential, qualification, or superficial characteristic is more important than a person’s practical computer skills” (Levy 31). This sentiment was echoed by several other participants, who cited a similar need for expertise that ranged from practical computer skills to gaming capital that could only be acquired through extensive experience with a title. Perhaps best exemplified through the formation of the *Project M* and *Zelda Randomizer* development teams, members of videogame hacking communities are often required to acquaint themselves with a game as a player — who has gained knowledge about a game’s logic, physics, and mechanics through repeated play — and a programmer, who understands the game’s underlying structures through technical inquiry. This type of expertise is not exclusive to hacking knowledge communities, however, as Chris Owen was quick to point out the overlap between hacking, speedrunning, and the puzzle races he created for *The Legend of Zelda: A Link to the Past*. In many ways, this accumulation of technical knowledge and gaming capital has created a space for both videogame hacking and forms of alternative play, through the development of specialized knowledge communities within broader fandoms.

This emphasis on technical expertise and game mastery seems to invariably lead to legal tensions between videogame hackers and media companies. Whether for the purpose of alteration or media archaeology, the practice often requires the acquisition and dissection of games, potentially violating intellectual property law and technical protection measures in the process. Despite how rarely it may occur, the impact of cease and desist orders and other legal

action on the outlook of videogame hackers cannot be overstated. The tactics deployed by of some of the earlier ROM hacking projects, such as the ill-fated *Pokémon Prism* and *Chrono Trigger: Crimson Echoes*, have been revised and reconsidered as hackers attempt to find cracks in the prohibitionist strategies laid out by media companies. Reflecting on his 2009 cease and desist order, ZeaLity surmised that surprise and anonymity should be a hacker's best friend, as that even well-established methods such as patch files may not provide protection against Nintendo's or Square Enix's vast legal resources. Despite these types of warnings, some hackers have chosen to go public, as demonstrated with the *A Link to the Past Randomizer*'s browser-based online ROM patching system. Others, such as *Super Mario 64* hacker Kaze Emanuar, have instead decided to leverage the persistence and anonymity of videogame hacking communities to simply re-upload flagged content quicker than it can be removed through copyright claims. Whether taking an official legal stance or simply finding gaps in the enforcement of laws and policies, videogame hackers are engaged in a fluid power struggle with media companies that wish to control the proliferation and alteration of their games.

Considering these various legal and technical barriers, pursuing videogame hacking in favour of other types of game creation and alteration may seem foolhardy. I suggested as much in my first research question — what motivates game developers to create tools and hacks that are undistributable through commercial markets and are at constant risk of legal action? No single answer could satisfy such a broad query, but many of my participants expressed similar motives for entering into the practice despite the various tensions found therein. Some were drawn to videogame hacking due to their love for a particular game's code, citing an admiration for a title's unique movement, physics, or logic. The *Randomizer* team embraces this approach, developing methods to play and replay *The Legend of Zelda: A Link to the Past* despite the

existence of numerous sequels, prequels, and remakes. Others viewed videogame hacking as a type of amateur media archaeology, taking joy in exploring supposedly antiquated games in order to unearth new content and learn more about their development history. ZeaLity expressed his delight in uncovering new secrets in *Chrono Trigger*, eventually creating the Chrono Compendium to house this knowledge alongside a vast collection of fan-created works. In addition to these hobbyist approaches, some may also turn their attention to hacking's commercial applications. In addition to taking their learned programming and game design skills and transitioning them into professional game development projects, such as with Ponoroff's *Starstruck* and Adam's *The Wu Xing*, many of my participants pursued other avenues to monetize the practice. Despite some legal disputes with Nintendo, Kaze Emanuar utilizes both Patreon and YouTube as methods for drawing an income from his hacking practice, and Axel Hellström hacks full-time as a developer for the popular Crowd Control Twitch extension. Such a diverse range of motivations results in a vast array of hacking outputs, ranging from long-form narrative hacks to online tournament games, and demonstrates the heterogeneity of the practice.

Research Limitations and Considerations

This research project has several key limitations. First and foremost, the sample size for the study was fairly modest, consisting of eight total participants. My pool of interviewees was smaller than expected for three key reasons. First, I hit many brick walls during the recruitment process due to the inaccessibility of many videogame hackers, who tend to hide their contact information and may be unresponsive through forums and social media. Second, my attempts to use the snowball approach to acquire more participants — through recommendations and referrals from existing interviewees — bore few results. And finally, it took much longer than expected to recruit, organize, and conduct interviews. Many of my participants took weeks (if

not months) to commit to a specific interview time and method, which vastly slowed my research timeline. In addition to the reduced amount of data that these challenges forced, this small participant pool also prevented me from gaining a multifaceted understanding of particular videogame hacking communities. Outside of my communication with the *A Link to the Past Randomizer* development team, I was only able to speak with a single member from the communities I set out to document. Thus, my ability to corroborate accounts and deepen my understanding of groups of hackers, such as Kajar Laboratories and the Project M Development Team, was somewhat stunted. Future studies may wish to consider alternative methods for participant recruitment and data collection, or to focus on building trust with a single community rather than multiple ones.

In addition to being reluctant to speak in the first place, there is a certain level of secrecy that — when coupled with a lack of record-keeping within many online communities — can further complicate the research process. When asked about important past events, such as the termination of *Project M* or the unofficial revival of *Pokémon Prism*, my participants would often leave noticeable gaps in their recollections. Some of this was due to an unwillingness to touch on certain sensitive topic areas — a more than reasonable position when considering the legal implications of their work, but one that left tangible gaps in knowledge. Others lamented that they simply could not recall the specifics of a particular scenario, or that certain information never passed through their hands in the first place. Although sprawling knowledge communities are a strength of these videogame hacking subcultures, they do keep information and expertise dispersed in a way that is difficult to account for. It is entirely possible that some histories will be lost forever due to the ephemerality of websites, archives, forums, and the community members themselves. I attempted to address these gaps by increasing the length of my interviews and

widening the scope of my videogame hack analysis, but I am unsure if it would be possible to entirely recover this type of missing community knowledge.

In addition to the limitations uncovered throughout my research process, I also brought forth my own set of challenges as a researcher with a strong personal connection to videogame hacking. My interviews and analysis were inevitably affected by my own history and biases, manifesting in both positive and negative ways. For example, I am certain that my experiences with videogame hacking, as well as my public persona as a hacker, granted me access to participants that may have otherwise been suspicious of an academic researcher. In contrast, my familiarity with the practice likely affected how I conducted both my interviews and my analysis of videogame hacks — perhaps missing nuances or making assumptions by over-relying on my tacit knowledge. I do believe that it is possible, and oftentimes necessary, to have a connection with fan communities in order to research them, but I still endeavoured to acknowledge this bias in both my thesis and through my reflective writing.

One final important limitation is that this study does not address how videogame hacking practices and subcultures differ across languages and cultures. Only two of my participants were from countries other than the United States (residing in Germany and England) and my research exclusively focused on English-language videogame hacking projects and communities. It was also quite rare for the people I spoke with to be aware of related practices in other countries and languages, and what similarities and differences they shared with their own work. Future studies that explore game alteration practices in other languages and jurisdictions would prove valuable in deconstructing which aspects of videogame hacking may be unique to North America.

Hack to the Future

At the onset of this study, my research questions primarily focused upon the “why” and “what” of videogame hacking. In essence, why do hackers engage in their practice and what are their cultural outputs? As I conducted interviews, analysed various videogame hacks, and became more acquainted with the multifaceted practice, new questions began to emerge. How do videogame hackers continue their practice in the face of legal and technical barriers? How are the words “hacking” and “modding” framed in popular and academic discourses? What do these labels mean to those who actively engage in the practice? How does one go about studying these sorts subcultures — communities of creative labour that exist in the margins of mediamaking and the fringes of the law? And finally, what does it mean to be a researcher who has a personal history with the communities in which he is studying? Although I tried my best to address these queries in the admittedly limited scope of my research, like so many other academics, I found myself with more questions than I could possibly answer. Yet, as I wrap up this thesis, I pose one final question to myself: where can this research go next?

Further ethnographic research on videogame hacking communities could prove valuable as an avenue to expand upon and challenge the findings in this thesis and other related academic studies. Whereas the scope of my study was relatively narrow, focusing mainly on ROM hacking and English-language games that were released in the nineties and early 2000s, the amount of potential participants and research objects was still bewildering. An exploration of how game modification ties into Japan’s dōjin game culture — independent video games or fangames created by hobbyists, usually based on pre-existing material — may prove particularly useful as an extension of this research. Where my thesis documents a tension between fans and media companies in North America, this tension appears to be more diffused in Japanese fan culture. It

would also be worthwhile to consider the afterlife of a single videogame console in the context of both commercial and hacker interests. Building upon the work of existing platform studies, such as Dominic Arsenault's writing on the Super NES, this sort of research could provide a rich account of what happens to a videogame platform and its game library in the aftermath of its commercial shelf life. As demonstrated throughout my thesis, outmoded consoles have seen continued creative interpretation by hackers, as well as sustained monetization by media companies through digital distribution platforms and re-releases. Exploring, in depth, the ways in which a single console can persist decades after its commercial retirement could offer insights to how corporate and consumer interests change over time.

Part of the focus of my research was to create a methodological template, and I believe that my approach could be adapted to facilitate both the study of other videogame hacking subcultures and gaming communities. As I learned throughout my own work, much of this type of research is exploratory in nature. Locating and engaging with ephemeral virtual communities often results in the unearthing of unforeseen revelations, requiring a certain fluidity on behalf of the researcher. Interviews, game analysis, and reflective writing provide a flexible and reflexive foundation for this type of work, allowing researchers to pivot based on the availability of participants and other considerations. Clifford Geertz notes that our understanding of culture grows in short bursts, beginning with a "fumbling for the most elementary understanding" (25) before progressing to supported claims by way of overlapping and repeated studies. Through a repetition of methods, and a diversity of studies on related subject matter, perhaps a broader understanding of videogame hacker practices can be achieved.

As these potential scenarios suggest, I still believe that there is a great deal to be learned by studying videogame hacking in various contexts. As my research has demonstrated, the

practice is an illuminating site for interrogating popular and academic definitions of computer hacking, documenting the tensions that exist between media companies and their fans, and exploring the motivations of people who wish to modify games for entertainment and profit. Whether considered through a historical perspective, such as the ethnographic work of Levy and Coleman, or a theoretical one, framed by de Certeau's and Jenkin's perspectives on the agency of media consumers, these practices have implications that reach far beyond niche communities and outmoded videogames. When people deeply engage with their favourite videogames, they grapple with the political, economic, and corporate structures that dictate our current media landscape.

References

Works Cited

- “All Bonds Cheat.” *GoldenEye Wiki*, goldeneye.fandom.com/wiki/All_Bonds_Cheat. Accessed 15 May 2019.
- Ang, Ien. *Living Room Wars: Rethinking Media Audiences for a Postmodern World*. Routledge, 1996.
- Anthropy, Anna. *Rise of the Video Game Zinesters: How Freaks, Normals, Amateurs, Artists, Dreamers, Dropouts, Queers, Housewives, and People Like You Are Taking Back an Art Form*. Seven Stories Press, 2012.
- Arcangel, Cory. “Super Mario Clouds.” *Cory Arcangel's Official Portfolio Website and Portal*, coryarcangel.com/things-i-made/2002-001-super-mario-clouds. Accessed 15 May 2019.
- Arsenault, Dominic. *Super Power, Spooky Bards, and Silverware: The Super Nintendo Entertainment System*. The MIT Press, 2017.
- “Atari 2600 Hacks.” *AtariAge*, atariage.com/hack_page.html?SystemID=2600&SoftwareHackID=6. Accessed 15 May 2019.
- Bailey, Wm. Ruffin. “Hacks, Mods, Easter Eggs, and Fossils: Intentionality and Digitalism in the Video Game.” *Playing the Past: History and Nostalgia in Video Games*, edited by Zach Whalen and Laurie N Taylor, Vanderbilt University Press, 2008, pp. 69-90.
- Blankenship, Loyd. “The Conscience of a Hacker.” *Phrack*, 8 Jan. 1986, phrack.org/archives/issues/7/3.txt.
- Boluk, Stephanie and Lemieux, Patrick. *Metagaming: Playing, Competing, Spectating, Cheating, Trading, Making, and Breaking Video Games*, University of Minnesota Press, 2017.
- Boyd, Jordan. “Icons: Combat Arena Revealed at EVO 2017.” *Dual Shockers*, 17 July 2017, dualshockers.com/icons-battle-arena-revealed-evo-2017.
- “C&D: Director’s Response.” *Chrono Compendium*, 11 May 2009, chronocompendium.com/Forums/index.php?topic=7420.0.
- Capello, Valerio. “Elf Qrin Interviews The Mentor.” *Elf Qrin’s Cyber Lab*, 31 May 2000, elfqrin.com/docs/hakref/interviews/eq-i-mentor.php.
- “Cease & Desist Letter.” *Chrono Compendium*, 10 May 2009, chronocompendium.com/Forums/index.php?topic=7396.0.

- Certeau, Michel de. "Making Do: Uses and Tactics." *The Practice of Everyday Life*. Translated by Steven Rendall, Berkeley: University of California, 1984, pp. 29-42.
- Coleman, Gabriella. *Coding Freedom: The Ethics and Aesthetics of Hacking*, Princeton University Press, 2013.
- Consalvo, Mia. *Atari to Zelda: Japan's Videogames in Global Contexts*, MIT Press, 2016.
- Consalvo, Mia. *Cheating: Gaining Advantage in Videogames*, MIT Press, 2007.
- Consalvo, Mia and Dutton, Nathan. "Game Analysis: Developing a Methodological Toolkit for The Qualitative Study of Games." *Game Studies: The International Journal of Game Research*, Vol. 6, no. 1, 2006, gamestudies.org/0601/articles/consalvo_dutton. Accessed 7 Apr. 2018.
- "Crowd Control: Frequently Asked Questions." *Crowd Control*, crowdcontrol.live/faq. Accessed 15 May 2019.
- De Koven, Bernard. *The Well-Played Game: A Player's Philosophy*. Cambridge: MIT Press, 2013.
- "Download Project M." *Archive.org: Project M*, web.archive.org/web/20150919194229/http://projectmgame.com/en/download. Accessed May 2019.
- Ebert, Roger. "Review: Hackers." *RogerEbert.com*, 15 Sep. 2019, rogerebert.com/reviews/Hackers-1995.
- Fraps: Real-Time Video Capture and Benchmarking. The Fraps Staff, fraps.com. Accessed 15 May 2019.
- Gach, Ethan. "Counter-Strike Pro Banner For Cheating, Now Regrets Ever Playing The Game." *Kotaku*, 25 Oct. 2018, kotaku.com/counter-strike-pro-banned-for-cheating-now-regrets-eve-1830010315.
- Geertz, Clifford. *The Interpretation of Cultures: Selected Essays*. Basic Books Inc, 1973.
- Gleiberman, Owen. "Hackers." *Entertainment Weekly*, 6 Oct. 1995.
- Good, Owen. "Fan-made Pokemon Uranium is shelved by its creators after Nintendo notices." *Polygon*, 14 Aug. 2019, polygon.com/2016/8/14/12472616/pokemon-uranium-Taken-down-nintendo.
- Green, Joshua and Jenkins, Henry. "The Moral Economy of Web 2.0." *Media industries: history, theory, and method*, edited by Jennifer Holt and Alisa Perren, Wiley-Blackwell, 2009, pp. 213-225.

- Herz, JC. "Game Theory; For Gamer maker, There's Gold in the Code." *The New York Times*, 2 Dec. 2019, [nytimes.com/1999/12/02/technology/game-theory-for-game-maker-there-s-gold-in-the-code.html](https://www.nytimes.com/1999/12/02/technology/game-theory-for-game-maker-there-s-gold-in-the-code.html).
- Horti, Samuel. "PUBG's anti-cheat system is banning more than 6,000 players a day." *PC Gamer*, 15 Oct. 2017, [pcgamer.com/pubg-banning-more-than-6000-players-a-day](https://www.pcgamer.com/pubg-banning-more-than-6000-players-a-day/).
- Iantorno, Michael. *Sub-Versions: Investigating Video Game Hacking Practices and Subcultures*, 2018, sub-versions.com.
- "Introducing New Ways to Support Workshop Creators." *Steam Workshop*, steamcommunity.com/workshop/about/paidcontent. Accessed 15 May 2019.
- Jansz, Jeroen and Theodorsen, Jesper. "Modifying Video Games on Web2.0: An Exploration of Motives For Publishing Creative Game Content." *Paper presented at the annual meeting of the International Communication Association*, Marriott, Chicago, IL, 21 May 2009.
- Jenkins, Henry. *Convergence Culture: Where Old and New Media Collide*. New York University Press, 2006.
- Jenkins, Henry. *Textual Poachers: Television Fans and Participatory Culture*. Routledge, 2nd ed., 2012.
- Johnson, Eric E. "Innovative Add-on Device for Video Game Console Not Copyright Infringement." Museum of Intellectual Property, [museumofintellectualproperty.org/features/game_genie.html](https://www.museumofintellectualproperty.org/features/game_genie.html). Accessed 15 May 2019.
- Joseph, Daniel. "Code of Conduct." *Real Life Mag*, 12 Apr. 2019, reallifemag.com/code-of-conduct.
- "K2K2 2002: The Conscience of a Hacker." *YouTube*, uploaded by Channel2600, 12 Sep. 2012, [youtube.com/watch?v=0tEnnvZbYek](https://www.youtube.com/watch?v=0tEnnvZbYek).
- "Kaze Emanuar is creating YouTube videos." *Patreon*, [patreon.com/Kazestuff](https://www.patreon.com/Kazestuff). Accessed 15 May 2019.
- "Lawrence Lessig: Laws That Choke Creativity." *Ted Talks*, uploaded by Ted2007, March 2007, [ted.com/talks/larry_lessig_says_the_law_is_strangling_creativity](https://www.ted.com/talks/larry_lessig_says_the_law_is_strangling_creativity).
- "Legal threats against The Pirate Bay." *Archive.org: The Pirate Bay*, web.archive.org/web/20090122235038/https://thepiratebay.org/legal. Accessed 15 May 2019.
- LeMieux, Patrick. "Everything but the clouds." *Vimeo*, uploaded by Patrick LeMieux, 8 Nov. 2017, vimeo.com/241966869.
- Levy, Steven. *Hackers: Heroes of the Computer Revolution*. O'Reilly Media, 1984.

Lewis Galoob Toys, Inc. v. Nintendo of America. No. 91-16205. Ninth Circuit Court of Appeals. 21 May 1992.

“Lunar IPS.” *Fu So Ya’s Niche*, fusoya.eludevisibility.org/lips. Accessed 15 May 2019.

Maaz, Wajeed. “Couple Who Ran ROM Site to Pay Nintendo \$12 Million.” *Motherboard*, 13 Nov. 2018, vice.com/en_us/article/bjezda/couple-who-ran-rom-site-to-pay-nintendo-dollar12-million.

Maiberg, Emanuel. “Nintendo’s Offensive, Tragic, and Totally Legal Erasure of ROM Sites.” *Motherboard: Read-Only Memory*, 10 Aug. 2018, motherboard.vice.com/en_us/article/bjbped/Nintendos-offensive-tragic-and-totally-legal-erasure-of-rom-sites.

Marsh. “Hacking and Philosophy: The Mentor’s Manifesto.” *Hackaday*, 4 Nov. 2013, hackaday.com/2013/11/04/hacking-and-philosophy-the-mentors-manifesto.

“Modification: Kajar Laboratories.” *Chrono Compendium*, chronocompendium.com/Term/Modification.html. Accessed 15 May 2019.

“Mother 3 Fan Translation Patch Notes.” *Mother 3 Translation*, mother3.fobby.net/or/. Accessed 27 June 2019.

Murray, Laura J. and Samuel E. Trosow. *Canadian Copyright, A Citizen’s Guide*, Second Edition. Between The Lines, 2013.

Onanuga, Tola. “All That’s Wrong with Nintendo’s Heavy-Handed ROM Crackdown.” *Wired*, 18 Aug. 2018, wired.co.uk/article/nintendo-roms-emulator-loveroms-loveretro-lawsuit. Accessed 13 Oct. 2018.

“Pokémon Prism File Patcher.” *Pokémon Prism*, pokemonprism.com/patcher.html. Accessed 15 May 2019.

Postigo, Hector. “Video Game Appropriation through Modifications: Attitudes concerning Intellectual Property among Modders and Fans.” *Convergence: The International Journal of Research into New Media Technologies*, vol. 14, no. 1, pp. 59-74, 2008.

Postigo, Hector. “Modification.” *Debugging Game History: A Critical Lexicon*, edited by Henry Lowood and Raiford Guins, The MIT Press, 2016, pp. 319-331.

Ribaldo, Nicolas. “YouTube, Video Games, and Fair Use: Nintendo’s Copyright Infringement Battle with YouTube’s Let’s Plays and Its Potential Chilling Effects.” *Berkeley Journal of Entertainment and Sports Law*, vol. 6, 2017, pp. 114-138.

- Schreier, Jason. "Nintendo Files Copyright Strikes Against *Super Mario 64 Online*." *Kotaku*, 20 Sep. 2019, kotaku.com/nintendo-files-copyright-strikes-against-super-mario-64-1818580029.
- Schreier, Jason. "People Are Doing Remarkable Things With *Zelda: A Link to the Past*." *Kotaku*, 20 July 2016, kotaku.com/people-are-doing-remarkable-things-with-zelda-a-link-t-1783990961
- Sihvonen, Tanja. *Players Unleashed! Modding The Sims and the Culture of Gaming*. Amsterdam University Press, 2011.
- Smith, Fern M. "Memorandum of Decision." *Lewis Galoob Toys, Inc. v. Nintendo of America*, United States District Court, N.D. California, 12 July 1991.
- Sotamaa, Olli. "Computer Game Modding, Intermediality and Participatory Culture." *New Media? New Theories? New Methods?*, 1-5 Dec. 2003, University of Århus, DK. Unpublished Seminar Paper.
- Speed Demos Archive. The SDA Staff, speeddemosarchive.com. Accessed 15 May 2019.
- Stallman, Richard. "The GNU Manifesto." *GNU Operating System*, gnu.org/gnu/manifesto.en.html. Accessed 15 May 2019.
- "Start Playing." *A Link to the Past Randomizer*, alttpr.com/en. Accessed 15 May 2019.
- "Super Mario Clouds 2002." *Whitney Museum of American Art*, whitney.org/collection/works/20588. Accessed 15 May 2019.
- Swalwell, Melanie. "Classic Gaming." *Debugging Game History: A Critical Lexicon*, edited by Henry Lowood and Raiford Guins, The MIT Press, 2016, pp. 45-52.
- The Copyright Act of Canada*. The Government of Canada Justice Laws Website, 19 June 2017. laws-lois.justice.gc.ca/eng/acts/C-42/FullText.html.
- "The Legend of Zelda: Mystery of Solarus DX." *Solarus Wiki*, wiki.solarus-games.org/doku.php?id=zelda_mystery_of_solarus_dx. Accessed 15 May 2019.
- Wark, McKenzie. *A Hacker Manifesto*. Cambridge: Harvard University Press, 2004.
- "Welcome to The Cutting Room Floor." *The Cutting Room Floor*, tcrf.net/The_Cutting_Room_Floor. Access 15 May 2019.

Mediography

Battlefield 1942. Windows PC Version, 2002.

Chrono Trigger. Super NES, 1995.

Duke Nukem. Windows PC Version, 1991.

Esmail, Sam, creator. *Mr Robot*. Universal Cable Productions, Anonymous Content, and NBC Universal Television Distribution, 2015.

Hackers. Directed by Iain Softley, MGM/UA Distribution Co, 1995.

Hackmud. Windows PC version, Drizzly Bear, 2016.

Icons: Battle Arena. Windows PC Version, 2018.

Live Free or Die Hard. Directed by Len Wiseman, Twentieth Century Fox, 2007.

Pokémon Crystal. Nintendo Game Boy Color, 2001.

Quake 3. Windows PC Version, 1999.

Space Invaders. Atari 2600, 1980.

Starstruck: A Music Adventure Game. Windows PC Version, TBD.

Super Mario 64. Nintendo 64, 1996.

Super Mario Bros. NES, 1985.

Super Smash Bros. Nintendo 64, 1999.

Super Smash Bros. Brawl. Nintendo Wii, 2008.

Super Smash Bros. Melee. Nintendo GameCube, 2001.

Swordfish. Directed by Dominic Sena, Warner Bros. Pictures, 2001.

The Legend of Zelda: A Link to the Past. Super NES, 1991.

Watchdogs. Windows PC version, Ubisoft, 2014.

The Wu Xing. Windows PC Version, TBD.

Zuiker, Anthony, Mendelsohn, Carol, and Donahue, Ann, creators. *CSI: Cyber*. Jerry Bruckheimer Television, and CBS Productions, 2015.

Hackography

Chrono Trigger: Crimson Echoes. chronocompendium.com/Term/Chrono_Trigger:_Crimson_Echoes.html. Accessed 15 May 2019.

Edwin and Jones. web.archive.org/web/20170323092021/http://edwinandjones.com. Accessed 15 May 2019.

HyperBound. michaeliantorno.com/portfolio/hyperbound. Accessed 6 June 2018.

Link to the Past Randomizer. alttpr.com/en. Accessed 15 May 2019.

Pokémon Brown. rijon.fandom.com/wiki/Pok%C3%A9mon_Brown. Accessed 15 May 2019.

Pokémon Prism. pokemonprism.com. Accessed 15 May 2019.

Project M. pmunofficial.com/en/download. Accessed 15 May 2019.

SM64 Last Impact. sm64hacks.com/hack.php?id=59. Accessed 15 May 2019.

SM64 Online. hacks.sm64hacks.com/hack/463. Accessed 15 May 2019.

Space Invaders Arcade. atariage.com/hack_page.php?SystemID=2600&SoftwareHackID=6. Accessed 15 May 2019.

Super Donkey Kong 64. hacks.sm64hacks.com/hack/85. Accessed 15 May 2019.

Super Mario Clouds. coryarcangel.com/things-i-made/2002-001-super-mario-clouds. Accessed 15 May 2019.

Appendix I: Participant Profiles

Adam

Adam was the main developer behind two major *Pokémon* ROM hacks: *Pokémon Brown* and *Pokémon Prism*. He worked on the latter title between 2009 and 2016, receiving help from the Twitch Plays Pokémon development team as the project neared completion. He halted his work after receiving a cease-and-desist order from Nintendo of Australia.

Since leaving the project, Adam decided to create his own monster videogame, *The Wu Xing*, announced in December 2018 and scheduled for release in 2021. Adam is located in California, USA.

Pokémon Prism

Pokémon Prism is a ROM hack of the Game Boy Color game *Pokémon Crystal*. Intended to be a sequel to Adam's previous ROM hack *Pokémon Brown* — and positioned, unofficially, within the same fictional universe as official *Pokémon* titles — *Prism* allows the player to traverse the newly conceived region called Naljo.

In addition to sampling elements from later entries in the series, such as additional *Pokémon* and combat abilities, *Pokémon Prism* introduces new types of gameplay that have not yet been presented in the official *Pokémon* series. For example, several portions of the game allow the player to take control of their *Pokémon* to complete mini-games or explore areas.

Following the cease-and-desist order, the source code for version 0.91 of *Pokémon Prism* was leaked without Adam's consent. A group of videogame hackers known as RainbowDevs took this nearly complete iteration of the hack, fixed many of its bugs, and have since released three follow-up versions (0.92, 0.93, 0.94). Although Adam is not involved in this continued

development *Pokémon Prism*, he is both aware and supportive of it.

Axel Hellström

Axel Hellström is one of the core developers of the *A Link to the Past Randomizer*, and has been responsible for adding new features and troubleshooting the *Randomizer*.

Axel's interest in *The Legend of Zelda: A Link to the Past* began when he was a child, after receiving the title as a Christmas present. Years later, he began watching speedruns of the game online and was eventually invited to participate by a speedrunner named SuperSkudge. By the time the *Randomizer* came to his attention in 2016, Axel was already a hobbyist videogame hacker — primarily working with *Super Mario World* for the Super NES — and joined the project with the intent of bringing it to completion. Parallel to his work on the *Randomizer*, Axel streams regularly on Twitch, focusing on casual speedruns, races, and developer streams.

Axel is currently employed by Warp World, where he helps develop the Twitch extension Crowd Control. His day-to-day work involves hacking *The Legend of Zelda: A Link to the Past* for integration into the extension. He is 34 years old and is located in Massachusetts, USA.

Chris Owen

Chris Owen is the community manager for the *A Link to the Past Randomizer*, and hack's randomization logic (the algorithms which determine how game elements are reshuffled through the *Randomizer*'s web application).

Chris' fascination with *The Legend of Zelda: A Link to the Past* began when he was a child, primarily through watching his older brother play the title on the Super NES. His interest was rekindled following the release of the Gameboy Advance remake, which he played,

replayed, and soon began speedrunning and challenge running. Chris eventually discovered the Speed Demos Archive online, which inspired him to start streaming his own speedruns on Twitch. In 2016, Chris came across an early iteration of the *Randomizer*, joined the development team, and has been a part of the community ever since.

Chris Owen is located in England, United Kingdom.

Veetorp

Veetorp is one of the core developers of the *Link to the Past Randomizer*, whose work focuses primarily on the randomization algorithm and the web application.

Veetorp originally came to the *Zelda* series through its first two releases, *The Legend of Zelda* and *Zelda II: The Adventure of Link*, before playing *The Legend of Zelda: A Link to the Past* in the 1990s. Years later, he discovered an early version of the *Randomizer* by watching online videos with his friends. Veetorp saw that many new features were scheduled to be added to the *Randomizer*, and beginning learning C# in order to contribute to the project. After the original developer ceased development, he rewrote the entire application from scratch in PHP.

In addition to his hacking work, Veetorp also hacks and speedruns *Goonies 2* for the NES. He describes himself as a “mediocre” *A Link to the Past* speedrunner and a “top-5” *Goonies 2* speedrunner.

Veetorp is in his mid-30s, is a computer programmer, and is located in the United States.

A Link to the Past Randomizer

The *A Link to the Past Randomizer* is centered around a web-based application that modifies *The Legend of Zelda: A Link to the Past* ROMs. When players upload a *Link to the Past* ROM to the application, it will rearrange the content of the game in a variety of ways. The exact

parameters of this rearrangement are determined through options provided by the application's graphic user interface.

The most popular mode of the *Randomizer*, the item randomizer, shuffles the location of *A Link to the Past*'s key items to enforce a non-linear exploration of the game world. As the randomization disrupts the standard flow of the game, players must use guesswork and logic to progress and may confront difficult obstacles before they are adequately prepared for them.

Through online competition on Twitch, players are encouraged to race against each other to complete the same "seed" - which determines the location of items in a ROM - as quickly as possible. These races have led to enormous tournaments featuring as many as 500 participants from across the world.

David Shayne

David Shayne was a core member of the development team for *Project M*, a modification (mod) of *Super Smash Bros Brawl*. A fan of the original *Super Smash Bros* for the Nintendo 64, David played casually with his friends for several years before becoming involved in the competitive scene following the release of *Super Smash Bros Melee* in 2001.

David's motivations for joining the *Project M* team are rooted in his dissatisfaction with the competitive qualities of *Brawl* — a sentiment he believes is echoed by many in the *Smash Bros* community — and a lifelong interest in tinkering with videogames. Prior to his involvement with the *Project M* team, he created custom maps for the PC game *Starcraft*.

David Shayne is located in Virginia, USA and is a web developer by trade.

Project M

Project M is a mod of the 2008 Wii fighting game *Super Smash Bros Brawl*. The project began as an effort to rework the mechanics of one of the game's characters, Falco Lombardi, to better match his presentation in *Brawl*'s predecessor *Super Smash Bros Melee*. However, the development team eventually decided to rework the game completely, sampling elements from both *Melee* and the original *Super Smash Bros* while adjusting the game's physics and gameplay to ostensibly restore competitiveness to the title.

Unlike many videogame hacks, which rely on ROM images and are played on PCs, the *Project M* mod is embedded on an SD card and requires both the original game and a Wii console to play. The *Project M* team made this design decision to support the desires of competitive players. Even the most accurate emulation can disrupt the meticulous control and timing required to play *Super Smash Bros Melee* competitively, so players view console play as a requirement for tournament inclusion.

Developed between 2010 and 2015, production on the mod was abruptly halted on December 1, 2015. Members of the *Project M* team have cited various reasons for this shutdown, including the potential of future legal concerns.

Kaze Emanuar

Kaze Emanuar is a videogame hacker whose work focuses primarily on *Super Mario 64* for the Nintendo 64. He began experimenting with videogame hacking at the age of 17 and has since released over sixty *Super Mario 64* hacks of varying length and complexity. Kaze showcases his hacking work on YouTube and Twitch, and earns roughly \$300 a month through his Patreon.

Kaze's most prominent hack is perhaps *SM64 Online*, which has been featured on gaming websites such as Kotaku and Polygon. During the height of the hack's popularity, Nintendo issued copyright strikes against Kaze's content on YouTube and Patreon shuttered his account for containing trademarked and/or copyrighted content. Since then, Kaze has continued uploading videos to YouTube and revived his Patreon by removing copyrighted and trademarked content.

Kaze Emanuar is a university student living in Germany. He considers hacking to be his full time job.

SM64: Last Impact

SM64: Last Impact is a videogame hack developed by Kaze Emanuar that was released on September 30, 2016. Kaze describes the project as a completely custom game built within *Super Mario 64*, and estimates to have spent over four thousand hours developing it.

The hack features new levels and objectives that were not present in the original *Super Mario 64*, and samples powerups, characters, and creatures from other entries in the Mario series (in addition to introducing original elements as well). Taking place in the same continuity as *Super Mario 64*, the game could be interpreted as a sequel or remix of the original title.

SM64 Online

SM64 Online is a videogame hack developed by Kaze Emanuar, alongside fellow hackers Melonspeedruns and Marshivolt, that was released in 2017. The hack introduces online multiplayer support to *Super Mario 64* using the web client Net64+ 2.0, allowing up to 24 people to play simultaneously using an emulated copy of the game.

In addition to multiplayer functionality, *SM64 Online* allows players to play as a variety of characters that were not present in the original title. This includes characters sourced from elsewhere in the Mario franchise, such as Luigi and Wario, to popular videogame characters, such as Sonic the Hedgehog and Kirby.

Max Ponoroff

Max Ponoroff is an independent videogame developer, currently working on his debut title *Starstruck: A Music Adventure Game*. Many elements of *Starstruck* are sourced from *Edwin & Jones*, an *EarthBound* ROM hack Max developed (but never completed) as a member of the online fan community Starmen.net.

Originally attracted to Starmen.net because of its focus on *Super Smash Bros*, Max eventually became a fan of *EarthBound* and joined the website's hacking community, PK Hack. He has since worked on several *EarthBound* hacking projects and is the primary developer of CoilSnake, which has become the community's central ROM hacking tool.

Prior to becoming an independent game developer, Max worked as a software engineer at a large North American company. He is currently developing *Starstruck* as a full time job, and is located in the United States.

Edwin & Jones

Edwin & Jones is an uncompleted and unreleased ROM hack of *EarthBound* for the Super NES. Developed primarily by Max Ponoroff, but featuring contributions from various members of the Starmen.net community, it was advertised as a completely new adventure built within *EarthBound*. Featuring new characters, locations, cutscenes, enemies, and music, the

game centers on two teenagers (the titular Edwin and Jones) who must fight a forgotten evil in their hometown.

Edwin & Jones was developed between 2012 and 2016, before Max abandoned the project to focus on *Starstruck*.

Starstruck: A Music Adventure Game

Starstruck: A Music Adventure Game is an independently produced videogame that was announced on December 15, 2018. Developed by a small development team led by Max Panoroff, *Starstruck* is described as “a music adventure game where you rampage as a gigantic human hand.”

The game does not currently have an official release date or platform.

ZeaLity

ZeaLity is a staff member at the Chrono Compendium, one of the largest *Chrono Series* fan websites on the internet. Originally a member of the OverClocked Remix forums — where he was heavily involved in discussions regarding *Chrono Series* fan content — he felt the creation of a standalone website was necessary to accommodate the wealth of fan interest in the series. In 2003, he was one of the driving forces behind the creation of the Chrono Compendium.

ZeaLity was one of the leader designers of the ROM hack *Chrono Trigger: Crimson Echoes*, developed between 2004 and 2009. ZeaLity has not engaged in any sustained *Chrono Trigger* hacking since the project disbanded following a cease-and-desist order in 2009, but is still an active member of the Chrono Compendium community.

Chrono Trigger: Crimson Echoes

Chrono Trigger: Crimson Echoes is a ROM hack of the Super NES game *Chrono Trigger*, developed by the Kajar Laboratories hacking team at the Chrono Compendium. It was conceived as an unofficial interquel in the series, taking place five years after *Chrono Trigger* and prior to its Playstation sequel *Chrono Cross*. The game introduces a new narrative built within the framework of the original game, while integrating characters and building upon plot threads from other entries in the *Chrono Series*. Some additional features added to the game include new maps, graphics, and mini-games.

On May 31 2009, a few weeks prior to the game's anticipated release date, Square Enix sent the developers a cease-and-desist order which led to the dissolution of the project. The game was described as being roughly 98% complete at the time of its cancelation, but Kajar Laboratories never distributed a final release. However, an alpha (leaked shortly after development was halted) and a beta (leaked in January 2011) eventually spread across the internet, the latter of which is playable from beginning to end.

Appendix II: Glossary of Terms

Alpha/Beta — Alpha and Beta versions of games are in-progress iterations that are created for testing purposes. Occasionally, games will have an “open beta” in which a limited pool of players can play the game and report bugs and errors.

Assembly Code (ASM) — Assembly is a low-level programming language for computers, microprocessors, microcontrollers, and other integrated circuits. It is a so-called “low-level” language that operates very close to hardware and, unlike high-level programming languages, cannot be easily ported between different types of hardware. Assembly was commonly used in early videogames, including titles for the Super NES and Game Boy.

ASM Hacking — ASM hacking involves editing the ASM (Assembly) code within a ROM image. There is no set pattern for ASM hacking, as the code varies widely from game to game, but most skilled ASM hackers either use an emulator equipped with a built-in debugger or tracer, or run the ROM through a disassembler, then analyze the code and modify it using a hex editor or assembler according to their needs.

Cease and Desist Order — A cease and desist letter is a document sent to an individual or business to stop purportedly illegal activity (“cease”) and not to restart it (“desist”). The letter may warn that if the recipient does not discontinue specified conduct, or take certain actions, by deadlines set in the letter, that party may be sued.

Challenge Run — A challenge run is a playthrough of a game wherein the player plays under self-imposed restrictions in order to increase the game’s difficulty and replay value. Some common challenge runs include 100% runs, where the player must complete every objective in the game, and minimalist runs, where the player intentionally skips items or bonuses that would ease their progress.

Compiler — A compiler takes a series of assembly files and puts them back together into a ROM image. This is a necessary step for videogame ROM hacking, as a disassembly is not playable using an emulator.

Copyright Strike — A copyright strike is a policing practice used by YouTube for the purpose of managing copyright infringement and complying with the Digital Millennium Copyright Act. YouTube will issue a copyright strike on a user accused of copyright infringement. When a YouTube user has three copyright strikes, YouTube terminates that user's YouTube channel, removes all of their videos, and prohibits them from creating another YouTube channel.

Developer Stream — Developer streams are online video streams in which a professional or hobbyist developer completes work while discussing it.

Digital Millennium Copyright Act (DMCA) — The Digital Millennium Copyright Act (DMCA) is a 1998 United States copyright law. It criminalizes production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works (digital rights management or DRM). It also criminalizes the act of circumventing an access control, whether or not there is actual infringement of copyright itself. In addition, the DMCA heightens the penalties for copyright infringement on the Internet.

Disassembler/Disassembly — A disassembler is a computer program that translates machine language into a human friendly version of the language, called Assembly language. A disassembler can separate a ROM image into a series of assembly files. A disassembler may add comments to code and names to functions, making the ROM image easier to edit.

Emulator — A program that enables one computer system (called the host) to behave like another computer system (called the guest). An emulator enables the host system to run software

and other components which were originally designed for the guest system. ZSNES, for example, allows users to run Super NES games on a PC.

Hex Editor — A hex editor is a fundamental tool for ROM hacking. They are used for editing text, other data for which the structure is known (for example, item properties), and Assembly hacking.

Patch File — A file that contains a set of instructions to alter the data within a ROM image. Patches can be applied to a ROM image using specialized patching software. Hacks are distributed as patches due to the legal concerns surrounding the distribution of pre-altered ROM images.

Personal Best (PB) — A personal best (PB) is a speedrunning term for the fastest time in which a particular speedrunner has completed a game. Speedrunners will often stream “PB grind” sessions in which they play a game over and over again to improve their time.

ROM Hacking — ROM hacking is the process of modifying a ROM image of a videogame to alter elements within the game, including (but not limited to) graphics, levels, dialogue, and music.

ROM Image (ROM) — A ROM image (often shortened to “ROM”) is a computer file that contains a copy of the data present on a read-only memory chip. ROM images can be sourced from a videogame cartridge, a computer’s firmware, or from an arcade game’s main board. Many cartridge based videogames are copied to ROM files, which can then be played on modern computers using an emulator.

ROM Map — A ROM map is a linear breakdown of a data stored within a ROM image. Using hexadecimal addresses, a map explains where certain assets (such as text, animation, and music) are stored.

Speedrun — A speedrun is a play-through (or a recording of a play-through) of a videogame performed with the intention of completing it as quickly as possible. Speedruns may cover a whole game or a selected part, such as a single level.

Appendix III: Glossary of Websites

Bits — Bits are a virtual good that can be bought through Twitch and are used to purchase Cheer. A Cheer is a chat message, often manifesting as an animated emote, that allows users to support a Twitch Partner Streamer. Twitch pays \$1 to a Twitch Partner for every 100 Bits used through Cheer.

Crowd Control — Crowd Control is a Twitch extension that allows viewers to exchange Bits for items that can help or hinder a streamer's progress in a game. As of January 2019, Crowd Control currently supports the titles *Super Mario World*, *The Legend of Zelda: A Link to the Past*, and *Super Mario Bros. 3*.

The Cutting Room Floor — The Cutting Room Floor is a website dedicated to unearthing and researching unused and cut content from videogames.

Discord — Discord is a proprietary freeware VoIP application and digital distribution platform designed for videogaming communities, that specializes in text, image, video, and audio communication between users in a chat channel.

OverClocked Remix — OverClocked ReMix is a videogame music community that hosts fan-made remixes as well as information about videogame music.

Patreon — Patreon is a membership platform that provides business tools for creators to run a subscription content service, with ways for artists to build relationships and provide exclusive experiences to their subscribers, described as "patrons".

ROMHacking.net — ROMhacking.net is a website that hosts classic videogame modifications, fan translations, console homebrew, utilities, and learning resources.

Speed Demos Archive (SDA) — Speed Demos Archive (SDA) is a website whose primary focus is hosting downloadable, high-quality speedrun videos. SDA organizes two annual

speedrunning charity marathons, Awesome Games Done Quick and Summer Games Done Quick.

Speedrun.com — Speedrun.com is a site that provides leaderboards, resources, forums, and other resources for speedrunning.

Twitch — Twitch is a live streaming video platform owned by Twitch Interactive, a subsidiary of Amazon. Introduced in June 2011 as a spin-off of the general-interest streaming platform, Justin.tv, the site primarily focuses on videogame live streaming. Content on the site can be viewed either live or through video on demand.

Twitch Extension — Extensions are interactive web applications that run on a Twitch broadcaster's channel, either overlaying their video or displaying below it in panels.

YouTube — YouTube is an American video-sharing website created in 2005. YouTube allows users to upload, view, rate, share, add to favorites, report, comment on videos, and subscribe to other users. Google bought the website in November 2006 and now operates it as one of its subsidiaries.