FrankenFRED:

A CUSTOM DIGITAL FORENSICS WORKFLOW AND DIGITAL PRESERVATION LAB FOR THE ARCHIVES OF ONTARIO

by
Blanche Joslin
B.A., Flagler College, 2007

A thesis

presented to Ryerson University

in partial fulfillment of the

requirements for the degree of

Master of Arts

in the Program of

Film and Photography Preservation and Collections Management

Toronto, Ontario, Canada, 2018

AUTHOR'S DECLARATION FOR ELECTRONIC SUBMISSION OF A THESIS

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I authorize Ryerson University to lend this thesis to other institutions or individuals for the purpose of scholarly research.

I further authorize Ryerson University to reproduce this thesis by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

I understand that my thesis may be made electronically available to the public.

FrankenFRED: A CUSTOM DIGITAL FORENSICS WORKFLOW AND DIGITAL PRESERVATION LAB FOR THE ARCHIVES OF ONTARIO
Master of Arts, 2018
Blanche Joslin
Film and Photography Preservation and Collections Management
Ryerson University

Abstract

Digital forensics allows cultural heritage institutions to validate, preserve, and recover digital objects. This thesis discusses the development and implementation of a custom digital forensics workflow for the Archives of Ontario. The justifications for the workflow are based on research into digital forensics, authenticity, diplomatics, and digital preservation. The workflow seeks to clarify best-practice policies and procedures for using a Digital Intelligence Forensic Recover of Evidence Device (FRED), an out-of-the-box digital forensics hardware solution. The Archive procured a FRED tower requiring an implementation plan and overall strategy for its effective use. Presented in this paper is a workflow built specifically for the needs of the Archives as well as justifications for the processes proposed within the workflow. The BitCurator processing environment is addressed as an integral tool for implementation. Also discussed are modifications made to the Archive's FRED tower to produce what I have called FrankenFRED.

Acknowledgements

I would like to acknowledge my thesis supervisor and first reader, Asen Ivanov. Also, Julienne Pascoe, my second reader whose archival knowledge and mutual forensics struggles were invaluable.

Jess Whyte, whose fantastic work at University of Toronto's Project Canopus guided my own processes, was a constant resource for humor and knowledge.

Thank you to all the friends and family that allowed me to ignore them for two years of graduate school.

Finally, I'm grateful for the emotional and intellectual fortitude of my helpmate, without whom this process would have been infinitely more laborious.

Table of Contents

List of Figures

List of Appendices

1. Introduction

At the FIAT/IFTA 2017 World conference, Richard Wright described the modern television archive workflow as a spider web, rather than the linear process of the past (Wright 2017). This conjures the image of the modern archivist as a spider, not sitting at the end of a funnel but skittering out to the far reaches of our webs to wrap up our content. This analogy can help us better understand the needs of born-digital archival objects. Born-digital objects are technologically complex and more likely to fly past archival workflows without being captured and processed, which in turn possess threats to their longevity as artifacts and authenticity as archival object. They are highly susceptible to loss due to accidental deletion and technological obsolescence and require a higher level of expertise to preserve than paper-based objects (Rothenberg 1998; Harvey 2008; Wright 2012).

Audio-Visual elements have been the unruly stepchildren of collecting institutions since they began finding their way into collections. Each innovation in audio-visual formats has caused its own archival innovation in turn. From the fires of nitrate film to the brown muck of magnetic tape's sticky shed syndrome, each new technology for audio-visual carriers has created a unique and difficult problem (Jones 2014). With the introduction of digital objects, this innovation became a problem for records outside of the audio-visual realm. Similarly, the introduction of word processing brought even simple written words into the fold of unwieldy objects (Kirschenbaum 2016). Today, collecting institutions are receiving a variety of born- digital carriers that have to be dealt with in ways that archivists have not had to accommodate before.

This thesis addresses the use of Digital Forensics as a method for the archival processing of born-digital carriers. Digital Forensics began as a set of methods and tools used

by law enforcement to locate and authenticate digital information stored on digital carriers. Likewise, within collecting institutions, Digital Forensics provides methods and tools for opening up the shell of born- digital carriers to get access to the information stored therein. Matthew Kirschenbaum's 2010 report for the Council of Library and Information Resources introduces the similarities between traditional digital forensics and digital forensics in collecting institutions:

> The same forensics software that indexes a criminal suspect's hard drive allows the archivist to prepare a comprehensive manifest of the electronic files a donor has turned over for accession. The same hardware that allows the forensics investigator to create an algorithmically authenticated "image" of a file system allows the archivist to ensure the integrity of digital content once captured from its source media. The same data-recovery procedures that allow the specialist to discover, recover, and present as trial evidence an "erased" file may allow a scholar to reconstruct a lost or inadvertently deleted version of an electronic manuscript (Kirschenbaum et al. 2010).

When processing analog carriers, the type of information resource (e.g., a book, photograph, or a film) being processed is immediately discernable from the carrier. A VHS tape is immediately identifiable as not a book and not a gelatin silver print. But when a CD lands on the processing desks of archivists, they could be looking at anything from a single photograph to a piece of software, or both. Furthermore, the physical disk is not viable for long- term preservation, and all information should be removed immediately (Iraci 2011; Iraci 2012). It is evident how this creates a much more complex processing environment that can yield unexpected difficulties that complicate archival processing. It also makes culling practices much more difficult as the digital objects must be fully explored before processing decisions can be made (Meister 2014; Wiedeman 2016).

1.1 Research Goals and Approach

This thesis project examines how the archival processing of digital carriers can be assisted by methods and tools from the field of digital forensics. The project took place

within the Archives of Ontario during a student residency. The goal of the research was to develop a process map in the form of a workflow to guide the integration of a Digital Preservation Lab into their born- digital carrier processing workflow. To do so, I used an action based research approach to produce a workflow that is ready to be implemented within the archive. My fieldwork took place during the first half of 2018. I consulted the available literature on Digital Forensics within Cultural Heritage institutions as well as the field at large. The methodology I employed required first to consult the literature as well as to seek expert advice and best practices on the application of digital forensics in the cultural heritage sector. Then, based on this theoretical knowledge, to use the available resources at the Archives of Ontario to develop and deploy an actionable digital forensics workflow.

1.2 Institutional Background

The Archives of Ontario were established in 1903 by Alexander Fraser who was appointed the first Archivist of Ontario to preserve the history of the province. In 2009, the archives moved to a purpose- built, cutting-edge archival facility on York University's Keele campus (Archives of Ontario 2013). The Archives and Recordkeeping Act of 2006 defines the current mandate of the Archives of Ontario:

(a) to preserve records of archival value;
(b) to provide access to the public to records in the custody or control of the Archives of Ontario;
(c) to promote good recordkeeping by public bodies to facilitate the preservation of records of archival value;
(d) to assist historical research and encourage archival activities in Ontario." (Archives and Recordkeeping Act 2006)

The current structure of the Archives falls within the Ministry of Government and Consumer Services and is referred to as the Information, Privacy, and Archives (IPA) Division. The Archives serves the public sector by providing access to information, privacy protection, and

records management to all ministries within the Ontario Government, as well as outlying Agencies, Boards and Commissions. (Ministry of Government and Consumer Services 2018).

Within the IPA, there are several units responsible for taking care of the various aspects of the IPA mandate. The Portfolio Management Office, where I completed my residency, is tasked with ensuring the division's project portfolio remains streamlined, collaborative, and delivers on priorities. This also includes working on division-wide digital initiatives, including long term preservation and access to Government and archival records. My experience in archival practices guided my processes by dictating the standards that the Archives of Ontario's Digital Preservation Lab must meet to fulfill all of these requirements.

Charles Levi, an archivist at the Archives of Ontario, published an article in *Archivaria* in 2011 detailing the challenges of working with obsolete carriers in the archive. This article detailed the process and justification for the archive building a Windows XP tower with legacy hardware and software to process floppy disks (Levi 2011). This is the standard process that will be used until the necessary hardware is purchased and my workflow can be fully implemented.

1.3. Research Process

The purpose of my research is to study the digital forensics literature and in particular the literature on digital forensics in cultural heritage institutions and to apply its principles and recommendations when creating a sustainable and scalable workflow for the Archives of Ontario's born- digital carriers. The question guiding my research developed based on the current needs of the Archives of Ontario. *How can digital forensics tools be best implemented within the born- digital workflow at the Archives of Ontario?*

To address this question, I examined the practical applications of digital forensics within cultural heritage institutions and studies on implementing digital forensics workflows in these institutions. I also spent time discussing in depth the workflows currently in place in other

Ontario institutions, such as the University of Toronto and the Ontario Securities Commission, with practitioners working in those institutions. I consulted current and past literature on digital forensics from several fields including law, cultural heritage, and audio-visual archives. I took an action research approach as my work required both tangible results and ongoing problem solving to implement new and effective processes within the archive (McKay and Marshall 2007).

2. Literature Review

In this literature review an introduction to digital objects is given, followed by a discussion of digital forensics, authenticity, diplomatics, digital preservation, and Digital Forensics Workflows and Technologies in Cultural Heritage Institutions. These topics are valuable to this project as they serve as an introduction to and justification for the workflow.

2.1 Traditional Digital Forensics vs. Archival Digital Forensics

The article "Archival Science, Digital Forensics, and New Media Art" written by Dianne Dietrich and Frank Adelstein compares and contrasts digital forensics approaches in traditional forensics settings versus archival forensics applications (Dietrich 2015). Dianne Dietrich is a librarian at Cornell University specializing in digital librarianship. Frank Adelstein is a Vice Chair of the Digital Forensics Research Workshop. The article was published in The International Journal of Digital Forensics & Incident Response. The beginning sections of the article are devoted to describing the goals of traditional and archival digital forensics investigators. The writers posit that archival forensics seek to ensure authenticity whereas traditional forensics seeks data integrity. Traditional forensics is not required to maintain the original files whereas archivists typically are. The same is true of accessibility in that traditional forensics does not deem this necessary and archivists must provide access. The article looks at archival digital forensics case studies where bit fidelity was not in line with the artist's intent and the archivist had to use their judgement and tools that would not be considered sound in traditional forensics to complete their work. This is useful in the context of my own work because it differentiates between traditional digital forensics and digital forensics in an archival environment. Also established is the need for archival digital forensics to serve goals that are different from that of a traditional forensics investigation. Clarifying the similarities and

differences between traditional forensics and archival forensics is necessary in my research to move forward with archival forensics recommendations.

2.2 Authenticity

Richard Wright published the article "The Real McCoy: What Audiovisual Collections Preserve" as a white paper for the BBC in 2011 where he was a Senior Research Engineer specializing in Archives Research for audio and video. The white paper deals with authenticity of digital objects once they are separated from their physical carrier (Wright 2011).Wright examines individual media that might enter an archive: photographs, sound, moving image, broadcasting. He discusses the carrier versus the content and how we must separate these two often to truly preserve the material. He provides a summary with hierarchal determinations of authenticity based on the content rather than the carrier. Defining authenticity is a problem applicable to born-digital files as well and this hierarchal decision-making tree will be useful in determining authenticity of the born-digital files I will be dealing with.

2.3 Born Digital Workflows

The article "'Born Digital' – Raised an Orphan?" was published in *The Moving Image* in 2008 and was written by Dylan Cave, the BFI's collections development manager (Cave 2008). The article discusses the future of audio-visual archiving in the face of born-digital objects entering archives. Cave begins by making the point that while film obsolescence is in the future, digital media are being made currently. He addresses the issues born-digital objects face and the minimum starting point required for their care. He discusses duplication and digital preservation systems environments. This article helps to create a baseline for born-digital archiving as it is one of the first dealing with the topic. The information in the article can help guide the development of workflows and policy for digital audio-visual archiving.

The second edition of *The Basics of Process Mapping* was published in 2011 by Productivity Press and was written by Robert Damelio. Damelio has been a productivity consultant since the late 1980s. This introductory guide to process maps covers relationship maps, cross-functional process maps, and flowcharts. The book details each map's strengths and applications by showing how each map can be used to detail the same processes. As developing a workflow is central to my thesis research, the book was used to identify the best process map and a flowchart for representing the workflow I developed.

2.4 Born-Digital Archiving

Joe Iraci is a senior conservation scientist with the National Archives of Canada who published the article "The Stability of DVD Optical Disc Formats" in the Restaurator journal in 2011. It describes his research into the longevity of DVD formats (Iraci 2011, 39-59). His conclusions are drawn by artificially aging the discs in high humidity and high temperature environments. Most of the formats he tested showed fair to very poor stability with only DVD+/-Rs that used a gold metal layer and a dye unaffected by the conditions showing very good stability. He contrasts this relative to CD media which do exist in a very stable CD-R with a gold and phthalocyanine layer. He concluded that no DVD media are recommended for long-term storage of digital information. This research is necessary context for my own as it asserts that digital information must be removed from all DVD media and most CD media if it is to be stored properly. Digital Forensics systems can transfer information from these media in a reliable and authentic manner.

Iraci documents his later research in "The Effect of Jewel Cases on the Stability of Optical Disc Media" which he published in 2012. This article details the results of his exploration of the

degradation effects jewel cases have on optical disc media (Iraci, 2012). He begins by examining the physical effects these cases can have on disc media such as scratching during removal but also details their methods of protecting the discs such as the center support which keeps the media from coming into contact with the case. However, the chemical makeup of these cases and any paper contained in them can have drastic effects on the media. He used the same accelerated aging conditions as in his previous work to determine these effects. His research determines that each type of disc media will have a different reaction to its container and paper inserts. He concludes with detailed instructions for disc storage based on the media and a flowchart to aid in making these decisions. This article further illustrates the fragility of optical disc media and the issues inherent in their storage. Institutions can be tempted to view optical disc media as preservation formats and these two Iraci articles will help to assert that this is not the case.

2.5 Applied Digital Forensics

Mechanisms: New Media and the Forensic Imagination was written by Matthew Kirschenbaum in 2008 and is one of the first works addressing digital forensics in new media environments (Kirschenbaum 2008). Kirschenbaum works at the University of Maryland as an Associate Professor. The book was published by MIT Press. This work provides is among the only theoretical works in new media digital forensics theory. It examines three new media works that each were designed to be inherently ephemeral and how they have become ubiquitously available online despite their intentionally ephemeral design. The book posits that digital works are not being considered through the mechanisms they exist on. He asks that the physical media that contain new media works be considered in their archiving. As one of the only historical digital forensics works this book serves to contextualize past and current uses of the technology within institutions and applied to new media works.

The document "You've got to walk before you can run: first steps for managing born-digital content received on physical media" was written by Ricky Erway for the Online Computer Library Center as a guide to institutions who have acquired born-digital materials and do not have workflows in place for them (Erway 2012). The document begins with a list of four principles for dealing with born-digital objects beginning with "Do no harm." It contains step-by-step instructions for cataloguing and triaging born-digital media for beginners. There also is a table of instructions for "Technical Steps of Readable Media" establishing guidelines for basic copying of the data on these carriers. This includes the use of a write-blocker. While short, this document is invaluable as a starting point for born-digital archiving. It is concise and easily understood making it an ideal reference point of beginners in born-digital archiving.

The presentation "Enabling Digital Forensics Practices in Libraries, Archives and Museums: The BitCurator Experience" was given by Christopher Lee and Kam Woods at the Digital Forensics Research Conference held in 2014 at Denver (Lee 2014). The presentation seeks to establish the needs of Galleries, Libraries, Archives, and Museums (GLAM) institutions using BitCurator and gives basic workflows for this software and links to a quick start guide. It details scripts and add-ons to derive more functionality from BitCurator. While short, this document provides an access point to dealing with BitCurator in a GLAM environment and provides a starting point for discussion of the use of BitCurator in a variety of digital curation contexts.

"Integrating Digital Forensics into Born-Digital Workflows: The BitCurator Project" was a poster from the 2012 proceedings of the American Society for Information Science and Technology presented by Martin Gegebach, Alexandra Chassanoff and Porter Olsen (Gengebach 2012, 1-4). The poster provides the preliminary findings from The BitCurator Project at the

University of North Caroline at Chapel Hill, a grant funded project to establish born-digital workflows in GLAM institutions. The poster is a detailed preliminary workflow to incorporating BitCurator into born-digital workflows. This established BitCurator as a forensics tool and shows its place within these processes.

The presentation "Video Camera Identification using Audio-Visual Features" from the 2014 proceedings of the European Workshop on Visual Information Processing in Paris provides a multi-modal approach to color filter array interpolation versus mono-modal approaches that were previously used (Milani 2014). This is an example of the highly technical and algorithmic breakdowns that readers expect when approaching digital forensics literature versus the reality of easily engaged hardware like write blockers or software like BitCurator.

Practical Digital Forensics was published in 2016 by Packt Publishing. It was written by Richard Boddington who has a background in police and intelligence investigations. He is a committee member at the Perth Branch of the Association of Certified Fraud Examiners. This book is an introductory, hands-on guide to beginning digital forensics investigators. It is aimed at investigators working in police or intelligence settings but offers simple step-by-step guides for digital forensics processes. This book was valuable both as a guide to performing digital forensics processes and as a guide to non-archival digital forensics environments.

Martin J. Gengenbach wrote "'The Way We Do It Here': Mapping Digital Forensics Workflows in Collecting Institutions" in fulfillment of his Masters of Science in Library Science at the University of North Carolina, Chapel Hill in 2012. The thesis presents interviews and workflows from several collecting institutions using digital forensics to manage their born-digital media. The detailed information on processes being implemented in other institutions was extremely valuable when developing the workflow for this thesis. Gengenbach's work also

provided a glossary of digital preservation tools and technologies that served as an introduction to the tools discussed in other works.

3. Digital Forensics: Concepts, Workflows and Technologies

3.1 Introduction to Digital Objects

A basic understanding of digital objects is necessary to contextualize much of what will be discussed throughout this thesis. Born-digital objects have only recently begun entering archives, and because of their relative immateriality, it is necessary to explore new preservation practices based on an understanding of digital objects and their carriers (Lischer-Katz 2017).

It has been argued that there is no one digital object, only layers of representation of digital information, each of which plays a role in accessing and understanding digital files. Kenneth Thibodeau defines three layers of representation that are inherent to all born-digital objects:

1. The physical layer, a physical representation or "inscription of signs on some physical medium";
2. a logical layer, a digital representation "recognized and processed by software"; and
3. a conceptual layer, the virtual representation "recognized and understood by a person, or in some cases recognized and processed by a computer application capable of executing business transactions" (Thibodeau 2018).

These concepts can be better understood when applied to a specific example. When dealing with a 3.5" floppy disk, the inscription on the magnetic disc within the plastic square casing is the physical layer. When a computer writes to a floppy disk, the disk spins and a window is opened up by the computer drive, exposing the disk. A magnetic head mounted on the end of a pivoting arm either writes a positive, which looks like a peak on the surface of the disc or leaves a void, which looks like a valley or flat space on the surface of the disk. This creates the physical layer from which the logical layer is interpreted.

The logical layer of a digital object is the binary code that is read by the floppy drive and computer. The peaks and valleys inscribed on the magnetic disk are interpreted as 1s and 0s when the disk is being read back. That binary, enclosed and formatted by a computer file format, is considered the logical layer from which the conceptual layer of the digital object can be accessed and interpreted.

The masses of binary that are commonly found on digital objects require a computer and its software to interpret and present them as files that can be accessed and meaningfully interpreted. The large quantities of 1s and 0s required to create a Word document, for example, are lumped into collections which are called bits. Those bits are categorized by the number of 1s and 0s within the collection. For example, an 8-bit system is based on sets of 8 (eight) 1s and 0s, similarly a 10-bit system uses groups of 10 (ten) 1s and 0s. The bit is what is interpreted by the computer and software to be visually represented as a file on the computer (Boddington 2016, 26).

The process of writing and reading digital objects is not limited to floppy disks. The logical layer likewise can be represented in a variety of file formats, some of which could be obsolete. Collectively these factors make accessing the conceptual layer of digital objects a complex endeavor. While there are some differences across various forms of media, the three layers of representation are inherent to all born-digital objects. For the purposes of this paper, a list of all the different types of born-digital carriers would only be limiting because a well-developed workflow should be able to process any type of born-digital carrier that the archivist encounters, providing the archivist has access to the right type of equipment. While handheld devices such as phones and tablets could eventually enter archives and would need further equipment and processes, these objects are not something archivists are currently receiving or expect to receive in the near future (Doherty 2016).

3.2 Digital Forensics

The role of digital forensics in archival practices is to recover, preserve and validate digital objects. Ensuring the longevity of digital objects is well-established as a challenging preservation practice. Terry Kuny argues that we are currently living in a digital dark age enumerating in depth the challenges that digital preservation faces. The permanent loss of large amounts of digital information and the ongoing obsolescence of information technologies are just two of the most pressing and dire circumstances facing born-digital objects (Kuny 1997). Digital forensics is one of the ways archivists are combating problems of born-digital objects entering archives.

Digital forensics originally developed as a law enforcement tool used for recovering digital evidence in criminal investigations. The objective of traditional digital forensics has moved from catching hackers and white-collar cybercriminals to providing critical trial evidence and more recently to facilitating counter-terrorism and military intelligence exercises. While the concerns of the cultural heritage sector can be far removed from these activities, the methods and tools developed by forensics experts represent a novel approach to key issues and challenges faced by digital archivists (Kirschenbaum et al. 2010, 1; Boddington 2016, 8).

There are a number of similarities between the concepts, principles and methods employed by digital archivists and traditional digital forensics investigators. Included are the concepts of provenance, original order, chain of custody and stratigraphy (Lee 2012; Kirschenbaum 2010). Moreover, the same goals are roughly present in each domain including ensuring the integrity of materials, allowing users to make sense of materials and understand their context and preventing inadvertent disclosure of sensitive data (Lee 2012).

The most widely used definition for digital forensics still heavily reflects traditional digital forensics. This definition was presented in 2001 by the Digital Forensics Research Workshop, defining digital forensics as "the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations" (Duranti 2009). This definition relies heavily on traditional digital forensics as Duranti does not make a distinction between the two fields in this definition because there are so many similarities. Any growth in one field can, in turn, strengthen the other and they should continue to mutually inform one another.

3.3 Authenticity

The concept of preserving digital records within cultural heritage institutions is a relatively recent development in archival studies (Dollar 1993). Yet the language of forensics, which is still used in legal systems today, has been in development since the 1600s when diplomatics was first introduced (Cohen 2015). Diplomatics, the science of document analysis based on a systematic study of extrinsic and intrinsic elements of documentary form, offers methods for authenticating legal and administrative documents (Rogers 2015). In contrast, the objects unlocked by digital forensics in the cultural heritage domain are mostly author works which have been written on word processors since the 1970s (Kirschenbaum 2016). Further, the use of diplomatics as employed in digital forensics to assess the authenticity of digital works, has only been in development since the late 1990s (Rogers 2015, 7). Current archival standards employed in the preservation of digital records draw from concepts that have been well-

established within traditional forensics. Dianne Dietrich and Frank Adelstein distinguish between the goals of traditional digital forensics, which is generally carried out by law enforcement in a legal setting, and archival digital forensics, which is carried out in collecting institutions. In particular, they argue that archival forensics seeks to ensure authenticity whereas traditional forensics seeks to ensure data integrity (Dietrich and Adelstein 2015). This distinction can be cited as the most salient conceptual difference between the two fields, which, as discussed earlier, largely employ similar methods and tools.

Importantly, according to Rothenberg, "authenticity… is not restricted to authentication, as in verifying authorship, but is intended to include issues of integrity, completeness, correctness, validity, faithfulness to an original, meaningfulness, and suitability for an intended purpose" (Rothenberg 2000, 5168). Within traditional forensics, maintaining the original file after an investigation or court case is not required. However, within the context of heritage institutions, archivists typically are required to maintain original copies. The same is true of accessibility, in that archivists aim to provide and maintain public access to collections, while traditional forensics does not deem this necessary.

Furthermore, traditional forensics must often deal with data that has purposely been tampered with, erased or altered, actions that directly compromise the integrity of the material. And since maintaining the physical objects after their use in court is not required, the work required to investigate what happened to the file can also be destructive in traditional forensics (Boddington 2016).

Within collecting institutions, issues of compromised integrity are rarely the result of deliberate actions, especially once files are in the care of an archive. However, it is often impossible to know what state a file will be in upon its arrival at a collecting institution.

Similarly, working with unstable data can be risky. For example, transferring data from its original optical disc format to a disk image can change the overall physicality of a work, and archivists may be required to make minor alterations in order to render the file worthy of preservation and access (Dietrich and Adelstein 2015, 141). The ultimate goal of any collecting institution thus is to preserve records in an authentic manner. This, however, can be complicated for a host of other reasons.

For example, a disk image is a sector-by-sector copy of the data that was stored on a physical medium. As such, the disk image is a "snapshot" of the medium's content, including all allocated files, file names, and other metadata information associated with the disk volume. Once a disk image has been generated, it is then stored as a single file or set of files. The disk image files serve as the most general of containers, because they can contain anything that has been stored on a computer (Woods et al. 2011). Dietrich and Adelstein discuss case studies where bit fidelity is compromised as a result of viewing an archival work using a modern hardware setup. Bit fidelity refers to the binary code encoded within a carrier, and how exact its copy is on a disk image. In this context, authenticity may best be understood in terms of fidelity to an artist's vision. It is the aim of the archivist to provide the user or observer with the same experience they would have had with the original file, however, in the process of transferring the files, it is possible for key components to change subtly as a result of bit fidelity. In these cases, the archivist may be required to compromise the integrity of the work in order to provide the user with a more authentic experience (Dietrich and Adelstein 2015).

Authenticity can also be viewed within the context of carrier versus content. How do we determine the authenticity of digital objects once they are separated from their physical carrier? To what extent is the carrier relevant to authenticity? This issue is still debated with regards to audio-visual files as original works are digitized and discarded to save conservation costs. While

audio-visual archives have traditionally prioritized content over the carrier, discussions around "destructive digitization," i.e. destroying the original object once it has been digitized, still take place (Wright 2011, 6). In *The Real McCoy*, Wright provides a useful framework for assessing the authenticity of audio-visual materials by summarizing hierarchical determinations including the original event, the original recording, the preservation copy through to the master preservation copy (Wright 2011, 8-11) This framework provides context for the preservation issues particular to born-digital object as it acknowledges the authenticity lost at each step of removal from the original event.

Like physical analog material, born-digital objects are also vulnerable to destructive processing techniques. However, in this case the discussion moves from the content within the carrier to the content within original file formats and codecs of born-digital material. For example, if a high resolution, lossless file is received, and the processes used transcode it into a lossy, low-resolution file, much of the original information has become irretrievable, and the object is essentially no longer authentic. While this is an acceptable process for an access copy, it is not sufficient for a preservation master.

Specifically, the future of audio-visual archiving requires a division of attention as increasing numbers of born-digital objects enter archives. Collections institutions will be faced with the duty of care to their existing film and analog videotape elements while planning to look after future formats and media (Cave 2008, 2). For example, the Archives of Ontario currently holds videotape and film elements almost exclusively. However, most current AV production is not recorded using these formats. As a result, the Archive is anticipating a future influx of modern born-digital audio-visual elements.

The article "'Born digital' -Raised an Orphan" by Dylan Cave discusses the future of audio-visual archiving in the face of born-digital objects entering collecting institutions. He explains

that film obsolescence is really an issue of the future while digital preservation is an issue that needs to be addressed presently (Cave 2008). Early file formats for digital media face insurmountable barriers to their preservation, such as codec obsolescence and hardware obsolescence. For example, 2" tape is currently in the last 10 to 20 years of its lifespan, and there aren't enough machines left in the world to digitize the amount of 2" tape that exists (Kuny 1997). Well-preserved film, in contrast, can have a lifespan of 100s of years if it is cared for properly. Magnetic tape can last decades (Klijn and Lusenet 2008, 81). Digital technology progresses at an exponentially greater pace than analog technology and even greater than magnetic tape technology, making obsolescence a constant and imminent threat.

Similarly, optical media such as CDs, CD-Rs and DVDs show poor stability for storing data. Optical media is not recommended for long-term storage of digital information (Iraci 2012). This research is necessary context for my own as it asserts that digital information must be removed from all DVD media and most CD media if it is to be stored properly.

3.4 Diplomatics

As mentioned earlier, diplomatics is the science of document analysis based on a systematic study of extrinsic and intrinsic elements of documentary form (Rogers 2015). Digital diplomatics includes both the use of digital computing methods to support classical diplomatics and the use of diplomatic methods to authenticate digital documents (Duranti 2009, Duranti 2010). This discipline gives archivists a methodology for analyzing the identity and integrity of digital records in electronic systems and thereby assessing their authenticity. For digital records to be verifiable through diplomatic principles they must consist of:

1. user-generated data (content);
2. system generated metadata identifying source and location;
3. application generated metadata managing the look and performance of the record, ex. native file format;
4. file system metadata; and
5. user generated metadata describing the data (Rogers 2014, 7).

Digital Forensics systems and practices are capable of capturing all of this information. Digital diplomatics, based on a foundation of traditional diplomatic principles, can identify digital records through their metadata and determine what metadata needs to be captured, managed, and preserved (Rogers 2014, 16-18). Traditional diplomatics uses key characteristics of a document to verify its authenticity such as the ink used to write the document. If we consider fonts the modern analog to ink, diplomatics has already been used to verify the authenticity of documents. During a 2016 investigation into political corruption, documents were determined to be forgeries based on the use of the Microsoft default font for word, Calibri, which

was not widely available until a year after the documents were supposedly created. Type designer Thomas Phinney proved this and other forgeries using his font expertise since first approached as an expert witness in 1999 (Fleishman 2017). Fonts can be a particularly challenging characteristic of a document to capture as there are many variations with little documentation, and it is often easier to extract just the text information from a legacy file format but fonts are already in use as evidence so they must be captured for archival documents to serve as records.

Public records are generally admissible for the truth of what they self-indicate and are presumed trustworthy (i.e. reliable, authentic, accurate) in the legal system (Duranti 2009). Given this understanding, it is vital that the Archives of Ontario, as a depository for all public records from the province of Ontario, preserve not only the content of digital documents but also the physicality and form.

3.5 Digital Preservation

The development of digital preservation references models has been the subject of a great deal of research in the past two decades. Out of these efforts, the leading model embraced by the digital preservation and archival community is The *Open Archival Information System* (OAIS). The OAIS reference model provides a framework of metadata in the form of information packages which "include a digital object and other types of information that should be associated with the digital object in order to preserve and provide meaningful access to it over time"(Lee 2010, 4026).

These information packages are broken down into the three main components of the archival process: ingestion, archival storage, and access. The Submission Information Package (SIP) is ingested into the system and contains the data object and its content information. The SIP provides the system with the descriptive information necessary to create the Archival Information Package, which is stored and preserved in the system for access by consumers through the Dissemination Information Package (DIP) (IASA 2018).

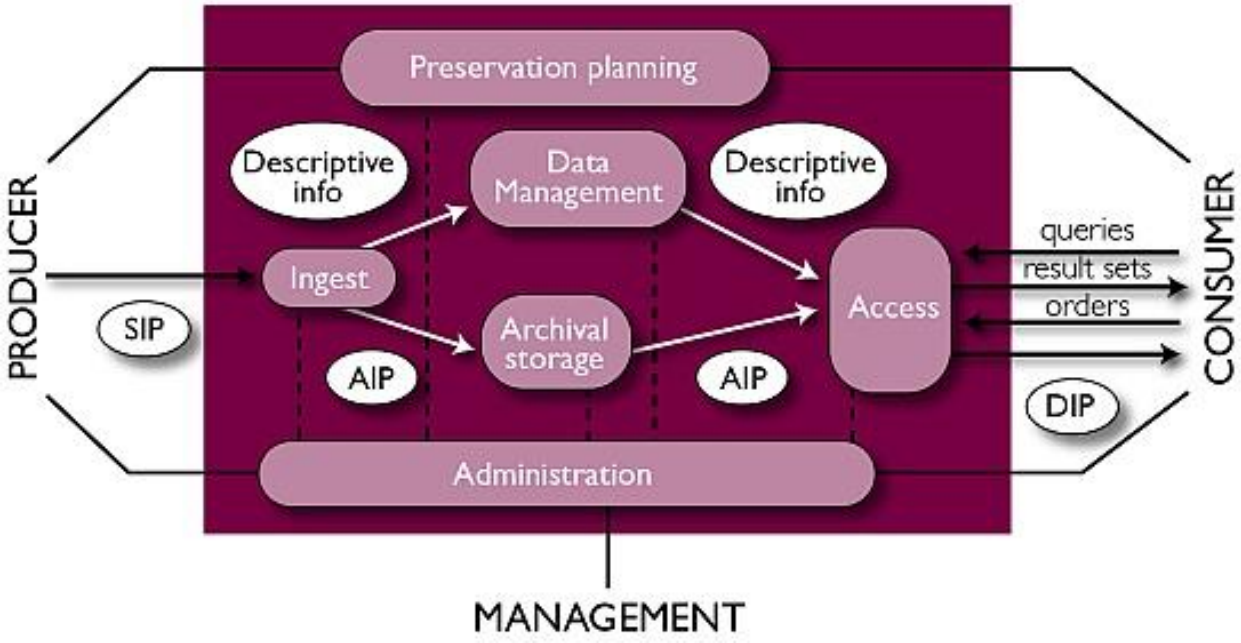


Figure 1 OAIS Functional Entities Model from IASA guide to digital preservation (IASA 2018)

The metadata contained within these packages provides descriptive information as well as information on the packaging, representation and preservation of the data object. However, it is not the data object that determines the standards on which these packages are built but a designated community among the archive's users that is "expected to independently understand the archived information in the form in which it is preserved and made available by the OAIS" (Lavoie 2014, 10). Therefore, the needs and requirements of this designated community determine what metadata should be included and how it is generated. In the case of the Archive, while its mandate may be to serve the general public, the designated community is that which has the expertise to understand the content independent of assistance, such as court researchers, department researchers, researchers or experts of that particular domain for instance from a University. As a result, the SIP, AIP, and DIP will need to be standardized once a preservation system is in place, as the preservations metadata will vary in both scope and complexity from one system to another. The metadata contained in the information packages can be used as evidence of authenticity as discussed in section 2.4 on diplomatics. The preservation metadata and fixity metadata created by digital forensics processes should be used in each of these packages to create a robust information package.

3.6 Digital Forensics Workflows and Technologies in Cultural Heritage Institutions

The community of digital forensics practitioners within Cultural Heritage institutions has been steadily growing. While the field is still relatively immature, a significant body of published works deal with digital forensics in these institutions. Importantly, this community has developed its own digital forensics tools. An example is the BitCurator digital forensics tool, which is a set of digital forensics tools that were developed and packaged together by a member-based consortium. A 2013 report created for the BitCurator project titled "From Bitstreams to Heritage" identifies the incorporation of digital forensics into collecting institution workflows as the greatest challenge facing full implementation of digital forensics practices (Lee et al 2013, 23). The BitCurator Project and resulting tool have helped to make this is a more achievable goal by offering software that is easily implemented (Huebner 2008).

In their presentation “Enabling Digital Forensics Practices in Libraries, Archives and Museums: The BitCurator Experience” Lee and Woods (2014) seek to establish the needs of collecting institutions using BitCurator and give basic workflows for this software and links to a quick start guide. The presentation details scripts and add-ons to derive more functionality from BitCurator. This document provides an access point to dealing with BitCurator in a collecting environment and provides a jumping off point to discuss the use of BitCurator in a variety of institutions. Similarly, Gengenbach provides preliminary strategies for incorporating BitCurator into born-digital workflows (Gengenbach et al 2012). This established BitCurator as a prevalent forensics tool and informed its place within these processes. John Durno presents solid reasoning for using the dd command to create raw disk images as they are likely to have the most longevity and prevalence (Durno and Trofimchuk, 2015).

Another useful source for this project is Matthew Gengenbach's Masters thesis from the University of North Carolina, Chapel Hill. In this thesis, Gengebach (2012) details the workflows of several collecting institutions. These are valuable when determining specific and proven uses for hardware and software forensics systems. Of particular value is the appendix with definitions of hardware and software tools for digital forensics workflows which can serve as an introductory guide for beginner digital archivists. I referenced heavily the City of Vancouver Archives workflow and documentation Gengenbach provides as they are another Canadian governmental archive.

The presentation "Video Camera Identification using Audio-Visual Features" from the 2014 proceedings of the European Workshop on Visual Information Processing in Paris provides a multi-modal approach to color filter array interpolation versus mono-modal approaches that were previously used (Milani et al 2014). This is an example of the highly technical and algorithmic breakdowns that readers expect when approaching digital forensics literature versus the reality of easily engaged hardware like write blockers or software like FTK Imager. Case studies like this one highlight the need for a preservation master. We cannot anticipate all the applications or needs of digital forensics but by creating a bit level preservation master, any disk image can be used for future processes that cannot be anticipated by the processing archivist. Similarly, digital forensics has been used for obtaining information from DSL cameras and various audio formats and devices (Camlot 2015; Aminova, Trapeznikov, and Priorov 2017).

Disk images serve as a preservation master and working copy of the original media. The process of creating disk images is well established as a digital preservation practice. It is necessary to remove digital objects from their carriers because the physical layer of representation for most born-digital objects has a very short shelf life when compared with previous archival materials such as paper (Gow and Ross 1999; Casey 2015). The common

approach that has been established for digital forensics is to preserve the logical and conceptual layers of representation digitally separate from the physical media (Woods et al. 2011). Digital forensics forces its practitioners to confront the dual identity of digital data both as an abstract, symbolic entity and as material marks or traces indelibly inscribed in a medium (Kirschenbaum et al. 2010, 5).

Figure 2 FRED Tower version used at the Archives of Ontario

While many pieces of hardware make the processes of digital forensics possible, the two hardware systems that form the basis of the workflow for the Archives of Ontario are the Forensic Recovery of Evidence Device (FRED) and Kryoflux. The FRED workstation in use at the Archives of Ontario is the FRED tower without RAID storage (Digital Intelligence 2018). This unit is ideal for modern digital carriers such as hard drives, USB storage devices, CF cards,

and SD cards. It comes pre-installed with software that is best suited to traditional digital forensics such as Tableau Imager and Encase.

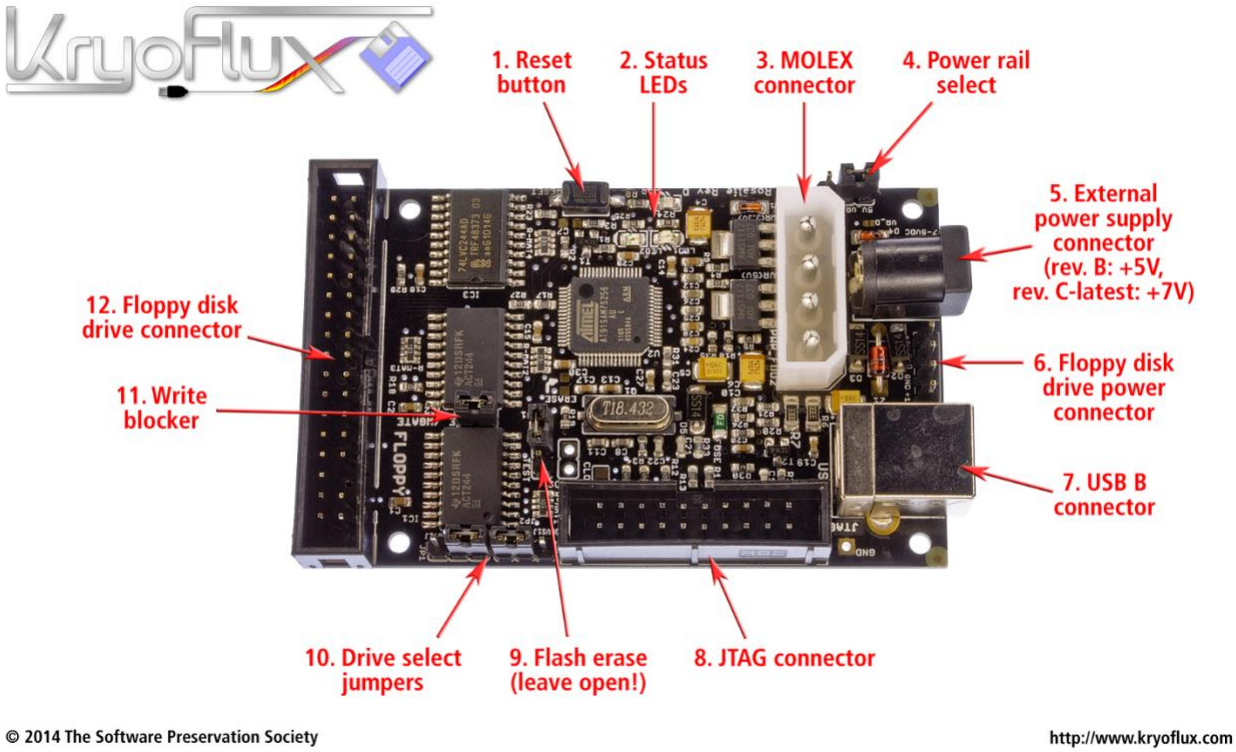


Figure 3 Diagram of the Kryoflux Unit

Kryoflux is a hardware and software combination that allows contemporary computers to interface with vintage floppy disk drives. It also allows 3.5” and 5.25” floppy disk drives to read disks formatted by almost any system.

Given that the FRED is built for traditional Digital Forensics work, it is not an ideal system for cultural heritage institutions. In order to make the FRED effective for the Archives of Ontario, I suggested adding the Kryoflux hardware and software to it since floppy disks comprise a large portion of their holdings. The Tableau software also is not ideal for legacy carriers and systems, to solve this I installed BitCurator, ClamAV, and FTK Imager. ClamAV is a command line based antivirus software, and FTK Imager is a disk imaging software. Before

these additions, the FRED had a very limited usefulness to the Archive. The additional hardware and software have made the FRED a more robust machine capable of handling all the born-digital carriers the archive currently receives. I have lovingly dubbed this altered machine the FrankenFRED when discussing the modifications with the Canadian digital forensics community.

In conclusion, the relative immateriality of digital objects when compared with traditional physical archival materials make it necessary to explore new preservation practices based on an understanding of digital objects and their carriers. Digital forensics is one such new preservation practice that allows cultural heritage institutions to validate, preserve, and recover digital objects. The validation of digital objects is achieved through the concept of authenticity, which evaluates the trustworthiness of materials based on its reliability, authenticity, and accuracy. The Open Archival Information Systems (OAIS) model is the industry standard for digital preservation. It covers three components of the archival process: ingest, storage and access. The dual identity of digital data both as an abstract, symbolic entity and as material marks inscribed on a medium necessitates the use of tools such as BitCurator to recover content. These concepts were used to develop a workflow for the Archives of Ontario.

4. Archives of Ontario Custom Workflow

The Archive has collecting workflows in place for born-digital carriers, but they do not have storage in place for the digital preservation packages. My workflow will be integrated after the objects have been received as this is a well-defined process and will end before their storage as a suitable digital repository has not been built. Theoretically, the workflow spans the stages of *Ingest* and *Archival Processing* in OAIS (See Fig. 1 above). This is by virtue that it (a) facilitates the processing of digital objects, and (b) it provides metadata evidence of authenticity necessary for the creation of archival information packages. As such, the workflow can be further integrated as an element of a digital archival repository, which the Portfolio Management Office is planning to implement in the near future. While the generation and storage of AIPs and the construction of a digital repository is an integral part of digital preservation that I consulted on, this work will continue to be conducted by others within the Portfolio Management Office and the provincial IT cluster placing it outside the scope of my project. The same is true of files transferred via a network or the internet directly to the archive. The workflow I developed only addresses the acquisition and archiving of born-digital objects transferred via digital carriers such as hard drives, modern digital carriers, optical media, or floppy discs. I will address extracting content from carriers, preserving, and authenticating that content but not the long-term digital preservation needed. (See Appendix I. Current vs. Proposed State Diagram)

Objects received on born-digital carriers will be identified and given a unique identifier by the processing archivist and delivered to the Digital Preservation Lab. There the physical carrier will be photographed and all label and identifying information recorded. The carriers will be processed with different equipment based on their format. The 3.5” and 5.25” floppy disks will be processed using the Kryoflux unit and software. Any optical disc media will be processed

with the FRED's optical drive. The majority of modern carriers can be read with the FRED with no extra peripherals via the Hot Swap Bays or Tableau UltraBay. Either FTK Imager, Tableau Imager, or Guymager software will be used to create a Raw (dd) disk image.

The image will be duplicated; one copy becoming the preservation master and the other to be processed. The inclusion of a preservation master is necessary for the archive as hidden or deleted data could become relevant in the future and because a preservation master should ideally be part of the AIP. Keeping a copy of the entire contents of the original disk is necessary in this institution. The Working Disk Image will undergo a virus check either via the command line using ClamAV or with Windows Defender.

The disk image for processing will be put through the BitCurator Reporting Tool and fiwalk to produce logs of user activity, disk image contents, and disk image creation such as:

a) DFXML reports on the disk image manifest (Woods et al. 2011)
b) checksums
c) System log information (Lee 2013)

These reports and metadata serve to fulfill standards in OAIS and diplomatics such as authenticity and fixity. BitCurator Disk Image Access Tool will be used to export image contents for processing. File identification software such as QuickView Plus, DROID (The National Archives, 2018), Xena (National Archives of Australia, 2018) will be used to determine the individual file formats and open the files for processing. The processing archivist will then describe the contents of the disk image in an Excel file and export an .xml document of the description. Metadata standards for this description are well established within the archive and use a slightly modified RAD.

Once the file has been processed, the metadata, photos, logs, records, checksums, processed disk image and preservation master disk image will be packaged with Bagger. This bag will become part of a Submission Information Package (SIP) to be submitted to a digital repository.

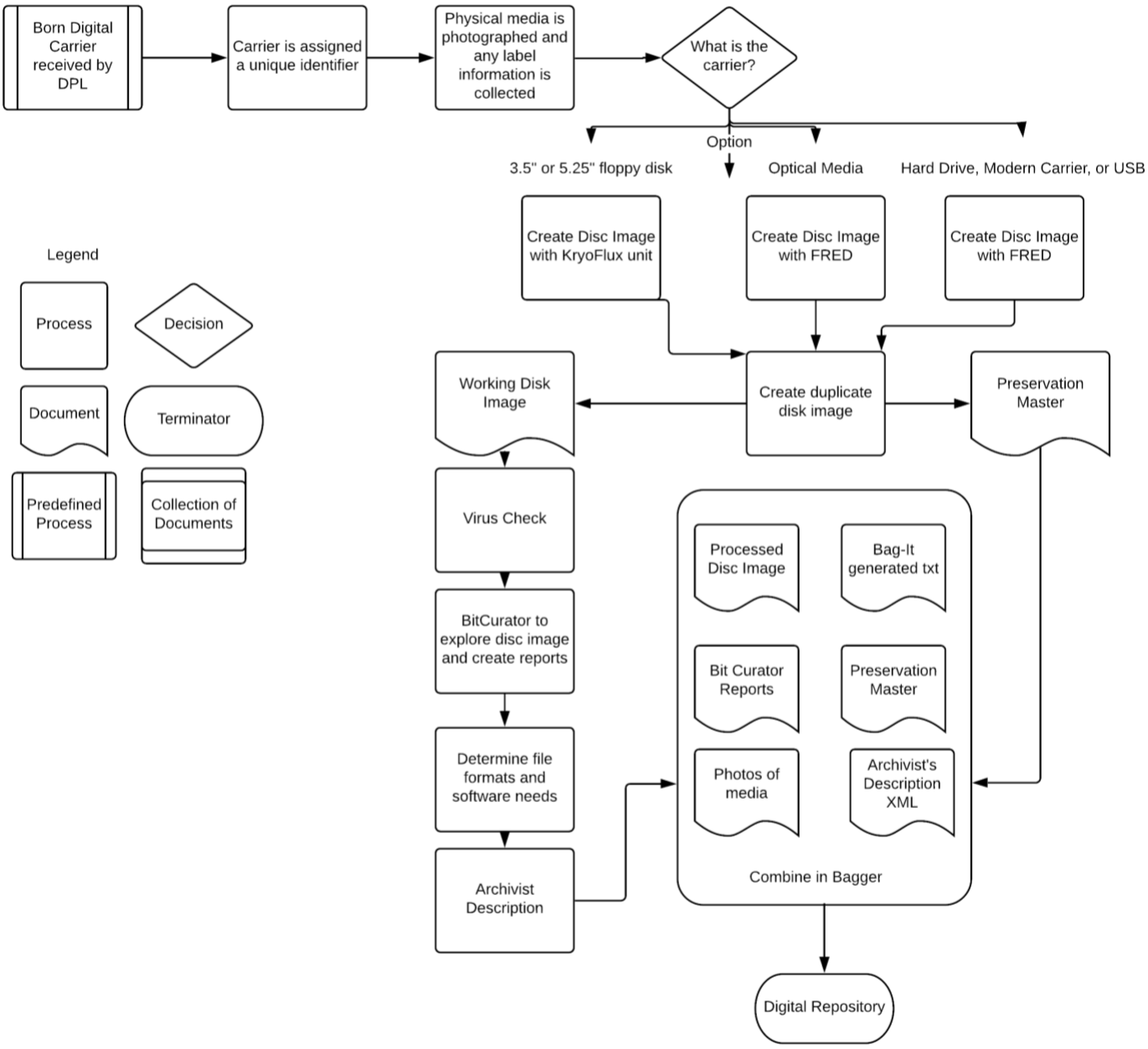


Figure 4 Workflow developed for Archives of Ontario

The processes within this workflow have focused on simplicity to create a low barrier to entry for archivists that will be approaching these concepts and processes for the first time. This workflow is preliminary and will likely undergo several iterations within the Archive as needs evolve and expertise develops allowing for more advanced processes. Most importantly, once a Digital Preservation System is in place, the workflow will need to be altered to suit the needs of that system. The workflow structure was chosen based on recommendations from *The Basics of Process Mapping*, an introductory text on creating process maps (Damelio 2011). As the Archives of Ontario does not use a standardized modeling language I built this to closely resemble the workflows already in use at the institution.

At the time of writing, the Portfolio Management Office had not procured all the hardware necessary to fully implement the workflow. Kryoflux hardware and software had not been ordered. Also, as the FRED does not have an internal RAID, a staging RAID needs to be purchased to allow for the processing of large carriers. I documented specifications and recommendations for this equipment, but an order had yet to be placed at time of writing.

Beyond the operational needs and mandate of the Archives of Ontario, I focused on creating a process that could be easily explained and taught to archivists without a technical background or digital archiving training. All archivists within the institution are expected to be generalists, and all archivists must be trained on all processes. This limited the scope of the digital preservation practices I used to those that are easily understood and trained.

5. Directions for Future Research

Work is currently being conducted within the archive to research storage for digital preservation systems. This has been noted as “Digital Repository” within my workflow but the processes will most likely need to be revised to accommodate the metadata and disk image format requirements of the specific digital repository. Likewise, emulation has been put forward as an area of digital preservation that will need to be researched and implemented in the future.

The processes for receiving digital files via FTP or other network transfer are also being developed. These files have not been addressed within my workflow as the processes have yet to be defined, however, the potential workflow is addressed in the Proposed State. (See Appendix I. Proposed vs. Current State Diagram). The scope of this workflow only encompasses born-digital objects on physical carriers. The processes for digital files transferred directly to the institution will need to match closely the Archival Information Package produced for files on born-digital carriers but until such time as these transfer protocols are in place they cannot be included in the workflow.

The processes I have proposed are a small part of the larger ecosystem of digital requirements the Archives of Ontario has yet to fulfill. The available hardware, software, and processes can be used for any immediate requests made before the hardware is in place to fully implement these processes.

6. Conclusion

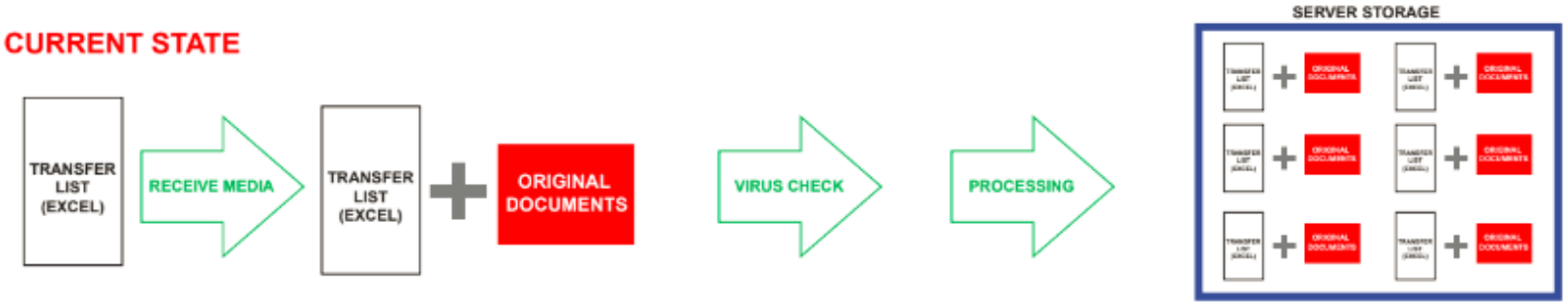
I have addressed my research question by creating a workflow that integrates digital forensics tools and practices into the existing business practices of the Archives of Ontario. The information gathered through this workflow can be used to determine the authenticity of the digital objects the archive is collecting. This information and the digital preservation systems I have consulted on procuring will provide an environment for digital preservation within the archive. My workflow and suggested processes were based on the available research from the digital archiving and digital preservation community.

Some digital preservation practitioners argue that digital preservation is capturing more than we realize (Harvey 2008; Bengtson 2012). While this can be a point of contention, certainly, the systems, tools, and standards are well tested and available for institutions to implement viable digital preservation practices (Erway 2012). Digital forensics methodologies can support archival processing and in doing so perform a vital role in mitigating the effects of the current digital dark age. This workflow provides an important step toward preserving the Ontario provincial digital records for future generations.

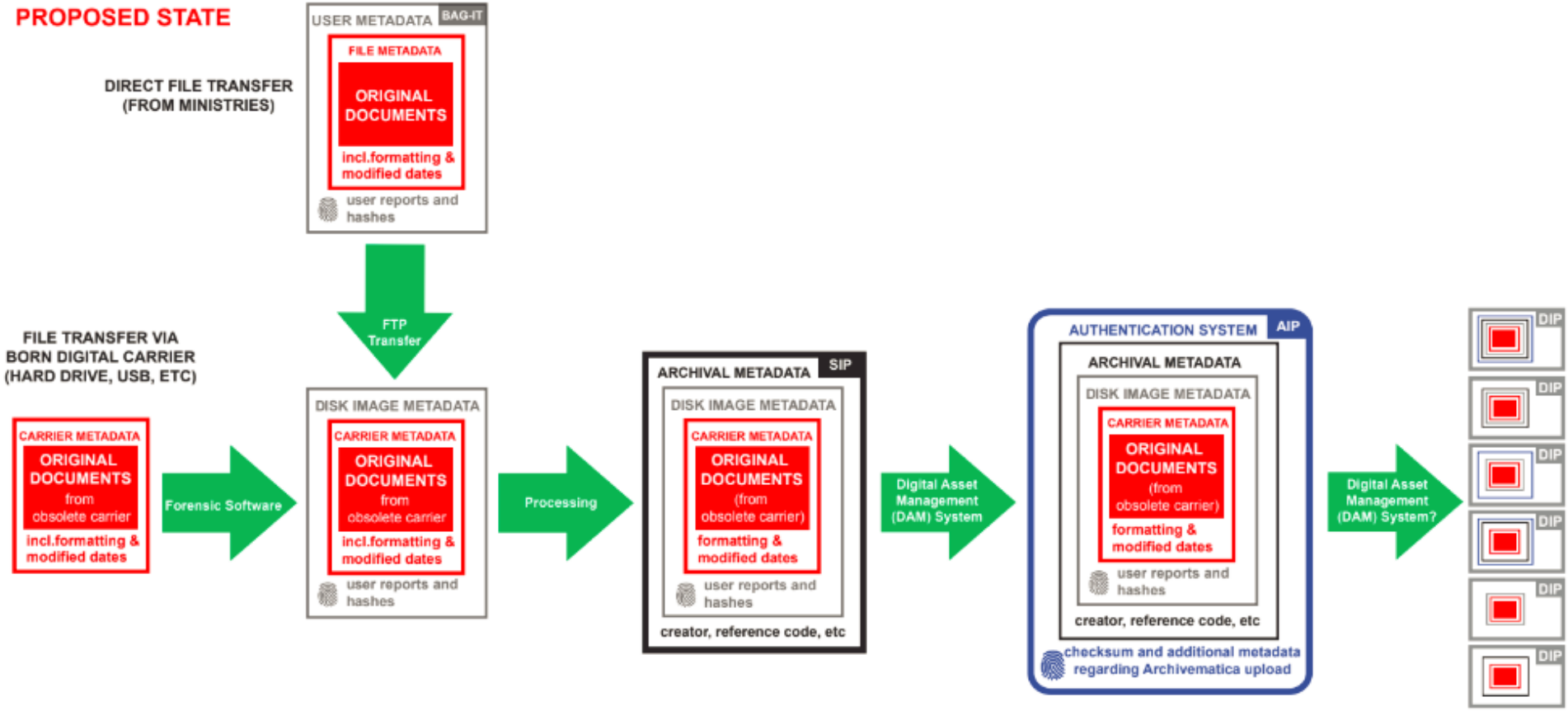
Appendix I. Current vs. Proposed State Diagram

This diagram depicts the current process for metadata collection of born-digital objects and how the process could be altered to meet digital preservation standards at the Archives of Ontario. It was produced in collaboration with the Portfolio Management Office as a tool to train the archivists on the metadata collection that needs to be implemented for born-digital objects.

CURRENT STATE



PROPOSED STATE



Appendix II. Resources for training and use

Univeristy of Toronto online repository of information
https://connect.library.utoronto.ca/display/DPG/Workshops+and+Class+Visits

FRED Manual
https://digitalintelligence.com/support/knowledgebase/3-setup-troubleshooting/docs/112-fred-manual

BitCurator Consortium: Getting Started
https://www.bitcuratorconsortium.org/getting-started

Kryoflux Manual
https://www.kryoflux.com/?page=download

The Archivist's Guide to KryoFlux
https://github.com/archivistsguidetokryoflux/archivists-guide-to-kryoflux

State Archives of North Carolina Introduction to Bagger
https://www.youtube.com/watch?v=VWNaUUeiLYI

Appendix III. Published workflows from other Collecting Institutions

The following are digital forensics workflows that have been published by other collecting institutions and on which I relied heavily when determining best practices to implement within the workflow I developed for the Archives of Ontario.

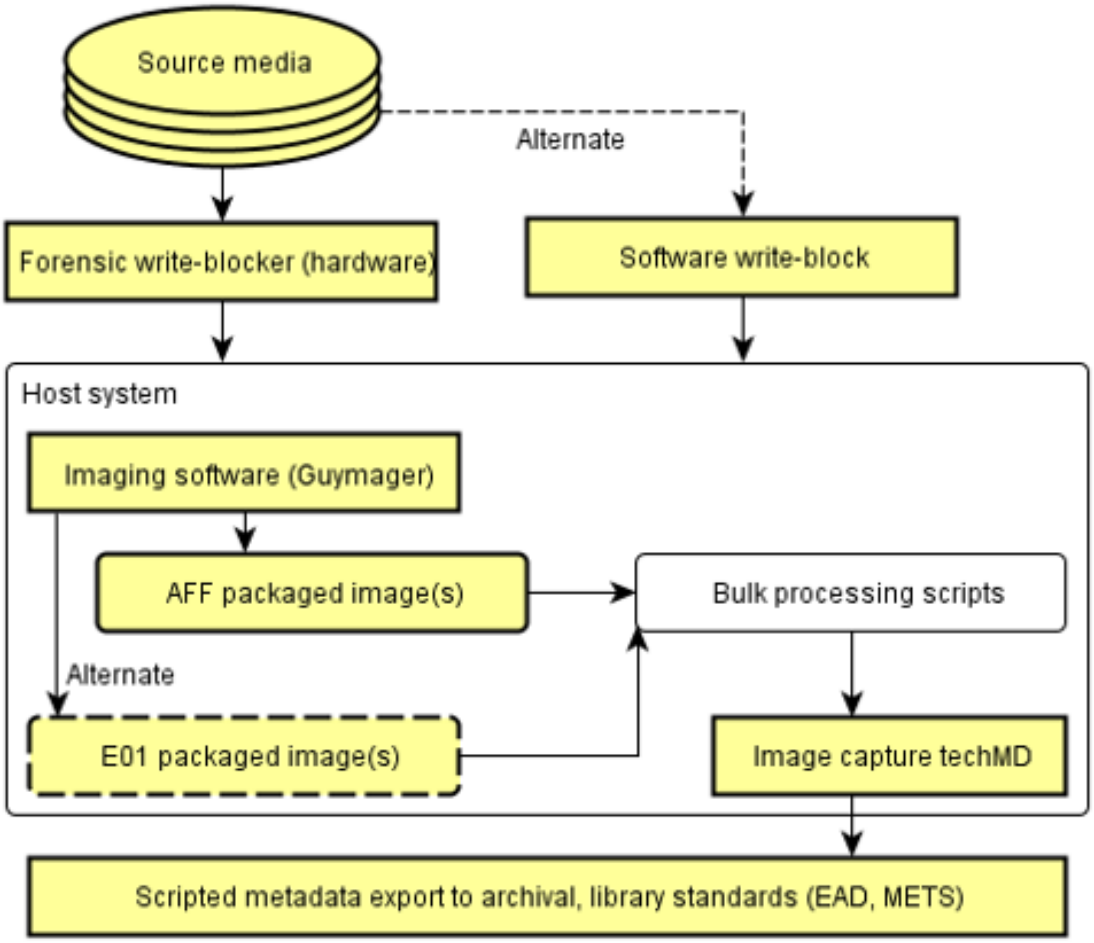


Figure 5 Dalhousie Forensic imaging workflow for BitCurator (Dalhousie University 2018)

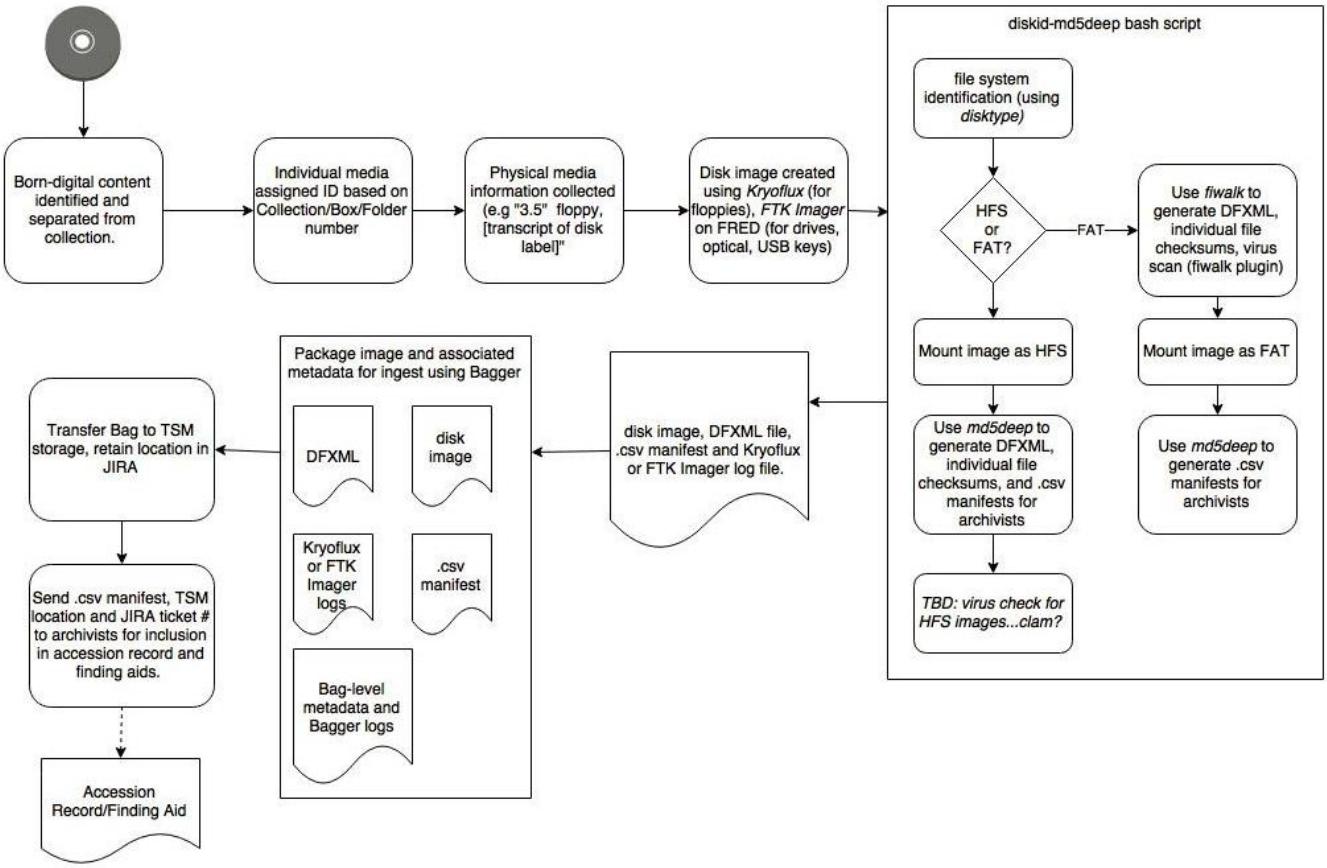


Figure 6 University of Toronto Fisher Digital Holdings Workflow (Whyte 2018)

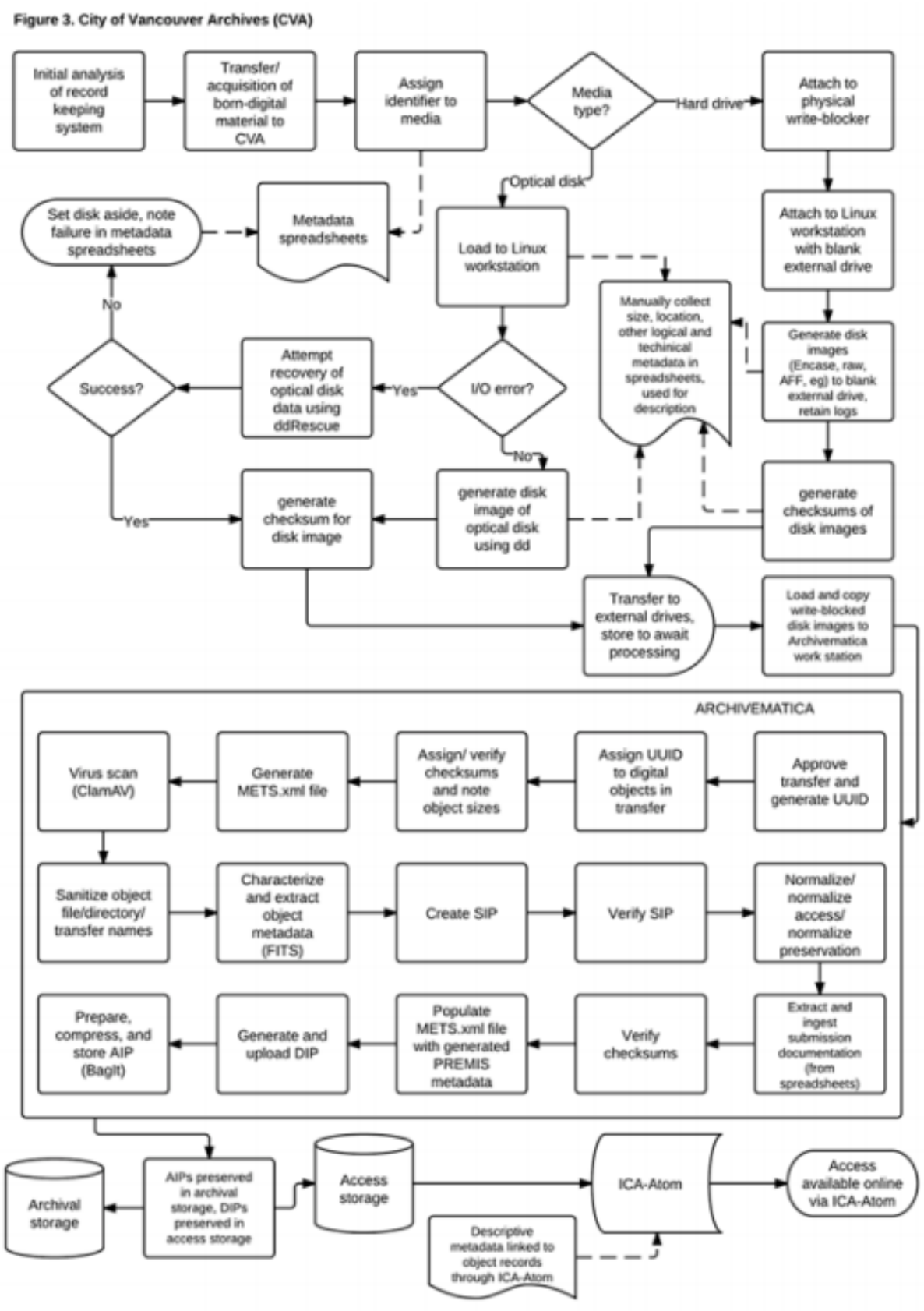


Figure 7 City of Vancouver Archives (Gengebach, 2012)

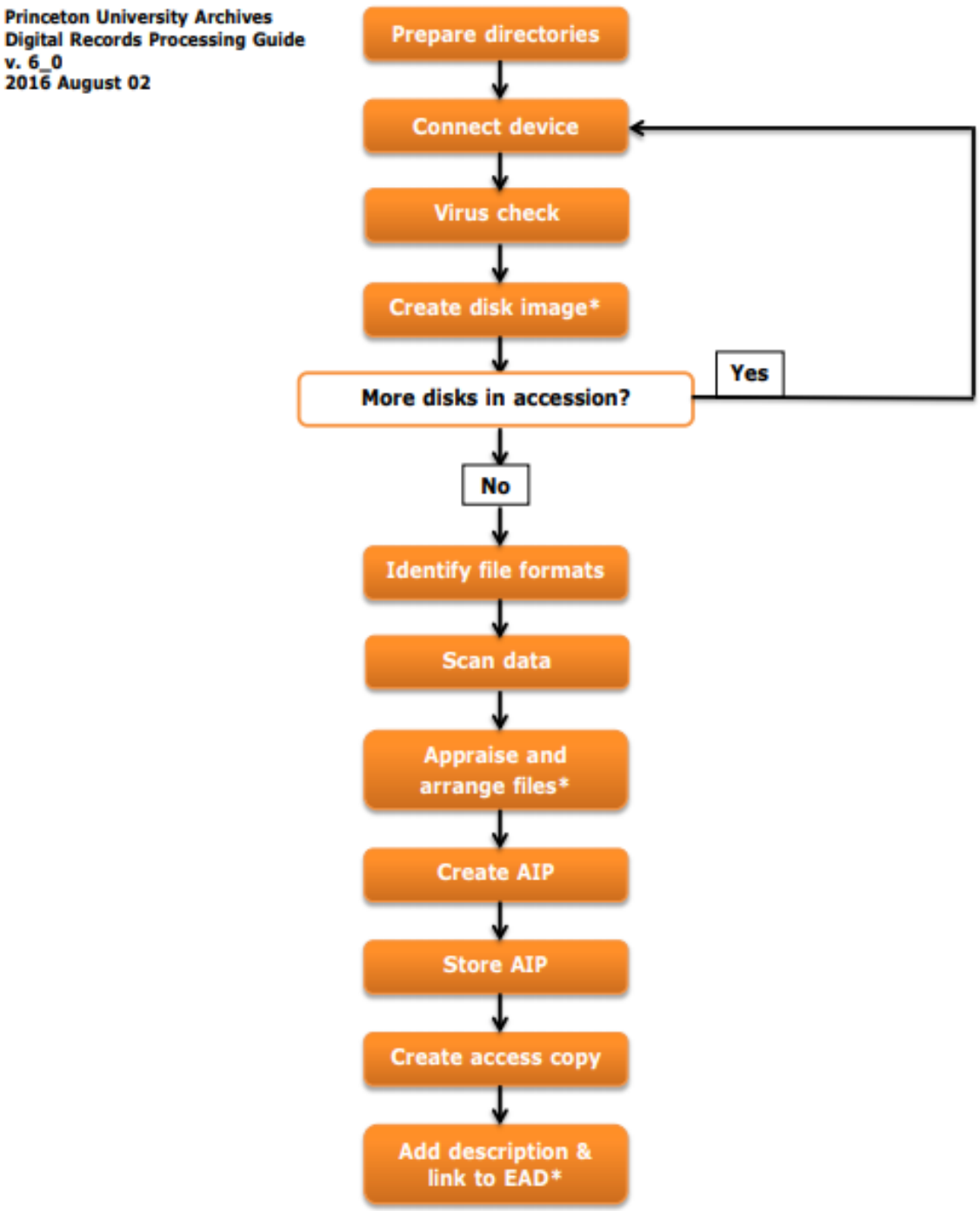


Figure 8 Princeton University Archives (Princeton University Library 2018)

Reference List

Aminova, E, I Trapeznikov, and A Priorov. 2017. “Overview of Digital Forensics Algorithms In Dslr Cameras.” *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences.* XLII-2/W4 199. doi:10.5194/isprs-archives-XLII-2-W4-199-2017.

Archives of Ontario. Documenting a Province: The Archives of Ontario at 100 / Chronique d’Une Province: Le Centenaire Des Archvies Publiques d’Ontario. Canada: University of Toronto Press, 2003, xv-xviii.

Archives and Recordkeeping Act, 2006, S.O. 2006, c. 34, Sched. A, s. 7.

Boddington, Richard. 2016. *Practical Digital Forensics*. Birmingham: Packt Publishing.

Bengtson, Jason. 2012. Preparing for the age of the digital palimpsest. *Library Hi Tech* 30 (3): 513-22.

Camlot, J. 2015. “Historicist Audio Forensics: The Archive of Voices as Repository of Material and Conceptual Artefacts.” *Interdisciplinary Studies in the Long Nineteenth Century* 19 (21). doi: http://doi.org/10.16995/ntn.744

Casey, Mike. 2015. “Why Media Preservation Can’t Wait: The Gathering Storm.” *IASA Journal* 44.

Cave, Dylan. (2008). “”Born Digital” — Raised an Orphan? Acquiring Digital Media through an Analog Paradigm.” *The Moving Image: The Journal of the Association of Moving Image Archivists*. 8 (1): 1-13.

Cohen, Frederick B. 2015. “Digital diplomatics and forensics: Going forward on a global basis.” *Records Management Journal* 25 (1): 21-44.

Dalhousie University. 2018. “Digital Preservation: Building a trusted digital repository.” Accessed June 5, 2018, https://libraries.dal.ca/research/digital-initiatives/digital-preservation.html.

Damelio, Robert. 2011. The Basics of Process Mapping. Productivity Press. New York, NY.

Dietrich, Dianne, and Frank Adelstein. 2015. “Archival Science, Digital Forensics and New Media Art.” *Digital Investigation* 14. doi: 10.1016/j.diin.2015.05.004

Digital Intelligence. *FRED Forensic Workstation*. Accessed May 23, 2018, https://digitalintelligence.com/store/products/fred

"Digital Forensics Lab." Dalhousie University Libraries. Accessed November 2, 2017. https://libraries.dal.ca/find/university-archives/digitalarchives/forensicslab.html

Doherty, Eamon P. 2016. *Digital Forensics for Handheld Devices*. London: CRC Press.

Dollar, Charles M. 1993. "Archivists and Records Managers in the Information Age." *Archivaria* 36.

Duranti, Luciana, and Barbara Endicott-Popovsky. 2010. “Digital records forensics: A new science and academic program for forensic readiness.” *The Journal of Digital Forensics, Security and Law* 5 (2): 45-62.

Duranti, Luciana. 2009. "From digital diplomatics to digital records forensics." *Archivaria* 68: 39-66.

Duranti, Luciana, and Barbara Endicott-Popovsky. 2010. Digital records forensics: A new science and academic program for forensic readiness. *The Journal of Digital Forensics, Security and Law: JDFSL* 5 (2): 45-62.

Durno, John, and Jerry Trofimchuk. 2015. "Digital forensics on a shoestring: A case study from the University of Victoria." Victoria, Canada.

Erway, Ricky. 2012. *You've got to walk before you can run: first steps for managing born-digital content received on physical media*. Dublin, Ohio: OCLC Research.

Fleishman, Glenn. 2017. "Meet the Font Detectives Who Ferret Out Fakery | Backchannel." *Wired*, September 20. https://www.wired.com/story/meet-the-font-detectives-who-ferret-out-fakery/.

“FRED System Selection.” Digital Intelligence Inc. Accessed October 10 2017. https://www.digitalintelligence.com//.products/fredselect

Gengenbach, Matrin. 2012. “ ‘The way we do it here’: Mapping digital forensics workflows in collecting institutions.” Unpublished master’s thesis, The University of North Carolina at Chapel Hill, Chapel Hill, North Carolina.

Gengebach, Matrin, Alexandra Chassanoff, and Porter Olsen. 2012. “Integrating Digital Forensics into Born-Digital Workflows: The BitCurator Project.” Proceedings of the *American Society for Information Science and Technology* 49 (1): 1–4. doi: 10.1002/meet.14504901343

Gow, Ann and Seamus Ross. 1999. "Digital Archeology: Rescuing Neglected and Damaged Data Resources." A JISC/NPO Study within the Electronic Libraries Programme on the Preservation of Electronic Materials, Library Information Technology Centre, South Bank University, London.

Harvey, Ross. 2008.“So where’s the black hole in our collective memory? A Provocative Position Paper (PPP).” Digital Preservation Europe.

Huebner, Ewa, and Zanero Stefano, eds. 2008. Open Source Software for Digital Forensics. Springer.

IASA. 2018. “The Open Archival Information System (OAIS).” *Guidelines on the Production and Preservation of Digital Audio Objects (web edition)*. Accessed May 29, 2018, https://www.iasa-web.org/tc04/open-archival-information-system-oais.

Iraci, Joe. 2011. "The Stability of DVD Optical Disc Formats." *Restaurator* 32 (1): 39-59. doi:10.1515/rest.2011.004

Iraci, Joe. 2012. “The Effect of Jewel Cases on the Stability of Optical Disc Media.” *Restaurator* 33: 17-47. doi: 10:1515/res-2012-0002.

Jones, Janna. 2012. *The past is a moving picture: Preserving the twentieth century on film.* University Press of Florida, Gainesville, FL.

Kirschenbaum, Matthew, Richard Ovenden, Gabriela Redwine, and Rachel Donahue. 2010. *Digital forensics and born-digital content in cultural heritage collections*. Council on Library and Information Resources No. 149. Wahington, D.C.

Kirschenbaum, Matthew G. 2008. *Mechanisms: New Media and the Forensic Imagination*. MIT Press. London, England.

Kirschenbaum, Matthew G. 2016. *Track Changes: A Literary History of Word Processing*. Cambridge, MA: Harvard University Press.

Klijn, Edwin, and Yola De Lusenet. 2008. "Tracking the Reel World: A survey of audiovisual collections in Europe." European Commission on Preservation and Access. Accessed May 27, 2018, http://www.tape-online.net/docs/tracking_the_reel_world.pdf.

Kryoflux. 2018. *Kryoflux Manual, Manual Revision 1.20, DTC version 2.72*. https://www.kryoflux.com/?page=download.

Kuny, Terry. 1997. "A Digital Dark Ages? Challenges in the Preservation of Electronic Information." *63rd IFLA Council and General Conference.*

Lavoie, Brian F. 2014. "The open archival information system reference model: Introductory guide." *Microform & imaging review* 33 (2): 68-81.

Lee, Cal, and Kam Woods. 2014. "Enabling Digital Forensics Practices in Libraries, Archives and Museums: The BitCurator Experience." Lecture presented at The Digital Forensic Research Conference, Denver, CO, August 2014.

Lee, Christopher A. 2012. "Digital Forensics Meets the Archivist (And They Seem to Like Each Other)," Provenance, Journal of the Society of Georgia Archivists 30 no. 1.

Lee, Christopher A. 2010. "Open archival information system (OAIS) reference model" *Encyclopaedia of Library and Information Science*. 4020-4030

Lee, Christopher A., Matthew Kirschenbaum, Alexandra Chassanoff, Porter Olsen, and Kam Woods. 2012. "BitCurator: tools and techniques for digital forensics in collecting institutions." *D-Lib Magazine* 18 (5/6): 14-21.

Lee, Christopher A., Kam Woods, Matthew Kirschenbaum, and Alexandra Chassanoff. 2013. "From Bitstreams to Heritage." A Product of the BitCurator Project.

Levi, Charles. 2011. "Five hundred 5.25-inch discs and one machine: A report on a legacy e-records pilot project at the archives of Ontario." *Archivaria* 72: 239.

Lischer-Katz, Zack. 2017. "Studying the Materiality of Media Archives in the Age of Digitization: Forensics, Infrastructures and Ecologies." *First Monday* 22 (1). doi: 10.5210/fm/v22i1/7263

McKay, Judy and Peter Marshall. 2007. "Driven by two masters, serving both: The Interplay of Problem Solving and Research in Information Systems Action Research Projects." In

Information Systems Action Research: An Applied View of Emerging Concepts and Methods, edited by Ned Kock, 131-158. Springer, Laredo, Texas.

Meister, Sam, and Alexandra Chassanoff. 2014. Integrating digital forensics techniques into curatorial tasks: A case study. *International Journal of Digital Curation* 9 (2): 6-16.

Milani, S., L. Cuccovillo, M. Tagliasacchi, S. Tubaro, and P. Aichroth. 2014. "Video Camera Identification using Audio-Visual Features." in *Proceedings of the 2014 European Workshop on Visual Information Processing (EUVIP 2014)*. 1-6. doi:10.1109/EUVIP.2014.7018382.

Ministry of Government and Consumer Services. 2018. "About the Archives of Ontario." Accessed June 4. http://www.archives.gov.on.ca/en/about/index.aspx

National Archives of Australia. 2018. Xena: Software for Digital Preservation. Accessed June 5, 2018, http://xena.sourceforge.net/.

Princeton University Library. 2018. "Born-Digital University Archives Workflows." Accessed June 5, 2018, https://rbsc.princeton.edu/workflows/born-digital/university-archives.

Rogers, Corinne. 2015. "Diplomatics of born digital documents – considering documentary form in a digital environment." *Records Management Journal* 25 (1): 6-20.

Rothenberg, Jeff. 1998. "Ensuring the Longevity of Digital Information." 26 *International Journal of Legal Info.*

Rothenberg, Jeff. 2000. "Preserving authentic digital information." *Authenticity in a digital environment* 5168.

The National Archives. 2018. Download DROID: file format identification tool. Accessed June 5, 2018, http://www.nationalarchives.gov.uk/information-management/manage-information/preserving-digital-records/droid/.

Thibodeau, Kenneth. 2018. "Overview of Technological Approaches to Digital Preservation and Challenges in Coming Years." Washington, D.C.: Council on Library and Information Resources. Accessed June 4, 2018, https://www.clir.org/pubs/reports/pub107/thibodeau/

Woods, Kam, Christopher A. Lee, and Simson Garfinkel. "Extending digital repository architectures to support disk image preservation and access." In *Proceedings of the 11th annual international ACM/IEEE joint conference on Digital libraries*, pp. 57-66. ACM, 2011.

Wiedeman, Gregory. 2016. Practical Digital Forensics at Accession for Born-Digital Institutional Records. *Code4Lib* (31)

Whyte, Jess. 2017. "Fisher Digital Holdings Workflow." University of Toronto, last modified August, 24. Accessed June 5, 2018, https://connect.library.utoronto.ca/display/DPG/Fisher+Digital+Holdings+Workflow.

Wright, Richard. 2012. "Preserving Moving Pictures and Sound." *DPC Technology Watch Report* 12-01 March 2012. http://dx.doi.org/10.7207/twr12-01

Wright, Richard. 2011. "The Real McCoy: What Audiovisual Collections Preserve." *BBC White Paper*. https://www.bbc.co.uk/rd/publications/whitepaper211

Wright, Richard. "Television Archives in a Post-Television World." Keynote presentation at the FIAT/IFTA World Conference, Mexico City, Mexico, October, 2017