# An Assessment of, and Improvements to, the Digital Forensics Acquisition Process of a Law Enforcement Agency

by

Bianca Esanu

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Applied Science
in
Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2022

## Author's Declaration

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

## Abstract

Forensics addresses the collection and analysis of evidence. Digital forensics is forensics in the context of digital devices. It is a rapidly evolving field employed in various organizations such as law enforcement, government, and the private sector. The acquisition of digital evidence is the step in digital forensics where digital evidence is preserved. The preservation of digital evidence in its original form is customarily deemed a necessary property in the context of digital forensics, as such evidence may need to be re-examined in the future.

In this thesis, we first analyze the acquisition phase of the digital forensics process of the Ontario Provincial Police (OPP) to determine whether it is forensically sound. The OPP is a law enforcement agency that serves a population of 14 million people who reside in the province of Ontario in Canada. We extract a set of properties that OPP's acquisition phase does, and should, uphold to achieve forensic soundness. We then evaluate whether the desired properties are met by comparing OPP's process to three standards on forensic soundness for law enforcement. We conclude by proposing improvements to the parts of the process that do not uphold desired properties.

While our thesis evaluates and provides suggestions to OPP's current process, it also serves a greater purpose. Our contributions allow OPP, and any other law enforcement agency, the framework needed to analyze an existing process, identify areas that may jeopardize forensic soundness, and implement changes that mitigate those threats.

## Acknowledgements

I would like to thank my supervisor, Professor Mahesh Tripunitara, for his mentorship and continued engagement throughout my MASc. I would also like to thank my committee members, Professor Patrick Lam and Professor Hiren Patel, for their time and valuable feedback on my MASc thesis.

I would like to express my sincere gratitude to the Digital Forensics Unit at the Ontario Provincial Police for their continued assistance and support on my research, and to CodyAllan Ferguson for sharing his insight and knowledge on digital forensics with me.

Last but not least, I would like to thank my parents. They have always inspired me to shoot for the moon.

## Dedication

*"What we do for ourselves dies with us. What we do for others and the world remains and is immortal."*

- Albert Pine

Thank you to those who serve others.

# Table of Contents

**List of Figures** **x**

**List of Tables** **xi**

**1 Introduction** **1**

1.1 Digital Forensics . . . . . . . . . . . . . . . . . . . . . . . . . . . . 1

1.1.1 Digital Evidence . . . . . . . . . . . . . . . . . . . . . . . . . 2

1.1.2 Four Phases of Digital Forensics . . . . . . . . . . . . . . . . . . . 2

1.2 Forensic Soundness . . . . . . . . . . . . . . . . . . . . . . . . . . . 3

1.3 Ethics . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4

1.4 Thesis Breakdown . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4

**2 Background** **5**

2.1 Criminal Charge Process in Ontario . . . . . . . . . . . . . . . . . . . 5

2.1.1 Case Law and Legislation . . . . . . . . . . . . . . . . . . . . . . 6

2.2 Digital Forensics at OPP . . . . . . . . . . . . . . . . . . . . . . . . 6

2.2.1 Digital Evidence at OPP . . . . . . . . . . . . . . . . . . . . . . 7

2.2.2 Computer Systems at OPP . . . . . . . . . . . . . . . . . . . . . 8

2.2.3 Digital Forensics Phases at OPP . . . . . . . . . . . . . . . . . . 8

2.2.4 Forensic Soundness at OPP . . . . . . . . . . . . . . . . . . . . . 9

2.2.5 Importance of Forensic Soundness at OPP . . . . . . . . . . . . . . 9

2.3 Our Work . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 10
2.3.1 Our Contributions . . . . . . . . . . . . . . . . . . . . . . . 11
2.3.2 Our Methodology . . . . . . . . . . . . . . . . . . . . . . . . 11
2.4 Resources . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 11
2.4.1 ISO/IEC 27037 . . . . . . . . . . . . . . . . . . . . . . . . . 12
2.4.2 SWGDE Best Practices for Computer Forensic Acquisitions . . . . 12
2.4.3 NIST SP 800-86 . . . . . . . . . . . . . . . . . . . . . . . . . 13

**3 Current Process and Properties 15**
3.1 Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . 15
3.2 Key Concepts . . . . . . . . . . . . . . . . . . . . . . . . . . . . 17
3.2.1 Property, Process, and Action . . . . . . . . . . . . . . . . . 17
3.2.2 Types of Properties . . . . . . . . . . . . . . . . . . . . . . . 17
3.3 Forensic Soundness . . . . . . . . . . . . . . . . . . . . . . . . . 18
3.4 Forensic Note-Taking . . . . . . . . . . . . . . . . . . . . . . . . 19
3.5 Preservation . . . . . . . . . . . . . . . . . . . . . . . . . . . . 20
3.6 Imaging Process . . . . . . . . . . . . . . . . . . . . . . . . . . . 20
3.6.1 Retrieval of Device from Storage . . . . . . . . . . . . . . . . 20
3.6.2 Isolation of Device Components . . . . . . . . . . . . . . . . . 22
3.6.3 Imaging Through a Write Blocker . . . . . . . . . . . . . . . . 22
3.6.4 Creation of a Forensic Image . . . . . . . . . . . . . . . . . . 23
3.6.5 Hashing . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 24
3.6.6 Return of Device to Storage . . . . . . . . . . . . . . . . . . . 25
3.6.7 Shared Network Drive - Upload . . . . . . . . . . . . . . . . . 25
3.7 Pre-Analysis Process . . . . . . . . . . . . . . . . . . . . . . . . 26
3.7.1 Shared Network Drive - Download . . . . . . . . . . . . . . . . 26
3.7.2 Hashing . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 28
3.7.3 Analysis . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 30

3.8 Other Related Actions and Properties . . . . . . . . . . . . . . . . . . . . . 30

3.8.1 Tool Testing . . . . . . . . . . . . . . . . . . . . . . . . . . . 30

3.9 The Problem . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 30

**4 Current Process vs. the Properties 31**

4.1 Our Framework . . . . . . . . . . . . . . . . . . . . . . . . . . . . 31

4.2 Forensic Note-Taking . . . . . . . . . . . . . . . . . . . . . . . . . 32

4.3 Imaging Process . . . . . . . . . . . . . . . . . . . . . . . . . . . 32

4.3.1 Retrieval of Device from Storage . . . . . . . . . . . . . . . . . 33

4.3.2 Isolation of Device Components . . . . . . . . . . . . . . . . . 33

4.3.3 Imaging Through a Write Blocker . . . . . . . . . . . . . . . . 34

4.3.4 Creation of a Forensic Image . . . . . . . . . . . . . . . . . . 34

4.4 Hashing . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 36

4.4.1 Return of Device to Storage . . . . . . . . . . . . . . . . . . . 36

4.4.2 Shared Network Drive - Upload . . . . . . . . . . . . . . . . . 37

4.5 Pre-Analysis Process . . . . . . . . . . . . . . . . . . . . . . . . . 37

4.5.1 Shared Network Drive - Download . . . . . . . . . . . . . . . 38

4.5.2 Hashing . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 38

4.5.3 Analysis . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 39

4.6 Other Related Actions and Properties . . . . . . . . . . . . . . . . . . . . . 40

4.6.1 Tool Testing . . . . . . . . . . . . . . . . . . . . . . . . . . . 40

**5 Amended Process 41**

5.1 Claim 14 and 15 . . . . . . . . . . . . . . . . . . . . . . . . . . . 41

5.1.1 The Proposed Amendments to Action 6 . . . . . . . . . . . . . 42

5.1.2 Action 6 vs. the Properties . . . . . . . . . . . . . . . . . . . 44

5.2 Claim 17, 18, 19 and 20 . . . . . . . . . . . . . . . . . . . . . . . 46

5.2.1 The Proposed Amendments to Action 8 and 9 . . . . . . . . . . . 46

5.2.2 Action 8 and 9 vs. the Properties . . . . . . . . . . . . . . . . . . . . . 47

5.3 Claim 2 and 16 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 49

5.3.1 The Proposed Amendments to Action 2 and 7 . . . . . . . . . . . . 49

5.3.2 Action 2 and 7 vs. the Properties . . . . . . . . . . . . . . . . . . . . . 50

5.4 Claim 22 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 50

5.4.1 The Proposed Amendments to Action 12 . . . . . . . . . . . . . . . . 51

5.4.2 Action 12 vs. the Properties . . . . . . . . . . . . . . . . . . . . . . . 51

**6 Related and Future Work** **52**

6.1 Related Work . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 52

6.2 Future Work . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 52

6.2.1 Other Phases of the Digital Forensics Process . . . . . . . . . . . . 52

6.2.2 Types of Devices . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 53

6.2.3 Adversary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 53

**7 Conclusion** **54**

**References** **55**

# List of Figures

2.1 OPP's Digital Forensics Process. Each box represents a phase of the process. The area shaded in red represents the scope of our thesis [17]. . . . . . . . . 10

2.2 OPP and ISO/IEC's Digital Forensics Process. The area shaded in red represents the scope of our thesis [4][17]. . . . . . . . . . . . . . . . . . . . . 12

2.3 OPP and NIST's Digital Forensics Process. The area shaded in red represents the scope of our thesis [19][17]. . . . . . . . . . . . . . . . . . . . . 13

3.1 Breakdown of OPP's Acquisition Phase in Two Sections: the Imaging and Pre-Analysis Process. The area shaded in red represents the scope of our thesis [17]. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 15

3.2 OPP's Network Topography. The arrow labelled "Digital Evidence" indicates chronology: the digital evidence travels from the Imager's Local Forensic Workstation, to the Shared Network Drive, to the Analyst's Local Forensic Workstation [17]. . . . . . . . . . . . . . . . . . . . . . . . . . 16

3.3 OPP's Imaging Process [17] . . . . . . . . . . . . . . . . . . . . . . . . . . 21

3.4 E01 Image [21] . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 23

3.5 RAW Image . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 23

3.6 Pre-Analysis Process [17] . . . . . . . . . . . . . . . . . . . . . . . . . . . 27

# List of Tables

2.1 Individuals involved in the digital forensics process and their roles and responsibilities. . . . . . 6

# Chapter 1

# Introduction

In this chapter, we introduce digital forensics and define the notion of forensic soundness.

## 1.1 Digital Forensics

Forensics is "the application of scientific methods or techniques to the investigation of a crime" [17]. Just as forensics applies to the physical world, it also applies to the digital world. Digital forensics is "the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law" [17]. While law enforcement agencies commonly practice digital forensics in the context of criminal and civil cases, it is also practiced in the private sector concerning internal corporate investigations or to settle contractual disputes via electronic discovery (ediscovery) [11]. Whether law enforcement, government, or in the private sector, many organizations have developed specific processes for handling digital evidence that upholds the properties considered most important to that given organization. Properties and priorities may differ from one organization to another, which is reflected in their digital forensics process.

McKemmish [23] has analyzed the digital forensics process of law enforcement agencies in eight countries and discovered that all have four main phases: *identification, preservation, analysis, and presentation* of digital evidence in a manner that was legally acceptable in the local jurisdiction. The identification phase is where devices with digital evidence are located and seized. In the preservation phase, digital evidence is extracted off a device. The analysis phase comprises of the interpretation of digital evidence, and in the presentation phase, that interpretation is presented in a court of law.

We define a phase as the following:

**Definition 1** (Phase)**.** *A phase is a chronological section of the digital forensics process. It is one of identification, preservation, analysis, or presentation of digital evidence.*

While the phases of the digital forensic process are similar in numerous law enforcement agencies internationally, there are differences, and these occur as a consequence of local laws and organizational policy.

### 1.1.1 Digital Evidence

Digital forensics was first introduced to combat the rise of electronic crime, or e-crime. E-crime includes identity theft, piracy, child pornography/abuse, cyberstalking/harassment, and hacking. However, as technology has become prominent in daily activities, digital evidence is now harvested and used to prosecute all types of crime and not just e-crime [10].

Digital evidence can take many forms including electric documents, search history, photos, and videos. Digital evidence is latent, similarly to fingerprints and DNA. Furthermore, it can be time-sensitive and easily altered, damaged, or destroyed [3]. Digital evidence exists on a device in binary form. Thanks to the digital forensics process, the binary data on a device can be extracted and rendered into a human-readable form to be presented in court as evidence.

### 1.1.2 Four Phases of Digital Forensics

The *identification phase* is where digital devices are physically identified, often on a crime scene or in the possession of a suspect [23]. Personal computers and mobile phones are no longer the only sources of digital evidence. For example, gaming systems can be used as a medium for instant messaging and smart fridges with built-in TVs can be used to store, view, and share illegal images and videos [3]. In the identification phase, all possible sources for digital evidence on a scene need to be identified.

The *preservation phase* is where data on the digital device is preserved and extracted from the device itself. Preservation of digital evidence is accomplished by analyzing the data in the least-intrusive manner [23]. The methods used to extract digital evidence from devices are closely examined in court to ensure that the digital evidence presented is an accurate representation of the digital evidence that lives on the device.

The *analysis phase* is where the digital evidence is analyzed and translated in human-readable form. The digital evidence extracted in the preservation phase is in binary [23]. In the analysis phase, the binary data is processed into their respective artifacts - whether it be a document, a picture, or any of the numerous types of digital evidence that can be found and extracted from a device. It is in this phase that the binary data on a device is rendered into digital evidence that will be presented in a court of law.

The *presentation phase* is the final phase of the digital forensics process. In this phase, the digital evidence identified, preserved, and analyzed in the prior three phases are presented in court. The presentation of digital evidence includes the digital evidence itself, the qualification and expertise of the presenter of the digital evidence, and the process used to extract the digital evidence being presented [23].

## 1.2 Forensic Soundness

Forensic soundness is the standard that digital forensics aims to uphold. If digital evidence is identified, preserved, and analyzed in a forensically sound manner, then there is reasonable assurance that the digital evidence presented in court was not altered, corrupted, or destroyed either on purpose or by accident [9].

A widely accepted definition of forensic soundness is "*the application of a transparent digital forensics process that preserves the original meaning of data for production in a court of law" [24]*. There are two main properties of a forensically sound process:

1. *"The acquisition and subsequent analysis of electronic data has been undertaken with all due regard to preserve the data in the state in which it was first discovered".*
2. *"The forensic process does not in any way diminish the evidentiary value of the electronic data through technical, procedural or interpretive errors" [24].*

For example, if a seized device is powered off and maintained in its original state from the identification phase through to the presentation phase, then this process may be deemed to be forensically sound. If, on the other hand, the device is powered on and changes are made to the data on the device, such as changing the time settings, then the process may not be deemed to be forensically sound.

While the concept of forensic soundness is universal, the specific details as to what is considered a forensically sound process can depend on the local laws and the organization's purpose for practicing digital forensics. For example, certain law enforcement agencies value the integrity of digital evidence over its availability.

## 1.3 Ethics

Our work raises the bar for OPP and law enforcement agencies internationally who practice digital forensics. We propose a framework that can be used to vet the digital forensics process for forensic soundness. This framework can be used by OPP in the future, and other law enforcement organizations, to evaluate whether their process upholds forensic soundness.

## 1.4 Thesis Breakdown

In the remainder of this thesis, we analyze OPP's acquisition phase to determine if it is forensically sound. In Chapter 2, we establish OPP's digital forensics process and OPP's definition for forensic soundness. In Chapter 3, we introduce OPP's acquisition phase as a set of actions and properties. In Chapter 4, we determine whether the set of actions uphold the set of properties they intend to meet. In Chapter 5, we recommend changes to the actions that do not uphold their respective properties. We conclude with Chapter 6 where we address related work in this area of digital forensics and suggest future work.

# Chapter 2

# Background

In this chapter, we introduce the digital forensics process of the OPP. The OPP serves over 14 million residents in the province of Ontario, Canada and is one of the largest deployed police services in North America [5].

## 2.1 Criminal Charge Process in Ontario

In Ontario, a suspect is presumed innocent until proven guilty. The suspect does not have to prove that they are innocent, but a Crown attorney has to prove to a judge/jury, beyond a reasonable doubt, that the suspect is guilty. The Crown attorney must provide the suspect and the Defense attorney what information the Crown has against the suspect, known as a disclosure package. This is the collection of information on a case from both the police and the Crown. At the trial, the Crown attorney will start by first presenting the evidence they have that the suspect is guilty of the charges laid. The suspect can present their own evidence, but may also choose to remain silent for the entirety of the trial. After all evidence is presented, the judge/jury must come to a decision whether the Crown attorney has, beyond a reasonable doubt, proven that the suspect is guilty [2]. The roles and responsibilities of the individuals involved in both the digital forensics process and the trial can be seen in Table 2.1.

| | |
|---|---|
| **Imager** | A person who performs the acquisition phase of OPP's digital forensics process |
| **Forensic Analyst** | A person who performs the identification and seizure phase, the examination and analysis phase, and the reporting and presentation phase of OPP's digital forensics process |
| **Expert Witness** | A person with significant experience and/or education relied upon to provide an un-biased opinion or knowledge to aid the court reach a decision |
| **Investigator** | A law enforcement officer that works on cases |
| **Defense Attorney (or Defense Counsel)** | The attorney who represents the accused and presents their case in court |
| **Crown Attorney (or Crown Counsel)** | The attorney who represents the Crown and acts as the prosecutors in court |

Table 2.1: Individuals involved in the digital forensics process and their roles and responsibilities.

### 2.1.1 Case Law and Legislation

Law in Canada originates from case law and legislation. Legislation is made up of statutes, regulations, and bylaws. Statutes are publicly debated and voted upon by the federal parliament or provincial legislatures before being enforced. Statutes outline the general rules that govern the lives of Canadian citizens [8]. Regulations and bylaws are the details created to allow for the implementation of the statute [7]. The Criminal Code of Canada consolidates all crimes and the criminal law procedure into one statute [12].

Case law originates from the decisions of judges in previous court cases. In Ontario, judges must follow previous rulings of other judges from both higher courts in the same province/territory and the Supreme Court of Canada on the same issue [7].

## 2.2 Digital Forensics at OPP

The OPP developed its own digital forensic process that is in-line with local laws and organizational policy. In Chapter 1, we present a commonly-adopted breakdown of the digital forensics process and a definition for forensic soundness. In this chapter, we introduce the digital forensic process as practiced by the OPP and OPP's definition for forensic soundness.

### 2.2.1 Digital Evidence at OPP

The digital forensics process of a law enforcement agency is focused on identifying, preserving, analyzing and presenting digital evidence. In Ontario, digital evidence is defined as:

**Definition 2** (Digital Evidence)**.** *Information stored or transmitted in binary that may be relied upon in court [17].*

Note that the definition for digital evidence in Ontario defines evidence as information that is stored or transmitted in binary. However, binary is not in a human-readable form and cannot be presented in court. Under the Canada Evidence Act, there exists a common law known as the Best Evidence Rule. This common law rule predates digital forensics but it is practiced in digital forensics as it bridges the gap between binary digital evidence and the evidence that is presented in court. The Best Evidence Rule originates from R v Betterest Vinyl Manufacturing Ltd 1989 CanLII 7251 (BC CA) [1]:

*"Where the contents of a document are material to the case, the traditional common law Best Evidence Rule requires that the party submit the original unless the party is unable to do so. The court can accept a secondary copy where it is satisfied that the original was lost, destroyed or otherwise unavailable all in good faith".*

In the context of digital forensics, the original digital evidence exists as a binary string on the device that was seized. Hence, the Best Evidence Rule applies to all digital evidence submitted in court. All digital evidence identified, preserved, analyzed, and presented in court is a secondary copy as the original copy is the device itself and the binary data that lives on it.

Section 31.2(1) of The Canada Evidence Act [16] outlines the application of the Best Evidence Rule to electronic documents:

*"The best evidence rule in respect of an electronic document is satisfied*

*(a) on proof of the integrity of the electronic documents system by or in which the electronic document was recorded or stored; or*

*(b) if an evidentiary presumption established under section 31.4 applies."*

Section 31.4 of The Canada Evidence Act [16] expands on electronic signatures and documents secured with electronic signatures, which is outside the scope of our work.

### 2.2.2 Computer Systems at OPP

Digital evidence is harvested from computer systems. The Criminal Code of Canada Section 342.1(2) [6] defines a computer system as the following:

**Definition 3** (Computer System)**.** *"Computer system means a device that, or a group of interconnected or related devices one or more of which,*

*(a) contains computer programs or other computer data, and*

*(b) by means of computer programs,*

*(i) performs logic and control, and*

*(ii) may perform any other function."*

This definition of computer system hence includes phones, routers, IoT devices, and all other electronics that may contain digital evidence.

### 2.2.3 Digital Forensics Phases at OPP

OPP adopts four main goals of digital forensics: *"to identify, collect, preserve, and analyze data in a way that preserves the integrity of the evidence collected so it can be used effectively in a legal case"* [17]. These goals are reflected in OPP's breakdown of the digital forensics process.

As per Figure 2.1, OPP's digital forensic process has 4 phases: (i) Identification and Seizure, (ii) Acquisition, (iii) Examination and Analysis, and (iv) Reporting and Presentation.

**Definition 4** (Identification and Seizure Phase)**.** *The identification and seizure phase is the first phase of the digital forensics process and it involves the search for, identification of, collection of, and documentation of digital evidence. It is in this phase that data storage devices such as HDDs, removable flash media, SD cards, USB drives are located [17].*

**Definition 5** (Acquisition Phase)**.** *In the acquisition phase, forensic copies of the media and data seized are created for preservation, analysis, and examination in the next phase [17].*

**Definition 6** (Examination and Analysis Phase)**.** *An in-depth search of exhibits relating to the incident, which is under investigation, is conducted in the examination and analysis phase.*

**Definition 7** (Reporting and Presentation Phase)**.** *The process concludes with the reporting and presentation phase in which a forensic report is written and provided to the investigator, the Crown attorney, and the Defense attorney, as per Table 2.1. The forensic report contains findings from the examination and analysis phase. It is used and relied upon for court proceedings and it should include what is needed for a testimony in court [17].*

### 2.2.4 Forensic Soundness at OPP

In Chapter 1, we introduce a definition for forensic soundness from [24]. However, our work specifically analyzes OPP's process. Hence, in order to determine whether OPP's acquisition phase is forensically sound, we adopt OPP's definition for forensic soundness.

**Definition 8.** *A forensically sound digital forensics process at OPP is one which is well documented, verifiable, repeatable, and ensures the integrity and survivability of the evidence.*

The digital forensics process is unique to every organization, but as we mention in Chapter 1, there exists overlap in both the digital forensic process and the definition for forensic soundness. Thanks to this overlap, we are able to reference international standards on forensic soundness for law enforcement to perform our analysis.

### 2.2.5 Importance of Forensic Soundness at OPP

One may ask what the purpose is for emphasizing the importance of forensic soundness with respect to the digital forensics process. This can best be answered by outlining what can happen if digital forensics is not practiced in a forensically sound manner:

- *"There is a risk of destroying valuable evidence."*

  If practiced incorrectly, digital evidence can be altered or deleted. That evidence may be key in a trial, both by either being inculpatory or exculpatory evidence.

- *"The forensic evidence gathered may be ruled inadmissible in the court of law."*

  If the digital evidence presented in court is not deemed to be a result of a forensically sound process, as described in Definition 8, the judge may rule that the digital evidence may not be used in the trial.

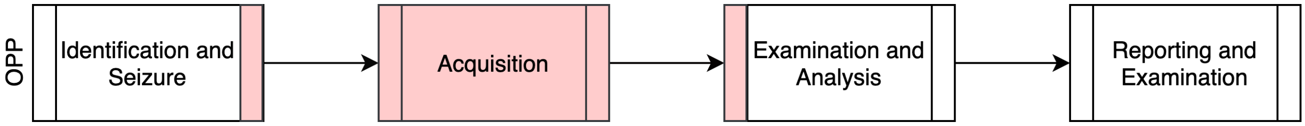

Figure 2.1: OPP's Digital Forensics Process. Each box represents a phase of the process. The area shaded in red represents the scope of our thesis [17].

- *"The character and work of a forensic analyst/imager/organization may be brought into question."*

  If errors are made or a non-forensically sound process is used to extract digital evidence and the evidence is ruled inadmissible in court, any future evidence presented to court by the same analyst/imager/organization may be brought into question.

- *"There is a risk of creating case law that works against the goals of the organization."*

  As per Section 2.1.1, case law originates from decisions made by judges. If the digital forensics process used to extract digital evidence from a device is ruled inadmissible in court, the judge may also decide to disallow the use of that digital forensics process in future trials.

- *"It may lead to possible administrative or civil action" [17].*

  Errors made or the use of a non-forensically sound process may lead to administrative action for the analyst/imager/organization or criminal liability if evidence is deemed to have been tampered with.

## 2.3 Our Work

In this thesis, we analyze the forensic soundness of the acquisition phase of OPP's digital forensics process. Our scope is from the end of the identification and seizure phase to the start of the examination and analysis phase, as seen in Figure 2.1. As we outline in Section 2.2, the acquisition phase is the phase where a forensic copy is made of the device. We only address digital storage media in our work, but the full acquisition process includes devices such as those that pertain to networks, wireless communications, and IoT.

Our analysis employs a level of abstraction that only conveys the results of using a tool/function rather than naming the specific manufacturer and version of the tool. This is because the strategy is to approach the analysis similarly to how a Defense counsel would approach it if given the same documents and process to review.

### 2.3.1 Our Contributions

Our contributions are:

1. a clear calling out of properties that OPP does and should seek to maintain to achieve forensic soundness,
2. an assessment of the current process,
3. improvements to portions of the process with clear justification based in (1).

Our contributions (1) - (3) together form a framework that can be used to assess a digital forensics process. This framework can be used by OPP in the future and other law enforcement organizations to evaluate their digital forensics process. We recommend our framework be used to evaluate a process anytime a change is made to the process itself. This constant vetting helps verify that the process remains forensically sound throughout the natural life cycle and changes that it will undergo.

### 2.3.2 Our Methodology

The process was extracted through a mix of: (i) observing the imagers perform the acquisition process, (ii) reviewing imager case notes from recent cases, and (iii) speaking to analysts who are proficient in the acquisition process to understand the reasoning behind certain procedures. (i) was observed for 2 months, (ii) and (iii) was observed for 8 months. Other material originates from the onboarding sessions used to train imagers. The roles and responsibilities of imagers and analysts are outlined in Table 2.1.

## 2.4 Resources

Several standards and guidelines have been published for digital forensics [4] [19] [25]. Many resources exist from various organizations that outline best practices and guidelines for digital forensics, but law enforcement organizations often have their own procedures and policies based on the laws, rules, and regulations in their respective jurisdiction. However, resources that suggest best practices can be used to vet an existing process and uncover potential shortcomings. We reference certain published standards and guidelines, more notably in Chapter 4, as we assess OPP's current process and suggest improvements.

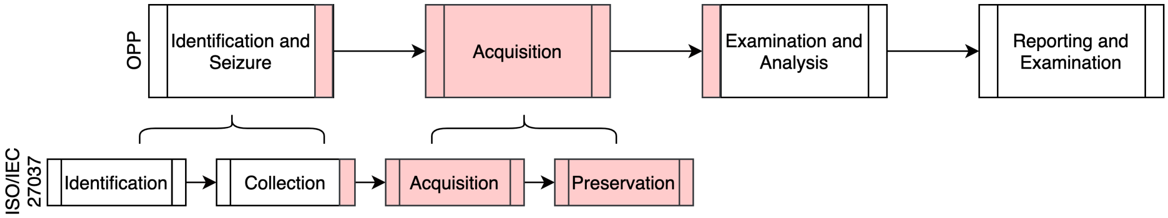

Figure 2.2: OPP and ISO/IEC's Digital Forensics Process. The area shaded in red represents the scope of our thesis [4][17].

### 2.4.1 ISO/IEC 27037

ISO/IEC 27037 is titled *Information technology - Security techniques - Guidelines for identification, collection, acquisition, and preservation of digital evidence.* The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) created ISO/IEC 27037 to provide guidelines for the activities performed with respect to identification, acquisition, and preservation of potential digital evidence.

ISO/IEC 27037's digital forensics process has four phases: (i) Identification, (ii) Collection, (iii) Acquisition, and (iv) Preservation. This can be seen in Figure 2.2. ISO/IEC 27037 acknowledges that the full digital forensics process includes other phases such as presentation of digital evidence, as can be seen in OPP's digital forensics process, but this standard focuses solely on the handling of evidence which is done in the first two phases of OPP's digital forensics process.

ISO/IEC 27037 covers various devices and circumstances, but we focus on the guidelines it suggests for digital storage media used in standard computers and more specifically, the acquisition of powered-off digital storage media.

### 2.4.2 SWGDE Best Practices for Computer Forensic Acquisitions

The Scientific Working Group on Digital Evidence (SWGDE) created a document titled *SWGDE Best Practices for Computer Forensic Acquisitions* that provides "*best practices for the forensics acquisition of digital evidence from computers and associated storage media*" [25].

Similarly to OPP and ISO/IEC 27037's digital forensic phases, the SWGDE has published, in complement to the *SWGDE Best Practices for Computer Forensic Acquisitions*,

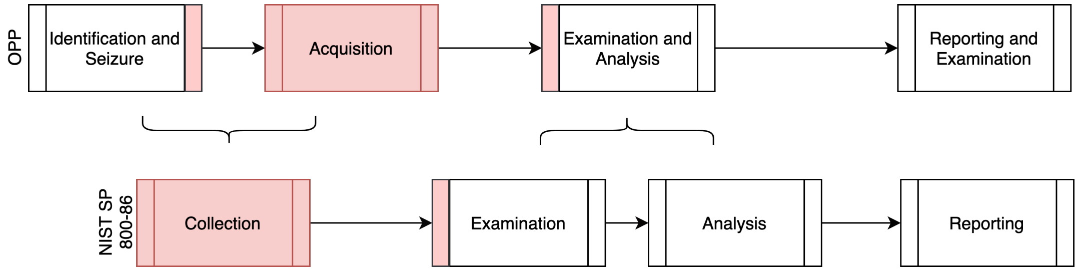

Figure 2.3: OPP and NIST's Digital Forensics Process. The area shaded in red represents the scope of our thesis [19][17].

three other documents:

- *SWGDE Best Practices for Digital Evidence Collection*,
- *SWGDE Best Practices for Computer Forensics Examination*, and
- *SWGDE Best Practices for Forensic Reporting.*

The set of SWGDE Best Practices documents cover various situations and devices, but only *SWGDE Best Practices for Computer Forensic Acquisitions* is used in our work as it directly fits our scope with respect to the acquisition phase of digital storage media.

### 2.4.3 NIST SP 800-86

NIST SP 800-86, titled *Guide to Integrating Forensics Techniques into Incident Response*, was created by the National Institute of Standards and Technology (NIST) to provide general recommendations for the four phases of digital forensics as per their breakdown, seen in Figure 2.3. NIST has specifically prepared this document to reflect a technical point of view as opposed to a law enforcement one.

NIST defines phases that overlap with OPP's phases for digital forensics. NIST's collection phase includes both OPP's identification and seizure phase and the acquisition phase, as seen in Figure 2.3. As with ISO/IEC 27037, NIST SP 800-86 covers best digital forensics practices for various circumstances and devices, but we focus on the acquisition component of NIST's collection phase for digital storage media used in standard computers.

### NIST's Computer Forensic Tool Testing Project

NIST developed the Computer Forensic Tool Testing (CFTT) project as a response to the increase in digital forensics acquisition tools on the market. Previously, there were no standards to test them so the NIST CFTT project created a rigorous testing procedure to validate the tools used in digital forensics [19].

# Chapter 3

# Current Process and Properties

In this section, we introduce OPP's acquisition phase, as per Figure 2.1, as well as the current properties OPP intends to uphold to achieve forensic soundness.

## 3.1 Introduction

The current acquisition phase is broken down into two parts: the imaging process and the pre-analysis process, as seen in Figure 3.1. One may note that our scope is not limited to the acquisition phase, but it also includes the end portion of the identification and seizure phase as well as the beginning portion of the examination and analysis phase. This is because portions prior and post to the acquisition phase impact the forensic soundness of the acquisition phase.

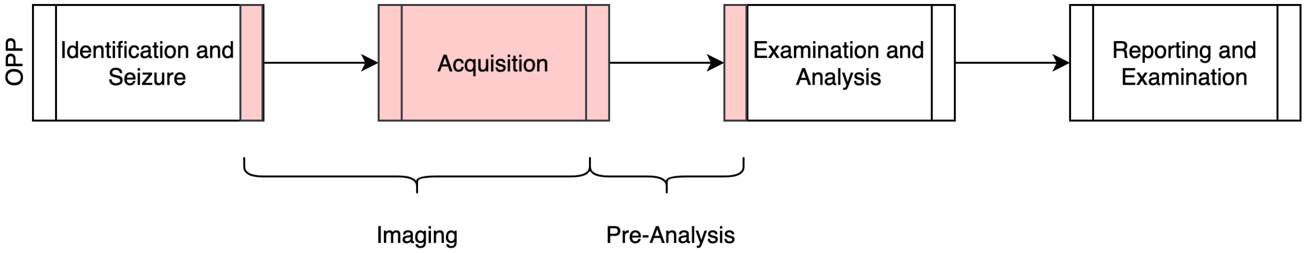

Figure 3.1: Breakdown of OPP's Acquisition Phase in Two Sections: the Imaging and Pre-Analysis Process. The area shaded in red represents the scope of our thesis [17].

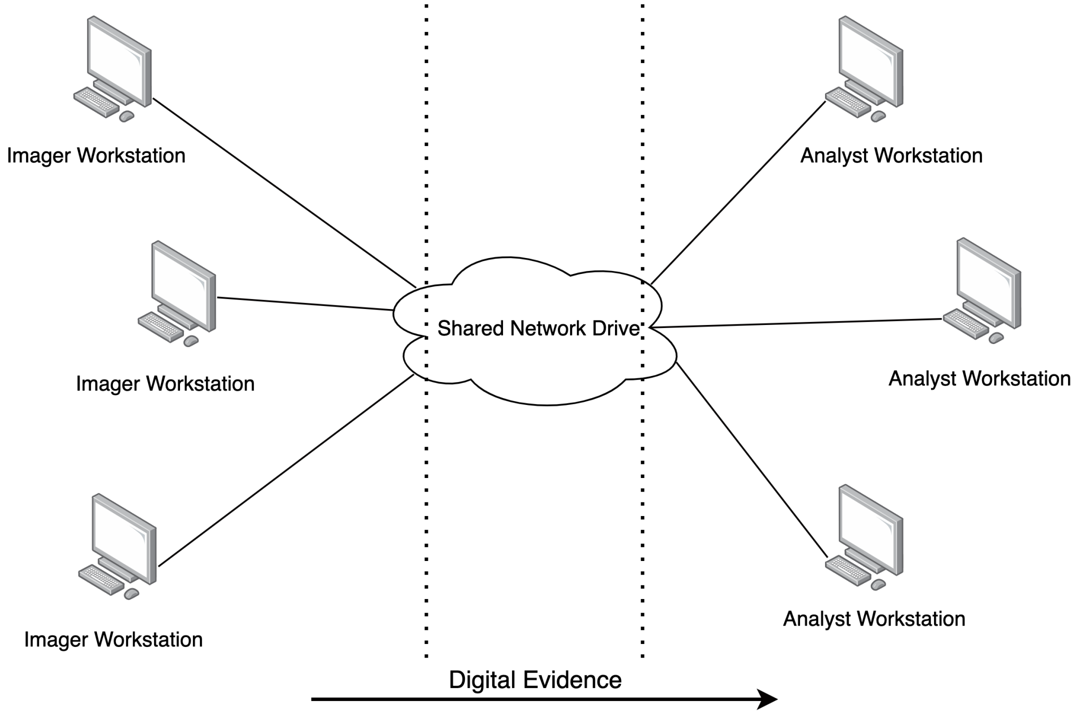

Figure 3.2: OPP's Network Topography. The arrow labelled "Digital Evidence" indicates chronology: the digital evidence travels from the Imager's Local Forensic Workstation, to the Shared Network Drive, to the Analyst's Local Forensic Workstation [17].

Before we define the imaging and pre-analysis processes, we establish the network topography of OPP's digital forensics unit. This aids in better understanding the path that the digital evidence passes through from the device it resides on to the forensic workstation it will be analyzed and examined on. Digital evidence flows from the imager's local forensic workstation, to the shared network drive, and ends up on the analyst's local forensic workstation, as seen in Figure 3.2. The flow of digital evidence through three different mediums also reinforces why our scope is best suited to include portions of the identification and seizure phase, and the examination and analysis phase.

We now define the imaging and pre-analysis process:

**Definition 9** (Imaging Process)**.** *The process the digital evidence undergoes from the device it resides on until it reaches the shared network storage.*

**Definition 10** (Pre-Analysis Process)**.** *The process the digital evidence undergoes from the shared network storage until it reaches the analyst's local forensic workstation.*

The main purpose of the imaging and pre-analysis process is to ensure that the digital evidence that resides on the local forensic workstation of an analyst at the end of the pre-analysis process, is a true copy of the evidence that resides on the device at the beginning of imaging process.

## 3.2 Key Concepts

We introduce some terms that add clarity and conciseness to our work.

### 3.2.1 Property, Process, and Action

A theme in this thesis is the important distinction between property and process. This is important in our work as we perform an analysis on whether the process OPP employs, as part of the acquisition phase, upholds the properties they intend to.

**Definition 11** (Property)**.** *A property is a declarative statement that can be assigned a value of 'true' or 'false'.*

**Definition 12** (Process)**.** *A process is an action, or a series of actions, taken to achieve a desired outcome.*

**Definition 13** (Action)**.** *An action is a single component of the process, i.e., something that is done. A process comprises of actions.*

### 3.2.2 Types of Properties

Another theme is the distinction between a dictated, extracted, and recommended property.

**Definition 14** (Dictated Property)**.** *A dictated property is a property that OPP has explicitly imposed in writing. Many dictated properties are a result of local laws and organizationally-enforced best practices.*

**Definition 15** (Extracted Property)**.** *An extracted property is a property that OPP has imposed but not explicitly. It cannot be found in writing.*

**Definition 16** (Recommended Property)**.** *A recommended property is a property we recommend in our work that OPP adopts.*

These are labeled accordingly throughout. We introduce the extracted properties immediately following the action from which they were extracted. This is so that the reader can make the logical connection between them. Properties are further introduced in the part of the process to which they apply, and the order in which they are introduced is merely the one that makes most chronological sense; the order does not speak to the order of importance of each property to OPP. Further, since the extracted and dictated properties originate from laws or organizational policy, we do not challenge them.

## 3.3 Forensic Soundness

First, we start by establishing some general digital forensics properties dictated by OPP. These apply to all four phases of OPP's digital forensics process, and not just the acquisition phase.

**Property 1** (Dictated)**.** *A forensically sound digital forensics process at OPP is one which is well documented, verifiable, repeatable, and ensures the integrity and survivability of the evidence [17].*

Note that this property originates from OPP's definition of forensic soundness in Section 2.2.4.

A process that is well documented is one in which the steps taken are logged in detail. This is further discussed in Section 3.4.

A process that is verifiable is one in which the process can be repeated with the same tools and with different tools and still produce the same results. A process that is repeatable is one in which the same process can be repeated on the same input in order to produce the same results. Repeatability is a subset of verifiability.

**Property 2** (Dictated)**.** *Two different analysts should be able to examine the same evidence, using different tools and methodologies, and arrive at the same conclusion, or be able to explain any discrepancies [17].*

Property 2 speaks to the verifiability of a process. Theoretically, a verifiable process should always produce the same output given the same input. However, that is not always the case. External factors like faulty inputs and tool errors can vary the output, but that does not imply that the process is unverifiable.

**Property 3** (Dictated). *Methodologies should start with the most and continue to the least forensically sound [17].*

Ideally, the most forensically sound process is to be used. However, external limitations like time, resources, and faulty inputs may require that non-forensically sound methods be employed. This is only acceptable if sufficient explanation can be given in court with respect to why a non-forensically sound method was used. It remains up to the judge to then decide if the evidence is ruled admissible.

**Property 4** (Dictated). *Actions should be taken under the assumption that a device could fail at any moment.*

## 3.4 Forensic Note-Taking

Note-taking is a component of the forensic soundness of not just digital forensics, but forensics as a whole. Note-taking, also referred to as documentation, is performed throughout the entire digital forensics process. Any action taken on a device or its forensic image must be documented including details like the time, date, what tools were used (including specific version and model number) and what action was performed. All notes taken are disclosable, and will be used in court to verify the admissibility of the evidence being presented.

Note-taking plays an important role in the legal aspect of digital forensics, but in our case, it plays a critical role in two ways: (i) it speaks to the integrity of the digital evidence, (ii) it is used to explain any discrepancies, as per Property 2.

**Action 1.** *Imagers and analysts must take notes after performing each action during the imaging and pre-analysis process. Notes include the following information:*

- *Time and date,*
- *Device in question (including brand, model, and version),*
- *Tool being used (including brand, model, and version),*
- *What action is being performed with the aforementioned tool, and*
- *The outcome of that action.*

The intent of the above action is to uphold Property 1.

## 3.5 Preservation

We divide the preservation of digital evidence into two parts. The digital evidence on a device should remain unaltered through its entire lifetime in the possession of OPP. We introduce two new properties to capture this:

**Property 5** (Extracted)**.** *At all times during acquisition, the digital evidence on a device is the same as what it was when the device was seized.*

**Property 6** (Extracted)**.** *At all times after acquisition, the digital evidence on a device is the same as what was on it at the time of acquisition.*

Property 5 highlights that the digital evidence on the device should not be altered by any action performed on that device during the acquisition phase. Property 6 applies to the handling of the device after the acquisition phase actions are completed. It states that measures should be implemented to preserve the availability and integrity of a device after it was imaged. Availability of a device after the acquisition phase is important as a Defense counsel may request that the imaging process be repeated.

## 3.6 Imaging Process

This process starts with a digital storage media device that contains digital evidence. In this process, forensic copies of the digital evidence are created for preservation and analysis.

### 3.6.1 Retrieval of Device from Storage

**Action 2** (Retrieval of Device from Storage)**.** *Before the imaging process starts, the device is retrieved from storage and removed from the property bag. When the device reaches the imaging process, it arrives powered off and in a sealed property bag. The device was placed in this property bag when it was seized.*

The intent of the above action is to uphold Property 5.

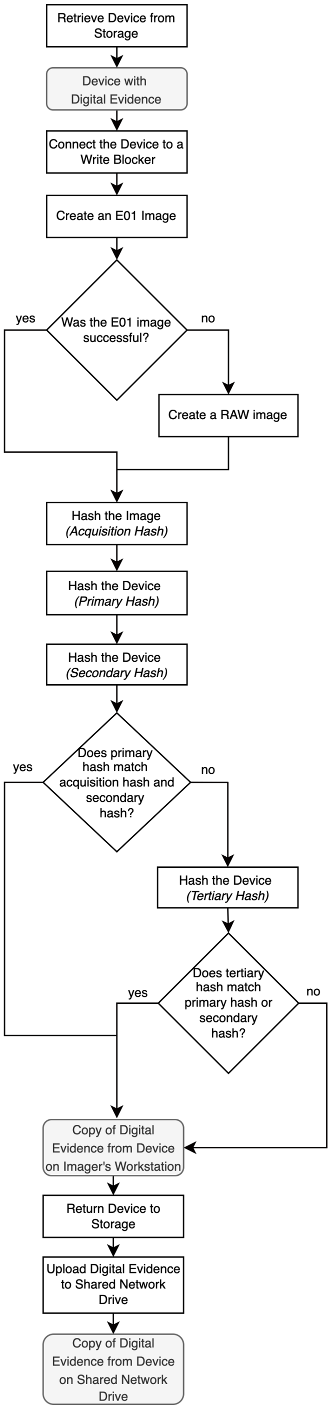
Retrieve Device from Storage
Device with Digital Evidence
Connect the Device to a Write Blocker
Create an E01 Image
Was the E01 image successful?
yes
no
Create a RAW image
Hash the Image *(Acquisition Hash)*
Hash the Device *(Primary Hash)*
Hash the Device *(Secondary Hash)*
Does primary hash match acquisition hash and secondary hash?
yes
no
Hash the Device *(Tertiary Hash)*
Does tertiary hash match primary hash or secondary hash?
yes
no
Copy of Digital Evidence from Device on Imager's Workstation
Return Device to Storage
Upload Digital Evidence to Shared Network Drive
Copy of Digital Evidence from Device on Shared Network Drive

Figure 3.3: OPP's Imaging Process [17]

### 3.6.2 Isolation of Device Components

**Action 3** (Isolation of Device Components)**.** *Digital storage media such as hard drives, solid state drives, USBs, and SD cards are removed from devices to preserve the data on them. Devices such as storage media often require external power to run; therefore, removing them while a device is powered off ensures the best probability of preserving their contents in the original state they were in when the device was seized.*

The intent of the above action is to uphold Properties 5 and 6.

### 3.6.3 Imaging Through a Write Blocker

A write blocker is a tool that prevents writing to a storage device. In other words, it strictly enforces read-only access. Write blockers fall into two categories: software and hardware. Software write blockers are programs or drivers that prevent the operating system from writing to storage. Hardware write blockers are physical devices which prevent data from being written to storage.

**Property 7** (Dictated)**.** *Hardware write blockers are more forensically sound than software write blockers.*

When correctly configured and used, both hardware and software write blockers are equally forensically sound. However, software write-blockers depend heavily on being configured, set up correctly, and regularly updated. If one of those steps are omitted, there is a significant risk that writing to the device could occur by accident. Therefore, software write blockers should be reserved for cases where all other methods have failed.

**Property 8** (Dictated)**.** *All evidentiary data storage is write-blocked in order to prevent inadvertent writes to devices.*

**Action 4** (Use of a Write Blocker)**.** *Digital storage media is connected to a hardware write blocker and the write blocker is then connected to the tool on the local forensic workstation that creates a forensic image.*

**Property 9** (Extracted)**.** *Tools and actions used to image devices should not introduce new data or alter original data.*

If Property 5 is satisfied, then Property 9 is satisfied. However, we note the following distinction. Property 5 states that the device itself must not be altered by the acquisition

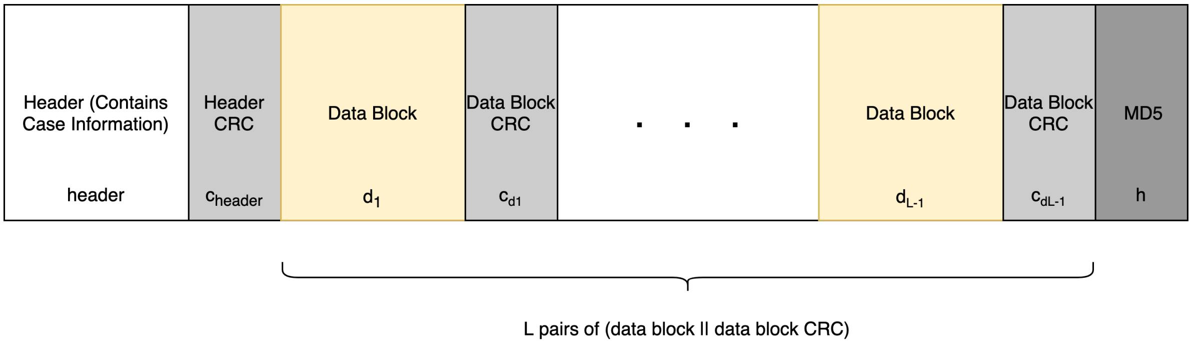

Figure 3.4: E01 Image [21]

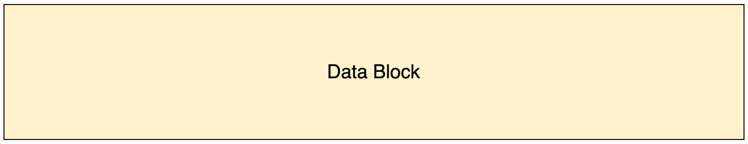

Figure 3.5: RAW Image

phase. If powered on, devices can change state by themselves via the operating system or by interacting and/or connecting to networks, Bluetooth, etc. This means critical information that indicates what the user was doing at or before the device was seized can be lost or overwritten. Property 9 states that any devices and tools that are used to extract the digital evidence should not introduce their own data to the digital evidence nor should it modify the existing data on the device.

In summary, Property 5 includes both changes caused by the device itself and those introduced by tools/processes used in the acquisition phase. Property 9 refers solely to changes introduced by tools/processes used in the acquisition phase.

The intent of the above action is to uphold Properties 7, 8, and 9.

### 3.6.4 Creation of a Forensic Image

There are two types of forensic images: physical images and logical images. Physical images are a bit-by-bit copy of the data which includes all system metadata, file/volume slack and unallocated space. Examples of physical images are E01, RAW, ISO, and VHD images.

Logical images are not a bit-by-bit copy of the data; they are a copy of the logical data only, which does not include unallocated space or volume slack, but may include file slack.

Volume slack is the difference between the end of file system and the end of the partition that the file system resides on [22]. File slack is the end of the file system and it does not have any unused space allocated to any cluster [22]. Examples of logical images are L01, AD1, and CTR images.

**Action 5** (Image Creation)**.** *A physical forensic image of a device is created. If creating an E01 image fails, then the creation of a RAW image is attempted.*

**Property 10** (Dictated)**.** *The creation of a forensic image is the first action performed on a device.*

**Property 11** (Dictated)**.** *RAW images are created only if creating an E01 image fails or if there is a possibility of drive failure.*

**Property 12** (Dictated)**.** *Logical forensic images are created when it is impossible to get a physical forensic image due to problems such as disk errors.*

**Property 13** (Dictated)**.** *Failed images are retained as there may be data in the failed image that may not exist in the successful image.*

The intent of the above action is to uphold Properties 3, 4, 10, 11, 12, and 13.

### 3.6.5 Hashing

**Action 6** (Hashing to Verify Integrity)**.** *Several MD5 hashes are computed of the device and the image created in Action 5. To describe the process precisely, we adopt the following notation:*

| | |
|---|---|
| $o_1(x, t)$ | *A hash function computed by Tool 1 on input $x$ at time $t$* |
| $o_2(x, t)$ | *A hash function computed by Tool 2 on input $x$ at time $t$* |
| $d$ | *(the digital evidence on) a device* |
| $m$ | *An image of the device $d$* |

*The action is as follows, in chronological order. We adopt positive integers, $1, 2, \ldots$ for the time a hash is computed. We assume that no two hashes are computed simultaneously. Note that Tool 1 is the tool that is used for imaging in Action 11.*

1. *The following are computed: $o_1(m, 1), o_1(d, 2), o_2(d, 3)$.*

2. *We perform the following two checks:*

$$o_1(d, 2) \overset{?}{=} o_2(d, 3)$$
$$o_1(d, 2) \overset{?}{=} o_1(m, 1)$$

3. *If the check $o_1(d, 2) \overset{?}{=} o_2(d, 3)$ from #2 above succeeds, the action ends with an outcome of "success." Otherwise, i.e., if $o_1(d, 2) \neq o_2(d, 3)$, then we compute $o_1(d, 4)$. This is called a "tertiary hash" of the device, d.*

   *We then perform the following two checks:*

   $$o_1(d, 4) \overset{?}{=} o_1(d, 2)$$
   $$o_1(d, 4) \overset{?}{=} o_2(d, 3)$$

   *If <u>either</u> of these two checks passes, then the action ends with an outcome of "success." Otherwise, i.e., if both checks fail, the action ends with an outcome of "fail".*

**Property 14** (Extracted)**.** *An image of a device is a true, bit-for-bit copy of the digital evidence on the device.*

The intent of the above action is to uphold Property 14.

### 3.6.6 Return of Device to Storage

**Action 7** (Return of Device to Storage)**.** *Once the actions that need to be performed on the device are complete, the device is placed back into the same property bag it was removed from in Action 2 and returned to storage.*

The intent of the above action is to uphold Property 6.

### 3.6.7 Shared Network Drive - Upload

**Action 8** (Upload to Shared Network Drive)**.** *The forensic image is uploaded to the shared network drive. This is done with a tool that copies the image from the source to the destination, then computes an MD5 hash of the image at the destination, and an MD5* *hash of the image at the source to ensure that integrity was maintained when the data was in motion.*

*To describe the process precisely, we adopt the following notation:*

| | |
|---|---|
| $o(x, l)$ | *A hash function computed by a tool on input $x$ at location $l$* |
| $m$ | *An image of a device* |

*The process is as follows, in chronological order. We adopt $s, d$ for the source and destination location of an image.*

1. *The image is copied from s to d*
2. *The tool calculates o(m, d)*
3. *The tool calculates o(m, s)*
4. *We perform the following check:*

$$o(s, m) \overset{?}{=} o(m, d)$$

5. *If the check $o(s, m) \overset{?}{=} o(m, d)$ from #4 above succeeds, the action ends with an outcome of "success." Otherwise, i.e., if $o(s, m) \neq o(m, d)$, then we the action ends with an outcome of "fail".*

The intent of the above action is to uphold Property 14.

## 3.7 Pre-Analysis Process

This process encompasses the route that the forensic copies take from the shared network drive to the analyst's local forensic workstation for the examination and analysis phase. Further checks are performed to verify the integrity of the digital evidence.

### 3.7.1 Shared Network Drive - Download

**Action 9** (Download from Shared Network Drive)**.** *For an analyst to commence analysis, the image of a device must be downloaded from the shared network drive to the analyst's local forensic workstation. This is done with a tool that copies the image from the source*

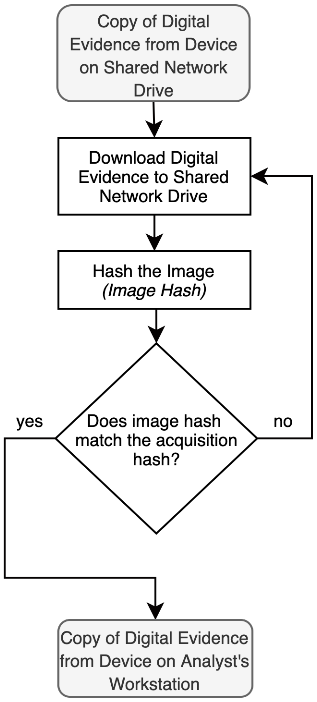
Copy of Digital Evidence from Device on Shared Network Drive
Download Digital Evidence to Shared Network Drive
Hash the Image
*(Image Hash)*
Does image hash match the acquisition hash?
yes
no
Copy of Digital Evidence from Device on Analyst's Workstation

Figure 3.6: Pre-Analysis Process [17]

*to the destination, then computes the MD5 hash the image at the destination, and MD5 hash of the image at the source to ensure that integrity was maintained when the data was in motion.*

*To describe the process precisely, we adopt the following notation:*

| | |
|---|---|
| $o(x, l)$ | *A hash function computed by a tool on input $x$ at location $l$* |
| $m$ | *An image of a device* |

*The process is as follows, in chronological order. We adopt, $s, d$ for the source and destination location of an image.*

1. *The image is copied from s to d*
2. *The tool calculates o(m, d)*
3. *The tool calculates o(m, s)*
4. *We perform the following check:*

$$o(s, m) \overset{?}{=} o(m, d)$$

5. *If the check $o(s, m) \overset{?}{=} o(m, d)$ from #4 above succeeds, the action ends with an outcome of "success." Otherwise, i.e., if $o(s, m) \neq o(m, d)$, then we the action ends with an outcome of "fail."*

The intent of the above action is to uphold Property 14.

### 3.7.2 Hashing

**Action 10** (Hashing to Verify Integrity)**.** *Before the examination and analysis phase commences, the image is verified to ensure that no changes have occurred.*

#### Physical Image - E01 Image

*To verify that the E01 image downloaded to the analyst's forensic workstation correctly, the image's self-verifying quality is used. The E01 image structure can seen in Figure 3.4. To describe the action precisely, we adopt the following notation:*

| | |
|---|---|
| $l$ | *The number of data blocks in an E01 image* |
| $d_i$ | *The data block $i$ where $0 \leq i < l$* |
| $c_i$ | *The CRC of data block $i$ where $0 \leq i < l$* |
| $h$ | *The MD5 of all data blocks $d_i$ where $0 \leq i < l$* |
| $header$ | *The header of the E01 image* |
| $c_{header}$ | *The CRC of the header* |
| $o(x)$ | *A hash function computed by a tool on input $x$* |
| $p(x)$ | *A hash function, which we think is CRC, computed by a tool on input $x$* |
| $a\|\|b$ | *The concatenation of two bit strings $a$ and $b$* |

*The action is as follows. Since this action is performed by a tool, the order of (1), (2), and (3) is unconfirmed and may depend on the specific tool used:*

1. *The following are computed: $p(header)$ and $p(d_i)$ for all $0 \leq i < l$*
2. *The following is then computed: $o(d_0||d_1||d_2||...||d_{l-1})$*
3. *The following checks are performed:*

$$p(header) \stackrel{?}{=} c_{header}$$

$$p(d_i) \stackrel{?}{=} c_i$$

$$o(d_0||d_1||d_2||...||d_{l-1}) \stackrel{?}{=} h$$

4. *If the checks above all succeed, the action ends with an outcome of "success." Otherwise, the action ends with an outcome of "fail."*

### Physical Image - RAW

*To verify that the RAW image downloaded to the analyst's forensic workstation correct, the image undergoes another verification action. The RAW image structure can seen in Figure 3.5. To describe the action precisely, we adopt the following notation:*

| | |
|---|---|
| $o(x)$ | *A hash function computed by a tool on input $x$* |
| $o_1(m, 1)$ | *The hash value of image $m$ computed in Action 6* |
| $m$ | *An image of the device $d$* |

1. *The following is computed: $o(m)$*

2. *The following check is performed:*

$$o(m) \overset{?}{=} o_1(m, 1)$$

3. *If the check above succeeds, the action ends with an outcome of "success." Otherwise, the action ends with an outcome of "fail."*

The intent of the above action is to uphold Property 14.

### 3.7.3 Analysis

**Action 11** (Analysis on Image)**.** *Forensic analysis is conducted on the image, and not the device.*

The intent of the above action is to uphold Property 6.

## 3.8 Other Related Actions and Properties

### 3.8.1 Tool Testing

**Action 12** (Testing of Tools)**.** *Tools used in the imaging and pre-analysis process are tested every six months. They are tested by performing the imaging process using non-evidence digital storage media devices with known hash values. The hashes generated from a mock acquisition are compared to the known hash values. All other software and tools are verified by ensuring that they are running the most recent updates from the manufacturer or developer.*

The intent of the above action is to uphold Property 9.

## 3.9 The Problem

In this chapter, we have introduced OPP's acquisition phase. It turns out that certain dictated and extracted properties are not necessarily met. In the next chapter, we show that there exist gaps between the dictated and extracted properties, and the properties that need to be upheld in order for the process to be forensically sound. Since the dictated and extracted properties are insufficient, we introduce recommended properties as a means to bridge that gap.

# Chapter 4

# Current Process vs. the Properties

In this chapter, we evaluate whether the extracted and dictated properties are upheld. We either show that a certain property is being met or that there exist scenarios that may undermine it. While there are properties that have been explicitly dictated by OPP or extracted via the process, we suggest other properties in this chapter to reinforce any existing loopholes.

## 4.1 Our Framework

One of the most serious allegations the Defense counsel may make is to suggest that the data, on a device or on the forensic image, has been changed by some means and at some point between when it was seized and when the analyst performed the examination and analysis. In order to back this allegation up, the Defense may try to show that specific actions undermine the properties they aim to uphold.

The proofs and justifications in this chapter are specific to OPP's current digital forensics process, but it's key to note that a thorough breakdown of a digital forensics process into actions and properties can be applied to the digital forensics process of any organization. By breaking down the process into actions, and grouping desired properties by said actions, it is easier to see if a process is forensically sound by identifying actions that jeopardize properties they should be upholding. Then, by proving that each action upholds its respective properties, we can show that the entire process then upholds the ultimate property of forensic soundness.

The proofs and justifications in this section will either be logical proofs or will use best practices recommended by NIST, SWDGE, or ISO/IEC, as per Section 2.4. Reliable organizations like NIST, SWDGE and ISO/IEC use researched methods adopted widely by other digital forensics organizations. If the Defense counsel were to question an action adopted from such a source, it would hold more water if the Crown counsel were able to tie it back to best industry practice.

## 4.2 Forensic Note-Taking

**Claim 1.** *Action 1 upholds Property 1.*

Property 1 dictates that a sound forensic process is one that is well-documented. A process in which detailed notes are taken of each action is a well-documented process. Further, detailed notes also act as a step-by-step instruction guide for someone if they wish to repeat the process with the same or different tools. This makes checking the process' verifiability and repeatability possible.

As per ISO/IEC 27037 [4], every action taken should be documented. This includes action taken in the identification, collection, acquisition and preservation process, as per Figure 2.2. This documentation should include details such as date and time, anything visible on the device screen such as programs and processes, the movement of physical devices themselves, as per chain of custody laws, and any unique identifiers of a device such as the serial number and unique markings.

As per NIST 800-86 [19], a detailed log of the process should be kept of every action taken to collect data. Such documentation should include details about who had physical custody of the device, the device specifications (such as model and serial number, media storage capacity), the actions performed and at what time, and the specifics of tools used (such as name, version number, and licensing information). Proper documentation could allow an analyst to refute claims of mishandling in court.

Since Action 1 is in-line with the ISO/IEC 27037 and NIST 800-86 guidelines, Action 1 upholds Property 1.

## 4.3 Imaging Process

We now introduce a set of claims with respect to the imaging process.

### 4.3.1 Retrieval of Device from Storage

**Claim 2.** *Action 2 does not uphold Property 5.*

ISO/IEC 27037 recommends that the environmental aspects be considered. *"Spoliation can result from magnetic degradation, electric degradation, heat, high or low humidity exposure, as well as shock and vibration."* [4]. Note that these environmental aspects need to be considered when a device is seized and handled for transportation, but that is outside the scope of our work.

Since Action 2 is not in-line with the ISO/IEC 27037 guidelines, Action 2 does not uphold Property 5.

### 4.3.2 Isolation of Device Components

**Claim 3.** *Action 3 upholds Property 5.*

Property 5 dictates that an action in the imaging process should not alter the digital evidence on the device that was seized. Action 3 is taken with the intention to uphold Property 5 for the time period between when a device is removed from the property bag it was placed in when it was seized to the point where it is imaged.

ISO/IEC 27037 [4] recommends that the device should be left powered off and the removable memory storage should be removed only when the device is ready to be acquired to not increase the risk of damage.

Since Action 3 is in-line with the ISO/IEC 27037 guidelines for ensuring evidence preservation for powered-off devices, Action 3 upholds Property 5.

**Claim 4.** *Action 3 upholds Property 6.*

By not powering on the device and not allowing the operating system to start and read/write to the digital storage media, the data on the digital storage media will not change and the the digital evidence on the device after it is acquired will be the same as what was on it when it was acquired.

Since Action 3 does not power on a device with digital storage media, it upholds Property 6.

### 4.3.3 Imaging Through a Write Blocker

**Claim 5.** *Action 4 upholds Property 7.*

Since Action 4 specifically states that a hardware write blocker shall be used, Property 7 is upheld.

**Claim 6.** *Action 4 upholds Property 8.*

Since Action 4 specifically states that a write blocker shall be used, Property 7 is upheld.

**Claim 7.** *Action 4 upholds Property 9.*

Not using a write blocker before imaging would mean that Property 9 could be compromised as imaging may inadvertently make changes to the digital evidence. This change would go undetected as by Property 10, imaging is the first action to be performed on the device, so no verification can be performed beforehand to ensure that a change caused by imaging would be detected.

A write blocker should be used regardless of the type of forensic image made. Hence, the use of a write blocker upholds Property 9 as its purpose is to "*prevent the forensic workstation's software or operating system from making any inadvertent changes to the original media, including adding, deleting, or modifying any information*" [20].

As per SWGDE Best Practices for Computer Forensic Acquisitions [25], write blockers are to be used whenever possible in order to prevent writing to the original device.

As per NIST 800-86 [19], write blockers should be used during the imaging process of the device to not alter the original digital evidence. When using a hardware write blocker, the device should be connected directly to the write blocker and then the write blocker should be connected to the computer or device used to create the forensic image. Write blockers must be tested regularly to ensure that they operate correctly on newer devices.

Since Action 4 is in-line with the SWGDE Best Practices for Computer Forensic Acquisitions and NIST 800-86 guidelines for the use of write blockers to preserve the integrity of the original digital evidence, Action 4 upholds Property 9. The assumption for this proof is that the write blocking tool is working correctly, which depends on Action 12.

### 4.3.4 Creation of a Forensic Image

**Claim 8.** *Action 5 upholds Property 3.*

An E01 image is considered forensically sound due to the embedded CRCs and MD5. Hence, by attempting an E01 image prior to a RAW image, Action 5 upholds Property 3.

**Claim 9.** *Action 5 upholds Property 4.*

In situations where a device might be in a failing state, it is more important to get the digital evidence off the device. Since Action 5 dictates that a RAW image should be taken if the device is in a failing state, this upholds Property 4.

**Claim 10.** *Action 5 upholds Property 10.*

Action 5 is the first action to be performed on a device as Action 3 pertains to the handling of the digital storage media and Action 4 pertains to the way it is connected to the local forensic workstation.

Action 5 is the first time in the imaging process that content on the digital storage media is read from. Therefore, Property 10 is upheld.

**Claim 11.** *Action 5 upholds Property 11.*

Since Action 5 dictates that an E01 image should be the first attempt, Property 11 is upheld.

**Claim 12.** *Action 5 upholds Property 12.*

A logical image is not made during the imaging process. That is an action that is performed solely by analysts in the examination and analysis phase if it is deemed necessary.

As per NIST 800-86 [19], a physical image should be made, as opposed to a logical one, in situations where the digital evidence is needed for prosecution. At OPP, all devices are imaged under the assumption that the digital evidence is needed for prosecution.

Since Action 5 dictates that physical images should be made in the imaging process, Property 12 is upheld.

**Claim 13.** *Action 5 upholds Property 13.*

If an attempt at Action 5 fails, the image that results from that attempt is not deleted. Hence, Action 5 upholds Property 13.

## 4.4 Hashing

**Claim 14.** *Action 6 does not uphold Property 14.*

*Proof.* For a counter-example, suppose both $o_1$ and $o_2$, for a device $d$, are constant functions. That is, given any device $d$ and at any time $t, t'$, $o_1(d,t) = o_2(d,t') = 1$. Then, the check $o_1(d,1) \overset{?}{=} o_2(d,2)$ passes, and Action 6 ends with an outcome of "success." Yet, it may be the case that $m$ is not a true, bit-for-bit copy of $d$.

One may counter with the following.

- One may argue that it is unlikely that $o_1, o_2$ are constant functions as we suggest above, given assurances from the respective vendors.
- These tools are tested, as per Action 12.

□

This brings us to propose the following property:

**Property 15** (Recommended)**.** *The process must (i) generate sufficient evidence so desirable properties can be established to be met, and, (ii) not generate any evidence that may be used to undermine claims of meeting a desirable property.*

**Claim 15.** *Action 6 does not uphold Property 15.*

*Proof.* A proof focuses on (ii) within the property. Suppose in Action 6, $o_1(d,1) = o_2(d,2)$, but $o_1(d,1) \neq o_1(m,3)$. The process ends with an outcome of "success." However, there exists evidence that the OPP has generated, specifically, $o_1(d,1) \neq o_1(m,3)$ which undermines the claim that Property 14 has been met. □

### 4.4.1 Return of Device to Storage

**Claim 16.** *Action 7 does not uphold Property 6.*

The same reasoning used for Claim 2 applies to Claim 16. Since Action 7 is not in-line with the ISO/IEC 27037 guidelines, Action 7 does not uphold Property 6.

### 4.4.2 Shared Network Drive - Upload

**Claim 17.** *Action 8 does not uphold Property 14.*

*Proof.* The purpose of Action 8 is to ensure that a change that occurs in the copying of files from one place to another is detected.

We start by analyzing the places where such changes could occur. Let $m_s$ be the image $m$ at the source $s$ and $m_d$ be the image $m$ at the destination $d$. This brings us to the following possibilities:

1. A bit $m[i]_s$ is changed at $s$ before $m[i]_d$ is written at $d$.
2. A bit $m[i]_s$ is changed at $s$ after $m[i]_d$ is written at $d$.
3. A bit $m[i]_d$ is changed at $d$.

Next, we analyze if Action 8 can recognize in the above possibilities.

1. A bit $m[i]_s$ is changed at $s$ before $m[i]_d$ is written at $d$: Image $m$ then becomes image $m'$ at $s$. The tool will then copy image $m'$ to $d$ and calculate $o(m', d)$ and $o(m', s)$ and $o(m', s) = o(m', d)$ so the action will end with an outcome of "success". This however violates Property 14.
2. A bit $m[i]_s$ is changed at $s$ after $m[i]_d$ is written at $d$: The tool will copy image $m$ to $d$. Then image $m$ becomes image $m'$ at $s$. The tool will then calculate $o(m, d)$ and $o(m', s)$ and $o(m', s) \neq o(m, d)$ so the action will end with an outcome of "fail".
3. A bit $m[i]_d$ is changed at $d$: The tool will copy image $m$ to $d$. Then image $m$ becomes image $m'$ at $d$. The tool will then calculate $o(m', d)$ and $o(m, s)$ and $o(m, s) \neq o(m', d)$ so the action will end with an outcome of "fail".

As can be seen in [1], it is possible that a change is not detected during Action 8. This undermines Property 14. □

## 4.5 Pre-Analysis Process

Next, we introduce a set of claims with respect to the pre-analysis process.

### 4.5.1 Shared Network Drive - Download

**Claim 18.** *Action 9 does not uphold Property 14.*

*Proof.* The same proof as the proof for Claim 17 applies to Claim 18. It is possible that a change is not detected during Action 8. This undermines Property 14. □

### 4.5.2 Hashing

**Claim 19.** *Actions 9 and 10 do not uphold Property 15.*

*Proof.* We start with the possibilities that were used for the proof to Claim 17.

1. A bit $m[i]_s$ is changed at $s$ before $m[i]_d$ is written at $d$.
2. A bit $m[i]_s$ is changed at $s$ after $m[i]_d$ is written at $d$.
3. A bit $m[i]_d$ is changed at $d$.

However, since Action 10 is followed by Action 9, we consider the results of above possibilities after both.

1. A bit $m[i]_s$ is changed at $s$ before $m[i]_d$ is written at $d$: Image $m$ then becomes image $m'$ at $s$. Action 9 will then copy image $m'$ to $d$ and calculate $o(m', d)$ and $o(m', s)$ and $o(m', s) = o(m', d)$ so the action will end with an outcome of “success”. If $i$ is a bit located in the data blocks or the header, the recalculated CRC and MD5 with high probability, will not match. Hence, Action 10 will end with an outcome of “fail”. If $i$ is a bit located in CRC blocks or the MD5 block, the recalculated CRC and MD5 with high probability, will not match. Hence, Action 10 will still end with an outcome of “fail”.

2. A bit $m[i]_s$ is changed at $s$ after $m[i]_d$ is written at $d$: Action 9 will copy image $m$ to $d$. Then image $m$ becomes image $m'$ at $s$. Action 9 will then calculate $o(m, d)$ and $o(m', s)$ and $o(m', s) \neq o(m, d)$ so Action 9 will end with an outcome of “fail”.

   The process would then be halted here.

3. A bit $m[i]_d$ is changed at $d$: The tool will copy image $m$ to $d$. Then image $m$ becomes image $m'$ at $d$. The tool will then calculate $o(m', d)$ and $o(m, s)$ and $o(m, s) \neq o(m', d)$ so the action will end with an outcome of "fail".

   The process would then be halted here.

[1] undermines Property 15, hence Actions 9 and 10 do not uphold Property 15. □

This brings us to another property that OPP should adopt:

**Property 16** (Recommended)**.** *A process should not have two actions, that aim to achieve the same goal, disagree.*

**Claim 20.** *Actions 9 and 10 do not uphold Property 16.*

*Proof.* Action 9 and Action 10 both aim to uphold Property 14. In (1) from the Proof for Claim 19, Action 9 ends with an outcome of "success" and Action 10 ends with an outcome of "fail".

Since there exists a scenario when two actions that aim to achieve the same goal disagree, there is evidence generated which undermines Property 16. □

### 4.5.3 Analysis

**Claim 21.** *Action 11 upholds Property 6.*

As per ISO/IEC 27037 [4], the original data should be used as little as possible in order to preserve the digital evidence.

As per NIST 800-86 [19], any analysis on the digital evidence should be done on the forensic image in order not to modify the original digital evidence on the device such that the process can be repeated if required.

Performing this action ensures that Property 6 is upheld during analysis as the original digital evidence on the device is not being analyzed. Therefore, Property 6 is upheld.

## 4.6 Other Related Actions and Properties

### 4.6.1 Tool Testing

**Claim 22.** *Action 12 does not uphold Property 9.*

As per NIST 800-86 [19], digital forensic tools should be tested rigorously. NIST developed its own standard for testing tools, namely the Computer Forensics Tool Testing (CFTT) project. This project outlines the tools that exist on the market that have been evaluated and passed their testing procedures and also developed a test scheme for tools to be regularly tested with. Testing includes informal requirements for imaging tools and software/hardware write blockers [18].

Since Action 12 does not test their tools regularly nor as thoroughly as recommended by NIST 800-86, Action 12 does not uphold Property 9.

# Chapter 5

# Amended Process

In Chapter 4, we iterate through a series of actions and their respective properties and show whether the actions upheld the properties. Certain actions did uphold the properties they intended to, but some did not. In this chapter, we propose changes to the actions that did not uphold their respective properties.

## 5.1 Claim 14 and 15

We adopt the following three principles.

1. To be able to claim that an image $m$ of a device $d$ is indeed a true, bit-for-bit copy with high probability based on the comparison of the output of a function to which each of $m$ and $d$ is subjected, that function must indeed be a cryptographic hash function. More specifically, that function must possess the second preimage property.

   **Definition 17.** *A function $f : A \rightarrow B$ is said to be second preimage resistant if given $a \in A$ chosen uniformly at random, it is computationally hard to detemine $a' \in A, a' \neq a$ such that $f(a) = f(a')$.*

   We can hypothesize that OPP's chosen function, MD5, is indeed second preimage resistant; that is likely a reasonable assumption. However, we must then establish that any function we actually use, e.g., $o_1$ from Action 6 in Section 3.6 is indeed MD5.

That is, our hypothesis is:

$$\text{md5}(x) = \text{md5}(y) \implies x = y$$

From that, we can infer:

$$f = \text{md5} \implies (f(x) = f(y) \implies x = y)$$

Thus, one of our challenges is indeed to be able to claim that a function we adopt is indeed MD5.

2. No information or evidence should be generated that violates Property 15; specifically, (ii) within that property. For example, if in any step of the process OPP follows, for a device $d$ and image $m$, $\text{hash}(d) \neq \text{hash}(m)$, OPP is responsible to provide the reason behind the hash mismatch. A similar situation arises if $\text{hash}_1(d) \neq \text{hash}_2(d)$.

3. Ideally, Property 15 should be met, but in extenuating circumstances, such as disk failure, that may not be possible. OPP should place care not to generate information or evidence that violate Property 15 by introducing more tools and actions than necessary, but violating Property 15 may be unavoidable in certain circumstances. In those circumstances, we propose a new property we recommend OPP adopt:

   **Property 17** (Recommended)**.** *In situations where Property 15 is violated, sufficient explanation in the form of documentation and data should be presented to show that the digital evidence was not tampered with via tools and actions used and that the integrity of the digital evidence cannot be undermined.*

### 5.1.1 The Proposed Amendments to Action 6

We first adopt what we call an oracle for MD5. That is, some software or hardware tool that claims to compute MD5, and there is public, widely-accepted agreement that indeed the tool computes MD5 of an input bit string. For example, one could adopt md.digest() from a recent version of the java.security.MessageDigest class of the Java Development Kit version 12. This oracle can be adopted as an OPP standard, i.e., it does not change over time.

We adopt the following notation similar to Action 6 in Section 3.6:

| | |
|---|---|
| $\mathrm{md5}(x,t)$ | the MD5 hash of $x$ computed at some time $t$ using an oracle for MD5 |
| $o_1(x,t)$ | A hash function computed by Tool 1 on $x$ at time $t$ |
| $o_2(x,t)$ | A hash function computed by Tool 2 on $x$ at time $t$ |
| $d$ | (the digital evidence on) a device |
| $m$ | An image of the device $d$ |

1. For a few, $n$, random bit strings $r_1, r_2, \ldots, r_n$ compute $\mathrm{md5}(r_1,1), \ldots, \mathrm{md5}(r_n,n)$, $o_1(r_1,n+1), \ldots, o_1(r_n,2n)$, $o_2(r_1,2n+1), \ldots, o_2(r_n,3n)$. Then check:

$$\begin{aligned}
\mathrm{md5}(r_1,1) &\stackrel{?}{=} o_1(r_1,n+1)\\
\mathrm{md5}(r_1,1) &\stackrel{?}{=} o_2(r_1,2n+1)\\
\\
\mathrm{md5}(r_2,2) &\stackrel{?}{=} o_1(r_2,n+2)\\
\mathrm{md5}(r_2,2) &\stackrel{?}{=} o_2(r_2,2n+2)\\
\\
&\cdots\\
\\
\mathrm{md5}(r_n,n) &\stackrel{?}{=} o_1(r_n,2n)\\
\mathrm{md5}(r_n,n) &\stackrel{?}{=} o_2(r_1,3n)
\end{aligned}$$

We record: each of $r_1, \ldots, r_n$, the MD5 hash of each as computed by the oracle $\mathrm{md5}(\cdot,\cdot)$, and the hashes output by $o_1(\cdot,\cdot)$ and $o_2(\cdot,\cdot)$.

If any of the above checks fails, whichever of $o_1$ or $o_2$ that corresponds to that failed test cannot be used without further investigation of that tool.

Two notes on this step:

(a) The value $n$ does not have to be large; however it should not be too small. For example, $n \geq 5$ should be fine. We could even pick a random $n$ between, say, 5 and 10 each time. Also, we could pick a random length for each $r_i$, which can be determined by typical sizes the OPP sees for devices.

(b) What "random" means in this step: the next time we execute this step, immaterial of whether it is for this same case/device or another case/device, we need to generate another, new set of random strings. Of course there is a (presumably small) chance that the same string $r_i$ from some previous instance of running this step is generated again. That is ok provided our method for generating/choosing the $r_1, \ldots, r_n$ is sound. A sound method would be, for example, reading the /dev/urandom filesystem object in a Linux system.

2. If the check in (1) above passes, we proceed to this step. We compute $o_1(m, 3n+1)$ and $o_1(d, 3n+2)$. We then check:

   $$o_1(m, 3n+1) \stackrel{?}{=} o_1(d, 3n+2)$$

   If this check fails, that is a "fail". The imaging process would then be restarted from Action 5 one more and the forensic image contained in this imaging attempt would be saved.

3. If all the checks in Step (2) above pass, then we proceed to this final step.

   We compute: $o_2(d, 3n+3)$. We then check:

   $$o_1(d, 3n+2) \stackrel{?}{=} o_2(d, 3n+3)$$

   A failure of the above check is again a "fail". The imaging process would then be restarted once more from Action 5 and the forensic image contained in this imaging attempt would be saved.

### 5.1.2 Action 6 vs. the Properties

**Claim 23.** *Action 6 upholds Property 14.*

*Proof.* We start with what we can articulate as a sub-claim: each of $o_1$ and $o_2$, with high assurance at the time we carry out the amended Action 6, realize MD5. This follows from the success of Step 1, which compares them to our oracle for MD5. Thus, along with the assumptions we make under Principle (1), the success of Step 2 implies that the device does not change with time. This in turn implies Property 5.

The inference that $o_1$ realizes MD5 and the successful check of Step 3 implies that Property 14 is satisfied.

□

**Claim 24.** *Action 6 upholds Properties 15 and 17.*

*Proof.* The success of Step 1 presents sufficient explanation that the tools used to perform the verification, with high probability do indeed realize MD5. Action 4 in conjunction with Action 5 provides sufficient explanation that proven measures were taken to ensure that digital evidence was not altered with due to tools used. In the case of a failure in Step 2 or 3, two situations could be at play:

1. One of the tools used to perform Actions 5 and/or 6 did not work correctly, or
2. The digital evidence on the device has changed between the time Action 5 was performed and either $3n + 1$, $3n + 2$, or $3n + 3$.

While it is unlikely that a tool used in Action 6 failed due to Step 1, we cannot disregard that possibility. However, a failure of the tools used in Action 6 does not undermine Property 17 nor 15 as due diligence was taken to ensure that those tools were working correctly prior to being used on the device. If tool failure is the cause of the mismatching hash, the data blocks $d_i$ of the E01 image on the second attempt would be the same as those on the first attempt and the RAW image on the second attempt would be the same as the first attempt. Two matching images on two different attempts from the same device would be sufficient proof that the image generated upholds Property 5. Images from both attempts, along with documentation showing the hash mismatch, would suffice to uphold Property 15 and 17.

The second option is that the device itself has changed due to factors like errors or degradation. In such a situation, it is important to limit actions performed on the device, as per Property 4. Hence, a tertiary hash is not performed. Instead, the device is re-imaged. If the device is failing or in a state of degradation, it would be possible to identify the failing sector(s) as the difference between the first and second image. Then, the difference in hash is explained with the memory location(s) of the changing device. Images from both attempts, along with the documentation to show what is causing the hash mismatch, would suffice to uphold Property 15 and 17.

Note that Action 5 and 6 would be performed at most twice. Once if Step 2 and 3 results in "success" and twice if either Step 2 or Step 3 results in "fail".

□

## 5.2 Claim 17, 18, 19 and 20

Action 8 and 9 do not uphold Property 15. Claim 17 and 18 are a result of the way that the action verifies the integrity of the data in motion. As Actions 8 and 9 hashe the image at the destination before the image at the source, it omits detection of a change if the image is changed at the source before is written at the destination.

### 5.2.1 The Proposed Amendments to Action 8 and 9

**Action 8** (Upload to Shared Network Drive). *The forensic image is uploaded to the shared network drive. This is done with a tool that computes the MD5 hash of the image at the source, then copies the image from the source to the destination, then computes the MD5 hash of the image at the destination to ensure that integrity was maintained when the data was in motion.*

*To describe the process precisely, we adopt the following notation:*

| | |
|---|---|
| $o(x, l)$ | *A hash function computed by a tool on input $x$ at location $l$* |
| $m$ | *An image of a device* |

*The process is as follows, in chronological order. We adopt, $s, d$ for the source and destination location of an image.*

1. *The tool calculates o(m, s)*

2. *The image is copied from s to d*

3. *The tool calculates o(m, d)*

4. *We perform the following check:*

$$o(s, m) \stackrel{?}{=} o(m, d)$$

5. *If the check $o(s, m) \stackrel{?}{=} o(m, d)$ from #4 above succeeds, the action ends with an outcome of "success." Otherwise, i.e., if $o(s, m) \neq o(m, d)$, then we the action ends with an outcome of "fail."*

**Action 9** (Download to Shared Network Drive). *For an analyst to commence analysis, the image of a device must be downloaded from the shared network to the analyst's local* *forensic workstation. This is done with a tool that computes the MD5 hash of the image at the source, then copies the image from the source to the destination, then computes the MD5 hash of the image at the destination to ensure that integrity was maintained when the data was in motion.*

*To describe the process precisely, we adopt the following notation:*

| | |
|---|---|
| $o(x, l)$ | *A hash function computed by a tool on input $x$ at location $l$* |
| $m$ | *An image of a device* |

*The process is as follows, in chronological order. We adopt, $s, d$ for the source and destination location of an image.*

1. *The tool calculates o(m, s)*

2. *The image is copied from s to d*

3. *The tool calculates o(m, d)*

4. *We perform the following check:*

$$o(s, m) \overset{?}{=} o(m, d)$$

5. *If the check $o(s, m) \overset{?}{=} o(m, d)$ from #4 above succeeds, the action ends with an outcome of "success." Otherwise, i.e., if $o(s, m) \neq o(m, d)$, then we the action ends with an outcome of "fail."*

### 5.2.2 Action 8 and 9 vs. the Properties

**Claim 25.** *Action 8 upholds Property 14.*

*Proof.* The purpose of Action 8 is to ensure that a change that occurs in the copy of images from one place to another is detected.

We start by identifying the potential places where such changes could occur. Let $m_s$ be the image $m$ at the source $s$ and $m_d$ be the image $m$ at the destination $d$. This brings us to the following possibilities:

1. A bit $m[i]_s$ is changed at $s$ before $m[i]_d$ is written at $d$.

2. A bit $m[i]_d$ is changed at $d$.

Next, we analyze if Action 8 can recognize the above possibilities.

1. A bit $m[i]_s$ is changed at $s$ before $m[i]_d$ is written at $d$: The tool calculates $o(m, s)$. Image $m$ then becomes image $m'$ at $s$. The tool will then copy image $m'$ to $d$ and calculate $o(m', d)$. $o(m', d) \neq o(m, s)$ so the action will end with an outcome of "fail".

2. A bit $m[i]_d$ is changed at $d$: The tool calculates $o(m, s)$. The it will then copy image $m$ to $d$. Then image $m$ becomes image $m'$ at $d$. The tool will then calculate $o(m', d)$. $o(m, s)$ and $o(m, s) \neq o(m', d)$ so the action will end with an outcome of "fail".

The change is detected in all possibilities. Hence, this action upholds Property 14. □

**Claim 26.** *Action 9 upholds Property 14.*

*Proof.* The same proof as the proof for Claim 25 applies to Claim 26. The change is detected in all possibilities. Hence, this action upholds Property 14. □

**Claim 27.** *Actions 9 and 10 uphold Property 15.*

*Proof.* We start with the possibilities that were used for proof to Claim 25.

1. A bit $m[i]_s$ is changed at $s$ before $m[i]_d$ is written at $d$.

2. A bit $m[i]_d$ is changed at $d$.

However, since Action 10 is followed by Action 9, we consider the results of above possibilities after both.

1. A bit $m[i]_s$ is changed at $s$ before $m[i]_d$ is written at $d$: Action 9 calculates $o(m, s)$. Image $m$ then becomes image $m'$ at $s$. The tool will then copy image $m'$ to $d$ and calculate $o(m', d)$. $o(m', d) \neq o(m, s)$ so the action will end with an outcome of "fail". If $i$ is a bit located in the data blocks or the header, the recalculated CRC and MD5 with high probability, will not match. Hence, Action 9 will end with an outcome of "fail". If $i$ is a bit located in CRC blocks or the MD5 block, the recalculated CRC and MD5 with high probability, will not match. Hence, Action 10 will still end with an outcome of "fail".

2. A bit $m[i]_d$ is changed at $d$: Action 9 calculates $o(m, s)$. It will then copy image $m$ to $d$. Then image $m$ becomes image $m'$ at $d$. The tool will then calculate $o(m', d)$. $o(m, s) \neq o(m', d)$ so the action will end with an outcome of "fail".

   The process would then be halted here.

Hence, Action 9 and Action 10 uphold Property 15 as no evidence is generated that can be used to undermine desirable properties. □

**Claim 28.** *Action 9 upholds Property 16*

*Proof.* Action 9 and Action 10 both aim to uphold Property 14. In (1) from the proof for Claim 27, Action 9 ends with an outcome of "fail" and Action 10 ends with an outcome of "fail".

Since Action 9 and Action 10 aim achieve the same goal of image integrity and both agree in their outcome given the same inputs, Property 14 is upheld. □

## 5.3 Claim 2 and 16

We propose OPP adopt ISO/IEC 27037's recommendations for storage of devices to protect from magnetic degradation, electric degradation, heat, high or low humidity exposure, shock and vibration [4].

### 5.3.1 The Proposed Amendments to Action 2 and 7

**Action 2** (Retrieval of Device from Storage). *After the device is seized and placed in the property bag, it arrives in the possession of the imagers. The device is then placed in an anti-static bag if the device is sensitive to static electricity. Additionally to an anti-static bag, magnetic storage media is further placed in packaging that is magnetically inert and free of particles. The device is then stored away from electromagnetic sources and in a storage environment free of static electricity. The storage environment is free of dust, moisture, grease, and chemical pollutants as this can accelerate oxidation deterioration and moisture condensation on magnetic components. The storage environment is also free from UV light and thermal shock as it may damage some types of digital media. When the device is handled, it is handled with lint-free gloves that are clean and dry.*

**Action 7** (Return of Device to Storage). *Once the actions that need to be performed on the device are complete, the device is placed back into the same property bag it was removed from in Action 2 with lint-free gloves that are clean and dry. The device is then placed in an anti-static bag if the device is sensitive to static electricity. Additionally to an anti-static bag, magnetic storage media is further placed in packaging that is magnetically inert and free of particles. The device is then stored away from electromagnetic sources and in a storage environment free of static electricity. The storage environment is free of dust, moisture, grease, and chemical pollutants as this can accelerate oxidation deterioration and moisture condensation on magnetic components. The storage environment is also free from UV light and thermal shock as it may damage some types of digital media. It is then return to storage.*

### 5.3.2 Action 2 and 7 vs. the Properties

**Claim 29.** *Action 2 and 7 uphold Property 5.*

Since Action 2 and 7 are in-line with the ISO/IEC 27037 guidelines, they uphold Property 5.

## 5.4 Claim 22

We propose OPP adopt NIST's CFTT project for testing and validation of digital forensics tools. NIST's CFTT project uses a tool testing mechanism based on "*well-recognized international methodologies for conformance testing and quality testing*" [14]. The CFTT project specifies the test procedures, test criteria, test set, and test hardware for all tools tested and their objective is to ensure that forensic tools consistently produce both accurate and objective results.

CFTT developed test suites specially designed for an organization to test their own forensic tools via the Federated Testing test suites. This test suite includes testing for *"disk imaging, forensic media preparation, forensic string search, hardware write blocking, and mobile forensics data extraction tools"* and in the future, will add testing for more forensic functionality and tools such as deleted file recovery and forensic file carving. The Federated Testing suite generates a report for the tool tested that includes how the tool was tested and what the results of those tests were [15].

### 5.4.1 The Proposed Amendments to Action 12

**Action 12** (Testing of Tools). *Tools are tested according to guidelines set out by NIST's CFTT project for each category of tool used and their specific manufacturer and version. The guidelines specify test procedures, test criteria, test set and test hardware. Testing of tools is performed any time a tool is used for the first time, updated, or produces incorrect results in either the imaging or pre-analysis process. Tools are also tested regularly at 6-month intervals. The Federated Testing report for each tool used in the imaging and pre-analysis process is attached to the forensic report provided to the investigator, Crown attorney, and Defense attorney.*

### 5.4.2 Action 12 vs. the Properties

**Claim 30.** *Action 12 upholds Property 9.*

Since Action 12 tests their tools as per guidelines recommended by NIST's CFTT project, Action 12 upholds Property 9.

# Chapter 6

# Related and Future Work

## 6.1 Related Work

Aijiola et al. [13] reviews and analyzes NIST SP 800-101 and ISO/IEC 27037 to identify similarities, differences, and limitations in both. It further proposes an implementation of both standards.

Verber et al. [26] compares the digital forensics process of a law enforcement agency in the Czech Republic to the ISO/IEC 27037 standard. The contributions of this work are similar in nature to ours. The paper acts as an exemplar for digital forensics experts from other countries and organizations who also want to compare their digital forensics process to the ISO/IEC 27037 standard.

## 6.2 Future Work

### 6.2.1 Other Phases of the Digital Forensics Process

In our work, we analyze the forensic soundness of OPP's acquisition phase. However, there are three phases in the digital forensics process that involve the handling of evidence, as per Figure 2.1. The identification and seizure phase involves the handling of the devices, and the examination and analysis phase involves the manipulation of the digital evidence from the device. Since both these phases also involve a form of digital evidence, they should all be analyzed using our framework to determine if they uphold forensic soundness.

### 6.2.2 Types of Devices

In our work, we strictly analyze the forensic soundness of the acquisition phase for digital storage devices, but digital evidence is harvested from various powered-on and powered-off devices including mobile phones, tablets, IoT devices, and servers. In our work, we investigate the forensic soundness of devices that have digital evidence in static memory. The preservation of data on such devices is more easily accomplished and the integrity of the data extracted can be more easily verified. However, that is not the case for all devices. For example, currently, mobile phones must be powered on and running during the imaging, ie. Action 5. A new problem now needs to be addressed with respect to the preservation of data and evidence integrity for powered-on devices.

### 6.2.3 Adversary

In our analysis, we do not consider the imagers and analysts who perform the digital forensics process to be malicious. They are not trying to corrupt evidence. We further do not consider an external malicious actor who may gain access to OPP's digital forensics resources, such as a local forensic workstation or the shared network drive in 3.2. Future work should be performed to determine how our framework could be applied to identify a malicious actor and tampered evidence.

# Chapter 7

# Conclusion

Our work analyzes the acquisition phase of OPP's digital forensics process. We begin by taking the process being implemented and extract a series of properties that OPP aims to uphold. We then analyze whether OPP upholds those properties and propose additional properties and amendments to parts of the current process that do not. While the result of our work is a thorough vetting of OPP's current process, it also serves as a framework that other digital forensics organizations can adopt.

# References

[1] Best Evidence Rule. URL: http://criminalnotebook.ca/index.php/Best_Evidence_Rule.

[2] Criminal Charge Process. URL: https://www.legalaid.on.ca/faq/criminal-charge-process/.

[3] Digital Evidence. URL: http://www.forensicsciencesimplified.org/digital/.

[4] Information Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. Standard ISO/IEC 27037:2012, Geneva, CH. URL: https://www.iso.org/standard/44381.html.

[5] Ontario Provincial Police. URL: https://www.opp.ca/.

[6] Section 342.1(2) - Definition of Computer System. https://www.criminal-code.ca/criminal-code-of-canada-section-342-1-2-definition-of-computer-system/index.html.

[7] Step 2: Primary Sources of Law: Canadian Case Law. URL: https://library.law.utoronto.ca/step-2-primary-sources-law-canadian-case-law-0.

[8] Step 2: Primary Sources of Law: Canadian Legislation. URL: https://library.law.utoronto.ca/step-2-primary-sources-law-canadian-legislation.

[9] What is Forensically Sound. URL: https://www.igi-global.com/dictionary/forensic-readiness-and-ediscovery/44368#:~:text=Forensicsoundnessgivesreasonableassurance,in:ForensicReadinessandeDiscovery.

[10] Common Types of Computer Crimes, Nov 2018. URL: https://jsberrylaw.com/blog/common-types-of-computer-crimes/.

[11] Digital Forensics, Nov 2021. URL: https://en.wikipedia.org/wiki/Digital_forensics.

[12] CPLEA Administrator. Criminal Code - General, Sep 2015. URL: https://www.law-faqs.org/national-faqs/criminal-code/criminal-code/.

[13] Akinola Ajijola, Pavol Zavarsky, and Ron Ruhl. A review and comparative evaluation of forensics guidelines of nist sp 800-101 rev. 1: 2014 and iso/iec 27037: 2012. In *World Congress on Internet Security (WorldCIS-2014)*, pages 66–73. IEEE, 2014.

[14] Thelma Allen. Computer Forensics Tool Testing Program (CFTT), Nov 2019. URL: http://www.cftt.nist.gov/.

[15] Thelma Allen. Federated Testing Project, Oct 2021. URL: https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/federated-testing.

[16] Legislative Services Branch. Consolidated Federal Laws of Canada, Canada Evidence Act. URL: https://laws-lois.justice.gc.ca/eng/acts/c-5/fulltext.html.

[17] Digital Forensics Unit - Ontario Provincial Police, Orillia, Ontario, Canada.

[18] Andreas Enbacka and Linas Laibinis. *Formal Specification and Refinement of a Write Blocker System for Digital Forensics*. Citeseer, 2005.

[19] Karen Kent, Suzanne Chevalier, Timothy Grance, and Hung Dang. Sp 800-86. guide to integrating forensic techniques into incident response. Technical report, 2006.

[20] Gary C Kessler and Gregory H Carlton. A study of forensic imaging in the absence of write-blockers. *Journal of Digital Forensics, Security and Law*, 9(3):51, 2014.

[21] Jan Krasniewicz and Sharon A Cox. Uncovering limitations of e01 self-verifying files. In *Encyclopedia of Information Science and Technology, Fourth Edition*, pages 1384–1394. IGI Global, 2018.

[22] Jing Leng and Tonghong Li. Research on computer system information hiding anti-forensic technology. In *8th International Conference on Social Network, Communication and Education (SNCE 2018). Atlantis Press*, 2018.

[23] Rodney McKemmish. *What is Forensic Computing?* Australian Institute of Criminology Canberra, 1999.

[24] Rodney McKemmish. When is digital evidence forensically sound? In *IFIP International Conference on Digital Forensics*, pages 3–15. Springer, 2008.

[25] Scientific Working Group on Digital Evidence. Swgde best practices for computer forensic acquisitions. Technical report, April 25, 2018.

[26] Jaromir Veber and Zdenek Smutny. Standard iso 27037: 2012 and collection of digital evidence: Experience in the czech republic. In *European Conference on Cyber Warfare and Security*, page 294. Academic Conferences International Limited, 2015.