2017-06-01

Measuring The Robustness of Forensic Tools' Ability to Detect Data Hiding Techniques

Samuel Isaiah Moses
Brigham Young University

Measuring the Robustness of Forensic Tools' Ability to Detect Data Hiding Techniques

Samuel Isaiah Moses

A thesis submitted to the faculty of
Brigham Young University
in partial fulfillment of the requirements for the degree of

Master of Science

Dale C. Rowe, Chair
Joseph J. Ekstrom
Barry M. Lunt

School of Technology

Brigham Young University

ABSTRACT

Measuring The Robustness of Forensic Tools' Ability to Detect Data Hiding Techniques

Samuel Isaiah Moses
School of Technology, BYU
Master of Science

The goal of this research is to create a methodology that measures the robustness and effectiveness of forensic tools' ability to detect data hiding. First, an extensive search for any existing guidelines testing against data hiding was performed. After finding none, existing guidelines and frameworks in cybersecurity and cyber forensics were reviewed. Next, I created the methodology in this thesis.

This methodology includes a set of steps that a user should take to evaluate a forensic tool. The methodology has been designed to be flexible and scalable so as new anti-forensic data hiding methods are discovered and developed, they can easily be added to the framework, and the evaluator using the framework can tailor it to the files they are most focused on. Once a polished draft of the entire methodology was completed, it was reviewed by information technology and security professionals and updated based on their feedback.

Two popular forensic tools – Autopsy/Sleuthkit and X-Ways – were evaluated using the methodology developed. Evaluation revealed improvements in the methodology that were updated. I propose that the methodology can be an effective tool to provide insight and evaluate forensic tools.

Keywords: forensics, anti-forensics, methodology, security

ACKNOWLEDGEMENTS

I would like to my thank my family and friends, who have supported me through this thesis, school, and life. Their support was monumental. Thank you to my committee for their guidance and support. Lastly, deep gratitude to our Lord. His blessings, support, and guidance is what has enabled me to be where I am today.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

Computing technology has become so commonplace in society that it is hard to imagine a world without computers and the comforts they provide. Computers have become a necessity. They are at the center of our commerce, our trade, our banking, our travel, our work, and our leisure, but it wasn't always that way. In 1948, the Manchester Mark I computer was designed and built at Manchester University in England by Fredric Williams, Tom Kilburn, and others. The Manchester Mark I is generally accepted as the first computer (O'Regan, 2008). This invention, the Manchester Mark I, was a significant advancement in computing due to its ability to store and run programs. These advancements are the foundation on which computer languages were built, allowing complex computation to be written in human readable code rather than the 1s and 0s of machine code. In our current state of technological advancement, most users interact with computers through graphical interfaces and applications. The everyday user can do so without needing to understand how the core code and machine language of a computer actually work.

The computer was invented to advance our understanding of sciences and to aid humankind. Sadly, some have found ways to exploit computers for malicious purposes. In the early decades, about 1960 to 1980, when less expensive computers were first being developed, their greatest threat was physical damage or sabotage. Most attacks were performed by individuals such as dishonest employees (Kabay, 2008). With the advent of computers starting

around 1970, malicious people realized they could use social engineering to get around computer safeguards. Social engineering is the use of information gathering and persuasion techniques that target human nature in order to sway people to conform to one's own desires and allow them to take advantage (Moses, Baker, & Rowe, 2016). People who began attacking computers and circumventing safeguards became known as the first hackers. A hacker is a person who uses computers to aid them in gaining unauthorized access to a computer or system. Criminal hacking includes web defacements, theft of computer files, changing settings or files on a computer without permission, etc. Kevin Mitnick is a famous and notorious example of criminal hacking. Around 1980, Mitnick used social engineering and hacking to break into phones and computers to perform malicious pranks (Kabay, 2008). As the 1990s approached, financial crime was on the rise and by the mid-1990s spam, a form of commercial advertising known to reach out to masses rather than a targeted demographic for monetary gain, and email attacks started growing. Today, cybercrime is a constant threat. Identity theft is a constant concern, which is when malicious attackers attempt to steal your personal and financial information. There is a profitable underground market for stolen data and computer resources.

With the proliferation of computers and the rise of cybercrime, the discipline of cyber forensics was formed to better counteract the criminal activity. Cyber forensics, sometimes referred to as digital forensics, is the application of investigative techniques and methods to gather digital evidence of a malicious attack. This data is gathered from devices such as computers, servers, or mobile phones and from the network traffic. The gathered data is used to discover information about breaches of information and malicious attacks. Often this data is used in the court of law as digital evidence. Forensic investigators and security professionals use these techniques to gather information to discover the who, what, where, when, and why of a

malicious attack. This information can be used to better defend against similar attacks in the future. For example, internet security expert Tsutoma Shimomura fell victim to some of Mitnick's malicious pranks (Kabay, 2008). After this, Shimomura helped the FBI track and arrest the hacker Kevin Mitnick. Using cyber forensics, the FBI and Shimomura were able to track down Mitnick. Modern day investigators use software and tools to help automate tasks and decrease the time of investigations. Filters are common options available in these software tools that perform forensic analysis by searching through a hard drive looking for specific content. Typically, this is done using the header, Trailer and/or the extension of a file as a signature for the forensic tool to read. Code at the beginning of the file that declares the file type is a header. A Trailer is a set of code at the end of a file that helps define the file type. Extensions are at the end of the file name designating the file type, for example doc, pdf, and txt. Using these as signatures, forensic tools can help to investigate malicious attacks and breaches.

Cyber forensics helps forensic investigators and security professionals learn more about the malicious attack, and what other criminal activity was performed with or assisted by a computer. To better obscure criminal activity and avoid incarceration, the discipline of anti-forensics was developed as a response to cyber forensic. Anti-forensics is the practice of using countermeasures to protect your personal data from being discovered by forensic analysis and investigators (Garfinkel, 2007). Anti-forensic tools and methods share common goals in their attempt to frustrate forensic tools, investigations, and investigators.

Table 1 - Goal of Anti-Forensics

Goals of Anti-Forensics:
Avoiding detection
Disrupting information collection
Increasing the forensic investigator's time
Casting doubt on a forensic report or testimony
Forcing a tool to reveal its presence
Subverting forensic tools
Leaving no evidence that the anti-forensic tool has been run

One way anti-forensics achieves the goal of avoiding detection is by the technique of data hiding. Data hiding involves moving or changing the data to avoid forensic investigators' searches using methods such as encryption. This allows anti-forensics to continue to thwart forensic tools, investigations, and investigators.

The purpose of this research is to develop and test a methodology for testing and measuring the robustness of forensic tools' ability to detect data hiding. To accomplish this, I will address the following research objectives:

- Develop and test a methodology for analyzing forensic tools' ability to detect 7 different file types.
- Determine which forensic tool or tools completed its automated analysis in the least amount of time.
- Determine which forensic tool or tools completed its automated analysis with the fewest false positives and false negatives (errors).
- Determine which forensic tool or tools found the most hidden files.

The rest of this thesis is separated into the following chapters:

- Chapter 2: Literature Review
    - An overview of academic research and publically available web blogs on the current and past research completed on forensics. The Literature Review has been separated into 4 sections: Forensics, Cybercrime, Anti-Forensics, and Standards and Methodologies.
- Chapter 3: Methodology
    - A detailed account of the research objectives and questions along with a description of the process followed for choosing the file types, building test files, and evaluating forensic tools.
- Chapter 4: The Methodology
    - The final draft of the methodology developed for testing the robustness of forensic tool's ability to detect data hiding including notes on how it was changed by reviewers' comments and testing. This also includes how flexibility and scalability were considered.
- Chapter 5: Evaluation of Forensic Tools
    - Results from application of the methodology developed in this thesis, including how the different techniques for each tool were implemented by the reviewer.
- Chapter 6: Forensic Tool Analysis
    - An analysis of the results from the evaluation of the forensic tools completed in Chapter 5.

- Chapter 7: Discussions and Future Work
    - A description of the methodology, discussion of how it was validated and what impact this research can have in cyber forensics.
    - Discussion of potential future research.

2 LITERATURE REVIEW

There is a large collection of research in cyber forensics and anti-forensics. This selection of that research is focused on data hiding. Academic and scholarly works are the main source of information of this literature review, but information was also reviewed and collected from books, websites, class materials, and blog posts. With the improvements in technology, and the growth and need in this industry; it is important to stay up to date on the current information. It is also important to pull information from the historical works that are still used in the field today and which helped shape the field. Relevant information for this thesis involving forensics and specifics about data hiding have been reviewed. The literature review covers forensics and how the current discipline is shaped today. It details what professionals predict needs to and should happen in the future. Cybercrime is reviewed and how it is increasing and affects forensics. The relevant information about anti-forensics has been reviewed, specifically information on categorization and what has been seen by digital investigators. Data hiding has been extensively reviewed and how it relates to this thesis and the developing of the methodology. Last, the evaluation standards and methodologies were reviewed to show the lack of work in this area, and to help meet reasonable standards in the development of this new methodology.

2.1 Forensics

One of the many disciplines covered in cyber security is cyber forensics. Cyber forensics is the application of investigative techniques and analysis methods to gather digital evidence from devices such as computers, servers, mobile phones or network traffic. Digital evidence is analyzed by forensic investigators and security professionals to decipher the purpose behind a cyberattack. Analysis can reveal what location an attack originated came from; what information or data the attacker was after; and whether they were attempting malicious destruction, theft of data, or extortion such as ransomware. The digital evidence or electronic evidence is to be handled using specific procedures and chain of custody to ensure that the evidence is admissible in court.

Digital Forensics Tools: A Comparative Approach (Kamble & Jain, 2015) explains how cyber forensics has become increasingly more important, especially with the advances in the computer and cellular industries. The journal article dives into how cyber forensics helps investigators examine many types of crimes and how most can be connected to computers (Kamble & Jain, 2015). Criminals engage in a variety of crimes, including but not limited to murder, kidnapping, theft, terrorism, and hacking. Sometimes the information stored on the victim's computer or other devices is key to identifying and prosecuting a suspect. Information stored on the suspect's computer can often identify them as the culprit responsible. Digital forensic tools are critical in providing reliable computer analysis, and in gathering digital evidence. The paper touches on two fundamental problems with the design of current cyber forensic tools:

1. The tools are designed to help forensic investigators examine and find specific pieces of evidence, not really assist with investigations.

2. Current forensic tools are created for solving crimes against people (murder, kidnapping, etc.). They were not created to assist in solving crimes committed with computers or against computers (hacking).

The authors of *Digital Forensics Tools: A Comparative Approach* conclude stating that as more knowledge is obtained about how crimes are committed with the aid of computers, the more forensic tools can be updated to gather evidence more efficiently to combat the increase in cybercrime. Digital forensics is a key part of solving crimes with digital devices, against digital devices, against people where evidence resides on a device. The authors believe that, in this evolving digital age, better development requires heavier research in digital forensics.

In *A Survey on Digital Forensics Trends,* (reference) the authors discuss how new developments and innovations have led to new types of cybercrimes. They describe how the correct tools are critical in completing a cyber-forensic investigation with efficiency and effectiveness. The paper discusses some possible options to speed the investigative process, such as identifying the content of a file by just looking at its graphical representation. Alterations to the file can cause issues with this approach. Forensic investigations struggle as scope widens with the research focus expanding to mobile devices and cloud based services. Beyond research in keeping up with technological advancements, anti-forensics is another trend the authors analyze.

Widely marketed forensic software can lead to exposing vulnerabilities in the software code. These vulnerabilities can be exploited, causing software to crash or potentially even destroy evidence. The authors of *A Survey on Digital Forensics Trends* conclude that cyber forensics now requires more coordination and focus to keep up with new and sophisticated cyberattacks (Damshenas, Dehghantanha, & Mahmoud, 2014). Computers and technology are

rapidly evolving, which has caused a rise in cybercrime and cyberattacks and an evolution of the type of attacks. These authors describe how these trends have created an opportunity for anti-forensics techniques and tools to be developed to obfuscate data, attack the forensic tools, or slow investigations.

In the paper *Digital forensics research: The next 10 years,* Simson Garfinkel explains how forensic tools are being used on a daily basis by forensic investigators and security professionals within the local, state, and federal government, military, and private industry. Garfinkel states that while the world had been enjoying a "Golden Age of Digital Forensics" in 2010, that it is quickly going to end (Garfinkel, 2010). More and more organizations are facing data that cannot be analyzed with current tools either because of formatting, encryption, or lack of training. Even if the data can be analyzed, it can be a couple of weeks or months until it is processed and reviewed due to the enormous amount of data auditing creates and its already growing backlog of data. The author states that unless something is done, the capabilities of the forensic tools will be degraded and lost. This paper-helps establish the current position of cyber forensics and predicts a crisis in forensics.

Another common forensic technique used in investigations is hash checking. A hash is a fixed length string of number and letters that will be the same for any identical set of data. Hash checking is a forensic technique of using an algorithm to verify and search for the hash, or specific string, of a file is on the computer or storage device being examined. In forensic investigations, analysts scan for known file hash values stored in large hash databases. The hash of files from the instigation are compared against the database to see if something matches. This is a common practice in cases where commonly known files are involved such as rootkits,

malware, backdoors, and in the case of child porn investigations, specific image files that get shared widely. Hash checking enables rapid searching for known files.

Current forensic tools and methods are working to stay updated with advances in technology and the development of new anti-forensic techniques. Forensic tools' programing code has vulnerabilities in it that can be exploited by anti-forensic techniques. These exploits created for forensic tools are usually planned to crash the investigating tools. Some existing anti-forensic techniques are subtler and attempt to hide key files needed for analysis and investigation. This is why it is necessary to continually update and improve forensic tools (Balan, Dija, & Vidyadharan, 2010; Garfinkel, 2010).

2.2 Cybercrime

In this 2015 feature article, *Cybercrimes: Legislation and Current Trends,* Raneta Mack reviews the rise of cybercrime throughout the world. Mack has taught criminal law, criminal procedure, while collar crime, and comparative criminal procedure at the Creighton University School of Law since 1991. Cybercrime has evolved in its reach of potential targets to include individuals, businesses, and national security infrastructures. These attacks will range from the simple Internet scams to complex cyberattacks. The following attacks constitute much of the current cybercrime trends: identity theft, when one person steals and uses another's personal information; hacking; phishing, sending a mass amount of enticing emails in an attempt to steal one's information; and spear-phishing, a targeted approach of sending a specific detailed email to steal a user's information. She predicted that social media will be the next large cybercrime trend. With many users sharing personal information, it has become at the efficient tool for

gathering information on a target. With the scope of cyberattacks ever expanding and attacks evolving, users need to be continually educated regarding the new threats of cybercrime.

When dealing with cybercrime, investigators are required to perform their due diligence to find the information within the limitations of a search warrant. Forensic investigators are doing their best, but backlogs of evidence are increasing due to an increase in cybercrime and the amount of available and affordable storage.

The growing capacity of storage devices that the data is stored on often leads to insufficient time for creating a forensic image and an investigator has insufficient time to analyze all the data. With the growing accessibility of the cloud infrastructure, sometimes the data or information needed can't even be obtained (Garfinkel, 2010). The backlog of evidence affects even the largest of forensic laboratories. Statistics from the State of Iowa Division of Criminal Investigation exemplifies the struggles forensic crime labs face. In 2012, the crime lab employed a staff of 50 investigative personnel, supported by 46 civilian personnel. Iowa's staff in 2012 performed 856 cybercrime forensic exams and made 91 cyber-crime arrests. In 2013, the crime lab employed the same amount of investigative personnel, and increased their civilian support to 49 people. Today, the Iowa crime lab's case load includes 1372 cyber-crime forensic exams and 49 arrests ("DCIFactSheets," n.d.). This constitutes a 60% increase in the number of investigations and a 46% decrease in arrests made when compared to the previous year. The increased workload creates a reliance on established forensic extraction and analysis tools. As discussed above, these tools have known weaknesses that can be exploited. Due to the increase in data, it is necessary to discover and expose the flaws in current forensic tools as to better understand where improvements can be made.

The digital evidence and forensic reports created by forensic tools need to be based on facts discovered through analysis. As one of the critical requirement to make these reports and evidence as reliable as possible, the results must be reproducible by independent third parties. The case of *Daubert v. Merrell Dow Pharmaceuticals Inc.* set a precedence for how judges determine whether scientific evidence is admissible in federal court (Garrie & Morrissy, 2014). Proper forensic reports that follow these rules have a much better chance of withstanding judicial scrutiny. The *Daubert* standard requires the following factors (Garrie & Morrissy, 2014):

1. Testing: Has the scientific procedure been independently tested?
2. Peer Review: Has the scientific procedure been published and subjected to peer review?
3. Error rate: Is there a known error rate, or potential to know the error rate, that is associated with the use of the scientific procedure?
4. Standards: Are there standards and protocols for the execution of the methodology of the scientific procedure?
5. Acceptance: Is the scientific procedure generally accepted by the relevant scientific community?

First off, this guideline provides a foundation for how judges approve scientific evidence being admitted in court. *Digital Forensics Evidence in the Courtroom: Understanding Content and Quality* continues and expands upon how a forensic report should include sufficient details so a third party can replicate the findings. As part of the report, the tools used in gathering evidence should be explicitly stated. This should include the version number of the tools utilized so supporting evidence can be replicated with exactness.

2.3 Anti-Forensics

The counter to cyber forensics is anti-forensics. Anti-forensics is the implementation of countermeasures used against forensic tools, techniques, and methods. Anti-forensics technics are used to prevent files and information from being discovered by forensic tools being used in an investigation. If hidden or made inaccessible, the data cannot be used by forensic investigators in the court of law. In the paper *Anti-Forensics and the Digital Investigator* categorizes four different anti-forensic methods: 1) data hiding; 2) data destruction; 2) trail obfuscation; and 4) attacks on the forensic process or tool (Kessler, 2007).

The anti-forensics method of data hiding is used to conceal data. It is an individual attempt to hide information by placing the data in the slack and unallocated spaces of a computer's hard drives. Data can also be hidden using stenography, which is the process of hiding information within other data. This could involve altering or changing the data to avoid detection by forensic tools. Encryption is another data hiding technique, and is the process of changing the data to be unreadable without the required password or secret key.

Other anti-forensic methods include data destruction and trail obfuscation. Data destruction is the process of removing and destroying key information. Executing this anti-forensic method properly requires more than just removing the data. It also includes overwriting it to make sure it is unreadable and cannot be recovered. Trail obfuscation is the anti-forensic process of hiding the path of an attack so that it cannot be retraced to the source. There are many ways trail obfuscation can be completed such as address spoofing, web anonymizers, and wiping or altering server logs. This is done with the goal of making it impossible for an investigator to trace an attack back to its source.

The last category Kessler discussed is attacks on digital forensic methods or tools. Attacking forensic tools requires targeting the known weaknesses in investigation procedures or well-known forensic tools. These attacks can include a Denial of Service (DoS), an attempt to crashing the forensic tool, or even forcing the tool to wipe data. Generally, the goal of attacking the tool is to target the credibility of the evidence, rendering it unusable in the court of law. At least cause, these attacks can force the investigator to spend extra time on the investigation (Kessler, 2007).

Kessler continues in *Anti-Forensics and the Digital Investigator* to explain that the goal of anti-forensic techniques and methods is to disrupt forensic investigations and remove the value of the evidence gathered (Kessler, 2007). When analyzing evidence, forensic investigators must follow established rules and guidelines within the confines of the laws. By following these guidelines, validation is provided to evidence when investigators present in court. Anti-forensic methods are developed to hide critical data, lengthen investigations and attack the credibility of that evidence. These anti-forensic methods continually create challenges for forensic investigators. Clearly, Kessler states that it has become critical that academia and industry coordinate together to research and develop ways to protect and defend against anti-forensic techniques. Part of this research should include considering new attack vectors and anti-forensic methods.

The work *Anti-Forensics: A Practitioner Perspective* (de Beer & Van Belle, 2015) explains the need for investigators to expect anti-forensic tools. Suspects have become more aware of the tools and methods investigators use and are creating more sophisticated attacks. De Beer, one author of *Anti-Forensics: A Practitioner Perspective*, explains how these challenges make it difficult for forensic investigators to stay informed on the current anti-forensic techniques. With

anti-forensic tools constantly being developed, any investigation has the inherent risks of evidence being overlooked, misrepresented, or destroyed (de Beer & Van Belle, 2015). As part of the research a questionnaire was distributed for forensic investigators to review the impact of anti-forensics. 85% of investigators stated that anti-forensics affects their ability to recover evidence during their investigations. Over 60% of the forensic investigators responded agreeing that anti-forensics has impacted their ability to present evidence, and that anti-forensics regularly impacts their ability to present usable evidence. *Anti-Forensics: A Practitioner Perspective* is limited because the methodology focuses on South African forensic investigators, but can be applied on a wider scale.

In *Anti-Forensics: Techniques, Detection and Countermeasures*, Garfinkel separates data hiding into three distinct categories: cryptography, steganography, and generic data hiding techniques. Cryptography is very effective at hiding and securing data, but the encrypted data itself is easy to detect. Encrypted data has high entropy in its files and many forensic tools can flag encrypted data. Entropy when related to digital information measures the randomness in a given set of values. Due to the algorithms used in encryption, the randomness increases causing the entropy of a file to increase when encrypted. Once the key to the encrypted data is obtained, the original data can be recovered. Current states of legal cases have shown that law enforcement and the courts force suspects to give up the key to encrypted information. In October 2014, a Virginia Circuit Court judge ruled that obtaining biometric data from a suspect is not divulging knowledge (Price, 2014). That means unlike passwords, fingerprints can be scanned and used involuntarily. So, if you use a biometric scan to protect your computer, they can unlock your computer and get access to your data. Due to this, a strong password or passphrase may seem better than biometrics, but authorities have been approved to persuade the suspect to disclose the

data. In the U.K., a computer science student was imprisoned for six months after refusing a court order to surrender his password (Price, 2014). Other countries have similar disclosure laws. In Australia, a six-month sentence is given to those who don't comply with the disclosure of their password. It can be up to seven years in India or in France, three years' prison and a $56,000 fine; while in South Africa, 10 years or $180,000 fine. Countries across the world are charging fines and imprisoning people for not disclosing their passwords. The United States varies across jurisdictions and the Supreme Court has yet to make a ruling.

Additionally, in *Anti-Forensics: Techniques, Detection and Countermeasures,* Garfinkel covers stenography and generic data hiding. Stenography embeds encrypted data in a cover text to avoid detection. This technique is normally used to embed text in picture, video, and audio files. Garfinkel goes on to describe how generic data hiding hides data by using unallocated space or other locations that are ignored by the current forensic tools. Generic data hiding can also camouflage data by altering the file to avoid detection from forensic tools. These techniques can include altering extensions and headers. One such technique is called transmogrification. Transmogrification allows a user to mask a file to be seen and analyzed as a different file type. When the user wants to access the data, they unmask the file back to the original file type. Paul Henry, Vice President of Secure Computing, stated in 2011 that it was the first ever method able to defeat EnCase file signature capabilities. EnCase is a commercial forensic tools used by government and forensic investigators file signature capabilities (Henry, 2011).

2.4 Standards and Methodologies

Policymakers, security researchers, and industry groups have been creating standards, guides, methodologies, and frameworks for years. Open Web Application Security Project (OWASP),

a charitable group that provides unbiased, practical, and cost-effective information about security (OWASP, 2017), and SANS Institute, a cooperative research organization that provides intensive, immersion training and information for cybersecurity and information technology (SANS, 2017), both have printed many frameworks. The National Institute of Standards and Technology (NIST) created by the United States Commerce Department has some documentation and information about computer forensic tool testing on their website (NIST, 2015). The NIST site has some technical information for disk imaging, preparation, write blocking, file recovery, mobile forensics, and others, but there is no methodology or guideline for testing files that have been altered to be hidden. Further review revealed the site was last updated August 11, 2015, which at the time of this research makes it about 1 year 9 months out of date. With the fast changing world of technology, the NIST site has fallen behind.

Jim Lyle gave a presentation to the American Academy of Forensic Sciences titled Computer Forensic Tool Testing at NIST (Lyle, 2006). The presentation was made in February 2006, but has some valuable points that was incorporated into the making of the methodology for this research. Lyle stated that one of the requirements for software tools is that they must have their accuracy and reliability tested with repeatable results (Lyle, 2006). In the presentation, Lyle explained that for forensic testing one needs to develop test assertions. These test assertions should be a single testable statement with established conditions for the test. The test must end with measurable results. Once the conditions are decided, test cases need to be developed with a focus on specific test objectives. Lyle continues to talk about some of the test assertions and developments that NIST is working on, but does not mention any work being developed to test data hiding.

3 METHODOLOGY

This thesis focuses on four research objectives and hypotheses:

Research Objective 1 (RO-1): Develop and test a methodology for analyzing forensic tools' ability to detect nine different file types that have been modified by five data hiding techniques.

Research Hypothesis (RH-1): There exist vulnerabilities in forensic tools related to hidden data in altered files.

Research Objective 1 (RO-2): Determine which forensic tool or tools completed its automated analysis in the least amount of time.

Research Objective 1 (RO-3): Determine which forensic tool or tools completed its automated analysis with the least number of false positives and false negatives (errors).

Research Objective 1 (RO-4): Determine which forensic tool or tools find the most hidden files.

3.1 RO-1: Develop and Test Methodology

The purpose of this research was to develop a methodology to evaluate the robustness of forensic tools' ability to detect files that have been altered to avoid detection. After a review of existing academic resources, it was clear that a methodology to do so either does not exist, or is proprietary to a company and not available for public consumption. This could be due to the

extensive testing required to approve tools for use in legal matters. Also, this could be to keep any testing information from users who would attempt to exploit the vulnerabilities in the tools. As such, I have decided to create a methodology for testing forensic tools. I agree with Garfinkel and Kessler in that the golden age of digital forensics has ended, and now is the time for academia and industry to partner in research. The goal should be to improve upon forensic tools and practices and to defend against anti-forensics (Garfinkel, 2010; Kessler, 2007).

3.1.1 Developing the Methodology

A thorough search was completed to find information on a methodology for testing forensic tools. The sources I found were *Digital Forensic Evidence in the Courtroom: Understanding Content and Quality*, NIST (Lyle, 2006; NIST, 2015), and *Digital Forensics Tools: A Comparative Approach. Digital Forensic Evidence in the Courtroom: Understanding Content and Quality* discusses the case of *Daubert v. Merrell Dow Pharmaceuticals Inc.*, which created a standard that judges use to test the evidence submitted in a court of law. The case of *Daubert v. Merrell Dow Pharmaceuticals Inc.* made some valuable points that I wanted to integrate into the new methodology for data hiding. One key point is that the procedure can be independently tested and should be repeatable. This process should be able to be completed by a third unbiased party when necessary. This was also a point discussed and explained in the NIST presentation, stating that tools are required to have reliable and repeatable results (Lyle, 2006). The second key point was that the tool should include a known error rate or potential error rate. To ensure the repeatable feature as part of the documentation for the methodology to test forensic tools' ability to detect data hiding, the following information will be recorded: the forensic tool, the tool within the forensic tool used, and the version of the forensic tool. Statistics on percentage

error will be recorded in following results: True Positive, True Negative, False Positive and False Negative.

NIST also had a few points that help guide the development of the methodology. First, is that the test assertions should be a single testable statement. In the case of this methodology, the test assertion is "the file is detected." Secondly, the test needs measurable results. In this methodology, we are measuring the time to completion for analysis, false positive rate, false negative rate, and true positive rate. These measurements will be on a per run and per file basis. Test cases were built with these constraints in mind, and are discussed more in section 3.1.2 Choosing File Types and Creating File Types.

From the literature review, *Digital Forensics Tools: A Comparative Approach* explained how cyber forensics is becoming increasingly more important, especially due to advances in technology. Digital forensics is a key component to providing information stored on suspect's computers and can often identify the culprit responsible. A section of *Digital Forensics Tools: A Comparative Approach* focused on the testing of processes and frameworks for forensic tools. As per the literature, the digital forensic investigation process includes the following phases: preservation, collection, examination, analysis, and reporting phases. In comparison, the integrated digital forensic process model focuses on the preparation, incident, incident response, digital forensic investigation, and presentation phases. While these processes did not contribute directly with the creation of this methodology, their method of presenting results seemed very effective (Kamble & Jain, 2015):

Table 3.2 Comparison of considered tools on the basis of Digital Forensic Investigation Process

	Preservation	Collection	Examination	Analysis	Reporting
Award Key Logger	Yes	Yes	Yes	No	Yes
Recuva	Yes	Yes	No	Yes	Yes
USBDeview	Yes	Yes	No	No	No
WinHex	Yes	Yes	Yes	Yes	Yes
OpenPuff	No	No	Yes	No	Yes

Figure 1 - Image from Digital Forensic Tools: A Comparative Approach

Following the example from *Digital Forensics Tools: A Comparative Approach*, this methodology employs a similar process for displaying the research results:

Forensic Tool: [TITLE OF MAIN FORENSIC TOOL]

Technique Used: [TITLE OF TECHNIQUE USED IN FORENSIC TOOL]

Version: [VERSION]

	Set 0	Set 1	Set 2	Set 3	Set 4	Set 5
TestFile1.extension						
TestFile2.extension						
TestFile3.extension						
TestFile4.extension						
TestFile5.extension						
TestFile6.extension						
TestFile7.extension						
TestFile8.extension						
TestFile9.extension						

True Positive
False Negative
False Positive
True Negative

Figure 2 - Experimental Matrix for Testing Forensic Tools

Each set includes the tool, technique, and version at the top. The file types that are being tested are displayed on the far-left column, while the different anti-forensic techniques used are described in the top column. Further discussion on which file types and anti-forensic technics were selected can be found in section 3.1.2 and 3.1.1.

3.1.2 Choosing the File Types

This methodology requires a set of files to be created for testing validation. The selection of files types was based on information gathered from academic and public sources. *Law Enforcement Cyber Center* describes how digital search warrants are structured, and the requirements they need to follow. Search warrants must explicitly describe the place to be searched and the items to be seized. One approached to structuring search warrants includes beginning with a search description of "all records," and then limiting language is added. It is the limiting language that states the crime and will include an explicit example of the specific records to be seized (CENTER, n.d.). So, depending on the wording in the search warrant, a forensic investigator could be able to examine any file type. Allowing all file types is too expansive for the scope of this thesis and the methodology will limit accordingly.

While the courts have upheld that search warrants authorize a full search of a computer, meaning it authorizes the investigator at minimum a cursory review of all files, forensic investigators are normally looking for specific file types that have a high probability of containing evidential data (Welty, 2011). The type of evidence required for a case will depend on the type of crime being prosecuted. For example, internal documents would be valuable in a case involving corporate espionage. Executables and programs would be valuable in a case against malicious hackers, where the investigator is looking for specific behaviors and digital

signatures. Finally, in the case of child pornography images and videos files are important key evidence (Daniel, n.d.).

With the limitation of this methodology in mind, nine different file types have been selected. This file types include three picture file types: JPG File, PNG file, GIF file; 3 document file types: Microsoft Word Document, Adobe Acrobat Document, Microsoft Excel Spreadsheet; one video file type: MP4 File; one audio file file: MP3 File; and one executable file: Application File. These types were selected as they are the most common file types investigators attempt to analyze. To ensure effective analysis, files type includes two digital files used for testing.

Eighteen specific files were utilized. They are listed below:

- Action.mp3
- David.mp3
- Bear.png
- Secret.png
- Cheyenne_jpg.jpg
- Found.jpg
- Crews.gif
- LaDiDa.gif
- ExifPro.exe
- explorer.exe
- Ranch.mp4
- River.mp4
- Resume.pdf
- ASEE.pdf
- Sales.xlsx
- Student.xlsx
- Story.docx
- Submission.docx

Action.mp3 was originally named Komiku_-_17_-_Action_Fight.mp3 and downloaded from a free music archive. ("Free Music Archive," n.d.) David.mp3 was also downloaded from a free music archive and was originally named

music%2FccCommunity%2FTRG_Banks%2FInstrumentals%2FTRG_Banks_-_01_-_David_Hemmings.mp3 ("Free Music Archive," n.d.) Bear.png was a file downloaded from a free image sharing site ("pngimg.com," n.d.). Secret.png, Found.jpg, and LaDiDa.gif were all created using MS Paint. Cheyenne_jpg.jpg is the image of a friend's horse taken with a digital camera. Crews.gif was downloaded from a free GIF website ("Giphy," n.d.). ExifPro.exe is a free image browser application ("EXIFPro," 2011). Explorer.exe is a standard application file that comes with a Windows operation system. Ranch.mp4 is a video advertising a friend's ranch. River.mp4 is a free stock video title "View of River From Boat" ("View Of River From Boat," n.d.). Resume.pdf is an old copy of my resume and ASEE.pdf was originally Practical_Data_Mining_and_Analysis_for_System_Administration_-_submitted.pdf and was the pdf downloaded from the American Society of Engineering Education. Sales.xlsx and Student.xlsx were two different excel document templates that were saved. Story.docx is a personal word document and submission.docx is another personal word document that is the word document copy of a paper submission.

3.1.3 Creating the Test Files

The goal of this research is to test the robustness of forensic tools ability to detect anti-forensic data hiding techniques. With the nine file types and eighteen actual files chosen for testing in section 3.1.2, copies of the files need to be altered by each of the anti-forensic methods that are being tested against. For performance of the testing phase, the files were altered and separated into six different groups:

Set 0 (Control Group) - Original files without any changes.

Set 1 (Extension Change) – Each file has just the extension of the file altered. For example, extensions have been changed to be .dll instead of .doc, with the file type .dll denoting a Dynamic-link library. Generally, a Windows operating system will have many .dll files, and .dll is a file type that a forensic analysist typically won't consider. As such, extensions have been changed to .dll for this research.

Set 2 (Extension Removed) - This technique attempts to hide the file by removing the extension altogether.

Set 3 (Encryption) – This method uses an algorithm to alter the file and protects its content with an encryption key (password, biometrics, etc.). Effectively, this method secures the file; the file is easily flagged as encrypted by most forensic tools due to its level of entropy. In most cases, encryption will attract unwanted attention (Garfinkel, 2007). The encryption on the files is enacted by the same user used for forensic analysis. So the encryption will not impact the file since it will be decrypted by Windows upon access.

Set 4 (Transmogrification) - Transmogrification is the process by which both the header and the extension of the file are changed to a different file type. The file type's header and extension will both be changed to .dll for the same reasons as changing the extension alone. For this research, we used the hexadecimal editor, HxD. HxD is free software that allows for the editing of files at the hexadecimal level (Horz, 2017). To change a file specifically to a .dll file the first four bytes were overwritten to be 4D 5A also known as MZ. This is the header for Windows/DOS executable files (Bruneau, n.d.; Kessler, 2017).

Set 5 (Cloaking Technique) - This is a new method that was developed for this thesis. It is based on a substitution cipher. Substitution ciphers are a form of weak encryption that are relatively

easy to reverse, but can require a significant amount of time from an investigator (Casey, 2002). Simple encryption schemes generally appeal less to people, but could potentially avoid detection from forensic tools due to the simple encryption not altering the entropy of the file. The cloaking method removes the extension of the file and alters the first part of the file (32 hexadecimal bytes) to scramble the header and make it unrecognizable. The hex editor, HxD was used as it was for Transmogrification. Instead of overwriting the first four bytes to a specific set, the first 32 bytes were overwritten and increased it by one. For example, a hex 2 would become a 3, a hex 9 become an A, and an F will overflow and become 0.

3.1.4 Choosing Forensic Tools to Test

Validation of the newly developed methodology was completed by testing against two forensic tools: X-Ways and Autopsy/SleuthKit. The two tools chosen are commonly used by law enforcement, military, corporate, and industry professionals. In order to get a good sampling of forensic tools, one is a commercial tool and one is an open source licensed tool.

X-Ways Forensics Version 17.5**:** X-Ways Forensics is an integrated computer forensic software used by forensic examiners ("X-Ways Forensics: Integrated Computer Forensics Software," 2016). The X-Ways Forensics platform is the flagship offering of X-ways, and runs on multiple version of Windows. For this research, two of the featured techniques available within the X-Ways Forensics software platform were tested: File Type Filter; and Specialist Tools: File Header Signature and Verify File Type.

Autopsy 4.0.0: Autopsy is an open source digital forensics platform with a graphical interface. It is used by law enforcement, military, and corporate examiners to investigate computers (Sleuthkit, 2016). For this research, four of the techniques available within the Autopsy forensic

platform were used: Views – By Extension; Views – By MIME Type; View Images/Videos; and Extension Mismatch Detected.

3.1.5 Evaluation Process

For the evaluation process, a computer and a storage device are necessary. A computer is needed to run the forensic software, and a storage device will be used to contain the file sets to be tested. To complete this methodology, testing will be performed on an Alienware Laptop running a Windows 10 64-bit operating system. The laptop has an Intel Core i7-6700HQ processor running 2.60GHz with 32.0 GB of RAM. This laptop was selected because its specifications are within the requirements for running the chosen forensic tools. Also, this laptop is one of the laptops issued to BYU's security analysts, and is used to perform forensic analysis.

A Lexar JumpDrive S77 was the storage device used in the research. This is a 64 GB USB 3.0 Flash Drive. To reduce variables and to create a controlled environment, the Lexar flash drive was new. It was formatted by the computer used for the forensic analysis. Test files were copied over once the drive was formatted. The evaluation and validation process of the methodology were accomplished by following the outline in "The Methodology", Chapter 4.

3.2 Determinations

Once the methodology is completed for a forensic tool, several factors help determining which tools meet a user's requirements. This methodology records the time to complete the analysis, number of true positives, number of true negatives, number of false negatives, and number of false positives. There are, for some tests, file sets that may not be applicable depending on the analysis technique used and they will be marked as true negative since they are

not expected to appear in the results. All this information is collected to complete the research hypothesis and research objectives.

3.2.1 RO-2: Determine the Fastest Forensic Tools

As part of the methodology, the time the tool takes to complete the analysis will be recorded. This will allow for comparison between the tools. If a tool has an internal clock, then it will be used to calculate the time to completion. Without an internal clock, a stopwatch will be used to measure the time to completion.

3.2.2 RO-3: Determine the Forensic Tool with Least Errors

To determine which forensic tool has the least amount of errors, the number of errors will be recorded. For this research, an error constitutes a result that is either a false positive or a false negative. The following formulas will be used to calculate the number of errors and the percentage error:

NUMBER OF ERRORS: [NUMBER OF FALSE POSITVES + NUMBER OF FALSE NEGATIVES]

PERCENTAGE ERROR:

$$\%\text{Error} = \frac{(\text{Number of False Negatives} + \text{Number of False Positives})}{(\text{Number of Files Tested X Number of Sets Tested (6)} - (\text{Number of True Negative})} X\ 100$$

Figure 3 - Errors Formulas

3.2.3 RO-4: Determine the Forensic Tool that Discovers the Most

To determine which forensic tool has the highest detection rate of hidden files, the number will be recorded. For this research, detection constitutes a true positive that a hidden file was discovered and categorized correctly. The following formulas will be used to calculate the number of files detected and the percentage correct:

NUMBER OF FILES DETECTED: [NUMBER OF TRUE POSITIVES]

PERCENTAGE Correct:

$$\%\text{Correct} = \frac{(\text{Number of True Positives})}{(\text{Number of Files Tested X Number of Sets Tested } (6)) - (\text{Number of True Negative})} X\ 100$$

Figure 4 - Formulas for Percentage Correct

4 VALIDATION AND EXPERIMENTAL FRAMEWORK

The following is a methodology to test the robustness of forensic tools' ability to detect data hiding. As discussed in the "Methodology," Chapter 3, the following methodology was created with the aid of related standards and methodologies. The legal requirements judges enforce and evaluate to allow digital evidence into the courtroom was reviewed and taken into consideration with the developing of this framework. Similar methodologies built by NIST were also reviewed to best compare to current standards. How the comparative results were displayed in *Digital Forensics Tools: A Comparative Approach* was also reviewed in the process of its development (Garrie & Morrissy, 2014; Kamble & Jain, 2015; NIST, 2015). The methodology has also been reviewed by eight information technology and security professionals and their feedback and advice has been incorporated into the final version; more about this in the next section.

4.1 Reviewer and Testing Generated Change

After completing development of the methodology, it was sent out for review by eight different information technology and security professionals. The selected professional were chosen from a variety of backgrounds and experience to provide a broad analysis. Four of these professional are more experienced. They have been working in the field of cybersecurity for over 10 years and have had experience with investigations. One of these four had completed the SANS Forensics course. Another selected professional received his training elsewhere, but also

has testified in court as an expert witness relating to forensic investigations he's performed. One is medium experienced. Constantly exposed to cybersecurity and having worked in the field of information technology for over five years. His primary job is programming and creating test cases to test programs and features capabilities. Three of the selected professionals are more novice. Having been working in cybersecurity in five years or less. These selected professionals work in cybersecurity, and have been exposed to forensics with their education, but have not been exposed to forensics or investigations with their current work experience.

These professionals were invited to make comments and edits to improve the methodology. The reviewers agreed that the methodology was conceptually sound, but several points needed improvement. Flow and syntax were the beginning points of improvement. Past those changes, comments were more specific. Based on the reviewers' feedback, the methodology was updated to warn users that while the big picture ideas are core points usable in any operating system or with any editing tool, the specific steps of the testing are specific to Windows and the HxD hexadecimal editor. Reviewers comments also helped clarify the specific language used to make it more exact in the explanations and directions. For example, while the initial draft used the term "file", the more exact term was "file name". These information technology and security professionals provided valuable feedback that helped the methodology have more clarity and exactness in the language and their aid was extremely helpful in completing a well thought out and professional final draft of this methodology.

After the methodology was reviewed by the professionals, the next phase of building out the methodology was to start testing. Testing the methodology generated some points of change after initial testing, that when consulting the reviewers, they agreed were helpful additions. The first change was the addition of a Notes and a Computer Specifications section. A note section

allows the reviewer to make any notes or comments for themselves of anyone who will be reviewing the reports to try to clarify decisions. This section is helpful for remarking of specific options one uses such as when searching for specific files types. Computer Specifications helps a reviewer give a more accurate rating for the forensic techniques. By giving the specifications of the machines themselves, hardware and versioning discrepancies can be taken into account, especially when the test results may widely vary. Usability also became a category that proved to be relevant. Reviewers are requested to rate the difficulty of use of a tool from 1, representing difficult to use, to 5, representing straightforward to use. This will give new forensic investigators an idea the level of experience or time required to become familiar with certain forensic techniques in tools.

4.2 The Methodology

This methodology was designed to test a forensic tool's capability to detect files that have been altered by data hiding techniques. The steps have been written to be understandable to a broad audience, but for the best comprehension a basic technical knowledge and understanding of security is preferred. Some steps will require more time to complete than others. The methodology has been built with flexibility and scalability considered so it is best to approach this methodology with an understanding of your situation and forensic needs.

The specific step by step instructions are for Windows Operating Systems; however, the main tasks explained can be used for any Operating System.

1. Determine File Types
    a. There are many different file types that can be relevant to what you are searching for. Determine which files types you want to test. You can test image files (jpg,

png, gif, etc.), documents (docx, xlsx, etc.) or any other file type you wish. The first step is determining a list of files types that you feel will be relevant and that you want to test against.

2. Find and/or Create Files
    a. Once you have determined what file types you want to test for, it is necessary to download or create files of that type. For example, MS Paint could be used to create image files, or images could be downloaded for free online.
3. Alter the Files with Anti-Forensic Data Hiding Techniques
    a. It is recommended that you organize these files in separate folders and/or label the files in a way that will aid in recognizing which files have been discovered by the forensic tool. A sample schema could be: <FILETYPE><SET#>.<EXTENSION>.
    b. Remove the metadata from each file.
        i. Hover your mouse over the file and right-click, showing a menu.
        ii. Click “Properties”.
        iii. In the Details Tab at the top, click on “Remove Properties and Personal Information” at the bottom.
        iv. Click the radio button for “Remove the following properties from this file”.
        v. Click the “Select All” button.
        vi. Click OK.
    c. Set 0: The Control Group
        i. These files do not need to be altered as they are your control group.

d. Set 1: Extension Change

    i. Hover your mouse over the file and right-click, showing a menu.

    ii. Hover the mouse over “Rename” and click it.

    iii. The file name becomes a text box. Remove the extension of the file and enter a new one. For example, remove “jpg” and enter “dll”. Hit enter, and click “Yes” to accept the change.

    iv. The file is now changed to a different extension.

e. Set 2: Extension Removal

    i. Hover your mouse over the file and right-click, showing a menu.

    ii. Click “Rename”.

    iii. The file name becomes a text box. Remove the extension of the file, including the period before the extension. For example, remove “.jpg”. Hit enter, and click “Yes” to accept the change.

    iv. The filename is now changed.

f. Set 3: Encryption

    i. Hover your mouse over the file and right-click, creating a menu.

    ii. Hover the mouse over “Properties” and click it.

    iii. In the General Tab at the top, click on the “Advanced” Button next to Attributes.

    iv. An Advanced Attributes window will open. Check the box for “Encrypt contents to secure data”. Click OK.

    v. Click Apply.

    vi. Select “Encrypt the file only” and click OK.

vii. A lock will appear on the file showing the file is encrypted.

g. Set 4: Transmogrification

i. The first step of Transmogrification is to change the file extension to the extension you desire. Please refer to "Extension Change" above to perform those steps.

Note: To finish the rest of the set you will need a hexadecimal editor. There are a variety to tools that can complete this task. If you don't know where to start, HxD is a good option of an open source tool that has good usability.

ii. Open the file in a hexadecimal editor.

iii. Overwrite the first 4 bytes so that they become 4D 5A.

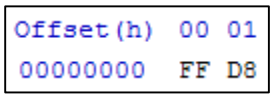


Figure 5 – Transmogrification: Initial Header

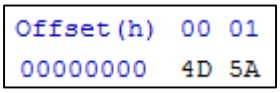


Figure 6 - Transmogrification: Changed Header

iv. Save the file.

v. Delete the .bak file.

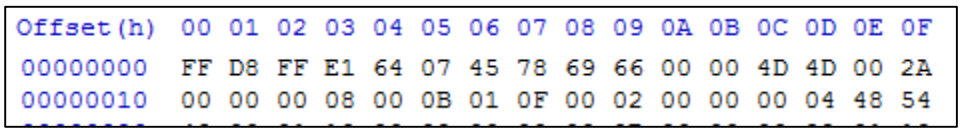
h. Set 5: Cloaking

i. The first step of Cloaking is to remove the file extension. Please refer to "Extension Removal" above to perform those steps.

Note: To finish the rest of the set you will need a hexadecimal editor. There are a variety to tools that can complete this task. If you don't know where to start, HxD is a good option of an open source tool that has good usability.

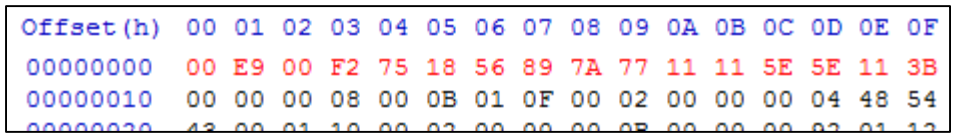
ii. Open the file in a hexadecimal editor.

iii. Overwrite the first 32 bytes, increasing each byte by 1.



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000000	FF	D8	FF	E1	64	07	45	78	69	66	00	00	4D	4D	00	2A
00000010	00	00	00	08	00	0B	01	0F	00	02	00	00	00	04	48	54

Figure 7 - Cloaking: Initial Header



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000000	00	E9	00	F2	75	18	56	89	7A	77	11	11	5E	5E	11	3B
00000010	00	00	00	08	00	0B	01	0F	00	02	00	00	00	04	48	54

Figure 8 - Cloaking: Changed Header

iv. Save the file.

v. Delete the .bak file

4. Prepare the Storage Drive

   a. Format the storage drive that will be used for forensic analysis. Copy the set of test files over once the drive is formatted in preparation for testing.

5. Evaluation of Forensic Tool

   a. Perform the analysis technique you want to test and record the results below.

   b. Repeat for each of the forensic tools you want to review and compare the results.

FORENSIC TOOL: [TITLE OF MAIN FORENSIC TOOL]

TECHNIQUE USED: [TITLE OF TECHNIQUE USED IN FORENSIC TOOL]

VERSION: [VERSION]

	Set 0	Set 1	Set 2	Set 3	Set 4	Set 5
TestFile1.extension						
TestFile2.extension						
TestFile3.extension						
TestFile4.extension						
TestFile5.extension						
TestFile6.extension						
TestFile7.extension						
TestFile8.extension						
TestFile9.extension						

True Positive
False Negative
False Positive
True Negative

TIME: [TIME THE TOOL SPENT TO COMPLETE ANALYSIS]

TOTAL NUMBER OF FILES EXAMINED:

NUMBER OF ERRORS: [NUMBER OF FALSE POSITVES + NUMBER OF FALSE NEGATIVES]

PERCENTAGE ERROR:

$$\%\text{Error} = \frac{(\text{Number of False Negatives} + \text{Number of False Positives})}{(\text{Number of Files Tested X Number of Sets Tested } (6)) - (\text{Number of True Negative})} X\ 100$$

NUMBER OF FILES DETECTED: [NUMBER OF TRUE POSITIVES]

PERCENTAGE CORRECT:

$$\%\text{Correct} = \frac{(\text{Number of True Positives})}{(\text{Number of Files Tested X Number of Sets Tested } (6)) - (\text{Number of True Negative})} X\ 100$$

USABILITY [Rate from 1 (difficult to use) to 5 (straightforward to use)]:

NOTES:

COMPUTER SPECEFICATIONS:

Operation System:

Processor:

RAM:

Figure 9 - Full Experimental Matrix for Testing Forensic Tools

4.3 Flexibility and Scalability

Technology is rapidly developing and moving forward. Cybersecurity has become an essential part of technology, as has been highlighted by current events and the media. Digital forensics as a study and practice has the possibilities to continue to expand as researchers and developers design new solutions for forensic oriented tasks. Anti-forensics will continue to be a growing discipline as new vulnerabilities are discovered and weaknesses are exploited to weaken investigations and destroy evidence. Due to the nature of these topics, the methodology developed in this thesis has been designed and planned to allow for flexibility and scalability as new techniques, methods, and technologies change the forensic environment.

Flexibility was designed in the methodology by allowing the reviewer to choose what files need to be tested. Generally, forensic tools are used to look for evidence, which could include documents, pictures, videos, or in some cases may involve specific files types that could need to be discovered upon investigation. The final methodology includes five different anti-forensic techniques of data hiding: 1) Extension Change; 2) Extension Removal; 3) Encryption; 4) Transmogrification; 5) Cloaking. As new anti-forensic techniques are developed, it is simple to add to the methodology's steps directions on completing the new technique to expand and accept it into the testing process and matrix. This provides practical scalability to the methodology as new advances are made and vulnerabilities are discovered in the future.

5 EVALUATION OF FORENSIC TOOLS

To determine the effectiveness of the methodology for testing the robustness of forensic tool's ability to detect data hiding, two forensic tools were selected as described in section 3.1.4. Each tool's variety of different analysis methods was used and evaluated using the new methodology defined in this research. The different techniques of analysis in each tool were subject to all the files created in the methodology and were recorded separately on their own matrix to accurately display the results.

5.1 Limitations

It should be acknowledged that there are limitations to this study. One limitation is the defined scope of the thesis. While the scope was reasonable for testing the validity of the completed methodology, it is limited in its ability to render an overall judgement of the forensic tools tested. Ideally, many different types of files would be tested beyond the nine selected and more than two of each file type would be tested to best determine the tool that completed its analysis in the least amount of time, with the least amount of errors, and the most detected files.

The environment in which the testing took place has limitations. A USB flash drive was used as the storage drive for testing. This is just one medium where files are stored and reviewed for cases. Often forensic investigators are required to search through hard drives and flash drives with more storage capacity and with a variety of more files that the investigator would need to

process whether it has relevance or not to their investigations. For the testing of this methodology, a more controlled environment was deemed appropriate: the USB flash drive. It should be noted that while this testing does well to test against data hiding techniques, it does limit the testing and analysis of the practical use of the forensic tools.

Human error, as always, must also be accounted for. A stopwatch was used to evaluate the time a forensic tool takes to process the storage device. To limit error, the same researcher was used to evaluate each tool, so the response time in each start and stop of the stopwatch should be similar enough, making the error negligible for the requirements of this research. There are some limitations and scope requirements that were qualified for specific tools and features and will be explained under that specific tool.

5.2 Autopsy/Sleuth

Autopsy is a free digital forensics platform with the graphical interface to Sleuth Kit. Law enforcement, military, and corporate forensic investigators use Autopsy to investigate computers and storage devices (Sleuthkit, 2016). For this research, four of the tools available within Autopsy's forensic platform were relevant and tested: 1) Views – By Extensions; 2) Views – By MIME Type; 3) View Images/Videos; 4) Extension Mismatch Detected.

The following steps were followed to enable Autopsy to process the USB flash drive for analysis and will guide you through the process:

1. Create a New Case in Autopsy. The wizard walkthrough will guide you on what information you need to enter.
2. Click "Add Data Source" with the large green + symbol at the top left of the Autopsy window.

3. For a USB select Local Disk as the data source type. Select the USB flash drive you want to examine from the dropdown options. Leave the checkbox "Ignore orphan files in FAT file systems" unchecked. Click "Next."
4. Select all Ingest Modules. Make sure the Process Unallocated Space checkbox is left checked. Click "Next."
5. It will begin processing the data source and adding it to a local database for analysis.
6. One or more Ingest Modules may fail. If this happens, review the error information available through Autopsy help pages to correct the issue. Often the module may not be needed. For example, if Virtual Machine Extractor fails, but there are no virtual machines to extract then this is not a needed module.

Once the flash drive was processed it was left plugged into the computer and the three different forensic techniques were reviewed.

5.2.1 Views – By Extension

Viewing the files by extension allows an investigator to quickly review each of the files sorted by type. This technique reviewed the 108 files and detected 32 files and missed 76. The percentage of files detected by this technique was 29.36%, missing 70.37% of the files. The only file types that this technique discovered was the control group, set 0, and the encrypted files, set 3. However, this technique missed the GIF file for every single set. Autopsy's method to View - By Extension was straightforward to use. In usability, the technique was given a 5 since it contained very few steps and was very intuitive to use.

The following steps were performed to complete this method:

1. In Autopsy's main window the left pane will reveal many different options. Select "Views."
2. More options should have appeared. Select "File Types."
3. Again, sub-options should have appeared. Select "By Extension".
4. You can now view how the files appeared through Extension analysis by Image, Video, Audio, Archives, Documents and Executable.
5. Review these options and mark the matrix according to how they appeared.

FORENSIC TOOL: **Autopsy**
VERSION: **4.3.0**
TECHNIQUE USED: **Views – By Extension**

	Set 0	Set 1	Set 2	Set 3	Set 4	Set 5
Action.mp3						
David.mp3						
Bear.png						
Secret.png						
Cheyenne_jpg.jpg						
Found.jpg						
Crews.gif						
LaDiDa.gif						
ExifPro.exe						
Explorer.exe						
Ranch.mp4						
River.mp4						
Resume.pdf						
ASEE.pdf						
Sales.xlsx						
Student.xlsx						
Story.docx						
Submission.docx						

True Positive
False Negative
False Positive
True Negative

TIME: **7 minutes 3.52 seconds**
TOTAL NUMBER OF FILES EXAIMED: **108**
NUMBER OF ERRORS: **76**
PERCENTAGE ERROR: **70.37%**
NUMBER OF FILES DETECTED: **32**
PERCENTAGE CORRECT: **29.63%**
USABILITY [Rate from 1 (difficult to use) to 5 (straightforward to use)]: **5**

Figure 10 - Autopsy Matrix: Views - By Extension

5.2.2 Views – By MIME Type

Since extensions of files can be easily manipulated, viewing the files by MIME Type goes beyond just the extensions. Determining the MIME type allows an investigator to analyze what each file type is through internal formatting and code. MIME or Multipurpose Internet Mail Extensions is a way of identifying files according to their nature and format ("MIME-TYPE.net," 2009). This technique reviewed the 108 files, detected 57 files and missed 51 files. The percentage of files detected by this technique was 52.78% correctly detecting just over the majority of files discovered and recognized with this technique. 47.22% of the files were still missed. Set 3, encryption was the only group of files that did not have a single file detected.

This technique has some limitations with the scope. Viewing the files by MIME has 14 different modules that an investigator can use to review files. Eleven of these modules were used with no changes, one was used with stipulations, one was used but may be only required for unusual cases, and one was not used. The one that wasn't used was Octet-stream. Octet-stream is a binary file and one of the most popular multipurpose application files. This type of file is generally used for identifying the data that is not associated with any specific application ("MIME-TYPE.net," 2009). In this test environment there were 107 different incidents, implying that in a less controlled situation, such as an actual court case, this technique would not be very practical due to the wide range of file types that it accepts. Vnd.microsoft.icon seems to be a special type of image file that may require encoding on transports not capable of handling binary ("Media Type 'image/vnd.microsoft.icon' Details," 2003). For this research we didn't have any, so there were no false positives and this category didn't detract or take away from the end results.

The x-msdownload module has stipulations placed on it. X-msdownload is generally used to figure out all of the executable and the system files associated with Windows Operating System platforms. The popular file extension .exe is associated with this particular MIME type ("MIME-TYPE.net," 2009). With the extension type being .exe and with .dll being related to .exe, any changed extensions types will be found in this folder. In this test environment there were 42 different incidents, so in a real case this technique is not very practical due to the wide range of acceptable file types. Considering part of this research included reviewing and detecting executable files, the results in this module were used to review executable files (.exe), but any file that was labeled as a dynamic-link library (.dll) was ignored.

Autopsy's method to View - By MIME Type was a straightforward and simple to use technique. The reviewer gave the technique a 5 for usability since it contained very few and simple steps, making it intuitive to use. The following steps were performed to use Views – By MIME Type:

1. In Autopsy's main window the left pane will reveal many different options. Select "Views."
2. More options should have appeared. Select "File Types."
3. Again, sub-options should have appeared. Select "By MIME Type".
4. You can now view how the files appeared through MIME type separated out by application, audio, image, and video.
5. Review these options and mark the matrix according to how they appeared.

FORENSIC TOOL: **Autopsy**
VERSION: **4.3.0**
TECHNIQUE USED: **Views - By MIME Type**

	Set 0	Set 1	Set 2	Set 3	Set 4	Set 5
Action.mp3	TP	TP	TP	FN	FN	FN
David.mp3	TP	TP	TP	FN	FN	FN
Bear.png	TP	TP	TP	FN	FN	FN
Secret.png	TP	TP	TP	FN	FN	FN
Cheyenne_jpg.jpg	TP	TP	TP	FN	FN	FN
Found.jpg	TP	TP	TP	FN	TP	TP
Crews.gif	TP	TP	TP	FN	FN	FN
LaDiDa.gif	TP	TP	TP	FN	FN	FN
ExifPro.exe	TP	FN	TP	FN	FN	FN
Explorer.exe	TP	FN	TP	FN	FN	TP
Ranch.mp4	TP	TP	TP	FN	TP	FN
River.mp4	TP	TP	TP	FN	TP	FN
Resume.pdf	TP	TP	TP	FN	FN	FN
ASEE.pdf	TP	TP	TP	FN	FN	FN
Sales.xlsx	TP	TP	TP	FN	FN	FN
Student.xlsx	TP	TP	TP	FN	FN	FN
Story.docx	TP	TP	TP	FN	FN	FN
Submission.docx	TP	TP	TP	FN	FN	FN

True Positive
False Negative
False Positive
True Negative

TIME: **7 minutes 3.52 seconds**
TOTAL NUMBER OF FILES EXAIMED: **108**
NUMBER OF ERRORS: **51**
PERCENTAGE ERROR: **47.22%**
OF FILES DETECTED: **57**
PERCENTAGE CORRECT: **52.78%**
USABILITY [Rate from 1 (difficult to use) to 5 (straightforward to use)]: **5**

Figure 11 - Autopsy Matrix: Views - By MIME Type

5.2.3 View Images/Videos

Many investigation focus on images and videos for critical evidence such as child pornography cases. To aid with this need, Autopsy has built into the tool a feature to help review these files. The View Images/Videos option enables an investigator to quickly review pictures and videos that Autopsy has been able to identify. This technique was responsible for reviewing 48 files. The remaining 60 files were expected to be True Negatives since they are not image or

video files. If any did appear, then the result would have been a false positive, but for this test every non-image and non-video file was not detected by this technique. View Images/Videos should have detected the six anti-forensic altered versions of the following eight files: Bear.png, Secret.png, Cheyenne_jpg.jpg, Found.jpg, Crews.gif, LaDiDa.gif, Ranch.mp4, and River.mp4. Of the total 48 files that this technique relates to, 28 files were detected, 20 files were left undetected. The percentage of files detected by this technique was 58.33%, missing 41.67% of the files. Set 3, the encrypted set of files, did not have a single file appear on discovery. However, as stated, there were multiple file types that were true negatives for this technique because it requires the file type to be either an image or a video.

Autopsy's method to View Images/Videos was intuitive to use. This technique was clearly labeled at the top of the window options as a button to help guide the forensic investigator or analysis to its use. The reviewer gave the technique a 5 for usability for these reasons. Without any prior knowledge of the technique, the reviewer understood what the technique appeared to be for, and was able to apply it with no hesitation. It was very natural to select this option and the graphical interface provided to view the files was clear and concise. The following steps were performed to complete this method:

1. Click "View Images/Videos" with the Blue Photo symbol at the top left of the Autopsy window. A new window will appear labeled in the tab "Image/Video Gallery".
2. In the left pane of the new window folders will appear. Click through the folders and review what images and videos appear and mark the matrix accordingly.

FORENSIC TOOL: **Autopsy**
VERSION: **4.3.0**
TECHNIQUE USED: **View Images/Videos**

	Set 0	Set 1	Set 2	Set 3	Set 4	Set 5
Action.mp3	TN	TN	TN	TN	TN	TN
David.mp3	TN	TN	TN	TN	TN	TN
Bear.png	TP	TP	TP	FN	FN	FN
Secret.png	TP	TP	TP	FN	FN	FN
Cheyenne_jpg.jpg	TP	TP	TP	FN	FN	FN
Found.jpg	TP	TP	TP	FN	TP	TP
Crews.gif	TP	TP	TP	FN	FN	FN
LaDiDa.gif	TP	TP	TP	FN	FN	FN
ExifPro.exe	TN	TN	TN	TN	TN	TN
Explorer.exe	TN	TN	TN	TN	TN	TN
Ranch.mp4	TP	TP	TP	FN	TP	FN
River.mp4	TP	TP	TP	FN	TP	FN
Resume.pdf	TN	TN	TN	TN	TN	TN
ASEE.pdf	TN	TN	TN	TN	TN	TN
Sales.xlsx	TN	TN	TN	TN	TN	TN
Student.xlsx	TN	TN	TN	TN	TN	TN
Story.docx	TN	TN	TN	TN	TN	TN
Submission.docx	TN	TN	TN	TN	TN	TN

True Positive
False Negative
False Positive
True Negative

TIME: **7 minutes 3.52 seconds**
TOTAL NUMBER OF FILES EXAIMED: **48**
NUMBER OF ERRORS: **20**
PERCENTAGE ERROR: **41.67%**
NUMBER OF FILES DETECTED: **28**
PERCENTAGE CORRECT: **58.33%**
USABILITY [Rate from 1 (difficult to use) to 5 (straightforward to use)]: **5**

Figure 12 - Autopsy Matrix: View Images/Videos

5.2.4 Extension Mismatch Detected

One anti-forensic technique that is very basic and easily completed is changing the file extension. This anti-forensic technique has been in practice for years, and to help combat this anti-forensic method Autopsy included a forensic technique specifically to identify these file types. The Extension Mismatch Detected module enables an investigator to quickly review files that Autopsy has been able to identify as an extension that does not match the file type. This

technique was responsible for reviewing 108 files and detected only five files. One hundred and three files were left undetected. The percentage of files detected by this technique was 4.63% and the percentage missed was 95.37% of the files. Set 1, Extension Changed, was the only set to have any files discovered.

Autopsy's method of Extension Mismatch Detected was not initially intuitive. This technique was fairly hidden and took a while to discover since instead of having an easily accessible button on the toolbar to use it was feature under the top menu Tools. Beyond that, an investigator would also have to know to run the Ingest Modules to be able to test use the Extension Mismatch Detector technique. Usability rating for this technique received a 4 from the reviewer since it was easy to use, but without any prior knowledge this option would not have been intuitive to find or utilize. A new user might not have discovered this technique because it is not a very natural process to select this option, and there is no graphical interface provided as there is for the other options in Autopsy. The following steps were performed to complete this method:

At the top menu options select under Tools, Run Ingest Modules:

1. Your USB Flash dive should be an option under this. Click on it.
2. Check Extension Mismatch Detector. Click "Start."
3. The findings should be saved under Results -> Extracted Content -> Extension Mismatch Detected.

Review these options and mark the matrix according to how they appeared.

FORENSIC TOOL: **Autopsy**
VERSION: **4.3.0**
TECHNIQUE USED: **Extension Mismatch Detected**

	Set 0	Set 1	Set 2	Set 3	Set 4	Set 5
Action.mp3						
David.mp3						
Bear.png						
Secret.png						
Cheyenne_jpg.jpg						
Found.jpg						
Crews.gif						
LaDiDa.gif						
ExifPro.exe						
Explorer.exe						
Ranch.mp4						
River.mp4						
Resume.pdf						
ASEE.pdf						
Sales.xlsx						
Student.xlsx						
Story.docx						
Submission.docx						

True Positive
False Negative
False Positive
True Negative

TIME: **7 minutes 3.52 seconds (+ 24.33 seconds for a scan to complete Extension Mismatch technique)**
TOTAL NUMBER OF FILES EXAIMED: **108**
NUMBER OF ERRORS: **103**
PERCENTAGE ERROR: **95.37%**
NUMBER OF FILES DETECTED: **5**
PERCENTAGE CORRECT: **4.63%**
USABILITY [Rate from 1 (difficult to use) to 5 (straightforward to use)]: **4**

Figure 13 - Autopsy Matrix: Extension Mismatch Detected

5.2.5 Overall

Forensic investigators will not just use on technique, but use every technique and method available in their forensic tool they have to use. The final matrix for a forensic tool, such as Autopsy, is a combination of all techniques that a forensic investigator may use. Autopsy's overall score combines the four matrixes used in the prior testing: Views – By Extension, Views – By MIME Type, View Images/Videos, Extension Mismatch Detected. Using all four of these

techniques, the number of files examined was 108. Seventy-three of those files were detected, leaving 35 files missed. The overall percentage detected by Autopsy was 67.59%. Autopsy missed 32.41% of the files with the majority of those being from Set 4, transmogrification, or Set 5 cloaking. Overall, Autopsy was intuitive and easy to use with four different forensic techniques easy to use earning it the usability rating of 4.75.

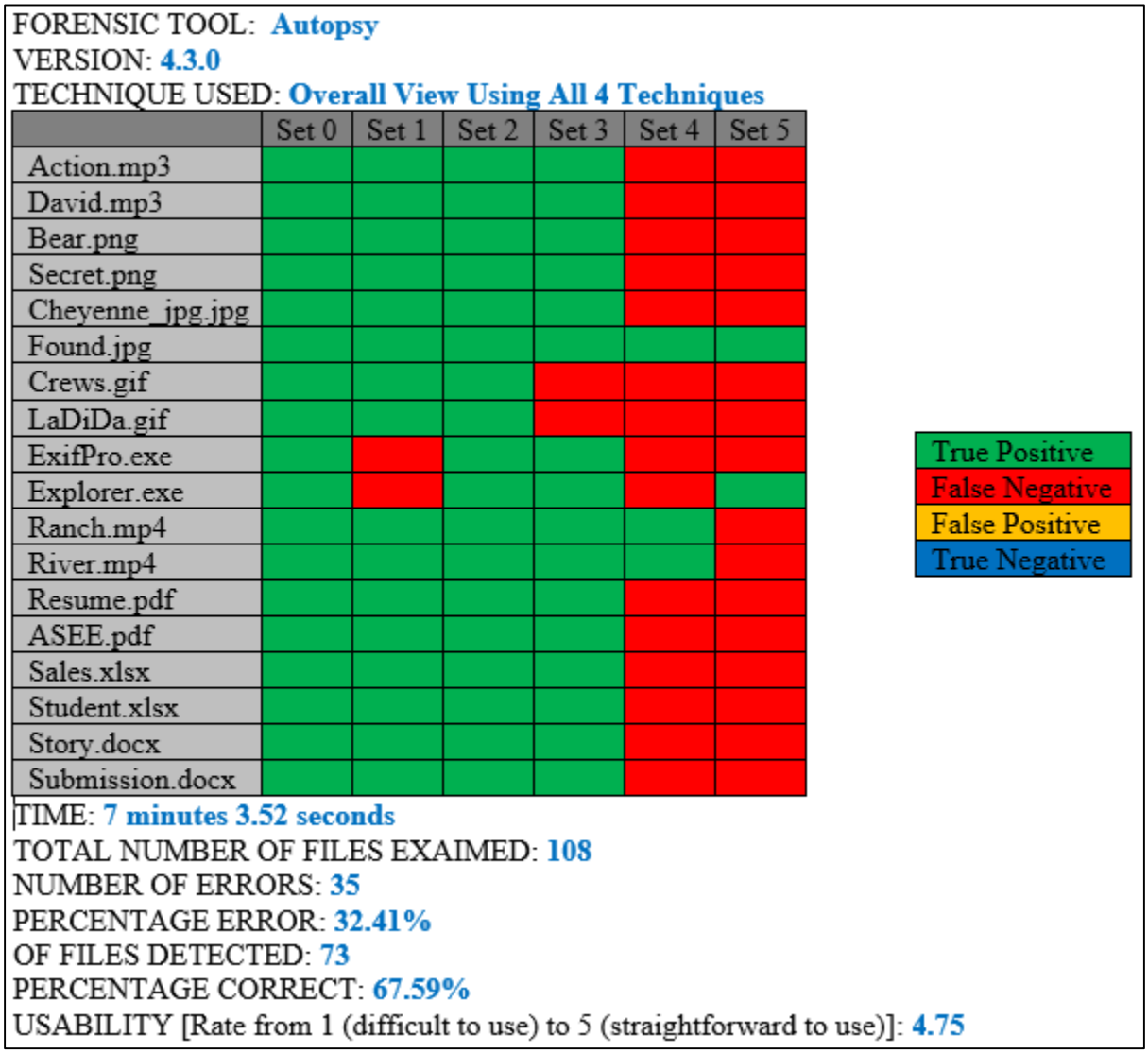


Figure 14 - Autopsy Matrix: Overall View Using All 4 Techniques

5.3 X-Ways Forensics

X-Ways Forensics is the flagship product of X-Ways and provides integrated computer forensic software for forensic investigators in governments, research, and industry internationally. Their forensic software is built to run on multiple Windows platforms and is based on WinHex and disk editor, with a planned workflow model to make it efficient for forensic investigators to share data and collaborate on cases ("X-Ways Forensics: Integrated Computer Forensics Software," 2016). For this research, two of the tools available within the platform were designed to search and analyze data discovered from USB flash drives: 1) File Type Filter; 2) Specialist Tools: File Header Signature and Verify File Types.

The following steps were followed to enable X-Ways to process the USB flash drive with the test files for analysis:

1. To start investigating the USB Flash Drive, click "File" in the navigation pane labeled "Case Data". Enter in the Case title/number, Directory information, and the other information the wizard requests, then click "OK."
2. Click "File" in the Case Data Navigation pane again, and click "Add Medium." A message box will appear. Review the information, and if you deem acceptable click "OK."
3. Restart X-Ways Forensics Now? message box will appear. Click "Yes".
4. Once again click File in the Case Data Navigation pane again, and click "Add Medium".
5. A new window should appear with a selection of different medium. Select the USB flash drive and click "OK".
6. The USB flash drive should now be loaded.

Once the flash drive had been processed it was left plugged into the computer while all forensic techniques for X-Ways were reviewed.

5.3.1 File Type Filter

The first technique used for X-Ways was viewing the information through a File Type Filter. This allows investigators to select which types of data they want the forensic tools to select for analysis. File Type Filtering was used to review the 108 files and detected 36, missing 72 files. With this technique, 33.33% of the files were discovered, making the percentage error 66.67%. All Set 0, the control group, and Set 3, encryption, were detected. However, none of the files in the following sets were discovered: Set 1, Extension Changed; Set 2, Extension Removed; 4, Transmogrification; 5, Cloaking.

Limitations were put on the file type filter technique. For this test, I selected the options to search for the file types in this research. "Text, Word Processing," "Spreadsheets," and under the main header "Page Layout" and the "pdf – Adobe Acrobat" option were all selected to capture all the document types. "Pictures," "3D Pictures," and "Video" were selected to capture all the picture and video files. "Sound/Music" was chosen to detect the audio files and under the main header "Programs" the option "exe" was selected to find the two executable files.

X-Ways File Type Filter was relatively simple to find and use, but was not displayed in a way that drew the forensic investigator to using it. To better analyze files, some limitations were required to be set up as well. This earned the File Type Filter the usability score of a 4. The following steps were performed to use File Type Filtering:

1. Go to Options -> Directory Browser…
2. Go to Filter on the type of files and click the funnel icon next to Type.

3. Select all the files you want to search for. For this test I limited to the file types in this research as stated above.
4. Click "Activate" which will close the window and turn the funnel icon blue.
5. Click "OK."
6. Review the file folders to see which appeared and mark the matrix accordingly.

FORENSIC TOOL: **X-Ways Forensics**
VERSION: **17.5 SR-6 x64**
TECHNIQUE USED: **Directory Browser File Type Filter**

	Set 0	Set 1	Set 2	Set 3	Set 4	Set 5
Action.mp3						
David.mp3						
Bear.png						
Secret.png						
Cheyenne_jpg.jpg						
Found.jpg						
Crews.gif						
LaDiDa.gif						
ExifPro.exe						
Explorer.exe						
Ranch.mp4						
River.mp4						
Resume.pdf						
ASEE.pdf						
Sales.xlsx						
Student.xlsx						
Story.docx						
Submission.docx						

True Positive
False Negative
False Positive
True Negative

TIME: **1 minute 55.38 second (time was started at requested restart of X-Ways)**
TOTAL NUMBER OF FILES EXAIMED: **108**
NUMBER OF ERRORS: **72**
PERCENTAGE ERROR: **66.67%**
NUMBER OF FILES DETECTED: **36**
PERCENTAGE CORRECT: **33.33%**
USABILITY [Rate from 1 (difficult to use) to 5 (straightforward to use)]: **4**

Figure 15 - X-Ways Forensics Matrix: Directory Browser File Type Filter

5.3.2 Specialist Tools: File Header Signature and Verify File Types

Specialist's technique of refining the volume snapshot was the next technique used for X-Ways. Under these options was a method that allows the investigator to review the files based on file header signature and verifies file types with signatures and algorithms. Part of the algorithms used detects for filename or file type mismatches and an internal file signature check (Fleischmann, 2017). File Type Filtering was used to review the 108 files and detected 84 of the files only missing 24. This technique detected 77.78% of the files, making the percentage error 22.22%. All of Set 0, the control group, Set 1, Extension Changed, Set 2, Extension Removed, and Set 3, encryption, were detected.

The Directory Browser settings were left enabled from the same set before since it narrowed down the files that the forensic investigator in this test case is searching for. File Header Signature and Verify File Types were used against two different mediums to see if there was any change in results. First, it was used against a closed image of the drive. Second, it was tested against the physical USB drive. The two scans detected the same files, but there was a difference in the time it took to review the files. Cloning the physical drive to make the image took 8 minutes 37.19 seconds and then to scan for the headers and signatures it took 9 minutes 53.63 seconds for a total of 18 minutes 30.82 seconds. Scanning the headers and signatures for the physical drive took a total of 7 minutes 4.03 seconds.

Usability for the Special Tools: File header Signature and Verify File Types received a rating of four out of five. Selecting the options, triggering the scan, and the displaying the results were all simple tasks. However, without any prior knowledge this tool would be difficult to discover on one's own and would take time to figure out. The following steps were performed to use the Specialist Tools: Filer Header Signature and Verify File Types:

1. Open the “Specialist” menu and select “Refine Volume Snapshot.”
2. Check “File header signature search” and check “Verify file types with signatures and algorithms.”
3. Select which piece of evidence you want to run this check on. For this research we ran this search on the Kingston USB image created.
4. Select which file types you are searching for by checking “In selected Evidence Objects”. For this research the following were chosen: Pictures, Documents, Music/Video, and under the Programs option Windows exec.
5. Click “OK.”
6. Review the file folders to review which files were detected and mark the matrix accordingly.

FORENSIC TOOL: **X-Ways Forensics**
VERSION: **17.5 SR-6 x64**
TECHNIQUE USED: **Specialist Tools: File Header Signature & Verify File Types**

	Set 0	Set 1	Set 2	Set 3	Set 4	Set 5
Action.mp3						
David.mp3						
Bear.png						
Secret.png						
Cheyenne_jpg.jpg						
Found.jpg						
Crews.gif						
LaDiDa.gif						
ExifPro.exe						
Explorer.exe						
Ranch.mp4						
River.mp4						
Resume.pdf						
ASEE.pdf						
Sales.xlsx						
Student.xlsx						
Story.docx						
Submission.docx						

True Positive
False Negative
False Positive
True Negative

TIME: **1 minutes 55.38 seconds (Booting X-Ways and connecting storage device)**
Cloning: 8 minutes 37.19 seconds
Scanning the headers and signatures - image: 9 minutes 53.63 seconds
Scanning the headers and signatures – physical drive: 7 minutes 4.03 seconds
TOTAL NUMBER OF FILES EXAIMED: **108**
NUMBER OF ERRORS: **24**
PERCENTAGE ERROR: **22.22%**
NUMBER OF FILES DETECTED: **84**
PERCENTAGE CORRECT: **77.78%**
USABILITY [Rate from 1 (difficult to use) to 5 (straightforward to use)]: **4**

Figure 16 - X-Ways Forensics Matrix: Specialist Tools

5.3.3 Overall

Forensic investigators will use every technique and method built into their forensic tool. X-Ways had two methods that combined together to create its overall score: Directory Browser File Type Filter, Specialist Tools: File Header Signature & Verify File Types. Using both techniques, the number of finals examined was 108. Of those files, 84 were detected, leaving 24 files still undiscovered. The overall percentage detected by X-Ways Forensics was 77.78%. X-Ways Forensics missed 22.22 % of the files with the missing files only being from Set 4, transmogrification, or Set 5, cloaking. Overall, X-Ways was a simple tool to use but some training or prior knowledge would aid with usability, earning X-Ways Forensics the overall usability rating of four.

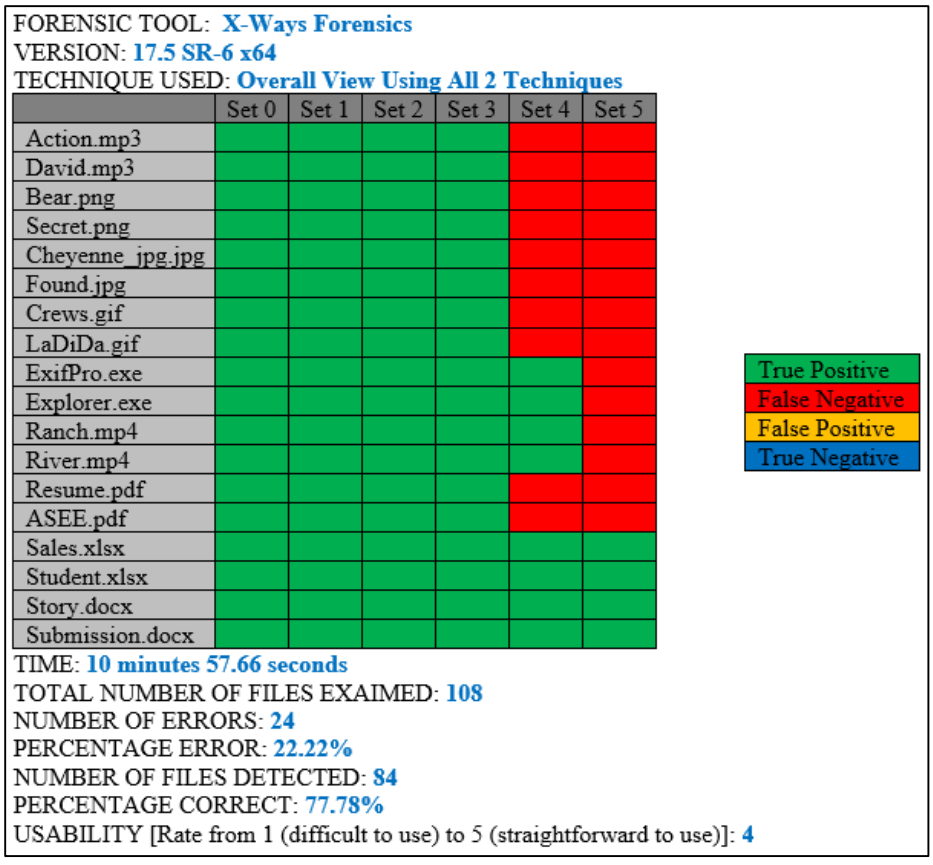


Figure 17 - X-Ways Forensics Matrix: Overall View Using all 2 Techniques

5.4 Summary

Each forensic tool, Autopsy/Sleuth and X-Ways Forensics, was tested against the methodology and provided valuable results. While completing the methodology against the tools, there were some points of improvement discovered, and the addition of a notes sections, computer specifications section, and a usability rating were all included in the final methodology. Two forensic tools were tested, but each had different techniques that were used for testing. Autopsy had four different techniques that were reviewed by the methodology and X-Ways had two different techniques reviewed. In total, six different techniques were reviewed by the methodology. An analysis of the forensic tools based on the results discovered using the methodology of this thesis is discussed next.

6 FORENSIC TOOL ANALYSIS

6.1 Autopsy/Sleuth Analysis

Two forensic tools were tested against this thesis's framework and observations were made from the results. Autopsy has an overall of four techniques that were utilized. First, Views – By Extension was able to observe sixteen out of the eighteen files from Set 0: Control Group, and Set 3: Encryption. Each file discovered with this technique had its original extension, so this method only seems to be effective for searching for files that have only been encrypted, not altered. Both the files undetected were GIF files. Since this technique missed the GIF files it implies that Autopsy may be missing some key file types. Autopsy does not offer modular settings or options when using this technique. Missing the GIF files implies that Autopsy's Views – By Extension needs updating to ensure that it includes all popular options. The next technique used, Views – By MIME Type, detected 25 more files overall while catching all the ones that Views – By Extension detected.

Using Autopsy, there were a couple of anomalies that caused further research. In the techniques Views – By MIME Type and View Images/Videos both discovered Found.jpg in Set 4, Transmogrification, and Set 5, Cloaking. I reviewed both JPG files (Found.jpg and Chyenne_jpg.jpg) and both files were altered properly. Trying to discover the difference, I was reviewing a library of file signatures by Gary Kessler (Kessler, 2017). Next, I noticed besides having a header signature, JPG files will have a Trailer. A Trailer is a set of bytes that appear at

the end of the file to help designate its file type. JPG files specifically have the Trailer FF D9 (ÿÙ). Analyzing the JPG files of Cheyenne and Found, I discovered that while the Found.jpg file did have the Trailer, Cheyenne_jpg.jpg did not. The Cheyenne photo ended with multiple 00 hexadecimal sets with no Trailer. After I reviewed the file, there was not a Trailer at the end of the set of 00 or right before it. This would appear to be the cause of detection of Found.jpg while the technique missed the Cheyenne_jpg.jpg file.

I was reviewing other file types that were tested for this research and discovered that GIF files also have a Trailer, specifically 00 3B (.;) (Kessler, 2017). Assuming that analyzing the Trailer is how Found.jpg was discovered, this lends credence to the fact that Autopsy does not search for GIF files. However, three other files types were discovered to have a Trailer and were still not discovered in Set 4 or Set 5. Docx and xlsx style files have a Trailer that starts with 50 4b 05 06 (PK..) and then is followed by 18 additional bytes, and PNG files have the Trailer 49 45 4E 44 AE 42 60 82 (IEND®B`,...). So, while this does appear as a way to analyze files based on their Trailer signature, I am unsure if this is a technique used by Autopsy for Views – By MIME Type. This is an area of future work discussed in Section 7.

The other anomaly in the results of Autopsy was that the technique Views – By MIME Type detected the cloaked version of the file explorer.exe. Reviewing this file, I am still uncertain as to why this specific file was discovered. I've reviewed the two different executable files and both had their headers changed and the process was followed correctly. Executable files do not have a Trailer, so I am unsure what the difference between these two files was that caused explorer.exe to be detected while ExifPro.exe remained hidden.

Last, the Extension Mismatch Detected technique was used. This technique only discovered five out of the 108 files that it scanned. This technique received the worst discovery percentage

of 4.63% and had the lowest usability score for Autopsy since use of the tool would take time for a new user to discover it or would require some preexisting knowledge.

After completing the analysis with Autopsy's four techniques relevant to this research, Autopsy was able to discover 67.59% of the files. Most files that remained hidden were in Set 4 and Set 5. One file set that was discovered and not discussed was Ranch.mp4 and River.mp4, but these files will be discussed in section 6.3. Autopsy did have a hole in the matrix missing two files in Set 1, Extension Change: ExifPro.exe and explorer.exe. For this research, the chosen file extension change was to change it to a dynamic-link library file with a .dll extension. Dynamic-link library and executable files are similar in that they share the same header. It would appear that this similarity is the cause of those two files being missed in Set 1.

6.2 X-Ways Forensics Analysis

X-Ways Forensics was the second of the two forensic tools reviewed through this experimental framework. Overall, two techniques available through X-Ways Forensics were used: Directory Browser File Type Filter and Specialist Tools: File Header Signature and Verify File Type. First, I set up the Directory Browser File Type Filter. Once that was established, X-Ways Forensics could properly sort every file that still had its proper extension, detecting every file from Set 0, Control Group, and Set 3, Encryption. This technique had many different options that could be chosen for different file types, but was also able to be adjusted to only search for the file types desired, which was what was done for this research and discussed in section 5.3.1.

Second, I used the technique Specialist Tools: File Header Signature and Verify File Types. For this technique, the Directory Browser File Type Filter settings were left in place to limit the

file types detected to the file types we were researching for this thesis. Performing Specialist Tools: File Header Signature and Verify File Types detected 77.78% of the files. A few files appeared in the Transmogrification, but these will be discussed more in depth in section 6.3. However, it was interesting that this technique did not detect Found.jpg or any of the other image file types, specifically GIF and PNG file types, that are known to have a Trailer.

Two other differences from Autopsy were notable. First was the discovery of ExifPro.exe and explorer.exe for Set 1, Change Extension. While dynamic-link libraries and executable files are similar, X-Ways modular capabilities allowed the setting to be set to search for executable files and not dynamic link libraries. With the second technique, X-Ways Forensics was able to discover the two related files that Autopsy failed to detect. The second difference was the detection of the Microsoft Excel files with extension .xlsx and the Microsoft Word Document files with extension .docx. These two file types were discovered with every different anti-forensic technique in this thesis used to alter the files. Reviewing the files more thoroughly, it was discovered that these files have subheaders within the file. A subheader is a signature that can be found within the file, not just at the beginning or the end, such as a header or a Trailer, respectively. A [Content_Types].xml signature appears multiple times through these types of files (Kessler, 2017). In the beginning of the hexadecimal code of the file, the string [Content_Types].xml is at the top of both the Microsoft Excel spreadsheets and the Microsoft Word document file types. Searching on the text string .xml through the spreadsheet file type revealed multiple instances of spreadsheet subheaders, including workbook.xml, sheet#.xml and others. The Word file revealed a similar pattern with multiple subheaders including document.xml, footnotes.xml, and more. It is logical to conclude that X-Ways can analyze the files beyond their extension and header information. X-Ways Forensics could have reviewed the

internal subheaders of the files to discover them, or used their Trailer, but since other file types that also have a Trailer were not discovered it would seem it relied on analyzing the internal subheaders.

Usability was an area where Autopsy had the advantage over X-Ways Forensics. Autopsy was very intuitive and natural to use. X-Ways Forensics offers a much more modular product and allows a forensic investigator to approach an investigation with a very broad or a very narrowed approach. Through the review completed for this research, this modular ability was a great advantage. While some training or time and experience to gain some pre-existing knowledge would be recommended, the modularity gave X-Ways Forensics an edge in analysis.

6.3 Transmogrification

Transmogrification was one of the more complicated anti-forensic data hiding techniques researched in the testing against forensic tools. Transmogrification is an anti-forensic technique that involves modifying the header and extension of a file so that it is no longer associated with the originally known file type, and hides against signature-based scanning methods. Once the results were completed for Autopsy and X-Ways Forensics, it was concluded that both tools could detect the video files, Ranch.mp4 and River.mp4, in Set 4, Transmogrification. Video files, specifically the mp4 type of files tested in this research, have longer than average headers, normally 24 bytes long, but can vary (Kessler, 2017). Each of these headers have a few points that are similar, but the one that we want to discuss here is the first six bytes. The first six bytes in each case of the mp4 type file header starts with 00 00 00 and after these bytes starts the header information. Since for our process of Transmogrification the dynamic-link library file type was chosen, there were complications. Dynamic-link library headers are only four bytes

long, denoted in hexadecimal as 4D 5A or text MZ. For this process, the overwriting caused only 0s to be overwritten and not the actual header information, therefore the transmogrification technique for these files was still discoverable. To properly implement the transmogrification technique with long headers is a complication.

There are other complications/weaknesses to the transmogrification technique that were discovered through analysis in this thesis. Some files have a Trailer at the end of the file, which also designates the file type. Any file with a Trailer would also need the Trailer deleted or changed to the new file type that was being implemented. Lastly, some files have had internal subheaders that help when analyzing the file for its signature. So, whether transmogrification will be discovered or not will depend on the length of the original header and the header it is changed to, a Trailer, and the internal subheaders of a file.

6.4 Determinations

As part of this thesis, four research objectives were defined. First, the research objective to develop and test a methodology to evaluate the robustness of forensic tools' ability to detect data hiding, which has been discussed and reviewed at length. The other three research objectives were defined to assist with the developing of the framework and to ensure measurable values of the capabilities of the forensic tools were being recorded for analysis.

6.4.1 RO-2: Determine the Fastest Forensic Tool Results

As part of the methodology, the time the tool spends to complete the analysis was recorded to allow for comparison. A stopwatch was used to measure the time with the same reviewer trigging the start and stop to help make response time changes to activating the stopwatch

negligible. The analysis time measured was digital capabilities of the tool to scanning completion, not the time the reviewer took analyzing the results. Most of the analysis times are the same, because multiple techniques were performed with the same scan. If a technique requires more time to be completed than the first initial scan, the extra time is added at the end of the other time. Final times used to determine the fastest forensic tools is the time required for the tool to run all the scans for all the techniques used. Of the two tools tested, Autopsy was the fastest with a time of 7 minutes 27.85 seconds. X-Ways Forensics took a time of 10 minutes 57.66 seconds to complete its scan.

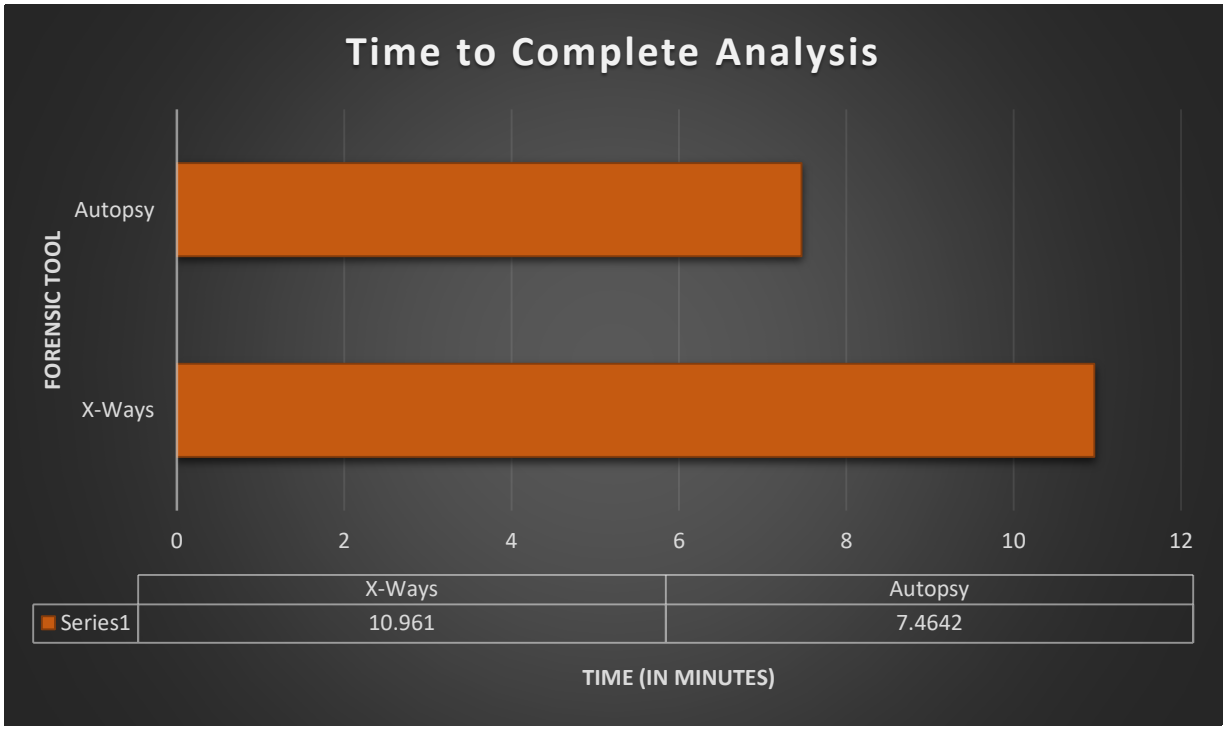


Figure 18 - Graph Showing Fastest Tool

6.4.2 RO-3 Determine the Forensic Tool with the Least Error Results

One of the research objectives was to measure and determine which tool had the least amount of errors. For this research, an error constitutes a finding that is either a false positive or a false negative. X-Ways Forensics was found to have the least amount of errors with the overall rating using its two techniques resulting in 24 errors and a percentage of 22.22% of files undetected. Autopsy had a total of 35 errors making it 32.41% of the files reviewed in this research undetected.

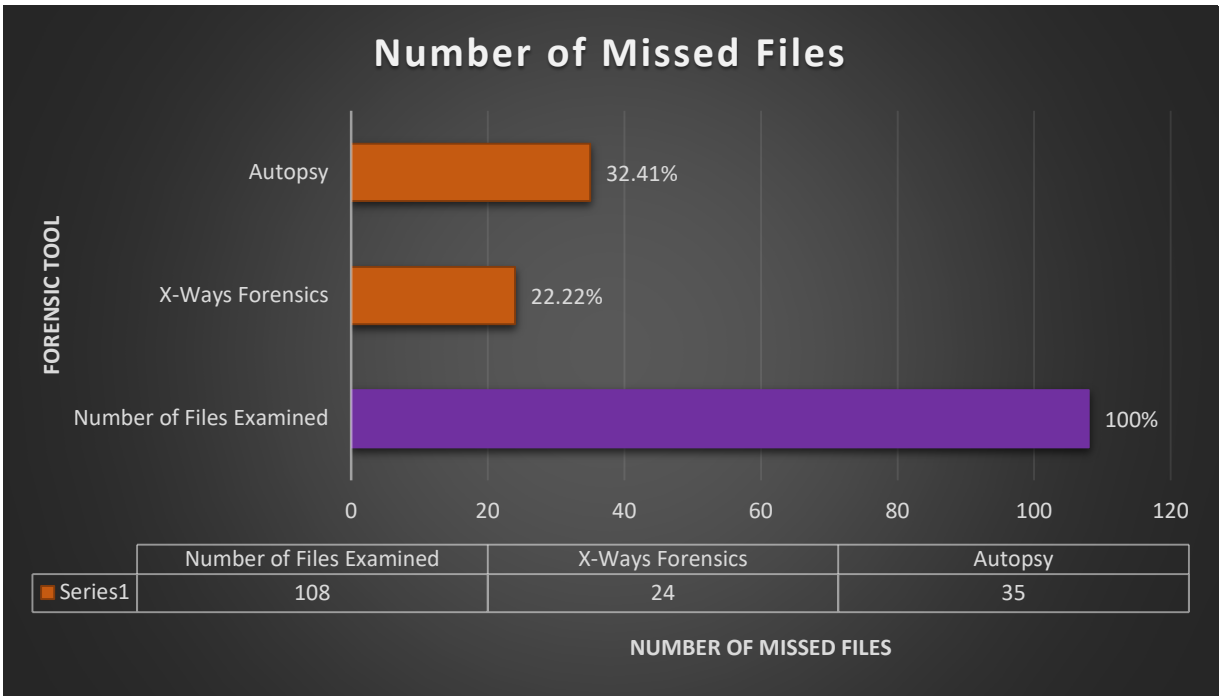


Figure 19 - Graph Showing Number of Errors per Forensic Tool

6.4.3 RO-4 Determine the Forensic Tool that Discovers the Most Results

Being able to detect files is key to being able to review them for cases and see if the evidence is relevant. Included in the research goals of this thesis was the result of determining which forensic tool detects the most hidden files. For this research, detection constitutes a true positive that a file was detected and categorized correctly. X-Ways Forensics detected the most files with the number of detected files being 84, and the percentage correct being 77.78%. Autopsy detected 73 files with the percentage correct being 67.59%.

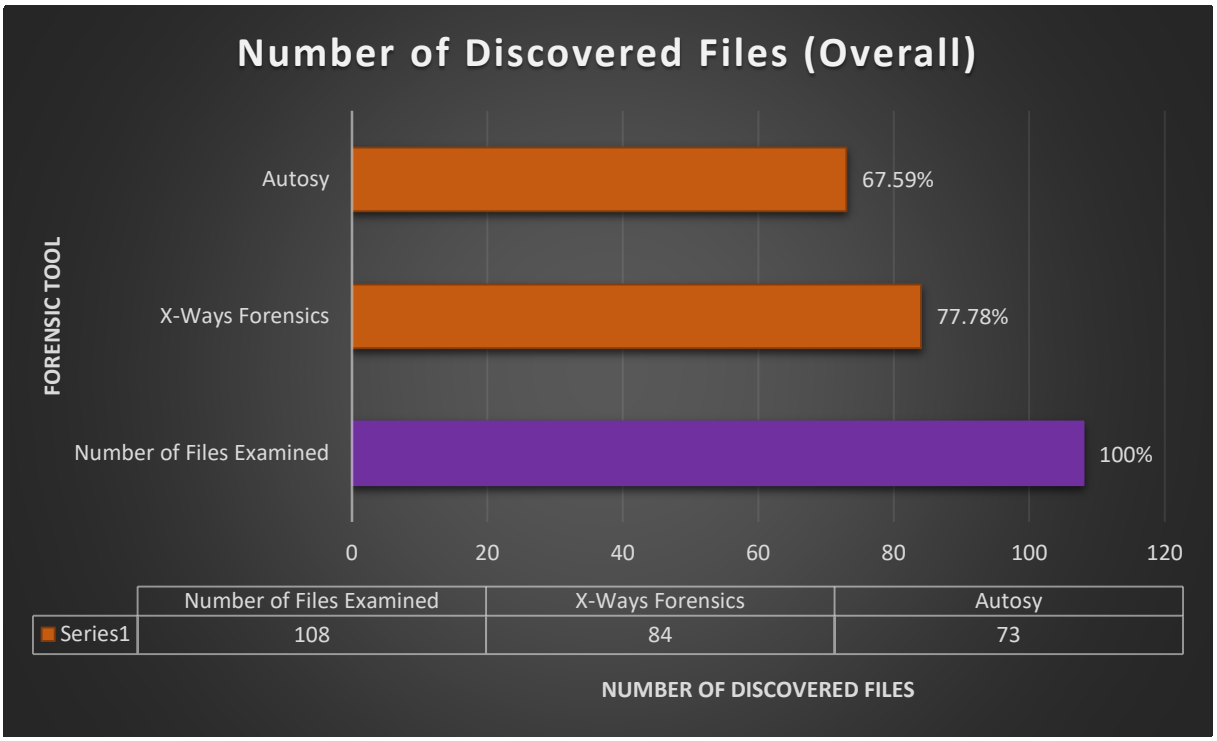


Figure 20 - Graph Showing Number of Discovered Files(Overall)

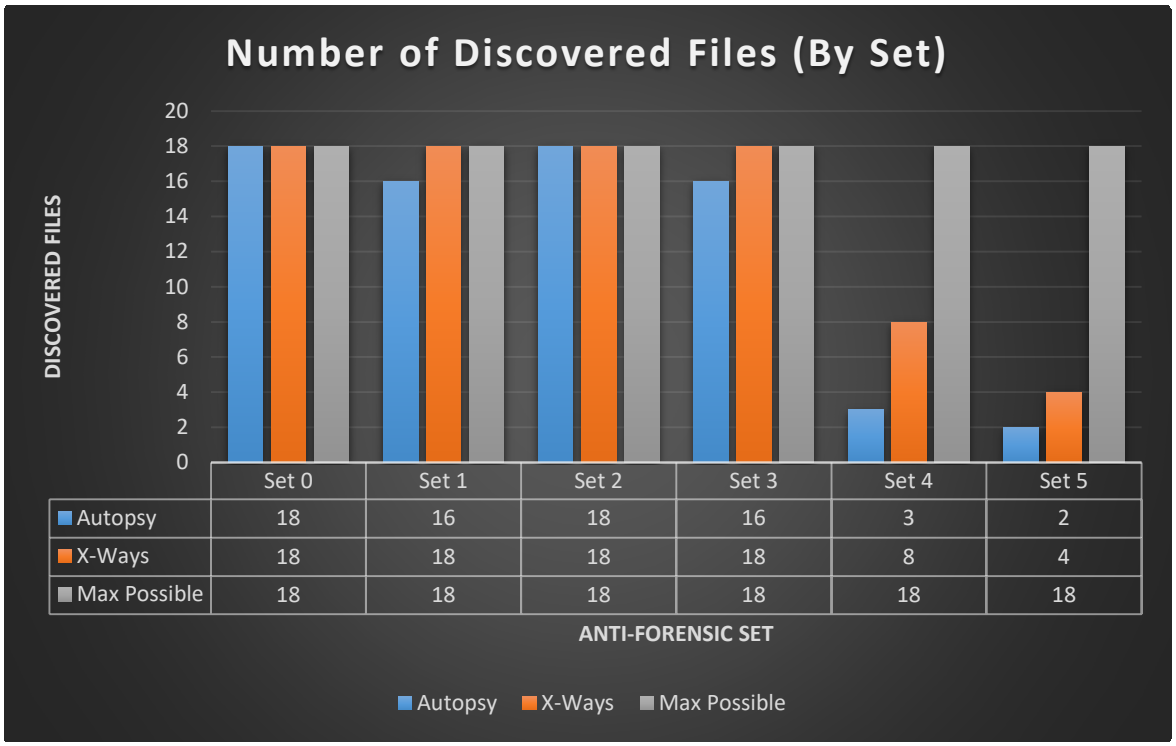


Figure 21 - Graph Showing Number of Discovered Files (By Set)

7 DISCUSSION AND FUTURE WORK

7.1 Detecting Hidden Files

There has not been an extensive amount of information on testing forensic tools against data hiding. The reviewed academic, scholarly, and other works contained concerns about vulnerabilities and weaknesses with forensic tools, but nothing specific to data hiding. This research provides a methodology for evaluating forensic tool robustness in detecting files that have been altered by anti-forensic data hiding techniques and it has been reviewed by eight information technology and security professionals. With their feedback, the methodology has been iterated upon and updated to the final edition included in this thesis. The methodology has been designed to be flexible to the needs of the reviewer and offers scalability as new anti-forensic techniques and methods of data hiding are discovered.

7.2 Validation of the Methodology

Validation of the methodology designed in this thesis was important as it is the primary contribution to cyber forensic security. Two goals were accomplished in the methodology for a forensic tool's ability to detect hidden files: 1) It brought insight to the state of current capabilities and 2) provided a framework that could be used to compare and contrast forensic tools and their effectiveness at detecting hidden files. I provided validation by evaluating the methodology in two ways. First, I had eight information technology and security professionals

peer review the methodology. From their reviews the methodology evolved and improved, causing edits, including the remarking of using a specific operating system, recommendations on tools, and making the directions more exact, clear, and focused. Their insights and feedback helped to round out the methodology to the completed format presented in this thesis. Second, I performed methodology on two forensic tools with a total of six techniques to gather information on the forensic tool and determine if the flow and process worked properly. These edits caused three major additions: the inclusion of a notes section, the addition of computer specifications being recorded during the testing phase for each tool, and the inclusion of a usability standard remarked on by the reviewer to give an estimate on how intuitive and straightforward the tools and different techniques are via an overall rating. These evaluation methods helped establish a well thought out and accurate methodology for testing the robustness of a forensic tool's ability to detect files hidden with anti-forensic techniques.

7.3 Impact

Chapter 6 details the reviewer's analysis of the forensic tools tested. Of the two tools tested, Autopsy was found to be faster, while X-Ways was found to be more accurate in file discovery. Usability of both tools was scored closely, with Autopsy earning a 4.75 and X-Ways earning a 4. Part of the reason for X-Ways' lower score was the configuration details that were allowed for its techniques. While a beginning investigator may struggle with some of the options, an average to experienced forensic investigator should have no issue using the more granular techniques to his or her advantage. The results suggest that forensic tools can handle the less complicated data hiding techniques but will have significantly more trouble detecting the more advanced techniques such as Transmogrification and Cloaking.

7.4 Future Work

Cyber forensics is a growing and evolving discipline that requires continued research to stay current and relevant. This research delved into the specific area of anti-forensic and generic data hiding. Garfinkel stated that around 2010 we would see an end to the "Golden Age of Digital Forensics," and the research completed in this thesis shows there are gaps and vulnerabilities in current tools (Garfinkel, 2010). Technology keeps advancing in processing power and storage with multiple areas of storage with external hard drives, USB flash drives, solid state drives, and cloud storage. The backlog of government forensic cases continues to increase. Forensic investigators now expect to run into anti-forensic techniques in their cases. It is an important time for academy and industry to focus research and improve forensic tools and techniques.

7.4.1 Content Based Files Analysis and Partnering with Industry

Detection of the file type through the content in the file could be an effective way of determining the file type. Some researchers have looked into methods involving frequency analysis, cross-correlation analysis, file header/Trailer analysis, and n-gram analysis (Amirani & Beheshti, 2008; Li, Wang, Stolfo, & Herzog, 2005; McDaniel & Heydari, 2003). Each of these new developments reported accuracy of over 90% depending on which algorithms were used. Briefly reviewing this research, it was completed ranging from nine to fourteen years ago. However, in this research X-Ways Forensics was our most accurate reporting tool with analysis recovered at 77.78%. While more research into these techniques would be fruitful, there is a disconnect between academic research and industry. Partnering with industry, academic research can bring more lasting value to their developments by creating new tools or improving existing ones for forensic investigators to use. More work can be completed to better understand

where this disconnect occurred, and to develop lasting partnerships between academia and industry.

7.4.2 Trailers in JPG Files

Further research into why one of the JPG test files has a Trailer and one JPG file didn't is needed. One of the files was created with MS Paint while one was taken with a digital camera. Further investigation and research would need to be completed to learn more about why some files have a Trailer while others do not.

7.4.3 Expand Data Hiding Types

Research into detecting data hiding has room to grow. Data hiding can be separated into the three categories: generic data hiding, cryptography and steganography. The research in this thesis focused on generic data hiding, specifically hiding files by altering them with different anti-forensic techniques, but further research can expand to other areas of data hiding. Generic data hiding includes hiding data in unallocated space and other locations in an attempt to be missed by forensic tools. Cryptography uses encryption to password protect the data. Steganography embeds data in other files to avoid detection, such as a message within a picture file. With the scalability and flexibility of the methodology developed for this purpose, the research can be expanded to include these forms of data hiding.

7.4.4 Faster Analysis

The growth in storage device capabilities and the accessibility of the cloud has caused a great increase in the data and information that needs be processed (Garfinkel, 2010). In one year, Iowa's crime lab saw their cyber-crime forensic exams increased by 516 from 856 cases to 1372

cases; a 60.28% increase ("DCIFactSheets," n.d.). Improving the processing power of tools to enable faster analysis is an area that future research needs to be centered on. For example, the testing and research preformed in this thesis was of a small sampling of data in a controlled environment. The flash drive was 60GB with the test files only being 622MB. Even with these small data sizes Autopsy took 7 minutes 3.52 seconds to review the data and X-Ways Forensics took 10 minutes 57.66 seconds. With hard drives capable of containing over a Terabyte of data, and normally containing many more files than 622 MB, this is an area of cyber forensics that needs to be improved.

7.4.5 Realistic Testing

Testing for forensic tools and their techniques are completed in controlled lab environments such as the methodology designed in this thesis. To provide a realistic level of testing and get a close as possible testing of a real case, academic research partnered with industry and/or law enforcement can create a beneficial testing environment. Research into forensic testing similar to a penetration test would be an interesting venture that could bring beneficial results. Penetration tests are ethical hacking tests where test parameters are established and attacks are performed against computer systems, networks, and web application to find vulnerabilities. Attacks are performed to see realistically how far can exploits can be used to compromise systems. Creating a similar process, such as research into creating forensic images with a variety of anti-forensic altered files hidden and allowing forensic investigators to perform analysis on them could prove an essential training and assessment technique. In a penetration test, the best way to test processes and monitoring of a network and system is to perform the test with only the directors and managers being aware of when a test is happening. Security analysts who perform the day-to-day operations are left in the dark. This allows the test to realistically gauge their

team's incident response. Further research into performing similar tests for forensic investigations where the director or manager would know the test is happening, but the forensic investigator would be in the dark and an image would be prepared by researchers to realistically test if the forensic team's current process and methods are effective, would be a worthwhile area of study and development.

REFERENCES

Amirani, M. C., & Beheshti, A. A. (2008). A New Approach to Content-based File Type Detection †. *IEEE Symposium on Computers and Communication*, (July 2008), 1103–1108. https://doi.org/10.1109/ISCC.2008.4625611

Balan, C., Dija, S., & Vidyadharan, D. S. (2010). The need to adopt agile methodology in the development of Cyber Forensics Tools. *2010 IEEE International Conference on Computational Intelligence and Computing Research, ICCIC 2010*, 461–464. https://doi.org/10.1109/ICCIC.2010.5705815

Bruneau, G. (n.d.). Hex File Headers and Regex for Forensics Cheat Sheet v1.0. Retrieved May 10, 2017, from https://digital-forensics.sans.org/media/hex_file_and_regex_cheat_sheet.pdf

Casey, E. (2002). Practical Approaches to Recovering Encrypted Digital Evidence. *International Journal of Digital Evidence*, *1*(3). Retrieved from https://www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf

CENTER, L. E. C. (n.d.). DIGITAL SEARCH WARRANTS. Retrieved May 10, 2017, from http://www.iacpcybercenter.org/prosecutors/digital-search-warrants/

Damshenas, M., Dehghantanha, A., & Mahmoud, R. (2014). A Survey on Digital Forensics Trends. *International Journal of Cyber-Security and Digital Forensics*, *3*(4), 209–234.

Daniel, L. E. (n.d.). Digital Forensics In Child Pornography Cases. Guardian Digital Forensics. Retrieved from http://winfredbar.org/images/Digital_Forensics_in_Child_Pornography_Cases.pdf

DCIFactSheets. (n.d.). *Division of Criminal Investigation*. Retrieved from http://www.dps.state.ia.us/DCI/DCIFactSheets.pdf

de Beer, R., & Van Belle, J.-P. (2015). Anti-Forensics: A Practitioner Perspective. *International Journal of Cyber-Security and Digital Forensics*, *4*(2), 390–403. https://doi.org/10.17781/P001593

EXIFPro. (2011). Retrieved May 10, 2017, from http://www.exifpro.com/

Fleischmann, S. (2017). *WinHex Forensics/WinHex Manual*. X-Ways Software Technology AG. Retrieved from http://www.x-ways.net/winhex/manual.pdf

Free Music Archive. (n.d.). Retrieved May 10, 2017, from http://freemusicarchive.org

Garfinkel, S. L. (2007). Anti-Forensics: Techniques, Detection and Countermeasures. *Naval Postgraduate School*. Retrieved from http://simson.net/ref/2007/slides-ICIW.pdf

Garfinkel, S. L. (2010). Digital Forensic Research: The Next 10 years. *Digital Investigation*, 64–73. Retrieved from https://www.researchgate.net/publication/222420855_Garfinkel_SL_Digital_Forensics_Research_The_Next_10_Years_Digital_Investigation_7suppl_64-73

Garrie, D. B., & Morrissy, J. D. (2014). Digital Forensic Evidence in the Courtroom : Understanding Content and Quality. *Northwester Journal of Technology and Intellectual Property*, *12*(2), 122–128. Retrieved from http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1218&context=njtip

Giphy. (n.d.). Retrieved May 10, 2017, from https://giphy.com/

Henry, P. A. (2011). Anti-Forensics: Considering a career in Computer Forensics? Don't quit your day job……. Secure Computing. Retrieved from http://www.layerone.org/wp-content/uploads/2011/01/Anti-Forensics-LayerOne-Paul_Henry.pdf

Horz, M. (2017). HxD - Freeware Hex Editor and Disk Editor. Retrieved May 10, 2017, from https://mh-nexus.de/en/hxd/

Kabay, M. E. (2008). A Brief History of Computer Crime : An Introduction for Students School of Graduate Studies. *Norwich University*, 1–51. Retrieved from http://www.mekabay.com/overviews/history.pdf

Kamble, D. R., & Jain, N. (2015). Digital Forensic Tools: A Comparative Approach. *International Journal of Advance Research In Science And Engineering*, *4*(2). Retrieved from http://embeddedsw.net/doc/Openpuff_paper_Digital_forensic_tools_a_comparative_approach.pdf

Kessler, G. C. (2007). Anti-Forensics and the Digital Investigator. Retrieved from http://www.garykessler.net/library/2007_ADFC_anti-forensics.pdf

Kessler, G. C. (2017). File Signatures Table. Retrieved May 10, 2017, from http://www.garykessler.net/library/file_sigs.html

Li, W., Wang, K., Stolfo, S. J., & Herzog, B. (2005). Fileprints : Identifying File Types by n-gram Analysis. *IEEE*, (June). Retrieved from http://ids.cs.columbia.edu/sites/default/files/FilePrintPaper-revised.pdf

Lyle, J. (2006). Computer Forensic Tool Testing at NIST (pp. 1–44). Seattle. Retrieved from https://www.cftt.nist.gov/presentations/AAFS-Seattle-2006-Engineering-Section.pdf

McDaniel, M., & Heydari, M. H. (2003). Content based file type detection algorithms. *System Sciences, 2003*. Retrieved from http://ieeexplore.ieee.org/document/1174905/

Media Type "image/vnd.microsoft.icon" Details. (2003). Retrieved May 14, 2017, from http://www.fileformat.info/info/mimetype/image/vnd.microsoft.icon/index.htm

MIME-TYPE.net. (2009). Retrieved May 14, 2017, from http://www.mime-type.net/mime-types.php

Moses, S., Baker, N. S., & Rowe, D. C. (2016). Helping the Human Element : Educating in Social Engineering. New Orleans: American Society of Engineering Education. Retrieved from https://www.asee.org/public/conferences/64/papers/17379/view

NIST. (2015). Computer Forensic Tool Testing. Retrieved May 11, 2017, from https://www.cftt.nist.gov/

O'Regan, G. (2008). *A Brief History of Computing*. Springer. https://doi.org/10.1007/978-1-84800-084-1

OWASP. (2017). About The Open Web Application Security Project. Retrieved May 11, 2017, from https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project

pngimg.com. (n.d.). Retrieved from http://pngimg.com/

Price, R. (2014, December 7). Can police force you to surrender your password? *The Kernel*. Retrieved from http://kernelmag.dailydot.com/issue-sections/features-issue-sections/11071/police-force-password-cellphone/

SANS. (2017). About. Retrieved May 11, 2017, from https://www.sans.org/about/

Sleuthkit. (2016). Autopsy. Retrieved October 5, 2016, from http://www.sleuthkit.org/autopsy/

View Of River From Boat. (n.d.). Retrieved May 12, 2017, from https://videos.pexels.com/videos/view-of-river-from-boat-2216

Welty, J. (2011). Warrant Searches of Computers. UNC Schhol of Government. Retrieved from http://www.ncids.org/Defender Training/2011SpringConference/WarrantSearchesComputers.pdf

X-Ways Forensics: Integrated Computer Forensics Software. (2016). Retrieved from http://www.x-ways.net/forensics/index-m.html