4-2020

Taxonomy for Anti-Forensics Techniques & Countermeasures

Ziada Katamara
kazi1101@go.stcloudstate.edu

Taxonomy for Anti-Forensics Techniques and Countermeasures

by

Ziada Katamara

A Starred Paper

Submitted to the Graduate Faculty of

St Cloud State University

in Partial Fulfillment of the Requirements

for the Degree

Master of Science

in Information Assurance

June, 2020

Starred Paper Committee:
Abdullah Abu Hussein, Chairperson
Lynn A Collen
Balasubramanian Kasi

Abstract

Computer Forensic Tools are used by forensics investigators to analyze evidence from the seized devices collected at a crime scene or from a person, in such ways that the results or findings can be used in a court of law. These computer forensic tools are very important and useful as they help the law enforcement personnel to solve crimes. Computer criminals are now aware of the forensics tools used; therefore, they use countermeasure techniques to efficiently obstruct the investigation processes. By doing so, they make it difficult or almost impossible for investigators to uncover the evidence. These techniques, used against the computer forensics processes, are called Anti-forensics. This paper describes some of the many anti-forensics' method, techniques and tools using a taxonomy. The taxonomy classified anti-forensics into different levels and different categories: WHERE, WHICH, WHAT, and HOW. The WHERE level indicates where anti-forensics can occur during an investigation. The WHICH level indicates which anti-forensics techniques exist. The WHAT level defines the exact method used for each technique. Finally, the HOW level indicates the tools used. Additionally, some countermeasures were proposed.

Table of Contents

Chapter Page

List of Tables

Table Page

List of Figures

Figure Page

Chapter I: Introduction

Introduction

Computers are electronic devices used almost by anyone and everywhere. Computers have become an important part of our everyday life since they can do so many things. They are equipped with many capabilities such as processing information very fast, giving accurate results, storing large amounts of data and information, and so on. However, these capabilities have also allowed criminals to misuse the computer by accessing unauthorized data, destroying or changing stored data, and so on. According to the United States Department of Justice (1989 as cited in Inc., n.d.), Computer crime is defined "as any violations or criminal law that involves knowledge of computer technology for their perpetration, investigation, or prosecution." Computer crime is also called Cybercrime or electronic crime. These computer crimes are committed by cyber criminals or computer criminals.

Digital Forensics, or Computer Forensics, is the process of recovering, interpreting, and investigating electronic data. The aim of digital forensics is to preserve evidence relevant to an investigation in its original form to use it in a court of law. For the evidence to be admissible in court of law, forensics investigators must follow strict procedures when collecting and analyzing the evidence. According to the United States Department of Justice (1989 as cited in Inc., n.d.), the forensics process consists of four phases: Collection, Examination, Analysis, and Reporting. The collection phase involves searching for the evidence, finding the evidence, and collecting and documenting the evidence. The examination phase involves recovering hidden or obscured information. The analysis phase involves analyzing the information recovered for its

importance and value. The reporting phase involves writing a report of the entire process—from collection to analysis.

Since computers have been misused by computer criminals in committing a crime, digital forensics has been very beneficial to catch these criminals who believe they do not leave any evidence behind.

Unfortunately, these criminals are now aware of the computer forensics tools used. To make it hard or almost impossible to recover evidence, computer criminals have come up, and continue to come up, with some anti-forensics techniques. Anti-forensics is a set of tools and techniques used to prevent the collection and interpretation of evidence during digital forensics investigation.

Anti-forensics methods can be applied at any stage of the computer investigation process. The aims of anti-forensics include hiding or destroying evidence, slowing down forensics' investigation, and causing uncertainty in a forensic report or tool (Garfinkel, 2007).

Lui and Brown (2006) discovered four primary goals for anti-forensics. These goals are "Avoiding detection that some kind of event has taken place, Disrupting the collection of information, Increasing the time that an examiner needs to spend on a case, Casting doubt on a forensic report or testimony" (Lui and Brown, 2006, as cited in Garfinkel, 2007).

Problem Statement

Computer criminals are becoming aware of the digital forensics' tools and techniques and are hence making the anti-forensics tools and techniques more sophisticated**.** With the increased use of anti-forensics tools and techniques, it has become challenging for digital forensics investigators to perform their investigation efficiently.

Nature and Significance of the Problem

Anti-forensics appears to be an obstacle for digital forensics, and this problem keeps growing significantly. In order to overcome this growing obstacle, digital forensics investigators need to keep themselves updated about the current anti-forensics tools, techniques and countermeasures.

This study will be useful not only to digital forensics investigators, but also for other research purposes. As previously mentioned, digital forensics need to keep themselves updated, therefore, new research initiatives and strategies will help address this growing problem.

Objective of the Study

The objective of this study is to perform in-depth research on some of the many anti-forensics' techniques and tools, then present strategies to detect them, and finally, discuss some countermeasures. A taxonomy will be created classifying anti-forensics into different levels and different categories . The goal of this research is not only to help digital forensics investigators but also to aid those doing the same research.

Study Questions/Hypotheses

1. What are the different types of Anti-forensics techniques?
2. Which method and tool can be used for each technique?
3. What are some countermeasures ?

Limitations of the Study

Every study has limitations, and just like any other study, some limitations were found in this study.

During the collection of secondary data, there was a lack of previous studies on the topic. A lot of books, articles, journals, and so on were carefully reviewed. However, because of the scope of this research topic, there were limitations of prior research studies that are relevant to this study.

Not only was it challenging to find specific answers to some of the questions researched; but verifying the validity of the data collected through secondary data was also a limitation. There are some questions that need to be answered before using a source such as:

- Who collected the data ?
- When was the data collected?
- How was the data collected? and so on.

These types of questions might help with the validity but one cannot be 100% sure.

Primary data was also used as part of this research. However, there was limited access to respondents. Only one person was interviewed for this research. Additionally, because of the organization's policy that the interviewee worked for, he was unable to answer every question asked leading to a lack of information needed.

Definition of Terms

- Anti-forensics: A set of tools and techniques used to prevent the collection and interpretation of evidence during digital forensics investigation.
- Counter-forensics: Another term for Anti-forensics.
- Countermeasure: An action one take to prevent a threat.
- Countermeasures: A countermeasure can be defined as an action taken or need to be taken to counteract a danger or threat.

- Cryptography: Transforming information into a more secure format.
- Cyber: Things that can be done using a computer.
- Cybercrime: A crime that involves the use of a computer and network.
- Cybercriminals: Individuals who use technology to commit malicious activities on digital systems or network.
- Data: Information stored or produced by a computer.
- Digital Forensics or Computer Forensics: The process of recovering, interpreting and investigating electronic data.
- Encryption: Encoding a message in such a way that unauthorized people cannot access it.
- Encryption: Encryption is a method of using an algorithm to protect data by scrambling it and making the data either unintelligible or undetectable.
- FDE : Full Disk Encryption.
- File extension: Indicates the format of a file.
- File header: File that may contain date, time, and so on a computer.
- Footprint: An area affected by something.
- Forensics tools: The main tools that the digital investigators use during an investigation to examine if any suspicious incident had occurred.
- Hard disk: A data storage device.
- Hardware: A hardware describes the physical aspects of a computer. This can be a computer monitor, keyboard, and so on.

- Hash function: A unique irreversible fixed value string which is created using a specific algorithm from any amount of data.
- Investigation: The action of investigating someone or something.
- Investigator: A person who performs an investigation.
- Linux: An open-source operating system for computers, servers, mobile devices, etc.
- LUKS: Linux Unified Key Setup—a hard disk encryption tool for Linux.
- MACE: Responsible to record Modification, Access, Creation timestamps of the file.
- Metadata: Data that provide information about other data.
- Network: A network consists of two or more computers that are linked or connected in order to share resources, exchange files, etc.
- NFTS : Stands for NT File System, and it is a file system used to store and retrieve files on a hard disk.
- Overwriting: Writing on top of another writing.
- Primary data: Data collected from first-hand sources. This includes data gathered from interviews, surveys, questionnaires, etc.
- Qualitative research: Qualitative research focuses on gathering non-numerical data in an attempt to interpret phenomena in terms of the meanings.
- Quantitative research: Quantitative research focuses on gathering numerical data to explain a particular phenomenon.
- Secondary data: Data collected from a source that has already been published. It can be obtained from books, articles, journals, newspapers etc.

- Software: “A software is a set of instructions, data or programs used to operate computers and execute specific tasks” (Rouse, 2019)
- Steganography: Hiding data within other data.
- Taxonomy: A scheme of classification.
- Techniques: A technique can be described as a process or procedure that needs to be followed.
- Tools: A tool can be described as a device or computer application that allows someone to do something.
- Windows: “A graphical operating system developed and published by Microsoft. It provides a way to store files, run software, play games, watch videos, and connect to the Internet” (Computer Hope, 2019).

Summary

This chapter introduced what anti-forensics is and how computer criminals came up with the anti-forensics tools and techniques with a purpose to make it hard or almost impossible for digital forensics investigators to collect evidence. The use of anti-forensics techniques is a big problem for forensics investigators therefore, the investigators must be aware of the techniques and tools used by these criminals. By knowing the anti-forensics techniques and tools, the forensics investigators might come up with some countermeasures. The next chapter will be a comprehensive literature review on anti-forensics.

Chapter II: Background and Review of Literature

Introduction

With the growth of computer crime, as well as the increased use of anti-forensics tools that interfere with forensic investigation, various authors have studied the different anti-forensics techniques and tools. Currently, there is no unique or standard definition of anti-forensics, different definitions have been previously proposed by different authors. Table 1 shows some of the many definitions for anti-forensics (Conlan, Baggili, & Breitinger, 2016).

Table 1

Different Anti-Forensics Definitions from Various Authors

Authors, Year of Publication	Anti-forensics Definitions
Shirani, 2002	Hiding a system intrusion attempt
Peron and Legary, 2005	Attempt to limit the identification, collection, collation and validation of electronic data
Grugp, 2005	Attempting to limit the quantity and quality of forensic evidence
Foster and Liu, 2005	Breaking tools or avoiding detection
Rogers, 2006	Attempts to negatively affect the existence, amount, and/or quality of evidence from a crime scene, or make the examination of evidence difficult or impossible to conduct
Liu and Brown, 2006	Application of the scientific method to digital media in order to invalidate factual information for judicial review
Harris, 2006	Any attempts to compromise the availability or usefulness of evidence to the forensics process
Kessler, 2007	Set of tools, methods, and processes that hinder forensic analysis
Garfinkel, 2007	A growing collection of tools and techniques that frustrate forensic tools, investigations and investigators
Berinato, 2007	An approach to criminal hacking that can be summed like this: make it hard for them to find you and impossible for them to prove they found you
Sremack and Antonov, 2007	The practice of thwarting a proper forensic investigation
Dahbur and Mohammad, 2012	Scientific methods are used to simply frustrate forensics efforts at all forensics stages
Albano et al., 2011	Methods undertaken in order to thwart the digital investigation process conducted by legitimate forensic investigators
Slamm et al., 2012	Disguising manipulation fingerprints or falsifying device specific fingerprints inadvertently introduced when a digital file is formed

Note: All the above references were cited in Conlan et al., 2016.

This chapter will present a literature review on anti-forensics techniques, tools, detection, and countermeasures. The chapter will be categorized into three main points: (a) background of the problem, (b) literature related to the problem, and (c) literature related to the methodology.

The background of the problem will include different reasons of why anti-forensics is a problem. The literature related to the problem will include different techniques and tools previously studied. The literature related to the methodology will consist of different solutions suggested.

Background Related to the Problem

Anti-forensic was discovered and recognized a few years ago as a legitimate field of study. According to Conlan et al. (2016), anti-forensics generally means “attempts to compromise the availability or usefulness of evidence during the forensics process. It has been a great concern for forensics investigators as it makes their job harder. As cited by Forte (2009), anti-forensics functions to remove all evidence of a digital event, or void or/and override the data by making it difficult or almost impossible to retrieve during an investigation. Anti-forensics techniques include securely deleting files by using software, making changes to the timestamp on a computer, and so on.

An example of the problem that anti-forensics techniques can cause to a law enforcement investigation is the case of the Federal Bureau of Investigation (FBI) vs. Apple. This case was about a terrorist shooting that happened in December 2015 in San Bernardino County in the United States. During this terrorist attack, 14 people were killed and 22 were injured. At the crime scene, the FBI seized an iPhone found on one of the terrorist shooters who also died during the shooting. Unfortunately, the phone was locked with a built-in anti-forensic technique that enforced encryption as well as an auto-wiping tool. To recover the data on the iPhone, FBI had to bypass the anti-forensic techniques with the help of Apple (Kharpal, 2016).

Kaspersky Lab (2017) experts, Global Research and Analysis Team, found a series of “invisible” targeted attacks. The purpose of the attackers was to hide their activities and make the

detection of the attack difficult to uncover. To do so, they used anti-forensic techniques and memory-based malware. Their traces were wiped from the system on the first reboot leaving forensic investigators with almost nothing to work with. More than 140 enterprises, including bank, government organizations, and telecommunication companies, in 40 different hidden countries were affected by the attacks (Kaspersky Lab, 2017).

Another example, according to Fox (2010), alleged Russian spies were arrested by the FBI. They were accused of encoding messages using Steganography into safe pictures. They did this by posting those safe pictures on public website, then extracting the coded messages from the computer data of the posted pictures, Experts market it as "the first confirmed use of this high-tech form of data concealment in real life" (Fox, 2010).

Furthermore, Holmes (2016), Managing Director of FTI consulting, stated that their computer forensics investigator, Bryan Lee, investigated the corporate employees. They wanted to check whether employees were stealing data or company funds, or whether they were committing fraud or involved in any suspicious activities. Since employees were aware of the investigation, most of them deleted their internet browser history to cover their tracks. Some employees used anti-forensics techniques to cover up illegal activities before their data was collected for the investigation. Not only was it time consuming, but it was very expensive to recover the deleted data.

As the use of anti-forensics techniques keeps increasing, it has become challenging for digital forensics investigators to perform their investigation. This is a big problem, therefore, strategies to detect them will be presented as well as some countermeasures.

Literature Related to the Problem

Garfinkel (2007) defined anti-forensics as tools and techniques that prevent digital forensics investigators from doing their job. These anti-forensics techniques are deleting or changing the data, inserting fake evidence, etc. He classified the anti-forensics techniques into four categories. First, the traditional anti-forensics which include overwriting data and metadata, cryptography, steganography, and so on. Second, there are anti-forensics techniques that minimize footprint; this category includes memory injection and syscall proxying, live cds, bootable USB tokens and virtual machines, and anonymous identities and storage. Third, there are anti-forensics techniques that exploit CFT bugs including failure to validate data, denial of service attacks, and fragile heuristics. Finally, there are anti-forensics techniques that detect computer forensics techniques which include countering forensic analysis with SMART, detecting network forensics (Garfinkel, 2007).

Pajek and Pimenidis (2009) explored the anti-forensics problems by comparing the computer forensics methodology to the anti-forensics, from both a theoretical and practical standpoint, in three different stages: elimination of source, hiding data, and direct attacks against computer forensics software. The Elimination of Source Stage can be done by deactivating tools that create the source or by wiping the log and disk. In the Hiding Data Stage, criminals hide the data in slack space such as hard drives. They can only use steganography or the encryption techniques to hide the data. In the direct attacks against Computer Forensic Software Stage, criminals compromise the computer forensics software. To do so, they might use the time stamp modification or the hash collision (Pajek & Pimenidis, 2009).

In his paper, Harris (2006) categorized the anti-forensics techniques based on various anti-forensics definitions. Harris compared the techniques proposed by Peron and Legary (2005, cited in Harris, 2006): destroy, hide, manipulate or prevent the creation of evidence; and those proposed by Rogers (2005, cited in Harris, 2006): data hiding, artifact wiping, trail obfuscation and attacks against the process and tools. By comparing and combining them, Harris came up with four categories: evidence destruction, evidence source elimination, evidence hiding, and evidence counterfeiting. Table 2 shows a detailed description for each category

Table 2

Classification of Common Anti-Forensic Methods

Name	Destroying	Hiding	Eliminating Source	Counterfeiting
MACE Alterations	Erasing MACE information or overwriting with useless data			Overwriting with data which provides misleading information to Investigators
Removing/Wiping Files	Overwriting contents with useless data	Deleting file (overwriting pointer to content)		
Data Encapsulation		Hiding by placing files inside other files		
Account Hijacking				Evidence is created to attempt to compromise the analysis of an image
Archive/Image Bombs				Evidence is created to attempt to compromise the analysis of an image
Disabling Logs			Information about activities is never recorded	

Furthermore, Littlefield (2017) provided an insight on how cyber criminals disrupt a forensic investigation. Just like Pajek and Pimenidis (2009) and Garfinkel (2007) pointed out, Littlefield also mentioned hiding data and destroying data techniques. For data hiding, techniques such as encryption, stenography, live CDs and virtual disks, and trail obfuscation can be used. Data can also be hidden within memory, slack space or hidden directories/partitions using slacker tool. For destroying data, disk cleaning and disk degaussing can be used. Littlefield also added other method such as physical intrusion detection, crime scene preservation, and legal thwarting. For physical intrusion detection, criminals can destroy the system using a USB zapper. However, this will not prevent the investigation, it will just make it harder and more time consuming for investigators to examine. For crime scene preservation, criminals leave false documentation and devices on purpose just to mislead an investigator. For legal thwarting, a criminal takes different precautions to exploit the legal boundaries such as creating enough doubt (Littlefield, 2017).

The de Beer, Stander, and Bell study (2015) study focused on identifying if digital forensics practitioners, from South Africa, can identify the use of anti-forensics in their investigation. In their study they also found various anti-forensics methods such as data hiding, data destruction, trail obfuscation, data contraception, data fabrication, and file system attacks. For each method, they identified the techniques as well as the tools that can be used. For example, for data contraception, the different methods that can be used are portable applications, live distros, syscall proxying, remote library injection, direct kernel manipulation, and utilizing “in-private” browsing on a web. As for the tools, for the portable application methods there are

tools like TrueCrypt and FTK Imager Lite. For Live distros method, Window CE and BartPE tools can be used.

Stamm and Liu (2011) presented a framework including various anti-forensic techniques designed to remove forensically significant indicators of compression from an image. To achieve their objective, they first developed a general framework that removes quantization fingerprints from an image's transform coefficients. After that, they used their framework to design some anti-forensics techniques to remove DCT coefficient quantization artifacts from JPEG compressed images and DWT coefficient compression artifacts from images compressed using wavelet-based coders. Their results showed the anti-forensic techniques proposed worked to erase the images without leaving any trace behind (Stamm & Liu, 2011).

Distefano, Me, and Pace (2010) researched anti-forensic techniques applied to mobile devices, specifically Android devices. First, they outlined the various techniques currently available for Android forensics: Android Debug Bridge (ADB), Nandroid backup, physical imaging by dd, commercial tools, serial commands over USB, simulated SD card, and software application. They then talked about the traditional anti-forensics techniques such as destroying evidence, hiding evidence, eliminating evidence sources, and counterfeiting evidence. Finally, for each traditional anti-forensics techniques, they developed a related feature exploiting the Android Application framework. These techniques were Android destroying evidence, Android hiding evidence, Android eliminating evidence sources, Android counterfeiting evidence (Distefano et al., 2010).

Sun, Weng, Lee, and Yang (2011) presented an anti-forensic steganography method that can embed and extract messages from images. To achieve high efficiency, high quality, and large

embedding ratios, their work presented two novel anti-forensics approaches of steganography : the highlight of EMD (HoEMD) and the adaptive EMD (AdEMD). The HoEMD included Embedding-Procedure and Extracting-Procedure. The AdEMD included Data Embedding and Data extracting (Sun et al., 2011).

As presented by Azadegan, Yu, Liu, Sistani, and Acharya(2012), many forensics tools follow the same steps to retrieve data from a smartphone. Detection of forensics tools enables various scenarios. Three anti-forensics approaches that can be used to weaken the data extraction process from smartphones were presented. These approaches were Sudden Death, Erase Sensitive Data, and Replace all Data (Azadegan et al., 2012).

Brand (2007) highlighted the growing sophistication of anti-forensic techniques used by malicious software or malware. Brand's research discussed the various anti-forensic techniques used by malware. These techniques include trail obfuscation, anti-disassembly, encrypted and compressed data, data destruction, anti-debugging, and so on. He also mentioned that automated detection and classification work is progressing in the forensics field. These include statistical structures such as assembly instructions, system calls, system dependence graphs, and classification through machine learning.

Geiger's (2005) paper focused on analyzing the performance of six anti-forensic tools, these tools were Window Washer, CyberScrub Professional, SecureClean, Evidence Eliminator, and Acronis Privacy Expert. To do so, Geiger analyzed the six anti-forensic tools by observing the tools' performance, then by examining the disk images using FTK (Forensic Tool Kit). The results showed that significant shortfalls were found in each anti-forensic tool examined which could benefit forensics investigator with data recovery.

In his study, Gogolin (2010) examined the level of digital crime experience and investigative capabilities of law enforcement in Michigan. To obtain the data needed, Gogolin interviewed members of the Michigan Sheriff Departments, The results of the study argued that the law enforcement was also facing some challenges when dealing with digital crime.

Sremack and Antonov (2007) defined anti-forensics as any activity that intentionally aims to deceive or impede the investigation. Then they identified two classes of threats than anti-forensics cause—threats to digital evidence and threats to legal process/admissibility. For digital evidence threats, they identified four main classes of threats as well as two subclasses for each class. Those classes were data preservation, data counterfeiting, data hiding, and data destruction. The subclasses were physical and technical. Finally, they created a taxonomy with the four classes, subclass, as well as an example for each. Table 3 represents their taxonomy.

Table 3

Digital Evidence Anti-Forensics Taxonomy

Class	Subclass	Example
Evidence Preservation	Technical	Prevention from writing to hard drive.
Evidence Preservation	Physical	Installation of data gathering equipment that does not communicate with host network, such as a silent sniffer.
Evidence Destruction	Technical	Deletion of log file entries.
Evidence Destruction	Physical	Chemical, magnetic, mechanical destruction of media containing evidence.
Data Hiding	Technical	Use of encryption or steganography.
Data Hiding	Physical	Use of smart cards or hardware cryptographic modules.
Evidence Counterfeiting	Technical	Creation of misleading log file entries
Evidence Counterfeiting	Physical	Physical replacement of system hard drive with a ghost image of the original hard drive with nonincriminating digital evidence

For the legal process threat, Sremack and Antonov (2007) identified four classes out of several classes that exist. The four classes were sufficient doubt, crossing jurisdictions, privacy, and significant changes in scientific foundation. Then, they created a taxonomy with the four classes as well as an example for each class. Table 4 represent their taxonomy.

Table 4

Legal Process Anti-Forensics Taxonomy

Class	Example
Sufficient Doubt	Perform crime from publicly-accessible or virus-infected computer.
Crossing Jurisdictions	Perform crime from a jurisdiction with no extradition and no working relationship with target jurisdiction.
Privacy	EU laws prevent certain EU citizen personal data from being sent to non-EU countries.
Significant changes in Scientific Foundation	Recent proofs in weakness in SHA-1 and MD5.

Literature Related to the Methodology

Garfinkel (2007) proposed some techniques on how to overcome or detect the anti-forensic techniques. Garfinkel stated that "Many of the anti-forensic techniques discussed in this paper can be overcome through improved monitoring systems or by fixing bugs in the current generation of computer forensic tools." Other solutions proposed were positioning data to prevent the cybercriminal from overwriting it, replacing weak file identification heuristics with stronger ones, and recovering cryptographic passwords and keys by using spyware.

Preventative Anti-Computer Forensics (PACF) framework was proposed by Simmons (2011). The PACF framework includes five components: acquisition, analysis, presentation,

deterrence, and baseline. The acquisition component is used to guarantee the integrity of the captured data. The analysis component analyzes the data captured to seek for relevant data. The presentation component is used to record all the results without deleting anything. The deterrence component helps the investigator understand the objective of the computer criminal, which can benefit the investigator in staying ahead. The baseline component presents a historical data for the machine learning process (Simmons, 2011).

Eoghan, Fellows, and Geiger (2011) discussed the severity of how the increase use of FDE (Full Disk Encryption) has been significantly affected digital investigators. Because the use of FDE prevent the evidence collected to be accessed, Eoghan et al. (2011) addressed this problem. They talked about all the challenges that FDE causes during an investigation and about some techniques on how to collect data from a crime scene in an unencrypted state.

Harris (2006) mentioned that anti-forensics methods leans on the vulnerabilities of the forensics process, therefore the forensics process should be more resistant. However, even with higher resistance, the anti-forensics methods will not be prevented completely but will only be minimized. This can be done by individually targeting each method. First, the human element—an investigator should be alert, educated, experienced, and an analytical thinker which could be beneficial during an investigation. Second, dependence on tools—an investigator should use various, accurate and effective tools. Finally, physical/logical limitations—investigators should have access to new and updated software and hardware that can help them identify new anti-forensics methods. Table 5 below provides a detailed description for each method.

Table 5

Exploits of the Methods

Name	Human Element	Tool Dependence	Physical/Logical Limitations
MACE Alteration	Investigator may assume accuracy of dates and times	Tools may not function with invalid or missing dates and times	Invalid dates and times make collating information from multiple evidentiary sources difficult or impossible
Removing/Wiping Files	Investigator may fail to examine deleted files	Methods of restoring deleted files are specific to the tool- so effectiveness may vary	Time required to restore wiped file contents may outweigh the evidentiary value of the data it contained
Account Hijacking	Investigator may fail to consider whether the owner of the account was actually the person at the keyboard	Tool may not be capable of extracting information that would aid investigator in determining who is in control of the account	Zombied computer accounts may produce so much indirection that it is almost impossible to actually find the origin of an attack. Lack of detailed information may keep investigator from determining actual account user
Archive/Image Bombs		Improperly designed software may crash	Useful information might be located in the bomb itself, but outside the logical limitations of the investigator's system
Disabling Logs	Investigator may not notice missing log records	Software may not flag events that indicate logging was disabled	Missing data maybe impossible to reconstruct

Littlefield (2017) stated that within the different phases of a computer forensics investigation (collection, examination, analysis, and report), the collection phase is where the anti-forensics method occurs. Littlefield gave multiple pieces of advice to investigators when at a crime scene. First, investigators have to move unauthorized people from computers and power supplies. Second, investigators should always take pictures and videos of everything at the crime scene. Third, computers should always be switched off with no main power source. Finally, everything found at the crime scene should be collected.

Shaw and Browne (2013) argued how digital forensics investigations have been conducted on an informal basis for many years. When the triage is conducted poorly, it can lead to unclear results. Shaw and Browne gave a high-level overview of how the system works and how it can be deployed in the digital forensic laboratory

Thuen's (2007) study focused on understanding the anti-forensics techniques used to determine a solution for solving thwarting. Thuen gave recommendations of how to secure and preserve a crime scene since most anti-forensics methods occur there. Some of the recommendations were removing and restraining unauthorized people from entering the area, collecting all evidence found, and taking photographs of everything. He also discussed different anti-forensics methods for hiding data and provided tools to detect them. For example, for steganography, the Stegdetect tool can be used to detect it.

Smith (2007) studied the different categories used to classify anti-forensics methods and then added important information about understanding disk-avoiding anti-forensics tools. Disk-avoiding tools comprise a category of the data contraception method. Data contraception is the method used to prevent data from being stored on a disk. Smith classified the disk-avoiding tools into five categories: syscall proxying, memory resident compiler/assemblers, remote library injection, direct kernel object manipulation, and LiveDistros. These tools present significant challenges to forensic investigators and understanding the tool would be beneficial.

Kessler's (2007) study described some of the many anti-forensics tools and method such as data hiding, artefact wiping, trail obfuscation, and attach on the forensics tools themselves. Kessler stated that even though anti-forensics is mostly used by criminals, in some cases it can also be used in a legitimate use for those who want to protect their privacy. He mentioned that

some anti-forensics method user does not want to prevent forensics analysis form occurring, they just want to slow down the investigation process until the data loses its value (Kessler, 2007).

de Beer et al. (2015) conducted a survey for the purpose of finding out whether the use of anti-forensic is affecting the ability of South African digital forensic practitioners to complete digital forensic investigations. They selected their respondents based on their current sectors (law enforcement, private sector, or corporate), and their demographic. Some of the questions on the survey were familiarity with anti-forensics techniques, familiarity with anti-forensics tools, anti-forensics techniques that mostly affect an investigation, and anti-forensics tools mostly found during an investigation.

Table 6

Familiarity with Anti-Forensics Techniques

Techniques	Data Hiding	Data Destruction	Trail Obfuscation	Data Fabrication	File System Attacks	Data Contraception	None of the Above
Awareness	71.4%	68.6%	31.4%	22.9%	22.9%	14.3%	11.4%

Table 7

Familiarity with Anti-Forensics Tools

Tools	Data Wiping & History Removal (CCleaner, Eraser etc.)	Encryption Tools (Truecrypt etc.)	Steganography Tools (Qquickstego Etc.)	Times To Mp (By Metasploit)	Rootkits	Transmogrify (By Metasploit)	The Complete A-Z Of Open Source Tools Out There
Awareness	89.0%	77.1%	40.0%	28.6%	11.4%	8.6%	2.9%

The results from the de Beer et al. (2015) showed that the most known techniques were data hiding and data destruction, and the most known tools were data wiping and history removal

(CCleaner, Eraser, etc.) and encryption tools (Truecrypt etc.). For the techniques that mostly impact their investigations, the results showed data destruction and data hiding. As for the tools, the result showed Transmogrify (by Metasploit), data wiping and history removal (CCleaner, Eraser, etc.), and encryption tools (Truecrypt etc.) .

The goal of the Rekhis and Boudriga study (2010) was to develop a theoretical technique of digital investigation which copes with anti-forensic attacks. Then, develop a formal logic-based model which allows you to describe complex investigated systems and generated evidences under different levels of abstractions, and finally extend the concept of visibility to characterize situations where anti-forensic attacks would be provable and traces regarding actions hidden by these attacks would become identified.

Böhme and Kirchner (2013) introduced a theoretical framework to define counter-forensics (also known as anti-forensics). The framework was then extended to include forensic analysis, authentication requirements, and roles of image models regarding the forensic decision problem. A terminology was then created through a technical survey of counter-forensics against image forensics with a focus on trace suppression and authentication interference; examples and brief evaluations were provided, along with a discussion of relations to other domains in multimedia security.

McLeod (2014) provided a demonstration about the forensic duplication process. McLeod argued that even though the rensic duplication process may not directly modify data on the evidence hard disk, a hard disk will usually modify itself during the forensic duplication process. He provided suggestions to help minimize the changes made to. the hard disk during the forensic duplication process

Afonin, Nikolaev, and Gubanov (2015) discussed some of the anti-forensic techniques used by non-expert criminal and also suggested some countermeasures that can be used during an investigation.

Sremack and Antonov (2007) emphasized on the issue that if anti-forensics were to flourish then, evidence will fail the Daubert standard. To resolve this challenge with anti-forensics, Sremack and Antonov suggested a classification of anti-forensic threats on digital forensics and on legal process. A robust taxonomy was then created with the goal of accounting for all types of investigations such as internal, civil, and criminal in addition to threats such as threats to digital evidence and threats to legal process/admissibility. They acknowledged that their taxonomy has limitations in scope, and that, in the future, they would expand their taxonomy, investigate social threats to forensics, and develop better controls for the forensic process.

Park, Park, Kim, Cheon, and James (2017) attempted to assess the problem of anti-forensics techniques commonly deployed in South Korea. First, they identified the challenges that anti-forensics techniques were causing. They then proposed a way to detect anti-forensics techniques, which can be beneficial for digital investigators. Finally they designed a prototype that would help with the detection of anti-forensics techniques.

In their study, Wundram, Moch and Freiling (2013) researched new attacks that can occur on digital forensics tools. Among the attacks they found that SQL Injection Attack was one of them as it can allows to infiltrate the analysis system. Furthermore, they argued that forensics tools need to overcome this attack and discussed some countermeasures.

The Qian and Zhang (2014) study highlighted a method for differentiating the uncompressed image from the anti-forensically processed image. Qian and Zhang looked at the noise distributions which are abnormal in the resulting images and looked at the quality of the processed image, which is poor compared with the original image. As a solution, Qian and Zhang proposed an improved anti-forensics method for JPEG compression

Summary

Many authors have studied and discussed computer anti-forensics techniques. This chapter reviewed previous studies on anti-forensics methods, tools and techniques, and why anti-forensics is a problem for forensic investigation. Some of the common anti-forensics methods found were data hiding, data destruction, trail obfuscation, and direct attacks against forensics tools. The chapter also reviewed various methodologies that various authors have presented, from when collecting the evidence at the crime scene to different tools that can be used to detect the anti-forensics techniques. Even though many authors have studied and discussed computer anti-forensics tools, new methods are being developed each day by cybercriminals. Further work on the topic will be beneficial to provide greater insight. The following chapter is a detailed methodology used for this study

Chapter III: Methodology

Introduction

The purpose or objective of this study was to perform in-depth research on some of the many anti-forensics' techniques or tools, then present strategies to detect them, and finally, discuss some countermeasures.

Some of the questions that needed to be researched answered to achieve the objective were:

1. What are the different types of Anti-forensics techniques?
2. Which method and tool can be used for each technique?
3. What are some countermeasures ?

The above questions helped provide guidance for the kinds of data that needed to be collected, analyzed, and interpreted. So, to make sure the questions above were answered accurately, and that the outcome desired was obtained, an in-depth research was done on the topic using different methodologies.

In this chapter, a detailed methodology will be described. The methodology will include how the information was gathered and generated as well as which specific techniques and procedures were utilized when analyzing the data. This chapter will be classified as follows: (a) design of the study used, (b) type of data collection used, and (c) tool and techniques used.

Design of the Study

Research methods can be divided into two methods—quantitative and qualitative methods. According to DeFranzo (2011) "Qualitative research is primarily exploratory research. It is used to gain an understanding of underlying reasons, opinions, and motivations. It provides insights into the problem or helps to develop ideas or hypotheses for potential quantitative

research." DeFranzo further stated: "Quantitative Research is used to quantify the problem by way of generating numerical data or data that can be transformed into usable statistics."

A qualitative approach gives the researcher a unique in depth understanding on the research topic, it is valuable in providing a rich description of complex phenomena. For this study, a qualitative approach will be used by creating a taxonomy to organize and interpret the data.. This approach is more suitable for this study because this study will be an in-depth research of various anti-forensics techniques and tools. Data will be collected from books, articles, magazines, newspapers, and so on. The data collected will be read through and assigned into different categories.

Data Collection

There are two types of data collection—primary data and secondary data. Primary data can be defined as data collected from first-hand sources. This includes data gathered from interviews, surveys, questionnaires, and so on. Data collected from primary data is more valid and accurate, however it can be quite expensive and time consuming compared to secondary data collection. Secondary data can be defined as data collected from a source that has already been published. It can be obtained from books, articles, journals, newspapers, and so on. For this study, both primary and secondary data were used for data collection.

To collect primary data, an interview was conducted. There are three types of interviews that researchers can choose from, The three types are Structured Interview, Unstructured Interview, and Group Interview (McLeod, 2014). First, Structured Interview (known as Formal Interview), "the questions are asked in a set/standardized order and the interviewer will not deviate from the interview schedule or probe beyond the answers received" (McLeod, 2014).

Structured Interviews consist of closed-ended questions, Second, in Unstructured Interviews (known as discovery interviews or informal interview), the questions are more like a conversation and not as strict as the structured interview. These questions are open-ended questions. Finally, Group Interview (known as focus group) “refers to interviews where a dozen or so respondents are interviewed together” (McLeod, 2014).

The type of interview that was done was an Informal Interview, Unstructured Interview. There was flexibility in the questions that were asked, meaning the questions kept changing depending on the interviewee’s answers. This type of interview was chosen because it increases the validity of the data collected as it allows the interviewer to ask for a deeper understanding on some unclear questions. It also allows the interviewee to answer with as much detail as they like and also using their own words.

The interviewee was a Senior Information Security engineer that works for the SOC (Security Operation Center) team at Mayo Clinic in Rochester, Minnesota. Part of his job includes doing digital forensics investigations. A lot of open-ended questions were asked during the interview, but, because with the organization policy, he was not able to answer all the questions asked due to privacy issues. However, sufficient information was collected from the interview.

To collect secondary data, different books on the topic were carefully read to find the accurate information. Different academic search engines were used such as Google Scholar, Microsoft Academic, Semantic Scholar, and many others. These sites were used because not only are they free, but they often provide links to full text PDF files.

With so much data available, different keywords were used to narrow the search and to help obtain the most relevant published sources. Some of the keywords used were anti-forensics, anti-forensics techniques, tools, taxonomy, digital forensics, and more. These keywords generated a lot of sources, some were relevant and some not so much. So, it is important to look further into each source because even if some of the sources are not relevant, they might reference more relevant sources.

Tools and Techniques

As previously mentioned, data was collected through conducting an interview as well as researching for some sources using different keywords. However, the data collected still needed to be processed and analyzed.

The tools and techniques used were as follows:

Primary Data Collection Process:

- Thinking about the research questions and writing down some questions that needed to be answered during the interview.
- Picking the right interviewees—forensics investigators.
- Reaching out to them about the research topic and asking them for a permission to interview them.
- Waiting for an approval to participate in the interview.
- Setting up a meeting with those that responded.
- Interviewing the respondent and writing down everything.
- Reviewing the data collected for relevancy and adding it to the research.

Secondary Data Collection Process:

- Researching and gathering data using different keywords.
- Organizing the data gathered and adding some side notes when necessary.
- Reviewing the data with reliable sources.
- Excluding data that is not relevant.
- Reviewing if the data collected answered the objective of this study.
- Using the data in this research.

Summary

In this chapter, a detailed methodology was described. The methodology included how the information was gathered and generated as well as which specific techniques and procedures were utilized when analyzing the data. For the design of the study, the framework used was a qualitative method. This approach was more suitable for this study since it consists of creating a well detailed taxonomy. For data collection, both primary and secondary data collection were used. Finally, a description of the tools and techniques used was also included. The following chapter will be an actual presentation of all the data collected.

Chapter IV: Data Presentation and Analysis

Introduction

It has become challenging for digital forensics investigators to overcome the increasing use of anti-forensics tools and techniques. Criminals are becoming aware of the digital forensics tools and techniques hence making the anti-forensics tools and techniques more sophisticated.

Anti-forensics appears to be a growing problem to digital forensics; this requires digital forensics investigators to keep themselves updated about the current anti-forensics tools, techniques and countermeasures.

In this chapter, a taxonomy will be created. The taxonomy will classify anti-forensics into different levels and different categories: WHERE, WHICH, WHAT, and HOW. The WHERE level will indicate where anti-forensics can occur during an investigation. The WHICH level will indicate which anti-forensics techniques exist. The WHAT level will define the exact method used for each technique. The HOW level will indicate the tools used.

Data Presentation

As mentioned above, the taxonomy will include four different levels: WHERE, WHICH, WHAT, and HOW.

Table 8

Levels of the Taxonomy

Levels	Indicator	Function
Level 1	Where	Indicate ‘Where’ anti-forensics can occur
Level 2	Which	Indicate ‘Which’ anti-forensics techniques exist
Level 3	What	Indicate ‘What’ method can be used for each technique
Level 4	How	Indicate ‘How’ tool used for each method

The first level is WHERE. This level will be describing where anti-forensics techniques can be found during an investigation. Anti-forensics can occur on data and on forensics tools.

The second level is WHICH. This level will cover which anti-forensics techniques exist for data and for forensics tools.

- For Data, there is data destruction, data hiding, and trail obfuscation.
- For Forensic tools, there is forensic software.

The third level is WHAT. This level will describe the different methods used in each technique.

- For data destruction, there is data wiping and physical destruction.
- For data hiding, there is encryption, steganography, program packer, and hiding data in the system area.
- For trail obfuscation, there is file headers manipulations, timestamp modification, and log deletion and modification.
- For forensic software , there is timestamp modification and hash collision.

The fourth or final level is HOW. This level will indicate the tools used for each method.

- For data wiping, the tools used are DBAN, CBL Data Shredder, Eraser, HDShredder, HDDErase.
- For physical destruction, the tool used are degausser, Crushers & Destroyers, Hard Drive Shredders, Disintegrators.
- For encryption, the tool used are BitLocker, FileVault2, LUKS, Veracrypt, 7-Zip, DiskCrypto, Encrypto, AESCrypt.

- For steganography, the tools used are Xiao Steganography, Image Steganography, Steghide, crypture, SteganographX Plus, rSteg, Camouflage, and OpenStego.
- For program packer, the tools used are Ultimate Packer for Executables(UPX), Exe Stealth Packer, PELock, CExe, Amadillo, dotBundle.
- For hiding data in the system area, the tools used are BMAP and slacker.
- For file headers manipulations, hex workshop, FITS4Win2, and Jhead are the tools that can be used.
- For timestamp modification, the tools are SKTimeStamps, NewFileTime, Time Stomp, and Change Timestamp.
- For log deletion and modification, CCleaner, BitRaser, and Auto deletion are the tools used.

Figure 1

Taxonomy

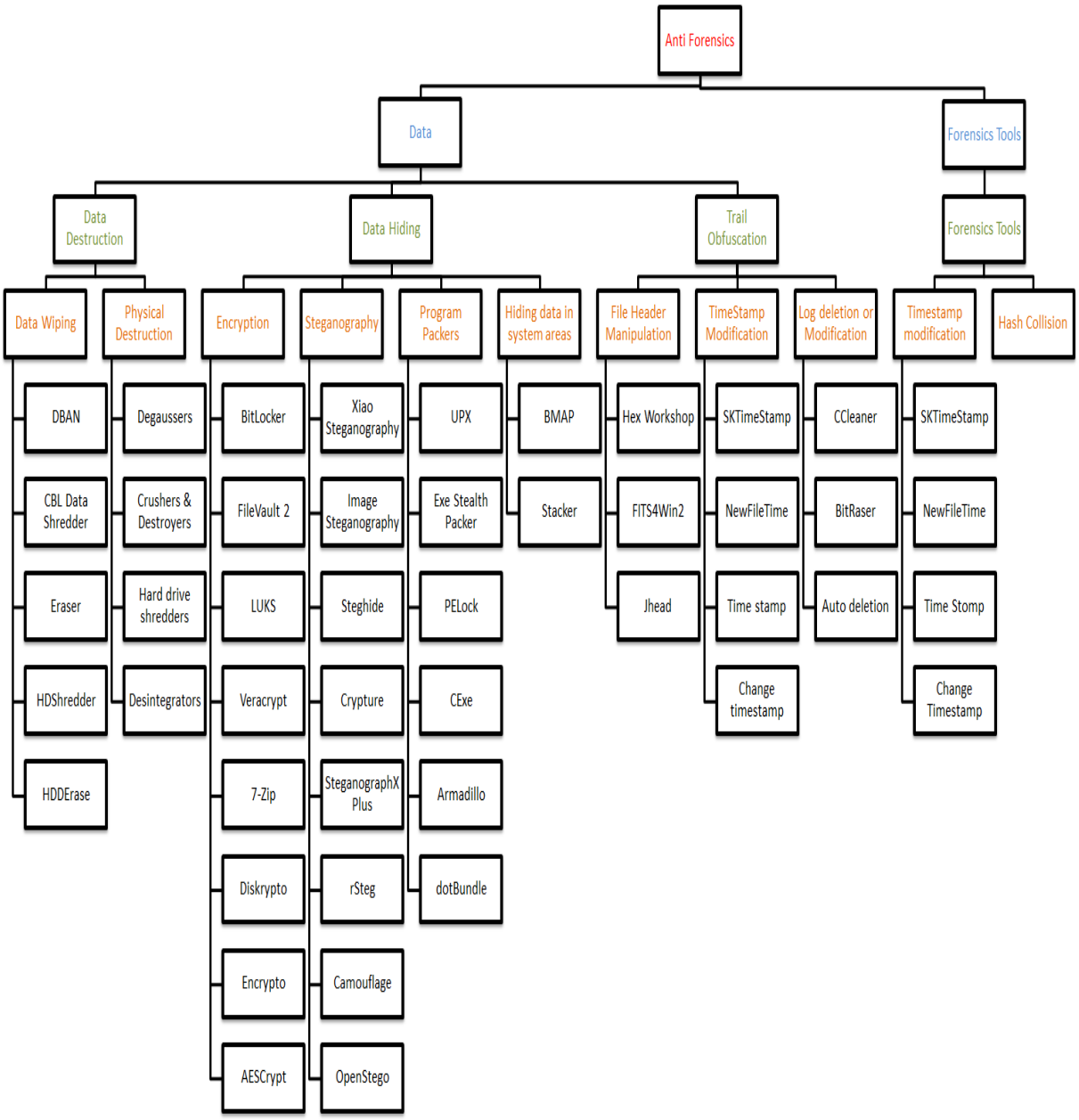


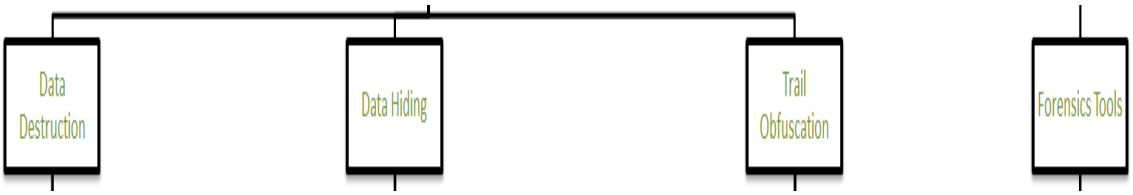
Figure 2

Level 1 of Taxonomy

Level 1: This is where anti-forensics can be found (Figure 2)

Figure 3

Level 2 of Taxonomy



Level 2: This indicates which anti-forensics techniques exist (Figure 3)

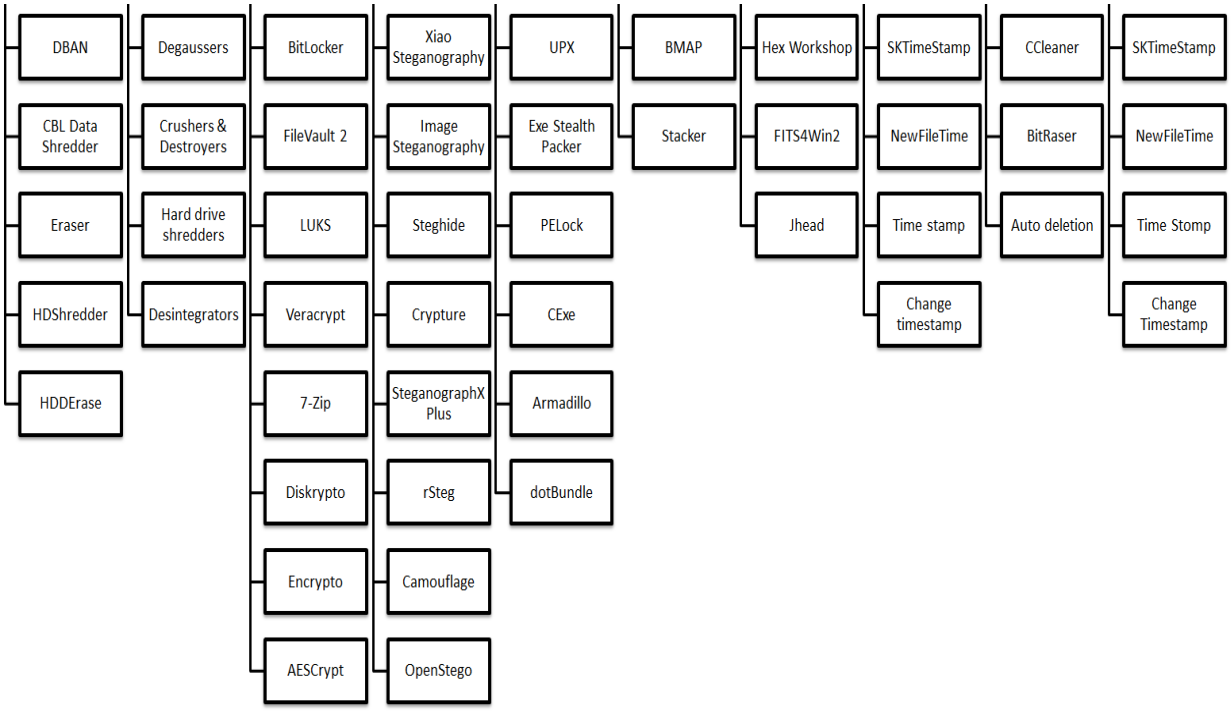
Figure 4

Level 3 of Taxonomy

Level 3: This indicates the method or methods that can be used for each technique (Figure 4)

Figure 5

Level 4 of Taxonomy



Level 4: Indicates the tool or tools used for each method (Figure 5).

Data Analysis

For data analysis, a detailed description on each level of the taxonomy will be presented below. Each method, technique, and tools will be described below.

Data

Data can be defined as information processed or stored by a computer (Data, n.d.). This information may be in the form of text documents, images, audio clips, software programs, or other types of data. Anti-forensics occurs on data by destroying data (data destruction), hiding data (data hiding), and trail obfuscation

Data destruction. Data destruction is the process of destroying data stored on tapes, hard disks and other forms of electronic media so that it is completely unreadable and cannot be accessed (Blancco, n.d.). This can be done by simply wiping the memory buffers or by overwriting data on the disk repeatedly. Data destruction has two techniques, data wiping and physical destruction.

Data wiping. Data wiping is done by securely deleting files. This is done by overwriting the clusters occupied by those files with null characters or some random characters such as data or numbers. According to (Poonia, 2014), two methods can be used for data wiping. Those methods are Data Sanitization method and File Shredder method. The Data Sanitization method occurs when data on a hard drive is overwritten using a software. The File Shredder method is when the file on any storage device, such as a hard disk, is permanently deleted.
The tools used for Data wiping are DBAN, CBL Data Shredder, Eraser, HDShredder, and HDDErase.

DBAN (Darik's Boot and Nuke) is a free open-source data wiping software. It can work by simply creating a bootable CD using any burning program such as CDBurnerCP or using a flash drive as pendrive and then booting the computer directly from the bootable CD or pendrive (Kishore, 2011). This is an example of a software that can be used using the data sanitization method.

CBL Data Shredder is a free data destruction program that permanently deletes data stored on the hard drive. It is a very flexible program as it can be run from both inside and outside windows. it can be used by either creating a bootable CD or Pendrive, or by just running it as a regular program for wiping (Fisher, 2020b).

Eraser is a data destruction tool for windows operating systems only. It works by overwriting data stored on a hard drive using carefully selected patterns.

HDShredder is a data destruction program that deletes completely everything that resides on a hard drive. It can work by either installing it like a regular windows program or by booting from it using an ISO file (Fisher, 2020a).

HDDErase is a bootable data destruction program that works by running off a disc, like a CD or DVD, or floppy disk. It can erase both the operating system and also everything running on the c:drive since it starts running before the operating system is loaded (Fisher, 2019).

Physical destruction. Physical destruction is the process destroying or crushing all data on a hard drive. Physical destruction can be done using degaussers, crushers and destroyers, hard driver shredders, or disintegrators.

Degaussers are magnetic media erasure devices that are compliant with all certifications and NIST 800-88 guidelines for sanitization (Destructdata. 2018). They destroy data by sweeping the drive with a powerful magnet leading the data to be unstable. There are different types of degaussers available. For example, there is a HD-3WXL Hard Drive Degausser, HD-2X Hard Drive and Tape Degausser, and so on.

Crushers and destroyers are tools that destroy a hard drive. There are fully automatic and manual models available. An example of the automated crushers is the MODEL HDDC-A. This model uses a solid conical anvil to exert up to six tons of pressure on hard drives (Ontrack, 2018).

Hard drive shredders are electronic media shredding machines. they were designed to physically destroy computer hard disks, copier hard drives, back-up tapes, DVD’s and assorted

e-waste (Ontrack, 2018) . Low Volume Hard Drive, SDD and Combo Shredders and Mid Volume Hard Drive, SSD and Combo Shredders are some of the shredders available.

Disintegrators are also machines used for physical destruction. There are different models of disintegrators including Model 200 Office Disintegrator, Light Model 3 Disintegrator, Medium Model 22 Disintegrator, and so on (Destructdata, 2018).

Data hiding. Data hiding is a method of packing data in irrelevant areas where it cannot be found. Moreover, this practice does not delete any relevant data, but hides it in such a way that seeing it and examining it is very challenging or impossible. Data hiding has four major techniques that differ from one to another, which are Encryption, Steganography, Program packers, and Hiding data in system areas.

Encryption. Encryption is a method of using an algorithm to protect data by scrambling it and making the data either unintelligible or undetectable. Encrypted data looks meaningless and is extremely difficult for unauthorized parties to decrypt it without the correct key.
There are 35+ free tools used for Encryption, some of them are BitLocker, FileVault 2, LUKS, Veracrypt, Z-Zip, DiskCryptor, Encrypto, and AESCrypt (Anon, 2018).

BitLocker is a full disk encryption tool for Windows. It comes preinstalled on most Windows computers and uses 128 or 256 bit AES (Advanced Encryption Standard) to encrypt all the data on the hard drive.

FileVault 2 is also a full disk encryption tool. The difference between FileVault 2 and BitLocker is that FileVault 2 is for MacOS only while BitLocker is for Windows. It works by encrypting all the data and uses a password for decryption.

LUKS (Linux Unified Key Setup) is a hard disk encryption tool for Linux. It allows users to transport and migrate encrypted data and to also manage multiple passwords

VeraCrypt is an encryption tool available for Windows, OS X, and Linux. It uses 256 bit AES (Advanced Encryption Standard) encryption by default, however, other methods can be used such as Serpent and Twofish. VeraCrypt is flexible as it enables you to choose what to encrypt.

Even though 7-Zip is a lightweight file archiver, it is also a strong file encryption tool. It is available for Windows, OS X, and Linux even though the official download is for Windows only. 7-Zip can encrypt one to multiple files at once.

DiskCryptor is an encryption tool for windows .The methods for encryption that it offers AEC, Twofish, and Serpent. The benefits of using DiskCryptor is that not only it is user friendly (easy to use) but it also encrypts quickly and also supports external devices encryption such as USB drives and DVDs.

Encrypto is a file encryption tool and it works by encrypting files before those files are sent via email, instant message, cloud sharing and so on.

AESCrypt is also a file encryption software that allows you to encrypt both files and folders. It is available for Windows, Android, MacOS, iOS, Linux, and Python.

***Steganography*.** Steganography is hiding data inside other data where the presence is not obvious or evident to the forensics investigator. This technique has a high adaptability to hide any kind of data. Moreover, this technique is very hard to detect which makes it difficult and challenging for digital investigators.

Just like for Encryption, there are also a lot of tools used for Steganography. Some of the tools are Xiao Steganography, Image Steganography, Steghide, Crypture, SteganographX Plus, rSteg, Camouflage, and OpenStego (INFOSEC, 2019).

Xiao Steganograhy is free and easy to use software for hiding data. It works by hiding secret files in BMP images or in WAV files. The advantage of this tool is that it also supports encryption.

Image Steganography is also free and can be used to hide information in image files. Any information such as text message, file, and so on , can be hidden in an encoded image. The output will look just like a regular image; however the image contains the secret data.

Steghide is also like image Steganography; however, with Steghide ,you can hide data not only in an image but also in an audio file. Steghide is a command line software meaning you need to learn the right command to use it.

Crypture is also a tool used for hiding secret data. Just like steghide it is also used in the command line. The disadvantage of using this tool is that the file you want to hide should be eight times smaller than the BMP file , making it useful for only small data.

Steganography plus works just like Crypture. It lets you hide just small confidential data inside a BMP image.

Rsteg is also a hiding data tool that is Java based. It allows you to hide textual data inside an image as well.

Camouflage is a tool that allows you to hide any type of file inside another file. Not only is it easy to use but it does not restrict you on any kind of file you want to hide.

OpenStego also allows you to attach any kind of confidential message file inside an image file. The input is hiding images in BMP, GIF, JPEG,PNG, and so on. The output is a PNG file.

***Program packers*.** Program Packers is encrypting and compressing an attack program and then integrating the file in a new 'packed' file that is wrapped with a suitable extractor. When the apparently safe process is running then simultaneously the packed attack application is then running.

There are many tools used to pack the files. The most used are Ultimate Packer for Executables(also known as UPX). Exe Stealth Packer, PELock, CExe, Armadillo, and dotBundle (The-Shadow-Fiend, 2016).

UPX (Ultimate Packer for Executables) is a software Packer. UPX works by taking an executable, compress it, and pack the compressed code into another section of the executable (Lamb, 2017).

Exe Stealth Packer is another packer tool. With this tool, you can pack a lot of files in one executable packer file.

PELock is a software that provides users with a simple means of protecting their executables. It works by generating keys with support for creating backups.

CExe or EXE Packer also works by compressing executable files (type EXE) or DLL-files.

Armadillo is a commercial protection for any Win32 program, it works just like any other packer.

DotBundle is a compressor/packer software for NET executables. It works by merging all the files into one single executable.

***Hiding data in system areas*.** Hiding data in system areas is a data hiding technique, which hides data that is reserved as system space or file slack. File slack or system space is an area between the logical file date and the end of the cluster. slack space is created when a file system allocates space for a file to be written. The tools used for this method are bmap and slacker.

Bmap is a data hiding tool that can use slack space in blocks (containers in a file system that store data) to hide data. When data is hidden in slack space, it makes it impossible for forensics tools to detect it (Computer Security Student, n.d.).

Slacker is a tool that is used to hide data in the slack space of NTFS. This tool works by breaking up a file into multiple pieces of files then placing each piece into another file's slack space. By doing so, it hides it from the forensic examination software.

Trail obfuscation. Trail Obfuscation is the deliberate activity to disorient and divert a forensic investigation on a digital system or network (Conlan et al., 2016). The trail obfuscation techniques include file headers manipulation, timestamp modification, and log deletion or modification.

***File header manipulation*.** Although manipulations of extension do not make any difference for forensic software, manipulation of file headers may potentially mislead forensic software. The tools used for this are Hex workshop, FITS4Win2, and Jhead.

Hex workshop is a tool used for editing files consisting of a set of hexadecimal development for windows. With the tool, you can edit, copy, cut, paste, insert, fill and delete binary data.

The FITS4Win2 header data is a free tool that can edit a file header. With the tool, you can bulk load, view, search, and update headers.

Jhead is a Digicam JPEG Exif header manipulation tool. It is used to display and manipulate data contained in the Exif header of JPEG images from digital cameras (Jhead, n.d.).

Timestamp modification. Computer forensics packages read every file's MACE (responsible to record Modification, Access, Creation timestamps of the file) values and give an indication to examiners about time and date issues of any updates and changes to the contents of a file (Pajek & Pimenidis, 2009). However, the values can be manipulated causing the real time and date stamps to not display correctly in computer forensics software. The tools used are SKTimeStamp, NewFileTime, Time Stomp, and Change Timestamp.

SKTimeStamp is a simple Explorer extension tool that is used to change the timestamps of any file. This tool provides a very simple way to manipulate or modify the timestamps (Williams, 2014).

NewFileTime is a timestamp manipulator tool for windows . With this tool, you can easily access any file and folder on your windows system then manipulate any of the timestamps on them (SoftwareOK.com, 2020).

Timestomp is a tool that can be used to modify or change the timestamp. Timestomp can be used on different platform such as Windows, Linux and macOS (MITRE/ATT&CK, 2015).

Change Timestamp is also a tool that allows you to quickly manipulate the timestamp of any file. This tool does not require any installation. To change the date and time of a file, you only need to open the tool and drag and drop the file (Other Government Agencies, 2017).

***Log deletion or modification*.** Log deletion or modification can be done to hide log entries that would identify the identity or action of the perpetrator. Deleting or modifying log files in a secure way can be done using various tools such as CCleaner, BitRaser, and Auto deletion

CCleaner is a program that can be used to delete log files on windows. With this tool you can easily scan your windows computer and app log files then delete them all at once (Flournoy, 2018).

BitRaser is a tool that permanently deletes hard drives, servers, desktops and so on. The tool completely gets rid of any trace left behind including log files. The data deleted can never get recovered.

AutoDeletions is a free windows tool that can permanently delete log files. This tool can delete a batch of log files at once. Not only AutoDeletion is easy to use but you can also set it up to follow a specific schedule (Andreo, 2014).

Forensics Tools

Forensics tools are the main tools that the digital investigators use during an investigation to examine if any suspicious incident had occurred. There are different forensics tools that can be used: ProdDiscover forensic, volatility framework, the sleuth kit (autopsy), and so on. Anti-forensics occurs on forensics software.

Forensic software. The investigators use different forensics software such as Autopsy, AXIOM, and FTK, during an examination. However, since nothing is 100% secure, computer criminals attack these computer forensics software. They attack the computer forensics software by exploiting them and using their vulnerabilities against them. There are two main methods on how computer forensic software can be compromised: time stamp modification and hash collision.

Timestamp modification. Just like on data, time stamp modification can also occur on forensics tools. As mentioned previously, every file has four values called MACE and they are responsible for recording Modification, Access, Creation timestamps of that file. Anti-forensics can be used by manipulating the real time and date stamps may not be displayed correctly on computer forensics software. The real date and time are important as they give an indication to the investigator about when an update or change was made. Knowing that the date and time can be manipulated, reduces the trustworthiness of the forensics software.

Different tools can be downloaded on the device where the forensics software is installed then use those software to manipulate the tool's timestamp such as SKTimeStamp, NewFileTime, Time Stomp, and Change Timestamp

SKTimeStamp is a simple Explorer extension tool that is used to change the timestamps of any file. This tool provides a very simple way to manipulate or modify the timestamps (Williams, 2014).

NewFileTime is a timestamp manipulator tool for windows . With this tool, you can easily access any file and folder on your windows system then manipulate any of the timestamps on them (SoftwareOK.com, 2020).

Timestomp is a tool that can be used to modify or change the timestamp. Timestomp can be used on different platform such as Windows, Linux and macOS (MITRE/ATT&CK, 2015).

Change Timestamp is also a tool that allows you to quickly manipulate the timestamp of any file. This tool does not require any installation. To change the date and time of a file, you only need to open the tool and drag and drop the file (Other Government Agencies, 2017).

Hash collision. Hash function is a unique irreversible fixed value string which is created using a specific algorithm from any amount of data (Pajek & Pimenidis, 2009). To do this, the investigator used tools to create images from the collected evidence. After the creation of the images, the tools then generate hashes to verify the integrity of the image and to give a guarantee that the evidence was not tampered with. However, in 2005, a Chinese student managed to create two identical hash outputs from two different sets of hash inputs. Therefore, the digital evidence credibility could be questioned if hash collision is performed.

Summary

In this chapter, a taxonomy was created. The taxonomy classified anti-forensics into different levels and different categories: Where, Which, What, and How. The WHERE level indicates where anti-forensics can occur during an investigation. The WHICH level indicates which anti-forensics techniques exist. The WHAT level defines the exact method used for each technique. The HOW level indicates the tools used. Then, a detailed description was given for each technique, method, and tool. Chapter IV will include the final results of this study, the conclusion, and some recommendations.

Chapter V: Results, Conclusion, and Future Work

Introduction

This chapter will include an overall summary of this entire study. This chapter will be divided into three main parts: Results, Conclusion, and Future Work.

The Results will summarize the overall methodology used. This will include the study design used as well as how the data was collected. Additionally, the results will also be discussed here as well. This means the answers to the research questions will be answered.

The Conclusion will summarize and bring all the loose threads together. It will include the purpose of this study as well as the findings.

The Future Work section will include some recommendations for future work as well as how this study can be beneficial in the future.

Results

This study consisted of a thorough research on anti-forensics methods, techniques, and tools. The purpose was to create a taxonomy including the methods, techniques and tools, then present some strategies to detect them. and discuss some countermeasures.

To obtain all the data needed for this study, research/study questions were used. These questions helped provide guidance with analyzing and collecting the data. The questions that needed to be researched and answered to achieve the objective were:

1. What are the different types of Anti-forensics techniques?
2. Which method and tool can be used for each technique?
3. What are some countermeasures?

A qualitative approach was used to help answer these questions . This approach was more suitable for this study because the purpose of the study was to provide a rich description of all the Anti-forensics tools and techniques.

To collect the data needed, both primary and secondary data were used. For primary data, an interview was conducted where the interviewee was a digital forensics investigator. For secondary data collection, books and scholarly articles were carefully read and reviewed. All the data collected was then reviewed and analyzed to find relevant data, data that relates to the research/study questions.

The result of this study was as follows:

1. What are the different types of Anti-forensics techniques?
    - There are different types of Anti-forensics techniques. These techniques can occur on Data and on forensics tools. The different techniques that exist for data are “data destruction,” “data hiding,” and “trail obfuscation.” The techniques that exist for forensics tools are just “forensics software.”
2. Which method and tool can be used for each technique?
    - There are different methods for each anti-forensics technique. For “data destruction,” there is data wiping and physical destruction. For “data hiding,” there is encryption, steganography, program packer, and hiding data in the system area. For “trial obfuscation,” there is file headers manipulations, timestamp modification, and log deletion and modification. For “forensic software,” there is timestamp modification and hash collision.

- For each method, there is also a tool or tools that can be used. For data wiping, the tools used are DBAN, CBL Data. For physical destruction, the tool used are degausser, Crushers and Destroyers, Hard Drive Shredders, Disintegrators. For encryption, the tool used are BitLocker, FileVault2, LUKS, Veracrypt, 7-Zip, DiskCrypto, Encrypto, and AESCrypt. For steganography, the tools used are Xiao Steganography, Image Steganography, Steghide, crypture, SteganographX Plus, rSteg, Camouflage, and OpenStego, For program packer, the tools used are Ultimate Packer for Executables(UPX), Exe Stealth Packer, PELock, CExe, Amadillo, and dotBundle. For hiding data in the system area, the tools used are BMAP and slacker. For file headers manipulations, hex workshop, FITS4Win2, and Jhead are the tools that can be used.. For timestamp modification, the tools are SKTimeStamps, NewFileTime, Time Stomp, and Change Timestamp. For log deletion and modification, CCleaner, BitRaser, and Auto deletion are the tools used.

3. What are some countermeasures?
    - Anti-forensics techniques can be overcome if forensics investigators stay properly trained and informed as the new anti-forensics techniques arise. There are many certification programs available that prepare computer investigators on how to detect anti-forensics techniques. Following is a list of some of them:
        - CHFI (Computer Hacking Forensic Investigator) certification program was designed for computer forensics, and incident response. From taking this

course, computer forensics and incident response would be able to understand how to identify if an anti-forensics technique was used, how to recover deleted or hidden data, and so on (EC-Council, n.d.d).

- CND (Certified Network Defender) certification program was designed to train Network Administrators on how to protect, detect, and respond to the threats on the network (EC-Council, n.d.c).
- CEH (Certified Ethical Hacker) certification program is an ethical hacking course designed to help information security professionals inspect the network infrastructures to find security vulnerabilities that a hacker could exploit. It helps a cybersecurity professional master penetration testing (EC-Council, n.d.e).
- ECIH (EC-Council's Certified Incident Handler) is a program that was designed and developed in collaboration with cybersecurity and incident handling and response practitioners. This program focuses on how to handle post breach consequences (EC-Council, n.d.a).
- EDRP (EC-Council's Disaster Recovery Professional) certification is designed to educate and validate a security professional on how to plan, strategize, implement, and maintain a business continuity and disaster recovery plan (EC-Council, n.d.b).
- ECSA (EC-Council Certified Security Analyst) certification program is more advanced than the CEH (Certified Ethical Hacker). Unlike most other pen-testing programs that only follow a generic kill chain methodology; the ECSA

presents a set of distinguishable comprehensive methodologies that are able to cover different pentesting requirements across different verticals (EC-Council, n.d.f).

- Additionally, organizations should invest in constant training for their employees since anti-forensics techniques keep getting sophisticated. These training will help them stay current with the new anti-forensics trends.

One of the questions that was asked during the interview conducted for this study was: How does your organization stay current with the rise of anti-forensics techniques? He answered that they do a lot of training to make sure that everyone in the organization is aware. He then gave an example of a training he was recently part of. The training was about investigating a compromised Linux Host. From the training, he learned that some of the things to look for are (a) check who is currently logged in, (b) check who has logged in, (c) review he command history, (d) review what is using all the CPU etc. He added that at the end of each training, they go over what to do if they have been compromised. From taking different courses on the topic, and constantly participating in different training, forensics investigators would be able to overcome anti-forensics techniques.

Conclusion

To conclude, the objective of this study was to perform an in depth research on some of the many anti-forensics' techniques and tools, create a taxonomy including different levels and categories and finally, discuss some countermeasures. The goal was to help both forensics investigators and any other researcher on the topic. Below are the steps followed to complete this study and reach the objective

The first step of this research was to look at the objective then create some study/research questions. These questions help provide guidance when analyzing and collecting data. To complete the study, these questions needed to be answered.

The second step was to brainstorm for all possible sources. To do so, some questions needed to be answered first, such as: Will this study use a qualitative approach, quantitative approach, or both? Will this study use a primary data, secondary data, or both? For this study, a qualitative approach was used as it was more suitable. Also, for data collection, both primary and secondary data were used.

The third step was to collect the data and to evaluate the sources for appropriateness. To collect primary data, an unstructured interview was conducted. The questions were open-ended questions which helped with the collection of data. To collect secondary data, books, articles, journals and so on were carefully read. However, with so much data available, different keywords were used to narrow the search and to help obtain the most relevant published sources.

The fourth step was to create a taxonomy including all the relevant data collected. The taxonomy created was categorized into four different levels:

- Level 1: Indicating where anti-forensics can occur.
- Level 2: Indicating which anti-forensics techniques exist.
- Level 3: Indicating what anti-forensics method can be used for each techniques.
- Level 4: How, indicating the tool or tools used for each method.

The fifth and final step was to talk about some countermeasures, what forensics investigators can do to overcome anti-forensics techniques. The answer to this was that they should always stay current with the anti-forensics techniques by participating into different

training and taking different courses on the topic. There are a lot of courses available on how to prevent anti-forensics techniques from occurring to what to do when it has occurred.

Future Work

Computer criminals are becoming aware of the digital forensics' tools and techniques and are hence making the anti-forensics tools and techniques more sophisticated**.** With the increased use of anti-forensics tools and techniques, it has become challenging for digital forensics investigators to perform their investigation efficiently. To overcome this challenge, digital forensics investigators need to stay current with the new anti-forensics method and techniques. A lot of research needs to be done on the topic so that more investigators can learn about all the techniques available.

As I was researching more on anti-forensics, I realized that there was a lack of previous studies or research on the topic. I could not find a book that solely focused on just anti-forensics. Additionally, as I was looking at different articles, journals, and so on, I also found that there was a lack of enough sources on the topic. Even the sources found, there was not any current one available.

My recommendation is that researchers should continually do research on the topic as anti-forensics techniques keep getting sophisticated.

Additionally, my study as well as other studies done by previous research can be used to support the new studies on anti-forensics. And hopefully, with enough research on anti-forensics techniques, forensics investigators would be able to do their job more efficiently. Awareness is the key to reducing risks.

References

Afonin, O., Nikolaev, D., & Gubanov, Y. (2015) Countering anti-forensic efforts: Part 2. *Forensic Magazine.* Retrieved from https://www.forensicfocus.com/articles/countering-anti-forensic-efforts-part-2/

Andreo, A. (2014). Remove log files. *SourceForge*. Retrieved from https://sourceforge.net/projects/autodeletions/

Anon, D. (2018). Best free encryption software: 35+ Free Tools. *Privacy.Net*. Retrieved from https://privacy.net/best-free-encryption-software-tools/

Azadegan, S., Yu, W., Liu, H., Sistani, M., & Acharya, S. (2012). Novel anti-forensics approaches for smart phones. *2012 45th Hawaii International Conference on System Sciences*, 5424–5431. https://doi.org/10.1109/HICSS.2012.452

Blancco. (n.d.). *What is data destruction?* Retrieved from BTG English website: https://www.blancco.com/resources/article-data-destruction-definition/

Böhme, R., & Kirchner, M. (2013). Counter-forensics: Attacking image forensics. In H. T. Sencar & N. Memon (Eds.), *Digital image forensics* (pp. 327-366). https://doi.org/10.1007/978-1-4614-0757-7_12

Brand, M. (2007). Forensic analysis avoidance techniques of malware. *Australian Digital Forensics Conference*. https://doi.org/10.4225/75/57ad403c7ff2a

Computer Hope. (2019). *What is Windows?* Retrieved from https://www.computerhope.com/jargon/w/windows.htm

Computer Security Student. (n.d.). *Data hiding: Lesson 1. Hiding data in slack space using bmap*. Retrieved from https://computersecuritystudent.com/FORENSICS/HIDING/lesson1/index.html

Conlan, K., Baggili, I., & Breitinger, F. (2016). Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. *Digital Investigation, 18*, S66-S75. https://doi.org/10.1016/j.diin.2016.04.006

Data. (n.d.). *Techterms.com.* Retrieved from https://techterms.com/definition/data

de Beer, R. D., Stander, A., & Belle, J. V. (2015) Anti-forensics: A practitioner perspectives. *International Journal of Cyber-Security and Digital Forensics, 4*(2), 390-403.

DeFranzo, S. (2011). *Difference between qualitative and quantitative research.* Retrieved from https://www.snapsurveys.com/blog/qualitative-vs-quantitative-research/

Destructdata. (2018). *Physical data destruction solutions*. Retrieved from https://www.destructdata.com/physical-destruction

Distefano, A., Me. G., & Pace, F. (2010). Android anti-forensics through a local paradigm. *Science Direct*. Retrieved from https://www.sciencedirect.com/science/article/pii/S1742287610000381

EC-Council. (n.d.a). *EC-Council certified incident handler v2*. Retrieved from https://www.eccouncil.org/programs/ec-council-certified-incident-handler-ecih/'

EC-Council. (n.d.b) *EC-Council disaster recovery professional v3*. Retrieved from https://www.eccouncil.org/programs/disaster-recovery-professional-edrp/

EC-Council. (n.d.c). *Certified network defender certification*. Received from https://www.eccouncil.org/programs/certified-network-defender-cnd/

EC-Council. (n.d.d). *Computer hacking forensic investigator certification*. Retrieved from https://www.eccouncil.org/programs/computer-hacking-forensic-investigator-chfi/

EC-Council. (n.d.e). *Certified ethical hacker certification*. Retrieved from https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

EC-Council. (n.d.f). EC-Council certified security analyst: Penetration testing. Retrieved from https://www.eccouncil.org/programs/certified-security-analyst-ecsa/

Eoghan, C., Fellows, G., & Geiger, M. (2011). *The growing impact of full disk encryption on digital forensics/Request PDF*. Retrieved from https://www.researchgate.net/publication/220346119_The_growing_impact_of_full_disk_encryption_on_digital_forensics

Fisher, T. (2019). HDDErase v4.0 review. *Lifewire.* Retrieved from https://www.lifewire.com/hdderase-review-2619137

Fisher, T. (2020a). *38 best free data destruction software programs. Lifewire. tool.* Retrieved from https://www.lifewire.com/hdshredder-review-2619138

Fisher, T. (2020b). CBL data shredder v1.0. *Lifewire*. Retrieved from https://www.lifewire.com/cbl-data-shredder-review-2619129

Flournoy, B. (2018). How to delete windows log files. *Techwalla.com.* Retrieved from https://www.techwalla.com/articles/how-to-delete-windows-log-files

Forte, D. (2009). *Different schemes for different teams*. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S1361372309700077

Fox, S. (2010). *FBI: Russian spies hid codes in online photos*. Retrieved msnbc.com website: http://www.nbcnews.com/id/38028696/ns/technology_and_science-science/t/fbi-russian-spies-hid-codes-online-photos/

Garfinkel, S. (2007). *Anti-forensics: Techniques, detection and countermeasures*. Retrieved from https://core.ac.uk/download/pdf/36736409.pdf

Geiger, M. (2005). *Evaluating commercial counter-forensic tools*. Proceedings of the 5th Annual Digital Forensic Research Workshop, DFRWS 2005, Astor Crowne Plaza, New Orleans, Louisiana, USA, August 17-19, 200513.

Gogolin, G. (2010). *The digital crime tsunami*. Retrieved from https://dl.acm.org/doi/10.1016/j.diin.2010.07.001

Harris, R. (2006). *Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem*. Retrieved from https://www.sciencedirect.com/science/article/pii/S1742287606000673

Holmes, K. (2016). *Understanding the impact of anti-forensics techniques*. Retrieved from https://www.ftitechnology.com/resources/blog/understanding-the-impact-of-anti-forensics-techniques

Inc. (n.d.). *Computer crimes*. Retrieved from https://www.inc.com/encyclopedia/computer-crimes.html#:~:text=The%20U.S.%20Department%20of%20Justice,dating%20to%201989%2C%20remains%20valid.

INFOSEC. (2019). *Best tools to perform steganography*. Retrieved from qiahttps://resources.infosecinstitute.com/steganography-and-tools-to-perform-steganography/#gref

Jhead. (n.d.). *Digicam JPEG Exif header manipulation tool*. Retrieved from https://www.systutorials.com/docs/linux/man/1-jhead/

Kaspersky Lab. (2017). *Invisible attacks: Cybercriminals breach enterprises in 40 countries using hidden malware*. Retrieved from https://www.kaspersky.com/about/press-releases/2017_invisible-attacks

Kessler, G. (2007). Anti-forensics and the digital investigator. Presented at *5th Australian Digital Forensics Conference, Edith Cowan University*, December 3, 2007-. https://doi.org/10.4225/75/57ad39ee7ff25

Kharpal, A. (2016). *Apple vs FBI: All you need to know*. Retrieved from https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html

Kishore, A. (2011). Five free programs to completely wipe a hard drive. Retrieved from https://helpdeskgeek.com/free-tools-review/5-free-programs-to-completely-wipe-a-hard-drive/

Lamb, C. (2017). Packers, how they work, featuring UPX. *DZone Security*. retrieved from https://dzone.com/articles/packers-how-they-work-featuring-upx

Littlefield, R. (2017). *Anti-forensics and cryptography: An insight into how offenders disrupt cyber-crime investigations*. Retrieved from Ryan Littlefield website: https://littlefield.co/anti-forensics-and-cryptography-an-insight-into-how-offenders-disrupt-cyber-crime-investigations-e44637513709

McLeod, S. (2014). The interview research method. *Simply Psychology*. Retrieved from https://www.simplypsychology.org/interviews.html

MITRE/ATT&CK. (2015). *Timestomp*. Retrieved from https://attack.mitre.org/techniques/T1099/

Ontrack. (2018). *Destroyers-crushers*. Retrieved from https://www.ontrack.com/au/products/data-erasure/destroyers-crushers/

Other Government Agencies (OGA). (2017). *Change timestamp 0.32*. Retrieved from https://www.majorgeeks.com/files/details/change_timestamp.html

Pajek, P., & Pimenidis, E. (2009). Computer anti-forensics methods and their impact on computer forensic investigation. In H. Jahankhani, A. G. Hessami, & F. Hsu (Eds.), *Global Security, Safety, and Sustainability* (Vol. 45, pp. 145-155). https://doi.org/10.1007/978-3-642-04062-7_16

Park, K. J., Park, J.-M., Kim, E., Cheon, C. G., & James, J. (2017). Anti-forensic trace detection in digital forensic triage investigations. *Journal of Digital Forensics, Security and Law, 12*(1). https://doi.org/10.15394/jdfsl.2017.1421

Poonia, D. A. S. (2014). *Data Wiping and Anti Forensic Techniques. Compusoft: An International Journal of Advance Computer Techniques, 3*(12), 1374-1376.

Qian, Z., & Zhang, X. (2014). Improved anti-forensics of JPEG compression. *Journal of Systems and Software, 91*, 100-108.

Rekhis, S., & Boudriga, N. (2010). *Formal digital investigation of anti-forensic attacks.* Retrieved from https://www.researchgate.net/publication/221411296_Formal_Digital_Investigation_of_Anti-forensic_Attacks

Rouse, M. (2019). Software. *WhatIs.com* website. Retrieved from https://searchapparchitecture.techtarget.com/definition/software

Shaw, A., & Browne, A. (2013). A practical and robust approach to coping with large volumes of data submitted for digital forensic examination. *Digital Investigation, 10*(2), 116-128. https://doi.org/10.1016/j.diin.2013.04.003

Simmons, C. B. (2011). A Framework and demo for preventing anti-computer forensics. *Issues in Information Systems, Vol. X11*(1), 366-372.

Smith, A. (2007). Describing and Categorizing Disk-Avoiding Anti-Forensics Tools. *Journal of Digital Forensic Practice*, *1*(4), 309–313. https://doi.org/10.1080/15567280701418155

SoftwareOK.com. (2020). *NewFileTime 3.99 Corrections and manipulation of timestamp*. Retrieved from https://www.softwareok.com/?seite=Microsoft/NewFileTime

Sremack, J. C., & Antonov, A. V. (2007). *Taxonomy of anti-computer forensics threats*. Retrieved from https://www.imf-conference.org/imf2007/8%20Sremack_IMF%20Presentation_Taxonomy_09122007.pd

Stamm, M. C., & Liu, K. J. R. (2011). Anti-forensics of digital image compression. *IEEE Transactions on Information Forensics and Security*, *6*(3), 1050-1065. https://doi.org/10.1109/TIFS.2011.2119314

Sun, H., Weng, C., Lee, C., & Yang, C. (2011). Anti-forensics with steganographic data embedding in digital images. *IEEE Journal on Selected Areas in Communications*, *29*(7), 1392–1403. https://doi.org/10.1109/JSAC.2011.110806

The-Shadow-Fiend. (2016). Packer: Keep calm and hide the evidence (Malware Analysis: Chapter 4). *Talent Cookie* Website. Retrieved from

https://www.talentcookie.com/2016/06/packer-hide-the-evidence/

Thuen, C. (2007). *Understanding counter-forensics to ensure a successful investigation*. Retrieved from https://pdfs.semanticscholar.org/d5b6/b658d9178dbcdf33e095a53c45b4f7a43fc8.pdf

Williams, M. (2014). *SKTimeStamp 1.3.4*. Retrieved from https://www.techadvisor.co.uk/download/system-desktop-tools/sktimestamp-134-3328108/ww.techadvisor.co.uk/download/system-desktop-tools/sktimestamp-134-3328108/

Wundram, M., Moch, C., & Freiling, F. (2013). *Anti-Forensics: The next step in digital forensics tool testing*. Retrieved from https://www.researchgate.net/publication/261038911_Anti-Forensics_The_Next_Step_in_Digital_Forensics_Tool_Testing