PRACTICAL DIGITAL FORENSICS:

A GUIDE FOR WINDOWS AND LINUX USERS

Akashdeep Bhardwaj
Pradeep Singh
Ajay Prasad

Bentham Books

Practical Digital Forensics: A Guide for Windows and Linux Users

Authored by

Akashdeep Bhardwaj

Pradeep Singh

&

Ajay Prasad
School of Computer Science
University of Petroleum and Energy Studies
Dehradun, India

Practical Digital Forensics: A Guide for Windows and Linux Users

Authors: Akashdeep Bhardwaj, Pradeep Singh & Ajay Prasad

ISBN (Online): 978-981-5305-57-9

ISBN (Print): 978-981-5305-58-6

ISBN (Paperback): 978-981-5305-59-3

First published in 2024.

need for a court order if at any point you breach any terms of this License Agreement. In no event will any delay or failure by Bentham Science Publishers in enforcing your compliance with this License Agreement constitute a waiver of any of its rights.

3. You acknowledge that you have read this License Agreement, and agree to be bound by its terms and conditions. To the extent that any other terms and conditions presented on any website of Bentham Science Publishers conflict with, or are inconsistent with, the terms and conditions set out in this License Agreement, you acknowledge that the terms and conditions set out in this License Agreement shall prevail.

Bentham Science Publishers Pte. Ltd.
80 Robinson Road #02-00
Singapore 068898
Singapore
Email: subscriptions@benthamscience.net

CONTENTS

FOREWORD

In the ever-evolving realm of digital forensics, where evidence resides in the intricate pathways of computers and digital devices, the need for a comprehensive and practical guide has never been greater. "Practical Digital Forensics: A Hands-on Guide for Windows & Linux Users" rises to this challenge, offering an invaluable resource for both seasoned investigators and those embarking on their journey into this critical field. This book transcends theory, providing a hands-on approach that empowers readers with the skills to navigate the complexities of digital investigations. From establishing a secure forensic workstation to meticulously recovering deleted data and analysing intricate file systems, the book delves deep, equipping readers with the tools and techniques needed to uncover the truth hidden within digital landscapes.

"Practical Digital Forensics" is more than just a collection of techniques; it recognizes the legal and ethical considerations paramount in this field. By addressing these crucial aspects, the book ensures that investigators not only gather evidence effectively but also maintain its integrity for use in legal proceedings. This book caters to a diverse audience, from law enforcement professionals to cybersecurity analysts and legal practitioners. Each chapter builds upon the foundation of the previous, ensuring a smooth learning curve for novices while offering valuable insights and advanced techniques for experienced investigators.

With its clear explanations, practical exercises, and real-world case studies, "Practical Digital Forensics: A Hands-on Guide for Windows & Linux Users" is poised to become a trusted companion in the ever-growing field of digital forensics. It empowers readers to navigate the intricate landscape of digital evidence, ensuring that no digital footprint remains hidden from the pursuit of justice.

Dr. Sam Goundar
RMIT University, Australia

PREFACE

Welcome to the ever-expanding world of digital forensics! In our increasingly digital age, evidence often resides not in physical objects but in the intricate pathways of computers and networks. This book, "Practical Digital Forensics: A Hands-on Guide for Windows & Linux Users", aims to equip you with the knowledge and skills necessary to navigate this complex digital landscape.

Whether you are a seasoned investigator, a burgeoning cybersecurity professional, or simply someone with a keen interest in digital forensics, this book provides a comprehensive yet accessible introduction to the field. We will delve into the core principles and methodologies that underpin digital forensics, ensuring you understand the foundation before diving into the practical aspects.

This book is specifically crafted for both Linux and Windows users. We will guide you through setting up a robust forensic lab environment on both operating systems, equipping you with the essential software tools and utilities needed for in-depth analysis. Throughout the journey, you will gain hands-on experience with critical forensic techniques, from acquiring volatile data and analysing file systems to dissecting Windows registries and investigating network traffic.

As technology evolves, so do the challenges faced by digital forensic investigators. We will explore advanced techniques for tackling web browser artifacts and delve into the ever-present threat of anti-forensic measures. This book equips you not only to uncover hidden evidence but also to document your findings and present them effectively in a court of law.

Finally, we will conclude by exploring the exciting advancements and emerging challenges within the field of digital forensics. By understanding the ever-changing landscape, you will be well-positioned to adapt your skills and stay ahead of the curve.

This book is designed to be an interactive learning experience. Each chapter builds upon the previous one, culminating in a well-rounded understanding of the entire digital forensics process. We encourage you to actively engage with the material, practice the presented techniques, and explore further resources to deepen your knowledge.

Get ready to embark on a thrilling journey into the world of digital forensics. With dedication and this book as your guide, you will be well on your way to becoming a skilled digital investigator, ready to uncover the truth hidden within the digital realm.

Akashdeep Bhardwaj

Pradeep Singh

&

Ajay Prasad
School of Computer Science
University of Petroleum and Energy Studies
Dehradun, India

CHAPTER 1

Navigating the Ethical Landscape of Digital Investigations

Abstract: This book aims to provide you with a comprehensive understanding of Digital Forensics, from its relatively new beginnings as a Digital forensics sub-discipline to its rapidly growing importance when combined with the more established digital forensic field of investigations. You should be able to comprehend the function of digital forensic professionals as well as the business and cybercrime contexts in which they are actively looking for proof of criminal and civil offenses after reading this chapter. You can gain an understanding of the difficulties faced by forensic practitioners and the intricacy of many cases by looking through case studies and examples presented in the book chapters.

Keywords: Cybercrime, Case studies, Criminal offenses, Digital forensics, Digital evidence, Forensic disciplines, Investigative techniques.

INTRODUCTION

Interest in Digital Forensics [1] as a subject for higher education and as a possible career path in business and law enforcement investigations has developed over the last ten years or more. To handle the increasing number of cases involving digital evidence, new forensic techniques and technology have emerged. But it is clear that practitioners are having trouble keeping up with the growing complexity, size, and quantity of cases. They also have limited funding and resources, and there is a dearth of qualified, experienced staff. The book aims to help practitioners, both current and prospective, address problems effectively in the future by discussing these challenges while providing some solutions that have helped me in my work and studies.

Due to the widespread use of personal computers in the workplace, inherent security issues with them have created new challenges for law enforcement. For instance, companies conducting internal audits or criminal investigations frequently must spend a lot of time going through computer data to locate digital evidence. New forensic procedures and instruments are desperately needed for these kinds of exams to support practitioners in doing their work more quickly. For practitioners looking to strengthen their crucial role in supporting the legal

Akashdeep Bhardwaj, Pradeep Singh & Ajay Prasad

community, these are exciting times. In terms of developments impacting evidence recovery and management, practitioners are at a crossroads when it comes to new entries into the field.

A category of forensic science called Digital Forensics investigates and analyzes digital devices and data to find evidence of fraud, espionage, cybercrimes, and other illegal activity. In order to collect, maintain, review, and present digital evidence in court, its guiding concepts and procedures are essential. Within this discipline, complacency, banality, and exhaustion are commonplace, and despite the work's intrinsic importance and excitement, the monotony and hefty caseloads can quickly stifle initial enthusiasm. This book presents new and efficient methods for cutting down on boredom and time-wasting, energizing practitioners, and bringing back the thrill of the evidence-gathering process. Courts and judicial procedures use digital forensic evidence, despite the opinions of certain purists who do not see forensics as science. Although the word may be deceptive, it might refer to the technology associated with certain disciplines rather than the sciences themselves.

The judiciary has become more aware of the growing use of digital evidence in court disputes. This places a great deal of pressure on digital forensic experts to strive to present reliable data and careful analyses of their findings, which may also be useful in establishing and evaluating precedents for future court rulings. Information security management must be improved because of the sharp rise in desktop computing and the spread of cybercrime that targets network infrastructure. It also calls for practitioners to sort through the chaos and try to hold the violators accountable. Specializations in digital forensics include the following domains as career options.

• Computer Forensics: This is the traditional area of digital forensics, which focuses on recovering and analyzing data from computers and other electronic devices. Computer forensic specialists are often involved in criminal investigations, but they can also be used in civil litigation and corporate investigations.

• Network Forensics: Network forensics specialists focus on investigating network traffic to identify security breaches and other criminal activity. They use a variety of tools and techniques to track down the source of attacks and to collect evidence.

• Mobile Device Forensics: As mobile devices have become more and more popular, the need for mobile device forensics specialists has grown. These specialists are experts in recovering data from mobile devices, such as smartphones and tablets.

• Cloud Forensics: Cloud forensics is a new and emerging specialization that focuses on investigating crimes that involve cloud-based storage and applications. Cloud forensic specialists need to have a deep understanding of cloud computing technologies and how they can be used to store and transmit evidence.

• Incident Response: Incident response specialists are responsible for responding to security incidents, such as data breaches and malware attacks. They work to contain the damage from the incident and to collect evidence that can be used to identify the attackers and bring them to justice.

The area of digital forensics emerged as more crimes involved the use of computer systems as the object of a crime, a tool for committing a crime, or a source of evidence for a crime. It did not take long to identify crucial tasks the need for looking at and analysing digital evidence while also making sure that the original evidence's integrity is maintained.

DIGITAL FORENSICS PRINCIPLES

The investigation and prosecution of cybercrimes and other digital offenses depend heavily on the concepts and procedures of Digital Forensics. Forensic specialists may efficiently gather, examine, and present digital evidence to support judicial processes and guarantee justice in the digital sphere by abiding by these guidelines and using reliable procedures. This section provides an overview of the concepts and procedures related to Digital Forensics.

• Evidence Preservation [2] is crucial to maintain the integrity of digital evidence. This involves protecting the digital environment, or crime scene, against manipulation. This ensures that the integrity of the evidence is maintained during its collection, preservation, and examination. Forensic specialists, for instance, take a forensic image of the hard disk while confiscating a computer used in a cybercrime investigation so they may work with a duplicate while protecting the original data.

• Chain of Custody [3] creates and preserves the formal chain of custody to ensure the admissibility and dependability of the evidence by documenting how it is handled, moved, and stored. For example, keeping track of who, when, and why someone used a confiscated device aids in preserving the integrity of the evidence.

• Volatility [4] involves if digital evidence is not handled quickly, it may be volatile and vulnerable to change or deletion. Before beginning a comprehensive investigation, forensic specialists give priority to gathering dynamic data first, such as real-time system information or network connections. For instance,

CHAPTER 2

Constructing A Robust Digital Forensics Environment

Abstract: Establishing a Digital Forensic laboratory is paramount in modern investigative practices. This chapter delineates the essential components and procedures necessary for setting up an effective Digital Forensic lab. It covers various aspects, including infrastructure requirements, hardware, and software provisioning, as well as the implementation of standardized procedures and protocols. Additionally, it discusses the significance of maintaining the integrity and security of Digital evidence throughout the Forensic process. By offering practical insights and recommendations, this chapter aims to empower Forensic practitioners with the knowledge and resources required to establish a robust Forensic laboratory capable of addressing the complex challenges of Digital investigations in today's Digital landscape.

Keywords: Digital forensic laboratory, Digital evidence integrity, Forensic investigation, Forensic environment, Infrastructure requirements, Standardized procedures, Technological advancements.

INTRODUCTION

The need for computer forensics labs [1] to gather and analyse digital evidence accurately is growing due to the rise in cybercrime assaults that affect both the public and private sectors. You might believe that only law enforcement organizations have access to digital forensics labs. This is untrue, though, as Fig. (**1**) shows that numerous American corporations keep state-of-the-art Digital Forensics labs equipped with cutting-edge investigative tools. Although digital forensics labs were first established by law enforcement and security services, most common crimes nowadays are linked to some form of digital evidence due to advancements in computing technology [2] and the increasing usage of smartphones and wearables.

This puts a strain on police labs by creating lengthy waiting lists for digital evidence from several court cases that need to be investigated. These waiting lists can occasionally go on for months or even years. This has prompted big and even medium-sized businesses to establish internal labs to investigate cybercrime concerns pertaining to their assets and work. These days, to expedite the investi-

gation process [4] and lower the numerous expenses related to digital investigations, banks, IT corporations, merchants (like Amazon and Walmart), and energy providers use their own Digital Forensics labs. Private companies have greater leeway when it comes to obtaining the newest hardware and software including upgrades necessary to outfit their labs than do police departments.

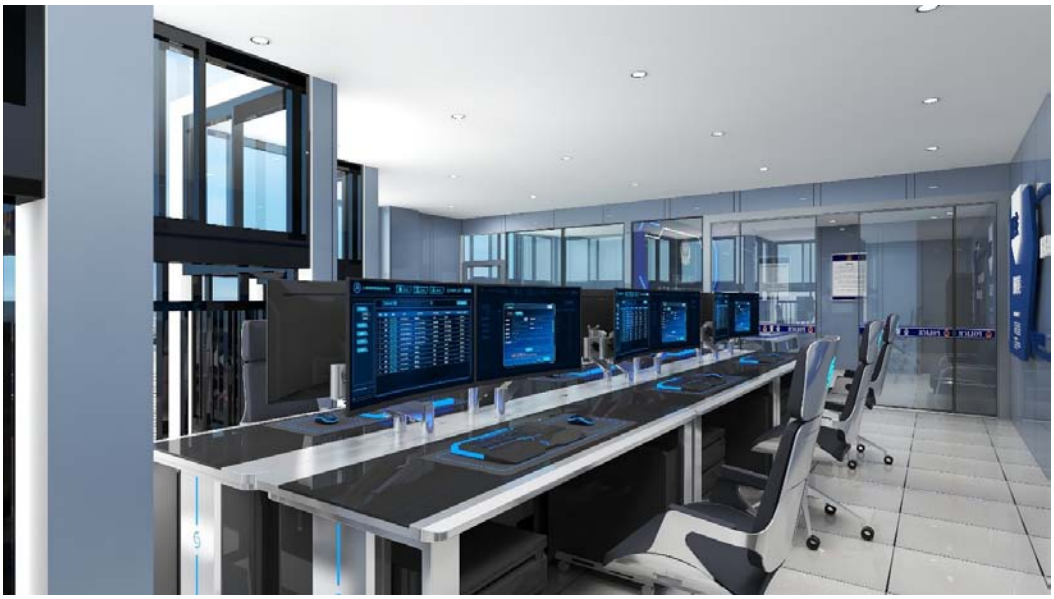

Fig. (1). Digital forensics lab [3].

However, due to financial constraints and a shortage of qualified personnel, some police laboratories can still be using outdated software versions. To resolve matters pertaining to their companies, in-house digital forensics experts typically collaborate closely with law enforcement organizations. For example, if someone witnesses or finds evidence of illegal activity (such as breaking company policy, industrial sabotage, leaking secrets, or other related crimes), the e-discovery team or the Digital Forensic investigators of the reporting company will get in touch with law enforcement and collaborate with them to gather and evaluate the evidence, as well as to take the case to court.

Any business that values its data assets should invest in an internal Digital Forensics lab [5], but this has costs associated with it. For example, even the smallest lab will require an annual budget of at least $150,000 if only one forensic analyst is recruited, and one forensic workstation is equipped with the primary tools required to perform the job (both hardware and software). If there are not many incidences, small businesses might not be willing to pay for this additional

expense. To cut expenses, a lot of small and medium-sized businesses contract out their Digital Forensics work to a recognized third-party lab.

Whether you intend to construct an in-house lab for your company or think about outsourcing your Digital Forensics work to a third-party supplier, accreditation of the Digital Forensics lab is an important consideration. A Forensic laboratory's accreditation guarantees that it adheres to the authoritative body's specified requirements for the use of dependable procedures, suitable hardware and software, and qualified staff in carrying out its responsibilities. Digital forensics labs can vary widely in size. While funding is undoubtedly important, the anticipated duties (or work scope) for this lab will serve as the primary guide in identifying the hardware and software tools required. Big businesses are spending, for example, in setting up state-of-the-art labs that can handle any kind of computer device and cases, including malware, network, GPS, and mobile forensics.

These labs are staffed by highly skilled individuals and equipped with a variety of specialized hardware tools as well as the most recent versions of forensic software. The bare minimum of equipment is required to gather, store, process, and display digital evidence in a forensically sound manner, regardless of the size of your forensics lab. The most common type is a small digital forensics lab because it can start up fast and just requires a little budget. These labs are often managed by one to five individuals and concentrate on managing a specific kind of device (e.g., Windows OS Forensic, or mobile Forensic). It does not require the expensive equipment that large labs require for networking and security, but it still needs the right digital forensic software to analyse evidence, along with necessary hardware like cables, a hardware write blocker (some of which are built into the forensic workstation itself), other electrical devices like digital cameras and UPS, and a dedicated forensic computer to perform the analysis.

LAB FACILITY

It is crucial to talk about the physical space requirements of the Digital Forensics lab before enumerating the hardware and software equipment required for the Forensic lab. Ensuring the safety and soundness of digital evidence, along with the technology in the lab, should be of utmost importance. This is because hackers may attack these labs to halt or disrupt investigations. When examining digital evidence, forensic examiners will spend hours at their workstations; therefore, to stay productive, they need to be comfortable in their seats. For forensic workstations, employ ergonomic seats that can be adjusted to the user's demands. Computer screens should also be of high quality because examiners will be staring at them for extended periods of time. To prevent potential health impacts

CHAPTER 3

Acquisition of Live Analysis and Volatile Data

Abstract: The process of conducting a proactive Forensic investigation begins with data acquisition. The process of obtaining Forensic data involves more than just moving files from one device to another. To generate a Forensic duplicate of the data, investigators use Forensic data acquisition to try and retrieve every bit of information from the victim system's memory and storage. Furthermore, the creation of this Forensic duplicate needs to ensure that the data's verifiable integrity is maintained and that it can potentially be used as evidence in court. The basic ideas of data acquisition are covered in this chapter, along with the several processes that make up the data acquisition methodology.

Keywords: Acquisition methodology, Data acquisition, Evidence integrity, Live analysis, Volatile data.

INTRODUCTION

Basics of Data Acquisition

The first stage in conducting the Forensic investigation on a potential evidence source is to duplicate the data from any digital storage device, such as a Solid-State Drive (SSD), Hard Disk Drive (HDD), Flash Drive, or SD Card that is discovered at the crime scene. It is up to Forensic investigators to decide whether to move the device to a secure location beforehand or complete the data-acquiring procedure on the spot. This chapter elaborates on live and dead acquisition and covers basic principles in data acquisition. The chapter objectives include:

- Understanding the basics of data acquisition
- Understanding various types of data acquisition
- Understanding the format of data acquisition
- Understanding the data acquisition methodology
- Perform the data acquisition on volatile data using FTK imager
- Perform analysis on live data acquisition using volatility framework
- Perform the static data acquisition using FTK imager.

Akashdeep Bhardwaj, Pradeep Singh & Ajay Prasad

The process of collecting and recovering sensitive data from a suspect computer and developing procedures to retrieve electronically stored information to obtain information about a crime or incident is known as data acquisition. The methods involved in acquiring data and presenting it to the law are the two most crucial aspects of Forensic work, and when these processes are completed, we will be able to comprehend the full chain of custody involved in this procedure. We will either work with a live system or an image of the system when doing Forensics. It is advised practice to image the system or create a copy of the necessary data and run Forensics on it to ensure accuracy. The entire procedure should be auditable and admissible in court, and the investigator must be able to confirm the accuracy of the data they have obtained. Finding the likely source of the evidence is the first and most important stage.

Time is an essential component to consider when gathering Forensic data. While information in certain sources, such as hard drives, remains intact and retrievable long after the system is shut down, data in some sources such as RAM are highly volatile and very rapidly changing and must therefore be collected in real-time. In accordance with this perspective, there are two types of data acquisition: live data acquisition and dead data acquisition.

Extraction of digital evidence from a computer system that is powered on is the technique known as live data acquisition. In Digital Forensics and incident response, it is an essential approach that lets investigators take a picture of a system in action. This makes it possible to get erratic data that is brittle and disappears when the system is turned off or loses power. These kinds of data are kept in RAM, caches, and registries. Volatile data is transient and vanishes when the system is terminated. Investigators can examine this data using live acquisition to look for indications of ongoing illicit activity, malware infestations, or hidden activities. Furthermore, real-time gathering of information is necessary because volatile data, like that in RAM, is dynamic and changes frequently. Nonvolatile data that stays in the system even after shutdown is gathered in dead or static data acquisition. In Digital Forensics, dead acquisition, often referred to as offline acquisition, is the recommended technique for gathering data from storage devices. Data collection is done from a device that is not powered on or from a storage device that is disconnected from the main system. Investigators can recover such data from Hard Disk Drive (HDD) as well as from slack space, swap files, and unallocated drive space. Additional non-volatile data sources are Solid State Drives (SSDs), Optical Discs (CDs, DVDs, Blu-ray Discs), Non-volatile Memory (NVM), PDAs, CD-ROMs, USB thumb drives, and cellphones.

ORDER OF VOLATILITY

The method by which Digital data is gathered for a Forensic investigation is known as the order of volatility. Since this kind of data vanishes the moment, the system is turned off, it gives priority to capturing the most volatile data first. Investigators must consider both the impact of data collection on the suspect system and the data's possible volatility when gathering live data. Since not all data are equally volatile, investigators must gather the most volatile data first before moving on to the least volatile data. An investigator must assess the data volatility order based on the circumstances and the suspected machine when gathering evidence. The order of volatility for a typical system is illustrated in Fig. (**1**).

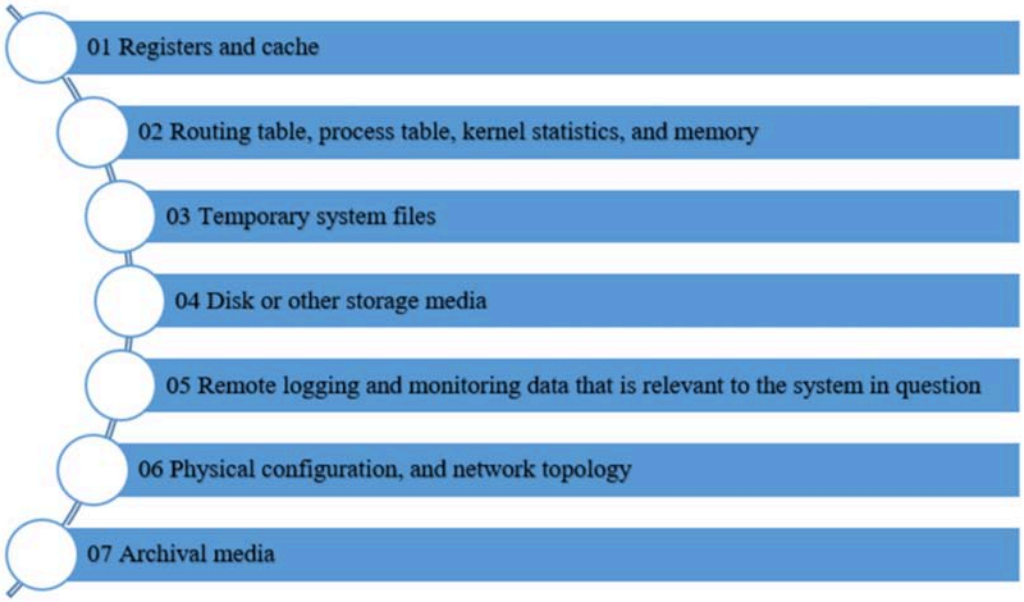

Fig. (1). Order of volatility.

According to RFC 3227 [1] Guidelines for Evidence Collection and Archiving, the sequence of volatility for a typical computing system is as follows:

- **Registers, processor cache:** These are areas of the central processing unit (CPU) where data that is presently being processed is temporarily stored. When the system loses power, this data vanishes. The computer's registers and proces-

CHAPTER 4

File System Forensics

Abstract: Hard Disk Drives (HDDs) and Solid-State Drives (SSDs) are two types of storage devices that are crucial information sources for forensic investigations. The information gathered from storage devices should be located and safeguarded by the investigator as evidence. As a result, the investigator must be familiar with the design and operation of storage devices. Additionally, the file system is crucial since it determines how data is distributed and stored on a device.

Keywords: Digital evidence, Data acquisition, Disk imaging, Data recovery, File system, HDD, Storage devices, SSD, System analysis.

INTRODUCTION - UNDERSTANDING STORAGE DRIVES

A computer's memory, or storage device, is a crucial part that stores data and information. There is a necessity to store even the operating system. A computer without storage is like a car without wheels. Computers store digital data on HDDs and SSDs. Because HDDs have moving elements and record data magnetically on a spinning platter, they are vulnerable to physical harm. SSDs do not have any moving parts and store data on NAND flash memory chips. Classification of computer storage is illustrated in Fig. (**1**).

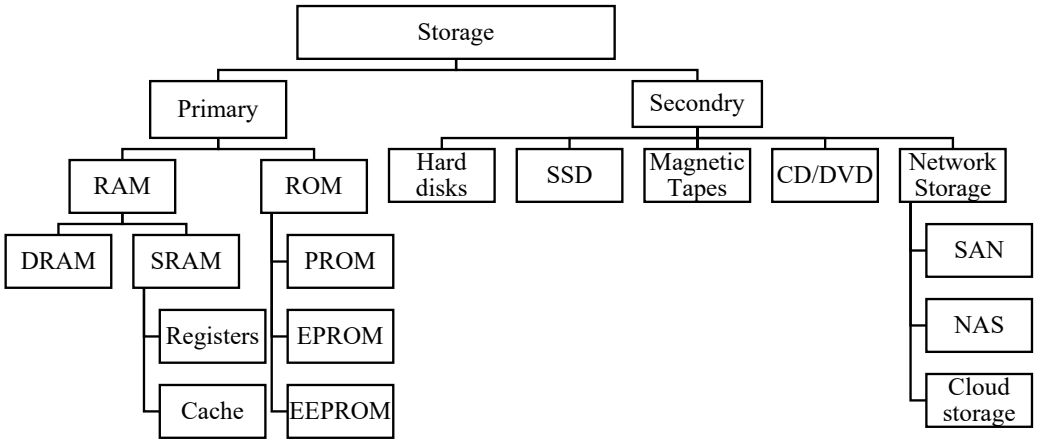

Fig. (1). Classification of computer storage.

The hardware and technologies used to store digital information are referred to as computer storage. It functions similarly to the memory on your computer, but unlike temporary memory (RAM), it can hold onto data even when the power is off. There are two main types of computer storage; Primary Storage and Secondary Storage

PRIMARY STORAGE

This is a quick internal memory that stores data that the CPU is currently using. Because it is volatile, data is lost when a computer shuts down. Primary memory, which is situated close to the CPU to facilitate speedy access, is made up of RAM and ROM. Primary memory can be accessed directly by the CPU.

RAM (Random Access Memory)

Consider it to be like a workstation you would use for a project. It contains the data that your computer requires to function at that precise instant, such as the open files, open programs, and any data you are working with right now. RAM is unique due to its speed, random access, and volatility. Any random location can be used to get data from a RAM, which is a volatile memory, meaning that if the power is interrupted, the data is lost. This is utilized for temporary storage and is incredibly quick, there are two kinds of RAM:

DRAM (Dynamic Random Access Memory)

DRAM uses discrete memory cells, each of which normally consists of a transistor and a capacitor, to store data. The real data, which is represented by an electrical charge in the capacitor and is a 0 or 1, is stored there as the fundamental unit of digital information. When it comes to limiting access to the capacitor so that data can be read or written, the transistor functions as a gatekeeper. Programs and data that the CPU requires instantly are stored in DRAMs. Cells used in Dynamic RAM (DRAM) construction store data as the charge on capacitors. Dynamic RAMs require periodic charge refreshing to preserve data storage because capacitors naturally have a tendency to discharge. Most systems use DRAM as their primary RAM option because of its speed and low cost. It offers the necessary temporary memory for your computer to perform programs and operations effectively, even though it is not for permanent storage.

SRAM (Static Random Access Memory)

SRAM is faster than DRAM because it uses latches, which are permanent data storage devices. This makes SRAM perfect for CPU caches and registers that require extremely quick access. However, there is a price for this speed: SRAM is

used sparingly for some jobs where speed is crucial because it is more costly, larger due to complicated circuitry, and power-hungry. SRAM is different from DRAM in that it does not require data refreshes, instead, it may store data for as long as power is on. In addition to being more costly, SRAMs are faster than DRAMs. SRAM is therefore only occasionally used. The main categories of SRAM available are Registers and Cache:

- **Registers:** A tiny amount of storage found inside the CPU is called a register. A few hundred are found in most contemporary CPUs. They are used to hold data, locations, or instructions that the CPU must access immediately. The CPU's lightning-fast partners for data manipulation are registers. They are the fastest memory devices in the hierarchy due to their small size and on-chip placement, but their capacity limitation forces them to handle just the data that is necessary for the CPU to perform its current functions.
- **Cache:** Cache is essential for improving computer performance because it keeps frequently used data easily accessible to the CPU. It is a clever method of bridging the processor and slower storage device speed difference. In computers, cache refers to the layer of transient data storage situated between the central processing unit (CPU) and random-access memory (RAM), or between RAM and slower storage devices such as solid-state drives (SSDs) and hard drives (HDDs). By keeping frequently requested information or instructions closer to the processor, it functions as a speed booster by enabling speedier retrieval than contacting the original data source.

ROM (Read Only Memory)

Read-only memory (ROM) on computers allows you to read data but not alter it, as the name implies. It is like one of those library books you can check out but cannot write in. During regular operation, data written on ROM cannot be removed or altered because it is permanent. Usually, a particular procedure or manufacturing process is used to program this information. Important instructions that your computer needs to correctly boot up are stored in the RAM. Firmware is the term for these instructions. Hardware components are powered on and the operating system is loaded from a storage medium by the basic input/output system (BIOS), an example of a firmware. Other necessary software applications or data that are rarely modified can also be stored in ROM. Calculators and a few embedded devices, for instance, store their operating programs in RAM. Different types of ROM are available namely PROM, EPROM, and EEPROM.

CHAPTER 5

Windows Forensics and Registry Analysis

Abstract: The evidence we seek in today's digital environment frequently resides in computer systems. The basic knowledge and abilities needed to carry out an extensive Windows forensics investigation are provided to readers in this chapter. We start by building a solid foundation of the fundamentals of Windows forensics. Methods for gathering volatile data, which is kept in memory, as well as non-volatile data, such as files and system records, are investigated. We then explore the skill of interpreting this abundance of data. The chapter will teach readers how to mine a variety of Windows data sources, such as program data, system configuration files, and user activity logs, for important evidence. Turning the page, the chapter presents the Windows Registry, an essential part that protects the configuration secrets of the operating system. Methods for examining both static and dynamic registry hives are offered, enabling detectives to find concealed proof of malicious activity or system alterations. Looking into internet browser history is a necessary step in any digital inquiry. To find possible leads and user activity patterns, this chapter walks readers through the process of extracting and analyzing web browser history, cookies, and cached data. This chapter provides readers with the necessary knowledge to enable them to extract and analyze digital evidence from Windows PCs with ease. This information is crucial for forensic investigations to be clear and for finding the truth.

Keywords: Cookie, Cache data, Metadata, Registry analysis, Windows forensics.

INTRODUCTION

One crucial area of cyber security is computer forensics, which is the collection of data about activities performed on computers. It is a subset of the larger area of "Digital Forensics," which deals with the forensic study of many kinds of digital devices, including data recovery, examination, and analysis. Digital and computer forensics have a wide range of uses. In the legal field, they are employed to confirm or deny a theory in a civil or criminal case. In the private sector, they are utilized for incident and intrusion analysis, internal company investigations, and other similar tasks. The desktop operating system that is currently most widely used is Microsoft Windows. It presently has about 80% of the desktop market share and is preferred by both private users and enterprises. For anyone interested in Digital Forensics, this means that performing forensic analysis on Microsoft Windows is a crucial skill to have.

Akashdeep Bhardwaj, Pradeep Singh & Ajay Prasad

Unquestionably, the digital world is currently influencing every aspect of our lives. From business and economics to communication and entertainment, computers are used for everything. Regrettably, criminal conduct can also be enabled by this digital environment. When this kind of thing happens, computers themselves can contain important evidence. The study of cybercrimes involving Windows computers is known as Windows forensics. It entails obtaining data from a Windows computer to identify and bring charges against the person or people responsible for a cybercrime. Because Windows is one of the most used operating systems, there is a greater chance that a Windows computer will be involved in an incident. Therefore, to locate information of potential use as evidence, investigators need to have a solid understanding of the many Windows OS components, including the file system, registry, system files, and event logs [1].

The process of locating, protecting, evaluating, and presenting digital evidence from a Windows operating system is known as Windows Forensics. Recovering data in a form that is legally admissible in court is its aim. Then, using the recovered data, legal actions can be supported, criminals can be identified, and events can be rebuilt. The main features of Windows Forensics are broken down as follows:

- Identification: Identifying possible electronic evidence on a Windows platform.
- Preservation: Protecting the evidence's integrity by gathering it in a way that adheres to forensic best practices.
- Analysis: Looking through the collected data to find pertinent details.
- Presentation: Clearly and succinctly summarizing the results in a way that is appropriate for court hearings.

Windows Forensics gives detectives the instruments and methods necessary to retrieve a Windows system's digital trail, which offers insightful information about previous actions. In the current field of digital forensics, Windows Forensics is essential. The capacity to retrieve and examine digital evidence from Windows computers is becoming increasingly important as long as criminals are using these platforms for their operations.

Any digital data that may have evidence value is considered a forensic artifact. They are essentially the digital traces that programs and users on a device leave behind. These relics may be essential for piecing together historical events and identifying possible criminal conduct. 'Artifact' is a term you will frequently see in forensic analysis. Forensic artifacts are vital bits of data that demonstrate human behavior. Items such as fingerprints discovered at crime scenes, broken buttons discovered on clothing, and tools involved in the crime commission are

examples of forensic artifacts [2]. With the aid of all these objects, the story of the crime's commission is rebuilt. Forensic artifacts in computer forensics might be tiny traces of past activity on the system. Because of the numerous artifacts that a Windows system generates for a particular activity, a person's activities on a Windows machine can be properly tracked down through computer forensics. Frequently, these relics are found in places that 'regular' users wouldn't go. These artifacts can serve as the trial run for an investigation of our goals if they are evaluated [3]. Here is a closer look at objects used in forensics:

- Examples: Common forensic artifacts include system logs, registry entries, file system metadata, deleted files, web browser history, email records, and temporary files.
- Worth: The ability to reveal details about the events on a device is what gives forensic artifacts their worth. A user's web browser history can disclose their online actions, whereas a deleted file record may suggest an attempt to conceal information.
- Hidden Nature: A lot of forensic artifacts have a hidden nature and are not easily visible. They can live in the memory of a computer, system files, or unallocated disk space. To locate and evaluate these artifacts in an efficient manner, forensic instruments and methods are needed.

Investigators can create a timeline of events, identify users involved, and unearth possible motivations behind illegal action by examining a variety of forensic evidence. These relics are essential to providing a complete picture of what happened on a digital device.

VOLATILE AND NON-VOLATILE DATA

A computer’s memory is an ever-changing landscape that holds volatile information. It includes active processes, open connections to networks, and data stored in RAM, all of which disappear when the power is turned off. But this transient data, which offers a moment-in-time picture of the system's condition, can have enormous forensic significance [4]. When a system is turned off, volatile data, which usually resides in system RAM, is lost. From a forensics perspective, it produces useful artifacts like command history, shared resources, network-related data, process-related data, open file information, and user log-in information [5].

Hard disks and solid-state drives are examples of storage devices that hold non-volatile data. This data is more historically oriented than its volatile cousin, as it continues to exist even after a shutdown. Data that is persistent and does not disappear when a system crashes or is turned off is referred to as non-volatile

CHAPTER 6

Network Forensics

Abstract: In the ever-expanding digital landscape, network security breaches pose a significant threat. Network forensics emerges as a vital weapon in the cybersecurity arsenal, enabling the investigation and analysis of network traffic to uncover evidence of malicious activity. This chapter delves into the core principles of network forensics, outlining the four-stage process: acquisition, preservation, analysis, and reporting. It equips readers with the knowledge to identify and collect various types of network evidence, including packet headers, network logs, and flow data. The chapter explores a range of open-source tools readily available on platforms like GitHub, empowering readers with the ability to capture and analyze network traffic using Wireshark and Bro. Furthermore, it acknowledges the inherent challenges faced in network forensics, such as the fleeting nature of network data and the growing use of encryption. To ensure the legality and effectiveness of investigations, the chapter emphasizes the importance of adhering to relevant laws and regulations. By understanding these essential concepts, readers gain valuable insights into how network forensics empowers cybersecurity professionals to combat digital crimes and safeguard network security.

Keywords: Digital forensics, Network forensics, Network traffic analysis, Open-source tools, Security onion, Wireshark.

INTRODUCTION

In today's hyper-connected world, data traverses networks at an unprecedented pace. While this interconnectedness fosters innovation and collaboration, it also creates vulnerabilities that cybercriminals exploit. Network forensics emerges as a critical discipline within cybersecurity, playing a detective-like role in uncovering evidence of malicious activity on a network. Network forensics can be defined as the application of scientific and investigative techniques to analyze network traffic for the purpose of identifying, collecting, preserving, and analyzing evidence of criminal or unauthorized activity. It is a specialized branch of digital forensics, focusing specifically on the data flowing across a network rather than data stored on individual devices.

Within the vast realm of digital forensics, two distinct disciplines illuminate the shadows cast by cybercrime: computer forensics and network forensics. While both share the overarching goal of uncovering evidence, their methods and areas

of focus diverge significantly. Understanding these differences is crucial for effectively investigating and combating security incidents.

Traditional computer forensics, the more established discipline, delves into the digital devices themselves. Imagine a meticulous investigator meticulously examining a computer, hard drive, or mobile phone. Their goal: is to identify traces of criminal activity, such as deleted files, hidden folders, malware remnants, and browsing history. The data source for this investigation lies within the storage media of these devices – hard drives, SSDs, and USB drives. This data is primarily static, consisting of files, system logs, and registry entries. The investigator's crucial first step involves creating a forensic image, a bit-by-bit copy of the storage media, to preserve the data in its original state. Following this, specialized forensic tools are employed to examine the image for evidence, a process that may involve data carving, file system analysis, and registry examination. Finally, the findings of the investigation are documented in a detailed report, outlining the methodology employed, the evidence collected, and the conclusions reached.

Network forensics, on the other hand, shifts the focus to the dynamic realm of network traffic. Imagine a detective following the flow of information through a network, instead of examining individual devices. Here, the investigator seeks to capture, analyze, and preserve network traffic data for the purpose of identifying and investigating suspicious activity. The data source for network forensics is the ever-flowing stream of information traversing the network, captured in the form of packets transmitted across it. Unlike the static data of computer forensics, this data is dynamic, consisting of protocols, IP addresses, and even the content of communications (if not encrypted). The investigator's challenge lies in the very nature of network traffic – its volatility. Unlike data on a storage device, once a packet is transmitted, it is gone unless captured beforehand. This fleeting nature necessitates proactive measures such as continuous traffic capture. The process of network forensics follows a similar structured approach: capturing the traffic data using specialized tools, preserving it in a forensically sound manner, analyzing it using network forensic tools to identify protocols, content, and potentially malicious activity, and finally, documenting the findings in a detailed report.

As cybercriminals develop increasingly sophisticated tactics, organizations require a robust arsenal of tools and techniques to combat these threats. Network forensics emerges as an indispensable weapon in this fight, acting as a digital detective meticulously examining the cybercrime scene – the network traffic itself. By analyzing captured network data, investigators can uncover evidence of malicious activity, reconstruct the timeline of attacks, and ultimately, identify the perpetrators. This understanding empowers security teams to effectively respond

to incidents, mitigate damage, and fortify their defenses against future attacks. The importance of network forensics stems from the very nature of today's digital landscape.

Traditional cyberattacks often involve physical access or targeted malware on individual devices. Today, the focus has shifted towards network-based attacks. Exploits leverage vulnerabilities in network protocols and configurations, allowing attackers to gain access to systems and data without ever physically setting foot on-site. For instance, the infamous SolarWinds supply chain attack compromised a network management software platform, allowing attackers to gain access to numerous organizations through software updates. Network forensics becomes crucial in such scenarios, as it allows investigators to identify the malicious network traffic used by attackers to compromise systems.

Unlike physical crimes that leave tangible evidence behind, cybercrimes often occur in the virtual realm, leaving behind faint digital footprints. Network forensics provides the tools and techniques to capture and analyze these fleeting traces of activity, enabling investigators to reconstruct the sequence of events and identify the perpetrators. Data is the lifeblood of modern organizations. As its value continues to rise, so do the threats targeting it. Network forensics plays a crucial role in investigating data breaches and exfiltration attempts. By analyzing network traffic patterns, investigators can identify unauthorized access attempts and pinpoint the data that might have been stolen. For instance, the Equifax data breach resulted in the compromise of sensitive personal information of millions of individuals. Network forensics analysis of the attacker's network traffic could potentially reveal the types of data exfiltrated and the methods used for data transfer.

Modern networks are complex ecosystems, encompassing a diverse range of devices, applications, and protocols. This complexity creates blind spots for security teams and provides potential avenues for attackers to exploit. Network forensic tools offer deep visibility into network traffic, enabling investigators to identify anomalies and suspicious activity that might otherwise go unnoticed. Imagine a large healthcare organization with a sprawling network connecting various medical devices, patient databases, and administrative systems. Network forensics can be used to analyze traffic patterns within this complex network, potentially revealing unauthorized access attempts from unauthorized medical devices or unusual communication patterns that might indicate a malware outbreak.

The increasing adoption of cloud computing presents both opportunities and challenges for network forensics. While cloud providers offer robust security

CHAPTER 7

Unmasking Web Browser Artifacts

Abstract: Web browser forensics plays a crucial role in digital investigations, offering insights into an individual's online activities and behavior. This chapter delves into the intricacies of web browser forensics, exploring methodologies, tools, and challenges encountered in extracting and analysing data from various browsers. Through a comprehensive examination, this chapter aims to equip forensic professionals and researchers with the necessary knowledge and techniques to effectively conduct investigations involving web browsers. This chapter provides a comprehensive overview of web browser forensics, encompassing methodologies, tools, challenges, and best practices. By equipping forensic professionals and researchers with the requisite knowledge and techniques, this chapter aims to enhance the efficacy and accuracy of investigations involving web browsers, ultimately contributing to the advancement of the forensic field.

Keywords: Acquisition, Analysis, Browser artefact, Parsing, Presentation, Reporting, Timeline.

INTRODUCTION

Web browsers have become integral components of modern computing, serving as gateways to the vast expanse of the internet. With the proliferation of online activities ranging from communication and commerce to entertainment and education, web browsers store a treasure trove of digital evidence crucial for forensic investigations. The examination of web browser artifacts [1] has emerged as a specialized field within digital forensics, enabling investigators to reconstruct an individual's online behavior, and uncover vital clues and insights. This introduction serves as a comprehensive primer on web browser forensics, elucidating key concepts, methodologies, and challenges encountered [2] in the analysis of browser-related data. It begins by elucidating the significance of web browser forensics in contemporary digital investigations, highlighting its relevance in uncovering evidence pertinent to criminal cases, cybersecurity incidents, and corporate misconduct. Subsequently, the introduction delves into the fundamental components of web browsers, elucidating their architecture and the mechanisms underlying data storage and retrieval.

Akashdeep Bhardwaj, Pradeep Singh & Ajay Prasad

Detailed examination of browser artifacts follows in subsequent sections, encompassing cookies, browsing history, cache files, bookmarks, and download records, among others. Through illustrative examples and case studies, this introduction underscores the pivotal role of web browser forensics in elucidating the digital footprints left behind by users, thereby facilitating the reconstruction of events and aiding in the attribution of activities to specific individuals or entities. Finally, the introduction delineates the overarching structure of the chapter, providing a roadmap for subsequent discussions on methodologies, tools, challenges, and future directions in web browser forensics.

It is imperative to delve deeper into the methodologies employed in web browser forensics. This involves elucidating the processes and techniques utilized to extract, analyse, and interpret browser artifacts effectively. Methodologies in web browser forensics encompass both manual and automated approaches, each with its advantages and limitations. Manual analysis involves the meticulous examination of browser data through forensic tools and scripts, allowing investigators to scrutinize artifacts in detail and uncover hidden traces left behind by user activities. Conversely, automated analysis leverages specialized tools and software to expedite the extraction and analysis of browser artifacts, enabling investigators to process large volumes of data efficiently. However, automated approaches may overlook nuanced details that could be crucial in certain investigations, highlighting the importance of a balanced approach that integrates both manual and automated techniques.

Moreover, the chapter delves into the diverse array of forensic tools available for web browser analysis, ranging from open-source utilities to commercial software suites. These tools facilitate the acquisition, parsing, and visualization of browser data, enabling investigators to navigate through complex datasets and derive actionable insights. Additionally, considerations pertaining to data integrity, preservation, and chain of custody are addressed, underscoring the importance of adhering to best practices and legal standards throughout the forensic process. Furthermore, the chapter explores the challenges encountered in web browser forensics, including encryption, anti-forensic techniques, and platform-specific idiosyncrasies. Encryption mechanisms employed by modern browsers pose significant hurdles to forensic analysis, necessitating innovative approaches to circumvent encryption barriers and recover encrypted data. Likewise, the proliferation of anti-forensic tools and techniques complicates the forensic landscape, requiring forensic examiners to adapt and evolve their methodologies continually.

BROWSER ARTIFACTS

Web browser artifacts [3] are the digital footprints left behind by users as they interact with web browsers. These artifacts encompass a diverse range of data elements stored by browsers during typical browsing activities [4]. Understanding and analysing these artifacts is crucial in digital forensic investigations, as they can provide valuable insights into an individual's online behavior, preferences, and activities. In this section, we delve into the intricacies of web browser artifacts, examining their types, locations, significance, and methodologies for extraction and analysis.

Types of Web Browser Artifacts

Cookies

Cookies [5] are small text files stored on a user's device by websites they visit. They contain information such as site preferences, login credentials, and tracking data. Cookies play a crucial role in web browser forensics, as they can reveal a user's browsing history, interests, and interactions with specific websites.

Browsing History

Browsing history [6] records the URLs of web pages visited by the user, along with timestamps. Analyzing browsing history can provide insights into the user's online activities, interests, and the chronology of their browsing sessions.

Cache Files

Cache files [7] store copies of web pages, images, and other resources locally on the user's device to expedite subsequent page loads. Examining cache files can reveal the websites visited by the user, even if the browsing history has been cleared.

Download History

Download history [8] records the files downloaded by the user through the browser. This artifact can provide information about the types of files accessed by the user and their sources.

Bookmarks

Bookmarks [9], also known as favourites, are shortcuts to specific web pages saved by the user for easy access. Analyzing bookmarks can offer insights into the user's interests, frequently visited websites, and organizational preferences.

CHAPTER 8

Anti-forensics Techniques

Abstract: Anti Forensics is a collection of methods and approaches to obstruct and avoid Digital Forensic investigations. For legal purposes, like criminal investigations or civil lawsuits, Digital Forensics includes gathering, preserving, analyzing, and presenting digital evidence. To make it more difficult for Forensic analysts to reconstruct events, assign acts to particular people, or prove guilt or innocence, people or organizations use Anti-Forensic strategies to obfuscate, distort, or delete digital evidence. The chapter presents techniques procedures and countermeasures for digital anti-forensics. The chapter also discusses anti-forensics ethical and legal ramifications.

Keywords: Anti-forensics, Cybercrime, Digital evidence, Digital forensics.

INTRODUCTION

Almost every human action in the modern world is connected in some way to one or more digital footprints. Because of this, Digital Forensics is now used in practically all cases, whether they are civil or criminal. A subfield of forensic science called “Digital Forensics” [1] is concerned with the recognition, storage, examination, and presentation of digital evidence in court. Finding information relevant to civil lawsuits, criminal investigations, or cybersecurity matters requires applying scientific methods and techniques to the gathering, analysis, and interpretation of data from digital devices and systems.

Digital forensics investigations follow a rigorous, consecutive process [2] as presented below:

i. Identification of digital devices and data sources relevant to an incidence.

ii. Maintaining the authenticity and custody chain of digital evidence to guarantee its acceptance in a court of law.

iii. Collection of digital evidence using forensically sound techniques to prevent alteration or contamination.

iv. Examination of the acquired data using specialized tools and techniques to extract relevant information and artifacts.

Akashdeep Bhardwaj, Pradeep Singh & Ajay Prasad

v. Analysis of the findings to reconstruct events, identify patterns, establish timelines, and attribute actions to specific individuals or entities.

vi. Presentation of the findings and conclusions in a clear, concise, and legally defensible manner, often through written reports or expert testimony in court.

Digital Forensics gathers, examines, and analyzes digital evidence using a range of methods and instruments. This includes network monitoring tools for recording and analyzing network traffic [3], Forensic analysis software [2] for parsing and interpreting data, Forensic imaging tools for making bit-by-bit copies of storage devices, and specialized hardware for removing data from embedded systems and mobile devices. Digital Forensics experts must follow all legal and ethical guidelines when conducting their investigation. This entails securing the required approval to carry out the investigation [4], guaranteeing the authenticity and admissibility of digital evidence, upholding people's right to privacy, and protecting the security and confidentiality of sensitive data. Since digital forensics offers insightful information about digital activity, it is essential to contemporary law enforcement [5], cybersecurity, and legal processes [6].

Contrary to the above statement, a digital investigator must be aware of such methods and be ready to overcome such situations where anti-forensics has been employed. Thus, Anti-Forensic Countermeasures [7] define certain tools and techniques designed specifically to detect and mitigate anti-forensic activities, employed by forensic investigators and security professionals. Anti-forensic tactics in cybercrime deal with examining how cybercriminals utilize anti-forensic techniques to cover their tracks and evade law enforcement [8].

Anti-forensics techniques can be viewed in the following three categories in terms of the approaches that are involved:

- Data Security tactics [9].
- Evidence Destruction tactics [10].
- Evidence Manipulation tactics [11].
- Obfuscation tactics [12].

Fig. (**1**) presents an outline of various means and methods of the above categories. The further sections of the chapter will discuss these in detail with various forensics countermeasures. The use of anti-forensic techniques raises important legal and ethical considerations [13]. While individuals may employ such tactics to protect their privacy or security, their use in criminal activities can have serious legal consequences. Additionally, the legality and admissibility of evidence obtained through anti-forensic methods [14] may be contested in court. Anti-

Forensics represents a cat-and-mouse game between those seeking to conceal their digital activities and those tasked with uncovering and analysing digital evidence. As technology continues to evolve, both forensic analysts and adversaries will continue to develop and refine their techniques in this ongoing battle.

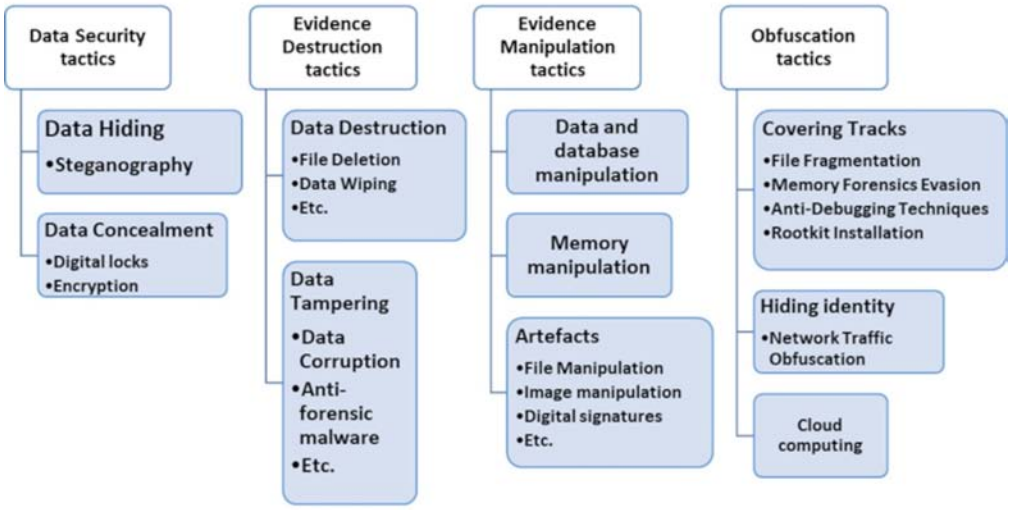

Fig. (1). Methods employed in Anti-Forensics..

ANTI-FORENCIS TACTICS

Several anti-forensics tools like cryptography, steganography, *etc*. are readily available as means of anti-forensics. These technologies can be used by the offenders to conceal or hide the evidence such that it can be found or opened while evidence gathering.

CRYPTOGRAPHY

The technique of secure communication with third parties, sometimes known as adversaries, is known as cryptography. It includes methods for data encryption and decryption to guarantee authenticity, confidentiality, and integrity. To put it briefly, cipher text (encrypted data) is created from plaintext (unencrypted data) using mathematical techniques, and vice versa. It is extensively utilized in many different applications, such as data protection, secure texting, e-commerce, and online banking, and it allows parties to interact securely over unsecured networks. Because it makes it possible for people or organizations to hide and shield sensitive data from forensic examination, cryptography is important to anti-forensics [15]. The notorious Silk Road [16] was a dark web black market that allowed the trade of illegal drugs, guns, and other contrabands. The mastermind behind Silk Road, and Ross Ulbricht, used various anti-forensic tactics to conceal his identity and evade law enforcement.

CHAPTER 9

Forensics Investigation Reporting

Abstract: Digital forensic investigation reports are integral components of forensic examinations, providing comprehensive documentation of the investigation process, methodologies employed, and findings unearthed. In a landscape inundated with digital complexities and evolving cyber threats, these reports serve as vital tools for legal proceedings, regulatory compliance, and organizational security measures. The chapter presents a set of abstract templates that may assist investigators to plan and document their proceedings. The sections will guide the investigators towards proper and foolproof case records and evidence collection. By documenting lessons learned and best practices, one can foster continuous improvement in digital forensic techniques. Ultimately, digital forensic investigation reports uphold the credibility and reliability of investigative outcomes.

Keywords: Chain of custody, Digital forensics, Digital evidence, Investigations, Investigation report.

INTRODUCTION

Digital investigations [1] employ methodical methodology to guarantee a comprehensive analysis of digital evidence while preserving data integrity. The steps in a digital forensic inquiry are as follows:

Step 1: Case Assessment and Planning [2]:

• Recognize the circumstances surrounding the case, such as the alleged offense, incident specifics, and the investigation's goals.

• Establish the investigation's parameters, the resources required, and any applicable legal issues.

• Create an investigation strategy that outlines the necessary actions, such as gathering, analysing, and reporting evidence.

Step 2: Evidence Identification [3]:

• Determine which digital evidence sources to look for, such as servers, mobile devices, PCs, network logs, and cloud storage.

Akashdeep Bhardwaj, Pradeep Singh & Ajay Prasad

• Keep track of the location, kind, and significance of every possible piece of evidence.

Step 3: Acquisition and Preservation of Evidence [4]:

• Make sure there is no illegal access to the crime scene by keeping it secure.

• To gather digital evidence while preserving its integrity, use the right methods and equipment. This includes taking forensic pictures of storage devices.

• To guarantee that any piece of evidence is admissible in court, record the chain of custody for each item.

Step 4: Analysis and Evaluation of the Evidence [5]:

• Examine the gathered evidence in-depth utilizing forensic instruments and methods.

• Examine digital artifacts, files, logs, and metadata to piece together what happened, find pertinent details, and find hints that might lead to it.

• To retrieve information, use forensic methods such as chronology analysis, data carving, and keyword searches.

Step 5: Data Reconstruction and Recovery [6]:

• Recover information that has been buried or erased that might be important to the inquiry.

• Reconstruct digital events and activities to comprehend the order in which persons engaged took their respective actions.

• Reconstruct files, emails, chat discussions, and other digital artifacts using specialist tools and techniques.

Step 6: Documentation and Reporting of Evidence [7]:

• Keep thorough records of all observations, findings, and analysis outcomes.

• Write reports that are easy to read and understand, summarizing the methods utilized, the findings, and the investigative process.

a. Provide pertinent logs, timestamps, screenshots, and other proof in the reports.

b. Make sure the reports meet all legal criteria and are appropriate for presenting in court.

Step 7: Reporting of Results [7]:

• Report the investigation's conclusions to the appropriate parties, including management, legal counsel, and law enforcement.

• If called upon in court, give expert testimony on the procedures and findings of the forensic analysis.

Step 8: Closure and Follow-Up [8]:

• Once all goals have been achieved and the matter has been settled, end the investigation.

• Make sure that case closure is properly documented, including final reports, how evidence is handled, and any necessary follow-up activities.

• To find opportunities for improvement in subsequent investigations and lessons learned, conduct a review of the investigation process.

To guarantee a successful digital forensic investigation, it is essential to follow legal and ethical norms [9] and [10], protect the integrity of the evidence, and maintain confidentiality throughout these procedures.

Proper reporting [11] plays a crucial role in digital forensics investigations for several reasons:

• Documentation: Reports provide comprehensive documentation of the investigation process, including the steps taken, methodologies used, and findings obtained. This documentation ensures transparency and accountability in the investigation process.

• Legal Admissibility: Well-documented reports increase the credibility and admissibility of digital evidence in legal proceedings. Courts and regulatory bodies require clear documentation of the investigation process to ensure the integrity and reliability of the evidence presented.

• Communication: Reports serve as a means of communication between forensic examiners, investigative teams, law enforcement agencies, legal counsel, and other stakeholders involved in the investigation. They convey important information, findings, and recommendations in a clear and organized manner.

SUBJECT INDEX

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W

Akashdeep Bhardwaj

Akashdeep Bhardwaj is working as professor and head of the cybersecurity (Center of Excellence) at the University of Petroleum & Energy Studies (UPES), Dehradun, India. An eminent IT Industry expert, Akashdeep mentors graduates, masters and doctoral students and leads several industry projects. Prof. Akashdeep has done post-doctoral work from Majmaah University, Saudi Arabia, and a doctoral in computer science from University of Petroleum and Energy Studies, Dehradun, India. He has published over 135 research papers in international journals. He has worked as technology leader for several multinational organizations during his time in the IT industry. Prof. Akashdeep is certified in multiple technologies.

Ajay Prasad

Ajay Prasad is working as cluster head and professor at the University of Petroleum and Energy Studies (UPES), Dehradun, India. Prof. Ajay has been working with cyber cell training the police and investigation agencies. Prof. Ajay is also an active reviewer in many international journals and conferences and has been highly instrumental in organizing many international conferences including the in-house Next Generation Computing Technologies (NGCT) in UPES, since the year 2015.

Pradeep Singh

Pradeep Singh is currently working as senior lab assistant in the Cybersecurity Center of Excellence at the University of Petroleum & Energy Studies (UPES), Dehradun, India. Prof. Pradeep Singh has completed his master's in cybersecurity degree from Uttarakhand Open University Haldwani, India and currently works in the digital forensics domain.