

Resolving Windows Forensic Artifacts in Windows 10



By

Maryam Zubair

(Registration No: 00000430008)

A thesis submitted to the National University of Sciences and Technology, Islamabad,

in partial fulfillment of the requirements for the degree of

Master of Science in

Cyber Security

Supervisor: Cdre. Dr. Nadeem Kureshi

Pakistan Navy Engineering College (PNEC)

National University of Sciences & Technology (NUST)

Islamabad, Pakistan

(2024)

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS thesis written by **Maryam Zubair** Reg No. **00000430008** of NUST- **PNEC** (College) has been vetted by undersigned, found complete in all respects as per NUST Status/Regulations, is free of plagiarism, errors, and mistakes and is accepted as partial fulfillment for award of MS degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have been incorporated in the said thesis.

Signature: _____ *nn*

Name of Supervisor Cdre Dr. Nadeem Kureshi

Dated: 27-03-24

Signature: HoD _____ *Aaliya Ali*

Dated: 27-03-24

AALIYA ALI
Lt Cdr Pakistan Navy
HOPGP Cyber Security
PNS Jauhar

Signature: (Dean/Principal): _____ *Uzma Khalid*

Dated: 27-03-24

UZMA KHALID
Cdr Pakistan Navy
HOD Computer Science
PNS Jauhar

APPROVAL

It is certified that the contents and form of the thesis entitled "Resolving Windows Forensic Artifacts in Windows 10" submitted by Maryam Zubair have been found satisfactory for the requirement of the degree.

Advisor: Cdre Dr Nadeem Kureshi

Sig: nk
Date: 27-03-24

Committee Member Dr. Ayaz Sherazi

Signature: MS

Date: 27-03-24

Committee Member Lt Cdr Aaliya Ali PN

Signature: Aaliya

Date: 27-03-24

National University of Sciences and Technology

MASTER'S THESIS WORK

We hereby recommend that the dissertation prepared under our supervision by: (Student Name & Reg No) Maryam Zubair (Reg No 00000430008) Titled: "Resolving Windows Forensic Artifacts in Windows 10" be accepted in partial fulfillment of the requirements for the award of Master's degree

EXAMINATION COMMITTEE MEMBERS

1. Name: Dr. Ayaz Sherazi

Signature: 

2. Name: LT Cdr Aaliya Ali PN

Signature: 

Supervisor's name: Cdre Dr Nadeem Kureshi

Signature: 


Date: 27-03-24


AALIYA ALI
Head of Department
HOPGP Cyber Security
PNS Jauhar

27-03-24
Date

COUNTERSIGNED

Date: 27-03-24


Dean/Principal
Cdr Pakistan Navy
HOD Computer Science
PNS Jauhar

CERTIFICATE FOR PLAGIARISM

1. It is certified that PhD / M.Phil / **MS** Thesis Titled "**Resolving Windows Forensic Artifacts in Windows 10 – PN as test subject**" by **Maryam Zubair (REG No 00000430008)** has been examined by us. We undertake the follows:

- a. Thesis has significant new work / knowledge as compared already published or is under consideration to be published elsewhere. No sentence, equation, diagram, table, paragraph or section has been copied verbatim from previous work unless it is placed under quotation marks and duly referenced.
- b. The work presented is original and own work of the author (i.e. there is no plagiarism). No ideas, processes, results or words of others have been presented as Author own work.
- c. There is no fabrication of data or results which have been compiled / analyzed.
- d. There is no falsification by manipulating research materials, equipment, or processes, or changing or omitting data or results such that the research is not accurately represented in the research record.
- e. The thesis has been checked using TURNITIN (copy of originality report attached) and found within limits as per HEC Plagiarism Policy and instructions issued from time to time.



Name & Signature of Supervisor

DR NADEEM KURESHI
Commanding
DEAN MIS
PNS JAUHAR

AUTHOR'S DECLARATION

I Maryam Zubair hereby state that my MS thesis titled "Resolving Windows Forensic Artifacts in Windows 10" is my own work and has not been submitted previously by me for taking any degree from National University of Sciences and Technology, Karachi or anywhere else in the country/ world.

At any time if my statement is found to be incorrect even after I graduate, the university has the right to withdraw my MS degree.

Name of Student: Maryam Zubair

Date: 27-4-2024

To the guiding lights of my life,

To my father, whose unwavering support and wisdom shaped the foundation of my dreams. Your memory fuels my determination, and I dedicate this thesis to the lessons you imparted and the love that continues to inspire me. To my resilient mother, whose sacrifices and love are the foundation of my strength. To my siblings, the source of shared laughter and enduring bonds. To my precious daughter, your joy fuels my purpose. To my husband, your unwavering support is my anchor in life's journey. To my teachers, your guidance shaped my intellect. To my supervisor, your mentorship was invaluable. This thesis is dedicated to each of you—my pillars of love, support, and inspiration. I am grateful for the impact you've had on my life and academic journey.

ACKNOWLEDGEMENTS

I extend my deepest gratitude to Cdre Dr. Nadeem Kureshi, not only for his role as my esteemed supervisor but also as the Dean of the department. His guidance, support, and unwavering commitment to academic excellence have been instrumental in shaping this thesis. I would also like to express my sincere appreciation to the members of the GEC, Dr. Ayaz Sherazi and Lt Cdr Aaliya Ali PN, for their valuable insights, constructive feedback, and dedication to fostering a rigorous academic environment. To my beloved daughter, whose understanding, patience, and encouragement sustained me throughout this academic journey. Your presence added a dimension of joy and purpose to each step of the way. To my husband, whose unwavering support and belief in my abilities were my constant motivation. Your encouragement was a driving force behind the completion of this thesis. To my sibling, thank you for being a source of inspiration and a pillar of support during both challenging and triumphant moments. Each of you played a pivotal role in this academic endeavor, and I am profoundly grateful for your contributions, encouragement, and belief in my capabilities. This achievement is a reflection of our collective efforts and the strength derived from your support.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS	viii
TABLE OF CONTENTS	viii
LIST OF TABLES	x
LIST OF FIGURES	xi
LIST OF SYMBOLS, ABBREVIATIONS AND ACRONYMS	XII
ABSTRACT	xiii
CHAPTER 1 : INTRODUCTION	1
1.1 Background	1
1.2 Research Objective	4
1.3 Contribution	4
1.4 Structure	5
CHAPTER 2 : LITERATURE REVIEW	7
2.1 Digital Forensics	7
2.1.1 Background	7
2.1.2 Definition of Digital Forensics	7
2.1.3 Digital Artefacts	8
2.1.4 Forensics Needs	9
2.1.5 Digital Forensics Process	9
2.1.6 Computer Crimes	10
2.2 International Standards	11
2.2.1 Digital Forensics Tools	11
2.2.2 Forensics Frameworks	14
2.2.3 Other Sources	17
2.3 Research Gap	17
CHAPTER 3 : METHODOLOGY	19
3.1 Introduction	19
3.2 Windows 10 OS	19
3.3 Significance of Windows 10 Artifacts used in study	20
3.3.1 Shimcache	20
3.3.2 Prefetch	20
3.3.3 Shellbags	21
3.3.4 Update Sequence Number Journal	21
3.3.5 UsuserAssist	21
3.3.6 Windows Event Logs	22
3.3.7 LNK Files	22
3.3.8 Windows Registry	23
3.3.9 Logs File	23
3.4 Experimental Setup	24
3.4.1 Case Study	24
3.4.2 Analysis Approaches	25

3.4.3	Forensic Image	26
3.4.4	Abstract Workflow	27
3.4.5	Workflow using two FTs	27
CHAPTER 4 : EXPERIMENTS AND RESULTS		29
4.1 Comparative study of FTs		29
4.2 Evaluation Parameters		29
4.2.1	Selection of FTs	29
4.2.2	Accuracy	29
4.3 Results of FTs used in study		30
4.3.1	FTK Imager	30
4.3.2	Registry Explorer	30
4.3.3	Autopsy	32
4.3.4	Regripper	34
4.3.5	Regshot	35
4.3.6	Access Data Registry Viewer	37
4.3.7	Sysmon Analyzer	38
4.3.8	Prefetch Analysis	40
4.3.9	Other System Artifacts	40
4.4 Discussion		43
4.5 Framework for Reporting and Presenting Digital Forensics Investigations		45
4.5.1	Introduction	45
4.5.2	Present case evidence in the legal context	46
4.5.3	Components of framework	47
4.5.4	Workflow of framework	47
4.5.5	Discussion	48
4.5.6	Users of proposed framework	51
CHAPTER 5 : RECOMMENDATIONS FOR EFFECTIVE FORENSICS MANAGEMENT		52
5.1 Introduction		52
5.2 Guidelines objectives		54
CHAPTER 6 : CONCLUSION AND FUTURE WORKS		55
6.1 Introduction		55
6.2 Applications at National level		55
6.3 Potential challenge and future work		56
REFERENCES		57

LIST OF TABLES

Table 1: OS related features via FTs	44
--	----

LIST OF FIGURES

Figure 1: Complete Forensics Process.....	27
Figure 2: Workflow using two Forensics Tools.....	28
Figure 3 CCleaner installed on system running Windows 10.....	31
Figure 4 CCleaner Un installed.....	31
Figure 5: Document Creation.....	32
Figure 6: Document Movement.....	32
Figure 7: Document MAC details.....	33
Figure 8: Software installation.....	33
Figure 9: Document emailed.....	34
Figure 10: Email address details.....	34
Figure 11: Rip process.....	35
Figure 12: Software installation through regripper.....	35
Figure 13: User details.....	36
Figure 14: Monitoring installation changes.....	36
Figure 15: Uninstallation changes.....	36
Figure 16: Installation path.....	36
Figure 17: Installation details.....	37
Figure 18: User details.....	37
Figure 19: Software Installation Details.....	37
Figure 20: User Details through Windows Event Logs.....	38
Figure 21: Software used to delete document.....	39
Figure 22: Document emails.....	39
Figure 23: Display name of User.....	40
Figure 24: Document deletion via Recycle bin.....	40
Figure 25: Run Count of CCleaner.....	40
Figure 26: Software Installation Details.....	41
Figure 27: Executable details.....	41
Figure 28: Shellbags analysis.....	42
Figure 29: Shellbags analysis via Shellbag Explorer.....	43
Figure 30: Workflow of framework.....	47

LIST OF SYMBOLS, ABBREVIATIONS AND ACRONYMS

DFMs	Digital Forensic Models
AF	Anti-Forensic
DF	Digital Forensic
CFT	Computer Forensics Tools
FTs	Forensics Tools
D4I	Digital Forensics Framework for Reviewing and Investigating Cyber-Attacks
SRDFIM	Systematic Digital Forensic Investigation Model
CFFTPM	Cyber Forensic Field Triage Process Model
IDFPM	Integrated Digital Forensics Process Model
OS	Operating System
FH	File History
Sysmon	System Monitor
NTFS	New Technology File System UsnJrnl
UsnJrnl	Update Sequence Number Journal
LNK	Link
CobiT	Control Objectives for Information and associated Technology

ABSTRACT

While the swift advancement and widespread usage of digital technology has greatly aided computer users in their jobs, there has also been a rise in digital occurrences. When computer machines are the victim of cyberattacks, specific artefacts are left on the target device storage that, when properly processed and analyzed, can disclose the identity and actions of cybercriminals. Forensic investigators mostly depend on meta-data and other artefacts stored by contemporary operating systems as computer crimes grow in frequency and sophistication. Microsoft Windows OS is utilized extensively across the globe and serves as the main target for modern attackers. When artefacts are positively identified, it can reveal information about how the user has interacted with installed programs and Microsoft applications. This research is conducted utilizing open-source tools to identify forensic artefacts in Windows 10 logs and, eventually, evaluate tool capabilities. It will streamline the different artefact collection processes and offer a quick reference guide for investigations. Additionally, because of insufficient instructions in reporting phase, digital forensic techniques are unable to offer comprehensive assistance for a cyber-attack investigation. This research suggests a methodical and comprehensive framework for illustrating distinct phases of genuine decision making, along with a procedure that an expert must follow in assessing the precision of case results to bolster legal actions.

Keywords: Windows Forensics, open-source tools, forensics framework management, digital evidence, IT governance, Windows 10.

CHAPTER 1 : INTRODUCTION

1.1 Background

Today, our world is rapidly dependent on digital devices and getting complex due to frequent technological advancements and interconnected devices. Every home, organization has a lot of digital devices, computer networks for communication and IoT devices has further complicate this situation (Rowlingson, 2004). Technology caused people to share their sensitive information via email, community / discussion groups and smart devices.

The development of huge amount of data also created problems like storage and security. World is increasingly moving towards digitization and crossing every milestone with every passing day. However, one problem which still persists from first day is safety of communication networks and data. Hackers are also going advance and used latest technology to gain insights. Although, development on both sides is take place but the safety of information is still a big problem.

The development of intelligent devices has posed a great threat to safety of organization. Today, major financial and national security institutions spent millions of dollars for safety of IT infrastructure, trained HR, security awareness and incident response. All these steps are still unable to resist cyber-crimes. The ratio and complexity with which cyber-crimes is increasing raised alarms for researchers and IT experts.

Most of the organizations lack basic facilities in their trusted areas including above sited issues. All these factors can be easily exploited by an attacker. Gain of unprivileged access to database, confidential files, exfiltration of data to outside network has become a matter of seconds. Above all, now it is very easy to erase the traces of any activity with the help of anti-forensics software(s). This increment has highlighted many shortcomings in our working environment like:

1. **Lake of proper and consistent training:** Awareness of current attacks and their countermeasure may be achieved through regular training. Well trained team can better cope up with untoward situation. Every person should know the occurrence of an event and set of actions expected from him.
2. **Technological obsolescence in small / medium organizations:** Due to non-standard practices, most of the organizations are reluctant to conduct cyber incident investigation. Acquisition of latest technologies, maintenance and training requires a lot of finances which is very difficult to allocate in every fiscal year. Large organizations although, spend huge amount but lack of proper planning and auditing hinder to get benefit from.
3. **Lack of regulatory laws:** Collecting evidence through lawful means is very critical and main objective for any investigative team. Legal standing of organization team is very crucial when they undergo in any trial. Organization policies, adherence to international standards, usage of industry accepted softwares and frameworks further strengthen the legal teams.
4. **Structure of Organization:** The creation of reporting structure is essential for the DF group. In case of cyber incident, it is very critical for organization to decide appropriate internal department to report to such as compliance, legal or risk management. Using the outsource forensics facilities by the organization is equally cumbersome as it brings new challenges of data privacy and security. Moreover, the forensics team's role inside the organization must also be identified, including whether they are leading, advising, or supporting.
5. **Lake of incidence response capability in most organizations:** Appropriate equipment and qualified / certified personnel are crucial to conduct internal investigations. Tools, training and state of the art infrastructure go side by side for success of any investigation.

Most of institutions does not have any knowledge about investigation of such crimes. If an organization attempted to investigate an incident, it does not have capabilities to conduct this activity at org level. Organizational framework and policies are crucial for the success of investigation. Even outsourcing investigation also possess multiple

questions at the capabilities and IT infrastructure at national level which hampers national and financial institutes to conduct incident investigation with true letter and spirit.

Although organizations are moving towards better management of their IT infrastructure and security of their data. But mostly organization still lack basic capabilities and dependent on outsource facilities for any incident handling. In case of any major incident, finding of right capabilities in low budget become very difficult for most of institutions. The basic requirements of any investigation require few things to be implemented like:

1. Proper logging of actions
2. Management / maintenance of implemented controls
3. Regular Auditing
4. Acquisition of investigative capabilities
5. Allocation of fix amount (at-least) in every budget for IT infrastructure

Although performing a forensic review of security vulnerabilities is important, many organizations do not have clear rules / guidelines, which frequently leads to inadequate results (Sinangin, 2002). Sometimes forensic review is not in the priority list of organization. In order for organizations to take proper action against wrongdoers in cases of abuse, computer forensics plays a critical role in safeguarding, conserving, and presenting evidence (Sheldon, 2004). It is critical to determine what caused the incident and comprehend the attacker's intentions.

Nowadays, DF tools and procedures are essential for any organization looking for meaningful and admissible evidence. It is essential to have forensic software, and guidelines (Guidance Software, 2005). A forensic expert must verify the veracity of the data and findings by applying well-established protocols, known as "frameworks."

Although DF technologies are essential for digital investigations and finding weaknesses in the information security architecture, companies use them for different objectives (Richardson, 2008). This entails strengthening information technology

governance structures and demonstrating compliance with laws (The Role of Digital Forensics within a Corporate Organization, 2006).

1.2 Research Objective

This research is mainly based on positive windows artifacts identification using various open-source tools for identification / reconstruction of computer crimes. A range of windows 10 artifacts will be explored in this work to effectively detect traces of existing or deleted files. The outcome of this research can have great potential to curb cyber-attack incidence in Pakistan. The research objectives are:

1. Literature review and survey of available best forensics investigation techniques.
2. To investigate the potential benefits of readily available tools in early extraction of relevant artifacts.
3. To explore various logs and their connection in Windows 10 for positive identification of suspicious activities using available tools.

In this way, investigators can guarantee a shorter investigation duration, offer evidence of compliance, and concentrate on a possible forensic investigation toolkit. When utilizing a tool in a certain context, it is important to be aware of its strengths and weaknesses.

1.3 Contribution

The following summarizes this research's primary contributions:

1. A unique digital forensics framework for cyber-crime reporting mechanism and generation of forensics capabilities that can be modified to support a multifaceted cyber incident and can be fitted easily in varied size organizations. This framework is designed on findings of open-source software(s) that can be equally useful for investigation.

2. A case study was conducted on Windows 10 OS for analysis of available open-source software(s). Windows 10 is the most popular OS worldwide. Keeping in view this fact, most relevant artifacts that could be or should be consider for forensics analysis are selected. Similarly, case study was designed meeting most seen incidents now a days. This comparative study will be useful in scenarios where outsource facilities are not the option.
3. A prioritization mechanism for collection of evidences and presentation phase of evidences are improved.

1.4 Structure

The remaining portions of this study are arranged as follows:

1. Chapter 2, will elaborate the history of digital forensics, its evolution, types and give detail explanation of various investigation phases involved in forensic process. It further highlights the various frameworks proposed over the time and explain how such frameworks play a pivotal role in conclusion of investigation.
2. Chapter 3, explains the significance of Windows OS and forensics artifacts generated during crime activity. This also explains the forensic tools used in this study and determining of appropriate softwares relevant to the crime. Comparative study of these tools will helpful in selection of softwares in case of non-availability of outsource digital forensics facilities. This chapter will also propose a framework which is equally applicable for low budget organizations for implementation.
3. Chapter 4, will analyze and compare results produced by various forensics softwares. The objective of this chapter is to provide guidelines about the viability of open-source tools in initial investigation of incident. It will further elaborate the significance of open-source tools for low budget organizations.

4. Chapter 5, suggest few recommendations in order to improve forensics practices at organization level. It emphasis on applying new techniques in placement of traditional forensics methods for early solution of the cases. It discusses the analysis done on case study and suggests a way forward.
5. Chapter 6 gives summary of the research project, along with a number of possible directions for future research and to provide some final remarks.

CHAPTER 2 : LITERATURE REVIEW

This chapter explains the significance of digital forensics and shed light on various aspects to help combat the cyber threat and compensate victims by upholding the law. Section 2.1 provides a detailed overview of the history of digital forensics, digital artefacts, the necessity of forensics, and the entire forensics process in light of NIST standardization. Section 2.2 elaborate diversified work carried out for development and assessment of forensics tools and management of various frameworks for court of law.

2.1 Digital Forensics

2.1.1 *Background*

The word "cyberspace" describes a borderless virtual society where communication is quick and anonymous in a digitally connected world. These benefits, meanwhile, can serve as a haven for cybercrime. Because of the growing value of information, criminals are better able to use computers for illegal purposes by leveraging their technological expertise and the anonymity they provide.

Cybercriminals frequently target particular industries, which causes financial losses for businesses. Based on Locard's Exchange Principle, a comprehensive inquiry is necessary in the event of a cyber incident (*Locard's Exchange Principle / Encyclopedia.com, 2013*).

The application of scientific techniques to legal matters is emphasized in several definitions of forensics. The preservation of the integrity of evidence in legal situations is contingent upon the investigative process in digital forensics. The quality of evidence is influenced by forensic equipment, whose admissibility in court plays a crucial role. This chapter lays out the fundamental basis of digital forensics while highlighting its importance and guiding ideas.

2.1.2 *Definition of Digital Forensics*

Within the field of forensic science, digital forensic science concentrates on the retrieval and examination of evidence connected to cybercrime that is discovered on digital devices. Initially, computer forensics and digital forensics were synonymous terms. Subsequently, it has broadened to encompass the examination of any gadgets capable of retaining digital information. Despite the fact that the Florida Computer Act and the first computer crime were documented in 1978 and 1979, respectively, the phrase "computer crime" did not gain attraction until the 1990s (EC-Council, 2023).

Digital forensics adheres to strict guidelines, such as the chain of custody and evidence principles, which are essential for evaluating digital evidence.

2.1.3 *Digital Artefacts*

Digital evidence, (Carrier & Spafford, 2005), is data that includes reliable information that either supports or refutes a claim about what happened.

Digital evidence, according to SWGDE and IOCE (2000), is binary-form data with probative value that incorporates digital audio and video in addition to conventional computers. Data that can establish the conduct of a crime or establish a link between the perpetrator and the act is referred to as digital evidence (Casey, 2004).

Criteria for evidence categorization set by (*Digital Evidence: Standards and Principles*, by SWGDE and IOCE (*Forensic Science Communications*, April 2000), 2020). These are the categories that are available:

1. **Category 1:** Consists of information that has been electronically or magnetically stored, transmitted, or eavesdropped on, including email messages, backups, logging information, and forensically retrieved information.
2. **Category 2:** Physical Evidence includes items that use physical media, such flash drives, to store or transport digital information.
3. **Category 3:** Data Objects are composed of metadata, directory information, and configuration data connected to physical objects or digital evidence.

Log files, file system activity, encrypted data, hidden images, erased files, password-protected files, memory content, active processes, and more can all be used to collect digital evidence.

2.1.4 Forensics Needs

The frequency of computer-related crimes has increased over the past ten years, which has led to a rise in businesses and goods that help law enforcement use computer-based evidence to figure out the who, what, where, when, and how of crimes. In order to ensure that evidence of computer crime is properly presented in court, the field of computer and network forensics has developed. Most people think of forensic tools and techniques in the context of computer security incidents and criminal investigations. These tools and techniques are used to gather and preserve evidence, reconstruct events, investigate suspect systems, and assess the current state of an event in response to an incident (Kent et al., 2006).

2.1.5 Digital Forensics Process

Finding and examining the relevant data can help one comprehend an event of interest better, which is the main objective of practicing forensics process. Forensics may be required in a variety of circumstances, including gathering evidence for court cases and internal disciplinary procedures, managing virus incidents, and handling peculiar operating issues. The four-phase method should be followed when performing forensics, regardless of the necessity. The specifics of these processes could change depending on the particular forensics requirement; the organization's policies, guidelines, and procedures should specify any deviations from the accepted practice (Kent et al., 2006).

1. **Collection:** Following policies and procedures that protect the integrity of the data, the initial stage of the process is locating, labelling, recording, and obtaining data from potential sources of pertinent data. Due to the possibility of losing dynamic data, such as active network connections, and data from battery-powered devices, such as cell phones and PDAs, collection is usually done in a timely way.

2. **Examination:** During an examination, a significant amount of acquired data must be forensically processed using both automatic and human techniques to identify and extract relevant data while maintaining the data's integrity.
3. **Analysis:** Subsequently, the examination results are analyzed using legally-justifiable methodologies and techniques in order to extract relevant information that answers the questions that motivated the collection and examination.
4. **Reporting:** The last step is to report the analysis's findings. This can involve outlining the steps taken, elaborating on the selection of tools and procedures, identifying any additional steps that need to be taken (such as forensic examination of additional data sources, securing found vulnerabilities, or enhancing current security controls), and making suggestions for how to improve the forensic process's policies, guidelines, procedures, tools, and other elements. Depending on the circumstances, the reporting step's formality changes significantly.

Whether evidence is required for internal use by an organization or for use by law enforcement, the forensic process turns media into evidence. In particular, the first transformation takes place during data collection and examination. This procedure involves removing data from media and transforming it into a format that forensic tools can analyze. Second, analysis is the process that turns data into information. Ultimately, turning information into evidence is similar to putting knowledge into practice since it involves employing the information gathered from the analysis in a variety of ways throughout the reporting stage. It might be used, for instance, as evidence to support the prosecution of a particular person, as useful knowledge to aid halt or lessen certain activities, or as insight into the development of fresh leads for a case (Kent et al., 2006).

2.1.6 *Computer Crimes*

Malware and cyberattacks have increased dramatically in recent years. The primary source of viruses and cyberattacks, which can occasionally seriously harm digital assets, is the Internet. Digital crimes can have a variety of motivations, including fraudulent program output, information theft, denial of service, online banking fraud, and data distortion. A cyberattack in the US state of Baltimore, where hackers seized a National Security tool and frozen thousands of systems, is one incident among many. Emails, real estate transactions, water bills, health alerts, and numerous other services were all affected by the three-week-long attack (Serketzis et al., 2019; Keshavarzi & Ghaffary, 2020; Niksefat et al., 2017). The yearly cost of pain is rising quickly; by 2021, experts predict it will reach \$6 trillion (Cybercrime to Cost the World \$10.5 Trillion Annually by 2025, 2018).

Cybercrime remains a persistent and dynamic threat as the Internet and its applications grow and the Information Society advances. Adware, malware, spoofing, phishing, and spam are some of the new threats (Johnson & Mack, n.d.).

As computers are the main targets of these malicious actions, evidence can be obtained from a variety of volatile and non-volatile storage media that are connected to computing systems.

2.2 International Standards

2.2.1 Digital Forensics Tools

In case of cyber incident, digital forensics is crucial for determining how malware operated or how hackers gained access to the system. This paper (Vasaka Visoottiviseth et al., 2023) focuses on Windows forensics, a significant area of computer forensics. Existing investigation technologies that are costly and require training to use can be used for Windows forensics, but there are currently not enough skilled people in the cybersecurity industry. Additionally, Windows forensic investigators must manually extract some data, like the Windows registry and event logs, during the evidence analysis process. This is a tedious and time-consuming task. As a result, authors suggested AXREL, an automated Windows evidence extraction tool with an intuitive graphical user interface, to help novice Windows forensic investigators. Python 3 is used to construct said application on the

Windows operating system. The main sources of data for Windows forensics are the Windows registry and event logs, which it can automatically extract.

Only the analysis and extraction of four hives from the Windows registry and event logs is supported by the AXREL. Other Windows artefacts that are crucial for Windows forensics, including NTUSER.dat, Windows prefetch files, shortcut (LNK) files, and so forth, should be supported which exposes its limited scope (Vasaka Visoottiviseth et al., 2023).

This paper (Wu et al., 2020) aims to identify software or forensic tools that have been developed largely for research and to analyze tools' additional aspects and any follow-up work. Digital forensics publications often include tools, which are tiny functioning software packages. These resources are frequently made available to the general public so that they can be used to duplicate the findings. To have a better understanding of the kinds of tools that are available and those that have disappeared owing to lack of maintenance, this work (Wu et al., 2020) manually analyzed almost 800 articles from relevant venues from 2014 to 2019. Following three research issues are addressed (Wu et al., 2020):

1. What tools (i.e., which digital forensics domains) have been made available;
2. Are they still maintained, up to date, and documented; and
3. Is it possible to improve the current situation?

The authors discovered 62 distinct tools that can be grouped based on the subfields of digital forensics. It was discovered that just 33 of these tools were accessible to the general public; most of them had not been maintained after development. A suggestion proposed in this paper (Wu et al., 2020) to improve the current situation is to create a centralized repository dedicated to tested tools. Because of this, tool researchers and developers will be able to devote more time to writing code documentation and, ideally, create plugins rather than standalone tools.

Digital forensics is used in this paper (Choi et al., 2021) to thoroughly examine the Windows FH function. Users can control and adjust the backup feature known as FH. Deleted files in unallocated areas are harder to retrieve these days due to the widespread

use of flash-memory-based storage devices. Files contained in backup target folders are backed up by FH once it is enabled.

To identify modified files, FH examines changes in the Update Sequence Number (USN) of backed-up files. Additionally, a three-stage examination process is suggested in this work (Choi et al., 2021), along with thorough considerations for each phase. The authors also examine the effects of a number of user-intentional or unintentional anti-forensic behaviors. Finally, an open-source tool for locating FH-related artefacts and examining user behavior during backup processes is also developed by this work.

Electronic evidence has grown in significance for legal processes and investigations in the age of digitization. To make matters worse, traceability is hampered by the ease with which anti-forensic tools and artefacts that were once employed for tracking can be erased. A unique framework for overcoming these constraints is presented in this research (Jihun Joun et al., 2023). This methodology makes it easier to trace residual files more precisely and thoroughly by using data remnants analysis, a forensic technique that looks for evidence of overwritten or deleted data.

Authors find and examine every data remnant in the system by methodically building a dataset on user behavior, which reveal file traces. Case study on Microsoft 365 has shown efficient and more accurate results and proof the viability of the suggested framework than the existing approaches. This method (Jihun Joun et al., 2023) helps with digital forensic investigations on Windows computers and provides insightful information on data remnants analysis.

DF field is entirely dependent on software programs and tools designed for collection, displaying, and analysis of digital data. Any further research that makes use of these FTs must produce consistent, dependable results that help establish the truth. Any mistakes made throughout the examination process have the ability to ruin the entire inquiry and jeopardize any findings that could be used as evidence. Undoubtedly, tool-testing is one of the most challenging problem of the DF domain (Horsman, 2019).

Although DF domain is highly dependent on digital forensic technologies, there are currently insufficient testing protocols and standards in place to verify their use during an investigation. Current state of FTs testing along with the challenges is examined in this article (Horsman, 2019). The article's findings offer a variety of perspectives on the consensus within the industry on tool dependability and testing. This growing worry stems from the demand that digital forensic companies must obtain ISO 17025 accreditation.

2.2.2 *Forensics Frameworks*

The purpose of this study (Dimitriadis et al., 2020) is to improve the inspection and analysis stages of the digital forensics process by putting forth a D4I framework. The two main components of the D4I are the suggested step-by-step instructional technique for analyzing and studying cyber-attacks, and the proposed categorization of artefacts and their mapping to the Cyber-Kill-Chain steps of attacks. By using the suggested D4I architecture, forensic examiners can undertake the examination and analysis phases to review and analyze a cyber-attack while selecting their preferred digital forensics procedure.

SRDFIM model (Agarwal, 2011) proposed which focused investigating cybercrime and cyberfraud as main objective. This model comprised of eleven phases which includes the analysis and examination. SRDFIM states that the examination phase's objectives are to find relevant evidence for the case, making it visible, and suitable for analysis. Data filtering, validation, pattern matching, searching strategies, recovering ASCII and non-ASCII data, locating odd hidden files or directories, file extension and signature mismatches, etc. are all suggested by SRDFIM. The data collected and extracted from the examination stage are technically reviewed during the analysis phase in order to find patterns, assess the data's importance, reconstruct the events, and make conclusions.

According to SRDFIM, analysis techniques include time frame analysis, analysis of hidden data, application analysis, file analysis, relationship analysis between data fragments, and analysis of hidden data. Because the model does not offer a systematic and sequential approach to conducting the examination and analysis stages, it is apparent that it is technique-centric (Agarwal, 2011).

To find, evaluate, and analyze digital evidence quickly, the authors (Rogers et al., 2006) devised the CFFTPM method. The model's main goal is to shorten the amount of time required to examine a crime scene. To obtain information from a Windows system, the model suggests a set of steps that should be followed. Plans, triage, usage/user profiles, timeliness/chronology, Internet activity, and evidence unique to a particular case are among the phases. The information that can be discovered by closely inspecting and analyzing particular Windows System artefacts is the source of each phase's name. It looks like a classification of artefacts. Furthermore, CFFTPM does not explain how the artefacts and their classification might be used to further an investigation. In summary, the phases appear to offer information about what has to be looked at, but not about how to use them to investigate a case.

To help investigators follow a consistent procedure while looking into cyberattacks, IDFPM (Kohn et al., 2013) suggests a four-step strategy. The steps of IDFPM include "Preparation," "Incident," "Digital forensics investigation," and "Presentation." The examination and analysis are included in the "Digital Forensics Investigation" phase. The Investigation phase focused on gathering obscured, obscured, erased, or visible digital evidence or data and converting it into a form that can be read by humans.

The goal of the analysis is to find information relevant to the case or hypothesis. The IDFPM suggests methods like hashes to discover known data. In order to facilitate quick evidence identification, it also suggests grouping digital evidence with comparable identifying patterns. Using established classifications developed earlier, comparable occurrences is one suggested way to achieve this. This means that it is not attack-agnostic or artifact-focused because it needs prior information. Lastly, a high-level recommendation is made during analysis that the arranged data be evaluated against the formulated hypothesis (Kohn et al., 2013).

A technologically independent framework (Jeong, 2006) designed to close the communication gap between technologists, attorneys, and investigators. This framework was developed using the Zachman architecture to include legal counsel and prosecutions

in the bigger picture. The following roles are suggested by the Zachman organization framework: planner, owner, designer, builder, and subcontractors.

The FORZA framework suggests the following roles:

1. **Principal Coordinator:** The person in charge of leading the case and making the crucial choice about whether to move further with the investigation, this person is in charge of the full digital investigative process.
2. **Stakeholder in the system:** The owner of the system that is being investigated, who may play the victim, suspect, or case sponsor.
3. **Legal Counsel:** The principal coordinator's go-to legal advisor when looking for legal advice.
4. **Security and System Architecture Expert:** Skilled persons with knowledge of security architecture and controls who may advise the lead coordinator on the parameters of the inquiry.
5. **Digital Forensics Strategist:** The expert in charge of formulating the overall plan for the whole DF investigation procedure and making necessary adjustments to it.
6. **DF Investigator and Operational Administrator:** The people who are actively conducting the investigation activities, such as data gathering, extraction, and the preservation and storage of evidence.
7. **DF Analyst:** The expert assigned to examine the data in order to support the established theories.
8. **Prosecution counsel:** Professionals in law who represent the case in court proceedings.

The framework by (Solms et al., 2006) provides an example structure that is comparable to the CobiT structure (Isaca, 2019) by proposing control goals as a foundation for users to use an organized method for incident investigation. This paradigm describes the DF process in four steps, with both high-level and more detailed DF control objectives at each stage. This framework provides a thorough, high-level conceptual structure that

consists of sub-objectives for control objectives. The aforementioned goals provide direction for the application of DF in an enterprise. Although the framework acknowledges the existence of a physical crime scene, its primary focus is on the digital investigation process. The framework also includes Proactive Digital Forensics (ProDF) components.

2.2.3 *Other Sources*

Methods for digital forensics have been suggested to assist in locating and examining incident-related data (Kent et al., 2006 & Sachowski, 2016). They are attack-agnostic and can be applied to attack investigation because they are predicated on generalized phases that comprise Collection, Examination, Analysis, and Report (Kent et al., 2006). They are insufficient as they are based on generalized phases, they do not provide digital forensics examiner with enough details to make sense of the analysis and examination phases of a cyber-attack investigation. Furthermore, the specifics of these processes may change based on a variety of requirements, including regulations, guidelines, and procedures (Kent et al., 2006 & Sachowski, 2016).

(Manson et al., 2007) highlight the benefits of open-source software. They conducted a comparison between the open-source software Sleuth Kit and commercial softwares EnCase and FTK. The outcome of the study has shown that both types produced same results with differing levels of complexity.

As computers are the main targets of these malicious actions, evidence can be obtained from a variety of volatile and non-volatile storage media that are connected to computing systems.

2.3 Research Gap

There is an urgent need to promptly and effectively tackle cybercrimes given their surprisingly high global rate. Cyberattacks on computers leave behind specific artefacts on the target device storage that, with the right processing and analysis, might reveal the identity and actions of cybercriminals. Due to the regular modifications of OS, programs, and the path, content, and structure of artefacts, previous studies demonstrated that a

sufficient number of tools have been developed for the investigation of artefacts. Their testing and dependability have not received enough attention, which could result in analytical results that are not accurate. Selecting the appropriate toolset for a given case can be somewhat challenging for investigators in general, and organizations with limited resources in particular. The purpose of this study is to address the problem of selecting a toolkit for resource-constrained organizations where there is no option for outsourcing facilities. Moreover, developing a framework for the efficient administration and application of DF capabilities in organizational context. After conducting a comprehensive analysis of prior studies, it has been determined that every framework has some limitations and addresses only a subset of objectives.

CHAPTER 3 : METHODOLOGY

3.1 Introduction

This chapter highlight the significance of artifacts produced by Windows OS and how they are helpful in solving cyber incident with the help of test scenario. Afterwards, it presents analysis of the strengths of open-source softwares based on results. Based on the research gap discussed in the preceding chapter, it provides a framework for the efficient administration and application of DF capabilities in organizational contexts. An extensive examination of the duties carried out at every stage of the planned framework is given in this chapter. The theoretical DF Framework was created with the purpose of simplifying the management and application of DF capabilities in organizational settings.

3.2 Windows 10 OS

Over 80% of desktop computers use the Microsoft Windows operating system (OS), which continues to dominate market shares. Because of this, this OS is still widely used in digital forensic investigations conducted all over the world (Desktop, Tablet & Console Operating System Market Share Worldwide, n.d.), because figuring out how a suspect used these platforms depends on knowing how their resident OS artefact's function. Over the course of nearly 20 years, forensic analysis of Microsoft Windows operating systems has generated a great deal of scholarly discussion and literature on topics ranging from memory analysis to registry and operating system artefacts (Desktop OS Market Share 2013-2019, n.d.).

Windows artefacts are evidentiary records that the Windows operating system automatically creates and saves as a result of human interaction with the computer. The Windows operating system includes numerous distinct artefacts that vary throughout versions. While certain artefacts are present in every version, others are only supported in certain versions at first glance due to requirements for future use or backward compatibility.

3.3 Significance of Windows 10 Artifacts used in study

3.3.1 *Shimcache*

This cache, often referred to as AppCompatCache, is a part of the Application Compatibility Database, which is used to track executables on Windows systems and find application compatibility problems. The executables on the system are identified by name and file path in this artefact. A lack of understanding of this artefact may lead to erroneous conclusions because executable records indicate that particular executables were acknowledged by the system, not that they were really run.

Windows registry recorded Shimcache under the registry key "HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatCache\AppCompatCache." The "SYSTEM" registry file, which is found in the "C:\Windows\System32\config" folder, is the file that contains the registry key. This artefact is very useful for identifying executables and malicious activity that occurred on the system. Moreover, it displays the directories in which executables were found, which can assist examiners in identifying intentionally hidden folders.

3.3.2 *Prefetch*

The Prefetch feature was first included in the Windows XP operating system and is still available in Windows 10; it allows Windows to load segments of commonly used programs at startup, which speeds up their loading times. Within the first ten seconds of a program running, Windows prefetch logs the application name, the date and time of the runs, the number of runs, and the path to the executable file.

The prefetch file has the extension ".pf" and the file name format is ".\XXXXXXXXXX.pf," where "XXXXXXXXXX" is the location path's hash value for the executable. Because executables might reside in different locations, the system may hold numerous prefetch files for the same program, each with a different hash value but the same application name. Prefetch files can be found at "C:\Windows\Prefetch," and the

Windows Registry value

"HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\MemoryManagement\Prefetch Parameters" contains the parameters for these files.

In addition to containing evidence of wiping tools, examiners can use prefetch to find out how many times a program was run from a given location, even if the program has been deleted. If the examiner suspects malware execution, it can also determine the location of the malware executable and its first and last run times.

3.3.3 *Shellbags*

Microsoft Windows keeps track of a folder's size, views, icon, and position via a collection of Registry keys called "Shellbags." It's an excellent artefact for quickly analyzing the system and figuring out which directories the user accessed, according to forensic examiners. It captures data such as the location, size, icons, related date, and time of the folder.

Shellbag data is stored in two files, NTUSER.DAT and UsrClass.dat; NTUSER.DAT is located at "C:\Users\" and UsrClass.dat is located at "C:\Users\\AppData\Local\Microsoft\ Windows." Data stored in Registry keys is user account specific and will persist even after a folder is deleted or a USB flash drive is detached.

3.3.4 *Update Sequence Number Journal*

NTFS has a feature called UsnJrnl that keeps track of volume changes. Upon activation, the system keeps track of any modifications, creation, deletion, overwriting, compression, and other actions made to files and directories on disc in the UsnJrnl. For time-stomping, anti-forensics, and malware and incidence response investigations, this artefact is a wonderful source of chronology information (*USN Journal*, 2022).

3.3.5 *UserAssist*

A Registry key called UserAssist keeps track of how users use certain applications. In Windows XP, frequently used programs are displayed on the left side of the Start menu by Windows Explorer, which is based on the entries in this Registry value. The main

distinction between it and the previously discussed Prefetch artefact is that, in contrast to Prefetch, it is user-specific. The NTUSER.DAT file in the "C:\Users\" folder contains UserAssist, and the registry entry "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Assist" is the unique registry key that stores UserAssist data.

The program route, run counter, last run time, focus counter, and focus time are all contained in the UserAssist. This artefact is excellent for finding out when a program was last launched, how often it is executed, when it was deleted, how long a user has engaged with a particular program, and many other user behaviors. It's an excellent resource for knowledge on machines and servers that don't have Prefetch enabled.

3.3.6 *Windows Event Logs*

Windows event logs are an effective source to proof when an event happened. The five primary categories of Windows events are Information, Warning, Error, Success Audit, and Failure Audit. Every event has the following details: log type, event ID, date and time stamp, source, task category, level (information, critical, and error), and user name. This event log information can be used by investigators to verify the exact time and manner of an incident. For instance, persistent Failure Audit events may be utilized to proof the reality of a wicked user's effort to log in.

Windows event is a logging system that keeps track of security logs, application logs, and server-based logs. All of the information about an event is recorded in these logs, which are kept in pre-formatted forms.

3.3.7 *LNK Files*

The Windows operating system keeps note of every action taken by the user and stores it as artefacts. These artefacts may offer the proof needed to put together a series of events that constitute a digital crime. One of these artefacts is the Windows Link File. A shortcut file, also called a link file, is kept in the Windows system's recent folder. A Link file contains a unique header value of 4 bytes that begins with 0x0000004C. The header size is thus represented by its decimal number, 76.

Link files may be generated by the system or by the user. An analyst can determine recently accessed files and folders with the help of Link File's forensic value, which enables the analyst to provide a starting point for search. Analysts can also discover whether any external media are being used. Links file artefacts can be used to determine whether a file has been used after it was downloaded, how long it has been on the system, and whether it exists on a specific volume or has been deleted. They can also be used to determine the Modified, Access, and Create (MAC) time of the file. Briefly, Link File offers details about MAC timings, disc type, file path, machine ID, and serial number.

In Windows, link file entries are logged in a recent directory. The Recent folder is created at location C:\Users\\AppData\Roaming\Microsoft\Windows\Recent.

3.3.8 *Windows Registry*

Windows uses the Windows Registry, a centrally controlled database, to keep track of installed and active apps. Although the Windows registry has a complicated architecture, a forensic analyst can benefit greatly from it. The registry can be a goldmine of information for forensic analysts, providing answers to inquiries about what, who, when, and where something happened on the system.

The registry is described as "a central hierarchical database in Microsoft Windows to store necessary information to configure one or more users, applications, and devices" in the Microsoft Computer Dictionary, Fifth Edition (Deland-Han, 2023). The Windows registry is organized into hives, each of which consists of values, keys, and subkeys. In reality, the Windows registry is a collection of several supporting files. The bulk of these auxiliary files are kept in the directory %SystemRoot%\System32\Config. The only hive relating to user profiles, [ntuser.dat], is kept in a different location, %SystemRoot%\Users/Username/ntuser.dat (stevewhims, 2021).

3.3.9 *Logs File*

As stated by Schwartz (2007), the third entry in the \$MFT is the Windows protected file \$LogFile. It maintains track of modifications made to files on the volume and designed to help in the system's recovery from an unplanned crash. The data are kept in a sequential

fashion, with a unique Log Sequence Number (LSN) assigned to each entry. This LSN is then saved in the \$MFT record of the associated file. A record is created in the \$LogFile that describes the impending alteration and stores a duplicate of the original data before any meta-data modifications are done for a file.

This way, the system can be restored to a working state in the event of a crash. It is worth-mentioning that the Log File is circular, which means that when the file fills up, the newest entries take precedence over the oldest ones (Polakovic, 2016). Its size is usually 64 MB or less, although it might vary depending on the size of the system volume (Oh, in 2013).

3.4 Experimental Setup

3.4.1 Case Study

New FTs are being developed to assist digital investigators in maintaining evidence on dead, remote and live systems. These technologies are using enterprise policy enforcement, electronic data discovery, and incident response with the principles of digital forensics. This study explores the strengths and drawbacks / shortcomings of free and open-source FTs such as RegShot, Regripper, and Autopsy within the framework of the digital investigation process as a whole. Furthermore, a Windows OS security breach test scenario is created to assess the efficacy of these tools. A comparison table and other improvements are suggested for tools used to process digital evidence on live systems in light of this research.

3.4.1.1 Test Scenario

The following scenario of unauthorized access was developed in order to evaluate the open-source forensics tools presented in this research.

1. **Initial access:** An attacker may have obtained unauthorized access to the target machine's Windows host, "HP," with IP address 192.168.0.5, by possibly using stolen credentials. This host featured a USB thumb drive (G:\), a network share (E:\), and an internal hard drive with two partitions (C:\ and D:\).

2. **Login to system:** Once inside the system, the attacker logs in using the compromised credentials or gains administrative privileges through privilege escalation techniques.
3. **Identifying target file:** The attacker identifies the files that he wishes to transfer or remove. These files may include private data, such as system logs, or they may contain other files that disclose organizational strategies. Additionally, an attacker might use email to exfiltrate a confidential file.
4. **Software installation:** The intruder then installed a specialized software for file deletion and used this system and organization's network as a launch pad.
5. **Covering tracks:** to cover his tracks, attacker attempted to erase evidences of his activities like uninstallation of file deletion software, clearing command history, modifying system logs. He may also delete any traces of sent emails from the system like clear browsing history.
6. **Exiting system:** Once the file deletion and email exfiltration are complete, the attacker may choose to log out of the system to avoid suspicion or may continue exploring the system for further malicious activities.

Functionality Review: Digital investigators must be able to identify the issue, assess the severity level and scope of the damage, and preserve the relevant evidence in order to successfully handle important incidents in an organization. This evidence was created with typical organizational working conditions in mind. The success of a project greatly depends on its working plans, related project files, PowerPoint presentations, and deadlines of related projects. Organizations strive to ensure that their vital project information are safe and secure, and that only individuals with the proper authorization can access them.

3.4.2 *Analysis Approaches*

Every case should be treated as a separate circumstance while resolving incidents. As such, depending on the specifics of each instance, a number of strategies may be used during the initial response. When handling a security incidence, there are two broad methods that can be employed: live analysis and post-mortem/static analysis.

When an analyst has a live system to investigate, they typically use the live analysis and acquisition technique. One item on the responder's "don'ts" list is to shut down the system (Mrdovic et al., 2009). Conducting preliminary analysis on the operational system yields significant insights that can direct the analyst's subsequent research. Static analysis, on the other hand, is a standard procedure in which the respondent gathers all the evidence from the incident site, whether it comes from operational or inoperative systems, and then uses the data gathered for static analysis.

This study has chosen static analysis approach as direct access to the system is available and the main focus was operating system analysis.

3.4.3 *Forensic Image*

In order to conduct investigations and acquire evidence that will be admissible in court, forensic imaging refers to the procedures and instruments used to duplicate electronic media, such as a hard drive. In addition to the contents that are visible to the operating system, this copy contains all of the data, including unallocated spaces, deleted files, master boot records, sectors, files, and folders. Every drive structure and piece of content is exactly duplicated in the picture.

The most common use for a forensic image is to confirm the image's integrity following a hard drive acquisition. Since a forensic image's integrity may be examined to ensure it hasn't been altered with after it has been made, law enforcement typically completes this task for courts.

This method has been used to solve numerous cases in the modern criminal world since it can find evidence that is not accessible through an operating system. In situations when you anticipate that your investigation's scope will grow in the future. Then “ALWAYS OVER COLLECT” if you are unsure of the project's scope. You can't obtain much more info than a forensic image, and it's better to have too much than not enough. Additionally, if you anticipate that you or a member of your team will have to attest to the collection's forensic soundness, forensic image is great (Kent et al., 2006).

3.4.4 Abstract Workflow

As the forensic process for each tool and artifact is so complex that comprehensive workflow of each step is very difficult to depict in form of workflow. Therefore, abstract level methodology is shown below:

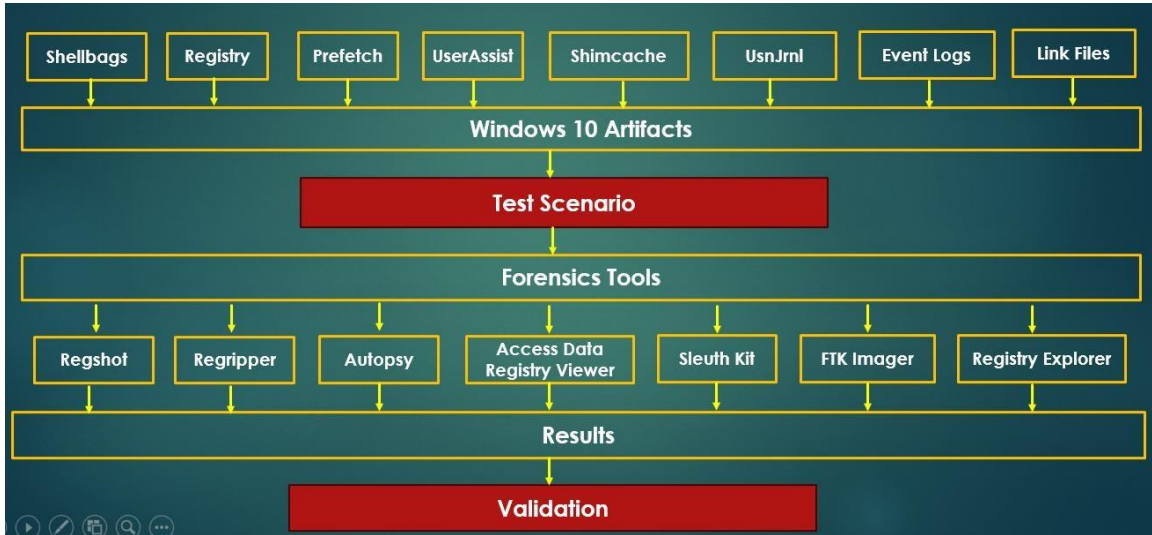


Figure 1: Complete Forensics Process

3.4.5 Workflow using two FTs

How the result validation will be done in this study, model using two FTs is shown below:

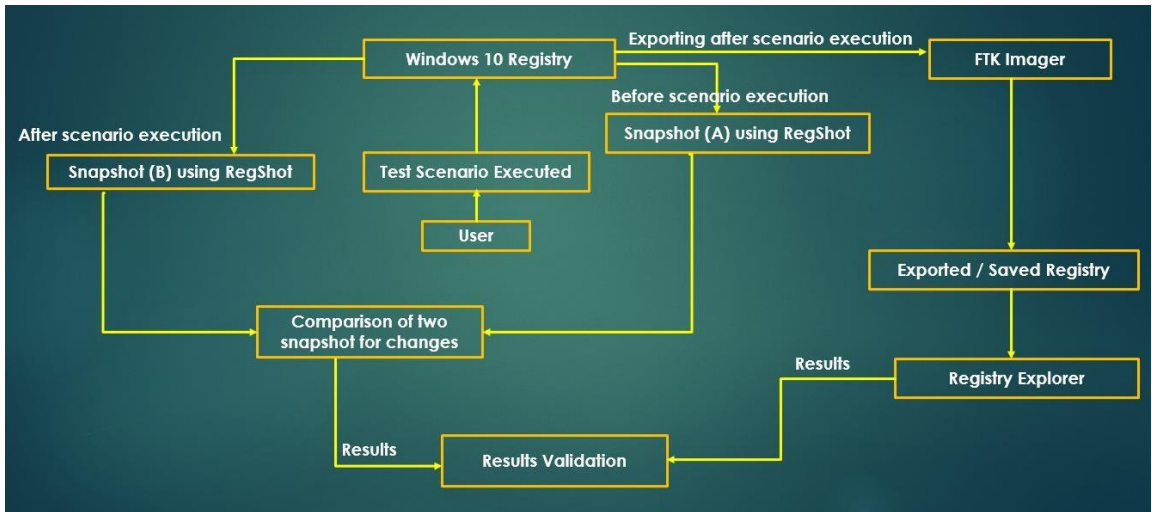


Figure 2: Workflow using two Forensics Tools

CHAPTER 4 : EXPERIMENTS AND RESULTS

4.1 Comparative study of FTs

Because technology in the digital world is always evolving and there are more ways than ever for it to be used illegally, performance calculation in terms of digital forensics tools and software might be considered a hard research subject. Digital forensics has produced a large number of developed tools and software, some of which are free to use and others of which require a license. However, the validity of the digital evidence that is gathered, examined, and presented by both is continuously questioned because some industry practitioners argue for commercial software while others support open-source software.

In this backdrop, I conducted a research study to extract and analyze digital evidence on the above cited test scenario, that has led me to investigate the capabilities of a range of open-source digital forensics tools.

4.2 Evaluation Parameters

4.2.1 Selection of FTs

This study has focused the reasons to not conduct forensics in various small and medium sized organizations due to low budget. Therefore, FTs are selected on the bases of ease of use, availability and their reputation in law enforcement.

4.2.2 Accuracy

The investigator must first gather the necessary evidence before starting Windows forensics. Without changing any data on the original disc, the investigator will typically clone the entire hard drive using specialized software like FTK Imager to produce the evidence image file. This image file is in the raw data format, which is the outcome of copying the data bit by bit from the original evidence disc.

E01 (EnCase/Expert Witness) and AFF (Advanced Forensics Format) are the two most widely used image formats. Because the forensic imaging tools already optimize the image size, event image files in these two formats will be smaller than the raw format (dd). I concentrate on the E01 format in my work since it is the format that law enforcement uses for forensic images (Sulkin & Courcier, 2017).

4.3 Results of FTs used in study

This comprehensive analysis focused on examining Windows logs through the Event Viewer, Sysmon logs, and registry analysis tools to gather insights into specific activities on the system. The creation, copying, and deletion of the "testresult.xlsx" document were meticulously traced using Sysmon logs, revealing that the user "HP" was responsible for these actions. The investigation extended to determining the run count of the CCleaner tool, which was found to be 14, and identifying that the user "HP" installed CCleaner on the system via the Microsoft Store. Additionally, the report delved into the path where CCleaner was installed and unveiled that CCleaner was used to delete the "testresult.xlsx" file. The analysis covered various aspects, including internet activity, file deletions via recycle bin and CCleaner, as well as the uninstallation of CCleaner. The findings were presented using tools like PECmd, registry explorers, Regshot, and Regripper, providing a comprehensive understanding of the system's activities.

4.3.1 FTK Imager

FTK Imager has the ability to produce flawless duplicates and forensic representations of computer data without altering the original evidence. Every aspect of the forensic image, including file slack and unallocated or drive free space, is the same as the original. It protects evidence from tampering or damage while the image is being used in the inquiry.

4.3.2 Registry Explorer

To check if the tool CCleaner was installed on the system or not and if yes then what is the path of the executable file for the tool, we needed to find these details in registry. Since, we already know the date and time the executable was created via the event logs

now, we only need to find the path where the tool was installed. For this purpose, I installed registry explorer, searched for the CCleaner, and found that the path where CCleaner was installed is “C:\Program Files\CCleaner” as shown in Figure 3.

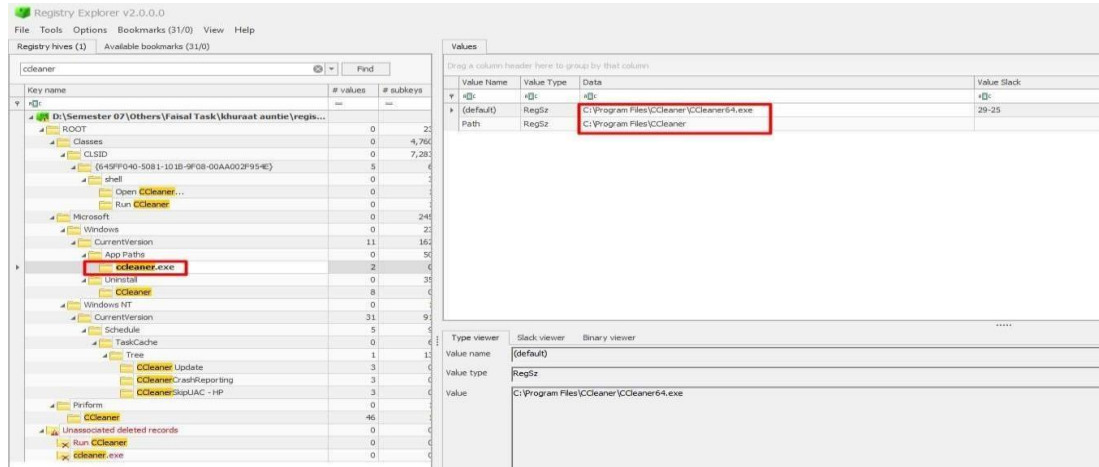


Figure 3 CCleaner installed on system running Windows 10

Since, registry contains the information for executable files being installed and uninstalled in the system, I explored the registry hive using registry explorer and found the following path for uninst.exe in CCleaner key value pair, which was responsible for the deletion of CCleaner from the system as shown in Figure 4.

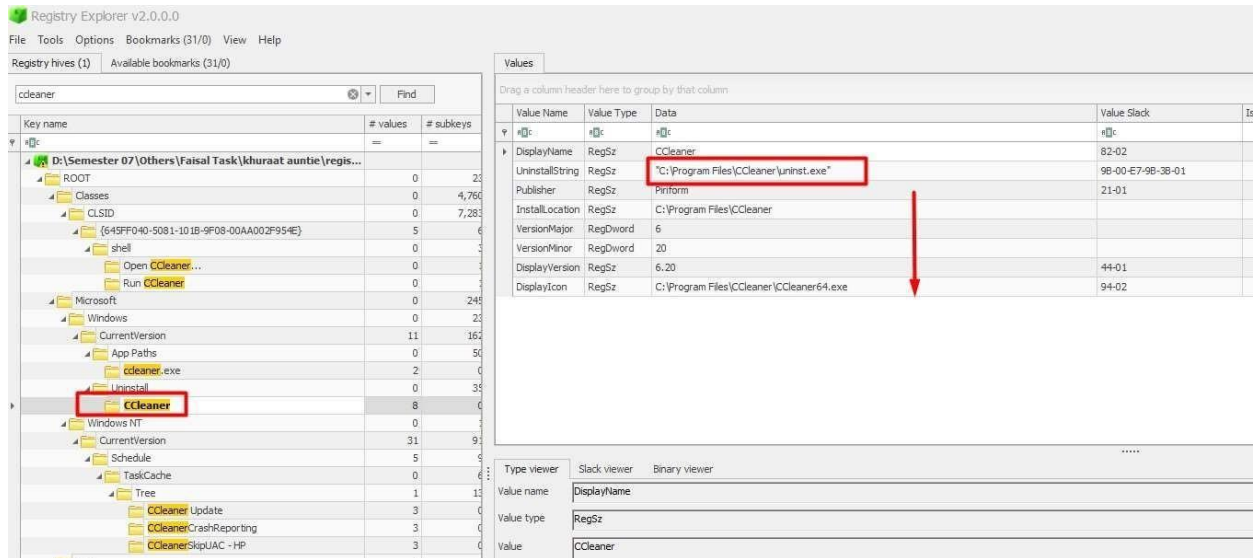


Figure 4 CCleaner Un installed

4.3.3 Autopsy

The process of document creation is shown by Figure 5.

Recent Documents 273 Results

Table Thumbnail Summary Save Table as CSV

Source Name	S	C	O	Path	Date Accessed	Data Source
Image1.LNK				E:\ThesisWork\Image1.docx	2024-02-02 10:06:21 PKT	ssd.E01
lecture slides.LNK				E:\lecture slides	2024-01-31 21:34:28 PKT	ssd.E01
NetworkForensics.LNK				E:\WordDocuments\NetworkForensics	2023-10-11 18:18:11 PKT	ssd.E01
screenshots.LNK				E:\ThesisWork\screenshots.docx	2024-02-01 11:19:41 PKT	ssd.E01
Sequence of actions.LNK				E:\ThesisWork\Sequence of actions.docx	2024-01-28 11:46:00 PKT	ssd.E01
testresult.LNK				C:\Users\HP\Desktop\testresult.xlsx	2024-02-01 08:40:21 PKT	ssd.E01
ThesisWork.LNK				E:\ThesisWork	2024-01-23 17:27:55 PKT	ssd.E01
1-s2.0-S1084804523001236-main.lnk				E:\ThesisWork\1-s2.0-S1084804523001236-main.pdf	2024-01-16 17:24:08 PKT	ssd.E01
1-e2.0-S2590005619300153-main.lnk				E:\ThesisWork\1-e2.0-S2590005619300153-main.pdf	2024-01-16 17:23:45 PKT	ssd.E01

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Figure 5: Document Creation

The process of document movement is shown by Figure 6.

SYSTEM.lnk				C:\Windows\System32\config\SYSTEM	2024-01-18 14:15:31 PKT
testresult.lnk				D:\testresult.xlsx	2024-02-01 08:40:21 PKT
The Internet.lnk				No preferred path found	2023-09-22 09:59:41 PKT
Thesis Defense.lnk				E:\ThesisWork\Thesis Defense.pptx	2024-01-16 17:16:47 PKT

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: 1 of 1 Result < >

Type	Value
Path	D:\testresult.xlsx
Path ID	-1
Date Accessed	2024-02-01 08:40:21 PKT
Source File Path	/img_ssd.E01/Users/HP/AppData/Roaming/Microsoft/Windows/Recent/testresult.lnk
Artifact ID	-9223372036854775710

Figure 6: Document Movement

This software provides details like file creation, access and modified time as well as size of document as shown in Figure 7. These details are very useful in investigation.

Page: 1 of 13 Pages: < > Go to Page: Save Table as C...

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
X 001E0000000008C49F36D64				2023-12-24 15:28:28 PKT	2023-12-24 15:28:28 PKT	2023-12-24 15:28:28 PKT	2023-12-24 15:28:28 PKT	0
X Ubuntu-64-bit-second.vmx				2023-12-24 15:26:57 PKT	2023-12-24 15:26:57 PKT	2024-01-03 14:10:50 PKT	2023-12-24 15:26:57 PKT	4016
X Ubuntu-64-bit-third.vmx.lck				2023-12-24 15:26:47 PKT	2023-12-24 15:26:47 PKT	2023-12-24 15:26:47 PKT	2023-10-14 10:56:40 PKT	48
X [current folder]				2023-12-24 15:26:47 PKT	2023-12-24 15:26:47 PKT	2023-12-24 15:26:47 PKT	2023-10-14 10:56:40 PKT	48
X [parent folder]				2024-01-11 20:43:31 PKT	2024-01-11 20:43:31 PKT	2024-02-07 21:42:36 PKT	2023-10-14 10:53:09 PKT	208
X M00214.lck				2023-12-24 15:26:47 PKT	2023-12-24 15:26:47 PKT	2023-12-24 15:26:47 PKT	2023-12-24 15:26:47 PKT	512
X Ubuntu-64-bit-third.vmdk.lck				2023-12-24 15:28:30 PKT	2023-12-24 15:28:30 PKT	2023-12-24 15:28:30 PKT	2023-12-24 15:28:30 PKT	48
X [current folder]				2023-12-24 15:28:30 PKT	2023-12-24 15:28:30 PKT	2023-12-24 15:28:30 PKT	2023-12-24 15:28:30 PKT	48
X [parent folder]				2024-01-11 20:43:31 PKT	2024-01-11 20:43:31 PKT	2024-02-07 21:42:36 PKT	2023-10-14 10:53:09 PKT	208
X M02495.lck				2023-12-24 15:26:50 PKT	2023-12-24 15:26:50 PKT	2023-12-24 15:26:50 PKT	2023-12-24 15:26:50 PKT	512
X testresult.xlsx				2024-02-01 08:43:03 PKT	2024-02-01 08:49:56 PKT	2024-02-01 08:49:21 PKT	2024-02-01 08:43:34 PKT	49164
X D37958.lck				2024-01-11 20:43:27 PKT	2024-01-11 20:43:27 PKT	2024-01-11 20:43:27 PKT	2024-01-11 20:43:27 PKT	48
X [current folder]				2024-01-11 20:43:27 PKT	2024-01-11 20:43:27 PKT	2024-01-11 20:43:27 PKT	2024-01-11 20:43:27 PKT	48
X [parent folder]				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
X M37958.lck				2024-01-11 20:43:27 PKT	2024-01-11 20:43:27 PKT	2024-01-11 20:43:27 PKT	2024-01-11 20:43:27 PKT	512
X M52443.lck				2024-01-11 20:43:25 PKT	2024-01-11 20:43:25 PKT	2024-01-11 20:43:25 PKT	2024-01-11 20:43:25 PKT	512
X M33615.lck				2024-01-03 14:47:41 PKT	2024-01-03 14:47:41 PKT	2024-01-03 14:47:41 PKT	2024-01-03 14:47:41 PKT	512

Figure 7: Document MAC details

This software provides installation details of any software as shown in Figure 8.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
GoogleUpdateCore.exe			0	2024-01-21 15:58:51 PKT	2024-01-21 15:58:51 PKT	2024-01-31 19:40:20 PKT	2024-01-21 15:58:53 PKT	22301
GoogleUpdateOnDemand.exe			0	2024-01-21 15:58:51 PKT	2024-01-21 15:58:51 PKT	2024-01-31 19:39:40 PKT	2024-01-21 15:58:59 PKT	10831
ccsetup620.exe			0	2024-01-26 13:22:15 PKT	2024-01-26 13:22:41 PKT	2024-02-01 08:47:35 PKT	2024-01-26 13:21:22 PKT	78731
CCleaner.exe			0	2024-01-11 21:29:58 PKT	2024-01-26 13:23:40 PKT	2024-02-01 16:01:42 PKT	2024-01-11 21:29:58 PKT	38311
CCUpdate.exe			0	2024-01-11 21:30:02 PKT	2024-01-26 13:23:41 PKT	2024-02-01 16:01:33 PKT	2024-01-11 21:30:02 PKT	71421
CCleaner64.exe			0	2024-01-11 21:29:58 PKT	2024-01-26 13:23:41 PKT	2024-02-02 09:19:54 PKT	2024-01-11 21:29:58 PKT	44541
CCleanerBugReport.exe			0	2024-01-11 21:29:58 PKT	2024-01-26 13:23:41 PKT	2024-02-01 11:25:36 PKT	2024-01-11 21:29:58 PKT	47031
CCleanerPerformanceOptimizerServi			0	2024-01-11 21:29:58 PKT	2024-01-26 13:23:41 PKT	2024-02-01 08:53:13 PKT	2024-01-11 21:29:58 PKT	10821
CCleanerReactivator.exe			0	2024-01-11 21:29:58 PKT	2024-01-26 13:23:41 PKT	2024-02-01 08:53:13 PKT	2024-01-11 21:29:58 PKT	10291

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Metadata									
Name:	/img_ssd.E01/Users/HP/Downloads/ccsetup620.exe								
Type:	File System								
MIME Type:	application/x-dosexec								
Size:	78733576								
File Name Allocation:	Allocated								
Metadata Allocation:	Allocated								
Modified:	2024-01-26 13:22:15 PKT								
Accessed:	2024-02-01 08:47:35 PKT								
Created:	2024-01-26 13:21:22 PKT								
Changed:	2024-01-26 13:22:41 PKT								
MD5:	49131cde71ee83c5f6a722d35b1ae550								

Figure 8: Software installation

Internet activity performed on system can also be viewed through autopsy. Figure 9 is shown that this document was emailed.

Source Name	S	C	O	URL	Date Modified	Date Accessed	Domain
Favicons				https://www.gmail.com/	2024-02-01 08:47:07 PKT	1601-01-01 05:00:00 PKT	gmail.com
Favicons				https://www.gmail.com/	2024-02-01 08:47:07 PKT	1601-01-01 05:00:00 PKT	gmail.com
Favicons				https://mail.google.com/mail/u/0/#inbox	2024-02-01 08:47:07 PKT	1601-01-01 05:00:00 PKT	google.com
Favicons				https://mail.google.com/mail/u/0/#inbox	2024-02-01 08:47:07 PKT	1601-01-01 05:00:00 PKT	google.com
Favicons				https://mail.google.com/mail/u/0/#inbox?compose=new	2024-02-01 08:47:07 PKT	1601-01-01 05:00:00 PKT	google.com
Favicons				https://mail.google.com/mail/u/0/#inbox?compose=new	2024-02-01 08:47:07 PKT	1601-01-01 05:00:00 PKT	google.com
Favicons				https://mail.google.com/mail/u/0/#inbox?compose=GTv...	2024-02-01 08:47:07 PKT	1601-01-01 05:00:00 PKT	google.com
Favicons				https://mail.google.com/mail/u/0/#inbox?compose=GTv...	2024-02-01 08:47:07 PKT	1601-01-01 05:00:00 PKT	google.com
Favicons				https://www.google.com/	2024-01-07 23:25:19 PKT	1601-01-01 05:00:00 PKT	google.com

Figure 9: Document emailed

Email address used for said activity can be seen in Figure 10. We can relate this activity through timeline.

Regular Expression	Keyword Preview	Modified Time	Access Time	Change Time
>-9%+ _]+ (\[a-zA-Z0-9%+ _]+)*(\[?]\@...)	identifiervalue : «leadermaryam3579@gmail.com»count : 1dat...	2024-02-01 08:50:42 PKT	2024-02-01 08:50:42 PKT	2024-02-01
>-9%+ _]+ (\[a-zA-Z0-9%+ _]+)*(\[?]\@...)	"maryam zubair", "\ " «leadermaryam3579@gmail.com», "\ htt...	2024-01-23 22:04:02 PKT	2024-01-23 22:16:16 PKT	2024-01-23
>-9%+ _]+ (\[a-zA-Z0-9%+ _]+)*(\[?]\@...)	tle : inbox (421) - «leadermaryam3579@gmail.com» - gmailpro...	2024-02-01 08:50:29 PKT	2024-02-01 08:50:29 PKT	2024-02-01
>-9%+ _]+ (\[a-zA-Z0-9%+ _]+)*(\[?]\@...)	tle : inbox (421) - «leadermaryam3579@gmail.com» - gmailpro...	2024-02-01 08:50:29 PKT	2024-02-01 08:50:29 PKT	2024-02-01
>-9%+ _]+ (\[a-zA-Z0-9%+ _]+)*(\[?]\@...)	tle : inbox (421) - «leadermaryam3579@gmail.com» - gmailpro...	2024-02-01 08:50:29 PKT	2024-02-01 08:50:29 PKT	2024-02-01
>-9%+ _]+ (\[a-zA-Z0-9%+ _]+)*(\[?]\@...)	erkjggg==" , "email": " «leadermaryam3579@gmail.com» , "fulln...	2024-02-01 08:51:44 PKT	2024-02-01 08:51:44 PKT	2024-02-01
>-9%+ _]+ (\[a-zA-Z0-9%+ _]+)*(\[?]\@...)	tle : inbox (421) - «leadermaryam3579@gmail.com» - gmailpro...	2024-02-01 08:50:29 PKT	2024-02-01 08:50:29 PKT	2024-02-01
>-9%+ _]+ (\[a-zA-Z0-9%+ _]+)*(\[?]\@...)	tle : inbox (421) - «leadermaryam3579@gmail.com» - gmailpro...	2024-02-01 08:50:29 PKT	2024-02-01 08:50:29 PKT	2024-02-01
>-9%+ _]+ (\[a-zA-Z0-9%+ _]+)*(\[?]\@...)	tle : inbox (421) - «leadermaryam3579@gmail.com» - gmailpro...	2024-02-01 08:50:29 PKT	2024-02-01 08:50:29 PKT	2024-02-01

Figure 10: Email address details

4.3.4 Regripper

Regripper takes a registry file like SAM, Security or Software or any else and outputs a comma separated file / txt file containing information on keys and value pairs of the registry as shown in Figure 11.

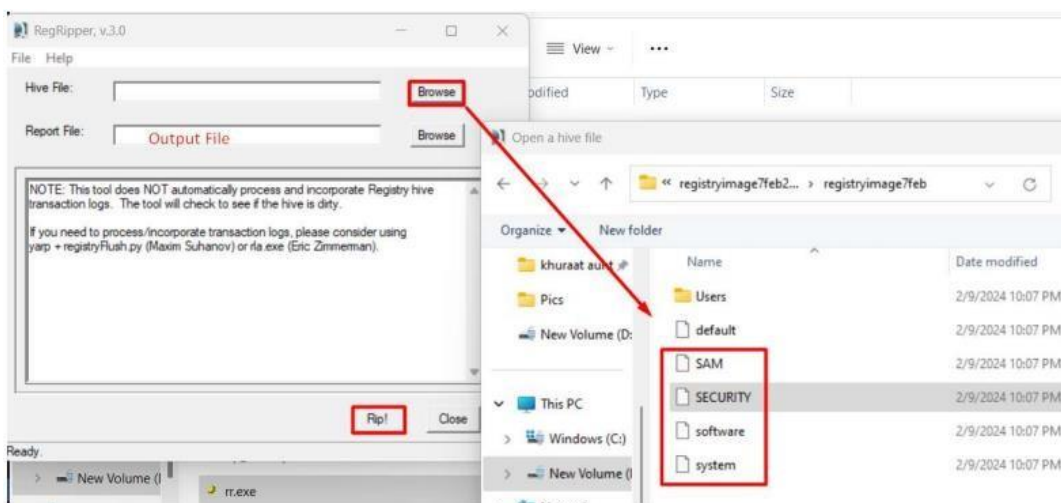


Figure 11: Rip process

This tool provides valuable information on the installed tools which can be seen in Figure 12.

```
-----
apppaths v.20200511
(NTUSER.DAT,Software) Gets content of App Paths subkeys
2024-01-26 08:23:44Z
ccleaner.exe - C:\Program Files\CCleaner\CCleaner64.exe
2024-01-01 11:20:37Z
WindowsPackageManagerServer.exe - C:\Program Files\WindowsApps\Microsoft.DesktopAppInstaller_1.21.3482.0_x64__8wekyb3d8bb
winget.exe - C:\Program Files\WindowsApps\Microsoft.DesktopAppInstaller_1.21.3482.0_x64__8wekyb3d8bbwe\winget.exe
2024-01-01 11:20:47Z
```

Figure 12: Software installation through regripper

4.3.5 Regshot

Regshot is a free and open-source registry compare tool that enables to rapidly take a snapshot of the registry and compare it with another one after installing new software or making system changes. All changes made between two snapshots are listed in the changes report, which can be generated in text or HTML format. Furthermore, it has the option to designate folders (as well as subfolders) to be checked for updates.

So, I installed Regshot before all the above tasks and took one of the snapshots and now that I am done with all the tasks, I took the 2nd snapshot and started comparing the

two. We can see in Figure 13, username for the system along with the comparison results including deleted and added keys and values in the registry during whole activity.

```

--res-x64.txt - Notepad
File Edit Format View Help
Regshot 1.9.0 x64 ANSI
Comments:
Datetime: 2024/2/17 15:52:00 , 2024/2/17 16:51:11
Computer: MARYAM , MARYAM
Username: HP , HP

-----
Keys deleted: 272
-----
HKLM\SOFTWARE\Classes\CLSID\{23C76460-3EBF-44AF-A840-130EBE953AD5}
HKLM\SOFTWARE\Classes\CLSID\{99E09232-BE6A-40CD-B563-F4ABD9AF1B09}
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\ApplicationUser\Data\1ba
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\ApplicationUser\Index\Application\348\1ba
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\ApplicationUser\Index\PackageUser\b98\1ba
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\ApplicationUser\Index\PackageUserAndApplication\b98^348
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\ApplicationUser\Index\PackageUserAndApplication\b98^348\1ba

```

Figure 13: User details

Here in figure 14 below, we can see the added keys and values from our tasks (mostly for CCleaner because it is the only tool that I installed in the span between two snapshots before comparison).

```

--res-x64.txt - Notepad
File Edit Format View Help
HKU\S-1-5-21-745266217-1623697403-621402039-1005\Software\WinRAR\DialogEditHistory\ExtrPath

-----
Keys added: 508
-----
HKLM\SOFTWARE\Classes\CLSID\{645FF040-5081-101B-9F08-00AA002F954E} \shell\Open CCleaner...
HKLM\SOFTWARE\Classes\CLSID\{645FF040-5081-101B-9F08-00AA002F954E} \shell\Open CCleaner... \command
HKLM\SOFTWARE\Classes\CLSID\{645FF040-5081-101B-9F08-00AA002F954E} \shell\Run CCleaner
HKLM\SOFTWARE\Classes\CLSID\{645FF040-5081-101B-9F08-00AA002F954E} \shell\Run CCleaner \command
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Packages\Microsoft.WindowsStore_22401.1401.2.0_neutral_~_8weky
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Packages\Microsoft.WindowsStore_22401.1401.2.0_x64_8wekyb3d8t
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Packages\Microsoft.WindowsStore_22401.1401.2.0_x64_8wekyb3d8t

```

Figure 14: Monitoring installation changes

CCleaner’s uninstall registry key is shown in Figure 15.

```

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppX\AppXAllUserStore\S-1-5-21-745266217-1623697403-621402039-1005\Microsoft.WindowsStore_22401.1401.2.0_neutral_~_8wekyt
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppX\AppXAllUserStore\S-1-5-21-745266217-1623697403-621402039-1005\Microsoft.WindowsStore_22401.1401.2.0_neutral_~_8wekyt
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\SamlSecurity\Microsoft\Windows\CurrentVersion\Uninstall\CCleaner
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\10710
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\13908
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\13908

```

Figure 15: Uninstallation changes

Installed folder for the tool is the same as I found in Registry Explorer.

```

-----
HKLM\SOFTWARE\Classes\CLSID\{645FF040-5081-101B-9F08-00AA002F954E} \shell\Open CCleaner... \command: "C:\Program Files\CCleaner\ccleaner.exe /FRB"
HKLM\SOFTWARE\Classes\CLSID\{645FF040-5081-101B-9F08-00AA002F954E} \shell\Run CCleaner... \command: "C:\Program Files\CCleaner\ccleaner.exe /AUTORB"
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Extensions\ProgIDs\AppX6hptmm8avg1gnv71j8jda9340qk79w89\Microso
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Extensions\ProgIDs\AppX6hptmm8avg1gnv71j8jda9340qk79w89\Microso
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Extensions\ProgIDs\AppX6hptmm8avg1gnv71j8jda9340qk79w89\Microso
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Extensions\ProgIDs\AppX6hptmm8avg1gnv71j8jda9340qk79w89\Microso

```

Figure 16: Installation path

The installation details (name, path and publisher of CCleaner) can be seen in Figure 17.

```

\NuCategoryId\": \"64293252-5926-453c-9494-2d4021f1c78d\")\"}
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\CCleaner\DisplayName: \"CCleaner\"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\CCleaner\UninstallString: \"C:\Program Files\CCleaner\uninst.exe\"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\CCleaner\Publisher: \"Piriform\"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\CCleaner\InstallLocation: \"C:\Program Files\CCleaner\"

```

Figure 17: Installation details

User responsible for installation of software ‘HP’ can be seen in Figure 18.

```

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\CCleanerCrashReporting.job: 38 C3 26 E3 A6 50 FF 12 E0 00 38 D4 A9 1F 8E AC
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\CCleanerCrashReporting.job: 0x2219c019
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{3A975A9E-656F-41B2-995B-AB902C7F81EF}\Path: \"\\CCleanerSkipUAC - HP\"
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{3A975A9E-656F-41B2-995B-AB902C7F81EF}\Path: 00 30 30 30 F0 68 C3 91 85 0B E5 2C 08 5B 20 91
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{3A975A9E-656F-41B2-995B-AB902C7F81EF}\Path: \"\\CCleanerSkipUAC - HP\"

```

Figure 18: User details

4.3.6 Access Data Registry Viewer

For registry viewer I downloaded the tool from the link: Registry Viewer 2.0.0 (exterro.com), but the results I found are the same as I found via registry explorer, Regshot and reg ripper. The information I found on CCleaner using Registry Viewer shown in Figure 19.

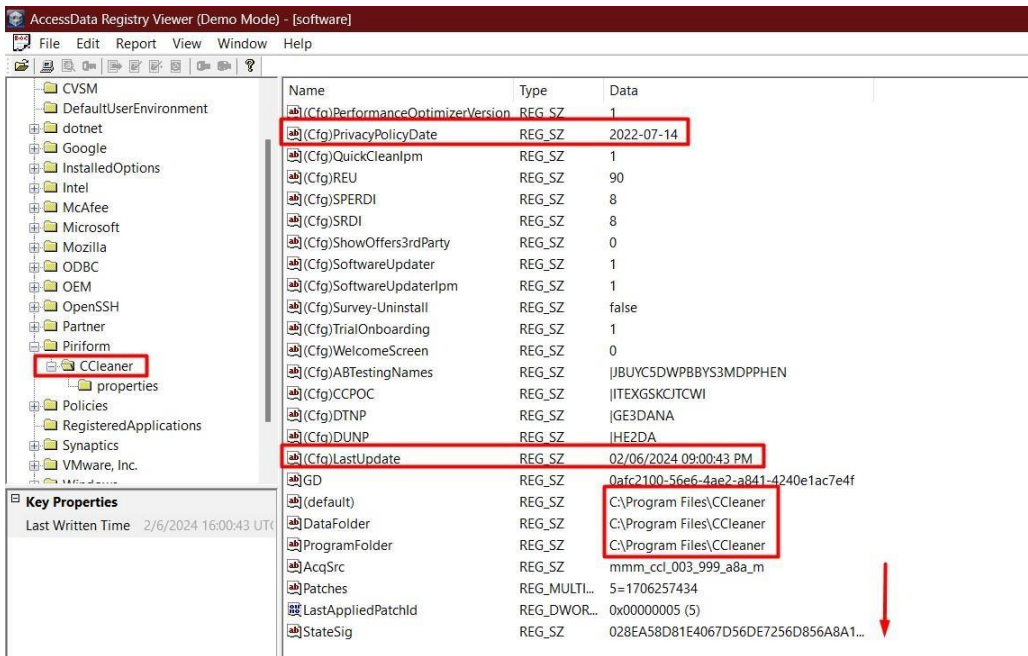


Figure 19: Software Installation Details

4.3.7 Sysmon Analyzer

Sysmon is a system service for Windows that stays on the computer to track and record system activity for the Windows event logs. It offers comprehensive details on changes to file creation times, network connections, and process creations. By gathering the events, we may spot suspicious or harmful activity and learn how malware and hackers function on a network. Since the service operates as a protected process, many user mode interactions are prohibited (markruss, 2024).

This utility has been installed for analysis of Windows Event Logs specifically. Configure Sysmon logs to capture events pertaining to file and process creation, deletion, DNS queries, registry value modifications, and other relevant activities. Access Sysmon logs through the Event Viewer in the "Applications & Services logs -> Microsoft -> Windows -> Sysmon -> Operational" path. Identify file creation events in Sysmon logs by referring to Event ID 11. Apply a filter to specifically extract logs related to file creation for more focused analysis.

With event id 01 logs filtered for process creation I found our target file testresult.xlsx in one of the filtered logs. As we can see in Figure 20, path of the file i.e., Desktop in the system and the user who created the file on Desktop i.e., **HP**.

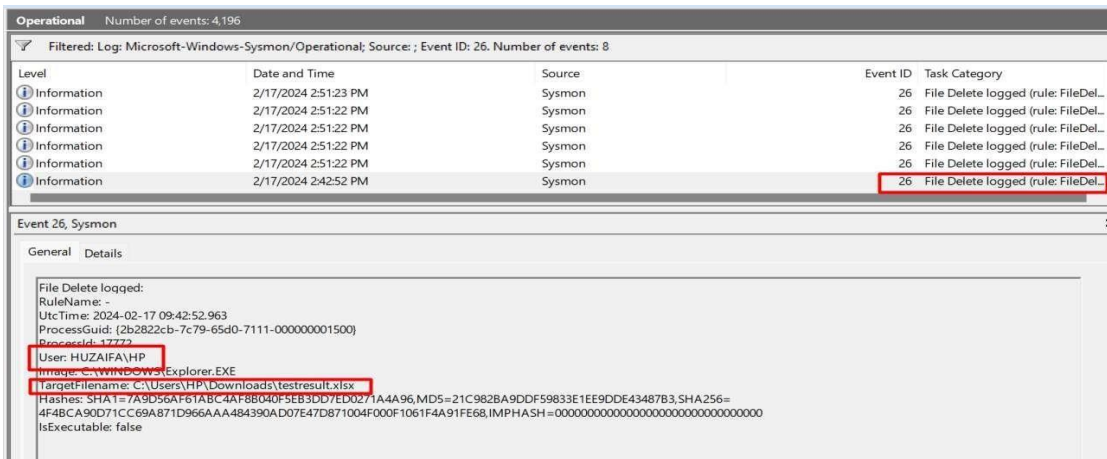


Figure 20: User Details through Windows Event Logs

Then, I filtered the logs with Event Id 26 for deleted files logs. From filtered logs, I looked for target file i.e., testresult.xlsx and figure 21 depicts that target file was actually deleted via CCleaner by **HP**.

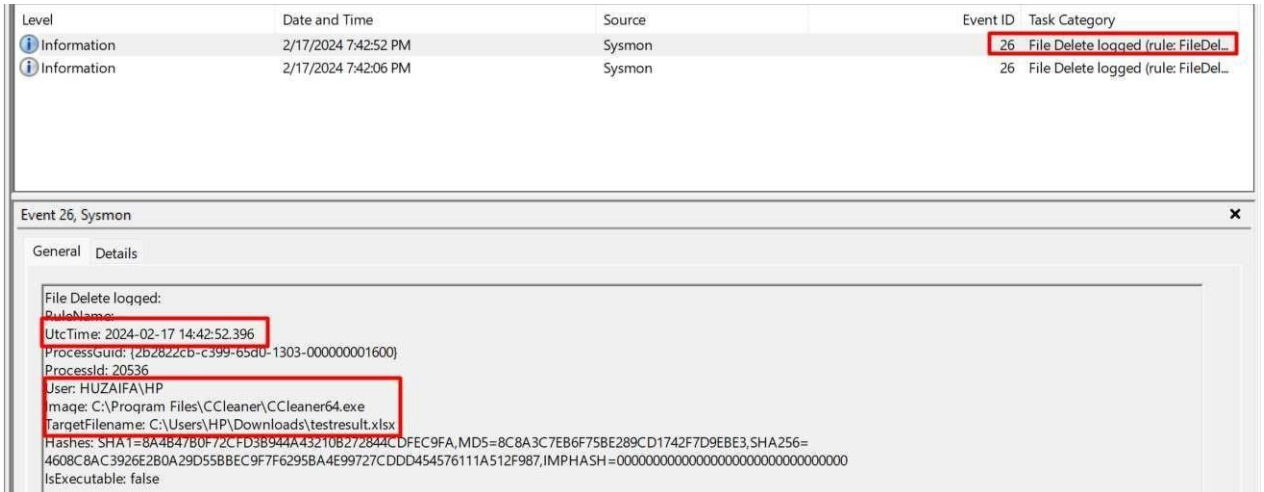


Figure 21: Software used to delete document

We noticed that neither registry hives, nor any log files contain logs that contain the data and details of an email either sent or received, so finding the details of the email where test results.xlsx was emailed to leadermaryam3579@gmail.com is nearly impossible. Event Id 22 is used for logs where network connectivity or DNS query is in question. So, I filtered logs and looked in the details for each log. I could not find the two of the email, but I found a log where account profile for user HP for outlook is used as shown in figure 22.

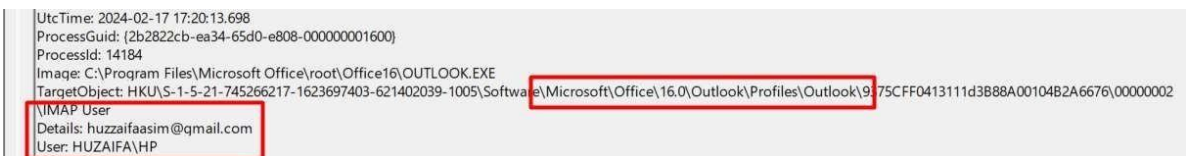


Figure 22: Document emails

I was also able to find name or Display name of the person who sent the email containing testresult.xlsx to leadermaryam3579@gmail.com in one of the filtered logs as shown in figure 23.



Figure 23: Display name of User

Windows events does not specifically stores the recycle bin deletion events with the name of the application as it does for other apps responsible for the deletion of files. These deletions via recycle bin are logged under the “**Forced Authentication**” technique because deleting from recycle bin results in permanent delete of files which required high level authorization hence the alert shown to permanently delete a file, So, as you can see in the screenshot below, testresult.xlsx is being deleted using Forced Authentication.

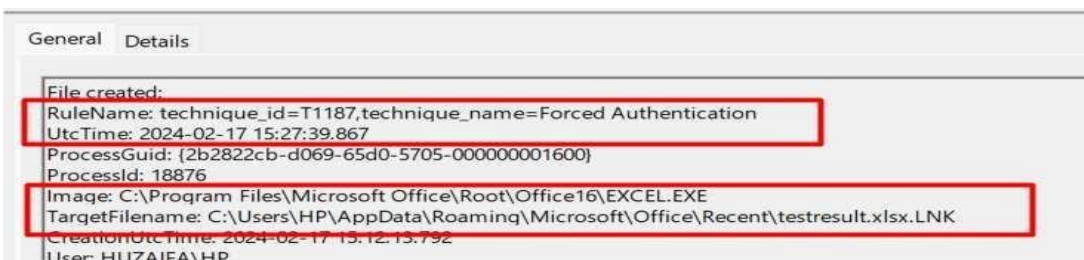


Figure 24: Document deletion via Recycle bin

4.3.8 Prefetch Analysis

The Windows prefetch folder holds .pf files for each executable in the system. To ascertain the run count for CCleaner, locate the "CCleaner.pf" file and execute command with PECmd "**PECmd.exe -f CCleaner.exe -o exports.**" will generate an "exports" folder in the current directory, containing Excel files with detailed information about the analyzed tool's prefetch file.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
te	SourceFilename	SourceCreated	SourceModified	SourceAccessed	ExecutableName	Hash	Size	Version	RunCount	LastRun	VolumeName	VolumeSerial	VolumeOC							
	CCLEANER64.EXE-779BD542.pf	2/14/2024 19:49	2/13/2024 9:50	2/14/2024 19:50	CCLEANER64.EXE	779BD542	185128	Windows	14	2/9/2024 4:08	VOLUME{01d9ed144802ae9a-72483784}	72483784	#####							

Figure 25: Run Count of CCleaner

4.3.9 Other System Artifacts

AppCompatCacheParser Tool was used Then I used to analyze Software registry hive and it produced a final report containing the results on the executable files in the hives.

68	000000900f00700c8a000000a000047ba000014c	Microsoft.SkypeAppKz8qxf38zg5c			Yes	FALSE	L	
69	C:\WINDOWS\system32\ipconfig.exe				2/14/2024 20:22	No	FALSE	L
70	000000b5d440800030000000000000000008664	Microsoft.OneDriveSync8wekyb3d8bbwe				No	FALSE	L
71	000000b5d440800030000000000000000008664	Microsoft.OneDriveSync8wekyb3d8bbwe				No	FALSE	L
72	C:\WINDOWS\TEMP\nst53D3.tmp.exe				11/9/2023 18:43	Yes	FALSE	L
73	C:\WINDOWS\system32\wlmrdr.exe				5/7/2022 5:19	No	FALSE	L
74	C:\Users\HP\AppData\Local\Microsoft\OneDrive\24.020.0128.0003\FileCoAuth.exe				2/17/2024 9:31	No	FALSE	L
75	C:\Program Files\Cleaner\CCleaner.exe				2/5/2024 17:18	No	FALSE	L
76	C:\Users\HP\AppData\Local\Microsoft\OneDrive\OneDrive.exe				2/17/2024 9:31	Yes	FALSE	L
77	C:\Program Files (x86)\HP\HP_Support_Framework\Warranty\HPWSD.exe				1/3/2024 20:41	Yes	FALSE	L
78	C:\Program Files\Cleaner\CCUpdate.exe				1/11/2024 16:30	No	FALSE	L
79	C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_16005.14326.21830.0_x64_8wekyb3d8bbwe\Application				2/17/2024 9:46	No	FALSE	L
80	00000093e8537655460000000000000000008664	microsoft.windowscommunicationsapps8wekyb3d8bbwe				No	FALSE	L
81	00000093e8537655460000000000000000008664	microsoft.windowscommunicationsapps8wekyb3d8bbwe				Yes	FALSE	L
82	000000b000a0000000603e8000a0000585d00008664	windows.immersivecontrolpanelcv5n1h2txyeyneutral				Yes	FALSE	L
83	C:\WINDOWS\TEMP\nsb38CF.tmp.exe				11/9/2023 18:43	Yes	FALSE	L
84	C:\Program Files\Cleaner\CCleaner64.exe				1/11/2024 16:29	No	FALSE	L
85	000000b000a0000000603e8000a0000585d00008664	Microsoft.Windows.ShellExperienceHostcv5n1h2txyeyneutral				No	FALSE	L
86	C:\Program Files\WindowsApps\Microsoft.OutlookForWindows_1.2024.207.500_x64_8wekyb3d8bbwe\olkPushNotificationBackgroundTask.exe				2/13/2024 9:14	No	FALSE	L
87	00000090001074800c0114000a0000585d08e8664	Microsoft.OutlookForWindows8wekyb3d8bbwe				No	FALSE	L
88	00000090001074800c0114000a0000585d08e8664	Microsoft.OutlookForWindows8wekyb3d8bbwe				No	FALSE	L

Figure 26: Software Installation Details

4.3.9.1 Shimcache

To collect information on test scenario, I first opened the following registry key in registry explorer “HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatCache\AppCompatCache”. This key is responsible for holding information about the executable files on the system as it can be seen in figure 27.

Value Name	Value Type	Data	Is ...	Value Slack	Data Record	Reallocated
CacheMainSdb	RegBinary	31-30-74-73-73-9E-8F-AE-1C-00-00-00-16-00-77-00-73-00-32-00-68-00-65...	<input type="checkbox"/>	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
SdbTime	RegBinary	27-76-1E-45-57-0B-DA-01-00-00-00-00-00-00-00-00-00-00-00-00-00-0...	<input type="checkbox"/>	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
AppCompatCache	RegBinary	34-00-00-00-C7-B0-00-00-00-00-00-00-13-07-00-00-03-00-00-00-00-00...	<input type="checkbox"/>	00-00-00-00-00-00-00-00-00...	<input type="checkbox"/>	<input type="checkbox"/>

Cache Entry Position	Program Name	Modified Time
5	E:\TOOLS\MFTECmd.exe	2022-10-20 17:37:02
6	E:\TOOLS\AppCompatCacheParser.exe	2023-03-07 20:12:59
7	C:\Windows\System32\w32tm.exe	2019-12-07 09:08:13
8	E:\TOOLS\ccsetup620.exe	2024-01-26 08:22:15
9	C:\Program Files\Cleaner\CCleaner.exe	2024-01-11 16:29:58
10	C:\Program Files\Cleaner\CCUpdate.exe	2024-01-11 16:30:02
11	C:\Program Files\Cleaner\CCleaner64.exe	2024-01-11 16:29:58
12	C:\Users\HP\Downloads\ccsetup620.exe	2024-01-26 08:22:15
13	E:\TOOLS\RegRipper3.0-master\rip.exe	2023-07-22 23:53:28

Figure 27: Executable details

4.3.9.2 Shellbags

I also checked for Bag MRUs in shell bags registries to look for any necessary information. For this purpose, I opened the following registry hive “HKCU\Software\Classes\LocalSettings\Software\Microsoft\Windows\Shell” in registry viewer and result I got shown in figure 28.

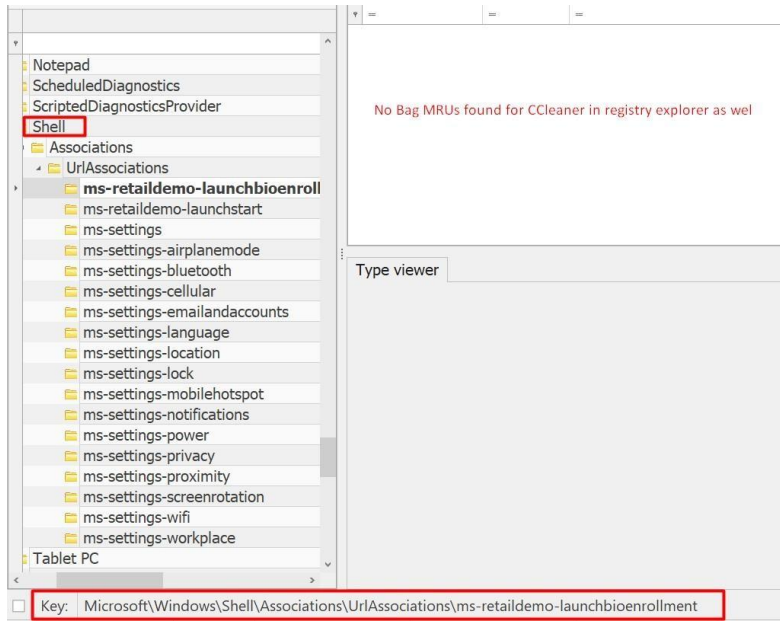


Figure 28: Shellbags analysis

There was no available information for Bag MRUs in shell hive in the registry hive defined above. To confirm this, I installed a shell bag explorer tool that there is no Bag MRU available for CCleaner. I downloaded the tool and opened the same registry file in it, and this was the result as shown in the screenshot below:

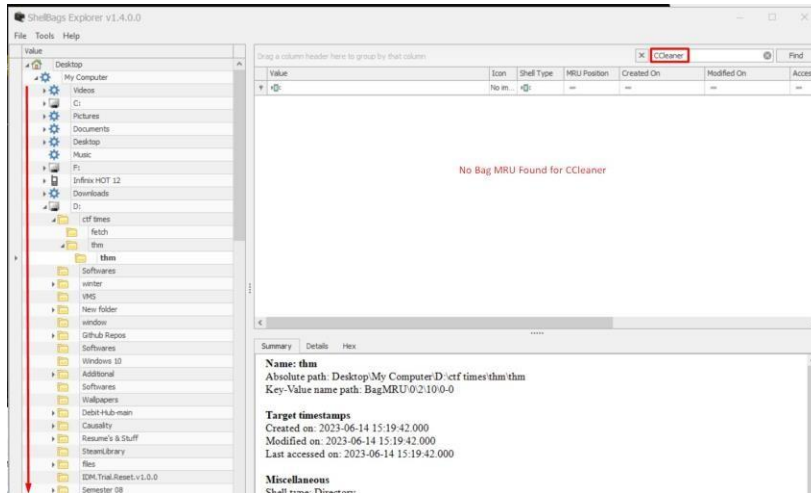


Figure 29: Shellbags analysis via Shellbag Explorer

4.4 Discussion

When an incident happens, Windows forensics looks into the operating system of the computer to identify traces of user or program activity. Examples of these traces include the manner in which a malicious program ran, the identities of those who accessed particular files or folders, the date and time of file deletions, browsing history, and more. Windows registry files and Windows event logs are the primary sources to look through and evaluate in order to provide answers to these queries.

The accuracy and validity of the results generated by the tools mentioned above have been verified by cross-validation and combination. Since Windows generates artefacts in a variety of formats and places, as is well known from literature, an attacker will find it more difficult to modify artefacts from several sites if he wipes out its operations from one area. Given this context, the investigator needs to be aware of how many artefacts he needs to examine and how many artefacts the system will produce if a certain action is taken on it.

The investigator needs to cross-validate the generated artefacts and results using several FTs. It will not only validate his work but also enhance confidence in the precision and genuineness of the equipment. Because each tool is designed to analyze a specific kind of artefact, an examiner has to have a variety of instruments to make the job easier. From

a technical standpoint, the investigator determines which digital forensic tools to use for evidence assessment based on the particulars of each case and its requirements.

Investigators can select the best tool for inquiry by carefully weighing all of its features, which will save time and work. This study performed an in-depth study of selected open-source tools and their features. As we have seen that each software has produced the positive indications of activities, it is possible that open-source tools "meet the guideline requirements equal to the closed source commercial tools" and can be utilized just as effectively. The aforesaid activity was summarized in Table 1.

Table 1: OS related features via FTs

Features/ FTs	Autopsy	Regshot	Regripper	Registry Explorer	Access Data Registry Viewer	FTK
LNK files	Y	N	N	Y	Y	Y
Prefetch files	Y	N	N	N	N	Y
Event logs	Y	N	N	N	N	Y
Registry	Y	Y	Y	Y	Y	Y
Installed programs	Y	Y	Y	Y	Y	Y
User activity	Y	N	N	Y	Y	Y
Recycle bin	Y	N	N	N	N	Y
Service analysis	N	N	N	N	N	Y

In conclusion, this detailed analysis of the Windows system, utilizing tools such as the Event Viewer, Sysmon logs, registry analysis tools, and additional utilities like PECmd, Regshot, and Regripper, yielded comprehensive insights into various system activities. From the creation, copying, and deletion of the "testresult.xlsx" document to the examination of CCleaner's run count, installation, and subsequent use, the investigation provided a thorough understanding of user actions and tool interactions. Sysmon logs proved instrumental in tracing file-related events, establishing "HP" as the user responsible.

The study also highlighted the effective use of registry exploration tools and the comparison capabilities of Regshot for analyzing system changes over time. Overall, this meticulous examination of system logs and registry data successfully uncovered a detailed narrative of user actions, software usage, and system modifications.

Organizations vary in terms of their structure and working environment, just as every scenario has unique requirements. Most organizations are unaware of the need for forensics or do not have any forensics capability. Thus, in the event of an occurrence, the organization chose to out-source this task at a premium rate. For those organizations who believe they can conduct incident investigation internally with minimal effort and budget allocation, this activity is a great source of motivation. The study's findings indicate that open-source digital forensic tools work effectively.

4.5 Framework for Reporting and Presenting Digital Forensics Investigations

4.5.1 Introduction

The need for digital evidence is underestimated by most organizations (Sommer, 2005). When proof of fraudulent transactions is needed, it is frequently the case that there is insufficient or unreliable evidence to connect the attacker to an incident. Organizations must make sure that every aspect of their working environment is ready for an internal inquiry or compliance test, as well as for DF investigations. When an incident happens, Windows forensics looks into the operating system of the computer to identify traces of user or program activity. Examples of these traces include the manner in which a malicious program ran, the identities of those who accessed particular files or folders, the date and time of file deletions, browsing history, and more. Windows registry files and Windows event logs are the primary sources to look through and evaluate in order to provide answers to these queries.

The suggested framework for evaluating and disseminating the results of cyberattack investigations is provided in this section. The goal of this framework is to improve and supplement current digital forensics procedures, not to replace them. As such, examiners of digital forensics might use this framework in conjunction with their preferred

method of digital forensics throughout the reporting stage. Regardless of the nature, style, or sophistication of an incident, the proposed framework offers a step-by-step and semi-automated cyberattack reporting process.

The methodology used is taken from (Dimitriadis et al., 2020), and the suggested framework is based on identified research gaps. There are hundreds of digital forensics investigation processes that have been developed globally for use in digital forensics investigation practices. Every organization often creates its own policies. While some concentrated on the technological aspects of data collection, others concentrated on the investigation's data analysis phase. Since many of these procedures were created to address distinct technologies utilized in the examined device, new procedures must be created if the target device's underlying technology changes.

This framework provides the necessary guidelines towards logical decision making for experienced but having low confidence in their decision-making capabilities as well as beginners. It may also serve as an organized process for developing sound conclusions on how to analyze any digital evidence.

4.5.2 Present case evidence in the legal context

Nearly all organizations have very poor reporting in the fourth step of the NIST forensics procedure. Not only does this problem affect every organization, but it also affects every global entity on a national and worldwide scale. The phases of gathering and examining the evidence are receiving the majority of the attention, whilst the reporting / presenting phase receive little to no attention. The base model (Dimitriadis et al., 2020) also improved and concentrated on the two phases of cyber event i.e., examination and analysis, but it offers no organizational or legal guidance on how to properly report evidence so that the case proceeds to a logical conclusion.

A practitioner in digital forensic investigations will typically identify several digital data points that they believe to be potentially evidence. Prior to choosing to share this information with their client, they must accurately assess the facts and comprehend how it would affect the inquiry. Error avoidance at this point is essential to minimizing any

detrimental effects on individuals engaged in the criminal justice system. Considering the grave ramifications of making a mistake, the choice to report on a piece of potential digital evidence should have been thoroughly examined and assessed before being submitted.

Presently, organizations have minimal or no standard operating procedures for handling incidents. In order to facilitate or advance the reconstruction of incidents, reactive digital forensics is an analytical and investigative technique that is used for the maintenance, identification, and extraction, as well as for documentation, examination, and interpretation of digital information for root-cause analysis. It also involves the presentation of digital evidence derived from digital sources.

4.5.3 *Components of framework*

1. Alternate descriptions
2. The intended audience
3. Peer review
4. Consistent with case objectives
5. Making investigative decision
6. Report cleaning

4.5.4 *Workflow of framework*

Workflow of proposed framework is shown in figure

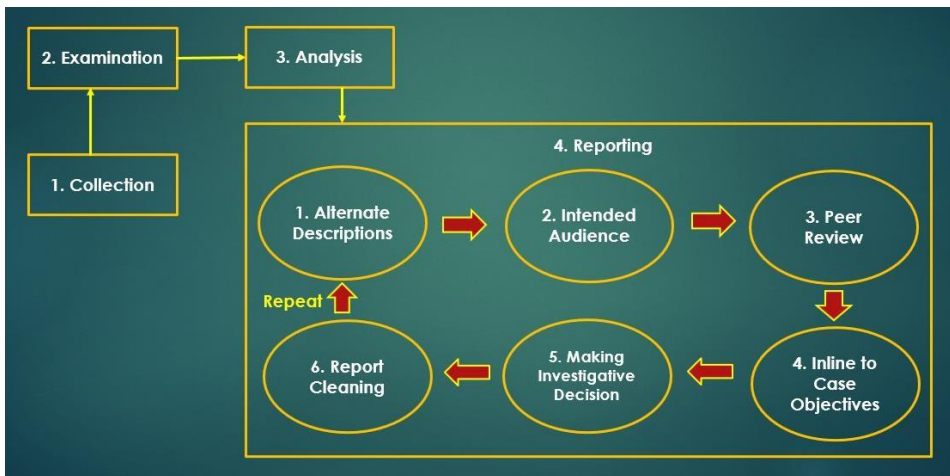


Figure 30: Workflow of framework

4.5.5 *Discussion*

It is imperative to explain that the framework under consideration is designed to present cases and reports at the micro-level of a digital forensic investigation, specifically pertaining to each specific "evidence type" that an investigator finds (e.g., deleted images, Internet search words, etc.). A framework should be applied to each type of evidence, for instance, if the practitioner finds two sets of potential evidence like set of removed pictures and search terms, to make sure that any findings, conclusions, deductions and assumptions about their relevance to the case at hand have been established correctly.

Reaching a conclusive explanation of an occurrence may not be feasible if the available information about it is insufficient. When there are two or more reasonable reasons for an incident, each should be taken into account in the reporting process. Analysts ought to address the task of proving or disproving each explanation methodically.

When there is an incident that needs law enforcement response, all information gathered must be reported in great detail, and copies of all obtained evidence may also be needed. As a result, it's critical to understand who will be viewing the data or information. An extensive view of network traffic and associated statistics may be desired by a system administrator. Senior management may only need a high-level summary of the events, including a condensed graphic depiction of the attack's mechanism and recommendations for mitigating future occurrences.

Error avoidance at this point is essential to minimizing any detrimental effects on individuals engaged in the criminal justice system. Considering the grave ramifications of making a mistake, the choice to report on potential digital evidence should have been thoroughly examined and assessed before being submitted. When a practitioner reports content as evidence, the choice to do so needs to be supported by solid forensic expertise and peer-reviewed testing. The processes and procedures carried out as part of an investigation should, in most situations, be repeatable and produce results with enough confidence to satisfy a decision maker standard. There should also be no room for misunderstanding. If the source is to be used in the interpretation of the evidence in the

present case, it must also be examined and verified by another qualified party. Every source that was found ought to have undergone thorough peer review and been recognized as known good knowledge in the field of digital forensics.

Before any findings can be safely reported, all working conclusions need to be confirmed by another qualified individual. Although it might be challenging to implement, peer review is an essential step in the validation process. Confidence-building is an essential component of investigative decision making. "Sufficient confidence" in (Pollitt et al., 2018) emphasizes the need of establishing confidence as a minimum level must be achieved in decision making process. In this backdrop, practitioner's comprehension about case's surrounding facts, ability to report on findings, confidence in data interpretation, and the reliability of any related testing that produced any conclusions weighs a lot.

The diversity of evidence types and the rapid pace of change mean that practitioners often find it difficult to find directly applicable material to rely upon. Restrictions on time and equipment are real and should be taken into account when conducting testing, even though the accuracy of investigation should not be jeopardized by resource limitations.

When the practitioner identified potential content for reporting, three parameters like inferences, assumptions and conclusions should be maintained about the context and significance of information within the parameters of investigation. Before deciding whether this information may be reported with confidence, the correctness of these inferences must be assessed and tested as this will ultimately help the criminal justice system and foster understanding of an offence.

Automation can speed up data processing for investigations and yield many benefits, but any results should not be published until a thorough analysis of their significance has been completed. It is suggested that the steps outlined in the suggested framework be followed in true letter and spirit when conducting this assessment as these steps are designed in light of guideline 'digital forensics is meant to be based on science, not supposition' provided by (Collie, 2018).

Finding useful information from data that can be put to use and enable an analyst to find new avenues of information is another aspect of reporting. For instance, the data may be used to create a list of contacts that could provide more details about a crime or an incident. Additionally, information that could stop future events could be discovered, like a worm that would spread at a predefined time, or a weakness that could be exploited.

Reporting needs to be thorough and logical in all respects and should be able to answer basic questions as defined in NIST process (Kent et al., 2006).

1. Why. A legal prosecutor should decide whether to proceed with the case to trial or to close it after extracting pertinent information and analyzing the data to see whether enough evidence has been gathered.
2. What. A prosecutor should think about the evidence he wants to present in court and if it is appropriate and admissible.
3. How. It is necessary for prosecutors to specify the litigation's field. For example, criminal prosecution may be applied in hacking case. It is also necessary to take the strategies employed in the legal proceedings into account.
4. Where: The location of the legal jurisdiction should be decided / confirmed while criminal prosecution processes are performed.
5. Who: Prosecutor must specify the list of question and witness(s) as well as witness order in order to pursue a case.
6. When. In addition, prosecutors should create a complete case based on the evidence that has been produced and identify any gaps in the chronology.

Digital forensic professionals are nonetheless susceptible to human error, knowledge gaps, and general mistakes, just like professionals in any other field (Christensen et al., 2014). It must be acknowledged in DF that errors may not always have a technical or procedural origin. Sunde (2017, p. 17) has identified non-technical sources of error, which include things like "misinterpretations of the meaning, value or reliability of a piece of evidence, a biased decision, or essential evidential information being overlooked." These non-technical sources of error should also be taken into consideration.

Evidence standards are compromised in situations when there is a lack of capacity to make forensically sound decisions. This raises the possibility of injustices or dropping the cases altogether. Because of this discrepancy in experience, it is crucial to challenge the validity of the investigation decisions made by digital forensic practitioners. In this backdrop, it is necessary to repeat steps of proposed framework at least for once in order to eliminate any discrepancies.

4.5.6 Users of proposed framework

1. The purpose of the framework is to assist those who need more officialized investigative help and are actively working on digital forensic cases. Although some professionals who have developed their abilities over many years may consider this kind of working to be an inherent part of their case processing, there is still opportunity to gain from the suggested framework in terms of reducing the possibility of errors and misinterpretations.
2. It is arguable that newbie practitioners need defined guidelines in order to facilitate trustworthy decision making along the course of the investigation. The framework highlights the essential skills needed from an examiner, such as the capacity for efficient research and testing, and is particularly directed towards those studying the field of digital forensics.
3. Lastly, the framework needs to be viewed as a quality management tool for senior personnel charged with upholding the level of work, whereby quality assurance protocols can be established at crucially important phases of the investigation process.

CHAPTER 5 : RECOMMENDATIONS FOR EFFECTIVE FORENSICS MANAGEMENT

5.1 Introduction

The purpose of this study is to stimulate the fundamentals of digital forensics in organizations, especially those with IT assets and trusted areas. The majority of the DF literature now in publication focuses on first line incident response, training needs, and the identification, management, and storage of evidence (Rowlingson, 2004). For these studies to be implemented successfully and produce useful results, a significant amount of HR is needed.

Having fundamental rules that are quickly put into practice and acknowledged by the business is essential for someone starting from scratch. As a result, after analyzing the literature, the following recommendations have been made. Since everything only functions properly when it is adequately prepared, planning comes first. These guidelines guarantee that adequate protocols, procedures, and technologies are in place to facilitate a successful, economical investigation with the least possible disruption to business operations. They also address the use of DF technology to improve the organization's security posture and exhibit good governance.

Following guidelines have been prepared on basis of findings and literature:

1. Policies are the fundamental units of management that give an organization a framework for managing digital forensics. Endicott has suggested that organizations should utilize policies to get ready for DF investigations (Taylor et al., 2007). Authors suggest that organizations establish a framework for DF policies that includes supporting sub-policies and a basic DF policy. An organization's general policy should give a summary of how DF is applied and what its strategic goals are when using it. Senior management should support

the forensic policy, which should be written by forensic and/or non-forensic stakeholders.

2. To enable DF in the organization, systems and processes must be designed, configured, and implemented in a certain way. This dimension takes into account the "management" facets of DF within a company. This covers the needs for strategic, tactical, and operational management in addition to corporate governance. Companies should create a DF strategy with goals and integrate DF into the organizational structure by designating a department for accountability and responsibility.
3. The core component of a forensics capacity is its forensics infrastructure, which can consist of three key elements: technology, architecture, and monitoring. These three elements are intrinsically linked. Even with the technology in place, it cannot function well without the right architecture. Furthermore, the architecture's capabilities will be determined by the state of technology available, including current systems, but it can also have an impact on the acquisition and decommissioning of technology.
4. When forensics policies are developed and senior management becomes involved, junior employees will naturally follow safety protocols and refrain from engaging in prohibited activities. Furthermore, it is critical to integrate a forensic culture into the organization in order to turn it into a success story. It is commonly believed that upper management sets the culture. The way that DF is implemented will be directly impacted by the organizational culture; for instance, DF implementation will be simpler in a culture that values open sharing.
5. To formalize its operations, forensics requires specialized knowledge and the establishment of a dedicated department. This department interacts directly with the compliance department and may be administratively under the audit department. In the event of an incident, this department will be in charge of

gathering any evidence and completing all legal requirements. Owing to stringent legal requirements, technologies utilized to analyze digital evidence must be certified by means of industry certification, expert testimony, or vendor certification.

6. The judiciary requirements for a country or operating environment must be determined as there is none global rules set for digital investigations. Further, organizations must have incident contained capabilities in order to continue complying with international bodies.
7. Training programs ought to be accredited by qualification authorities so that staff members can receive accreditation at specific levels. In the event that personnel hold accreditation, their credibility as expert witnesses will increase the weight of the evidence collected and the protocols observed while utilizing DF tools and technologies in a court of law.

5.2 Guidelines objectives

1. Assure evidence availability, give organizational management a comprehensive understanding of the factors to take into account while getting ready for forensic investigations, and provide evidence of compliance.
2. Establish an organizational structure for digital forensics using the least number of resources possible.
3. Boost IT performance and information security by using DF tools responsibly to increase organizational efficacy and efficiency.
4. Effectively look into occurrences to identify their underlying causes and bring successful charges against those responsible.
5. Compile and examine the data related to cyber incidents.

CHAPTER 6 : CONCLUSION AND FUTURE WORK

6.1 Introduction

The field of digital forensics is constantly evolving due to the discovery of new or hitherto undiscovered digital artefacts during investigations. As a result, no single tool in the field can fully perform all tasks, and researchers frequently create new tools to fill in the functional or capability gaps left by these tools.

Organizations encounter difficulties in applying DF tools in a practical manner, which leads to investigations that are fruitless because of insufficient evidence or contamination. Effective DF application requires proper organizational infrastructure configuration. Existing literature makes clear that organizations lack comprehensive DF frameworks for implementation and management.

6.2 Applications at National level

The percentage of cyber events in Pakistan is rising at the same rate as it is rising worldwide. For a variety of known and unknown causes, including budgetary constraints, a lack of local forensics expertise and awareness, a lack of national forensics policies, and many more, organizations in this region invest little to no efforts in protecting their IT assets and trusted regions. In light of this, this activity is a meagre attempt to raise awareness among the general public and among organizations in particular. The majority of organizations have very little infrastructure for forensics. Organizations are hesitant to deploy forensics capabilities since they are exceedingly expensive, as evidenced by the literature, and instead attempt to hide the occurrence of cyber incidents.

The state-of-the-art research on computer forensics was presented in this study, which also highlights research needs. In order to motivate organizations to begin applying forensics in organizational contexts, well-known FTs were leveraged to produce results. Every tool has advantages and disadvantages that should be considered before applying it

in a certain situation. Investigators might use our investigation as a guide to compare toolkits under use with other toolkits and potentially invoke updates for forensic tools.

6.3 Potential challenge and future work

Proposed framework for reporting incidents is a concept that has not been proven in the actual world. Casey's specifications or instances of actual incidents can be used to assess the usefulness of this framework.

Following are some potential areas of research:

1. Use this study to assess Pakistani organizations' DF capability.
2. Examine the suggested framework components to assess an organization's level of readiness for forensic reporting.
3. Examine how well-performed open-source tools in comparison to proprietary tools in order to extend the evidence approach and add more attributes to their design.
4. To strengthen our forensics skills, carry out additional study and make improvements to the suggested framework.
5. More research may be done to determine how artificial intelligence is applied during the reporting phase.
6. Open-source tools need to be produced using a transparent, consistent, and good coding practice-abiding methodology in order for the DF community and legal courts to accept them as trustworthy.

REFERENCES

- Vasaka Visoottiviseth, Arnon Noonkhan, Phonpanit, R., Picha Wanichayagosol, & Sumedt Jitpukdebodin. (2023). *AXREL: Automated Extracting Registry and Event Logs for Windows Forensics*. <https://doi.org/10.1109/icsec59635.2023.10329743>
- EC-Council. (2023). *What is Digital Forensics | Phases of Digital Forensics | EC-Council*. EC-Council Logo. <https://www.eccouncil.org/cybersecurity/what-is-digital-forensics/>
- Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response*. <https://doi.org/10.6028/nist.sp.800-86>
- Jihun Joun, Lee, S.-J., & Park, J. (2023). Data remnants analysis of document files in Windows: Microsoft 365 as a case study. *Forensic Science International: Digital Investigation*, 46, 301612–301612. <https://doi.org/10.1016/j.fsidi.2023.301612>
- Dimitriadis, A., Ivezic, N., Kulvatunyou, B., & Mavridis, I. (2020). D4I - Digital forensics framework for reviewing and investigating cyber attacks. *Array*, 5, 100015. <https://doi.org/10.1016/j.array.2019.100015>
- Choi, J., Park, J., & Lee, S. (2021). Forensic exploration on windows File History. *Forensic Science International: Digital Investigation*, 36, 301134. <https://doi.org/10.1016/j.fsidi.2021.301134>
- Wikipedia Contributors. (2019, July 4). *List of Microsoft Windows versions*. Wikipedia; Wikimedia Foundation. https://en.wikipedia.org/wiki/List_of_Microsoft_Windows_versions
- UserAssist*. (2006, August 6). Didier Stevens. <https://blog.didierstevens.com/programs/userassist/>
- Solms, S., Louwrens, C., Reekie, C., & Grobler, T. (2006). A Control Framework for Digital Forensics. *IFIP Advances in Information and Communication Technology*, 343–355. https://doi.org/10.1007/0-387-36891-4_27
- View and optionally change the folders Settings of Windows Explorer*. (n.d.). NirSoft. https://www.nirsoft.net/utils/shell_bags_view.html
- Zimmerman, E. (n.d.). *Eric Zimmerman's tools*. [ericzimmerman.github.io](https://ericzimmerman.github.io/#). <https://ericzimmerman.github.io/#>
- Hintea, D., Bird, R., & Green, M. (2017). An investigation into the forensic implications of the Windows 10 operating system: recoverable artefacts and significant changes

- from Windows 8.1. *International Journal of Electronic Security and Digital Forensics*, 9(4), 326. <https://doi.org/10.1504/ijesdf.2017.10008013>
- stevewhims. (2021, January 7). *Registry - Win32 apps*. Learn.microsoft.com. <https://docs.microsoft.com/en-us/windows/desktop/sysinfo/registry>
- Horsman, G., Caithness, A., & Katsavounidis, C. (2018). A Forensic Exploration of the Microsoft Windows 10 Timeline. *Journal of Forensic Sciences*, 64(2), 577–586. <https://doi.org/10.1111/1556-4029.13875>
- Windows Security Log Encyclopedia*. (n.d.). www.ultimatewindowssecurity.com. <https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/>
- Park, S., & Lee, S. (2022). DiagAnalyzer: User behavior analysis and visualization using Windows Diagnostics logs. *Forensic Science International: Digital Investigation*, 43, 301450. <https://doi.org/10.1016/j.fsidi.2022.301450>
- BalaGanesh. (2021, November 3). *Most Common Windows Event IDs to Hunt – Mind Map - Security Investigation*. <https://www.socinvestigation.com/most-common-windows-event-ids-to-hunt-mind-map/>
- drewbatgit. (n.d.). *Run and RunOnce Registry Keys - Win32 apps*. Learn.microsoft.com. <https://learn.microsoft.com/en-us/windows/win32/setupapi/run-and-runonce-registry-keys>
- Block, F., & Dewald, A. (2019). Windows Memory Forensics: Detecting (Un)Intentionally Hidden Injected Code by Examining Page Table Entries. *Digital Investigation*, 29, S3–S12. <https://doi.org/10.1016/j.diin.2019.04.008>
- RegRipper*. (n.d.). DFIR Training. <https://www.dfir.training/tools/regripper>
- Carrier, B., 2002. Open Source Digital Forensics Tools: the Legal Argument. Technical Report stake
- Abulaish, M., & Haldar, N. A. H. (2018). Advances in Digital Forensics Frameworks and Tools. *International Journal of Digital Crime and Forensics*, 10(2), 95–119. <https://doi.org/10.4018/ijdcf.2018040106>
- Raval, H. (2020). Computer Forensic Methodology and Tools. *Digital Forensics (4n6) Journal*, 15–20. <https://doi.org/10.46293/4n6/2020.02.02.02>
- sleuthkit/autopsy_addon_modules*. (2020, May 29). GitHub. https://github.com/sleuthkit/autopsy_addon_modules
- Johnson, E., & Mack, T. (n.d.). Retrieved March 21, 2024, from <https://docs.broadcom.com/doc/istr-09-april-volume-xiv-en>

- Horsman, G. (2019). Tool testing and reliability issues in the field of digital forensics. *Digital Investigation*, 28, 163–175. <https://doi.org/10.1016/j.diin.2019.01.009>
- Mothi, D., Janicke, H., & Wagner, I. (2020). A novel principle to validate digital forensic models. *Forensic Science International: Digital Investigation*, 200904. <https://doi.org/10.1016/j.fsidi.2020.200904>
- Elyas, M., Ahmad, A., Maynard, S. B., & Lonie, A. (2015). Digital forensic readiness: Expert perspectives on a theoretical framework. *Computers & Security*, 52, 70–89. <https://doi.org/10.1016/j.cose.2015.04.003>
- Jeong, R. S. C. (2006). FORZA – Digital forensics investigation framework that incorporate legal issues. *Digital Investigation*, 3, 29–36. <https://doi.org/10.1016/j.diin.2006.06.004>
- Casey, E., & Stanley, A. (2004). Tool review – remote forensic preservation and examination tools. *Digital Investigation*, 1(4), 284–297. <https://doi.org/10.1016/j.diin.2004.11.003>
- Wu, T., Breitingner, F., & O’Shaughnessy, S. (2020). Digital forensic tools: Recent advances and enhancing the status quo. *Forensic Science International: Digital Investigation*, 34. <https://doi.org/10.1016/j.fsidi.2020.300999>
- Horsman, G. (2019). Formalising investigative decision making in digital forensics: Proposing the Digital Evidence Reporting and Decision Support (DERDS) framework. *Digital Investigation*, 28, 146–151. <https://doi.org/10.1016/j.diin.2019.01.007>
- Desktop OS market share 2013-2019.* (n.d.). Statista. <https://www.statista.com/statistics/218089/global-market-share-of-windows-7>
- USN Journal.* (2022, May 6). Wikipedia. https://en.wikipedia.org/wiki/USN_Journal
- Deland-Han. (2023, March 8). *Windows registry for advanced users - Windows Server.* Learn.microsoft.com. <https://learn.microsoft.com/en-us/troubleshoot/windows-server/performance/windows-registry-advanced-users>
- Cybercrime To Cost The World \$10.5 Trillion Annually By 2025.* (2018, December 8). Cybercrime Magazine. <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021>
- Serketzis, N., Katos, V., Ilioudis, C., Baltatzis, D., & Pangalos, G. (2019). Improving Forensic Triage Efficiency through Cyber Threat Intelligence. *Future Internet*, 11(7), 162. <https://doi.org/10.3390/fi11070162>

- Keshavarzi, M., & Ghaffary, H. R. (2020). I2CE3: A dedicated and separated attack chain for ransomware offenses as the most infamous cyber extortion. *Computer Science Review*, 36, 100233. <https://doi.org/10.1016/j.cosrev.2020.100233>
- Niksefat, S., Kaghazgaran, P., & Sadeghiyan, B. (2017). Privacy issues in intrusion detection systems: A taxonomy, survey and future directions. *Computer Science Review*, 25, 69–78. <https://doi.org/10.1016/j.cosrev.2017.07.001>
- Digital Evidence: Standards and Principles, by SWGDE and IOCE (Forensic Science Communications, April 2000)*. (2020). FBI. <https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm>
- Carrier, B. D., & Spafford, E. H. (2005). Automated Digital Evidence Target Definition Using Outlier Analysis and Existing Evidence. *Digital Forensic Research Workshop*.
- Casey, E., & Dunne, R. (2004). Digital evidence and computer crime : forensic science, computers and the Internet. Elsevier Academic Press.
- Casey, E. (2007). Digital evidence maps – A sign of the times. *Digital Investigation*, 4(1), 1–2. <https://doi.org/10.1016/j.diin.2007.01.004>
- Sulkin, O., & Courcier, S. de. (2017). Windows forensics cookbook : 61 recipes to help you analyze Windows systems. Packt Publishing.
- Desktop, Tablet & Console Operating System Market Share Worldwide*. (n.d.). StatCounter Global Stats. <https://gs.statcounter.com/os-market-share/desktop-tablet-console/worldwide/#monthly-201810-201910>
- Agarwal, A., & Gupta, M. (2011). Systematic Digital Forensic Investigation Model.
- Rogers, M., Goldman, J., Mislán, R., Wedge, T., & Debrota, S. (2006). Computer Forensics Field Triage Process Model. *The Journal of Digital Forensics, Security and Law*, 1(2). <https://doi.org/10.15394/jdfsl.2006.1004>
- Kohn, M. D., Eloff, M. M., & Eloff, J. H. P. (2013). Integrated digital forensic process model. *Computers & Security*, 38, 103–115. <https://doi.org/10.1016/j.cose.2013.05.001>
- Carrier, B. D., & Spafford, E. (2003). *Getting Physical with the Digital Investigation Process*. ResearchGate; unknown. https://www.researchgate.net/publication/220542528_Getting_Physical_with_the_Digital_Investigation_Process

- markruss. (2024, February 13). *Sysmon - Sysinternals*. Learn.microsoft.com. <https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon#configuration-entries>
- Sinangin, D. (2002). Computer Forensics Investigations in a Corporate Environment. *Computer Fraud & Security*, 2002(6), 11–14. [https://doi.org/10.1016/s1361-3723\(02\)00610-3](https://doi.org/10.1016/s1361-3723(02)00610-3)
- Richardson, R. (2008). *The latest results from the longest-running project of its kind*. <http://www.sis.pitt.edu/jjoshi/courses/IS2150/Fall10/CSIsurvey2008.pdf>
- The Role of Digital Forensics within a Corporate Organization. (2006). <http://digitalforensics.ch/nikkel06a.pdf#search%3D%22digital%20Forensic%20readiness%22>
- Isaca. (2019). *COBIT | Control Objectives for Information Technologies | ISACA*. Isaca.org. <https://www.isaca.org/resources/cobit>
- Sachowski, J. (2016). Implementing Digital Forensics Readiness : From Reactive to Proactive Process. William Andrew.
- Log, N., Blueangel, T., & Oh, J. (n.d.). *FORENSIC INSIGHT; DIGITAL FORENSICS COMMUNITY IN KOREA*. Retrieved November 28, 2023, from <http://forensicinsight.org/wp-content/uploads/2013/06/F-INSIGHT-NTFS-Log-TrackerEnglish.pdf>
- NTFS LogFile Parser*. (2016, January 20). CodeProject. <https://www.codeproject.com/Tips/1072219/NTFS-LogFile-Parser>
- Sommer, P. (2005, September 1). *Directors and corporate advisors' guide to digital investigations and evidence*. Wwww.iaac.org.uk. <https://eprints.lse.ac.uk/13779/>
- Pollitt, M., Casey, E., Jaquet-Chiffelle, D.-O., & Gladyshev, P. (2018). *A Framework for Harmonizing Forensic Science Practices and Digital/Multimedia Evidence*. <https://doi.org/10.29325/osac.ts.0002>
- Collie, J. (2018). Digital forensic evidence—Flaws in the criminal justice system. *Forensic Science International*, 289, 154–155. <https://doi.org/10.1016/j.forsciint.2018.05.014>
- Christensen, A. M., Crowder, C. M., Ousley, S. D., & Houck, M. M. (2013). Error and its Meaning in Forensic Science. *Journal of Forensic Sciences*, 59(1), 123–126. <https://doi.org/10.1111/1556-4029.12275>
- Sunde, N. (2017). Non-technical sources of errors when handling digital evidence within a criminal investigation. *III + Vedlegg*. <http://hdl.handle.net/11250/2446090>

- Rowlingson, R. (2004). A Ten Step Process for Forensic Readiness. *International Journal of Digital Evidence*, 2.
- Taylor, C., Endicott-Popovsky, B., & Frincke, D. A. (2007). Specifying digital forensics: A forensics policy approach. *Digital Investigation*, 4, 101–104. <https://doi.org/10.1016/j.diin.2007.06.006>
- Manson, D., Carlin, A., Ramos, S., Gyger, A., Kaufman, M., & Treichelt, J. (2007). Is the Open Way a Better Way? Digital Forensics Using Open Source Tools. *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*. <https://doi.org/10.1109/hicss.2007.301>
- Mrdovic, S., Huseinovic, A., & Zajko, E. (2009, October 1). *Combining static and live digital forensic analysis in virtual environment*. IEEE Xplore. <https://doi.org/10.1109/ICAT.2009.5348415>
- Locard's Exchange Principle* | *Encyclopedia.com*. (2013). Encyclopedia.com. <https://www.encyclopedia.com/science/encyclopedias-almanacs-transcripts-and-maps/locards-exchange-principle>