COMPUTER AND CYBERCRIME FORENSICS INVESTIGATION IN MYANMAR

TIN MAUNG MAUNG

UNIVERSITY OF COMPUTER STUDIES, YANGON

April, 2022

Computer and Cybercrime Forensics Investigation in Myanmar

Tin Maung Maung

University of Computer Studies, Yangon

A thesis submitted to the University of Computer Studies, Yangon in partial fulfilment of the requirements for the degree of

Doctor of Philosophy

April, 2022

Statement of Originality

I hereby certify that the work embodied in this thesis is the result of original research and has not been submitted for a higher degree to any other University or Institution.

12/04/2022 ……

Date

…….. Tin Maung Maung

ACKNOWLEDGEMENTS

First of all, I would like to expand my thanks to His Excellency, the Minister, the Ministry of Science and Technology for full facilities support during the Doctoral Course at the University of Computer Studies, Yangon.

Secondly, I would like to express very special thanks to Dr. Mie Mie Khin, the Rector, the University of Computer Studies, Yangon, for her continuous guidance and advice during the period of my study. I'm deeply grateful to you for your permission.

I would also like to expand my very special thanks to Dr. Mie Mie Thet Thwin, former Rector, the University of Computer Studies, Yangon, for allowing me to develop this thesis and giving me general guidance during the period of my study.

I would also like to extend my special appreciation and thanks to Dr. Thin Lai Lai Thein, Professor, Course coordinator of the Ph.D 10th batch, the University of Computer Studies, Yangon, for the useful comments, advices and insight which are invaluable to me.

I would like to express my deepest gratitude to my supervisor, Dr. Khaing Khaing Wai, Professor, the University of Computer Studies, Yangon, for her excellent guidance, caring, patience, and providing me with excellent ideas for doing research.

I would also like to express my deepest gratitude to my co-supervisor, Dr. Cho Cho San, Lecturer, the University of Computer Studies, Yangon, for her guidance, caring, and patience for doing research.

I would like to expand my deepest gratitude to my former supervisor, Dr. Mie Mie Su Thwin, Professor, the University of Computer Studies, Yangon, for her patient supervision, tenderness, encouragement and providing me with excellent ideas throughout the study of this research.

I would also like to express my respectful gratitude to Dr. Khine Khine Oo, Professor, former Ph.D 10th batch teacher, the University of Computer Studies, Yangon, for her deepest guidance for this research.

I would like to express my respectful gratitude to Daw Aye Aye Khine, Associate Professor, Head of English Department for her valuable supports from the language point of view and pointed out the correct usage in my dissertation.

I also thank my friends from Ph.D 10th batch for providing support and friendship that I needed.

I am very much indebted to my parents and my wife for always believing in me, for their endless love and support. They are always supporting and encouraging me during the years of my Ph.D study.

ABSTRACT

Communication technology and devices are timely changing and increasing various levels and different operating systems in all over the world. In this day and age, our country is just developing country and most of the people are not accustomed to use the modern communications system and digital devices. The rapid increase of smart technologies and Internet usage creates new attack surfaces for cybercrime. In society, information is the new challenge for security, privacy, and cybercrime. To prevent cyberspace from exploitation of vulnerabilities it is essential to understand current and future threats with the use of social media, mobile device, virtual worlds, and mixed reality.

Digital Investigators do not have to try and read people's minds anymore because people's interests, hidden secrets, financial information and even their love life are all on their computer. The usage of Standard Cyber Laws and Policy for Cybercrime Investigation can provide an ethical, secure and monitored computing environment. Acceptable Evidences can be obtained by examining sensible clues from any digital devices such as computer, mobile smart phones, tablets, GPS and IoT devices via traditional way or cloud. The most important part of forensic investigation is to gather the “relevant” and “acceptable” information for cyber evidence on court. There is a need for forensic examiners to investigate the locating and documenting the remnant data on various digital devices to trace the criminal offensive activities.

Computer users think that by simply deleting traces of their activity, everything is gone. What they do not realize is that by using the right Digital Forensics tool, that can locate, extract and analyze what was once there and get it back. There will be amazed by the number of artifacts that can be recovered and extracted, even from the tiniest of devices. Therefore, forensic investigators need to emphasize how file system timestamps work. At the present time, most of the computer users are familiarity in Windows Operating System of Microsoft Platform and mobile phone users almost used in Android and iOS operating systems in Myanmar. Utilization of Open Source forensics tool has not only helped reduce and prevent cybercrime but also cost of investigation and protect the country from cybercrime.

In this research, the workable process flow which consists of six stages and a detailed analysis framework have been proposed for the forensics investigation on Windows and Mobile systems. Consequently, the scope of this research includes Windows, Android and iOS operating system for computer and cyber forensics. The discovered data remnants can provide the forensic examiners generating the effective evidences in real-world forensics. The discovered data remnants can lead the forensic data reduction. Finally, an applicable tool (MYANFOSICS) with many useful features has been proposed for the forensics investigation on Windows, Android and iOS operating systems.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

Nowadays, digital devices are rapidly developed and especially IoT devices have become the modern protocol for people all over the communication. As a consequence, this growth of digital devices such as smart phones, tablets, personal digital assistants, smart home and IoT devices lead to the cyber-criminal activities.

Cybercrime forensics investigation is not a new field but still based on new practices and new threats encountered; it is an evolving one. Forensic investigation is the vital phase for Cybercrime analysis because the analysis totally depends upon the quality, fine granularity, effectiveness, systematic and legal investigation process being carried out by the computer forensics experts. So, for that purpose the investigations should be systematic, expert, customized and sound enough making it a process been done in less time and therefore causing more relevant information to be collected and subsequently being investigated.

Digital devices will facilitate to store various data and install many applications on their storage and operating system. The cyber criminals may use these features and services for their personal gain and to interrupt the victim community. Therefore, cyber forensics is an emerging practice to discover evidence from these digital devices and prosecute criminals in a court of law.

Digital Evidence – encompasses any and all digital data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator.

The IT security is the most complex area inside the digital world because there are exposed to a huge number of threats and dozens of malwares (virus, Trojans, spies, worms and ransomwares) come up every single day, including other hundreds of variants. Malwares are becoming more sophisticated by adding rootkits techniques in their codes, by using anti-forensic techniques to hinder the analysis by experts, by abusing of encrypted codes and lots of other tricks.

One area of growing concern among forensic examiners is what and where a file has been. While many digital artifacts exist to prove that a file was opened, the

most essential piece of information needed is the file's timestamp information. This research proposed an overall solution framework and process flow that can be followed systematically to produce forensically sound evidence. This solution will support and cover to collect evidence data in different forensics field such as static, cloud and social network environments. The solution is an adaptation or combination of several existing forensic stages. This framework and process flow will support and cover to collect evidence data in different operating systems such as Microsoft Windows, Android and iOS environments. The purpose of doing this research is to provide an applicable forensics tool for our treasured country Myanmar.

1.1 The Problem Statement

In this day and age, a boundless crime being perpetuated by using computer and mobile phones like hate messages, incitement, social harassment, extortion, fraud, child exploitation, terrorism, drug trafficking, and money laundering are on increase in Myanmar. But more often than not evidence presented before Myanmar courts of laws are inadmissible due to lack of proper Digital Forensics framework. It is very important that the gathered information need not only to be fast but also to be in correct manner. This necessitated ministry of transportation and communication to institute some regulatory policies like requiring all mobile subscribers to register their SIM card with effect from 2017. In Myanmar, ICT is rapidly developing with international service provider such as Mytel, Telenor, Ooredoo.

Internet is widely used to share information and easily then its impact is large. Nowadays, some illegal actions can use ICT on social network for propaganda such as incitement, terrorism events of in Myanmar. According to the chain of custody, information is miss distribution by hiding the actual or ground information and replacing with photo or movie of previous event in other country using social network or effective broadcasting. The primary objective of this research is to carry out an organized and structured investigation in order to preserve, identify, extract, document and interpret information that is then utilized to prevent, detect and solve cybercrimes.

1.2 The Proposed Solution

In this dissertation, the workable process flow has been proposed for the forensics investigation on Windows and Mobile systems which consists of six stages.

They are (1) Case Confirmation, (2) Scope Determination, (3) Requirement Readiness, (4) Examination and Imaging, (5) Extraction and Analysis, and (6) Reporting and Review. A detailed analysis framework has also been proposed for Examination and Imaging stage. It is divided into two main parts – Live Forensics and Static Forensics because if the investigator does not notice the Live Forensics, the data on memory can be easily lost.

Finally, an applicable tool (MYANFOSICS) with many useful features has been proposed that would support the analysis framework. It consists of four main parts: (i) data acquisition and collection, (ii) examination (iii) reporting, and (iv) management process.

1.3 The Objectives of Research

This research aims to ensure that in the case of digital evidence is required, it will be available and in an acceptable form. It can also serve to complement the plans of other organizations in a process of investigation, including disaster recovery and business continuity. Therefore, this research proposed for the following objectives:

- To identify the exact nature and seriousness of the incident
- To collect evidence accepted by law
- To gather information to get evidence from the crime scene
- To minimize interruptions in operation by the investigation
- To allow investigation to proceed at a cost comparable to the incidence
- To ensure that the impact of positive evidence on the outcome of any legal action
- To propose the effective tool for Cyber Crime Investigation System

1.4 The Organization of Research

This dissertation is organized with six chapters, including introduction of cybercrimes, computer and cyber forensics, problem statements, and objectives of the research. Chapter 2 surveys the different sources to digital forensics frameworks and process flows in literature. The theory background of cyber offensive and attacking techniques, the differences in cyber forensics methodology are described in Chapter 3. The architecture of the system, framework and process flow for cybercrime forensics investigation are presented in Chapter 4. Chapter 5 describes the implementation of the

MYANFOSICS system and the evaluation of the experimental results by testing with different forensics open source tools. Finally, Chapter 6 presents the conclusion extracted from this research and depicts the future works.

CHAPTER 2

LITERATURE REVIEW AND RELATED WORK

This chapter discusses literature review in the development of forensics methodologies such as process flows, analysis frameworks, acquisition methods, tools and techniques.

2.1 Process Model and Framework for Digital Forensics

Authors in [7], purposed of the research was to develop a digital forensics framework that will serve as a blueprint for Kenyan courts of laws in apprehending digital criminals. Existing DF models were surveyed and then adopted to create a specific application framework. The finding can be used by both government and private agencies in developing countries like Kenya as a guide in providing Digital Forensics services whether Internal investigation, disciplinary hearing or court case.

In [27], the authors purposed the model based on the grouping of the overlapping and similar phases, Phase 1 of GCFIM is known as Pre-Process. And Phase 2 is Acquisition & Preservation phase. Next phase is Analysis and after that Presentation phase comes. Last Phase is Post-Process phase. This phase relates to the proper closing of the investigation exercise and the lesson can be learnt and used for improvement of the future investigations.

In 2011 [3], the researchers Agarwal and colleagues proposed a systemic approach to digital forensic investigation. There are 11 phases in this model named Preparation, securing the scene, survey and recognition, documentation of scene, communication shielding, evidence (both volatile and non-volatile) collection, preservation, examination, analysis, presentation, result and review is shown in Figure 2.1.

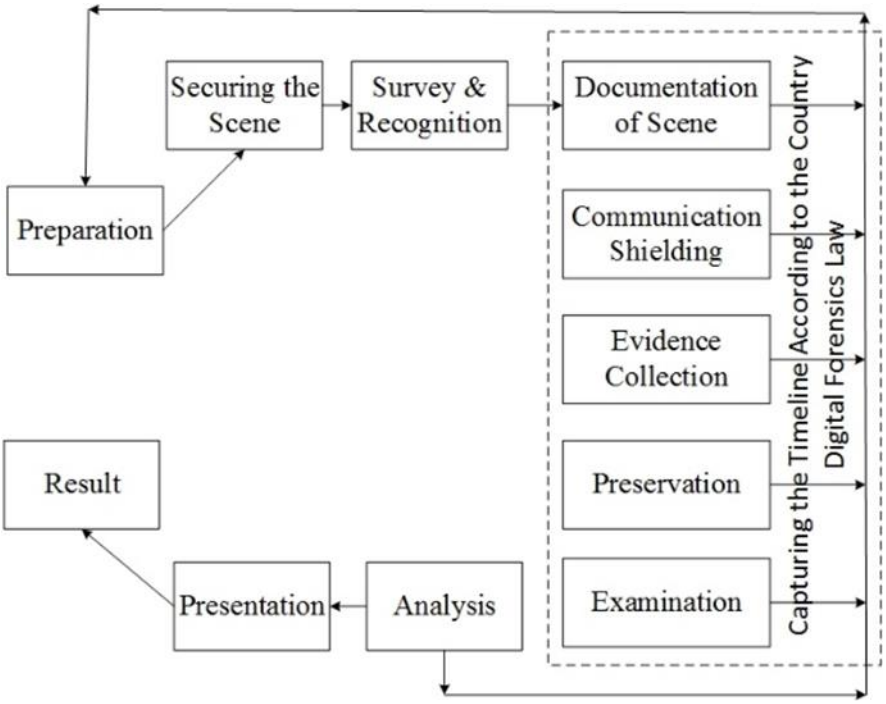

Figure 2.1 A Systematic Digital Forensic Investigation Model

In [13], the researcher has discussed how the stages on Digital Forensics Readiness (DFR) within the solution of the preservation of digital evidence. Minimize the duration and cost of the investigation, it has proposed a new scheme called Digital Forensics Readiness Schema (DFRS). In principle, DFRS have to accommodate the interests and the need to conduct an investigation in order to readiness digital forensic process.

In this research [10], the authors discussed the research category in computer forensics and identifies key research issues of each of the category. It provided foundation and new ideas for the researcher to better understand the concepts of computer forensic. The outcome presents came from thoroughly review of recent computer forensic literatures.

In [5], the researcher discussed that they are introducing a new digital Forensic model which will be capture a full scope of an investigation process based on Malaysia Cyber Law. The proposed model is also compared with the existing model which currently available and being apply in the investigation process.

In another research [17], the author proposed business model already accommodates major components of digital forensics (human, digital evidence,

process) and also considers the interactions among the components. This will give support to law enforcement to deal with cybercrime cases and can be a reference for each institution and organization to implement digital forensics activities.

In [18], the author collected the researches of investigation procedure of cybercrime in the recent years. By introducing the research investigation procedure of these papers, they will discover the features of every procedure. Then they compare these investigation procedures via the traditional investigative procedure's compatibility, cybercrime behavior analysis, evidence forensic procedures, case analysis and verification, the methods of evidence collection and analysis, and the area of judicial jurisdiction. Finally, they will propose the viewpoints of cybercrime investigation and forensic procedures, and they wish this paper will help the research of investigation and forensic procedures.

Authors in [27] presented Malaysian Chief Government Security Office (MCGSO) is using their own unstandardized digital forensic procedures that will be practiced by a digital investigator in carrying out digital investigation activities. The procedures are depending on cases. Concluded in their procedure are the elements of digital forensic. The job space for MCGSO staff in digital forensic field was to provide protection security advice from physical aspects, documents, personnel, and ICT security. In other word, the cases that will be investigated were not specifically to be used in judgment. Simultaneously, it did not applicable in digital forensic framework approach as this kind of procedure had stated that their goal is to made the crimes been judged in the court of law. That is why, this study will focus on proposing the business model for MCGSO.

The contribution to this case study was a generic digital forensic business model for MCGSO so that the interaction between human, interaction between human and digital evidence, and interaction between human and the process of digital forensic will be applied accordance to their digital forensic procedures.

2.2 Computer Forensics

In this research [20], the authors examined distinctive forensic tools used for analyzing security flaws in digital forensics and also the detailed review of cyber forensics. The new process model is opted to collect crucial evidence quickly and

investigate the cases immediately. The Stepwise Forensic Process Model presents the stepwise and in-situ approach provides incident identification, recovery, analysis. The SFPM suggest a new investigational model for selecting the target and analyzing the relevant evidences only. It is based on the crime scene circumstance and is intended to quickly selecting and investigating the system, to overcome the limitations of traditional forensic model. This research provides a provisional study of the tools regarding cyber forensic analysis.

In [21], the author introduced the current situation of information crime and computer forensics and the production of the class. On the basis of this, the author summarized the development and thought about the trend of the discipline. Information crime and computer forensics is a cross subject. It combines computer science with forensics and law. Although it is a young subject, it is a super excellence way to resolve the increasingly serious information crime situation. Thus, the subject will develop very soon. The author assumed that new research work will come out in the big data era.

2.3 Mobile Devices Forensics

In this research [24], the author reviewed totally 100 Mobile Forensics models. Using different terminologies, the scholars in this field have made use of various approaches regarding the number of phases in the investigation process. This article started with reviewing all existing Mobile Forensics studies; then, it discussed the challenges, limitations, and drawbacks of the field, and suggested a number of solutions to the limitations identified. In the following, some ideas are recommended for future research in the Mobile Forensics field:

- Improving and validating the proposed investigation process model (HMFIPM);
- Development of a meta-modeling language that can be applied to structuring, managing, organizing, sharing, and reusing the created Mobile Forensics knowledge;
- Development of a definite Mobile Forensics source for the purpose of storing and retrieving the knowledge formed in the Mobile Forensics field.

In [25], the researcher presented that the dramatic rise in digital technology gives rise to new avenues for digital penetrators to devise new and sophisticated attack

methods in order to bypass security defense, trap the victim and breach the security setups. Across the globe, digital attacks performed by these determined cyber penetrators have impacted huge masses and nagged billions of dollars. The emergence of digital crimes and dependence on technology has led to the development of Digital Forensics which acts as an armor in this battlefield. This research provides a brief on digital forensics process, its evaluation metrics, and proposes a taxonomy of digital forensics tools which provides a detailed overview and comparison among different forensics tools based on different features in their categories. Furthermore, they identified several indispensable challenges in this fascinated area.

2.4 Computer and Cyber Forensics Tools

In another research [23], the author explained that there is a need to analyze the existing legal regime relating to use and admissibility of cyber forensics in crime investigation and trial. For the purpose, various tools and techniques used for disc and device forensics should be analyzed. These tools and techniques can be made more useful in criminal investigation and trial. The analysis of the provisions of law where under these Cyber Forensic tools can be used by the investigation agencies and the courts in law enforcement should also be done. The present relation of cyber forensics and law is of new friends, which needs to be furthered and achieved to the level of a wedded couple.

In this research [19], the author presented as forensic examiners, there is no shortage of techniques to prove that something occurred and when it occurred. However, being able to prove the Why, How and most importantly, when a specific file(s) was created or used goes further to prove who was behind the keyboard during the time of the incident than merely finding the file(s) and determining that the case is solved. This paper includes compares and experimental results of file system timestamps work not only between NTFS, FAT32 and exFAT, but also between Windows Operating Systems testing with Window XP, Window 7, Window 8.

FTK Imager is one of the most famous tools in the forensics world. The tool allows the investigator to acquire various types of storage devices and store them in different formats for analysis. It is extremely important to remember to use Write Blockers when acquiring images for a hard disk, so that it won't destroy or alter

important data on the disk. FTK is a commercial tool. However, the free version has many useful features that an investigator could benefit from.

Live Response Collection is a very handy framework from Bambiraptor, which can collect various and useful information from a machine. The tool offers many acquisition types; each one is used depending on the data we're interested in. Live response is very easy to use. All that is needed is to select the type of acquisition wanted. Live response offers a "secure" option that allows the investigator to protect the acquired data with a password. The process will take time depending on which option choose. Once it's done, it will find a folder with the machine's name inside the tools directory. The folder will contain the images taken, the data collected, and verification data alongside a log file. In the forensics images Folder, it will find the hard disk and RAM images. The hard disk images can be loaded, mounted and analyzed using FTK. The RAM image on the other hand is best analyzed using Volatility. In the Live Response Data, it will find most of the evidence.

Volatility comes pre-installed with Kali Linux, and can also found in exe format for running on Windows machines. When using volatility, it should first determine the OS that the image was taken from with the image info flag. Volatility will analyze the image and give suggestions. Once the investigator has the profile name, it should supply with every command with the --profile flag.

Some tools offer data splitting alongside imaging, which make handling large size image files easier. One popular tool to image a disc in raw format is the DD tool, which is available for both Linux, by default, and Windows.

Many commercial tools for imaging implement their own file format. Those special/proprietary file formats usually contain the original data (usually encoded in a way only their tool can understand) plus a header with metadata such as hash value or CC embedded within. Proprietary tools also use compression for more space efficiency but make the imaging and the analysis process slower. The advantages of using proprietary formats are space efficiency, all the case related metadata, data are on a single file (Case number, device name etc.) Usually gives the investigator the ability to do all their work on a single framework since most proprietary tools include imaging, analysis and reporting modules. On the other hand, using proprietary tools and format

is slower due for the compression/decompression and encoding/decoding processes done.

Also binds the investigator to the framework they're using because proprietary file formats are rarely cross platform. Some of the famous proprietary formats are:

- Expert Witness Format (EWF) which is used by EnCase.
- IDIF, IRBF, IEIF used by ILook Investigator.
- sgzip used by PyFlag.

Different formats have different attributes and tools to be analyzed with. Finally, some proprietary formats have space limits. For example, some old EWF's are limited in size to 2GB per image. If the suspect's disk is larger than 2 GBs, it has to be broken into 2 GBs chunks and then the combined for the analysis. Advanced Forensics Format (AFF): is an open image format developed by Basis Technology. Alongside compression, which helps save disk space, and integrity check, most AFF tools allows the investigator to add customary fields. It also allows the investigator to either embed that metadata within the image or on a separate file. The AFF also gives the investigator flexibility, since it is supported by many open source tools and frameworks. AFF based tools copy the data from the suspect's device in 16 MB blocks (usually called Pages). Early versions of AFF suffered from a few issues. For example, it wasn't possible to collect live, data and it lacked encryption. It also had problems while dealing with NTFS metadata (due to the 16 MB page size). A later version addressed most of these issues; however, an investigator would still encounter a problem if they have to work on an image captured by frameworks that are still using the old format.

2.5 Chapter Summary

In this chapter, the concept of the nature of digital forensics were presented. With the rapidly growth of information technology in everyday, there is a need for computer and mobile device forensics was highlighted. After learning the fundamental of digital forensics, the cyber forensics process was emphasized and many commercial computer and mobile device forensics tools such as Encase, Belkasoft, Autopsy, FTK, UFED etc. were discussed. Moreover, the previous related work of process model, framework and tools for digital forensics were reviewed. According to the literature reviews of previous studies, there is no research on computer and cyber forensics tool

for Myanmar, depending on the desired process flow and framework for our country. At this time, there is a lack of cyber laws enforcement in Myanmar. In the next chapter, the background theory of this research will be discussed in detail.

CHAPTER 3

THEORETICAL BACKGROUND

In developing countries, ICT is rapidly developing with international service provider. Internet is widely used to share information and easily then its impact is large. The rise of technology has brought about new waves of criminal activities and how criminals conduct traditional crimes. Nowadays, some illegal actions can use ICT on social network for propaganda. Cybercrime Forensics Investigation is urgently requirement matter for developing countries. Digital forensics (or digital forensic science) is a discipline of forensic science, which is the recovery and investigation of artifacts found in digital devices, often in relation to a computer crime. [34]

3.1 Cybercrime

It is nothing but where the Computer and Digital Devices used as an object or subject of crime. Cybercrimes can be basically divided into four major categories:

- Cybercrime against person
- Cybercrime against poverty
- Cybercrime against Government
- Cybercrime against society at large

Major challenges in Cyberspace Security are

- Cyber warfare (CNE and CNA)
- Lack of Cooperation Between Nations
- Lack of Knowledge regarding Technology
- Lack of Utilization of Available Technology
- Dark Web
- Inadequacies of Law Enforcement

3.2 Cybercrime Forensics

Forensics is the application of scientific test or technique used in criminal investigation. Cybercrime forensics is the process of uncovering and interpreting electronic data for the detection and investigation of crime committed on computers, computer networks, the internet and other digital devices. With technology entering every aspect of our lives, the applications of digital forensics are growing rapidly. In

general; the main goal of digital forensics is to answer the big five W's, regarding any digital incident.

What Where When Who How

Cyber Forensics can also be used to support non-digital civil and criminal cases such as proving intent. For example, finding "how to make bombs" in someone's browsing history could be used as an indicator linking that person to terrorism. In comparison with conventional crimes, digital crimes impose new challenges to investigators. A conventional crime might be something like stealing a cashier's wallet. While a digital crime could be done by using different hacking techniques, such as phishing, skimming, etc.

There are the fundamentals of most common digital investigations, which include Digital Evidence, Digital Forensics Tools and Scientific Method. [45]

3.2.1 Digital Evidence

In any crime investigation, the foundation is the evidence: for instance, a fingerprint in a homicide case. In the digital world, evidence is defined as any digital information that is stored, transmitted or produced from electronic devices and/or software. Examples of digital evidence are

- Pictures produced by cameras
- Print logs saved on printers
- Temporary files produced by a web browser
- Downloaded files
- Email messages
- Deleted files

One should always carefully collect evidence, but in crime scenes with digital media involved, it's an even more critical issue. That's why investigator should be aware of how digital media and applications work because digital evidences can be easily altered or lost during their life cycle. If any procedure was conducted incorrectly, then the evidence might become inadmissible in court. Also, be aware that investigator knowledge and expertise in handling the evidence determine the evidence quality and importance in court, which affects the jurors' decision. [43]

3.2.1.1 Types and Sources of Digital Evidence

An Investigator can find all types of data in a number of different devices, so it could say that investigation may involve any device that is able to store digital data, and these could be categorized in, but not limited to:

- Image Files
- Hidden Files
- Software applications
- Encrypted Files
- Known Remote Access Tools
- Hidden partitions
- Deleted Files
- Computer Systems
- Desktops, laptop, etc.

It is the richest source of artifacts and contains valuable information about the suspect and what they were doing. The investigator may find various types of artifacts like email, chat logs and financial information.

- Storage Devices are hard drives and external hard drives. These devices differ in size and the way they process and store data. These devices may contain valuable artifacts for analysis.
- Removable media is any type of storage device that could be removed while the system is running, such as a CD. These devices are used by people to store information or applications they use.
- Thumb drives are small storage devices can easily be hidden and transported, so they may be used by a suspect to hide important files.
- Memory cards could be found in many devices, such as digital cameras and mobile phones. Even with its small size, it can find a large amount of data inside these cards such as pictures and other files.
- Handheld Devices are a close friend for most people; it can tell you great details about your suspect, as it can store data, images, global positioning system (GPS) information and other valuable information.

- Peripheral Devices may be helpful to find the last thing the suspect did. For example, if an investigator finds a printer it could know what documents have been printed recently, and the same for other devices, including scanner, fax, etc.

Computer Networks contain the largest amount of data the investigator could ever analyze. When the case involves a company or a large organization investigation may include network devices. These devices, such as Authoritative name server, will provide valuable information such as IP address, which could be used to relate an incident to a suspect device.

An example of hidden storage devices is a chip hidden inside USB cable, or A/C power-pack that contains a hidden camera. These types of evidences are difficult to notice unless realize their existence, and they are sure to contain important artifacts. The investigator may find unexpected evidences inside digital devices, for example, even if iPod devices are only used to hear music, it may find document files stored on it. In each case there will be different devices to deal with, but whatever the device involved in the case investigate, the investigator should be familiar with how to deal with this type of evidence and data it contains. It should also know exactly how this device works, how data is stored and processed in it. In cases where encounter evidence is not familiar with, it should call an expert to help complete the analysis to avoid wrong procedures that causes data loss or dismissal of evidence in court. Digital Evidence should have the following characteristics:

- Admissibility- accepted in a court
- Authenticity- relevant to the case
- Complete- no missing information

The digital evidence life cycle consists of three phases. It is advised to follow these phases to guarantee evidence admissibility, regardless of evidence type or the incident forensics investigate. [63]

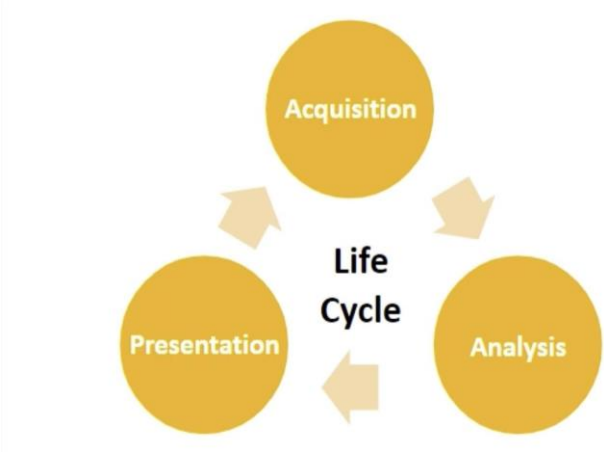

Figure 3.1 Digital Evidence Life Cycle

3.2.1.2 Digital Evidence Life Cycle: Acquisition

Acquisition is the process of obtaining a forensic sound image (physically or remotely) of the evidence to be analyzed. It is an important phase, as the evidence validity depends on it. Evidence acquisition is important because the validity of other steps depends on the validity of this phase, which means that evidence collection done incorrectly or illegally will result in evidence being unacceptable in other steps. In the CSI series Grissom says, “To get to the evidence, we might destroy the evidence”.

Investigators should have the basic experience to deal with digital evidence in order to avoid destroying it. The investigators should also guarantee that:

- The delivery of the evidence is as it was found.
- The evidence will not be exposed to alteration.

Acquisition steps should be done carefully because any wrong action will ruin the evidence and could lead to completely different results.

If the device is running, there is a need to insure the continuity of the power supply until creating the image, as cutting off the power might cause loss of valuable artifacts. Be careful of any destructive program(s) running (i.e., performing a wipe operation).

Finally, in the case of a running or turned-off device, seal the evidence in a container for later analysis. Make sure to use proper and secure containers to secure evidence. Use digital safe containers for evidence keeping, such as antistatic bags and antistatic pads. Make sure that those containers are well padded. Write notes on the

tape to prevent tampering with the evidence, ensure that temperature and humidity ranges are adequate for all evidence.

The investigator should document all steps of acquisition, to indicate its soundness; before moving on, the investigator may inspect the scene to search for a password or any other important note. All mentioned steps will guarantee the authenticity and soundness of the evidence.

3.2.1.3 Digital Evidence Life Cycle: Analysis

The most important thing to consider is preserving the original evidence without alteration, which is why it's very important that before starting analysis, there should be create a forensic image of the evidence and perform analysis on this image (sometimes it is not possible). It is very important to validate all analysis steps to ensure results later, and to leave no holes for questioning by a defense attorney. Just like the acquisition phase, the documentation is paramount in the analysis phase; there must be need to document all tools that used during analysis and the procedures. The Digital Forensics field is rapidly changing and evolving.

According to the hypothesis, the forensic analysis conducted to generate one of the following:

- Inculpatory Evidence: Supports a hypothesis
- Exculpatory Evidence: Contradicts a hypothesis
- Tampering Evidence: Indicates system tampering with the aim of deception

DF analysis is defined as scientific method, which starts by gathering facts from the evidence have, building a hypothesis to explain an incident, and extracting artifacts to prove or refute this hypothesis. The scientific method is a generic approach used in most fields and not just restricted to digital forensics. In every case it should prepare a new special device (storage) for analysis, if this is impossible to achieve, it should perform a forensic wipe on the disk to remove old data on the disk before copying the new evidence. Some digital devices will need special treatment. For example, if it need to analyze a wireless device, this device should be isolated from the surrounding environment to prevent a new connection which will alter the evidence because of new data packets flowing in and out of the device wiping the old packets from the device. In physical cases, investigators collect observations from evidences they have, such as

a victim's wounds to help in determining how the incident crime happened, when and by whom.

Digital analysis works the same as physical cases; it starts by gathering observations from the evidence, building a hypothesis that explains what caused the evidence, and by whom to gain an understanding of the whole case. For example, reading a suspect email may indicate the existence of important information that was sent to the suspect on CD, or the analyzer has to search the internet for evidences like chats between the suspect and victim. Analysis may encompass recovering deleted files, specifying the time of creation and linking it to a suspect. Also, the evidence it finds could lead to further evidences from different resources. [44]

3.2.1.4 Digital Evidence Life Cycle: Presentation

The last investigation phase is presentation, where investigator should provide a report of analysis results by mentioning the artifacts. Steps investigator followed to reveal these artifacts, and the tools used for analysis. Depending on investigator experience, there will be provided a reasonable explanation for these artifacts and how it will help in the current investigation. What report should specifically include mostly depends on the party that asked for the investigation such as court, police, company, or even individuals. Regardless of whoever requested the investigation, when it present in court, investigator task will require more effort for the proper presentation of evidence. Juries (especially when they do not have any technical background) are usually convinced when they see the physical evidence; therefore, it is forensics investigation to present the digital evidence in its best physical form. The amount and types of digital evidence it will have to analyze will differ from case to case and depends on different criteria. In situations where there is a large amount of data, there will be only need to extract enough artifacts to incriminate the suspect or explain the incident that occurred.

The analysis steps, tools and types of valid evidence may pertain to judicature. Unfortunately, legalized practices are not generalized among countries and it should be aware of the country's forensics legalized practices to build forensics case and form analysis steps or ask a local attorney office.

3.2.2 Digital Forensics Tools

Tools have an important role in the forensic investigation process. But, Digital Forensics isn't about just using tools. An investigator is expected to have a deep understanding for the underlying technology investigator is dealing with. Knowing how to the tool works is important, but digital investigators should also know how data is acquired, processed, interpreted and displayed by the tool investigator is using. There are different types of DF tools available for investigator to use

- Proprietary tool
- Open source tool
- Own tool

There is a need to choose the best tool for investigation depends on cybercrime nature and on the grounds policies.

3.2.3 Scientific Method

An investigator is also expected to be able to:

- Apply the Scientific Method during the investigation.
- Analyze data and compare samples.
- Notice any abbreviation, abnormalities, and characteristics.

This is not possible if the investigator is not aware of the regular characteristics of data and technology. The Scientific Method is the investigator's most useful ally in mission to present reliable evidence.

The methodology is simple:

- Observing
- Collecting data and facts
- Finally, building a hypothesis based on data collected

The next step for the investigator is to start making predictions based on the hypothesis formulated. Such prediction must be testable and provable; otherwise. it is meaningless. To minimize the chances of having an error, investigator has to consider alternative hypothesis and disapprove them. Proving or disapproving is done through collecting specific data which supports the investigator's prediction. The reason there must be follow scientific procedures in extracting artifacts and building the hypothesis is that

investigator need a scientific base to verify and explain the results which reached. If there is no scientific reason to explain any procedure investigator have done, this will undermine the credibility of the forensic analysis and the evidence will be considered unreliable to be accepted in the court.

3.3 Digital Forensics Process Flow

Many process models have been proposed for digital investigation procedures and researchers have mainly focused on the nature and number of steps involved in the investigations process of cybercrimes. [44]

3.3.1 Kruse and Heiser Model [1]

The earliest known methodical approach employed to computer forensic. The first phase involves acquiring the data evidence. It is recommended that the data integrity should be ensured. The second step is to check the validity of the collected data by authentication process. The third phase is the analysis of data keeping intact the data integrity and validity. A generalized view of the framework is given in figure 3.2 below.

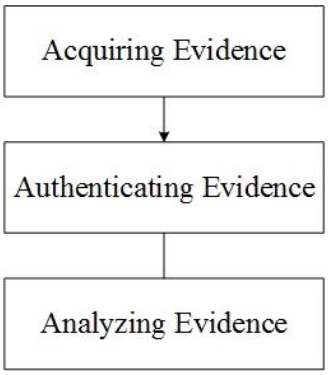

Figure 3.2 Kruse and Heiser model

3.3.2 US Department of Justice (USDOJ) Model [2]

This model is primarily based on the standard crime scene investigation protocol and comprises of four steps, the collection, examination, analysis, and reporting. The fourth step is reporting or presenting of evidence in the court of law. The simplest schematic workflow is shown in figure 3.3 below.

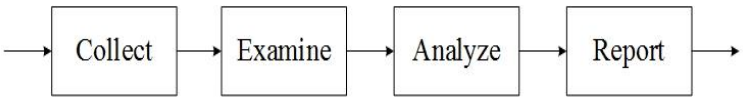

Figure 3.3 USDOJ model

3.4 NIST Forensics Investigation Process

NIST forensic process model includes the four phases: collection, examination, analysis and reporting. The relevant data are identified, labeled and record in the collection phases and collected data are accessed and extracted in examination phase. And then the results of the examination are analyzed to drive the useful information as shown in figure 3.4.

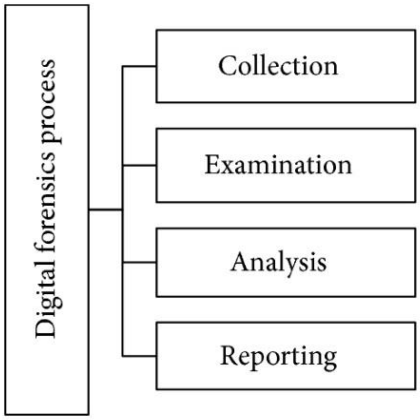

Figure 3.4 NIST Forensics Investigation Process

3.4.1 Collection

Much like everything in Information security, Forensic Investigations starts by "gathering data". As an investigator, a scenario where a machine which is supposed to hold the evidence searching for. That machine could either be a victim's machine, or a suspect's machine. That image would be a copy from everything on the machine's storage device. Data Acquisition is the process of taking an image from a machine. It is making a forensic copy of evidence, which could be any type of media (Hard disk drive, USB, CD/DVD, etc.). In order to avoid many an investigator should never conduct analysis on the actual physical machine. Instead, an investigator should always take an image of the machines they encounter during an investigation, so that they can analyze it later. That image would be a copy from everything on the machine's storage device.

Imagine a case where there are investigating a breach on a cooperate network server. It doesn't make sense to take the whole server back to the lab to look for evidence. Finally, with only one copy (which is the original machine) there is no way for multiple teams or investigators to work on the same case in parallel.

Imagine a case, an investigator (A) wants to analyze the machine's registry, while investigator (B) wants to analyze the machine's logs. That would be nearly impossible without data accusation. Before deeper into imaging, there is an important note to remember. The original image is usually verified then saved, alongside other parameters to protect it from tampering, while all the work is done on copies of the original image.

Figure 3.5 Data Volatility

Data volatility is defined as the rate or the likeliness for a change on a data set. In other words, how easy it is for a set of data stored on some medium to change. A change could either be alteration or destruction. For example, the data stored in the computer's RAM is more volatile than the one stored on that hard disk; a restart would erase the data stored in RAM unlike the data stored on the hard disk.

The investigator should always consider the order of volatility when acquiring data from a device. As mentioned in the previous example, the data within the machine's RAM has definitely a higher priority over the data stored on the machine's HDD because it is more volatile. The Storage mediums can be arranged from the most volatile to the least. The data is most volatile when stored in the CPU's registers. The values inside the CPU's registers changes with almost every assembly instruction. Data is least volatile when stored on a secondary storage device such as a HDD. Order should be taken into account when acquiring data from a device.

Data acquisition techniques and methods can be divided into Static Acquisition and Dynamic/Live Acquisition. Choosing which technique to apply depends on data volatility and the case. Static Acquisition is gathering nonvolatile data. In other words, gathering the data that remains intact after the system's reboots or goes down. Such

acquisition is usually performed on hard disks and Flash disks. Dynamic Acquisition is gathering volatile data usually while the device is still running. In this technique we are interested with the data that will get lost if the system goes down. It is usually preferred to start with live data acquisition since the risk of losing it is higher than the risk of losing the data stored on disks. It is also worth mentioning that sometimes it is possible to come across volatile data while conducting static data acquisition. This case is usually encountered when the investigator finds a Memory page that has been previously paged from the RAM over the hard disk.

There is also another type of acquisition usually referred to as Dead Acquisition refers to the attempt to acquire data from the suspect's machine without the operating system assistance. This is usually done with the help of the machine's hardware. The reason why there is a need for Dead Acquisition over the normal acquisition is that in many cases, the suspect's OS cannot be trusted. Some attackers may install tools (such as Rootkits) that manipulate the OS's behavior. In that case, the OS can't be trusted to be performing the tasks, it is asked to. [43]

3.4.1.1 Storage Formats

When taking an image file, one of the important things to take into consideration is the file format which the image file will be stored in. Depending on the tool used for reading, writing, and analyzing, the image format could vary. Raw Format is the simplest format to save an image. As the name suggests, the data is read from the source device's disk and written on a file. That image file can be mounted later and analyzed for evidences. Using raw format offers fast transfer rate, and since it is popular on most forensic tools, it gives the investigator the flexibility of moving between different frameworks and compare their outputs. One point worth mentioning is that raw format imaging tools neglect small errors on the source disk. It is also important for the investigator to prepare enough storage to save the images since the image file will take the same space of the target device driver's size.

3.4.1.2 Imaging and Copying

It is important to mention that imaging isn't copying. The major difference between imaging and copying is that: Imaging mirrors the device's entire storage on a file. Copying mirrors only the "useful" data from the source device. Copying, on the

other hand, mirrors only the "useful" data from the source device. For example, if 60% of the hard disk capacity is used and the rest 40% is rubbish (deleted files and random bytes), then imaging that disk will mirror both the bytes on both the used and the unused parts. Copying on the other hand would mirror only the used 60% part.

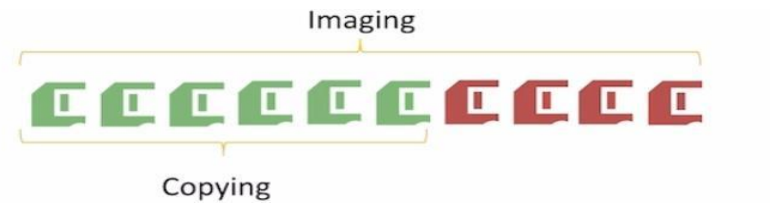

Figure 3.6 Imaging and Copying

Acquisition Issues as mentioned earlier, an investigator should not work on the original image/Dataset acquired. Instead, it should be preserved and copied. This should help in establishing the chain of custody and allow the investigator to make as many images as needed. However, there are some issues the investigator needs to take into consideration while copying an image:

- First, when copying, make sure that the copy is an exact replica of the original image.
- Make sure that the original source is safe from tampering.
- Otherwise, all the work done on the images will be rejected, since there will be no way to prove that the presented evidence is authentic.
- Make sure that the copying process will not alter the original image or corrupt parts of it.

There are two main approaches in which data acquisition could be performed, each with different output.

- The first way is from disk drive to image file (imaging)
- The second one is from disk drive to disk drive (cloning)

Disk drive to image (imaging), as the name suggests, mirrors the suspect's hard disk content into an image file. Imaging a drive creates what is called a "forensic image". The advantage of this method is scalability and efficiency. The investigator would be able to create as many images as needed and all the only thing needs is enough space to save the images. Creating a forensic image does not have to be for a full disk drive, the investigator might have a drive that has more than one partition. An example

is the system partition "C:". In this situation, it could only create a copy of this particular partition, also referred to as a forensic image.

Check the difference between imaging and cloning figure, to determine which need to do. There is also a special case of Disk Drive to Disk Drive acquisition. Sometimes the source disk isn't the whole physical disk but a partition from it. For example, if the machine has one HDD with two partitions (C:\ and D:\). If the investigator wants to image the D:\ partition only, then it is considered Logical Disk Drive to Disk Drive acquisition. One important piece of advice when dealing with evidence is to make copies of the forensic image and use a copy for work and investigation. Do not create only one and use it for investigation, the investigator never knows if a faulty tool might interact with the image and either corrupt it or even jeopardize evidence stored on it. A forensic image could be stored anywhere. The investigator can save it on the same disk (not recommended), on an external disk drive or even sent through the network to a network share. The flexibility of dealing with a forensic image is very high. Disk Drive to Disk Drive (clone) on the other hand, mirrors the suspect's hard disk content into another hard disk. The tools which supports that type of data acquisition usually rebuilds the second disk so it becomes exactly similar to the source disk, and that is why it is also called a "clone". Sparse Acquisition is when the investigator doesn't mirror all the disk content. Instead, the investigator will selectively forensic copy a list of defined folders and files. Also, the investigator could copy all the bytes residing within the unused (unallocated) parts of the HDD. Sparse acquisitions are extremely useful for cases where it cannot take the suspect's system offline or if the target of interest's HDD volume capacity is very big and might take hours to forensically image or clone the drive.

The investigator must either know what to select for acquisition and have a checklist, or, he will leave some evidence behind. So be careful when the investigator must go with this method. There is no one right method that works every time. Different cases have different circumstances, and with different circumstances, different methods are needed.

Using images is more efficient as one storage device with enough space could hold multiple images. However, sometimes, due to bugs or errors, it is not possible to produce a digital image of a hard disk. So using the Disk to Disk method is a much

better solution even though it takes a new physical hard disk for every data acquisition disk. Both Sparse Acquisition and Logical Disk to Disk imaging are good options when the time is limited. Sparse acquisition is usually faster than Logical Disk to Disk. However, if evidence resides on a file that isn't preconfigured into the tool's list, it won't be collected, unless the investigator specifies it manually. While Logical Disk to Disk will take more time (depending on the volume's size) it will mirror everything within that partition.]

3.4.1.3 Live Data Acquisition

Live Data acquisition is used to collect data while the machine is running. Usually an investigator looks for volatile data during live acquisition. Volatile data resides in a memory that can't hold the data after a reboot. Volatile data usually resides in RAM and cache. Volatile data isn't just more likely to be lost due to reboot. It is more susceptible to modification and alteration. This is because the process running on the machine uses the RAM and cache continually. Any move made on the machine will definitely have an impact on the device's RAM. Sometimes, volatile data is as important as it is fragile. As running processes use RAM, it is very likely to find stored passwords, messages, domain names and IP address belonging to those processes.

This could be very important in cases such as Malware analysis and hunting. Using an encryption key extracted from memory may allow the investigator to extract and decrypt the traffic going between Malware and its operator. It is worth mentioning that there might be volatile data stored on a non-volatile medium. Examples of such files are Temporary files and log files. Log files are frequently trimmed and rounded, and temporary files are often automatically deleted. In the remainder of this section, we'll look at some example of the data we collect during acquisition and some of the tools used. SYS Info is a generic term that describes Basic system information about the machine, the running OS, its configuration and the installed applications. It includes things such as, the OS version, build and product key. It also includes computer name, accounts, Manufacturer and specs (CPU model, RAM size etc.). OS configuration is also an important thing to collect.

Configurations such as:

- installed languages

- time zones
- uptime
- installed updates and hotfixes

These could help an investigator in uniquely identifying a machine or proving that two files came from the same origin. Knowing what processes were running at the time of the acquisition might be crucial for the investigation. It should help the investigator know what to look for when analyzing the RAM dump the investigator acquired (which is another important piece of information to acquire). Sometimes, most of the investigation's time is spent looking for and in Logs. Getting those details could help the investigator in building the incident's timeline. There is no main log to look through, as logs and logging are dependent on various applications and utilities. Logs could be Operating System event logs, specific process logs, login logs and network logs. Time Stamps also play a major role in crime reconstruction. In fact, there is a spate investigative process called "Timeline analysis" where the investigator analyzes time stamps and try to find a correlation between the events in the logs and time stamps. Networking configurations are also important, especially when there is a network attack. Details such like number of NICs and their modes, MAC and IP addresses, could also help the investigator during the investigation. Although it might be the only solution sometimes, memory forensics isn't an easy task. Unlike file systems, Operating Systems, and networking protocols, RAMs have no built-in mechanisms to help forensic investigators.

There are many cases where most methods of forensics investigation (File, OS, Network) fails to extract the required evidence for the case. In those situations, an investigator is only left with a few options. Full Disk Encryption, for example, is one case where memory forensic is the way to go. There are many security solutions which allow a user to encrypt hard disk's content making normal disk imaging useless. In these cases, the best option is to extract the key used for encryption from memory images. Another example of a situation where we may need memory forensics is when tracing malware, especially rootkits and advanced persistent threats. Those types of malware tend to hide their presence by erasing themselves and making almost no contact with the hard disk. They do most of their work at the RAM making it the best place to hunt for them. It could also find network packets' contents, Internet browsing

data, injected code (in case of malware and BOF attacks) and unpacked executables (packing is usually used to hide malware) in addition to processes data and clipboard's data.

All of which aren't obtainable through other means. An investigator could image the content of the RAM by using tools such as "Live Response." Many tools could Analyze that image and look for data. Different tools can be used to look for all sort of data (Emails Chat, etc.). Some tools are designed to identify and protect the evidence provider's personal data, such as credit card numbers and social security numbers. Many tools and utilities could be used to avoid some of the problems encountered while acquiring data. Sometimes it is possible to alter the original device state while acquiring data which could ruin the investigation because evidence has been tampered with.

3.4.1.4 Write Blockers

Write Blockers are devices that allow the investigator to perform data acquisition while eliminating the chance of damaging or altering the disk's content. Write Blockers works by blocking the hard disk from writing allowing for safe data acquisition procedure. This is done by filtering out the write commands and preventing it from being executed. Write blockers could either be hardware or software. Some write blockers extend the prevention to include a list of commands selected by the investigator. Common Write-blockers are

- WiebeTech® Forensic UltraDock from CRU Inc.
- Tableau Forensic Imager TD3 from Guidance Software

Figure 3.7 Write Blocker

Bootable Disks usually holds a self-contained fully functioning, bootable OS. This allows the investigator to launch an OS on the suspect's machine without touching and modifying the device's main disk. In many cases, the investigator will have an acquisition tool acquiring data and dumping it onto an external storage, typically a disk with a USB connection. The problem is that this disk contains the evidence might be altered by Windows when connected to it; this would damage the evidence's integrity. However, since they might not be available (since not all countries allow them), it can take advantage of a feature in the OS itself to block it from writing on the USB devices.

Microsoft introduced a USB-write blocking feature for the first time in Windows XP. It can be activated from the registry and it will prevent the write access on the USB devices preserving the evidence integrity. It enables the write protect on Windows 7 and later versions using the registry editor.

3.4.1.5 Validating Evidence

The most critical part, which could ruin any forensic investigation, is the evidence's integrity. If the integrity of the evidence cannot be validated, then it is useless. Validating evidence is usually performed through Hash Functions. Hash functions are One Way Cryptographic Functions which takes variable length input and produces fixed size output string. The resulting string is considered a fingerprint for the input. Any change no matter how small it is to the source file will result in totally different hash output.

Hash strings can be used to prove that the file has not been tampered with because any changes to the file will result in changing the hash value when re-computed. This is why hashes are used for validation. It is very important to note that the hash value should be saved securely. If an attacker gets their hands on the hash value and the disk, they can introduce whatever changes they want on the disk, recomputed the new hash for the malformed disk, and then save the new disk and the new hash adding false evidence to the investigation.

This would make the original image inconsistent with the copies that the investigators use for analysis. There are many hash functions in the industry today. Some of the hash function are SHA-1, SHA-2, SHA-3 and the old MD-5.

Windows Evidence Validation unlike Linux, Windows does not have a built-in hashing tool. This is why a third party application needs to be installed. It will create a text file and write the phrase "This is a test for hash" inside. And, it can open hashcalc and feed it the file after choosing the format and path. One good thing about Hashcalc, is that it calculates the fingerprint of the file using many different hash functions. An investigator will make a minor change to the file and recalculate the values. Just like the last time, the fingerprints have changed significantly.

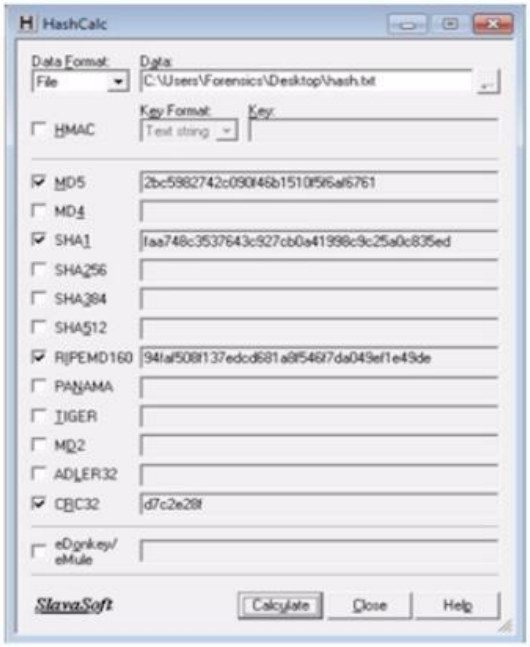

Figure 3.8 Different Hash Function on HashCalc

The investigator can depend on hashing to make sure our evidence has not been tampered or played with it. Every time the investigator acquire evidence, it needs to calculate the fingerprint (hash value) for the evidence and have it available with forensics evidence. This is what will prove the evidence is legit, and that it has been stored securely. After successfully and forensically obtaining evidence, the next step would be to either start the analysis or explore the evidence to get an idea of what is there. To do that, an investigator need to connect the evidence to analysis workstation so that it can use tools for investigation. Evidence could be stored in a forensic image, or maybe by duplicating the drive. Depending on the type of evidence, it will require different ways to connect them to workstation. Also, evidence might be using a different filesystem, so it will need a way to connect this alien filesystem to

workstation's filesystem. There is a mounting the evidence, just like when it attaches a USB thumb drive to PC/Laptop, but with one major difference, it will be mounting the image in Read-Only mode.

One of the most critical aspects in digital forensics is time. When acquiring evidence, it is very important that record the day and time of acquisition, especially time zone information. This should be done for every single event when evidence is acquired. Time is a critical factor of any crime, regardless if this is a digital crime or not. Do not want to be pointing fingers at an innocent person that was not even present at the time or did not even access the media on that specific time or day. Writing down the time for every single evidence could even help the investigator if any evidence integrity breach was discovered. Within the file, usually, those stamps would be in hexadecimal notation. And it is up to the analysis tool's responsibility to interpreter those hexadecimal characters to a human-readable form. Unfortunately, sometimes the tool's time interpretation abilities might not be reliable and may lead to providing an incorrect date and time. This arises, especially when dealing with different evidence programs, with each storing time differently. Failing to identify time correctly could lead to a big problem. One great tool out there that handles time issues properly is Dcode. Dcode is a tool which can convert the timestamps from various time formats to more human readable.

3.4.2 Examination

Appearances are often deceiving. A digital investigator is not to be deceived by the file evidence. For example, a PNG file might contain a hidden zip file. Even a JPEG can masquerade itself by changing the extension into DOC. The blocks used to build a file (i.e., bits and bytes) and different ways a computer can represent them. Humans have 10 fingers, which is the reason why it uses a Decimal counting system that consists of 10 digits (0-9). Computers, on the other hand, use a different system called Binary system which has only two values (0-1). The reason for using this system has nothing to do with the number of fingers. Computers are electrical machines, they do not have fingers, but they can recognize two states. The presence of an electrical current (symbolized as 1) and the absence of the electrical current (symbolized as O). The smallest unit in the binary system is a bit, which could take either the value 0 or 1. The next unit is Byte (B), which equals 8 bits. A Kilobyte (KB) is 1024 byte, where a

Megabyte (MB) is 1024 Kilobyte. A Gigabyte (GB) consists of 1024 megabyte, and a Terabyte (TB) is 1024 Gigabyte. Nowadays, most personal computers storage disks are between 500 (GB) up to 2 (TB) for gaming and business laptops.

Hexadecimal is another format used to express data and numbers. Decimal has 10 numbers (0-9), while binary has 2 numbers (0-1). The hex system has (16) symbols. ASCII is a system used by computers to represent characters and symbols in a numerical form. Each symbol is given a number/code. Some tools translate ASCII code to characters directly when dealing with file analysis or network traffic. The first step to identify a specific file type is its extension, like PDF and DOC. Identifying the file type by its extension is a common technique in Windows operating system. For example, .PDF files are opened by Adobe reader in windows. If a JPEG file extension changed to .PDF, the file will not be opened on windows. The reason is that windows will try to open the file using Adobe reader which cannot read the JPEG file contents. Another thing to note is that for each file type there should be a reader that knows how to read its contents. It is easy to change the file extension using file rename. This tells us that searching for JPEG files might not reveal all JPEG files if their extension has been changed. Not all operating systems rely on file extension to identify the file type. Linux rely on file signature to determine its type.

The next step is to identify the file type is by its structure. Regardless of the operating system, every file has a specific structure to arrange its components; those components are file name, size, signature, contents, etc. The files structure is universal and the same for any operating system. In order to open a specific file, the operating system will use a specific reader; this reader knows where to find the file name or size within the different file components. Files regularly have several readers. For example, PDF files could be viewed by Adobe Reader or Foxit Reader.

3.4.2.1 Metadata

Metadata in general is defined as "Data describing other data". To understand this term, let's use mailing a letter as an example. When people want to send a letter through mail, they write the letter down on a piece of paper, then put it in an envelope. And on that envelope, they write things such as the Sender's address, receiver's address, date, etc. The things we wrote on the envelope is the best example for Metadata. The sender's and receiver's address are not part of the original letter we're sending. They are Metadata. Data that is used to describe the original data they are sending as the letter.

So, file metadata is the data that describes the file itself and is used by the OS' applications to make opening, recognizing, and processing that file easier. Metadata can be found in many places and forms within the files. For example, metadata may be found in the file or somewhere else (another file). It may take the form of binary string or text (e.g. ASCII) string.

Metadata is found in different locations, but as a starting point, the three locations need to start looking for metadata when analyzing a file are MFT records, File header, Magic number. MFT stands for Master File Table and is used by the NTFS file system to store metadata which is necessary to retrieve files from the NTFS partitions. Each file has one or more MFT record.

- Standard Information - Store info regarding access mode (read-only, read/write, etc) timestamp, and link count
- Attribute List - Location of other attributes that were not able to fit in a single entry
- File Name - Stores file names. There will be more than one if a long file name or POSIX file name is used
- Data - Stores file data. NTFS allows a single file to have more than one $DATA attribute
- Object ID - A unique file identifier across the whole volume
- Reparse Point - Mounting drives
- Index Root - Implementation of directories and other indexes
- Index Allocation - Implement B-tree structure for large directories and large indexes
- Bitmap - Represent the status of an entity
- Volume Information - Only found in Volume system file, and includes volume version
- Volume Name - Contains the name of the volume
- Security Descriptor - Store file security information (e.g. Access Control Lists)

The data itself is an attribute. MFT records can be used when searching for files within the file system. It is also worth mentioning that those records could be used as an evidence to prove the existence of lost or deleted files. Normally, MFT records are

not visible to the users through Windows Explorer. This is why it needs to use file system examining tool in order to be able to view those records. Directory Snoop is a great tool to perform the required task. It allows the examination for both NTFS and FAT32 disks on a low level, allowing the investigator to examine the MFT records and other system related files. Another great tool for NTFS attribute examination is DiskExplorer for NTFS from Runtime Software.

3.4.2.2 File Headers

As the name suggests, file header is a unique identification section found at the beginning/head of every file. The header usually contains data used by the application that opens the file. The header could contain things like name, author, date of creation, size, or data that helps performing error detection and correction before opening the file. Different files have different headers. It is important to remember that some headers are known standards and others are preparatory. It is also worth mentioning that some files don't have a header at all. The header is usually checked by the reader application before opening the file. This is why Adobe Reader, for example, could recognize a damaged PDF file right after opening it. A final note worth mentioning is that most file formats have a header and a trailer. A header is usually found at the beginning of the file, while a trailer is usually found at the end of the file. It is also common to have additional sections, e.g., PDF files have a section called "XREF" in addition to the header and trailer. Headers and trailers can be checked using any hex editor.

Magic number is another method used by applications (mostly Unix/Linux) to try and ID the file without the need for reading the whole header. A magic number is a unique string, usually at the beginning of the file, which can be used to identify the type of the file. In Linux, the File command can be used to identify the type of the file. A list of magic numbers can also be found on most linux systems in: /usr/share/file/magic

In general, Metadata is data that is used to describe other files of data. However, metadata files which are relevant to forensic investigations and can be categorized into three main type are System metadata, Substantive metadata, Embedded metadata and External Metadata. System metadata files are usually generated by the file system. Substantive metadata contains information on the modifications over a document. Embedded metadata is usually embedded by applications that edit or create files within

the file itself. External metadata is normally created separately by file management software to keep track of the managed files.

System metadata are created, edited and used by the Operating system of many purposes. The Operating system file system is one of the main components that heavily relies on metadata to keep track of the files it manages. It is worth mentioning that system metadata files aren't just used to manage hard disks. Other drivers such as Disk Drives (CD, DVD) and removable devices (Flash disks and external Hard disks) also rely on the use of system metadata. Storage devices in general (fixed and removable) use system metadata to track the addresses of the contained files and how they are stored. From an investigation perspective, the system metadata can be used, as mentioned before, to track a file that doesn't exist anymore (removed, deleted, moved). System metadata files can also help construct a timeline for the events that occurred on that file. It is worth mentioning that system metadata files wouldn't help in retrieving the content of the file.

When conducting an investigation, there are mainly interested in 4 attributes within the metadata. The create, accessed and modified entries are usually referred to as MAC. Additionally, NTFS disks add another entry called entry modified. Create Metadata usually describes when the file was first created. It is important that the date find does not always indicate the date which the data was originally created at.

3.4.2.3 Document Management System

Document management systems are systems used to log, manage and organize the storage of digital documents. Microsoft usually keeps track of stored documents and users who own, modified and/or viewed those documents. OpenKM is an example of such systems. It can manage and organize various types of files through a web interface. Document management systems tends to create many metadata records and files to help keep track and manage the stored files. Encountering a MS within the investigated environment is both good and bad news. DMS metadata are usually a rich source of information since they are used by the DMS itself to work. However, the investigator needs to understand how and where the DMS stores its metadata before they are able to extract or analyze information from it. It is always recommended to go through the DMS documentation before gathering data. Some features and techniques

are common among most systems. However, it is not unlikely to encounter a product specific feature, formant or functionality.

Many applications and software embeds metadata within the files they produce. These embedded metadata can be very useful in many cases. Some of those metadata can be examined by just viewing the properties of the file. Each file type or software may have its own embedded metadata. For example, when taking an image with a mobile camera, the camera drivers embeds metadata within the JPEG image. Metadata such as the phone's brand, model and the camera's configuration when the picture was taken. The knowledge of product related metadata is also essential in any investigation. Not just for collecting evidence but also working on anti-exfiltration cases. Since different applications have different metadata fields within the file, it is possible to face a data thief who is trying to hide stolen data within a file's metadata for later view. Even though there are easily editable, metadata may contain many keys to solve cases when knowing what and where to look for. Information such as usernames, computer names, previous versions of the same documents, etc.

Temporary files are normally created and used by an application or an OS for a short period of time. When an application or system is running, it creates file with intent of removing them later once the applications exit. Different applications create temp files for different reasons. For example, text editing applications creates temp files to track and handle the users' edits on spot and allow to recover older versions of the same document. The OS itself creates temporary files for many reasons. For example, when an application is not being used within the RAM and the space is needed, the OS dumps the unused process non-essential data from the RAM to a temporary file on the hard disk. This file is removed and the content is resorted to the ram later. This process is known as swapping.

Basic OS utilities such as internet browsers also create temp files and data in what is known as cashing. Browsers tend to save parts and objects from the most recently visited pages to make loading them easier the next time. Different applications create different temp files for different reasons at various places. It is not possible to list all the types and purposes of all temp files. It is necessary to read about the temp file creation and management for the applications encountered during an investigation. It is also worth mentioning that even though temporary files are, as the name suggest,

not supposed to exist for long period of time. There are scenarios where this isn't the cases. The most common issue that allows a temp file to exist as permeant file is Crashes. When an application or an OS crashes, it will not terminate in the standard way which includes deleting temp files. This would leave a previously created temp file on the hard disk. Sometimes, temp files are useful source of information containing metadata and/or previous or unencrypted versions for the document. It is also important to remember that temp files are just like any other files. When they are removed, they can still be recovered and examined, assuming the space they were at on the hard disk was not overwritten by another application. This is why deleted files recovery is an important step when looking for evidences.

3.4.2.4 Data Hiding Locations

Forensics procedures are all about finding what/who does not want to be found. Depending on the level of the suspect, locating valuable evidence or sensitive data may sometimes only requires examining a few logs and few metadata entries. In other cases, however, when facing an experienced suspect, one has to be creative and look at places that are not normally used to store data. There is no full list for every "non-usual" place where data could hide. It is a cat and mouse game that depends on the underlying system and the creativity of the user. Those places are: Metadata, Windows registry and ADS. The best way to think about Windows Registry is to think of it as a big directory containing many configuration files. Those configurations files are used by the OS and the applications on it to store configurations related to how the application behave. For example, in order to know what programs should be launched and executed at startup, Windows keeps a record of those applications in the:

HKLM\ software\ microsoft\ windows\ currentversion\ run

Registry is usually organized into directories which are called Keys, each key contains Values. Each value has a data within. The registry values and their corresponding data can be viewed, edited or created using many tools. Regedit is the most common tool used by sysadmins to do so. The tool comes pre-installed on Windows Machines. The Registry has a fairly complicated structure. Adding a new key with a value deep within the registry tree could easily go unnoticed for an inexperienced eye. It is important to remember that the concept of the registry is present in Windows

platform only. Unix/Linux systems don't implement or have the concept of a registry. Instead, in Linux everything is a file. Most the configuration files are stored in the /etc directory. Another interesting place to hide data is in the documents' metadata itself. The process of finding data hidden with a document's metadata sounds easy when the investigator knows where to look. However, on a machine or within a Document management solution, which may contain thousands of files of different types and format, things become less convenient.

The Windows file search tool could be used to look for data within a document's metadata, since it searches for the supplied string within the content and the document's metadata. The Strings tool could also be used to dump strings from a file. The string tool will be explained later within the PE file analysis. Using the Alternative Data Stream is another place where data could be hidden. It is important to note though, that this feature is only present in the NTFS filesystems.

The Alternative Data Stream is a feature the NTFS introduced to allow for compatibility with Macintosh file systems. The ADS allows a user (malicious or normal) to store data within a file without affecting its size or view. This could be exploited to hide data within a file where it’s hard to notice. The ADS for a file could be accessed using the: character. After creating the file.txt, open the hidden.txt file within its ADS. After writing on the hidden file, and leaving the original file empty. It can notice that the original file's size remained zero despite the text that is written within hidden.txt. There are many tools which can inspect a file's ADS, such as Streams.exe from Sysinternals and ADS Detector. One effective technique to neutralize the data exfiltration through ADS threat is to move the suspicious file to a FAT32 partition. Since FAT32 systems don't support ADS, the data hidden within the ADS will be gone. There are more advanced techniques usually used with data exfiltration attacks such as Steganography and Network Protocols covert channels.

3.4.3 Analysis

Digital/Electronic evidence is extremely volatile. Once the evidence is contaminated it cannot be de-contaminated. Chain of Custody is crucial. The courts acceptance is based on the best evidence principle. With computer data, printouts or other output readable by sight, and bit stream copies adhere to this principle. With all

of this information, forensicates can then provide a “What” the file is, “Where” the file resides, “Why” it could be residing there, “How” it got on the device and most importantly narrow the “Who” put it there.

3.4.3.1 Microsoft Word Analysis

DOCX is the extension and format used by Microsoft word 2007 and later editions. Microsoft Word 2003 and earlier versions used another format called DOC. The old DOC files were binary files used by oldest Microsoft Office product. Each file type (doc, ppt, xls) had its own format structure and content. It is also worth mentioning that those formats used to change from one Microsoft version to another. It is common to hear the term OLE used to refer to these types of files. A DOC file consists of many sections such as Mainstream, which contains the files main data with a header containing information about the document and pointers to other elements within the document. This header is also known as File Information Block. The summary section contains the summary for the document, and a table stream contains the objects pointed to by the File Information Block in the main stream header. Starting from Microsoft Office 2007, Microsoft started using the office open XML format. Moving to an open xml-based file format made the process of decomposing and parsing the file much easier. In the older binary versions of Microsoft Office files, each format required a pacific parser.

Another advantage of the Open xml-based file format is that they are less susceptible to exploitation by attackers than the older binary files. On the low level, DOCX files are compressed files which contains XML files and binary files. It can verify that by opening any DOCX file in WinZip or WinRAR. A DOCX file starts with 50 4B 03 04 14 00 06 00 08 00 00 00 21. The trailer, or the last section of the file, usually starts with docProps/app.xml string. The DOCX metadata are usually found in the docProps file within the compressed document in the form of XML files. The folder contains two files are Core and app. The core files contain fields that are used to describe the origin of the document. Fields such as the author's name, the last editor and the creating and editing dates. The other file, app.xml usually contains data describing the content within the document. The file describes the number of words, characters, lines and the application which was used to create the document. Just like any other software, Microsoft Office could also be used to deliver malicious payloads

to the victims' machine. This could either be done by embedding a macro script and malicious macro script within the Microsoft Office file or by creating a specially crafted file which exploits a certain vulnerability in one of Microsoft Office Products.

3.4.3.2 JPEG Analysis

JPEG stands for Joint Photographic Experts Group. A lossy compression method is used to for images especially photos that were taken by camera. As like many other formats, JPEG has also a pre-defined file structure. A header, metadata and a footer. JPEG files can be found under many extensions such as "ipg, jpg, jpe and tiff". Sometimes the terms JFIF, TIFF, EXIF and JPEG are used interchangeably. It is important to distinguish and note that the JFIF, TIFF and EXIF are different file formats compressed and encoded using the same algorithm which is JPEG. A JPEG file usually: Starts with FF D8 bytes. Consists of section and the value FF is typically used as a delimiter to indicate the start of a new section. In many cases (not always though) the FF D8 at the beginning of the image is followed by FF E0 (in some cases FF E1). Within the file header, there are many interesting information that an investigator may find. Information such as software signature, date, camera and OS details, etc. In this example, it can see the FF D8 FF E0 signature at the beginning of the file. The file is a JFIF file. But the most interesting part is the Photoshop signature. This tells as that this photo has been produced by Photoshop. The JPEG files usually ends with the FF D9 string. It is also important to note that those fields are editable using any hex editor. This should always be kept in mind when analyzing a file.

3.4.3.3 PDF Analysis

The Header within the PDF contains the version of the used PDF. In this example, we have PDF 1.4 between two comment symbols % %. The non-printable ASCII values are typically used to tell the application to expect a binary data not just text. The Body of the PDF file contains the data (strings, image, flash, etc.). Different types of data are usually referred to as objects. The body is what is usually displayed to the user by the reader. It's important to note that objects can also work as references to other objects. Those object pointers are usually defined by an object identifier and the generator number. An object body is usually contained between obi and endobi keywords. A series of objects belonging to the same entity are usually called streams.

Streams are typically used to represent large data types such as images, flashes and videos. A stream is usually defined by the stream and endstream keywords. For optimization purposes, streams are usually compressed in order to take less space on disk. This should be kept in mind when analyzing a file since it may take extra effort during the process.

Streams and objects are not the only things an investigator should look for when analyzing a PDF file. There are other keywords, its existence indicates the presents of an interesting content within the PDF. Keywords such as action, URI, JavaScript, etc. should be looked for closely within a file since they could greatly help the analyst in the examination process. The JavaScript, RichMedia and JS keywords indicate that there is a JavaScript code embedded within the PDF file. Action, OpenAction, Named, Launch and macroform also important keywords to look for. Most of the time they indicate the existence of an action which must be taken executed upon opening the document. Actions and JavaScript content work hand-in-hand in exploiting and delivering malicious content within a PDF file. JavaScript objects may be used to deliver shell codes and other malicious payloads to the victim machine. Actions on the other hand can be used to perform an action on the victim's machine, such as opening a port and establishing a listener behind it. Another approach would be to use the URI in order to connect to malicious remote devices containing malicious content. The encrypt keyword indicates that there is an encrypted content within the PDF file. Actions and JavaScript content work hand-in-hand in exploiting and delivering malicious content within a PDF file.

JavaScript objects may be used to deliver shell codes and other malicious payloads to the victim machine. Actions on the other hand can be used to perform an action on the victim's machine, such as opening a port and establishing a listener behind it. The trailer is the last section of the file. It always begins with the word trailer and ends with the %EOF string. The content of the trailer is contained within the <<>> signs. The Size field, indicates the number of entries within the reference table. It is also possible to find other important stuff such as Author and creation date, which can usually be found after the Author Tag. In this example, the document author's name is FOR and the document was created using Microsoft office.

<</Author(FOR)/Creator(..M.i.c.r.o.s.o.f.t/creationDate(O:201707250845[8+03:00°;r -d.•2.0.1.3)

/ModDate(D:20170725084518+03'00')/Producer(...M.i.c.r.o.s.o.f.t...W.o.r.d. .2.0.1.3) >>

It is worth mentioning that those fields could also be editable using any hex editor. An investigator should keep that in mind when analyzing a document. It is important to remember that some PDF readers allows the user to examine those fields directly. In Acrobat Reader for example, the Document Properties option allows the reader to examine the fields mentioned earlier.

3.4.3.4 EXE Analysis

As puzzling as that may sound, EXE files are just another type of file which could analyze and extract data from. It may sound strange at first, because there are used to "viewing files" (text, DOCX and PDFs) not "executing" them. EXEs (and executables in general) are files which contains instructions to be executed. Think of an executable file as a text file that contains instructions which the processor reads and executes. It is worth mentioning though that executable files formats differs based on the operating system. In the Windows Environment, executable files are usually called Portable Executables (or simply EXE). On Linux systems, executables are called ELF (Executable Linkable Format) or Binary files.

EXE files are usually produced by compilers. That is, write the code on a file in programing language (C, C++, CH or JAVA), then Compiles the exe. The compiler takes the original code and translates it to machine code which the processor understands. The compiler will also add a header to the code before putting them together in the final EXE. Each executable has its own pre-defined format. As the case with most file types, an executable file also has a header containing very useful metadata from an Investigative perspective. Usually, executable analysis is mostly encountered when analyzing a suspicious file. The executable's content and metadata, if understood, provides great insight on the behavior and purpose of the analyzed exe. In some cases, it may also aid in proving or disapproving the origin of the executable.

Investigators can analyze a malicious EXE looking for signs or patterns which could help link the analyzed EXE to other well- known incidents, attacks or

organizations. For example, with the late Wannacry Ransomware attacks, many analysts analyzed the malware looking for signs that may link the malware to other attacks which were known to have been conducted by the cyber warfare divisions of other countries (. e.g. North Korea). EXE files (or Portable executable files) have headers, but their content also is divided and arranged into sections. Sections are as important as the headers when it comes to forensics investigations.

Exports functions within that executable which other executables can call. To understand the purpose of that field and the next one, Imports. PE files contains code which the CPU reads and execute. One important note to keep in mind is that PE files don't come in exe extension only. DLL files are also PE files containing code. The only difference between the two is that DLL files can't be executed by double clicking on them. When someone is building an application, it doesn't have to write all the code from scratch. A programmer can take a code built by others and "link" it to own code. Linking is different than copy/pasting the code. Linking allows the programmer to call another code and get to execute within application. This process is also called Importing. The EXE files Imports code from another file (DLL file). In short, think of a DLL file as repository that contains data which any exe can import. The process of allowing other programs to import and run a code from a .DLL file is called exporting. In most cases, the exe file will be importing code from a DLL file which is exporting the code to other EXEs. Code within the DLL file is usually separated into segments which are typically called Functions.

When an EXE wants to import a code from a DLL file, it doesn't have to link the whole DLL file into the EXE code. It can ask the DLL to export a function by its name which makes the linking process more efficient. Even though the code within a .DLL file can't be executed by double clicking on it, importing isn't the only way to run the code within a .DLL file. In the Windows environment, there is a System EXE file called rundil32 which takes a DLL file name and a function name and executes them. An investigator could file the names of the functions that PE imports from other DLLs or exports to other EXE. It can view the functions linked to the PE using a tool called Dependency Walker. The tools allow us to view the imported DLLs within the PE and the functions that the PE imports from each DLL. One useful feature of the tool, is that

clicking on any function from the boxes will open a search page using the MSDN website.

For a malware analyst, knowing what each DLL contains and the general purpose for the functions contained within Windows DLLs is an important skill. For example, finding that an offline game that does not need online access imports WSOCK32.DLL file, which contains the functions needed to create and manage sockets, would be a suspicious sign. Another field which could be found within the PE header is Time Stamp. It indicates when the program was first compiled. It is worth mentioning though that some compilers always add a fixed time. For example, some Delphi compilers will always add 1997 as the date of creation.

Malware authors manipulate the time stamp field in order to make things harder for the investigators and malware analysts. The Sections field contains the names of the section and their size on disk and within memory. The Subsystem field tells whether this is a PE GUI application or a command line application. The Resources field contains the "resources" which the PE uses, such as Strings, Icons, Menu, etc. Unlike other formats where the file has a header and a one block body, P files' body is divided into segments. Each segment holds a different type of data and/or code. The segments are text, data, data, rsrc, reloc. The text segment holds the PE executable code. It is where the CPU reads the instruction from and executes. When reverse engineering an application, this is the most interesting segment to look at. The next section is the data section, which holds information about the imported and exported code. It may encounter a case where the import and export information are stored separately.

The import information would be stored in idata section, and the export information would be stored in the data section. The rsrc section includes external resources that are used by the PE. Resources including are icons, strings, menus etc. This section is where most of the work happens when translating an application or adding another language to it. In some x64 bit applications, there is a pdata section which contains the exception handling information. Analyzing a PE file is little bit more complicated than analyzing a normal document or image, since the PE was meant to be executed not read. In theory, it is possible to analyze an EXE file using a hex editor like a normal document. Due to the complexity of the PE files, it would not be

efficient to rely on hex editors only. There are other tools and methods which it can use to analyze a PE file.

In general, there are two main techniques Static Analysis and Dynamic Analysis. Static analysis involves analyzing the EXE without running it. This includes analyzing the PE header (Basic Static analysis) or reverse engineer the content/code of the EXE and view the assembly code or the CPU language (Advanced Static Analysis). Dynamic Analysis is another method to analyze a PE file. This method involves either running the PE within a contained environment (Virtual Machines) and monitor its behavior using some tool (Basic Analysis) or running the PE code step by step within a debugger and monitor its behavior (Advanced Analysis). When analyzing a suspicious PE, the easiest step Is to scan it using antivirus engines sites such as https://www.virustotal.com/. Such sites will run multiple antivirus instances over the file and provide a feedback. PEview is a great tool to view the PE header and sections within the PE file in a convenient way. It is important to note that some sections and headers within the PE file are legacy and not used anymore.

The IMAGE DOS_HEADER and MS-DOS Stub Program are two examples of such fields. The IMAGE_FILE_HEADER entry contains information about the PE itself. The machine field indicates the architecture of the machine which this binary was compiled on. The Number of Section indicates the number of sections within the PE. This field is necessary since there are optional sections which may or may not be present within the file. The Time Date Stamp tells when this PE was first compiled. Assuming the date there is correct, this field could be quite useful when investigation a malware attack. Since it could allow to determine how long the attack has been going. The problem with the time stamp is that malware authors tend to put a fake value when writing a malware. This must be kept in mind if a strange date was found.

The IMAGE OPTIONAL HEADER also contains several useful pieces of information. The subsystem, as mentioned earlier, tells whether this is a GUI or a CMD application.

00000144 0002 Subsystem IMAGE_SUBSYSTEM_WINDOWS_GUI

In example, it can see that it is a GUI application. The IMAGE SECTION HEADER describes the various sections within the EXE. The data contained within

these fields mostly describes those sections in terms of Memory location. The Virtual Size describes how much space the section needs when the PE is loaded into memory. The RAW DATA section describes the space needed on the main disk. Normally, the two values should be equal or very close. Finding a large difference between the two sizes may suggest that the code has been packed, especially if the size of the text section in memory is much larger than the size on disk.

3.4.4 Reporting

As much as it is painful to admit (and to write), reporting is arguably the most important part in most security-related work. This is because security is usually a non-functional feature for most project. That makes the report the only deliverable a security expert can give at the end of investigation. No matter how brilliant the technical work was, it will all go for nothing if it is not associated with a well-written report that explains the work done. That means that the report is sometimes the only thing that will judge the quality of investigation. Remember that report may be used to prove someone's innocence or guilt. It may also be the reason why suspect person will keep hiring or not. If investigator familiar with penetration testing remember that, as important as it is, there is no one way to write the report. Investigator will often encounter different formats and templates depending on the organization's type and needs. Instead, it will explain the sections that investigator will likely encounter in any forensic the report. Investigator may find useful when writing the report. Before there will be dive deeper into the different sections of forensic investigator be including the report may be useful just a few tips that should be kept in mind regardless of what format choose to write report in.

3.4.4.1 The Importance of Reporting

First thing to remember, TIME, TIME and TIME. Time management is the key to success in anything. As much as it is tempting to spend all time tackling technical challenges, other parts of the investigation are equally important. That includes the report writing, organizing, filling official paper and even attending court sessions and providing testimonies. If there will be added any references to the report, make sure they are updated and easy to find. Do not just copy-paste from bookmark or older the reports. Also make sure that the facts that the assumptions which investigator is trying

to support are valid and up-to-date. For example, the phrases "There are no known remote exploits on Windows 7 operating systems" would have been true in any report before 2017. Since a vulnerability that allows remote code execution was discovered in Windows 7 earlier this year. The second thing an investigator must take into consideration is to realize that reporting is not a separate stage which should be addressed after the investigation is done.

One thing that an investigator must NOT do, is to finish all the acquisition and Analysis and then reverse engineer work in order to write the report. Back tracking work for reporting may cause many mistakes that might compromise the whole investigation. As hard as this may be sometimes, reporting and documents must accompany each stage of the investigation. The report must start as the investigation starts and gets updated as the investigation progresses. With the known unpopularity of the reporting and documentation process, some investigators tend to make the report as short as possible by limiting it to a simple listing of evidence. Without the proper analysis and reasoning an evidence is nothing but a meaningless piece of data. It's the investigators analysis and reasoning what gives the evidence its value. Make sure to include the analysis as a separate section in report. A side note that must also be taken into consideration when writing the report is to try to stay away from using absolute terms.

The analysis is the investigators interpretation of the evidences and not an absolute truth. So, it is better to stay away from phrases like "we are sure" or "we are certain" in the analysis. Whether investigator is working as a freelancer consultant or working as a part of big firms' blue team, it is crucial to have a well define template for reports. Having a predefined well-studied make the communication consistent and easier between different organizational units or different team members. The final and arguably the most important thing to remember is to clearly separate the report into well-defined sections. Even though report contains a narrative part, yet investigator is not writing a novel. The report must be organized in a way that makes it easier for someone to find what is looking for directly without the need to read the whole report.

3.4.4.2 A Report Writing

When writing a report, there are describing events that happened in the past. It is common to use the past tense when writing the report. Also, remember to avoid using exhaustively long phrases. Filling the report with phrases 25-30 words long will make reading the report a nightmare for the reader. It distracts the reader and makes focusing harder. Remember to read the report to check and re-write such phrases if they exist. Although there is not usually a dedicated section for it, remember to write down what investigator have not done, as it is important as documenting what investigator have done. Make sure to mention the reasons, especially if they are technical, that prevented investigator from doing what could not do.

Avoid using Jargons. Jargon is like a type of shorthand between members of a particular group of people, often words that are meaningless outside of a certain context. Again, that not all the readers have an IT or Forensics background.

Avoid inconsistency when writing. Do not use different terms to describe the same thing in the report. For example, terms like Public Key Algorithm and Asymmetric algorithms are usually used interchangeably. If there is use one of them, stick with it throughout the whole report. In addition to consistency in terms used, make sure that format is also consistent. Things like fonts, colors and spacing are expected to be consistent throughout the report. The date and time format is another thing that it should keep consistent in the report. That includes dates written on the report and the dates produced by the tools used. Using MM.DD.YYYY and DD.MM.YYYY formats in the same report may create lot of confusion for the reader.

For archiving purposes, it is a good idea to start a report with a cover page or a title page. The title page can include things like the cases serial number, the name of the client or any other information that may help identify that report. It is also recommended to add a table of content at the beginning of the report to make searching within the report easier. That way, a reader will not have to go through the whole report when looking for a certain section.

The first part of the body report is the executive summary. Writing this part is the most difficult, but the important task of the documentation process. The importance of this part comes from the fact that this part is what a senior nontechnical manager

will look at when they want to make a decision. The executive summary must contain an overall high-level description of the case and the most important findings. The objective section, which usually comes after the executive summary, includes the client requests or the reasons behind the investigation and the goals that were in mind when it started. The evidences section should include an exhaustive list of the evidences found including:

- their serial number
- their hash value
- the name or the ID of the investigator who first acquired them alongside other chain of custody related information.

After the evidences are listed, it makes sense to talk about the analysis conducted on each of those evidences next. This is where the technical talk comes in. The section should include the tools the investigator used to perform his analysis. It is crucial to make this section clear and consistent. Otherwise, the report may be refused in court. After the evidences are analyzed, the investigator should describe their own reconstruction of the crime. That includes listing events in the sequence which the investigator think they occurred. Finally, the investigators should summarize their work in a conclusion section where they list and summarize the most important parts of the report. Just like how there are things that are expected to be found in any forensic report, there are other sections that are closely associated with the type of working environment or client. For example, when working for a law enforcement agency investigator should expect to find additional fields related to the chain of custody and evidence handling. Additionally, some reports include parts related to the incident in general such as:

- first responders list
- first responders' testimonies
- crime scene description

The First responders' list mentions the names of people who first noticed and reported the incident. It is a common practice to arrange the names by the time of the arrival to the crime scene. Additionally, the report may include a 2-3 lines section that documents the responder's first impression about the crime scene. Some reports add a

section for the main witnesses in the report. That section, much like the first responders, includes a brief information on the witnesses related to the case and a short testimony. The references section should include references to all external resources used in the report. Remember to check what kind of resources are accepted as a reference at the company/court/client presenting the report. For example, a court may not accept an anonymous web blog if there is cite it as a reference for one of claims. Also, make sure to add a list of tables and figures to the report. This will make examining and searching for certain information within the report much easier for the reader.

At the end of report, investigator should add a section that explains all the acronyms and technical terms that it used in the report. This is to help the reader avoid looking up every acronym they come across. Sometimes it need to support the report with large files such as witnesses' testimonies and log files. Since it does not make sense to include them in the report body, there are usually added as appendices.

The forensic reports main goal is to help decision makers making the decisions. The quality of a forensics report can be measured by the level of help it provided for the decision makers. A report that lacks one of the elements mentioned earlier would definitely fail to contribute to the decision making process. Another factor that makes a good forensics report is to be presentable for all people involved in the investigation. Ideally, investigator wouldn't want to write a different report for every group that is involved in the investigation. Imagine the time and effort needed to write 3-4 different versions of the report. If there is need to write multiple versions of the report for the clients (i.e., report for the Management Dept. and another for the IT Dept.), then there is probably something wrong.

A good report should include everything anyone involved in the investigation might need. Another sign of a good report is the percentage of supported claims vs hunches or assumptions. Ideally, every claim in the report has to be supported by an evidence. The less assumptions have the more reliable the report is in a court. A good report must be understandable by readers from different backgrounds. This is why it is recommended to use figures, pictures, charts and even statistics to make the understanding of what there are writing easier.

3.5 Chapter Summary

This chapter describes the background theory of cyber forensics investigation and the process flow. The chapter begins with a discussion of the cybercrime, followed by the attacks and techniques for Cybercrime Offensive and the threats of cyberspace. The chapter then continues with descriptions of the cybercrime forensics which includes Digital Evidence, Digital Forensics Tools and Scientific Method. Next, the discussion centers on digital forensics process flow, focusing on the digital evidence life cycle includes three main phases as acquisition, analysis and presentation. Finally, the NIST process model with collection, examination, analysis and reporting stage are discussed.

CHAPTER 4

THE PROPOSED METHODOLOGY

This chapter will explain about the forensics process flow and framework. Next, present the MYANFOSICS system for Windows live forensics. This chapter discusses the windows system and user related artifacts. The chapter then continues with descriptions the MYANFOSICS system for mobile live forensics.

4.1 Process Flow for Cybercrime Forensics

Process Flow for Cybercrime Forensics involves the case confirmation, scope determination, requirements readiness, examination and imaging, extraction and analysis, and reporting and reviewing of digital devices for evidentiary as shown in figure 4.1.

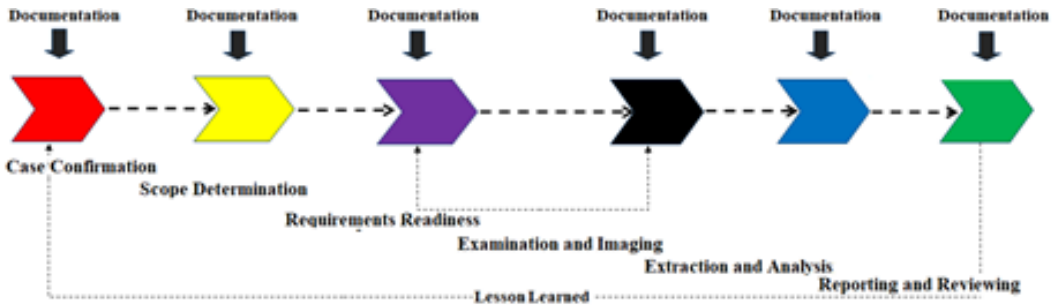

Figure 4.1 Process Flow for Cybercrime Forensics Investigation

Case Confirmation process at cybercrime department, investigator prepares for cybercrime such as identifying possible sources of data, approving the confirm case and opening case for warrant. It gains an understanding of a particular issue or aspect of an investigation. All facing errors and difficulties along with the process model deployment must be recorded. During the Scope Determination process, investigator examine infrastructure and digital devices and determine the boundary of an investigation. In Requirements Readiness process, investigator arranges evidence collection bag and necessary tools according to types of cybercrime.

Forensics or systems security experts need to consider their policy decisions and technical responsibilities, actions in the context of existing laws. The important point for forensics investigators is that evidence must be collected in a way that is legally required and can be admissible in.

One of the most important aspects of securing the crime scene is the preservation of the scene to ensure there is minimal or no contamination and disturbance of physical evidence.

Forensics Techniques are as follows:

- Hashing: To quickly identify a file and to provide authenticity that an image or file was not modified, the forensic community adopted cryptographic hashing. Modern hashing functions use one-way Cryptographic functions to obtain a hash. The uniqueness of the hash depends on the cryptographic function used. MD5 hashing was developed in 1991 by Ron Rivest and was rapidly adopted by the forensics community.
- Imaging: One of the first techniques used in a digital forensics investigation is to image, or copy, the media to be examined. Though this seems to be a straightforward step at first, modern Operating Systems (OSs) perform many operations on file systems when connected, such as indexing or journal resolution. Without care, media can be modified, however slightly, and the integrity of the evidence can be compromised.
- Carving: One category of tools in the digital forensic toolkit is called file carvers. These tools allow the Scanning of disk blocks that don't belong to current files to find deleted data. Carvers use known header and footer signatures to combine these 'unused' nodes into the original files that were deleted. Carving can recover deleted but not overwritten files as well as temporarily cached files on media. Recent advances in carving allowing fragmented files to be recovered with more accuracy.

Examination and Imaging process which is investigator to search relevant and acceptable evidence with live analysis and collects raw evidence data. Integrity for Imaging of storage device using Hashing. Extraction and Analysis process at cyber forensic lab, investigator to extract evidence data from Imaging devices. Reporting process presents the findings as the outcome of the investigation. Review of the investigation process should be done so that the lesson can be learnt and used for further investigation.

4.2 Framework for Cybercrime Forensics

As the ICT sector grows in Myanmar, services will evolve and risks will increase. For example, online-banking, ecommerce, e-government, email, social networking and online shopping, etc. Therefore, a high-level framework of the overall solution is to support Cybercrime Forensics Investigation as shown in figure 4.2.

The first step, we do need to determine the scope of the Crime Scene and then examine infrastructure and digital devices involved in the scene. After that investigate the static or live forensics according to the device status.

By traditional digital forensics it is focused on examining a duplicate called copy of disk to take out memory contents, like the files which are deleted, history of web browsing, file fragments, network connections, opened files, user login history, etc. In static analysis, different kind of software and hardware tools are used for memory dumping and sorting of evidence data for analysis and presentation purpose.

Live Forensics Investigation flow depends on the situation and cases to be investigated. Without any specific requirement, a typical live forensics investigation flow can be depicted in framework. The most important information to be verified and identified during the investigation is to identify the target machine being used for illegal upload of identified matter together with the identity of the user, current user and any web related account information. According to this requirement, the live forensics toolkits should be formulated to collect relevant data.

Firstly, capture physical and virtual memory and then examine the current network connections. Secondly, investigate the files and registry information and current execution process information. After that, collect the current connected network, IP address, and check the network status such as current network path and network broadband device configuration. Also, investigate the current user information and system configuration.

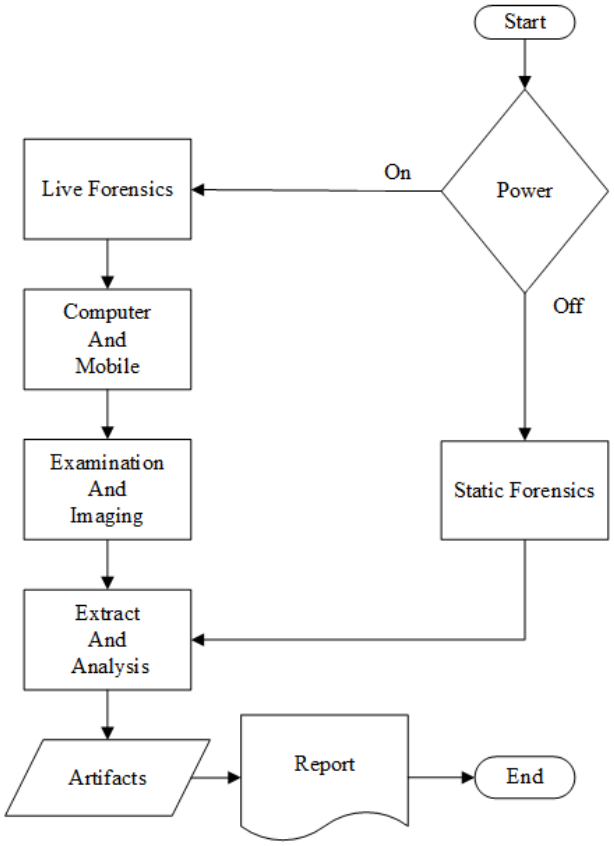

Figure 4.2 Framework for Cybercrime Forensics

4.3 Live Forensics System for Computer

This system can examine preset the process and service list and collect file and directory information and event log. Therefore, forensic examiner can extract current process lists, CPU, Cache, Memory, Network information, Data sharing and transfer archival media, RAM and Storage device imaging for Windows computer that can serve as cyber evidence as shown in figure 4.3.

Because of storage device imaging for static forensics, inspector can examine or analyze such as malicious software, advanced persistent threat and stenography process. If there is some sample still need to investigate, examine at Professional Forensics Lab and extract the secret information and analyze these data and send to the court.

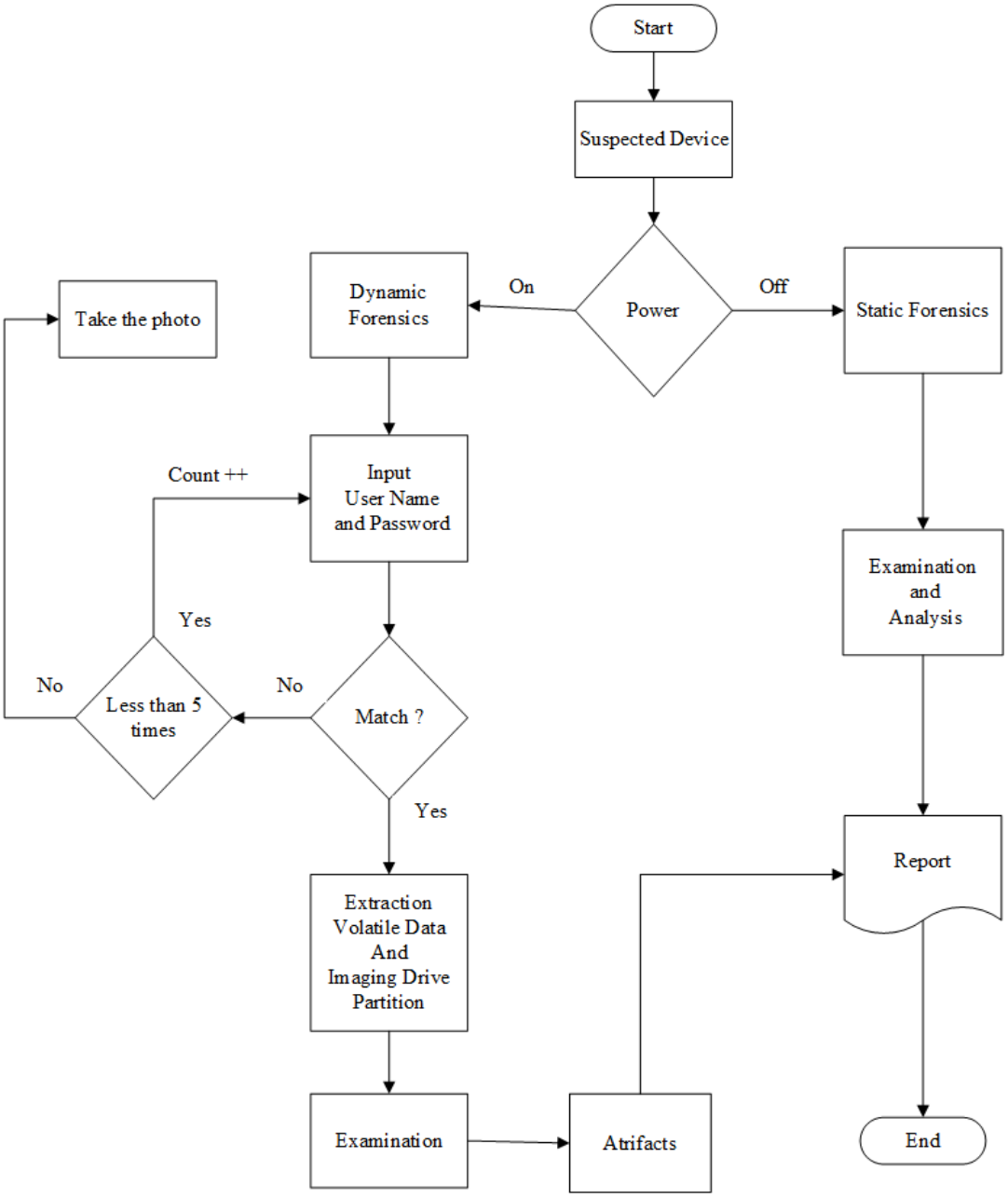

Figure 4.3 Live Forensics System for Computer

4.4 WINDOWS Artifacts

Windows Versions are not all the same. So, there is a need to know differences between Versions. Then, they are not just one Operating System.

It can divide Digital forensic artifacts on a Windows system into system and user related artifacts. The system artifacts are for data that could be collected related to system activity in response to some stimuli, while the user artifacts are those artifacts that are found related to user activity and/or files that have been used by the user.

4.4.1 Shortcuts

According to Microsoft, the lnk file is "a data object that contains information that can be used to access another data object." They are commonly called as Shortcuts. They are small files with a lnk file extension .lnk files are metadata files. It can try to carve them out. Metadata are found as the following,

- Path of target
- MAC address of the host computer (not always)
- The target size when it was last accessed
- Serial number of the volume where the target was stored
- Network share name
- Different attributes: Read-only, hidden, system, volume label, encryption, compressed, etc.
- Distributed link tracking information.

The absolute Path to the file is not stored in the lnk file. The most common locations to find .lnk files are my Recent Documents Locations, which is found in \%USERPROFILE% Recent and \%USERPROFILE%\Application Data\Microsoft \Office\Recent. These files have their own MAC timestamps. At the time a target file is opened, the MAC timestamps of the target file are read and stored within the associated link file itself. The FILETIME format using 8 bytes is used to record the date of these files. Information that could be found:

- Creation time: this is an indication of the first time the file was opened
- Modification time: this leads to an indication of when the last time the file was opened

The link file in the Office Recent folder appears to always contain embedded dates when it is first created but the one in the Recent folder contains no embedded dates because of reference. It not Just a "lnk" file, as it could be configured to run malicious code.

4.4.2 Thumbcache

Before Windows Vista/7, thumbnail files were located within the same directory the pictures are stored in and has the name Thumbs.db. This file stores a

thumbnail version of the existing and also deleted pictures. It is a hidden file and usually ignored by users, some even keep deleting them. It also provides the following details are

- Version of the picture
- The file name and the date and time of the last modification

This is why Thumbs.db files are very useful in cases related to photos (e.g., child pornography cases). Starting from Windows Vista/7, all the Thumbnails files are stored in a single directory located at:

%USERPROFILE%\AppData\Local\Microsoft\Windows\Explorer

With the file named as Thumbcache.db. Therefore, no longer need to search the whole disk for them, they are all stored in that location. Even if the user deletes the whole picture's folder. Modern Windows versions allows users to view files in different sizes.

4.4.3 Volume Shadow Copy Service

The Volume Shadow Copy Service as a Windows service that provides snapshots for a specific point back in time. Sometimes it might find named as restore points. Snapshots could be even turned on for specific directories and not just volumes. VSS was first introduced with Windows Server 2003. A limited edition was in Windows XP in order to support the NT Backup Service. After that, and starting from Windows Vista/7, it began providing a more comprehensive implementation. VSS supports the very useful feature found in the "Restore previous versions" used by Windows Explorer. Such a feature allowed users to roll back a file or directory to a previous state using the snapshot taken.

An investigator's point of view, if a snapshot was taken, it might find useful information that was present in the past. There is a limit to the number of snapshots found, and when reached the system will start deleting old snapshots and creating new ones. The system restore service can automatically create snapshots based on the following factors,

- A service is installed
- A Windows update is done
- When a new driver installation
- On a daily basis via scheduled tasks

- Finally, users and applications can also manually request a snapshot

Forensic value of VSC is a useful way to recover for

- Files
- Registry keys
- Log entries
- Other data that an attacker may
- have deleted or tampered

Beware when accessing VSCs on Live Systems, as they might contain harm (e.g., a Malware). By default, it saves a copy every hour, offline cache is 5% of disk space, and keeps saved versions forever. It will back up are Libraries, Desktop items, Contacts, and Favorites. From the file history config. file, an investigator could obtain as following:

- Directories the user selected for back up
- The User ID of the user that is backing them up
- PC name
- Retention policy for saved file history
- Frequency to back up
- Where the backups are stored (includes: volume path, drive type, and drive letter)

4.4.4 Jump Lists

Jump lists could contain are

- Tasks
- Links to recent files
- Frequently used files
- Links to pinned files

The common location that JumpLists are found in is %USERPROFILE%\AppData\ Roaming\ Microsoft\Windows\ Recent\

Every application has an id known as AppID. It is formed of 16 hexadecimal digits.

Table 4.1 AppID of Internet Browsers

AppID	Application Description
5d696d521de238c3	Chrome Versions 9.0.597.84 /12.0.742.100 /13.0.785.215
cfb56c56fa0f0a54	Mozilla Version 0.9.9
5c450709f7ae4396	Firefox Version 1.0 to 3.0
5df4765359170e26	Firefox Version 4.0.1
1eb796d87c32eff9	Firefox Version 5.0
1461132e553e2e6c	Firefox Version 6.0
28c8b86deab549a1	Internet Explorer Versions 8 or 9
16ec093b8f51508f	Opera Version 8.54 /9.64 /11.50
8a1c1c7c389a5320	Safari Version 3.2.3 (525.29)
1da3c90a72bf5527	Safari Version 4.0.5 (531.22.7) to 5.1 (7534.50)

Table 4.2 AppID of Image/Documents Viewers

AppID	Application Description
f0468ce1ae57883d	Adobe Reader Version 7.1.0
c2d349a0e756411b	Adobe Reader Version 8.1.2
ee462c3b81abb6f6	Adobe Reader Version 10.1.0
b3f13480c2785ae	Paint Version 6.1
3594aab44bca414b	Windows Photo Viewer
d33ecf70f0b74a77	Picasa Version 2.2.0
83b03b46dcd30a0e	iTunes Version 10
271e609288e1210a	MS Office Access 2010 x86
8a1c1c7c389a5320	Notepad (32-bit)
be71009ff8bb02a2	MS Office Outlook ×86

Table 4.3 AppID of Media Players Viewers

AppID	Application Description
6bc3383cb68a3e37	iTunes version 7.6.0.29 to 8.0.0.35
7593af37134fd767	RealPlayer Version 6.0.6.99 and 7 and 8 and 10.5
f92e607f9de02413	RealPlayer Version 14.0.6.666
4acae695c73a28c7	VLC Version 0.3.0 and Version 0.4.6

Table 4.4 AppID of Utilities

AppID	Application Description
3dc02b55e44d6697	7-Zip version 3.13 /4.20 /4.65/9.20
337ed59af273c758	Sticky Notes
290532160612e071	WinRAR version 2.90 / 3.60 / 4.01
b74736c2bd8cc8a5	WinZip version 15.5
bc0c37e84e063727	cd.exe for 32-bit

Forensic value of Jumplists can find useful forensic value when checking Remote Desktop jump lists.

4.4.5 Libraries

Libraries are list of Monitored folders which is used to assist users to find and organize their media:

- Documents
- Music
- Pictures
- Videos

Users could have their own custom libraries, so do not just check the default system prepared libraries. Search, Apps and Settings are saved on a per user basis and stored as an MRU list in the NTUSER.dat file. In Windows 8.1, a user could search for files, settings, applications on his/her system, plus use the Search Everywhere feature to search for the term or keyword not only on their computer but even on Internet.

4.4.6 Windows Recycle Bin

When the user on Windows Explorer deletes a file, the file is moved into a temporary storage location for deleted files. This storage location was named Recycler now Recycle Bin. The recycler was first introduced in Windows 95. This feature gives users the ability to change their mind and restore their deleted files before they are deleted from disk. Today, with the recycle bin, each user has his/her own recycle bin directory. This is why it is trivial for a forensic investigator to understand these directories, their permissions and privileges in order to be able to analyze them and

acquire useful information such as reconstructing the contents. Users could easily bypass the Recycle Bin by using the shift + delete key combination. First, even though users could bypass the recycle bin, it still is important to understand how to analyze this feature, because users still use it. Second, the case where a user shift + deletes a file could be analyzed going back to a lower level, and diving into the file system and disk level. Analyzing the system on a file system and disk level could aid in such scenario.

4.4.7 Prefetch Files

Each executable has its own prefetch file and contains the following:

- The executable's name
- The absolute Path to the executable
- The number of times that the program ran within the system
- The last time the application ran
- A list of DLLs used by the program

All prefetch files are located under: %SystemRoot%\Prefetch\. Every prefetch file has a "pi" extension. If same executable ran from two different paths (locations), then it will find two different prefetch files. Example, if we have C:\Windows\System32\ cmd.exe and C:\Users John\cmd.exe and they were both ran, then it will find two prefetch files. One for the first found in the System32 directory, and another for the one in John's directory.

Settings related to prefetch files are written in the following registry key:
HKE\YLOCALMACHINE\SYSTEM\CurrentControlSet\ControlSessionManager\MemoryManagement \PrefetchParameters
Under the EnablerPrefetcher registry value, it can find one of the data values below:

- O: This means that prefetching is disabled.
- 1: This means enable applications prefetching only.
- 2: This means enables boot prefetching only.

4.4.8 Application Compatibility Cache

A component of the Application Compatibility Infrastructure used by the Windows OS to quickly identify the applications that require shimming due to compatibility issues.

Prefetch files are specify the file being executed on the system and they are disabled by default on Windows Servers. So, ShimCache are a great alternative. Artifacts of Application Compatibility Cache can be found at: Windows XP: HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatibility\ AppCompatCache

Windows Vista/7/8, etc: HKLM\SYSTEM\CurrentControlSet\Control\Session\Manager\AppCompatCache\ AppCompatCache

The file on a Windows 7 is named RecentFileCache.bcf. If the Microsoft update KB2952664 is installed, then amcache.hve is found instead. Starting with Windows 8, it is now replaced with a registry HIVE called amcache.hve which can be found: %SYSTEMROOT%\AppCompat\Programs\

An important note to remember is all the information is retained in memory and is only written to the registry when the system is shutdown. This drawback impacts the ability of getting this source of evidence when conducting live response.

4.4.9. Windows Registry

Windows Registry could be considered a special type of file system used by Microsoft Windows operating systems to store different settings. The registry stores low-level system settings, application settings, and user preferences and settings to.
It could have a great effect on the examination. Below is a partial list of useful artifacts that could be mentioned and found in the registry:

Maintains system configurations and functionality settings Whether the system is to clear the page file on shutdown. Recycle Bin settings and whether to bypass it or not. Settings related to enable/disable Windows Firewall. User preferences and historical activity such as opening files, and recently used stuff. It can also find what programs will automatically start when the Windows starts (Autostarts).

- **Registry Categories**: The windows registry could be divided into two categories: System Registry Files %Windir%\System32\Config and User Registry Files %UserProfile%
- **Registry Structure**: It is divided into a couple of data structures: Hives: contain keys (directories) and values Keys: might contain subkeys and/or

values Subkeys: no difference between key and subkey structure Values: store data (E.g. settings)

- **Registry ROOT Keys**: There are four root keys, which are:

    1. HKEY CLASSES ROOT
    2. HKEY CURRENT USER
    3. HKEY LOCAL MACHINE
    4. HKEY USERS

The windows registry hives are also Known As (AKA) the following:

- HKCR HKEY CLASSES ROOT
- HKCU HKEY_ CURRENT_USER
- HKLM HKEY LOCAL MACHINE
- HKU HKEY USERS
- HKCC HKEY CURRENT CONFIG

One of the important concepts to understand when dealing with the Windows Registry, is the hive relationships. There is a need to understand which hive is related, connected, or a parent of which hive, etc. When there are required to gather evidence from the windows registry, it is extremely important to know where each registry file is stored. The storage locations will differ based on the version of the Windows being investigated. But, not all windows versions are the same. Common Hive Locations:

- **HKLM\BCD**: %SystemRoot%\system32\config\BCD-Template
- **HKLM\SYSTEM**: %SystemRoot%\system32\config\SYSTEM
- **HKLM\SAM**: %SystemRoot%\system32\config|SAM
- **HKLM\SECURITY**: %SystemRoot%\system32\config\SECURITY
- **HKLM SOFTWARE**: %SystemRoot% \system32 \config\SOFTWARE
- **HKLM\HARDWARE:** Volatile hive
- **HKLM SYSTEM\ Clone**: Volatile hive
- **HKU\DEFAULT**: %SystemRoot%\system32\config\ DEFAULT
- **HKU\UserProfile**: «profiles folder>\NTUSER.DAT

4.4.9.1 HKEY LOCAL MACHINE (aka HKLM)

HKLM hive contains system-wide configuration subkeys as listed below:

- **BCD**: Boot configuration data replacing boot.ini

- **HARDWARE**: maintains descriptions of the system's hardware and all hardware device-to-driver mappings.
- **SAM**: holds local account and group information.
- **SECURITY**: stores system-wide security policies and user-rights assignments.
- **SOFTWARE**: stores system-wide configuration information not needed to boot the system.
- **SYSTEM**: contains the system-wide configuration information needed to boot the system.

The registry key holds the following:

A signature

- Found at offset Ox0 and is 4 bytes long.
- Holds the ASCII string regf and all hive files will start with this signature.

The last write timestamp (last time the key was written). A major and minor version numbers. The root cell offset.

This is the date/time format that is used throughout the NTFS file system, and is very common within the Windows Registry and numerous Microsoft software products. It is important to note that the displayed date/time is subject to the correct offset from GMT/UTC to correctly translate, the examiner must determine the regional settings used on the subject's installation of Windows. 8-byte value (always ends to 0x01) number of 100-nanosecond intervals from January 1, 1601 (GMT) to the specified moment.

4.4.9.2 Registry Dates and Times

The FILETIME is not the only time format used on a Windows operating system. Another time used is Unix 32-bit Date/Time, which uses 4 bytes. For example, the Software hive in Windows 10 stores the Installation Date/Time under the value name, Installation with a Unix 32-bit value. So, in forensics software, select the correct offset from GMT/UTC, as Unix Numeric Values are common. The data values are stored in Unicode, so remove the "Ox00" (8 bits) and only compute the numbers. It is the only object that consistently records a modification date/time is the key/subkey. All Value Names, Types, and Data don't record a last modified date/time. If a child object

of the subkey is changed (values), the last modified date/time of the subkey will reflect the date and time of the change. The hardware subtree is mounted and active when the Windows operating system starts running. It gets dismounted when Windows is shutdown.

4.4.9.3 Security Account Manager

If the live view of the Security Accounts Manager (SAM) file using RegEdit, then please note that it is extremely limited (default permissions do not allow viewing). Default Security Identifier(s) or SIDs

- S-1-0-0 (Nobody): A group with no members
- S-1-1-0 (Everyone): A group that includes all users
- S-1-2-0 (Local): Users who logged on locally
- S-1-2-1 (Console Logon): Users on the phys. console
- S-1-3-0 (Creator Owner): The user who created a new object
- S-1-3-1 (Creator Group): The primary group of the user who created a new object
- S-1-5-2 (Logon Network): Users logging on via network
- S-1-5-7 (Anonymous): Anonymous logged on users
- S-1-5-18 (Local System): The OS itself
- S-1-5-19 (Local Service): Service account
- S-1-5-20 (Network Service): Service account Installation dependent (unique!)
- S-1-5-21-?????-500: This is the system's Administrator
- S-1-5-32-544 (Administrators): Group of all administrators

4.4.9.4 Registry Artifacts

- **Artifact #1 - ControlSet No.**

  This key contains system configuration information such as device drivers and services. It is stored in the following key:

  HKEY LOCAL MACHINE\ SYSTEM

  A system could have several control sets, and this depends on the following: How often system settings are changed. If there are problems with the settings chosen.

- **Artifact #2 - Time Zone Information**

One of the critical issues during any forensic examination, is determining the offset from UTC/GMT. The correct interpretation of the data/time depends on the correct offset from GMT that will be applied to the evidence. All time zone information could be found in the SYSTEM hive under:

SYSTEM\ControlSet###\ Control\ TimeZonelnformation

Daylight Name and Standard Name both refer to the TZRES.DLL with a string identifier. Within this DLL file, there are string identifiers that refer to the specific time zone offsets. Here is an explain of what each one of these actually mean:

Daylight Bias: Number of minutes offset from the bias for DST settings

Standard Bias: Number of minutes offset from the bias for standard (usually zero)

Daylight Start & Standard Start

Bias: Number of minutes offset from UTC for the Time Zone Setting

ActiveTimeBias: Number of minutes offset from UTC for the current time setting

TimeZoneKeyName: Friendly Time Zone Setting Name

Year: If the year is zero, it reoccurs every year

Month: # indicates the month (1-12)

Week: week in the month when the setting will start

Hour: # hour of the day in 24-hour format

Minutes: # of minutes when the setting will start

Seconds: # of seconds when the setting will start

Milliseconds: # of seconds when the setting will start

Day: Day of the week when the setting will start

Time zone analysis example: Assume for example the following Standard Start value data (hex)

00 00 0B 00 01 00 02 00 00 00 00 00 00 00 00 00

Year: 00 00 = every year

Month: OB 00 = 11 (November)

Week: 01 00 = 1 (first week of the month)

Hour: 02 00 = 2 (2nd hour of the day, 0200 hours or 2AM)

Minutes: 00 = 0 (no offset)

Seconds: 00 = 0 (no offset)

Milliseconds: 00 = 0 (no offset)

Day: 00 = 0 (no offset)

If a user selects the option to NOT automatically adjust for daylight savings, the value data for the value name "DynamicDaylightTimeDisabled" changes from a 0 to 1.

- **Artifact #3 - Windows Product Info.**

  This information is located in

  SOFTWARE\Microsoft\WindowsNT\CurrentVersion\

  Some of the useful information found there are:

  Installation Date (InstallDate, Decode as Unix Date)

  Product Name (ProductName, Unicode)

  Registered Owner (RegisteredOwner, Unicode)

  Registered Organization (RegisteredOrganization, Unicode)

  System Root (SystemRoot, Unicode). This determines assigned volume letter to Windows (usually C)

- **Artifact #4 - Windows Computer Name**

  The friendly name of the computer as it appears on the network (netbios). This value is stored in Unicode. It could be located:

  SYSTEM\ControlSet00#\Control\ComputerName\

- **Artifact #5 - Windows ServicesEach subkey name denotes the name of the service.**

  Location:

  SYSTEM\ ControlSet00#\Service\

  SYSTEM\ ControlSet00#\ Service\<name>\Start

  Value that determines how the service will behave:

  0= boot

  1 = system

2 = automatic

3 = manual

4 = disabled

- **Artifact #6 - Windows DHCP Config**

  The Windows DHCP IP Address could be found at:
  SYSTEM\ControlSet00#\Services\Tcpip\Parameters\Interfaces\{GUID]\DhcplAddress
  The value is also stored in Unicode.

- **Artifact #7 - Legal Notice & Text**

  Maybe an investigator wants to check the legal notices that appear to the user at the logon screen. They can be found:

  SOFTWARE\Microsoft\Windows\CurrentVersion\Policies|System\

- **Artifact #8 - NTFS Last Accessed**

  Starting from Windows Vista, the NTFS file system is configured by default to no longer record the last accessed date and time in the standard information attribute of the each MFT record. This could be turned on | off by the user. Location:

  SYSTEM \ControlSet###\ Control\ FileSystem

  The values are:

  1 = not updated

  0 = updated

- **Artifact #9 - Autoruns**

  When there are interested in locating what programs are started automatically, when the system comes up, then there are different registry locations to check:

  HKLM\SOFTWARE\
  Microsoft\Windows\CurrentVersion\Run/RunOnce

  HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\ Rubw.\RunOnce

The biggest problem here, is things might be started from anywhere; there is no "authoritative list" from Microsoft available to all the locations that could be used for autoruns. A very useful tool is, AutoRuns which is from the Microsoft's SysInternals Suite.

- **Artifact #10 - Installed Applications**

Software might be installed, although not visible as an icon on the desktop or in any start menu. Registry keys are usually created during installation, but not always removed when the program is uninstalled. Such keys are found under:

HKLM\SOFTWARE\Microsoft\Windows\C.V.\App Paths

HKLM\SOFTWARE\Microsoft\Windows\C.V.\Uninstall

This means that separate registry keys for application settings might exist too. So, there is a need to check for the actual executable at the contained path and it's good to check the timestamps of the registry key.

- **Artifact #11 - Windows Firewall**

The Windows Firewall is normally turned on by default. The registry keys for the firewall could be found in the key below. The Registry values below determine the state of the Windows Firewall for all network profiles available:

Private (standard)

SYSTEM\ControlSet###\Services\SharedAccess\Parameters\FirewallPolicy\ Standard Profile\EnableFirewall

Public

SYSTEM\ControlSet###\Services\SharedAccess\Parameters\FirewallPolicy\PublieProfile\EnableFirewall

- **Artifact #12 - Remote Desktop**

Remote Desktop is a feature that allows a user to log in to a computer from a remote location and run the OS, access files, run programs, as it they were sitting in front of the physical device. It might be asking, why examiners should care about this feature? The reason is because it might get

this response: Someone logged into computer and did this, not user. The location for RDP settings is:

SYSTEM\ControlSet###\Control\TerminalServer\fDenyTSConnections

1 = RD is turned OFF

0 = RD is turned ON

Network Location Awareness (NLA) - For each network interface the PC is connected to, the network location awareness (NLA) will aggregate the network information available to the PC and generate a globally unique identifier (GUID) to identify each network (a profile). Windows Firewall can use this information to apply rules from the appropriate Windows Firewall Profile. For example, a Public network could get a very restrictive set of rules, a Home network could get a less restrictive set of rules, and a Managed network could get a set of rules determined by an administrator.

Domain

SYSTEM\ControlSet###\Services\SharedAccess\Parameters\FirewallPolicy\ DomainProfile\EnableFirewall

The value O means OFF while 1 means it is ON. There are other subkeys which store service restrictions and firewall rules (standard and user-defined).

- **Artifact #13 - Network History**

  The cache for networks history could be found:

  HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\Nla\ Cache

  Managed networks location refers to one where the computer is part of a domain. The location is found here:

  HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\ Signatures\Managed\

  While Unmanaged network location is, by default and logically, the one where a computer is not part of a domain. The location is found here:

  HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\ Signatures\Unmanaged

- **Artifact #14 - Network Types**

  The types of networks, could be found under the following:

  HKLM\SOFTWARE\Microsoft\WindowsN\CurrentVersion\Network List\Profiles

  Under the profiles key, there will be a number of keys as GUIDs, each representing a network profile.

- **Artifact #15 - Shutdown Details**

  The value used to identify the shutdown time(ShutdownTime) is found:
  HKLM\SYSTEM\ControlSet001\ Control\ Windows

- **Artifact #16 - Applnit_DLLs**

  The Applnit_DLLs is a value that contains a list of DLLs that will be automatically loaded whenever any user. mode application that is linked to user32.dll is launched. This means, if an attacker manages to adds a malicious DL to this value, its code will effectively be injected into every subsequently launched application. The location is:

  HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Windows\Applnit_DLLs

  Since this value could be disabled globally, then there is a need to the corresponding settings for it, which is supposed to be 0x0 and found:
  HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Windows\LoadApplnit_DLLs

4.4.9.5 User Hives (Registry)

- **Artifact #1 - Windows Recycle Bin**

  The properties of the Windows recycle bin have been consistent since Vista. User can send (move) files to the Recycle Bin or completely bypass it (similar to Shift + Delete command). The Location is found in the NTUSER.DAT file:

  NTUSER.DAT\Software\Microsoft\Windows\CurrentVersionExplorer \BitBucket\ Volume\{GUID) NukeOnDelete

  The settings are:

1 = bypass Recycle Bin

0 = move to Recycle Bin

All these settings are user specific unless they are set by a group policy. Max capacity of the user's Recycle Bin is also found in the value Max Capacity (hex to decimal = megabytes of maximum files in the bin).

- **Artifact #2 - Last User Logged In**

One of the important user artifacts, is to know when was the last time the user logged into the system. This value data will list the user's name (stored in Unicode). It could be found:

SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUl\ LastLoggedOnUser

- **Artifact #3 - User Sessions**

During a live Windows session, the logged on users arerecorded in the volatile registry path found here:

SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\ SessionData\<#>\LastLoggedOnSamUser

Do not forget, this value is DELETED once the machine is powered off. Parent subkey LogonUI, holds a subkey called SessionData. The child subkey names of SessionData are numbers beginning with 1, 2, and so on. Within the "#" subkey is the value, "LastLoggedOnSamUser". The LastLoggedOnSAMUser value stores the computer name and user name in Unicode. These session subkeys are created when the OS is running and at least one user is logged in. Session subkeys are created for other users who login too. After a normal shutdown or even disconnecting power, the session subkeys are deleted.

- **Artifact #4 - Local Users**

Windows stores local user account information in the SAM hive (name, password, login date/time, hints, etc). Under the SAM hive, they are found:

SAM\Domains\ Users

Exploring the content using Windows Registry Explorer. Under the Users subkey, it will find a series of user folders that are written in hex

notation. Each user is assigned a Security Identifier (SID). The last 3+ digits of the SID is referred to as the Relative Identifier or RID. If convert the hex value to decimal, this will result in the RID value for that user.

Example: 000001F4 = 500

The Windows Administrator is a built-in account on the local machine which has the RID value of 500. This is found on all Windows installations since Windows NT until today.

Local Users... ProfilelmagePath

Domain accounts appear under SAM\Domains\Names

However, there is no way to determine the user's RID (or full SID) from the values. Therefore, the investigator must check the SOFTWARE hive as follows:

SOFTWARE\Microsoft\Windows N\ CurrentVersion\ ProfileList

Then search for the ProfilelmagePath value.

Local Users... UserPasswordHint

It can even check the user account's password hint which is also stored in the registry. Located and stored in Unicode:

SAM\SAM\Domains\Account\Users\<32-bit-hexvalue>\UserPasswordHint

- **Artifact #5 - Local Users... Login Tile**

  It can also check the user's login tile (graphic), which is stored in:

  SAM\SAM\ Domains\Account\Users\<32-bit hexvalue>\ UserTile

  The photo is stored within the value data as a bitmap regardless of the original format. At offset 12 (4 byte value), it can find the size of graphic used. And at offset 16, is the beginning of bitmap data, starting with "BM". At the end of the value, the file type (BMP), volume letter, full path, and file name are stored for the tile.

- **Artifact #6 - User Account Control (UAC)**

  UAC was first introduced in Windows Vista. It is a security component that enables users to perform common tasks as non-administrators, called standard users, without having to switch to an administrative role or user

account. A limited user has no administrative rights and cannot install software or perform other administrative functions without the permission of the administrator. If a limited user opts to install software, the administrator's password (standard user or administrator) is required. AC is enabled by default, but users can turn this feature off through the Windows Control Panel. The settings for UAC are found at:
SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA

0 = UAC disabled

1 = UAC enabled (default value)

- **Artifact #7 - User Assist Keys**

These are Registry values that can track a user's interactions via the Windows Explorer shell, primarily when a user clicks or double clicks certain items. They are used by Windows to tailor the user experience. For example, display menu items the user mostly uses. They could be found here:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\userAssist

By investigating UserAssist keys, it can: Understand frequency of program execution (per user). Identify the last time a program was launched. Which items were being launched most often. Evidence of programs after deletion/uninstall. The clever reason of why checking them, is Evidence of absence. "My Documents" directory empty and no items within it, but was launched, let's say, 33 times! This means there could have been something there. The user activity is tracked beneath these subkeys:

1. GUID
2. Count

The value names and value data are encoded with ROT13 encoding. It will find to Count subkey below each of the GUID subkeys. A GUID is a globally unique identifier. Subkeys represent Windows Explorer, Internet Explorer, etc.

{CEBFF5CD-...}= Executable Files

{F4E57C4B-...}= Shortcut File Execution

There are some GUIDs which are related to program locations instead of programs.

Table 4.5 GUID subkeys of Some Programs

Location	GUID
ProgramFilesX64	6D809377-
ProgramFilesX86	7C5A40EF-
System	1AC14F77-
SystemX86	D65231B0-
Desktop	B4BFCC3A-
Documents	FDD39AD0-
Downloads	374DE290-
UserProfiles	0762D277-

- **Artifact #8 – LastKey Viewed**

It can even check what was the last Registry Subkey that was viewed by the user.

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit\ LastKey

The last subkey viewed by the user is displayed in the value data. This key is user specific for each user account.

- **Artifact #9 - Hidden Files Settings**

It can also check the Show / Hide Files Windows Explorer feature that allows us to hide files a directory. They are those files with hidden attributes set. They can be found here:

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden

0 = Do Not Show Hidden Files

1 = Show Hidden Files

- **Artifact #10 - Hiding File Extensions**

  Not just hiding files, but even the Show / Hide File Extensions too could be checked here:

  NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt

  0 = Show File Extension

  1 = Do NOT Show File Extension

- **Artifact #11 - IE TypedURLs**

  When a user types a URL in Internet Explorer (IE), they are actually stored. They could be found within the Internet Explorer Settings Location:

  NTUSER.DAT\ Software\ Microsoft\Internet Explorer

  This key holds latest URLS typed in the browser by the user:

  0 is the most recent

  1 is the next previous

4.4.9.6 Shellbags

ShellBags are a set of Windows Registry keys located in NTUser.dat and USRClass.dat registry hives that maintain view, icon, position, and size of folders when using Windows Explorer. All directory traversal done with Windows Explorer is tracked and maintained in the registry. This is why shellbags are extremely useful evidence to understand user's navigation activity on the system. This data includes multiple timestamps and other pieces of information that provide context, and can be used to show knowledge and intent when it comes to accessing directories or other resources on a computer. ShellBags Forensic Value are as following:

- May point to evidence that existed at one point in time
- May assist the examiner in looking at the broader picture when only a piece is known
- Information persists even when the original directories, files, and physical devices have been removed from the system

- Can serve as a "history" into data that was previously on a system but may have since been removed
- Can be the Desktop item, a Control Panel Category, a Control Panel item, a drive letter, or a directory, etc
- Could be used to track a cyber-intruder's actions on a host system after compromise if the actor uses for example: RDP or other Remote Connection controls
- Windows Explorer to drop binaries onto the system
- Access network resources. Browse compressed archives

ShellBags located on Windows Vista and newer could be in any of the following locations:

- HKCU\Software\Microsoft\ Windows\Shell\ Bags
- HKCU\Software\Microsoft\Windows\Shell\BagMRU(ntuser.dat)
- HKCU\Software\ Microsoft\ Windows\ShellNoRoam Bags

Under NTUSER.DAT:

- HKCU\Software\ Microsoft\ Windows\ ShellNoRoam\BagMRU

Under USRCLASS.DAT:

- HKCU\Software\Classes\LocalSettings\Software\Microsoft|Windows\Shell\BagMRU
- HKCU\ Software\ Classes\ LocalSettings\Software \Microsoft\Windows\ Shell\Bags

Each ShellBag contains binary data (seen in hexadecimal) that defines what the ShellBag represents. Some ShellBags contain strings (both ANSI and Unicode) representing things such as directory names or UNC paths. There are several dates and times embedded in the binary data as well as MFT entry and sequence numbers. It is possible to determine that a directory existed on this system, based on the contents of the ShellBag. Also, the existence of MUListEx that reflects the order the ShellBags were opened with the most recently opened bag being listed first. As ShellBags are opened, the MRUListEx values are shifted to the right and the most recently opened value is added to the leftmost position.

4.4.10 USB Forensics

Another important task that it might need to investigate is when dealing with Universal Serial Bus (USB) devices. USB devices are used daily for different reasons.

Sometimes they are not only used for storage, but even booting. For that reason, it is important to understand where to look for evidence and when did that USB device get plugged into the system and it could be attached to the computer using a USB interface. It can attach a thumb drive, printer, camera, etc. So there is a wide range of devices out there.

When a USB is first connected to the system, it has the appropriate driver installed and all this is logged in a couple of different log files that we'll see shortly. Every device has a serial number, but if it does not a serial number then Microsoft Windows will generate one for the device. The serial number is a unique number usually assigned by the manufacturer, something similar to network card's MAC Address. Even when a device is removed (disconnected) from the system, the details regarding the device is still there. So, it can check the registry, the logs, and the serial number details to identify different details related to USB devices and when they were used on the system. Therefore, usually an investigator will gather different evidences from different locations to prove a point regarding a USB device. Locations of USB Device Evidence. USB device evidence could be found into two categories:

- Windows Registry
- Specific System Log Files

4.4.10.1 Windows Registry of USB

The details of USB devices stored in the registry as mentioned earlier are inside the USBSTOR key. This key is found under:

HKLM\ SYSTEM\ ControlSet00?\ Enum\ USBSTOR

The USBSTOR key holds the following:

- A subkey for each USB device connected to the system. This subkey holds:

  1.Vendor

  2.Product

  3.Revision Number

- Sub subkeys holding the serial number if it existed. Else Windows will generate one
- A ParentldPrefix value which corresponds to the MountedDevices key

Mounted Devices: To locate where the device is mounted, check the MountedDevices registry key. This key is located at:

HKLM\SYSTEM\MountedDevices

A basic way of checking, is going to the location where it will notice entries such as:

- \DosDevices\D:
- \DosDevices\E:
- \DosDevices\F:

They are all the same values found under USBSTOR. And if it looks closely, it can see that 4C530001280103104220 corresponds to the USB device of interest, as this is its serial number.

4.4.10.2 System Log Files

When the USB device is first plugged in, the Windows system will perform a different set of operations, including installing the appropriate drives and handling different hardware issues related to the device. All these activities are completely logged in files. The files that we can check to find details of the USBs that have been plugged into the machine are stored in plain text files so they can easily be collected and checked. The logs files of interest (not limited to these though) are:

Under a Windows XP: setupapi.log located under C:\Windows. While under Windows Vista and up, two different locations are found.

- **Location #1** - Files under C:\ Windows\INF\
  1. setupapi.dev.log
  2. setupapi.offline.log
  3. setupapi.setup.log
  4. setupapi.upgrade.log
- **Location #2** - Files under C:\Windows
  1. setupact.log > holds setup actions done during installation
  2. setup.err.log > holds error message to actions that happened during installation.

4.4.11 Browser Forensics

Web browsers are the most popular computer applications today. They retrieve, process, and present data. Data is most commonly Hypertext Markup Language

(HTML) and numerous multimedia formats. When rendered HTML + multimedia = web page. Web browsers can retrieve data from:

- A local computer
- Remote computer (server or a site anywhere in the world)

Locations consist of:

- Stored in the Windows Registry
  1. Autocomplete
  2. Typed URLs
  3. Preferences
- Stored in the File System
  1. Cache
  2. Bookmarks
  3. Cookies

4.5 Live Forensics System for Mobile

Therefore, forensic examiner can be extract profile information, installed application list, contact list, call logs, SMS logs, media and file list, browser history, Bluetooth list, Wi-Fi history and location history from various makes and models of mobile smart phones that can serve as cyber evidence. For some circumstances, there will be more to investigate information about internet forensics usage, inspector can extract specifies evidence data from email, and social networking sites. These investigations assist in the recovery of internet and application data of smart phone devices data that are used to conduct these transactions.

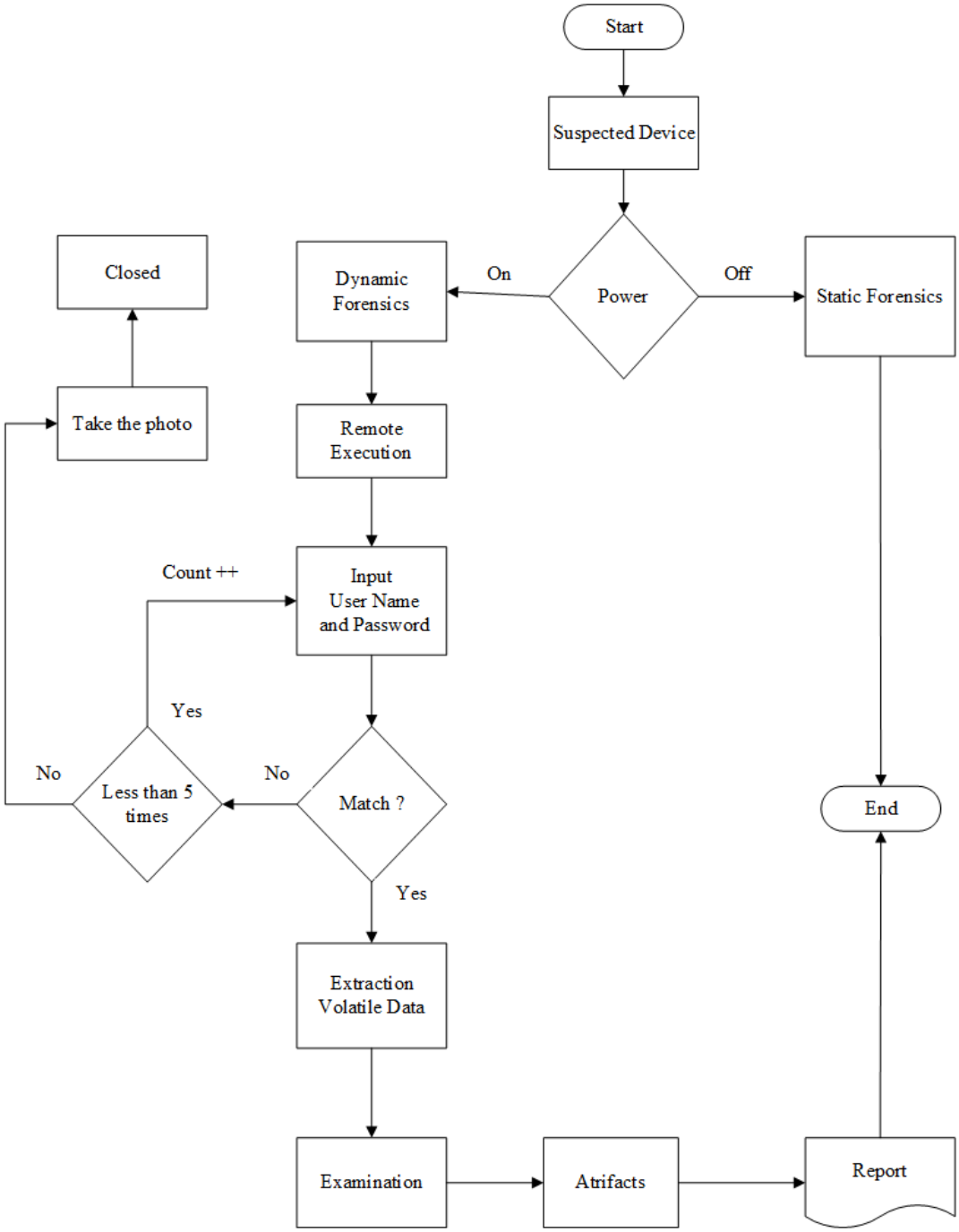

Figure 4.4 Live Forensics System for Mobile

4.6 Chapter Summary

This chapter described the research methodology used to collect and analyze the data required to address the research questions. This chapter discussed a six-stages process flow and an analysis framework. The chapter begins with a continues with descriptions of the windows operation system for the computer forensics followed by the data integrity in cryptography and data carving using data remnants. The detailed

implementation and experimental setup of the MYANFOSICS tool suite will demonstrate in the next chapter.

CHAPTER 5

IMPLEMENTATION AND EXPERIMENTAL RESULTS

The MYANFOSICS tool is based on the open-source tools and nature of the forensic investigation. This tool supports two main categories for cybercrime forensics (computer and mobile) in cybercrime investigation. This chapter explained the MYANFOSICS tool suite which supports four categories: data collection, examination and analysis, reporting and management was highlighted.

5.1 MYANFOSICS System

This MYANFOSICS tool was developed by Python, Java and Swift programming language. It supports across multiple platforms, including Windows, iOS, and native Android as shown in table 5.1 and testing environment as presented in table 5.2. It includes login feature with username and password as shown in figure 5.1. After login, investigator can investigate for cybercrime forensics. Before analysis the live artifacts, it used MYANFOSICS tool to extract dynamic data that support to all other investigation processes.

Forensics investigator can retrieve dynamic artifacts (Screenshot Computer Monitor and Open Applications, Extract Current Process, Network Traffic Capture, IP and Ports for Specific Running Processes, Browser Cookies and Cache, Bookmarks, RAM imaging, Trace Files, Username and Password, Profile and History, Time Sequenced Logs, Event and Transaction Logs and etc.) for computer as shown in figure 5.2 to 5.8, and (Screenshot Phone Screen and Status, Extract Dynamic Data, System Information, Application List, Contact List, Call Logs, SMS Logs, File and Folder List, Browser History, Bluetooth and Wifi History, Location History and etc.)for mobile device are shown in figure 5.9 to 5.18. And then it can save not only specific information but also detail other information.

After recorded to all information from the entire storage device and memory, forensic investigator can logical and physical imaging with MYANFOSICS tool by using Hashing for data integrity.

Table 5.1 Technical Environment for MYANFOSICS System

Operating System	Version	Programming Language
Window	Window 7 / 8 / 10 / 11	Python 3.8
Android	Android v 5 (Lollipop) v 6 (Marshmallow) v 7 (Nougat) v 8 (Oreo) v 9 (Pie)	Java
iOS	iOS v 8 / 9 / 10 / 11 / 12 / 13	Swift 5
Server		PHP (Laravel Framework)

Table 5.2 Testing Environment for MYANFOSICS System

Computer	Acer Intel(R) Core(TM) i3-7100 CPU @3.90GHZ 4.00GB RAM Windows 7 Ultimate Lenovo Intel® CoreTM i5-5200U CPU@2.20GHz 8.00GB RAM Windows 10 Enterprise (64-bits) HP AMD Ryzen 3 3200U with Radeon Vega Mobile Gfx 2.60 GHz 8.00GB RAM Windows 10 Home (64-bits) Dell Intel® Core™ i3-9100 CPU @ 3.60GHz 4.00GB RAM Windows 10 Pro (64-bits) Dell Intel® Core™ i3-9100 CPU @ 3.60GHz 8.00GB RAM Windows 11 Pro (64-bits)
iOS	iPhone 6 Plus, iPhone 7 Plus iPad Air 2, iPad Pro 2021
Android	Huawei C8650+ Samsung Galaxy Grand 2 Samsung Galaxy J4 VIVO 1906 VIVO 1904 XIAOMI Redmi 8A

5.2 MYANFOSICS System for Computer Forensics

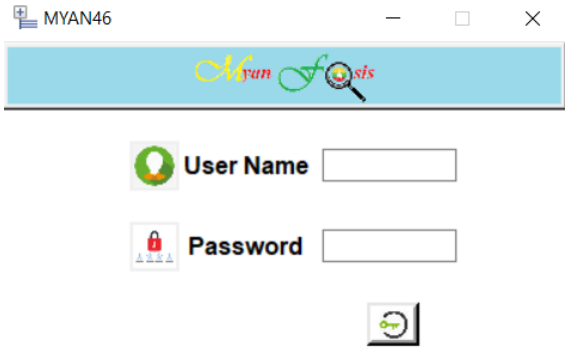

Figure 5.1 MYANFOSICS System Login Page

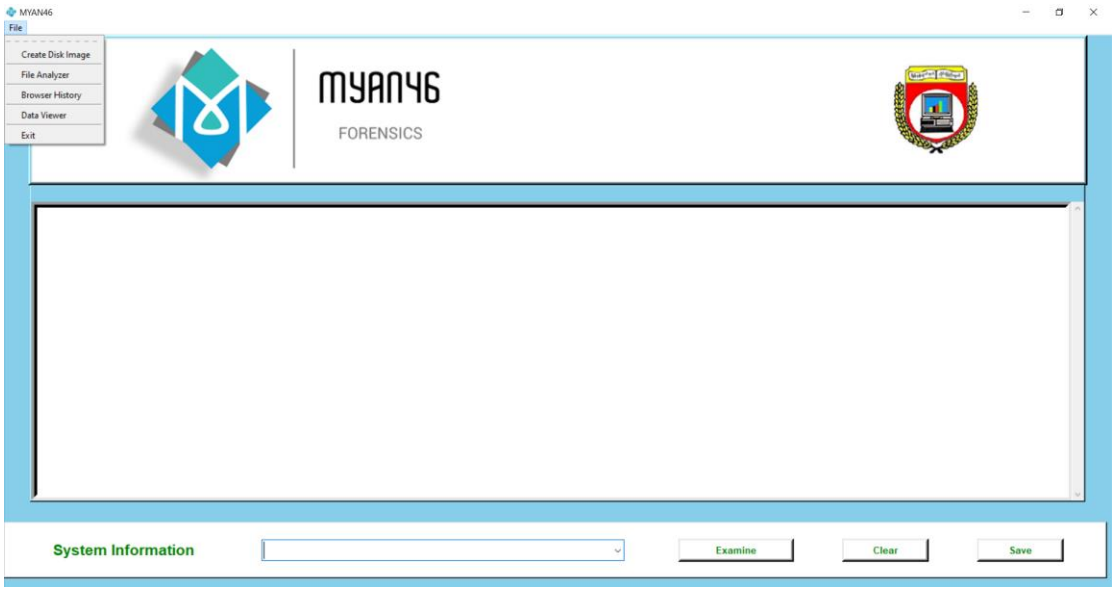

Figure 5.2 MYANFOSICS Home Page

5.3 Extract Volatile Data

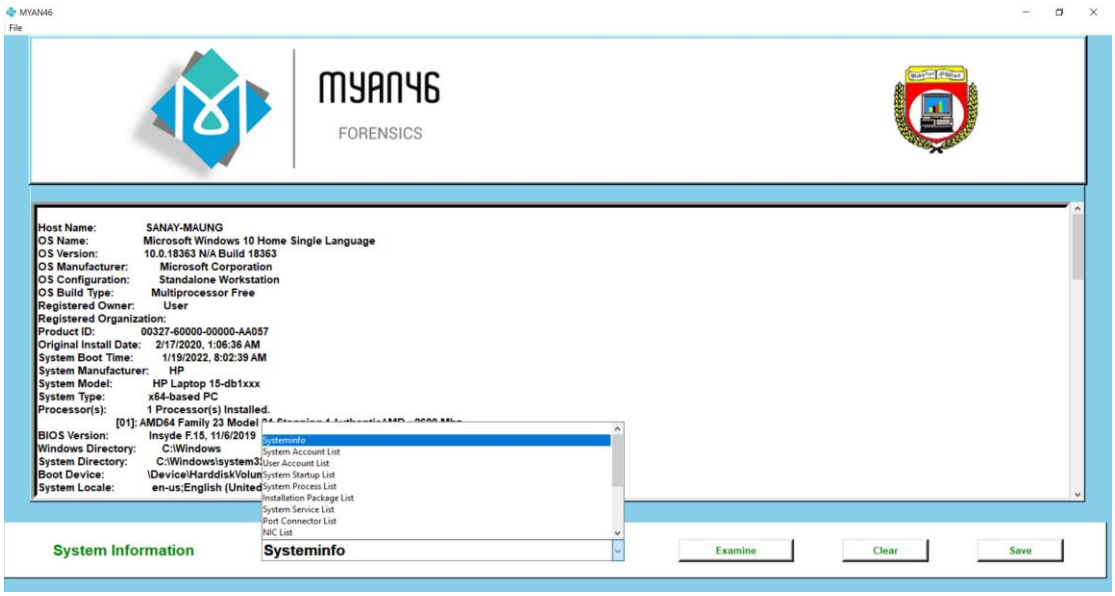

Figure 5.3 Extract Volatile Data

In this phase, forensics inspector can read specific device information (Manufacturer, Model, Version, Original Install Date, Time Zone, System Boot Time and etc.), Process, Memory, Network and Port Connector as shown in figure 5.3. And then it can save not only specific information but also details of other information.

5.4 Create Disk Image

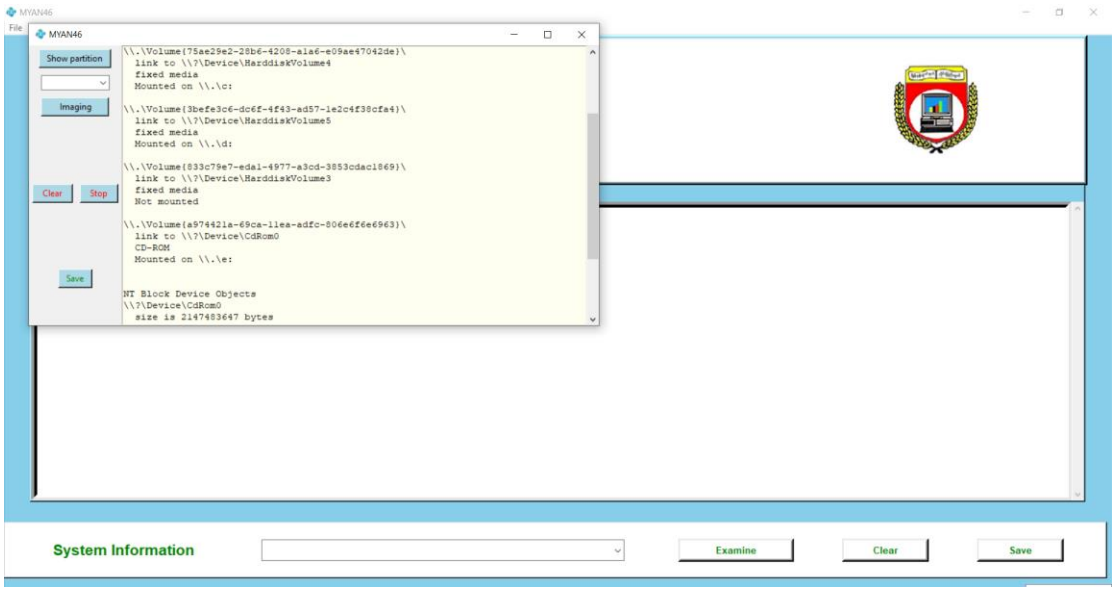

Figure 5.4 Create Disk Image

Storage Imaging is acquired the entire storage device and memory with logical and physical imaging. During the time of seizure, if the power of evidence device is off that investigator will lose volatile data. Because most of the power off device needs to restart and it will be lost volatile remnant data on memory.

This feature does the Bit-by-bit copy from all partitions of Windows and External Storage Devices. It replicates all sectors that contain logically bad sectors and blank sectors. Otherwise, it can call the sector-by-sector clone. The investigator can check details Windows partitions and External Storage Devices list for the imaging process.

During the time of seizure, if the power of evidence is on that investigator can capture a lot of volatile and remnant data on device is known as Live forensics. The first version of MYANFOSICS provides interesting information about live system as shown in figure.

5.5 File Type Analyzer

Electronic files have a file signature which the operating system and programs need to select the appropriate program to open or run the file. File Type Analyzer analyzes the file signature (extension and header code) whether the files are corrupted or not.

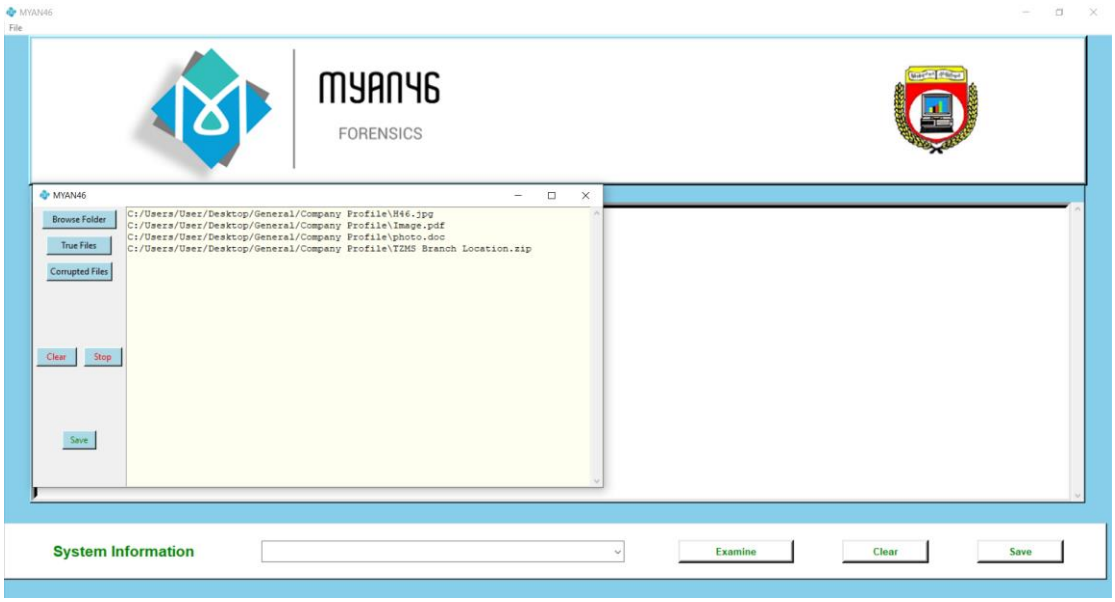

Figure 5.5 File Type Analyzer

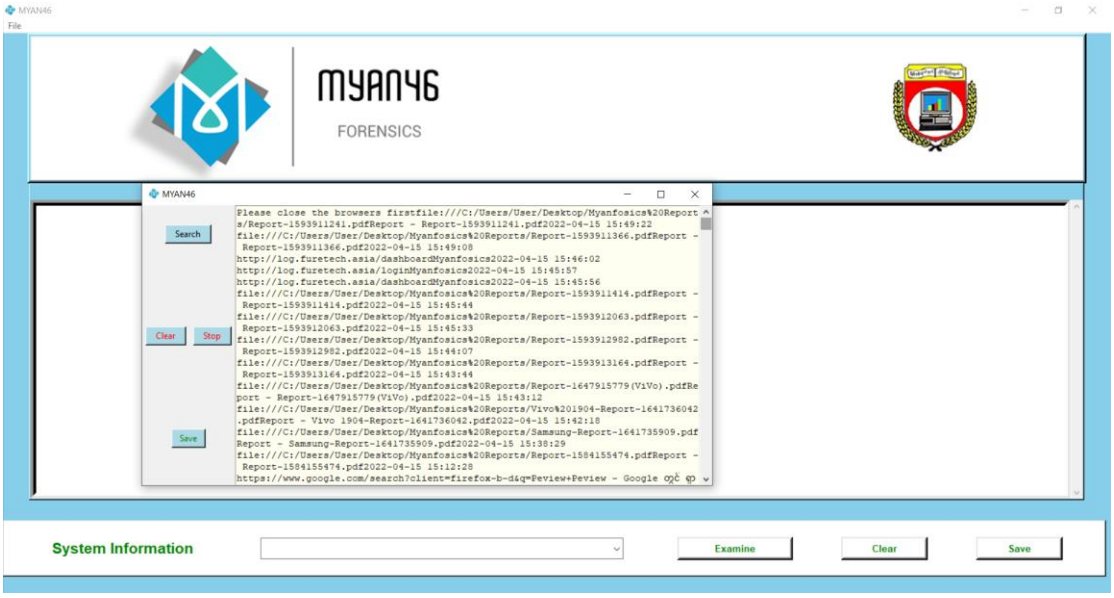

Figure 5.6 Browser History Data

5.6 Data Viewer

Data Viewer analyzes the *.m46 extension files that contain browser history file, system info file, user account list file, system startup list file, driver list file, event triggers file, exe ports file, network configuration file, process list file, USB connected list file, software installed list file, printer list file, etc. It provides keyword searching feature with check one by one with color and remove case sensitive.

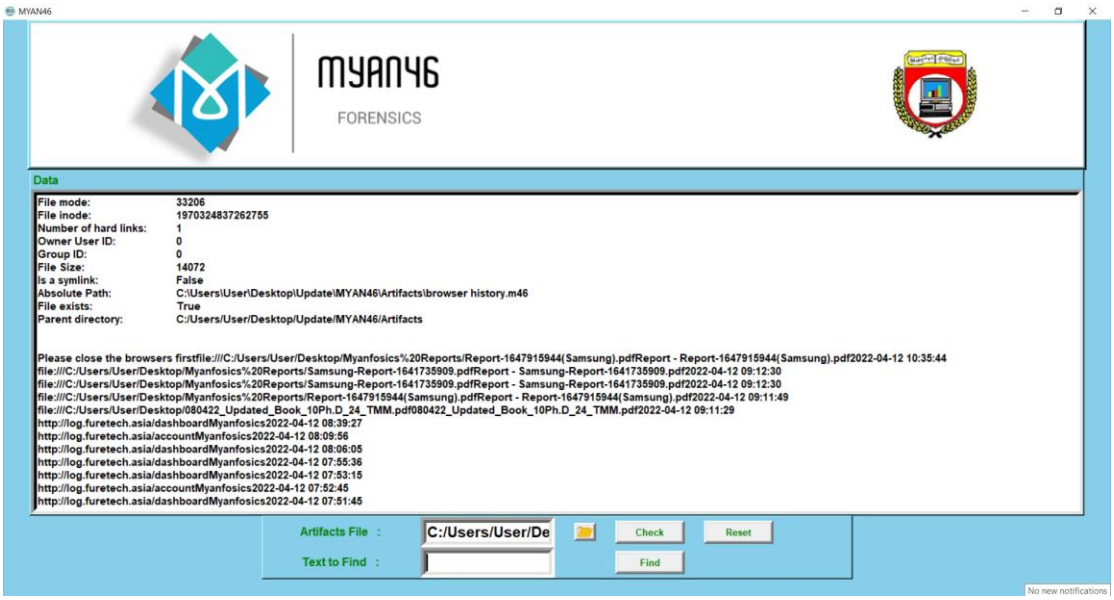

Figure 5.7 Data Viewer

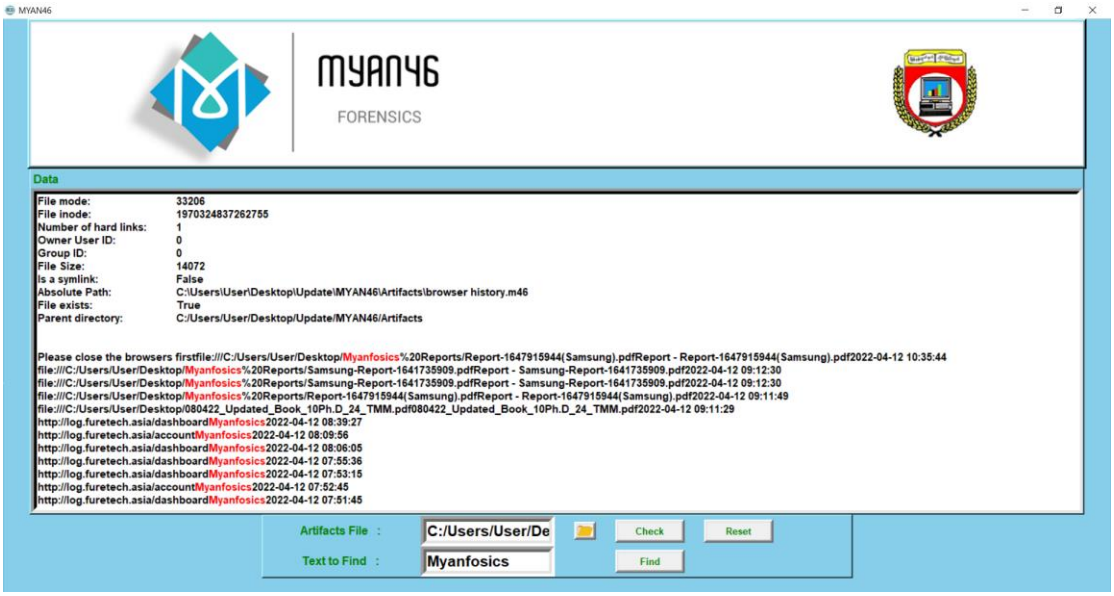

Figure 5.8 Keyword Search

5.7 MYANFOSICS System for Mobile Forensics

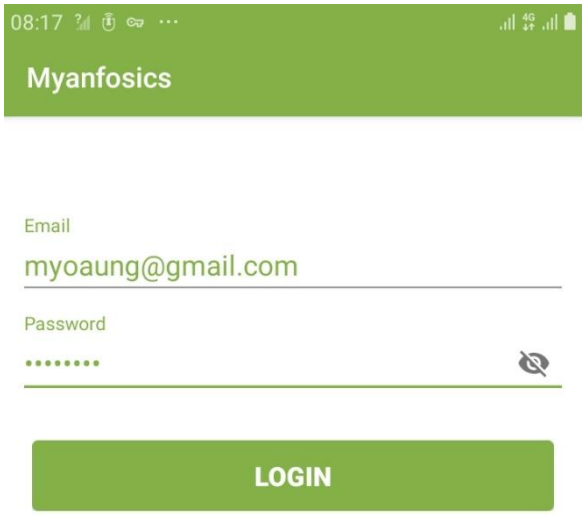

Figure 5.9 Mobile Login Page

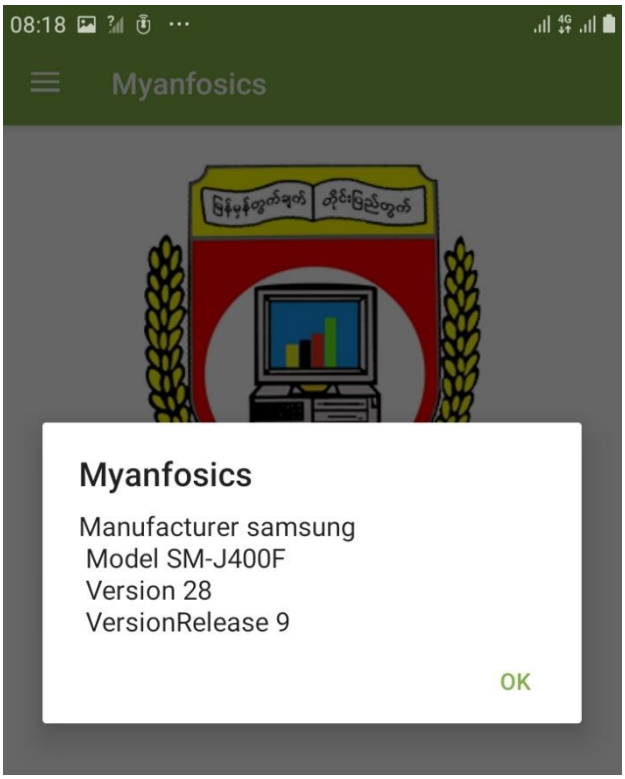

Figure 5.10 Device Specification

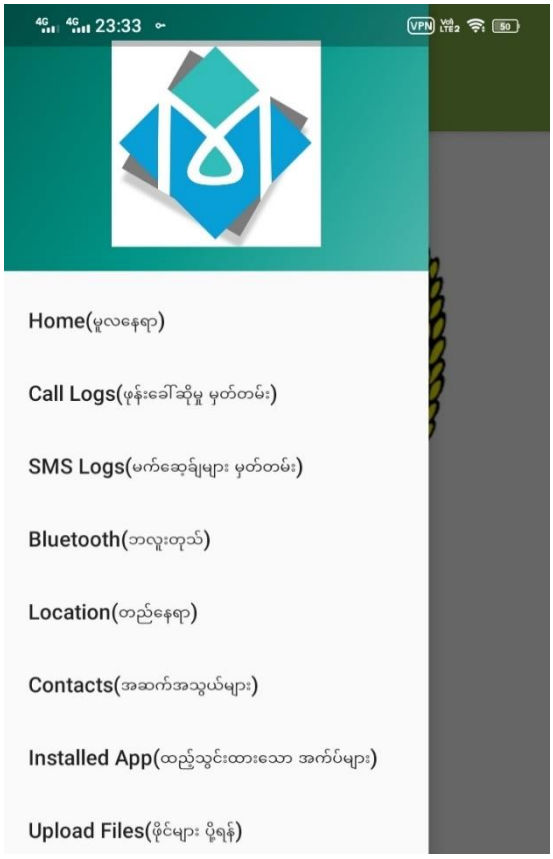

Figure 5.11 Application Menu

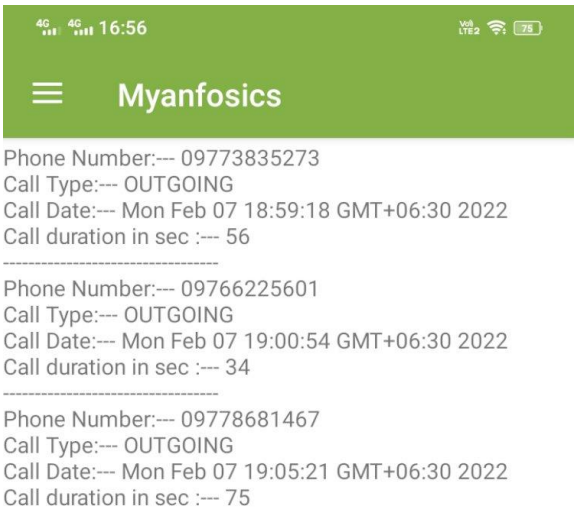

Figure 5.12 Call Logs

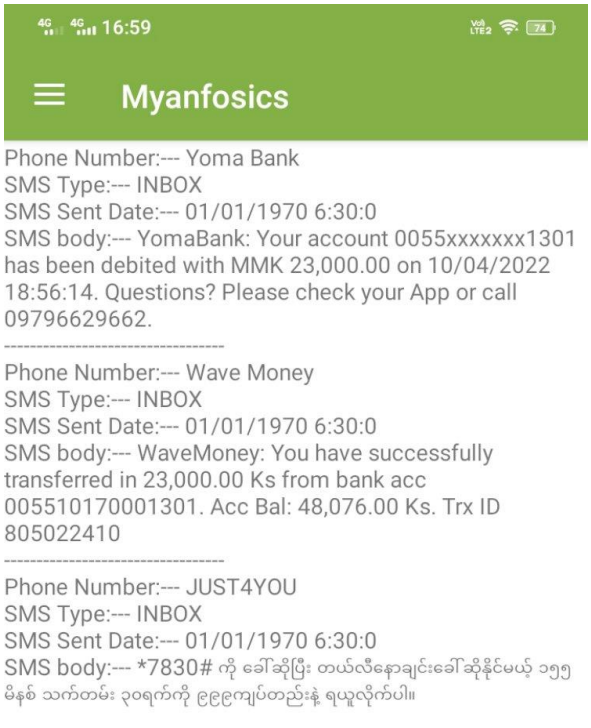

Figure 5.13 Message Logs

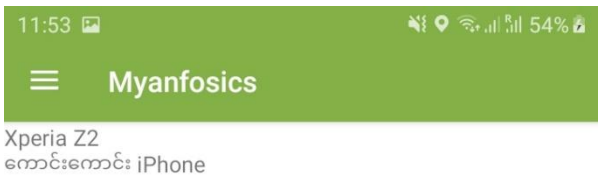

Figure 5.14 Bluetooth Logs

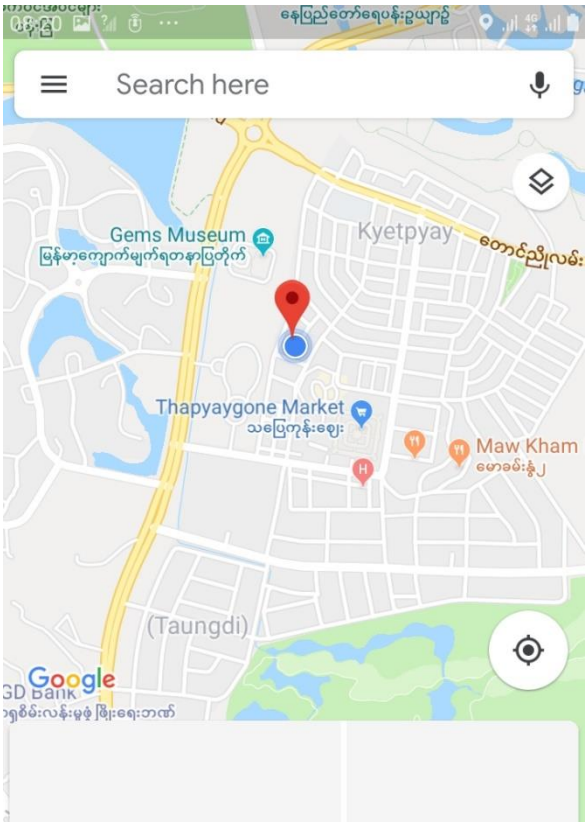

Figure 5.15 Last Location

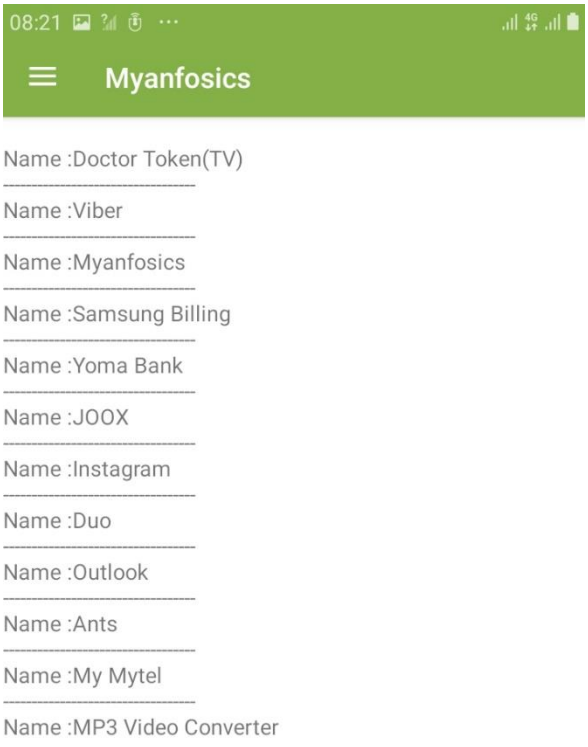

Figure 5.16 Installed Application Logs

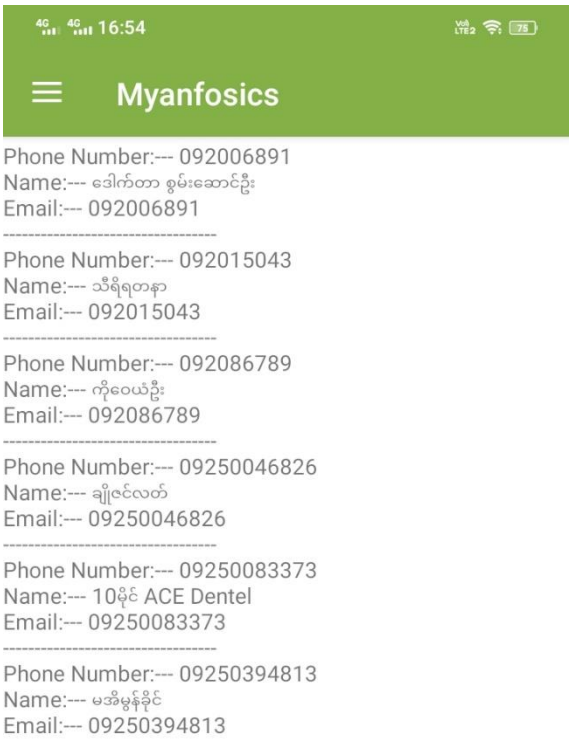

Figure 5.17 Contact Logs

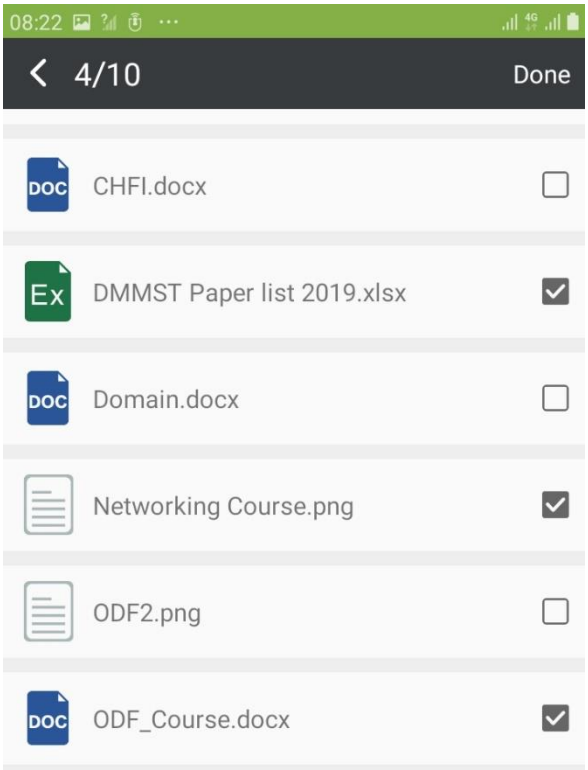

Figure 5.18 File List

5.8 MYANFOSICS System for Server Side

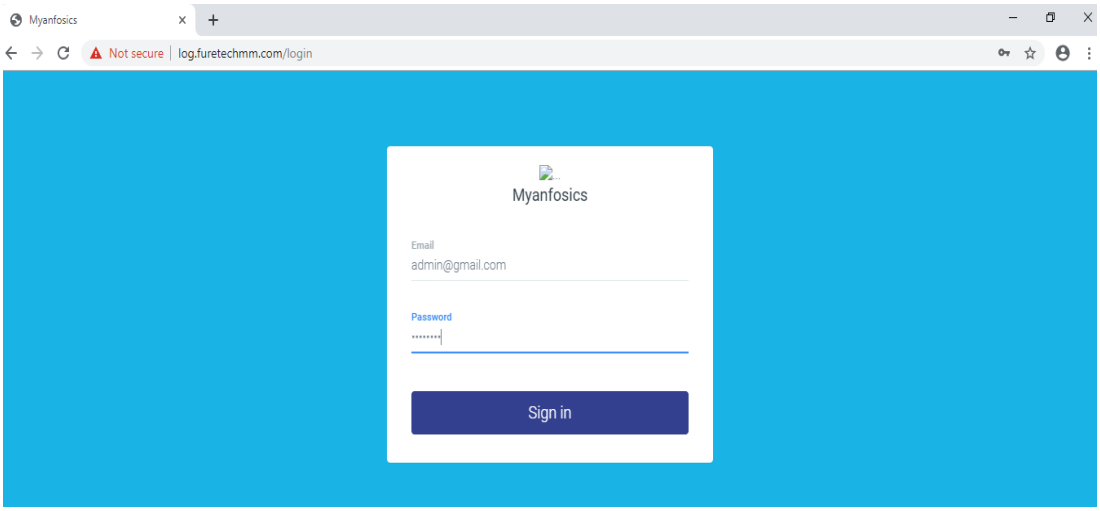

Figure 5.19 Server Log In Page

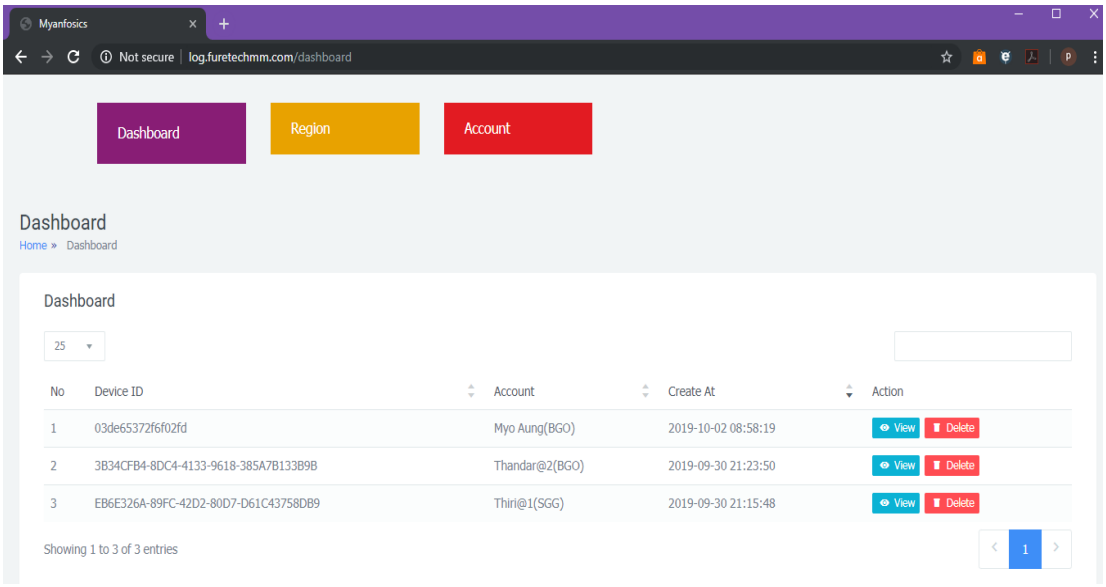

Figure 5.20 Dashboard in Server

There are three portion in MYANFOSICS System for Server Side. They are Dashboard, Region and Account. In Dashboard portion, it can see device id, first responder name, case created date and time. And it can view and delete the artifacts data. Also it can export the report file. In Region, it can edit and delete the region name.

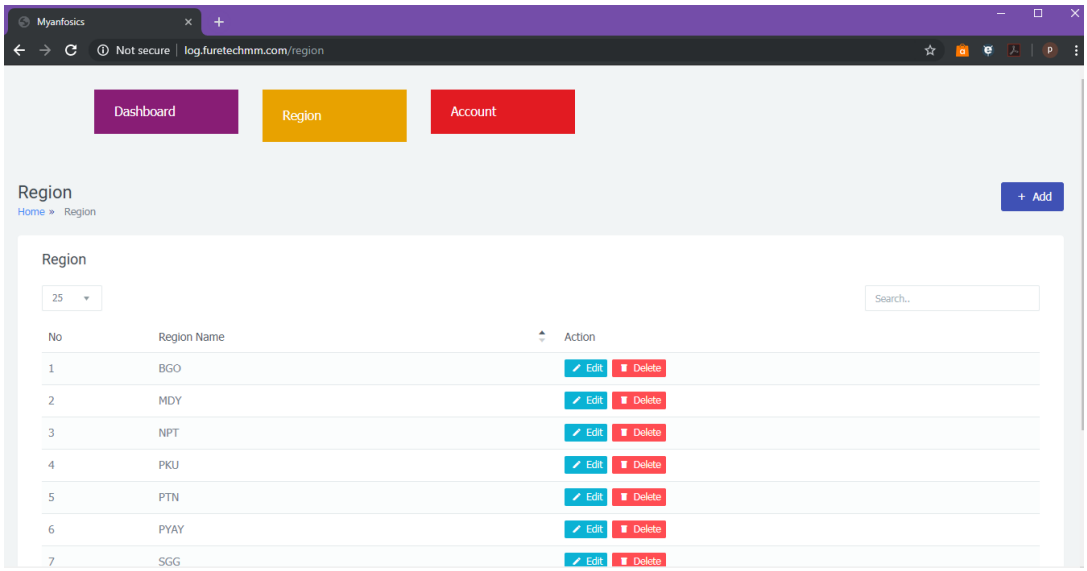

Figure 5.21 Region Data in Server

In User Account Management feature, administrator can create user accounts for accessing the MYANFOSICS tool. It can also check users list and delete the user. In Management settings, other users can access only password update feature. MYANFOSICS System for Server Side screenshot are shown in figure 5.19 to figure 5.30.

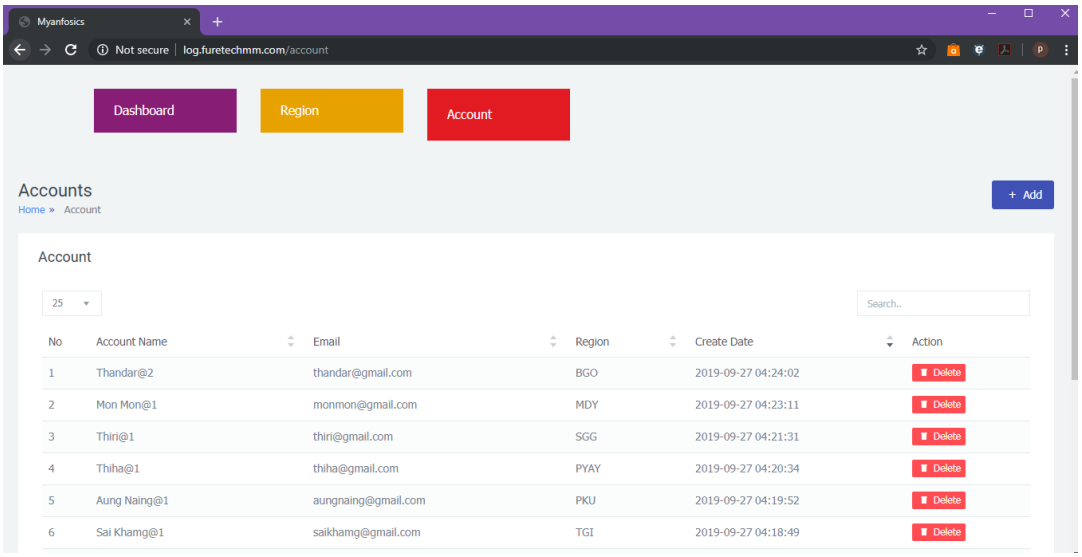

Figure 5.22 Account Management in Server

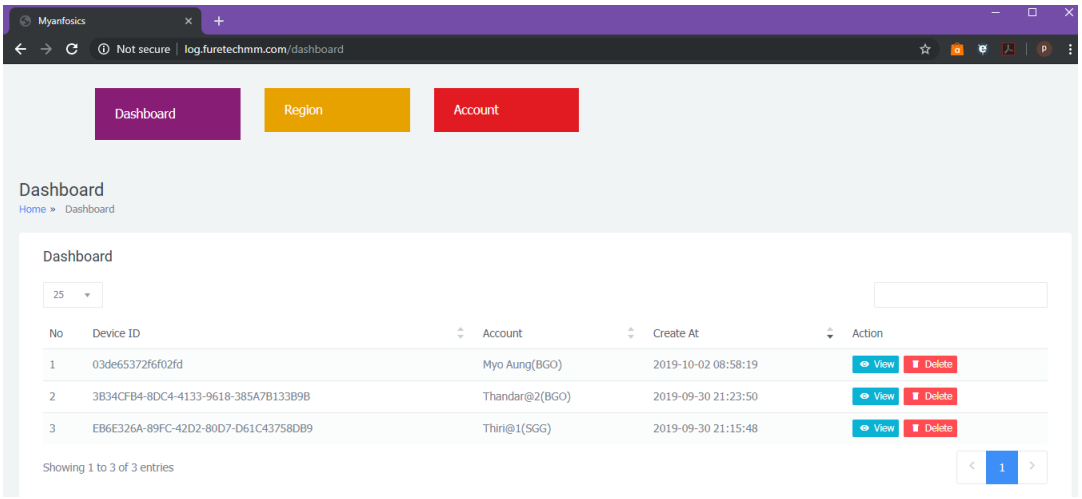

Figure 5.23 Device Logs in Server

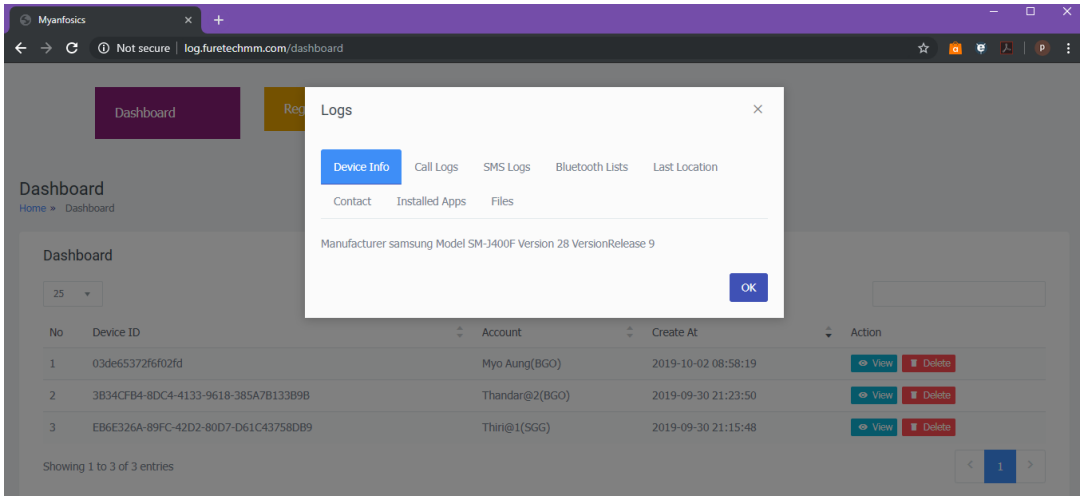

Figure 5.24 Device Information in Server

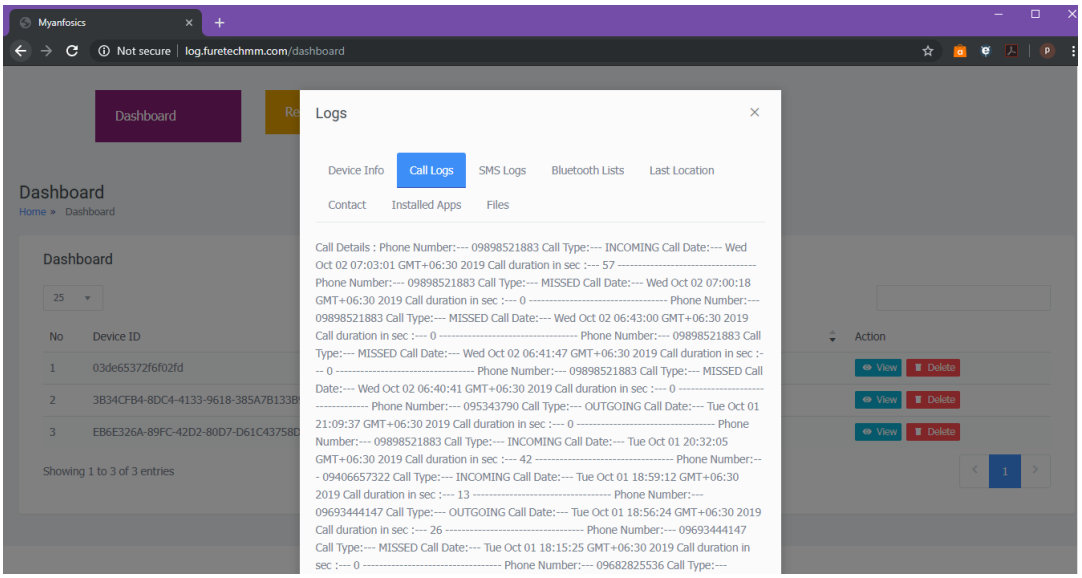

Figure 5.25 Call Logs in Server

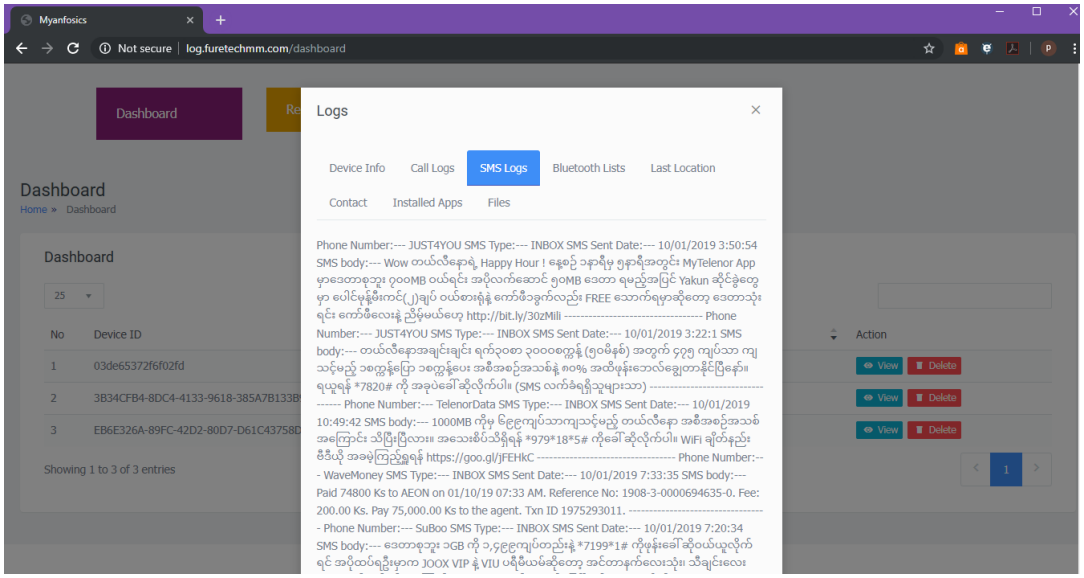

Figure 5.26 SMS Logs in Server

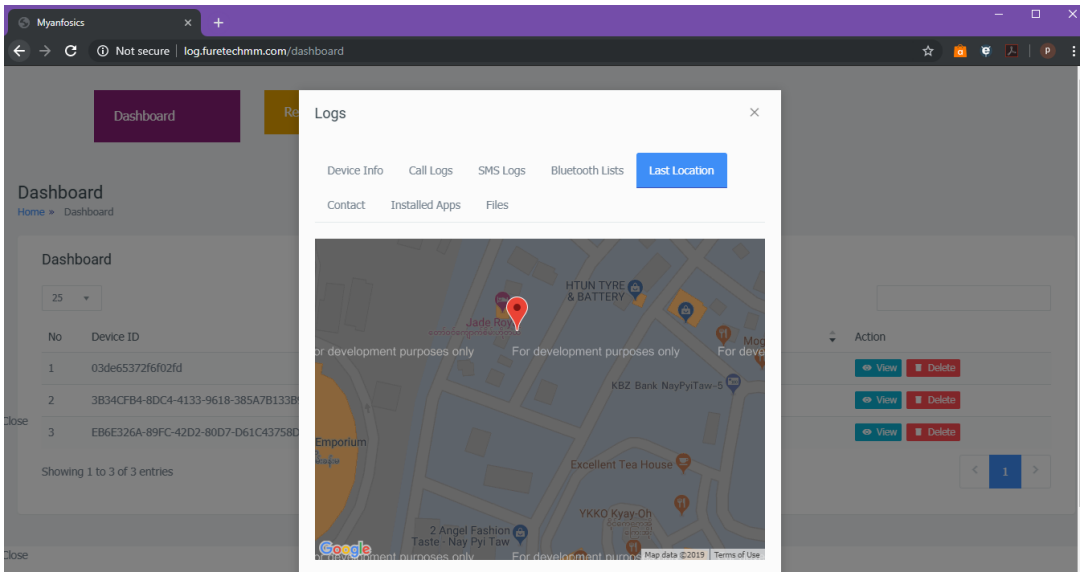

Figure 5.27 Location Logs in Server

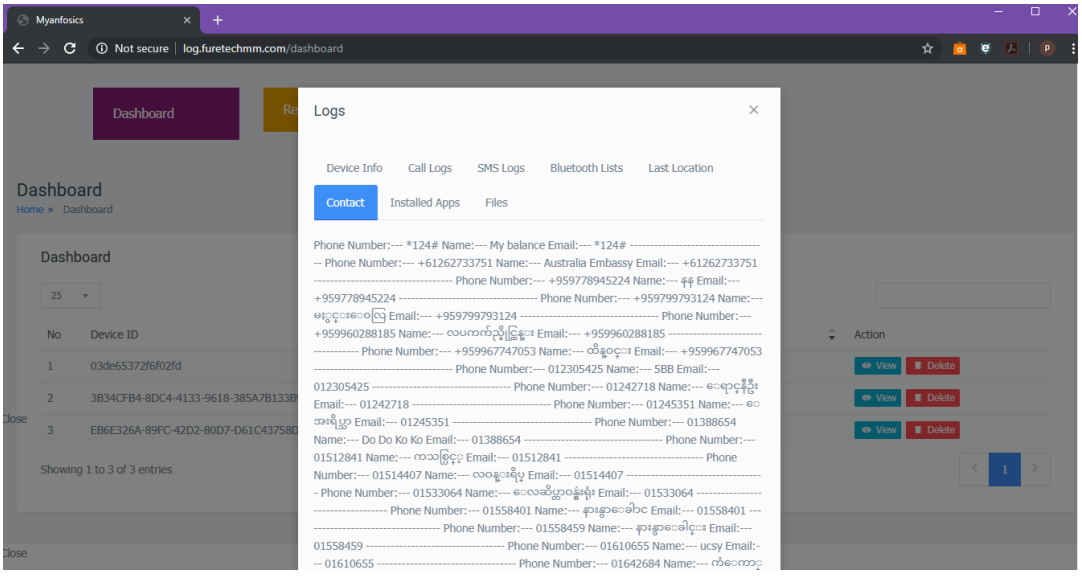

Figure 5.28 Contacts Logs in Server

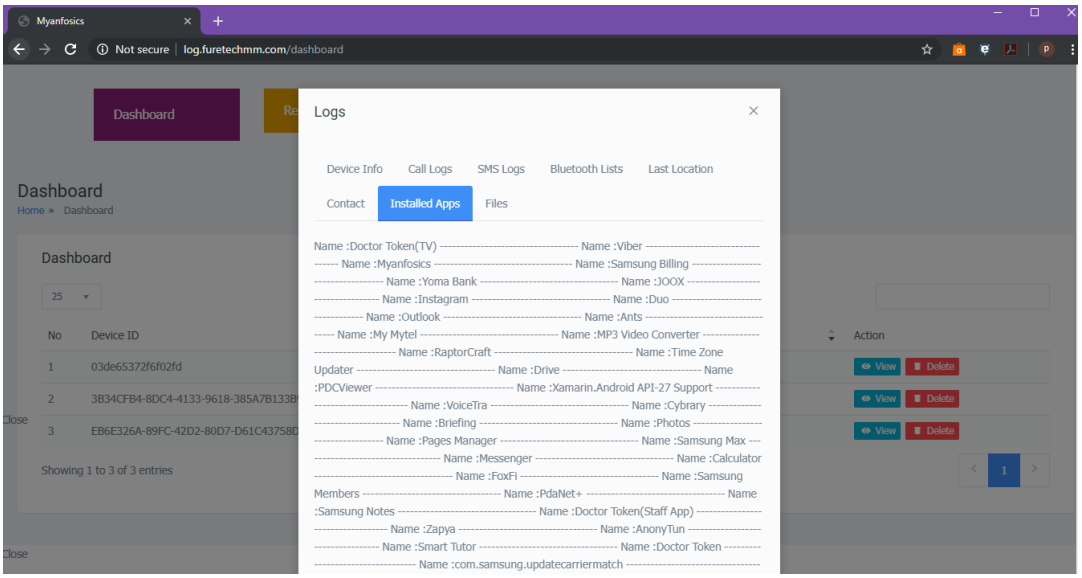

Figure 5.29 Installed Apps Logs in Server

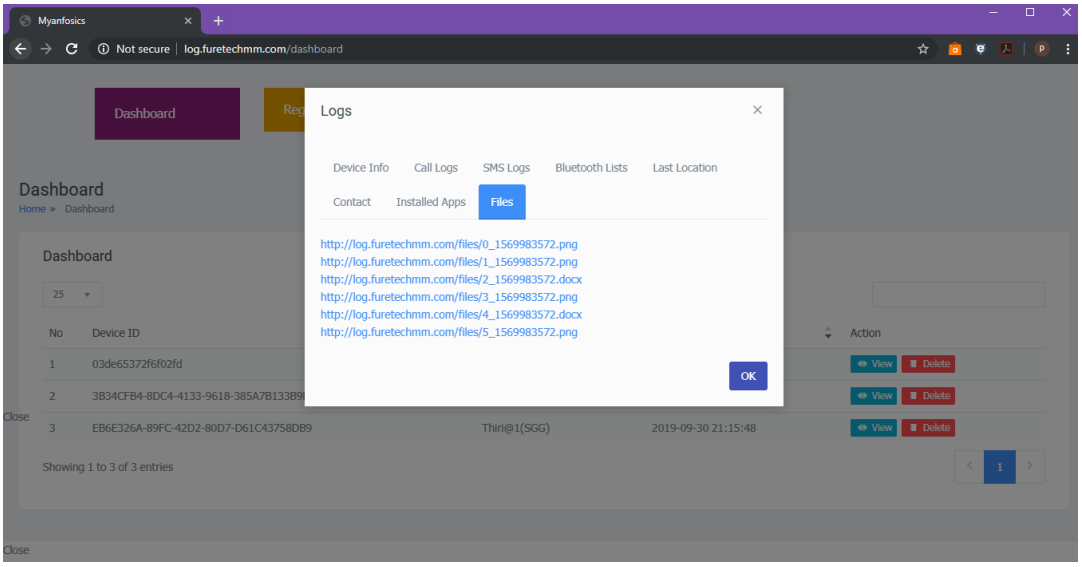

Figure 5.30 Files Logs in Server

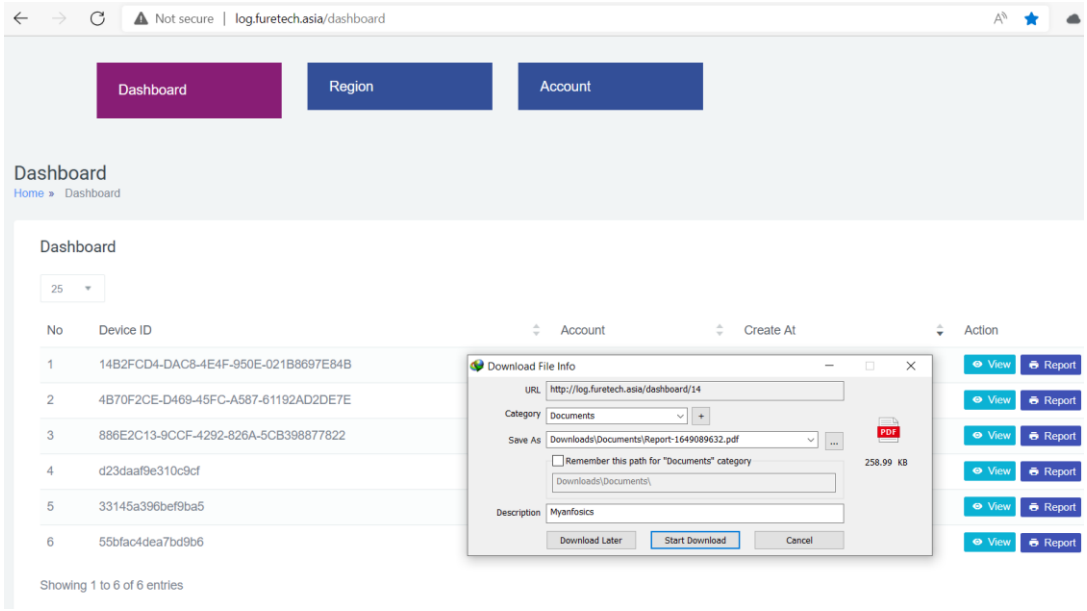

Figure 5.31 Report File Downloading in Server

This part is one of the important things for forensics investigation process. MYANFOSICS tool provides reporting feature that generate the report pdf file. In Main Report, it contains four subtitle reports – (a) Device Information, (b) Call Logs, (c) SMS Logs, (d) Contact List, (e) Location History, (f) Installed Applications and (g) Media files are shown in figure 5.32 to figure 5.38.

Myanfosics

2022-01-09 20:14:57

Device Info

Manufacturer	Model	Version	VersionRelease
VersionRelease	SM-J400F	28	9

Figure 5.32 Device Information in Report File

Call Logs

Phone Number	Call Type	Call Date	Duration
09779921571	MISSED	Wed Sep 29 11:57:19 GMT+06:30 2021	0
5557	MISSED	Fri Sep 24 19:03:51 GMT+06:30 2021	0
09979046325	MISSED	Thu Sep 23 11:03:23 GMT+06:30 2021	0
09979046325	MISSED	Thu Sep 23 10:50:39 GMT+06:30 2021	0
09694653027	MISSED	Mon Sep 20 11:25:18 GMT+06:30 2021	0
09779921571	OUTGOING	Tue Sep 14 21:43:17 GMT+06:30 2021	0
09698321177	OUTGOING	Tue Sep 14 17:11:38 GMT+06:30 2021	0
09698321177	OUTGOING	Mon Sep 13 21:12:49 GMT+06:30 2021	4
5556	MISSED	Sun Sep 12 20:26:20 GMT+06:30 2021	0
09698321177	OUTGOING	Sat Sep 11 17:31:07 GMT+06:30 2021	0
09694653027	MISSED	Tue Aug 31 20:01:41 GMT+06:30 2021	0
09898521883	OUTGOING	Tue Aug 31 12:37:32 GMT+06:30 2021	0
09698321177	OUTGOING	Tue Aug 24 09:08:23 GMT+06:30 2021	0
09698321177	OUTGOING	Mon Aug 23 16:53:33 GMT+06:30 2021	0

Figure 5.33 Call Logs in Report File

SMS Logs

Phone Number	SMS Type	SMS Sent Date	Message
Google	INBOX	10/12/2021 11:49:25	G-212234 is your Google verification code.
+959764246062	INBOX	10/09/2021 10:22:50	ကိုညီညီ thurathanlwin@icloud.com
+959668580712	INBOX	10/08/2021 2:47:31	Coffeebarမှာ ဘာလိုလဲ
+959258712028	INBOX	10/04/2021 4:53:3	Meeting ဆရာ
09691996236	INBOX	09/29/2021 1:13:51	bro ရေ SOC လား SIEM လား sharing ပို့ပေးပါဦး

Figure 5.34 SMS Logs in Report File

Contacts

Phone Number	Name
*124#	My balance
+61262733751	Australia Embassy
09421056549	ကို ဘိုဘို ကား
09451107273	ကိုစိုးနိုင်
095070547	ကိုနေ
019666141	ဝိတိုရိယ
012305425	5BB
09689802016	ဆရာကား
09723953361	ဖိုးသား
01388654	Do Do Ko Ko
09779921571	အပါး
018605088	MRT

Figure 5.35 Contact List in Report File

Location

Latitude, Longitude
16.8875788,96.1238639

Page - 122

Figure 5.36 Location History in Report File

Install App

Names
Carrier Matching
Myanfosics
Ads
Voice Recorder
Samsung Checkout
Yoma Bank
Seesaw Class
Outlook
QuickSupport Add-On AOSP 7
Time Zone Updater
WavePay
TikTok
Briefing
Samsung Max
Messenger
Calculator
Samsung Notes
Smart Tutor
com.samsung.updatecarriermatch
Gboard

Figure 5.37 Installed Application List in Report File

Files

Links
http://log.furetechmm.com/47
http://log.furetechmm.com/files/0_1569983572.png
http://log.furetechmm.com/files/1_1569983572.png
http://log.furetechmm.com/files/2_1569983572.docx
http://log.furetechmm.com/files/3_1569983572.png
http://log.furetechmm.com/files/4_1569983572.docx
http://log.furetechmm.com/files/5_1569983572.png
http://log.furetechmm.com/files/0_1574586868.pdf
http://log.furetechmm.com/files/1_1574586868.xlsx
http://log.furetechmm.com/files/2_1574586868.jpeg
http://log.furetechmm.com/10
http://log.furetechmm.com/15
http://log.furetechmm.com/9
http://log.furetechmm.com/2019-10-02 09:02:52
http://log.furetechmm.com/2019-10-02 09:02:52

Figure 5.38 File List in Report File

5.9 Case Scenario

Company Tango Mike's IT department got a tip regarding employee misconduct. One of the users might have violated the company's policy by installing different illegal applications and spreading the photo that it includes information for company’s new project by using social media and other stuff. The project information security standard is secret. The IR team managed to respond immediately and take a full forensic image of the user's system. After that they seized computers and mobile phone devices and searched to responsible who is capture and send. To make sure an investigator gathered enough information from computer and mobile phone devices as follow:

- Profiling the system used
- Analyzing the Windows Registry: SAM HIVE
- Analyzing user search queries
- Analyzing recently used DOCS
- Analyzing browser history
- Analyzing Prefetch files
- Analyzing Thumbcaches
- Checking for user libraries
- Analyzing Jump lists and Libraries
- Analyzing Windows Registry Artifacts to Locate used USB Devices
- Exporting mobile phone device profile, contact list, call log, SMS log, Bluetooth log, browser history, installed applications, media and file list.

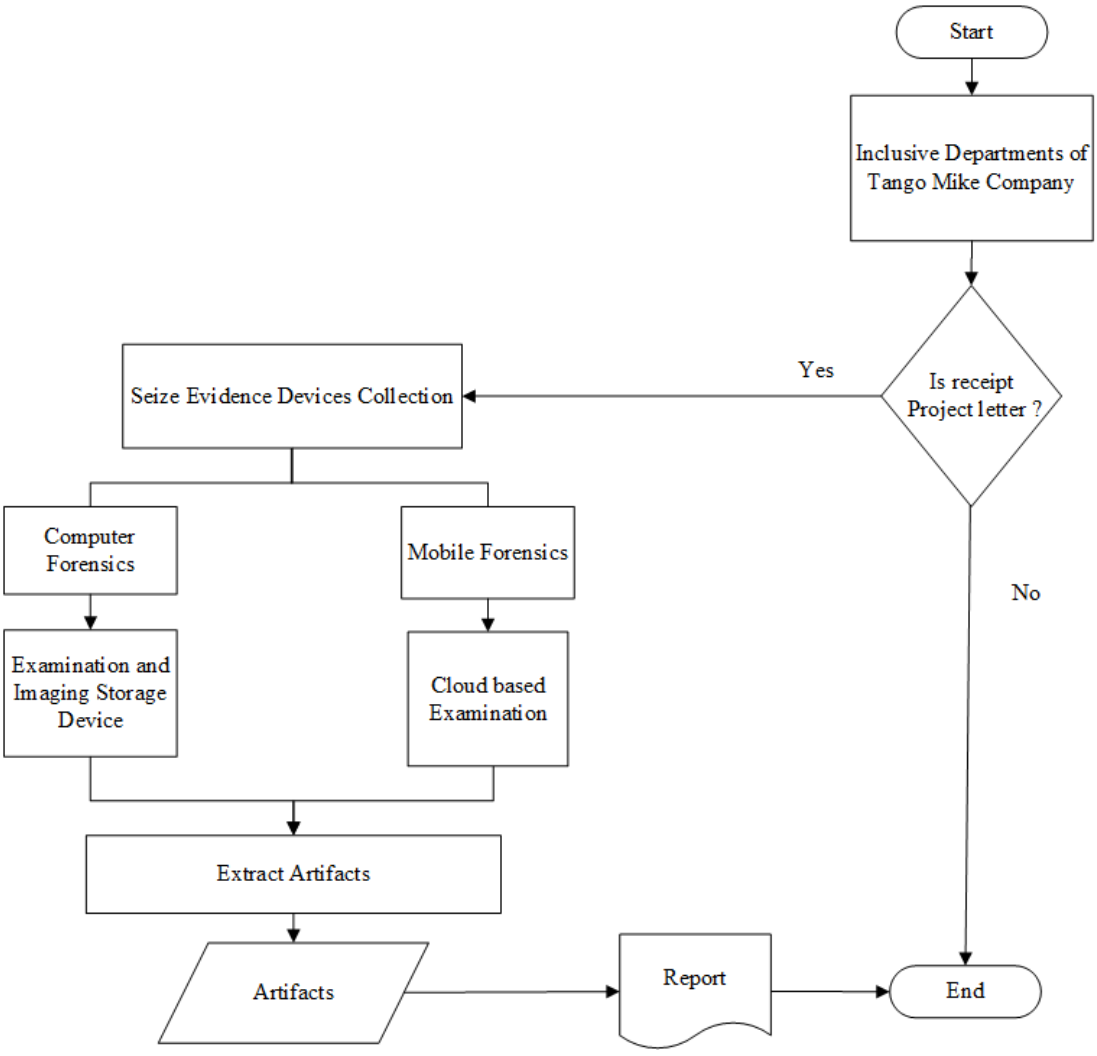

Figure 5.39 Forensics Investigation Process Flow for Case Scenario

After they have done investigation process by the figure 5.39, they can extract the artifacts and the report in time with MYANFOSICS tool suit. According to the clues and timeline analysis, they can arrest the criminal.

5.10 Comparison of Some Forensics Tools and MYANFOSICS System

In this section, the comparison of some forensics tools and MYANFOSICS tool suite will be described. This comparison is based on the features of MYANFOSICS to measure the performance. It analyzed on seven main features, namely, collection, examination and analysis, management, reporting, computer and mobile operating systems, open source and export data.

It is set to 'Yes', 'No', depending on which feature the tool supports as reported in Table 5.3 that have been implicated in research. As shown in Table 5.3, the MYANFOSICS tool are evaluated with Encase, Autopsy, Belkasoft, UFED (Demo) and FTK Imager free version.

Table 5.3 Comparison of Some Forensics Tools and MYANFOSICS System

		Myan46	Encase	Autopsy	Belkasoft	UFED	FTK Imager
Data Collection	Volatile acquisition	Yes	Yes	No	No	Yes	No
	Logical acquisition				Yes		Yes
	Physical acquisition				Yes		Yes
Examination and Analysis	File Signature	Yes	Yes	Yes	No	No	No
	Keyword Search	Yes	Yes	No	Yes	Yes	No
	Integrity	Yes	Yes	No	Yes	Yes	Yes
Management	Tamper Protection	Yes	Yes	No	No	No	No
Reporting	Live and Static	Yes	Yes	Yes	Yes	Yes	No
Open Source		Yes	No	No	No	(Demo)	(free version)
Windows, Android and iOS		Yes	Yes	No	No	No	No
Export Data		USB/ TCP	USB/ TCP	USB	USB/ TCP	USB	USB

5.10 Chapter Summary

This chapter describes the implementation of the applicable dynamic forensics investigation via client-server architecture with MYANFOSICS system. And the experimental results of this system are also presented in this chapter. In addition, the comparison of some forensics tools and the MYANFOSICS tool suite was demonstrated. The next chapter describes the conclusion of this study, some limitations, and future work.

CHAPTER 6

CONCLUSION AND FURTHER EXTENSION

Cyber-attacks happen on all types of organizations and individuals. To effectively protect systems from exploitation of vulnerabilities, it is a necessity to further comprehend all the current threats and how they exploit the current vulnerabilities.

6.1 Conclusion

In this research, an applicable process flow is presented for Cybercrime Forensics Investigation in Myanmar. This process flow can even support non-technical person well handle for Cybercrime Forensics Investigation in Myanmar. This process flow can support Cybercrime investigator to get the must to do list and facing decision choice for possible different environments. This process flow is based on the standard process flow from NIST and employed more efficient, simple and effective stages. Especially, the implementation of the process flow starting from the crime scene until the reporting process to court has been done for our country, Myanmar, flexibly. In this workable process flow has been proposed for the forensics investigation on Windows and Mobile systems which consists of six stages. They are (1) Case Confirmation, (2) Scope Determination, (3) Requirement Readiness, (4) Examination and Imaging, (5) Extraction and Analysis, (6) Reporting and Review.

A detailed analysis framework for Examination and Imaging stage was presented. It is divided into two main parts – Live Forensics and Static Forensics because if the investigator does not notice the Live Forensics, the data on memory can be easily lost. This framework focused on not only the technical view but also the policies and rules for investigation. Evidences are the needle in the haystack. Therefore, this framework and process flow assist for seizing relevant and meaningful evidence and reduces or saves time and cost consuming.

It is from existing gaps that this framework and process flow that will provide guidance in digital forensics processes, particularly in developing countries like Myanmar. New forensic challenges arise with the introduction of newly released and latest operating systems. While on one hand, these newly released versions of Windows

are aimed at making things easier for users, many of the functions. Cyber-attacks happen on all types of organizations and individuals. It is important to train forensics investigators cannot be compromised and setting up of more forensics labs.

Finally, an applicable tool (MYANFOSICS) with many useful features has been proposed that would support the analysis framework. It consists of four main parts – (i) data acquisition and collection, (ii) examination (iii) reporting, and (iv) management process. This research discussed the process flow and framework for cybercrime forensics investigation. The improvement of this tool with IoT and other processes or features will be continued. Therefore, it is hoped that this research work can effectively support in cybercrime investigation in Myanmar.

6.2 Benefits of the Research

This research provides general-purpose open source computer forensic analysis open source tool [MYANFOSICS] that are rapidly been used for modern-day forensic investigation. The framework includes various strategies for optimizing and managing evidential data, managing and need for the due process of the evidence gathering. The forensics tool (MYANFOSICS) was presented.

There are basically some benefits why so much research and effort has been made by doing the forensics investigation process.

- This system is developed for own tool because of our country necessary due to environmental factors.
- It is not only a forensics tool in investigation process, but also an applicable tool which is easy to apply for some of buffer zone in Myanmar.
- It is useable forensics tool for Myanmar in Cybercrime investigation because of the Sanction.
- It is efficient tool that it reduces the cost for Initial, Annual and Training of the Commercial and License tool.
- It is protective tool that it can give secure more than other countries developed tools because of privacy.
- It is reliable tool that is easy to modify and support flexible.

- It is effective tool that can be user friendly.

Although some commercial tools provide the entire life cycle of forensics investigation, they are not only expensive both initial fees and annual fees but also breach data for privacy and security. This tool is adaptable and can extend new features.

6.3 Limitations of the Research

Although this research is done to fulfil the requirement as far as possible, there is some limitations and still need to improve. Especially, Since Myanmar is a developing country, too much practical experiments cannot be supported with related materials on this research. Thus, the experiments are only done on a few popular brands for testing devices. In this day and age, our country is just a developing country and most of people are not familiar with using the modern communications system and digital devices. The rapid increase of smart technologies and Internet usage creates new attack surfaces for cybercrime, this present work still needs to develop. However, this system has some weakness because it does not consider the sense of specific and deeply analysis for cybercrime forensics investigation.

6.4 Further Extension

There are some challenging parts beyond the current proposed work. As the future work, it is necessary to collect the IoT devices evidence from the crime scene. The IoT devices are gradually widespread use in the modern technology. Moreover, there is a need the recovering the deleted files from victim's devices. In addition, the feature of malware analysis, reverse engineering and others will be carried out in the future.

LIST OF ACRONYMS

AC	Alternating Current
ADS	Active Directory Services
AFF	Advanced Forensics Format
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
BMP	Bitmap
BOF	Buffer Overflow
CC	Creative Commons Attribution license
CD	Compact Disc
CPU	Central Processing Unit
CMD	Command Line Interface
CNA	Computer Network Attack
CNE	Computer Network Exploitation
CSI	Crime Scene Investigator
DBMS	Database Management System
DF	Digital Forensics
DFR	Digital Forensics Readiness
DFRS	Digital Forensics Readiness Schema
DHCP	Dynamic Host Configuration Protocol
DLL	Dynamic Link Library
DMS	Document Management System
DOC	Microsoft Word document
DOCX	Newer version of Microsoft Word document

DVD	Digital Video Disc
EOF	End Of File
EWF	Expert Witness Format
exFAT	Extensible File Allocation Table
EXE	Executable
EXIF	EXchangeable Image Format
FAT32	File Allocation Table32
FTK	Forensic Toolkit
GB	Gigabyte
GMT	Greenwich Mean Time
GPS	Global Positioning System
GUI	Graphical User Interface
GUID	Globally Unique Identifier
HDD	Hard Disk Drive
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
ICT	Information Communication Technology
ID	Identification
IDIF	Includes Protective Mechanisms to Detect Changes from the Source Image Entity to the Output Form
IEIF	Encrypts Disk Image
IRBF	Non-compressed Form
iOS	iPhone Operating System
IOT	Internet of Thing
IP	Internet Protocol

IR	Incident Response
IT	Information Technology
J2SE	Java 2 Standard Edition
J2EE	Java 2 Enterprise Edition
JDK	Java Development Kit
JFIF	JPEG File Interchange Format
JPEG	Joint Photographic Experts Group
JS	JavaScript
JSON	Javascript Object Notation
KB	Kilobyte
MAC	Media Access Control
MB	Megabyte
MD 5	Message-digest Algorithm
MFT	Master File Table
MRU	Most Recently Used
MSDN	Microsoft Developer Network
NetBIOS	Network Basic Input/output System
NICs	Network Interface Controllers
NIST	National Institute of Standards and Technology
NTFS	New Technology File System
OLE	Object Linking and Embedding
OS	Operating System
PDF	Portable Document Format
PE	Portable Executable Format
PNG	Portable Graphics Format

PPPT	PowerPoint Presentation
PyFlag	A General Purpose, Open Source, Forensic Package
RAM	Random-access Memory
RDP	Remote Desktop Protocol
reloc	Relocation
RID	Relative Identifier
rsrc	Resource
SAM	Security Account Manager
sgzip	A Free and Open Source Algorithm for File Compression
SIDs	Security Identifiers
SHA	Secure Hashing Algorithm
SIM	Subscriber Identity Module Card
SMS	Short Message Service
TB	Terabyte
TIFF	Tagged Image File Format
UAC	User Account Control
UNC	Universal Naming Convention
URI	Universal Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTC	Universal Time Coordinated
VSS	Volume Shadow Copy Service
XLS	Microsoft Excel Spreadsheet File
XML	Extensible Markup Language

AUTHOR'S PUBLICATIONS

[P1] Tin Maung Maung and Mie Mie Su Thwin, University of Computer Studies, Yangon Myanmar, "**Proposed Effective Solution for Cybercrime Investigation in Myanmar**", The International Journal of Engineering and Science (IJES), Volume 6, July, 2017.

[P2] Tin Maung Maung and Mie Mie Su Thwin, University of Computer Studies, Yangon Myanmar, "**Proposed Applicable CCFIM Framework for Cybercrime Forensics Investigation in Myanmar**", ICCA 2017, International Conference, University of Computer Studies, Yangon Myanmar.

[P3] Tin Maung Maung and Mie Mie Su Thwin, University of Computer Studies, Yangon Myanmar, "**The Threats of Cyberspace and Utilization of Open Source Forensics Tool for Cybercrime Investigation in Myanmar**", CSTD 2017, Defence Services Academy, Pyin Oo Lwin, 1st November 2017.

[P4] Tin Maung Maung and Mie Mie Su Thwin, University of Computer Studies, Yangon Myanmar, "**HACKFOSICS: Forensics Tool for Extract Live Remnant Data and Examine Dead Artifact**", 13th BWCCA 2018, Tunghai University, Taichung, Taiwan, SCI Conference.

[P5] Tin Maung Maung and Mie Mie Su Thwin, University of Computer Studies, Yangon Myanmar, "**Applicable Dynamic Forensics Investigation via Client-Server Architecture with Myanfosics**", 13th IMIS 2019, University of Technology Sydney, NSW, Australia, Springer Book Series, Advances in Intelligent Systems and Computing.

BIBLIOGRAPHY

[1] W. G. Kruse and J. G. Heiser, “Computer Forensics: Incident Response Essentials”, 1st ed., Addison Wesley, 2002.

[2] M. Reith, C. Carr, and G. Gunsch, “An examination of digital forensic models”, IJDE, vol. 1, issue 3, 2002.

[3] Brendan Choi, "Introduction to Python Network Automation", Springer Science and Business Media LLC, 2021.

[4] Mohd Taufik Abdullah, Ramlan Mahmod, Abdul Azim Ab. Ghani, Mohd Zain Abdullah, and Abu Bakar Md Sultan, “Advances in Computer Forensics”, IJCSNS V8 N2, 2008, Malaysia.

[5] Sundresan Perumal, “Digital Forensic Model Based on Malaysian Investigation Process”, IJCSNS V9 N8, 2009, Malaysia.

[6] Ed Hild, "Building a Presentation Server-Side within a Web Part", Pro SharePoint 2010 Solution Development, 2010.

[7] Ahmed Hasswa, Hossam Hassanein, "Managing Presence and Policies in Social Network dependent systems", IEEE Local Computer Network Conference, 2010.

[8] A. Agarwal, M. Gupta, S. Gupta, and S. C. Gupta, “Systematic digital forensic investigation model”, IJCSS, vol. 5, issue 1, pp. 118-131, 2011.

[9] Obwaya Mogire, “Digital Forensics Framework for KENYAN Courts of Laws”, 2011.

[10] Yunus Yusoff, Roslan Ismail and Zainuddin Hassan, “Common Phases of Computer Forensics Investigation Models”, IJCSITvol. 3, no. 3, 2011.

[11] "Advances in Network Security and Applications", Springer Science and Business Media LLC, 2011.

[12] Abdelmajid, Nabih T.(Hossain, M. Alamgir, Shepherd, Simon and Walied, Khalid), "Innovative Location Based Scheme for Internet Security Protocol. A proposed Location Based Scheme N-Kerberos Security Protocol Using Intelligent Logic of Believes, Particularly by Modified BAN Logic.", University of Bradford, 2011.

[13] Chen, Guangxuan, Yanhui Du, Panke Qin, and Jin Du, "Suggestions to digital forensics in Cloud computing ERA", 2012 3rd IEEE International Conference on Network Infrastructure and Digital Content, 2012.

[14] Chen, Guangxuan, Yanhui Du, Panke Qin, and Jin Du. “Suggestions to digital forensics in Cloud computing ERA”, 2012 3rd IEEE International Conference on Network Infrastructure and Digital Content, 2012.

[15] Gianni Fenu and Fabrizio Solinas, “Computer Forensics Investigation an Approach to Evidence in Cyberspace”, 2013, Italy.

[16] Esan P. Panchal, “Extraction of Persistence and Volatile Forensics Evidences from Computer System”, International Journal of Computer Trends and Technology (IJCTT)-volume Issue5-May 2013.

[17] Rabil Shafique Satti and Fakeeha Jafari, “Domain Specific Cyber Forensic Investigation Process Model”, Journal of Advances in Computer Networks, Vol. 3, No.1, March 2015.

[18] Ahmad Luthfi and Yudi Prayudi, “Process Model of Digital Forensics Readiness Scheme (DFRS) as a Recommendation of Digital Evidence Preservation”, IEEE, 2015.

[19] Gyu-Sang Cho, “NTFS Directory Index Analysis for Computer Forensics,” IEEE, 2015.

[20] Lei Chan, Lanchuan Xu, Xiaohui Yuan and Narasimha Shshidhar,” Digital Forensics in Social Networks and the Cloud,” IEEE, 2015.

[21] Shams Zawoad and Ragib Hasan, “FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things,” IEEE, 2015.

[22] Yudi Prayudi Ahmad Ashari, and Tri K Priyambodo, “A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia”, 2015, Indonesia.

[23] Jia-Rong Sun, Mao-Lin Shih, and Min-Shiang Hwang, “A Survey of Digital Evidences Forensic and Cybercrime Investigation Procedure”, IJNS vol. 17, No.5, 2015.

[24] Fu-Hau Hsu, Min-Hao Wu, Syun-Cheng Ou, Shiuh-Jeng Wang, "Data concealments with high privacy in new technology file system", The Journal of Supercomputing, 2015.

[25] Harlan Carvey, "Case Studies", Elsevier BV, 2016.

[26] Tony Knutson and Richard Carbone, “Filesystem Timestamps: What Makes Them Tick?” GIAC GCFA Gold Certification 2016.

[27] Mandeep Kaur, Navreet Kaur, and Suman Khurana, “A Literature Review on Cyber Forensic and its Analysis tools”, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 1, 2016.

[28] Tang Ling, “The Class of Information Crime and Computer Forensics”, Advances in Social Science, Education and Humanities Research (ASSEHR), volume 75, 2016.

[29] Nihad Ahmad Hassan, Rami Hijazi. “Data Hiding Forensics”, Elsevier BV, 2017.

[30] Urvashi Sharma Mishra, “Application of Cyber Forensics in Crime Investigation”, International Journal of Research and Analytical Reviews (IJRAR), volume 5, Issue 3, 2018.

[31] Bhupendra Singh, Upasna Singh. “Program execution analysis in Windows: A study of data sources, their format and comparison of forensic capability”, Computers & Security, 2018.

[32] Nurul Haswani Saiman and Mazura Mat Din, “A Generic Digital Forensic Business Model: Malaysia as Case Study”, International Journal of Innovative Computing 8(1) 21-26, 2018.

[33] Ivans Kigwana, H.S. Venter, “A Digital Forensic Readiness Architecture for Online Examinations”, South African Computer Journal (SACJ) 30 (1), 2018.

[34] Xiaodong Lin, "Introductory Computer Forensics", Springer Science and Business Media LLC, 2018.

[35] Mohammed I. Alghamdi , “Digital forensics in cyber security - recent trends, threats, and Opportunities”, Periodicals of Engineering and Natural Sciences, Vol. 8, No. 3, 2020.

[36] Arafat Al-dhaqm, Shukor Abd Razak, Richard Adeyemi Ikuesan, Victor R. Kebande and Kamran Siddique, “A Review of Mobile Forensic Investigation Process Models”, IEEE Open Access Journal, Volume 8, 2020.

[37] Bhawna Narwal and Nimisha Goel, “A Walkthrough of Digital Forensics and its Tools”, Test Engineering and Management Journal, 2020.

[38] Haris Iskandar Mohd Abdullah, Muhammad Zulhusni Mustaffa, Fiza Abdul Rahim, Zul-Azri Ibrahim et al, "Smart Grid Digital Forensics Investigation Framework", 2020 8th International Conference on Information Technology and Multimedia (ICIMU), 2020.

[39] Timothy McIntosh, Paul Watters, A.S.M. Kayes, Alex Ng, Yi-Ping Phoebe Chen, "Enforcing situation-aware access control to build malware-resilient file systems", Future Generation Computer Systems, 2021.

[40] "Advances in Digital Forensics XVII", Springer Science and Business Media LLC, 2021.

[41] Brian Carrier, “File System Forensic Analysis”, 2005, USA.

[42] Steve Anson, "Applied Incident Response", Wiley, 2019.

[43] Ali Hadi, “Digital Forensics Courses”, www.ine.com.

[44] www.medium.com.

[45] www.ijert.org.

[46] www.researchgate.net.

[47] www.slideshare.net.

[48] www.lowmanio.co.uk.

[49] www.sans.org.

[50] yashgorasiya.medium.com.

[51] www.dfir.training.

[52] www.github.com.

[53] www.coursehero.com.

[54] blogs.technet.com.

[55] www.ijrar.com.

[56] www.ijdacr.com.

[57] www.scribd.com.

[58] www.mecs-press.org.

[59] www.aspfree.com.

[60] www.dfir.training.

[61] www.derebek.com.

[62] www.2brightsparks.com.

[63] www.isaca.org.

[64] www.bellamyjc.fr.

[65] www.ijarcce.com.