

KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY

KUMASI

**ENHANCING DIGITAL FORENSIC MODEL USING DESKTOP
VIRTUALIZATION.**

BY:

EBENEZER QUAYSON (MPHIL. COMPUTER SCIENCE)

PG1139913

THIS THESIS SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE

KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY

IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF PHILOSOPHY IN COMPUTER SCIENCE

DEPARTMENT OF COMPUTER SCIENCE, COLLEGE OF SCIENCE.

MAY 2016.

DECLARATION

I, do hereby declare that this submission is my own work and that, to the best of my knowledge and beliefs, it contains no material previously published by another person nor material which has been accepted for the award of any degree of the University, except where due acknowledgement has been made in the text.

Quayson Ebenezer

(PG1139913)

(Student's Name & ID) (Signature) (Date)

Certified by:

Dr. M. Asante

(Supervisor) (Signature) (Date)

Dr. J. B. Hayfron - Acquah

(Head of Department) (Signature) (Date)

ACKNOWLEDGEMENTS

I wish to acknowledge the Lord Almighty for the grace given me by Him to come this far in my course of study. In spite of all the difficulties I passed through during my stay in school and the challenges I encountered while undertaking this project work. I have been able to finish successfully by his grace.

My sincere thanks and appreciation goes to Dr. M. Asante who supervised my work diligently to give me the direction I needed and also to ensure I did a great job in this project work.

I am truly grateful to Dr. Osei Adjei and Mr. K. O. Peasah for the unflinched support and guidance in helping me assume the needed confidence understanding and courage needed to execute this project work.

I also want to express my heartfelt to my family and loved ones for their immense financial and moral support. I thank everyone who gave their comments, criticisms, and positive feedbacks on the project. Your feedback has given me great insight and has helped me to carry out this research.

To everyone who in diverse ways helped or contributed towards the successful completion of the project, I say, God richly bless you.

DEDICATION

I dedicate this work to the Lord Almighty and my dear parents.

KNUST



ABSTRACT

The internet and advanced technologies have been used as tools by criminals these days to perpetrate diverse forms of crime and the digital world is exploited to facilitate crimes which are mostly technology driven. The evidence of such crimes which are technologically driven are in digital form hence the need to employ techniques, procedures, and methodologies that are technology inclined to reconstruct events and uncover evidence that are admissible in court. Digital forensics therefore provides the investigative techniques, scientifically derived and proven methods for preserving, collecting, validating, identifying, analyzing, interpreting and presenting admissible digital evidence derived from digital source(s). The development of several forensics investigation models by digital forensic researchers are designed to provide a well-tailored, accurate and efficient means of acquiring, authenticating and analyzing digital evidence while ensuring the integrity and sanctity of the evidence to make it admissible in court of law. However, these models are not without some inherent shortfalls whilst majority of them seems not to cater for investigation processes or activities done on the virtual environment. Virtualization is a proven software technology that is rapidly transforming the hosting landscape and fundamentally changing the way that businesses compute. In this research, some digital forensic process models were reviewed, digital forensic investigative platform setup up on a virtual desktop environment to allow digital forensics investigations to be conducted on the virtual environment. The results of this implementations were recorded, analyzed and used to improve a digital forensic investigation process model.

TABLE OF CONTENTS

DECLARATION.....	ii
ACKNOWLEDGEMENTS.....	iii
DEDICATION.....	iv
ABSTRACT	v
LIST OF TABLES.....	x
LIST OF FIGURES	xi
LIST OF ABBREVIATION.....	xii
CHAPTER ONE	
1	INTRODUCTION
.....	1
1.1 Background of the Study	1
1 1.1.1.Digital Forensics	
4	
1.1.2 Virtualization	4
1.2 State of the problem	5
1.3 Problem Statement	
6	
1.4 Research Questions	
7	
1.5 Aims of the Research	7
1.6 Significance of Study	7
1.7 Project Scope	8
1.8 Project Motivation	8
1.9 Limitations of the Research	8
1.10 Organization of the thesis	9
1.11 Summary of Chapter	10

CHAPTER TWO	
11 LITERATURE REVIEW	
11	
2.1 Introduction	
11	
2.2 Digital Forensics in Perspective.....	11
2.2.1 Digital Forensics	12
2.2.2 Digital Evidence.....	13
2.2.3 Digital Data and Location	14
2.2.4 Key Elements of Digital Forensics Investigation	16
2.2.5 Digital Forensics Tools	18
2.3 Digital Forensics Models	19
2.3.1 Abstract Digital Forensics Model (ADFM, 2002)	20
2.3.2 The Enhanced Digital Investigation Process Model (EDIP)	21
2.3.3 Computer Forensics Field Triage Process Model (CFFTPM)	23
2.3.4 Generic Computer Forensics Investigation Process Model (GCFIPM)	25
2.3.5 An Integrated Digital Investigation Process (IDIP)	27
2.3.5.1 Discussion	
29	
2.3.6 Forensic Computing Models: Technical Overview	29
2.3.6.1 Discussion	
30	
2.4 Virtualization as a Technology	30
2.4.1 Hypervisor.....	32
2.4.2 Virtualization Techniques	
33	
2.4.3 Categories of Virtualization	35
2.4.4 Digital Forensics on a Virtual Machine	38
2.4.5 A virtual digital forensics laboratory	39
2.4.6 Analyzing the impact of a virtual machine on a host machine	40
2.5 Summary	
41	

CHAPTER THREE	42
RESEARCH METHODOLOGY.....	42
3.0 Introduction	42
3.1 Research Strategy.....	44
3.2 Research Approach	46
3.3 Data Collection: Experiment and Observation	47
3.4 Implementation	48
3.4.1 Implementing the Virtual Desktop Environment	48
3.4.2 Selection of a Virtualization Solution	48
3.4.3 Installing Virtualbox	50
3.4.4 Setting up the Forensic Platform on the Virtual Machine	51
3.4.5 Conducting Digital Forensic Investigation	55
3.4.6 Forensic Imaging	56
CHAPTER FOUR	67
FINDINGS AND DISCUSSIONS	67
4.0 Experiment	67
4.1 Repetitive Hashing	68
4.2 Code listing for hashing the image file using md5 hash	68
4.3 Comparative study on the forensic tools	69
4.4 Proposed Forensic Model	70
4.5 Comparative Analysis	72
4.6 Conclusion	74
CHAPTER FIVE	75
CONCLUSION AND FUTURE WORK	75
5.0 Conclusion	75
5.1 Recommendations	76
5.2 Future Works	76

REFERENCES	78
------------------	----

KNUST



LIST OF TABLES

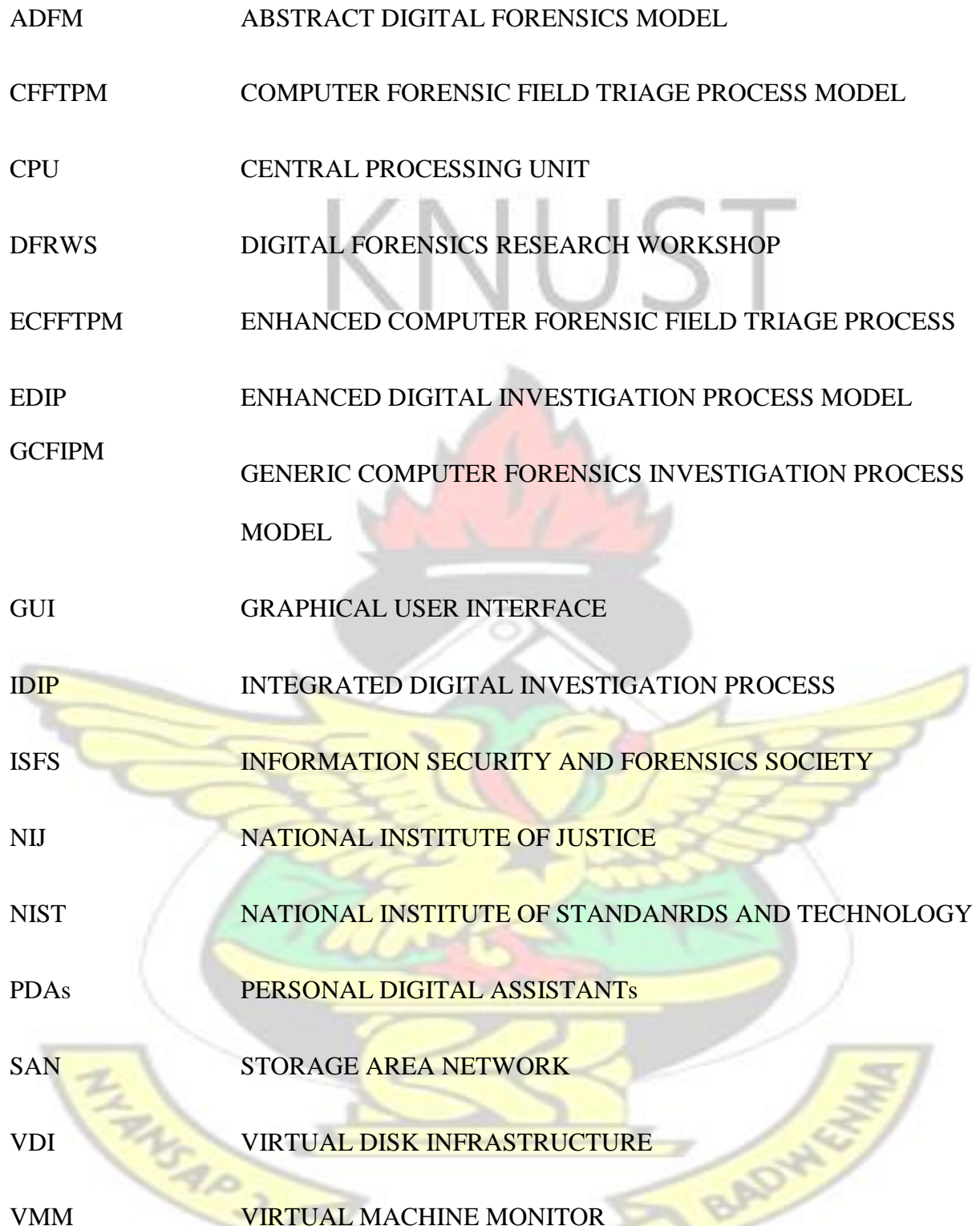
Table 3.1: Foremost command options and descriptions.....	61
Table 3.2: Scalpel command options and descriptions	64
Table 4.1: Comparative analysis of Foremost and Scalpel forensic tools	70
Table 4.2: Phases of some forensic process models	72
Table 4.3: Comparison of features of selected digital forensic models with the proposed	73



LIST OF FIGURES

Figure 3.1: Initial setup screen of VirtualBox Installer	50
Figure 3.2: Window of a newly installed VirtualBox	51
Figure 3.3: Virtual Machine creation screen.....	52
Figure 3.4: Window for creating VM Hard disk	53
Figure 3.5: VirtualBox Disk Image (VDI) screen	54
Figure 3.6: Virtual Hard Disk Infrastructure screen	54
Figure 3.7: Newly created Virtual Machine screen	55
Figure 3.8: Screen showing the recover1 directory	62
Figure 3.9: Screen showing the content of recover1 directory	62
Figure 3.10: Foremost Audit File.....	63
Figure 3.11: Scalpel configuration file	65
Figure 3.12: screen showing content of recover2 directory	66
Figure 4.1: The md5 hashing algorithm screen	68

LIST OF ABBREVIATION



ADFM	ABSTRACT DIGITAL FORENSICS MODEL
CFFTPM	COMPUTER FORENSIC FIELD TRIAGE PROCESS MODEL
CPU	CENTRAL PROCESSING UNIT
DFRWS	DIGITAL FORENSICS RESEARCH WORKSHOP
ECFTPM	ENHANCED COMPUTER FORENSIC FIELD TRIAGE PROCESS
EDIP	ENHANCED DIGITAL INVESTIGATION PROCESS MODEL
GCFIPM	GENERIC COMPUTER FORENSICS INVESTIGATION PROCESS MODEL
GUI	GRAPHICAL USER INTERFACE
IDIP	INTEGRATED DIGITAL INVESTIGATION PROCESS
ISFS	INFORMATION SECURITY AND FORENSICS SOCIETY
NIJ	NATIONAL INSTITUTE OF JUSTICE
NIST	NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
PDA _s	PERSONAL DIGITAL ASSISTANT _s
SAN	STORAGE AREA NETWORK
VDI	VIRTUAL DISK INFRASTRUCTURE
VMM	VIRTUAL MACHINE MONITOR

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

Advancement in technology and digital systems has to a large extent affected the modus operandi of executing activities and task as well as the human computer interactivity. This advancement in technologies and tools has brought about pervasive and ubiquitous forms of computing allowing individuals to interact and communicate from anywhere and everywhere. Indeed computing paradigm have changed greatly in recent times due to the advancement in technology.

Recent development shows that, an increasing number of people are using computers and devices with complicated and efficient computing capability. For example, one can communicate by sending and receiving electronic mail (e – mail) messages from a portable or handheld devices including mobile phones, PDAs or smart phones. Again, through digital networks such as the internet, one can engage other game players simultaneously in an online computer games or manage their individual finances as well (ISFS, 2004). This holistic acceptance and in – depth penetrative ability of digital devices and electronic related services commonly referred to as (e – services) allow everyone to interact with these technologies in diverse ways or the other. This is a clear indication of the fact that, the change in computing paradigms is not limited to technologies alone but to devices as well. There are proliferation of devices capable of storing, processing and transmitting digital data or information causing digital data to abound in diverse format and representations.

This emerging technologies though useful, has not only made execution of work easy and faster, it has also been employed as weapons by criminals to perpetrate diverse forms of crimes ranging from identity theft, credit card theft, fraud, denial of service attack, child pornography,

etc. These criminals use the technological devices as tools to commit those crimes or the technological devices are themselves targets of these crimes. Since these crimes are committed in digital environment where data are represented in zeros and ones, any digital footprints or traces of evidence may appear invisible to human eyes thereby necessitating the need to undertake a digital forensics investigation.

This implies most of this evidence will be represented in digital format which calls for effective and careful ability or means of extracting relevant digital evidence in a way to secure the value and integrity of the data. This buttresses the rationale for a careful, step – wise procedures for primarily gathering digital data and the need for computer forensics as a discipline. (ISFS, 2004).

Records shows that, within the past decades, an emerging pattern of crime or crime scenes has become predominant. These are crimes initiated and perpetrated within electronic or digital domains, particularly within cyberspace or internet enabled environment. The need to undertake investigations into crimes committed holistically or partially over the internet or other electronic media is a challenge Criminal justice agencies throughout the world are being confronted with. As part of the challenge also include the resources and procedures required to effectively locate, search for, and preserve the integrity of all types of electronic evidence. This digital evidence comprises of child pornographic images to encrypted data used to propagate a variety of criminal activities (Lee et al, 2001).

(Bem et al, 2008) argued that, like all crime, this new class of crime in which computer is used as a means or target requires reliable evidence for successful prosecution.

Digital forensics therefore emerged as a field of study and a response to combat the escalation of digital related crimes committed under the umbrella of anonymity. Perpetrators of these crimes employ computer system as the target of the crime or an instrument used to commit a

crime, or an evidential repository of a related crime. Digital forensics works date as far back as the early 1984 where the FBI laboratory together with other law enforcement agencies commenced the development of programs to undertake analysis of computer evidence. (Noblett et al, 2000).

The Digital Forensics Research Workshop (DFRWS, 2001) formally defined digital forensics as the use of scientifically derived and proven methods toward the collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

Computer forensic therefore helps in the administering of justice by helping investigators to gather and present valuable evidence admissible in the court of law. It also helps prosecutors to apply the right law in a given case under consideration. The sanctity and integrity of the investigative process or procedure used to acquire evidence herein referred to as digital evidence in a digital forensic investigation is very paramount thereby driving home the need to give a critical attention to the process or procedure used in the acquisition of the evidence. This notion is buttressed by (Yusoff et al, 2011) that, in undertaking a computer forensic investigation, the choice of process models or investigative procedure has a proportionate effect on the results of the investigation. Thus, selecting an inappropriate process models will eventually result in an insufficient or inadmissible evidence, missing one procedural step or even toggling any of the steps culminate in an inconclusive results; thereby giving rise to invalid interpretation. Digital evidences acquired in an unplanned or haphazard manner is likely to face the risk of being inadmissible in a competent court of law. This research looks at two

technologies, thus digital forensics and desktop virtualization and how to harness the capabilities of both technologies to result in effective and efficient investigations.

1 1.1.Digital Forensics

Digital forensics could be seen as the application of forensic science in a digital enabled environment to gather and preserve digital evidence as oppose to traditional forensics which gather and preserve evidential traces such as fingerprints as well as other physical artifacts with evidential value.

Digital evidence refers to an information or data of probative value to a digital forensics investigation which is either stored on, received or transmitted by an electronic device. (NIJ, 2008). Digital evidence has some inherent complexities making it delicate and fragile in nature. Hence its acquisition must be done through a well thought standardized and acceptable procedures so that its inherent probative value will be secured to ensure that it becomes admissible in any legal proceeding. Again, the proliferation of digital devices has caused digital evidence to in different format or representation as well as increased sources of digital evidence. In a digital forensic investigation, the following data are worth considering, active data (metadata, temporary files and communication data), residual data (slack space, backup data) and sources of data.

1.1.2 Virtualization

Virtualization hinges on the concept of partitioning, whereby a singular physical infrastructure such as storage disk, network and physical servers are logically divided into logical storage partitions, virtual network, and logical servers respectively. After the partitioning is done, each logical infrastructure runs independently with its set of instructions, and allocated resources including operating systems and application.

Virtualization therefore allows instances of multiple operating system to be executed simultaneously on a single computing system providing an avenue for decoupling hardware from the underlying operating system.

The virtual computer running inside the physical computer which is also known as the “guest” operating system coordinated by a hypervisor which may be referred to as Virtual Machine Monitor (VMM). The virtualization layer or system is sandwiched between the hardware and the guest. The VMM manages the guests’ use of the processor (CPU), memory, and storage enhancing the migration from one computing machine to another. An enhanced elucidation to harness the benefits of the decentralized as well as centralized deployments is virtualization.

Implementing virtualization technology lay off the cost overhead of procuring and maintaining one – to – one relationship between an application and an entire computer. With the aid of virtualization, several independent operating system may be installed to reside on a centralized hardware to control each application. With this infrastructure, advantages such as stability and security derived from a decentralized system is realized. (Keyman, 2012) Virtual desktops can provide a forensic platform which can be harnessed to undertake a digital forensics analysis processes. One of the advantages is the booting of a forensically acquired image in a virtual environment which does not require restoring unto the given hardware and operating system the forensic image of the existing system as pertained in the conventional method. Again, complementing forensic investigation with virtual environment technique can enhance the rate of execution and can be repeated where necessary. To enhance the distribution of workload in a big digital forensic case could be easily done by booting a forensic image into a virtual machine. This will aid a novice investigator to undertake a firsthand examination that may guide the professional investigator to determine the direction of the investigation.

1.2 State of the problem

A digital forensic investigative processes basically encompass the following; identifying the digital evidence, preserving the evidence as well as the examination and presentation of the digital evidence in order to ensure the admissibility of the evidence in a legal proceeding. This however, presents the need to choose the appropriate methodology, steps, procedures and tools so as to preserve the integrity and validity of the digital evidence.

In addition, the relevance of a digital evidence is a function of time hence the need for efficient and effective digital forensics investigation processes. This calls for the setting up of labs with sophisticated devices and high computing capabilities. Such setups requires huge capital investments and requisite skills to man the facility. Another challenge is the fact that, crime acts and investigation does not begin at the lab but rather at the crime scene. Therefore, the need arises for some immediate experiment to be done on the scene. Replicating the physical servers and other infrastructure all over is practically not feasible. Virtualization provides the technology to harness the power of this legacy infrastructure to ensure that preliminary investigation are properly done to ensure effective and efficient results.

In this project, relevant study of the virtual environments or virtual machines is done, a virtual desktop is setup or created, forensics investigation is conducted in a virtual desktop environments, some digital forensic models is reviewed or investigated and an improved digital forensic model using virtualization is proposed.

From the analysis of the problem, the problem statement derived is as follows

1.3 Problem Statement

Setup a virtual desktop environment to be used for undertaking a digital forensic investigation and use the resulting information as well as the concept of virtualization to improve a digital forensic model. This research work will also form the basis of future forensic lab development.

1.4 Research Questions

- i. How is digital forensic investigations conducted on a virtual desktop environment?
- ii. What edge does desktop virtualization provide in enhancing digital forensics investigations?
- iii. How useful is digital forensic investigation in a virtual environment compared to the conventional method?
- iv. In what ways can desktop virtualization be used to improve existing digital forensic model?
- v. What benefit will the research provide digital forensic investigators with respect to this technology?

1.5 Aims of the Research

- i. To demonstrate how digital forensic investigations could be conducted on a virtual desktop environment.
- ii. Identify the edge desktop virtualization provide in enhancing digital forensics investigations.
- iii. To propose the ways in which desktop virtualization may be used to improve existing digital forensic model.
- iv. To examine the benefit(s) digital forensic investigators derive with respect to this technology.

1.6 Significance of Study

The primordial drive of this research study is in tandem with the relevance of digital forensic investigation which gather, preserve, analyze and present digital footprints or evidence to combat crime. Digital related crime is on the ascendancy hence the need for digital forensic investigation.

Again, this research seeks to discover how virtualization technology can provide the platform for efficient digital forensic investigations. The result of the study will help improve and enhance digital forensic models used to undertake forensic investigation. The study will help identify how virtualization technology can help investigators especially the novice to acquire real time experience in digital forensics investigation while maintaining the integrity of the evidence.

1.7 Project Scope

Virtualization technology is a broad area which spans from storage virtualization, network virtualization, server virtualization, desktop virtualization, to application virtualization. However, this project focuses on desktop virtualization and digital forensic investigation conducted in a virtual desktop environment. The result of the study may be used to improve or enhance all digital forensic investigation model (CFFTPM).

1.8 Project Motivation

The need to find efficient and effective means of conducting forensic investigation to combat technological related crimes which are increasing so rapidly making the cyberspace an unsafe realm.

To contribute knowledge to digital forensic investigation in virtual environments which present some new and interesting areas for research.

1.9 Limitations of the Research

The research was carried out in a laboratory with a laptop with the following specifications; 1 Terabytes hard disk drive, 8GB memory and core i5 1.8GHz processor. This implies just a sizeable amount of the following resources were used to create the virtual desktop environment. This affected the size of the storage disk which was used for the digital forensic investigation,

in that if the storage device under investigation is greater than that of the virtual machine, forensic imaging could not successfully be done.

Again, the research focus on one type of virtualization which is the desktop virtualization. However, looking at the immense benefits that can be derived from the various favors of virtualization technology. Also the workload or volume of data for the performing the investigation may not reveal a true picture of how a real world investigation which may involve extra volumes of data.

1.10 Organization of the thesis

Chapter 1 deals with some background study as well as the formulating the research problem, outline of the research questions, the scope and main objectives of the project.

Chapter 2 basically is in four folds, the first part looks at the general perspective of digital forensics, digital evidence and sources of digital data. The second parts reviews and discusses papers on digital forensics models by eliciting some advantages and disadvantages of those models. The third part looks at the virtualization as a technology and discussing publications on digital forensics in virtual environments. The last part summarizes the reviews done.

Chapter 3 explains the research methodology used in undertaking this research. It looks at the research strategy used hence the research approach in setting up the virtual environment and the forensic investigation undertaken. In this chapter, the implementation of the idea is also broken down and explained involving technologies used and how the different technologies were merged to attain the research goal.

Chapter 4 gives an in – depth analysis of the results obtained from the experiments carried out to prove the hypothesis and the results that were obtained. Observations on the results were also analyzed.

Chapter 5 gives a summary of the whole research including the limitations. Suggestions on future work with the research were also mentioned.

1.11 Summary of Chapter

This chapter looks at the changing computing trends or paradigms, the upsurge of computer or technological enabled or related crime(s), the need for digital forensics investigation and how virtualization technology could be harnessed to augment the investigation processes. It also outlines the research questions, the scope and main objectives of the project including identifying the problem, the significance of the study being carried out, the research targets, the motivation for carrying it out and the scope it will cover.



CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter firstly reviews digital forensics in general, digital evidence, its characteristics, sources of digital data and some digital forensic tools.

2.2 Digital Forensics in Perspective

Computing paradigms have changed drastically in recent times due to the advancement in technology. The usage of computers and devices with computing capability in recent times is on the ascendency. For instance, electronic mail (e – mail) messages can be sent and received via portable or even handheld devices (Personal Digital Assistant (PDA), mobile phones). One can also engage simultaneously in an online computer gaming with other players via the internet or other digital networks and also manage their finances over the internet (ISFS, 2004).

This advancement in technology has not only made execution of work easy and faster, it has also been employed by criminals to perpetrate various levels of crimes. According to (Kristin et al,), 21st century criminals leverage the internet and advanced technologies in undertaking crimes considered to be traditional; notably sex trafficking and dealing in illicit drugs. Again, the digital world is exploited by the criminals to perpetuate diverse technology driven crime with relative ease. Some notable crimes perpetrated with the aid of technology include intellectual property theft, identify theft and payment card fraud. Since those crimes are committed in digital environments where data are represented in zeros and ones, digital footprints or traces of evidence may appear invisible to the human eye just by physical observation or inspection thereby necessitating the need to undertake a digital forensic investigation to retrieve essential evidential data in such a way to conserve the integrity and value of the data.

2.2.1 Digital Forensics

The formal definition of digital forensics according to the Digital Forensics Research Workshop (DFRWS, 2001) is rendered as the scientific means of preserving, collecting, validating, identifying, analyzing, interpreting, documenting and presenting digitally acquired evidence from digital sources for the purpose of facilitating or furthering the reconstructing of events identified as criminal, or assisting to preempt unauthorized actions recognized as disruptive to planned operations.

Digital forensics enhance the reconstruction of activities undertaken in the past with the assistance of information stored electronically at hand, thereby fostering the legal proceedings and investigations. The fundamental goal of digital forensics is to comprehend and restructure events which occurred in a crime scene in order to vividly and eventually identify, organize and fix responsibility to the perpetrators.

Digital forensics is a broad discipline encompassing branches like network forensics, computer forensics, cyber forensics, etc. Not only does digital forensics assist to recover evidences for reconstructing after a committed crime by or through a stand-alone computers but also it assist in the reconstruction of evidences from digital sources to enhance interpretation.

Digital forensics could be seen as the application of the science of forensics in a digital enabled environment to collect and preserve digital evidence as oppose to traditional forensics which is used for collecting and preserving physical data such as fingerprints or other physical evidence. Digital evidence is delicate and fragile in nature; hence the collection should be undertaken with care in a recognized and prescribed manner to preserve the probative value of the evidence acquired to make it admissible in a court of law.

2.2.2 Digital Evidence

Digital evidence as defined by (Casey, 2011), is any data transmitted or stored with a computing system to support or refute the notion of an occurrence of an offense or addresses essential elements such as alibi or intent of the crime.

This evidence may be retrieved from securely seized electronic devices for examination. Digital evidence is characterized by the following;

- Like DNA evidence or fingerprints, it is latent in nature. Thus, they are not visible to the human eye so appear to be hidden.
- Quickly and easily transcends or crosses borders of jurisdictions. Crimes may be committed at a particular geographic location hence the evidences may cross several jurisdictions.
- Is easily tampered, destroyed or damaged due to the digital nature of the evidence, the least alteration of the digital evidence will compromise the integrity of the evidence.
- Is sensitive with respect to time. Thus, the relevance of a digital evidence is a function of time since the evidence is to assist in an ongoing investigation.

Apart from the digital evidence being volatile and fragile in nature, it inherits the complexities of physical evidence. For an evidence to be accepted in a legal proceeding, the digital evidence ought to be accurate and precise in order to ensure that the integrity is conserved and not heedlessly spoiled. The model process in digital forensic assist forensic investigators in the reconstruction of evidences associated with the digital forensic to construct a guideline for the quick development of digital forensic methodology so that evidence can be easily solicited, analysed and processed.

2.2.3 Digital Data and Location

Due to the proliferation of digital devices in every facets of our human existence, in almost all disciplines such as the automobile industry, medicine, etc, data abounds and in diverse formats. Likewise, during the investigation of digital related crime, knowledge of some forms of data and where those data can be located may facilitate the recovery of some data with probative value. Modern computing devices are equipped with high storage media. A typical example is seen in most mobile devices, which have storage capacity greater than some computers that existed in the 90's. Vast amounts of data are therefore stored on modern computing device and these data may either be active data, residual data, backup data or other related source of data.

TYPES OF DATA

Digital data may either be active data (metadata, temporary files and communication data), residual data (slack space, backup data) and sources of data.

ACTIVE DATA

Refers to the visible data of the system's application software or OS with which it is developed. Active data excludes data which is not stored on the local storage device or media and is also accessible without modification or reconstruction. Examples of active data include metadata, temporary files, and communications data.

Metadata

Metadata is structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource (Guenther, et. al, 2004). It is a data about data. The metadata provides a contextual or extra information about other data. Eg:

Information relating to a document's subject, title, enhancements, typeface, as well as the size of the data file form the metadata about that document. The constituent of the metadata stored

within a given document may be the history of the document, comprising all users who saved and / or modified the document. Additionally, it keeps track of the directory structure of all machines on which the document was saved and even the printers it was printed on.

Operating System data

Computer's operating system can provide forensics specialist with data which may serve as a rich repository containing details of user activities such as visited websites, transaction of e – mail messages received and sent, etc.

Web browsers use cookies to keep track of user visited websites while surfing the internet. Since cookies stores all forms of data including passwords, it serves as a valuable source of information concerning a user's activities over the internet which may be retrieved while undertaking forensics investigations.

Temporary Files

Temporary file also referred to as a foo file or temp file is a file created to temporarily hold information during file creation. In the Windows operating system environment, temporary files are created on execution as bits of data are stored by working programs in files called temp or temporary files (Berger, 2015). In a word processor for an example, a program executed by a user temporarily saves data on the hard drive.

Communications Data

Data used in communication such as mobile phones or computers creates digital trail which can provide information regarding whom the user communicated with, the conversation which transpired between both parties, the time of the conversation, individuals who were privy to it, types of documents transmitted, attempt to compromise or delete records of communication if any.

All these potentially recoverable and electronically stored data may reside in the user's computer as well as the devices that are attached to the network or that forms part of the network. E.g. routers or intrusion detection systems.

Residual Data

Residual data refers to traces of data which unknowingly remain on a computer media. After attempting to delete data or data has been forgotten or after decommissioning a media on which data resides; there exist remnant data. (Chow et. al, 2004).

A directory of the location and name of each deleted file is recorded by the computer's operating system notwithstanding the perception some users have about deleted files that deleting a computer file results in the complete removal of the files. When a file is deleted by a user, the file is not removed by the operating system. However, the OS only earmark the space as available. Until overwritten by some specialized programs, the content of a deleted file remains in place (Garfinkel et. al, 2003). It is for this reason why advanced software such as data recovery software can recover the deleted files.

Residual data are mostly known as unallocated data and file fragments. They may consist of fragments of files embedded within other files or distributed on the drive surface. Residual data which can also be found in the slack area (unoccupied space located at the end of the allocated space for a file) are essential for undertaking digital forensic investigation.

2.2.4 Key Elements of Digital Forensics Investigation

In undertaking a digital forensics investigation, four elements are key and these are identifying, preserving, analyzing as well as presenting the digital evidence. These key elements are also defined by the National Institute of Standards and Technology (NIST) as collection, examination, analysis and reporting.

The identification of digital evidence is the prime phases in the digital forensic process. In that, selecting the appropriate techniques, processes and methodology to be used in facilitating the recovery of evidence depends on the extent of knowledge on the nature of the evidence, format or digital representation of the evidence and how it is stored. In the recovery of digital evidence, focus must not be solely on personal computer but should transcend to cover any available or identifiable electronic device with the capability of saving and transmitting data such as electronic organizers, cellular or mobile phones and smart card.

The preservation of digital evidence: Preservation of digital evidence in a digital forensics process is a critical element considering the fragile and delicate nature associated with evidence retrieved from (digital evidence) coupled with the need to ensure the admissibility of the evidence in a court of law. It is therefore important that a least intrusive manner be adopted to conduct any form of examination on data stored electronically. Circumstances may arise that will warrant an alteration to a given data making changes to data inevitable in some instances. In those situation, the impact of the changes should result in minimal impact and reasons for those changes must be justified.

Digital evidence analysis: Analyzing a digital evidence is perceived generally as core phase of the digital forensic process. The activities carried out at this phase include extracting evidence, processing as well as interpretation of digital data. After extracting digital evidence, processing of the evidence is necessary before it can be read and understood by both technical and non – technical individuals.

The presentation of digital evidence includes presenting the actual evidence in a court of law. In the presentation of the digital evidence, issues comprising the credibility of the methodology used to create the evidence, the skill, expertise and qualification of the presenter as well as the mode of presentation is critical. The outcome of the analysis is reported or captured in this final

phase and may comprise essential information such as techniques, tools, guidelines, procedures, recommendations for improving policies as well as some facets of the forensics process. (Sabah et al, 2012).

It is worth knowing that several additions in terms of steps and phases have been added to these key element of the forensics process to derive various models which will be treated in depth in this section as well.

2.2.5 Digital Forensics Tools

Digital (Computer) forensics tools are developed to enhance better research and investigation into computer, internet and technology related crimes. Selection of digital forensic tools by investigation agencies and researchers are motivated by several factors such as budgeting, available experts on the investigative team and competence level. Some notable categories of digital forensic tools are file analysis tools, disk and data capture tools, registry analysis tools, file viewers, internet analysis tools, mobile devices analysis tools, Email analysis tools, Database forensic tools, Mac OS analysis tools, and Network forensics tools. (InfoSec, 2014).

In line with the focus of this research, we would consider the following categories of forensic tools; disk and data capture tools, file viewers and file analysis tools.

Disk and data capture tools

They are tools for detecting the data present, making a forensically sound image of the data unto a suitable drive and securely wipe the data from the source drive to ultimately ensure the integrity of the data. These tools help to perform in a quick, complete and incontestable manner to secure the integrity and validity of data such that it cannot be questioned in subsequent searches and analyses.

File Viewers

These are software programs or tools capable of properly displaying information stored in a file. This is a tool or application that presents the data stored in a computer file in a human – friendly and human – readable form which could also be printed.

File analysis tools

These are used to construct actionable and comprehensive map of an institution's unstructured voluminous data, access rights and ownership. (Bourgeois, 2014). Thus, file analysis tools are developed to provide a graphical view of the various characteristics of the data under investigation and also enable the user to either manage, manipulate and / or migrate specified datasets for some benefits to the forensic investigations.

File analysis tools or software are very efficient at ensuring control of large volumes of unstructured data and control visualization in incredibly short time frames. That is to say, with file analysis tools, without expensive or complex adoption demands, tangible, meaningful and high – impact value are rapidly realized without any end – user's impact

2.3 Digital Forensics Models

Digital forensics models are techniques that are developed to assist in the reconstruction of digital evidences from digital sources by professionals undertaking investigations in digital forensics. Constructing investigative models used in digital forensics have been done in a manner to provide a step by step order of procedure for inspecting evidences. (Gulsan et al, 2012).

Through the models, examiners and investigators of digital evidence are able to acquire or retrieve in – depth and transparent information in connection to sections, aspects or phases to be considered in the digital forensic investigative process.

2.3.1 Abstract Digital Forensics Model (ADFM, 2002)

(Reith, et. al, 2002) proposed the Abstract Digital Forensics Model (ADFM) which was both an inspiration from and enhancement of the model developed by the Digital Forensic Research Workshop (DFRW). The DFRW model consisted of the Identification phase, presentation phase, collection phase, examination phase, analysis phase and presentation phase.

The ADFM model introduced three new phases as an addition to the modal phases previously developed by the DFRW and these were the Preparation phase, Approach Strategy phase and Returning Evidence phase making ADFM a model with nine (9) phases. The phases are; Identification, Preparation, Approach Strategy, Preservation, Collection, Examination, Analysis, Presentation and Returning Evidence.

This model starts with the **Identification** phase where the type of incident is determined based on the indicators recognized from the incident. The **Preparation** phase deals with assembling of techniques and tools, acquisition of search warrants and authorization from management as well as support to conduct further investigation where necessary. Then is the **Approach Strategy** phase with the aim of maximizing the retrieval of evidence with high integrity while reducing the impact of the victim. Next is the **Preservation** phase which isolates, preserves and secures the current state of the digital and physical evidence. With the phase that deals with the **Collection of evidence**, standard and acceptable methodologies are employed to record the physical scene and a clone of the digital evidence. Detailed step wise procedural investigation for evidence in relation to the activities of the suspected crime is undertaken at the **Examination** phase deals with the construction of an in – depth report for conducting analysis. Following the Examination phase is the **Analysis** phase where significance is determined, reconstruction from data fragments is done, and conclusions drawn upon evidence found in order to support or refute a crime theory. In the **Presentation** phase, findings are collated to

provide explanation of conclusions which is mostly done in such a way that a layperson can comprehend and finally the **Returning Evidence** phase which ensure rightful owners regain custody of their physical and digital property and determining the kind of criminal evidence to be removed.

Advantages

- i. It is a diverse methodology which can be applied to an array of current or future digital devices.
- ii. It is a generalized methodology that can assist non – technical observers to identify with technology.
- iii. Is a potential model that can ensure the inclusion of non-digital, electronic technologies within the abstraction

Disadvantages

- i. Some classification or groupings defined within the model appear to be less practical due to its generality.
- ii. There is no easy or obvious methodology for testing the model
- iii. To an extent, there is an overlap or replication of the activities in the second and third phases of the model. In the second phase, selection of tools, techniques, etc done are premise on the strategy selected.

2.3.2 The Enhanced Digital Investigation Process Model (EDIP)

The Enhanced Digital Investigation Process Model mostly referred to as EDIP was developed by Baryamureeba et al (2004). The EDIP is an investigative model to improve an existing model developed by Brian Carrier and Eugene Spafford known as the Integrated Digital Investigation Model (IDIP). EDIP seeks to ensure the redefinition of the forensic process and related advancement by expanding the deployment phase in the IDIP model. The expansion as accounted by Baryamureeba et al (2004) includes crime investigation which may be physical

and digital in nature while introducing the trace back phase which establishes a link to the primary crime scene (computer) employed to perpetrate the crime. The EDIP model has two categories of crime scenes which is the suspect's or the primary crime scene and the victim's or the secondary crime scene.

This model has five major phases namely, readiness, deployment, trace back, dynamite and review. The model starts with the **readiness** phase where operations and infrastructure readiness is undertaken. Thus, the capacity based of the personnel are enhanced through training and equipping with needed skills to deal with the situation and a check is done to ascertain that the existing infrastructure is capable enough to handle any probable incident that occurs. The **deployment** phase provides mechanism for detecting and confirming an incident. This phase has five sub – phases which includes detection and notification phase where incident is detected and the respective individuals or authorities notified appropriately, Physical crime scene investigation is where examination of the scene traces as well as the tangible artifacts is conducted to discover evidence in digital format while investigation of the digital crime scene involves examining electronically identifiable electronic device to acquire digital evidence and if possible estimate the level of damage or impact. The confirmation sub phase is triggered in an event of a confirmed incident and legal authorization is acquired to undertake search and further investigation at the suspect's premises. The presentation of the evidence derived from both the physical and digital crime scenes to corporate management or legal team is done at the submission sub phase. The **traceback** phase tracks down the operations of the suspect's physical crime scene so as to identify devices used to perpetrate the crime. This phase encompasses two sub – phases; digital crime scene investigation and authorization phase. Succeeding the traceback phase is the **Dynamite** phase which conducts investigation at the primary crime scene with the aim of retrieving and analyzing objects discovered on the scene to acquire additional evidence to ascertain the origin of the crime to help apprehend potential

culprits. In the **Review** phase, there is a review of the entire investigative process so as to identify possible area of improvement.

Discussion

Though Enhanced Digital Investigative Process model is an improvement over the IDIP there exist some ambiguity with some activities carried out in some phases or some clarification have to be provided. There is a submission sub – phase under the deployment phase which states that; presentation of the physical and digital evidence is made to the legal entity or corporate management (Palmer, 2001). The unanswered question here is, what are they to do with that presented material and how does the outcome of that sub – phase affects the investigative process?

This model has duplicate activities. E.g. Digital crime scene investigation activity appears under the Deployment phase, Traceback phase, as well as Dynamite phase. It may be argued that, due to the iterative nature of the investigative model proposed. According to Palmer (2001) EDIP separates the investigations at the primary and secondary crime scene while depicting the phases as iterative instead of linear. That notwithstanding, it would have been appropriate to give the output at each phase or per each activity in the phase so as to draw some distinction and also serve as checks for the investigation.

2.3.3 Computer Forensics Field Triage Process Model (CFFTPM)

Rogers et al (2006) proposed this model. It is a model which is suited for on-site investigation in identifying, analyzing and interpreting digital evidence in a quick time frame, devoid of the overhead of taking the system(s) media back to the lab for further investigation or acquisition of a sound digital forensic image(s). This investigative model is needful in situations where rapid investigations and information leads outweigh the need for detailed examination of

possible potential digital evidence back in a laboratory. Hence the model is mostly used on the field or at scene (Rogers et al, 2006).

The three basic components of forensic investigation by Kruse II et al (2002) also called the “3As” of computer forensics investigation guided the formulation of CFFTPM foci. The CFFTPM was developed with the following foci; quick identification of usable evidence, identifying victims as minimal risk, safe guard the investigation in progress, identifying potential charges and rightfully assessing the offender’s threat to the society and at the same instance preserving the integrity of the evidence and / or potential evidence for further investigation. The CFFTPM has six (6) main phases with two (2) of the phases having three (3) sub – phases each and these are, Planning, Triage, User Usage Profile (Home, File Properties, Registry), Chronology Timeline, Internet (Browser, Email, IM) and Case Specific.

This model begins with the **planning** phase where proper prior planning is undertaken with the investigator formulating some indicators and directions highly probable to result in successful investigation. After the Planning phase is the **Triage** phase where priority based activities are executed. Hence objects, traces of artifacts with evidential value, or probable evidence containers are highly important or the most transient are first dealt with. In the **User Usage Profile** phase, actual examination and analysis is performed on evidence found on digital media in order to link the evidence to a specific, identifiable suspect. **Chronology Timeline** phase builds the crime incident from organized chronology to sequence the probable crime activities mostly by using some timing model such as the MAC (Modification, Access and Creation) times. With the **Internet** phase, examination of artifacts related to internet activity such as Instant Messaging (IM), e – mail and web browsing is performed. The final phase is the **Case Specific Evidence** phase whose success largely depends on the competence of the investigator employing the model in an investigation. In this phase, adjustments are made concerning the

focus of every examination of that case as well as reconciliation of conflicting requirements are done in a manner to suit each specific set of circumstances.

Advantages

- i. This model is much concerned about time, hence help to undertake quick information and investigation in a time critical situations.
- ii. This model is conducive for conducting on scene investigations to provide investigators with positive feedback where possible.
- iii. It enables digital forensics investigators to quickly analyze and perform modification to their search warrants whilst on the based on input from the primary investigator(s) as well as those in direct contact with the suspect.

Disadvantages

- i. This model is only appropriate for investigation conducted at the scene
- ii. It may be seen as an incomplete investigative model should the case under investigation require additional work to be done off the scene.
- iii. This is a time critical model, hence in the usage of this model some investigative process or phase may be compromised thereby affecting the results or outcome.

2.3.4 Generic Computer Forensics Investigation Process Model (GCFIPM)

Yusoff et al (2011) came up with a digital forensic investigation model known as the Generic Computer Forensics Investigation Process Model after reviewing existing forensics investigation models from 1984 to 2010.

The models which were reviewed as well as the phases under those models were giving unique ids without being oblivious of the relationship between the models and their respective phases. After assigning the ids, the tasks and not just the nomenclature which are performed under each phase was considered resulting in a five (5) generic grouped phase proposed model. The

GCFIPM phases include, Pre – process, Acquisition & Preservation, Analysis, Presentation and Post – process.

The Pre – process phase deals with activities that are carried out before the official commencement of the investigation and the actual collection of data such as getting the necessary approval from relevant authority, etc. Under the Acquisition & Preservation phase, tasks related to identifying, collecting, transporting, storing and preservation are performed. Next is the Analysis phase which is considered as the core of the forensic investigation processes and various types of analysis are performed on the acquired data to identify the crime source and possibly the perpetrator of the crime. The Presentation phase is where various outcomes derived from the Analysis phase are documented and reported to authority in a format which is easily understood and mostly backed by sufficient and acceptable evidence. Finally is the Post – Process phase where proper closing of the investigation exercise is done, rightfully owners are given the needed digital and physical evidence and review of the investigation process is done for lessons to learnt and improvement be done for future investigations.

Advantages

This model puts phases of several models into groups making the model suitable or applicable to diverse types of forensics investigations.

For the development of new digital forensics investigative model or its enhancements, this model serves as a broad or generic framework that will provide a good starting point for such development.

Disadvantages

The phases within this model was formed by grouping phases of other models which eventually introduces duplicate activities in the grouped phases. Due to the generalized nature of this model, it is perceived to be more of a directive framework than a model.

2.3.5 An Integrated Digital Investigation Process (IDIP)

This model proposed by Brian and Spafford considers two conceptual and relevant crime scenes namely the physical and digital crime scenes and how to integrate these crime scenes' investigations to identify suspected perpetrators of the digital activity (Brain et al, 2003).

The authors of the paper undoubtedly admitted that while digital investigations have recently become prevalent, clues and experiences from physical investigations which has existed thousands of years ago could be co – opted to augment digital investigations. Hence, the introduction of the concept whereby a digital crime scene may be delineated to possess its own unique evidences, witnesses, events and activities which may necessitate investigation using the same model as a physical crime scene.

The digital crime scene according this paper is the digital environment created by the hardware and software as oppose to the school of thought which considers every crime scene with a computer or other digital device as a computer crime scene.

This process model encompasses seventeen (17) phases organized into five (5) groups which are the readiness phase, deployment phase, physical crime scene investigation phase, digital crime scene investigation phase and the review phase.

- i. **Readiness Phase:** The goal of this phase is to ensure that the operations and infrastructure are fully capable to support an investigation. The operation readiness sub – phase deals with the provision of skill orientation and requisite equipment for the skilled personnel

conducting the investigation into the incident. Ensuring the presence and availability of the needed data for complete investigation is done at the infrastructure readiness sub – phase.

- ii. **Deployment Phase:** Deals with the provision of a mechanism for the incident to be detected and confirmed. The tasks performed under the deployment phase include; detecting and notifying where an incident is detected and the appropriate entities are notified. The confirmation and authorization phase deal with activities that help to acquire the legal authority to conduct full investigation into the incident and crime scene.
- iii. **Physical Crime Scene Investigation Phase:** The phase aims at collecting and analyzing the physical evidence in order to reconstruct the events that preceded the occurrence of the incident. This goal is attained by undertaking the following sub – phase activities; preserving, surveying, documenting, searching and collecting, reconstructing and presentation of the physical crime scene.
- iv. **Digital Crime Investigation Scene:** In this phase, each digital device is considered a separate crime scene hence the objective is to identify electronic activities undertaken on the system identified during the physical crime scene investigation. This phase is triggered when the physical digital device considered to be a crime scene is retrieved primarily from the physical crime scene as a physical evidence or when captured network traffic is critically examined for evidence. This phase is made up of six sub – phases namely; preservation, survey, documentation, search and collect, reconstruction and presentation of the digital crime scene. The results of this phase are used as feedback for the physical crime scene investigation phase.
- v. **The Review Phase:** It entails activities carried out as introspection of the investigative process to identify areas for improvement. For digital incidents, this involves the collaboration between the physical and digital investigation work coupled with the determination of the magnitude of the existing digital and physical evidence enough to

solve the case. The results derived after the review phase may be one of the following: realization of new methodology, improved new or improved model for training purposes, or in a case of failed plan, nothing is achieved.

2.3.5.1 Discussion

It is an out and out model which considers the dual investigative nature of the digital forensic investigation by integrating the physical crime scene investigation phase and the digital crime scene investigation phase. The model envisaged that although the crime was perpetrated using a digital device as a means or target, the forensic investigation encompass both physical and digital crime scenes hence the need to include them in the investigations.

Since replication in the digital environment is easy, it is not uncommon to produce a full forensic image backup of the system to allow for analysis at the lab. Unlike many process models that focus primarily on the digital evidence, this model clearly shows the interaction between the physical and digital environment.

2.3.6 Forensic Computing Models: Technical Overview

In this paper, Gulsan et al (2012) considers the techniques for the reconstruction of a committed crime from the clues or digital traces. That is a uniform approach of the digital forensic models for digital forensic investigation. The paper considers the diverse digital forensic models and their limitation and concludes with a new digital forensic model.

The paper gives a brief history on how digital forensics have evolved in the passage of time. This evolution is chronicled in the paper by looking at some notable digital forensic related issues from 1978 where the first crime involving an unapproved and deletion of a computer system's data occurred in Florida to 2015 where publication of an ISO standard (ISO 17025, General requirements) for the competence of testing and calibration laboratories.

The paper looked at digital evidence and its characteristics with this suggestion, “Digital evidence is very delicate to deal with. Any improper handling will result in the spoilage of its integrity.” This clue is relevant and must be adhered to cautiously by digital forensic investigators. In line with the above assertion, the paper looks at the need for digital forensic model which provides techniques for the reconstruction of the digital evidences from digital sources. The authors reviewed some digital forensic models available from 2001 through to 2011 looking at some weakness inherent in these models.

2.3.6.1 Discussion

The paper gives some insights to the background of digital forensics by looking at the history, previous work done in the field of digital forensics and review of some digital forensic process models.

However, after providing some inherent weakness associated with some of the models in some instances, the paper did not propose any new model as captured in the objectives of the paper. The authors concludes by reiterating the need for digital evidences to be precise, accurate as well as ensuring the integrity of the evidence to enhance easy admissibility in a law court.

Finally, the authors joined the numerous calls to formulate a guideline to swiftly develop digital forensics procedures that can be easily interpreted, analyzed and processed. Although a laudable appeal, whom it was addressed to still remains anonymous.

2.4 Virtualization as a Technology

Virtualization is a technique for simulating a hardware platform in a software. The hardware platform may be a server, storage device or network resource. According to John K. Waters, virtualization may be defined as the technologies developed to create an abstracted layer between the software and the underlying hardware. Hence in virtualization, all of the functionalities of the system are simulated thereby separating it from the underlying hardware

to create a “virtual instance” which has the capability to operate and provide the traditional, hardware solution.

Virtualization hinges on the concept of partitioning, whereby a singular physical infrastructure such as storage disk, network and physical servers are logically divided into logical storage partitions, virtual networks and logical servers respectively. After the partitioning is done, each logical infrastructure runs independently with its set of instructions, and allocated resources including operating systems and applications.

Virtualization therefore allows instances of multiple operating system to be executed simultaneously of a single computing system providing an avenue for decoupling hardware from the underlying operating system. The virtual computer running inside the physical computer which is also known as the “guest” operating system coordinated by a hypervisor which may be referred to as Virtual Machine Monitor (VMM). The virtualization layer or system lies or is sandwiched between the hardware and the guest. The VMM manages the guest’s use of the processor (CPU), memory, and storage enhancing the migration from one computing machine to another. An enhanced elucidation to harness the benefits of the decentralized as well as centralized deployments is virtualization.

Implementing virtualization technology lay off the cost burden of procuring and maintaining a one – to – one relationship between an application and an entire computer. With the aid of virtualization, several independent operating system may be installed to reside on a centralized hardware to control each application. With this infrastructure, advantages such as stability and security derived from a decentralized system is realized. (Keyman, 2012)

2.4.1 Hypervisor

According to Popek and Goldberg, virtualization is achieved through the idea of a virtual machine monitor (VMM) and this software is usually characterized by three vital features; first

is the provision of the environment identical to the one provided by the physical system. Secondly, there should be little degradation in speed experienced by programs that run on the simulated environment and finally, the VMM should have complete control of the system resources. However, not all of the x86 processor set meets the “classical virtualization” criteria defined above so an intermediary must be used to resolve the issues regarding the problematic small subset of the entire instruction set of the x86 architecture. Hence the concept of hypervisors which is a well – isolated, additional but minimal software (Revelle, 2011).

In virtualization technology, multiple OS or instances of the same operating system running of a single computing system is managed by a software called hypervisor also known as Virtual Machine Monitor (VMM). (Diane et al, 2010).

In summary the main job of the hypervisor is to provide solution to the needs to effectively manage the guest OS in a manner that multiple operating systems and its instances run seamlessly so that they do not interrupt one another.

Hypervisors can be divided into two types:

- **Type 1:** Executes or runs directly on the hardware of the host computer to manage its hardware resources and manage the guest operating systems. It is therefore referred to as bare – metal or native hypervisors. With the type 1 hypervisor, the hypervisor is the first thing or the operating system directly installed on the hardware, hence no need for an underlying operating system. The hypervisor will enhance direct communication between the guest application and the underlying physical server hardware. Those resources are then paravirtualized and delivered to the running VMs.

Examples of Type 1 hypervisors include VMware ESXi, Citrix XenServer, Microsoft Hyper-V hypervisor and the open source Kernel – based Virtual Machine (KVM).

- **Type 2:** Unlike the type 1, the installation of the type 2 hypervisor is not done directly on the bare – metal hardware but on a live OS already installed on the system, commonly referred to as hosted hypervisors.

With this architecture, the guest OS run at the third level above the hardware thereby limiting the extent to which resources are controlled by the hypervisor. This is due to the fact that, the hypervisor executes as an application installed on an already configured operating system whilst the guest OS runs on the hypervisor is the virtual machine.

Some examples of type 2 hypervisors include Parallels Workstation, Microsoft Virtual Server, VMware Server, and VMware Workstation.

2.4.2 Virtualization Techniques

VMWare played a pivotal role in the resolution of the virtualization challenge faced by the x86 processor architecture. The binary translation techniques developed by VMWare in 1998 provide three pragmatic alternative techniques for handling instruction so as to virtualize the CPU on the x86 architecture. These techniques are: full virtualization, paravirtualization and hardware – assisted virtualization.

Full Virtualization

The virtualization technique where the underlying hardware is entirely simulated to provide a virtual machine environment is known as full virtualization and provide each virtual machine with all the services of the physical system, such as virtual BIOS, virtual devices, and virtual memory management. This is achieved by using a combination of binary translation and direct execution. Since virtualization abstracts the hardware layer, any software which successfully execute on the physical hardware can be run in the VM, likewise any operating system which

the underlying hardware supports can be run in each individual virtual machine (Barret et. al, 2010).

In full virtualization, majority of the guest OS code runs unmodified which implies the code runs on the host computer directly making the guest OS “perceive” it is being executed on a real machine. The usefulness of such virtualization technique can be realized in OS development, where portions of code or beta versions of the OS can be executed simultaneously with older versions, each in a separate virtual machine.

Some benefits derived from full virtualization include security and isolation for virtual machines in addition to simplified migration and portability which is due to the fact that the same guest OS instance can run on virtualized or native hardware (VMWare, 2007).

Paravirtualization

With paravirtualization, there is modification of the operating system’s kernel bridging the processing done at the hardware level and the applications. Instructions that are not virtualized are substituted with hyper calls that communicate directly with the virtualization layer hypervisor to carry out critical kernel related tasks such as interrupt handling, time keeping and memory management.

In paravirtualization, virtual machine emulator is launched after the host operating system is launched. The kind of emulator used depends on the platform in that the virtual machine can execute with VMLAUNCH emulator developed by intel or the VMRUN emulator by AMD. In paravirtualization, when the guest is running in an active state, the host enters or runs in a suspension state. The open source Xen project is an example of paravirtualization.

Hardware – Assisted Virtualization

Due to the fast penetrative ability of virtualization technology, it is rapidly being embraced by hardware vendors who are researching and developing new features to simplify virtualization methodologies with first generation enhancement such as Intel Virtualization Technology (VT – x) and AMD’s AMD – V. (VMware, 2007).

Hardware vendors used different nomenclature to refer to hardware – assisted virtualization. Some of these names are native virtualization, accelerated virtualization, or hardware VM.

Hardware – assisted virtualization refers to the technology equipped with a new CPU execution mode feature which enables the virtual machine monitor to execute privileged instructions in a new root mode below the OS kernel level (ring 0). The need for hyper calls and binary translations which exist in paravirtualization and full virtualization respectively are eliminated in hardware – assisted virtualization which adopts the use of sensitive and privileged calls that are automatically set to trap the hypervisor. Either VM control structure developed by Intel or control Blocks developed by AMD are used to store the guest state depending on the manufacturer of the CPU.

2.4.3 Categories of Virtualization

Server Virtualization

Server hardware proliferation which has its inherent problem of increased cost and energy consumption, etc in organizations and institutions. Ideally, a server hardware fundamentally serves a specific functionality (i.e file server, internet server, enterprise resource planning server, mail server, etc). The problem however is that, only a portion of the processing power are utilized by the application which run on the server. The “one application, one server” hurdle is dealt with by the introduction of server virtualization which facilitate the consolidation of numerous servers into one physical server.

In other words, several virtual machines are able to run on one physical server through server virtualization making the user to perceive the virtual servers exactly like physical servers. The resources of the physical servers such as memory, processor, hard drive, and network are shared culminating in efficient utilization of the physical server's resources. Through the hypervisor, all these shared resources are allocated to the virtual machines to use, which leads to better utilization of the physical server's resources.

Network Virtualization

Network functionality performed by software to decouple the underlying network hardware from virtual network is called Network virtualization (Baca, 2013). Network virtualization can be considered in two folds, as a technology capable of integrating numerous physical network to attain a single logical (virtual) network or on the other hand as a technology to partition logically a single physical network into several logical or virtual networks. Through the use of network segmentation and virtual IP management, multiple networks, each customized to a specific purpose is attained with network virtualization.

Installed software and services are used for the management of shared computing cycles, storage and applications in network virtualization. Thus, services and servers within the network are treated in network virtualization as a unit repository of resources which can be accessed without recourse to its physical components.

Network Virtualization's goal is to provide a network overlay to decouple a logical topology from the physical topology allowing for connection to be established between the virtual or physical computing system and physical or virtual network services irrespective of the location of the data center.

Storage Virtualization

Storage virtualization aids in addressing the challenge of storage and data management by enhancing the execution through the provision of easy back – up, recovery and archiving tasks in a short time frame. Through storage virtualization functionalities of the storage area network (SAN) are aggregated and its complexity is encapsulated.

The functions of the SAN such as back – up, archiving and recovery are easily and rapidly executed through the installation of software applications and high – speed sub network of shared storage devices. Virtualization can be seen as the accumulation of several network storage devices in order to appear as a single storage unit.

Kay (2008) says a new layer of hardware and / or software is introduced between servers and storage systems in a manner that applications runs seamlessly without regarding the specific drive, storage sub systems or partitions on which the data resides. This allows system administrators to identify, provide and manage distributed storage as an integrated single resource.

Configuration or structure of storage virtualization may be done in three ways:

- **Host-based:** With this structure, a legacy device driver controls the physical drives whilst a software layer introduced above the device driver intercepts I/O requests, redirects I / O and looks up metadata.
- **Storage-device-based:** In this type of setup, virtualization can be built into the storage fabric; for example, newer RAID controllers allow other storage devices to be attached downstream. A primary storage controller handles the pooling and management of metadata, providing interface for direct attachment for other storage controllers.

Replicating and migrating of cross controllers services are provided in such setup system.

- **Network-based:** This structure views storage virtualization as a networked device connected using a Fiber Channel to attain a storage area network. Here, too, an appliance or switch-based implementation is most common.

Application Virtualization

Software installed onto a host computer's operating system hard – codes its settings on the entire system to suit the needs of the application. However, application virtualization enables an application to execute its own set of configurations on – demand leaving the host operating system and existing settings unaltered.

Application virtualization as defined by VMware is the deployment of software without modification to the host computer, local operating system, registry or file system. This technology enables the deployment of an organization's customized and commercial software across the enterprise without system changes, installation conflicts, or stability or security impact.

Application virtualization also known as application service virtualization is layered on top of other virtualization technologies, such as storage virtualization to allow computing resources to be distributed dynamically in real time.

2.4.4 Digital Forensics on a Virtual Machine

Juan et al (2011) used the concept of hardware virtualization and how they can be employed in digital forensics. The paper presents four main steps used to undertake a digital forensics investigation on a host machine to identify, retrieve and a virtual machine. The steps include;

i. Creating a forensically sound image ii. Identifying and recovering sensitive information iii. Analyzing virtual machine iv. Documentation

The first step though common in a conventional investigation, is also an essential procedure for investigating a virtual machine as well. Ensuring a non – modification of the data and that the image is complete should be the focus of this process. A hardware write – blocker is used before an image is created in order to ensure that no modification detrimental to the investigation will be made to the real disk.

During the sensitive information identification and recovery, the investigator has to find out whether an illegal activity was done from the host machine or from a virtual machine. Depending on the extent of the illegal activity or activities, some sophisticated tools and methodologies may be employed in the analysis.

2.4.5 A virtual digital forensics laboratory

Craig et. al (2008) alluded to the fact that, most criminal activities are aided by digital devices; prompting the need to consider digital evidence whilst investigating a crime. Moreover, the process of collecting, storing, examining and presenting digital evidence are activities that mostly take place in a centralized laboratory. The paper admits the above methodology is an insufficient model with respect to the fact that there is a duplication of resources that are available elsewhere by hence the need to setup the virtual digital forensics laboratory proposed by the paper.

To setup a modest laboratory well – suited for a digital forensic investigation can cost huge sums of money in the range of several dollars, considering the costs of procuring computers, storage devices, training of digital forensic professionals and appropriate forensic tools. In view

of that, the paper envisaged that, in the future a digital forensic laboratory will be virtual in nature. The concept of a virtual digital forensics laboratory (VDFL) creates a laboratory whose nature is virtual operations is not confined or limited within a geographic boundaries.

The paper in its conclusion admits that before the virtual forensic laboratory can become operational, there remain numerous challenges to be addressed. However, these anticipated challenges do not nullify the prospect or the single best hope this proposed facility will provide law enforcement agencies to cope with the surge of digital evidence.

2.4.6 Analyzing the impact of a virtual machine on a host machine

This paper authored by Dorn et al (2009) investigates a growing and emerging technology which is virtualization. The focus was to investigate or peruse numerous vital areas in relation to the behavior or functionality of the virtual machines popularly referred to as VMs and their impact on the respective host machine.

As virtualization presents a cost effective and efficient means of computing, it is employed as a tool or means to perpetuate or commit crime either on the virtual platform or on the host platform. In that view, Dorn et. al (2009) admit the prevalence of virtualization has warranted the need to comprehend the virtualization and its impact on the process of recovering evidence from the traces of digital footprints left behind by those who commit such crimes.

With respect to the tracing of the evidence, the paper focused on digital data acquired from executing and installing virtual machines on their host machines. It looks at the acquisition of vital and useful information with respect to file types and locations the virtual machine applications installed, as well as the processes generated by running virtual machines and the structure. In addition other things of evidential or probative value such as the identity of virtual machines, their host operating environment, ancillary files and associated artifacts are searched for.

In order to achieve the focus of the paper, a hypervisor or VMM was installed to create the virtual environment. The virtual machine was fed with test files for the execution, modification and deleted while properly tracking and recording every activity. The host hard drive was then forensically cloned and with the aid of forensic software, analysis is done on the image.

The paper mentioned the usage of some tools such as a new Dell Optiplex 755 machine as the host machine, other virtual machines and other forensic tools. However, the paper did not cite sufficient reason(s) for the choice of these tools. Moreover, some comparative study or analysis of the VMs as well as other forensic tools could have been done for proper understanding or conclusion on the choice of such tools.

2.5 Summary

This chapter provides a review of digital forensics in general, digital evidences and sources of digital data as well as some digital forensics investigative tools. It also reviews existing digital forensics investigative models by discussing their merits and demerits together with some unanswered questions. It also evaluates virtualization technologies and how it can be used to conduct some digital forensics investigations. Some related or existing works in forensic investigations in virtual environments was also reviewed. The review shows that most digital forensic works and models were done generally with the conventional computing system in mind with less work in the virtual environment. Also they do not seek to provide how virtualization technology can augment or use to improve digital forensic investigative models.

CHAPTER THREE

RESEARCH METHODOLOGY

3.0 Introduction

This chapter presents the methodology of the project. The implementation of a virtual desktop laboratory for digital forensic investigation. A virtual machine monitor will be installed to

create the virtual desktop environment. The setting up of the forensic platform using a Debian or Linux based operating system called Kali Linux with an integrated functionality and tools of undertaking forensic investigation, penetrating testing and other security related works undertaken in the digital landscape.

The need for this research has come about as a result of the recent study which reveals that there is a proliferation of digital devices and technologies as well as the undue advantage other malicious individuals take to use this innovation to commit crime in this digital age. Again, the need for this study is relevant at this period of diverse digital crime hence warranting a research into how virtualization technology to be specific, desktop virtualization could be employed to augment the digital forensic processes and possibly to improve digital forensic model. This is evidenced in chapter two of this work after a review of existing literature. Issues and review of related literature identified some models were suited for onsite digital forensic investigations with the primary aim of soliciting relevant and time essence evidence within the shortest possible time and on the spot. Also, the fact that most digital forensic investigations are done targeting conventional computing system. In the light of this review, conducting digital forensic investigation using virtual desktop as the forensic platform is timely and an excellent method to improve the existing methodology and model.

Conducting digital forensics investigation on a virtual desktop as a way of implementing virtual digital forensics will provide a real time platform for efficient digital forensic training.

Thus, with this model, digital forensic investigators especially novice will be able to undertaking real time experiment and analysis on a suspected digital media without compromising the integrity of the digital evidence. Again the experiment will be conducted by using two closely related digital forensic tools to undertake the same task in order to do accurate analysis on the outcomes or results of each forensic tool. This comparative analysis will provide

grounds or additional knowledge to inform the choice of a given digital forensic investigation tool.

The implementation of digital forensic investigation in a virtual desktop environment will provide a cost effective way of undertaking digital forensic investigations. In that, considering the complex and delicate nature of the digital evidence coupled with the essence of retrieving those evidence which is to make it admissible in court. With this in mind altering or causing any damage to the digital evidence will be too detrimental to the whole data forensic investigation process. Digital forensic investigation in a virtual desktop environment will however provide an easy and efficient means of creating and mounting the image of the storage device under investigation while keeping the original storage media intact to check the veracity and authenticity of the evidence should the need arise.

In the next section, details are provided about the research strategies employed to solve the research issues recognized above, implementations, coupled with the modality of data collection for analyzing the data including laboratory experiments and observation, and then proceed on the conceptual framework for data analysis. Moreover, spiny issues relating to potential limitations and challenges inherent in the selected research strategy and its implementation.

3.1 Research Strategy

The empirical research in this study is interested in proving the hypothesis that, if the desktop virtualization is implemented as a digital forensic investigative platform, the efficiency and effectiveness of digital forensic investigation will be attained. It will also be used to improve digital forensic model and techniques in order to enhance the learning of digital forensic investigation. This was carried out by setting up a virtual desktop environment, setting up a digital forensic software tools on this virtual desktop environment, undertaking digital forensic

investigations using some forensic tools, analyzing the outcomes or results of the investigations and undertaking comparative comparison of those forensic tools.

According to Yen (2003), there are various forms of research which can be; Experiments, survey. Case Study, etc. Your choice of strategy is dependent on the nature and characteristic of the research.

Conducting research using case study targets in enhancing the understanding of issue or object which are complex in nature, transcending experience or adding strength to what is already known through previous research. Case study emphasizes on detailing contextual analysis of specific number of activities or condition and their relationships. This research method has been used by researchers for several years across diverse discipline of study especially the social sciences. Researchers in the social science discipline have embraced and made popular use of this qualitative research method to analyze contemporary real – life situations and present platform for the implementation of ideas and extensions of procedures. Case study as defined by Yen (2003) refers to the empirical inquiry that investigates a contemporary phenomenon and context are not clearly evident; and in which multiple sources of evidence are used.

Action research is a research embarked to provide solution to an urgent problem or a reflective process of progressive problem solving initiated by entities working with others in teams or as part of a “community of practice” to enhance the procedures of addressing issues and solving problems (Myers, 1997).

The above research strategies together with Survey based strategy fail to address the aims of this research which deals with conducting Laboratory experiments on computers to find the relationship between two objects or variables.

The research strategy to be used to select a suitable strategy to implement empirical research such as this is the experimental research. What does experimental research represent and how is it suitable for this research?

An Experiment refers to the use of methodologies which are empirical in nature arbitrating competitive models or hypotheses (Denzin & Lincoln, 1994). Experimenting therefore provides means for testing existing theories or new hypotheses in order to refute those theories and hypotheses or affirm them. An experiment is a stepwise methodology that is conducted with the aim of checking the veracity, refuting or proving the validity of a hypothesis. With the above definition, experimental research usually aims at testing a new or existing hypothesis, with the view of ascertaining how a specific process model or phenomenon works. As such, a carefully and well conducted experiment will yield results that either confirm or refute the hypothesis and carefully conducted, the result will either support or disprove the hypothesis and this is a very primary component of the engineering and scientific method. Hypothesis is the heart of experimental research. Experimental method also assist in the provision of investigative methods adopted to derive and establish basic relationships among phenomenon under controlled condition or, simply put, to determine the criteria influencing the occurrence of a given phenomenon. Experiments also aim at manipulating certain environmental or external conditions and analyzing or examining how those conditions or behavior is affected and this is done in a highly deliberate and systematic manner. About four main characteristics make experimental research different from other research strategy like case study. These are;

- i) It is under control which implies the removal or minimization of the influence of such variables by different methodologies such as randomization, ii) Manipulated where there is intentional manipulation of the indicators or conditions by the research team or researcher, iii) identifies the manipulative effect(s) of the dependent and independent variables, and then iv) Replication which also deals with undertaking a number of sub experiments instead of one.

These and other characteristics of Experimental Research make it the best Research strategy for this project.

3.2 Research Approach

In essence, experimental research such as this is basically qualitative but not quantitative in nature. According to Denzin et al (1994), Qualitative research is the studying of things in their default settings, seeking to decipher, or interpret the phenomenon guided by the interpretation people bring to them whilst quantitative research are suitably used in the natural sciences discipline such as physics, to examine natural phenomena employing methodologies such as laboratory experiments as well as mathematical modelling, although quantitative research may adopt survey techniques within social settings be used in collaboration with qualitative methods (Myers 1997). From the above definitions, it could be seen that, Qualitative research focuses more on collecting, analyzing, and interpreting data by means of observing what people do or say and it is subjective. In quantitative research, greater emphasis is placed on measurements and quantities, hence majority of the scientific research which undertaken tends to be quantitative research due to the fact that it deals with quantifiable data.

These experiment were carried out on an 8GB memory, Intel core i5 processor and 500GB hard disk size desktop machine.

3.3 Data Collection: Experiment and Observation

This research is much of qualitative and will be undertaken by means of experimental research strategy. Research will be conducted on a desktop computer system with certain specifications suitable for running the required desktop application. According to the research strategies, virtualization tools and software needed to establish the virtual desktop environment will be setup, scripts and commands as well as manipulation will be done to config files. Scripts and commands to undertake digital forensic tasks will be executed to demonstrate how to harness

virtualization technology as a digital forensic platform. Data from the experiment will be gathered or retrieved to perform in – depth analysis so as to prove the hypothesis.

A number of Data collection techniques exist, such as Sampling, Questionnaires, simulation, Observatory, etc.

Boyd et al (1997) have defined experimentation as: A research methodology where one or more variable are modified under conditions that enhance data collection, demonstrating effects if any, of such variable in an unambiguous manner. Collecting data by experimentation is performed in such a way to ensure relatively comprehensible interpretation. In the field of science, experiment determines and proves cause – and – effect relation.

It is noted that, observation is another technique used in collecting data in this research. Observation involves looking carefully. In order to overcome the challenges of observation as a data collection technique, self- inference and effect were fully minimized on the testing process. When observation is used to collect data, the researcher examines and investigates the effects of the modification of the dependent and independent variables.

Therefore, by the above definition, the suitable methodologies to be employed in undertaking this research is by Experimentation and Observation. Experiments were carried out by setting up a virtual desktop environment provide an emulated forensic platform to undertake digital forensic investigation such as data recovery and carving using digital forensics tools. The results from the digital forensic investigation in the virtual environment is observed and examined to improve digital forensic investigation model.

3.4 Implementation

3.4.1 Implementing the Virtual Desktop Environment

Virtualization and its related benefits have been reviewed in chapter two (Literature Review).

In this section, a quick recap of the benefits of virtualization is done. The relevance include;

- i) Ability to run multiple operating systems in a lab ii) Run Linux on a Windows host
- iii) Ability to safely test software iv) Provide a platform for learning and under studying another Operating System
- v) Ability to run older operating system and software vi) Able to set up OS for kids to use and easily restore if it mess up.

3.4.2 Selection of a Virtualization Solution

There are several virtualization solutions available, be it commercial and non – commercial ones. Some of the notable and best known virtualization solution is VMWare which offer a full suite of products ranging from their VMWare Player to fully redundant enterprise solutions. On the other hand is the virtualization solution offered by Microsoft which spans from Virtual PC (Desktop) to Hyper – V (enterprise solution) and several products in between. On the Macintosh platform, the two popular virtualization solution are

VMWare's Fusion products and Parallel's suite of products. Out of the several number of options available on the Linux platform, the notable ones are KVM, Xen and VirtualBox.

After several research and perusal, VirtualBox was chosen to setup the virtual desktop environment. The reasons for selecting the VirtualBox does not imply the other virtual machine monitors (VMMs) are not suitable for setting up virtual desktop environment but a justification for selecting virtualBox.

- i) Licensing is free for private and personal use.
- ii) It is a type 2 hypervisor which runs within an operating system so it becomes easy to manage.
- iii) VirtualBox executes on Windows OS, Linux distributions, Macintosh, Solaris, etc.
- iv) VirtualBox can run the following as Guest Operating systems; Windows 3.1 upwards,

Linux 2.4 upwards, Macintosh OS, Solaris and Open Solaris, FreeBSD and OpenBSD, DOS, OS/2, Netware, BeOS, etc.

In summary, VirtualBox is an efficient virtualization product which runs on the x86, AMD64 / Inter64 processor architecture and suitable for enterprise and home use. Apart from VirtualBox having a rich feature and having a high performance. VirtualBox is also a free profession solution with GNU General Public Licensing (GPL) version 2.

Currently, VirtualBox executes on several host operating system such as Macintosh, Solaris, Linux and Windows host and provides supports for the installation of the following guest operating system; Windows operating systems, DOS / Windows 3.x, Linux, Solaris, OS/2, open Solaris, and OpenBSD. Development of VirtualBox is actively done ensuring frequent releases with an ever increasing list of features, supported guest OS and host platform. In order to ensure the product always meets professional standards, Oracle have a VirtualBox community for contributions.

3.4.3 Installing Virtualbox

To start installing the VirtualBox, a VirtualBox setup or executable file is needed. To get the VirtualBox installer package, it is available for free from the developer's website, <http://www.virtualbox.org>. Ensure that the downloaded installer package rightly corresponds to the correct version of your host operating system. In this experiment, the VirtualBox is installed on a Windows OS (Windows 8), which is the host operating system. There are multiple choices for Linux versions, therefore choose the package that matches your host OS.

After downloading the correct version of the VirtualBox installer package, double – click the setup file to display the dialog box



Figure 3.1: Initial setup screen of VirtualBox Installer

Following the instructions on the dialog box and subsequent dialog boxes whilst keeping all of the options set to their default settings will result successful installation of the Virtual Machine Monitor in this instance, the VirtualBox

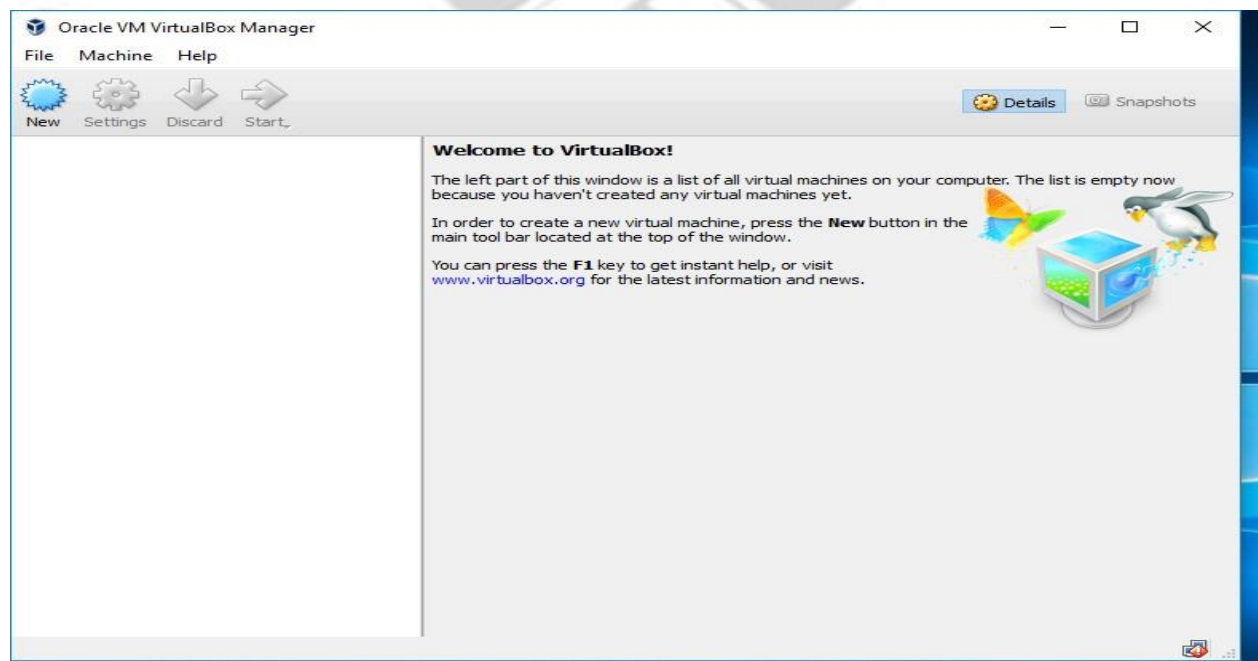


Figure 3.2: Window of a newly installed VirtualBox

3.4.4 Setting up the Forensic Platform on the Virtual Machine

Having successfully installed the VirtualBox, a digital forensic investigative platform is setup on the virtual desktop environment using an open source operating system integrated with forensic investigative tools called Kali Linux.

Kali Linux is a Debian – based Linux distribution with a collection of security and forensics tools designed for digital forensics, penetration testing and other security related tasks. It is an open source project that is maintained and funded by Offensive Security Limited, a leading information security training company. It features timely security updates, support for ARM architecture, and a seamless upgrades to newer versions. Released in 2013, Kali Linux is a complete, top – to – bottom rebuild of BackTrack Linux, adhering completely to Debian development standards.

The following steps will outline how to setup the digital forensic investigative platform on the virtual desktop using Kali Linux;

To install Kali Linux on the VirtualBox or in the virtual desktop environment, we will execute the following related tasks;

- Creation of a new Virtual Machine
- Creating a new Virtual Disk Infrastructure (VDI), preferable using dynamic allocation option.
- VirtualBox settings modification which include the allocation of physical and logical memory, selecting OS Type, CPU acceleration, etc.
- Loading the Kali Linux ISO file
- Booting the Kali Linux ISO file to install the OS on the virtual desktop environment
- Finalizing installation and running Kali on VirtualBox

After launching the VirtualBox application, click on the “New” button or press Ctrl + N keys to display the dialog box below;

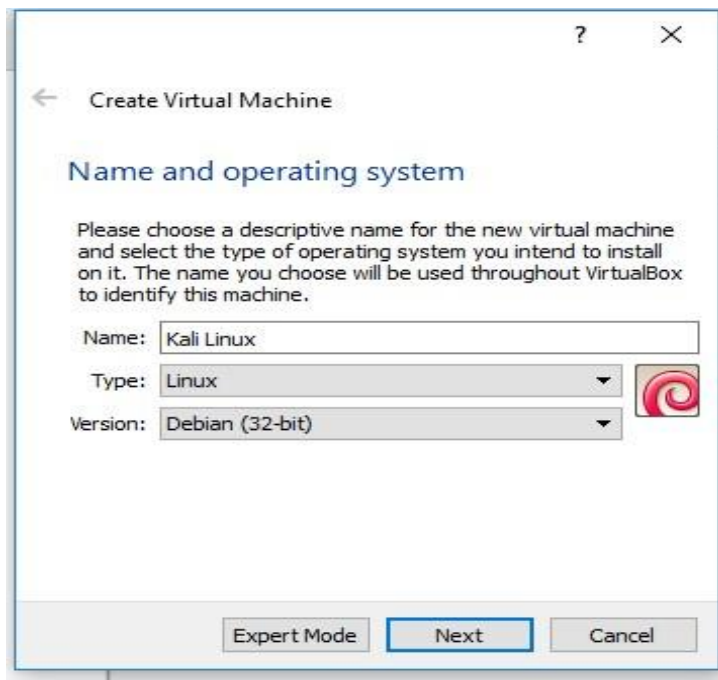


Figure 3.3: Virtual Machine creation screen

Choose the name for the virtual machine, E.g: Kali Linux. Choose the OS type as “Linux” and version as “Debian (32 – bit)”. The Debian (32 – bit) corresponds to the version of Kali Linux OS being installed for this experiment. Click on “Next” to proceed.

Next is to allocate memory / RAM for the virtual machine. The default is 256MB but change it to 1024 MB (1GB) and click the “Next” button to proceed.

For the creation of the virtual machine hard disk drive. Select the “Create a virtual hard drive now” option and click on the “Create” button in order to create a new virtual disk.

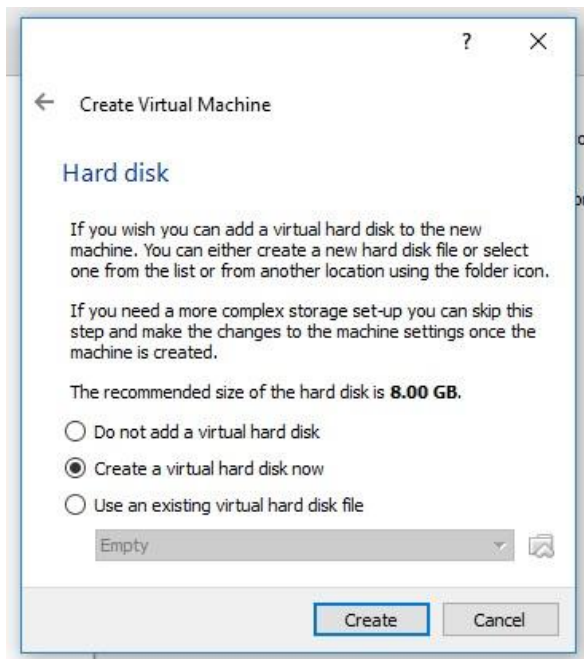


Figure 3.4: Window for creating VM Hard disk

In the dialog box that appears next, select the option, “VirtualBox Disk Image (VDI)” and click the “Next” button. In the next dialog box that pops up, select Dynamically Allocated and click “Next” on the Storage on Physical hard drive screen.

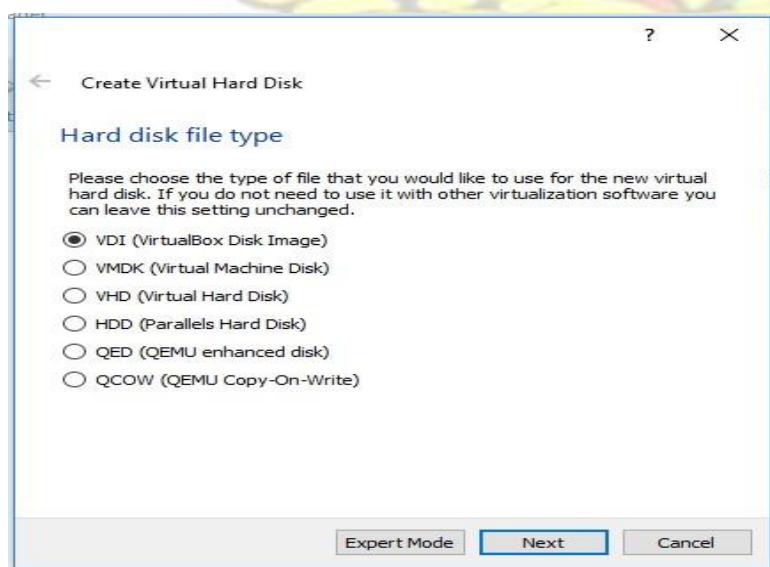


Figure 3.5: VirtualBox Disk Image (VDI) screen

Now, select Physical hard drive allocation type. Allocate at least 20 GB of storage disk size for the instance of virtual machine and click the button captioned “Create”.

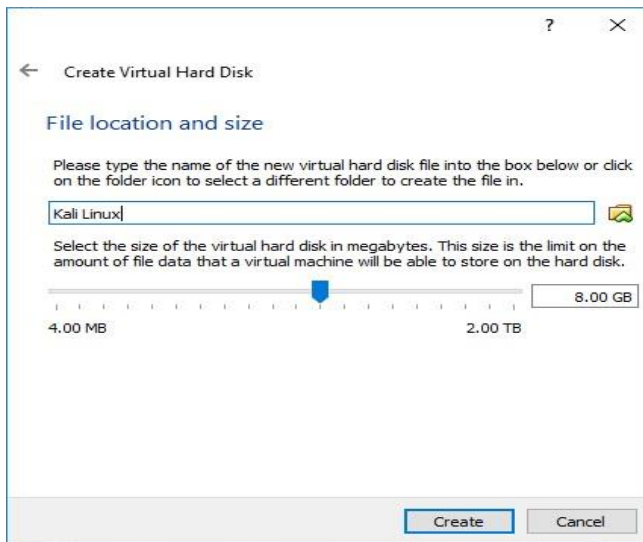


Figure 3.6: Virtual Hard Disk Infrastructure screen

The virtual machine instance is now created. Hence the time is now appropriate to boot into the selected operating system or digital forensic investigation platform.

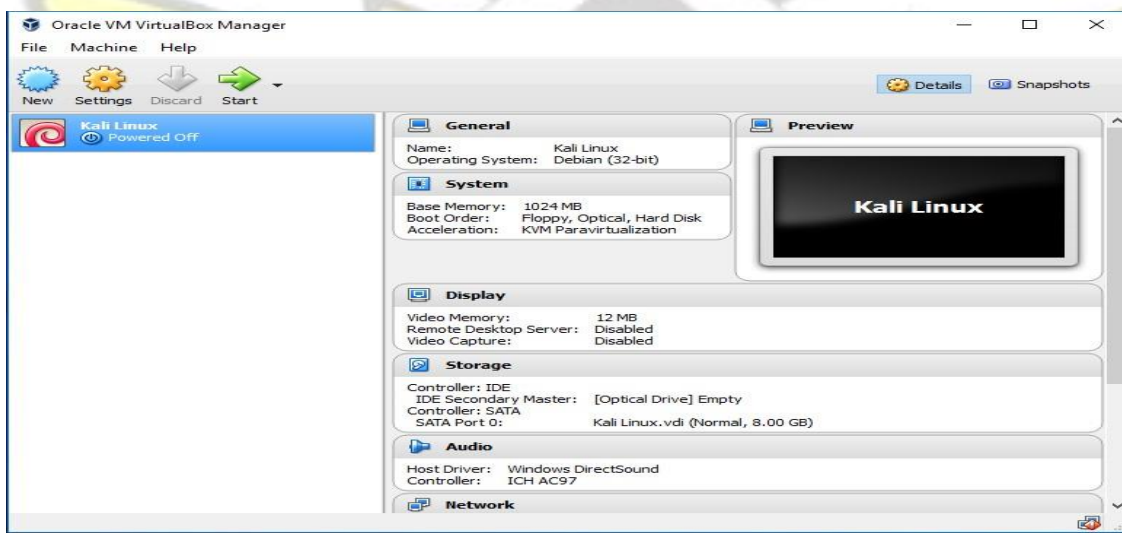


Figure 3.7: Newly created Virtual Machine screen

Before booting into Kali Linux, few changes ought to be made. Click on the “Settings” buttons to display the Settings dialog box. Click on the tab labelled “System” and select the processor and enable the option “Enable PAE / NX” and click button captioned “OK”.

Finally, run the virtual instance and browse to locate the Kali Linux ISO file and click start to begin the installation process. From the screen that pops up, select the option “Install” and press the “Enter” key whilst effecting the necessary configurations.

3.4.5 Conducting Digital Forensic Investigation

In investigating a suspect’s storage drive, we will virtually perform the following

- tasks; i. Secure the evidence ii. Photograph the evidence iii. Maintain the chain of custody iv. Make an image of the device
- v. Perform a forensic analysis on the image drive and not on the drive itself.

Out of the above enumerated tasks, the first three tasks is physically done hence the concentration will be on the fourth and fifth tasks which will be done with a digital forensic platform or laboratory.

3.4.6 Forensic Imaging

Forensic imaging simply implies making forensic copies. Forensic copies may be a logical copy or a physical copy.

Logical copy is done using the following commands: **copy, cp, copy and paste**. In digital forensic investigation, deleted data cannot be recovered using any of these commands since the deleted data is allocated in free space.

Physical copy copies all data, whether allocated and unallocated data bit by bit from beginning to the end. Commands used for making physical copy includes; **dd, dcfldd, dd_rescue, FTK Imager (Windows)**.

The other term for physical copy also include Bit – Stream, Bit – level, image and clone. When making a forensically sound copy, it is important to have a write blocker. The write blocker prevents any alteration of the data and probable destruction of the disk.

Pseudocode for imaging the drive

- i. Find the drive to be image ii. Create file in the
- mount directory iii. Mount the image that was created
- iv. Browse into the mount directory to view its content
- v. Change to the root directory in order to access the image file

Implementing the pseudocode for imaging the drive

Launch the terminal from the Kali Linux OS and run the following commands in the terminal. Each command or line of code can be viewed as a function. These functions are not piped, neither have they been grouped to run in batch as a batch file. Each command (pre – defined function) is run individually with different output, however the commands in totality will result in the creation of a forensically sound image of a drive. // **command for creating the image of the suspected drive**

```
fdisk -l cd /root / Desktop / dcfldd if = /dev
```

```
/sdb1 of = image.dd mkdir /mnt/recover
```

```
mount /root/Desktop/image.dd /mnt /recover
```

```
cd /mnt
```

```
ls
```

```
cd /recover cd
```

```
/root/ Desktop
```


Discussion of the code

The sequence of code above does numerous but distinct tasks.

The **fdisk -l** command displays the storage devices including the storage drive under investigation. In this instance the device under study is identified as **/dev/sdb1**

The **cd /root/Desktop/** command changes the directory to the Desktop. To test if your current directory is the desktop, enter the **pwd** command at the terminal. The result will display **Desktop**

The **dcfldd** command or pre – defined function creates the image or clones the storage medium. As a function, it takes two arguments or attributes, the **if (input file)** and **of (output file)**. The **if** attributes takes the storage drive as an input file and produces the image file with the file name provided in the **of** attribute.

The **mkdir /mnt/recover** command create a directory called recover in the **mnt** directory.

After creating the recover directory in the mnt directory, **mount /root/Desktop/image.dd /mnt/recover** command mount the image file unto the recover directory created within the mnt directory.

The **cd /mnt** command change the directory into the mnt directory making it the current directory.

The **ls** command displays the content of the current directory (/mnt).

The **cd /recover** changes the directory into the recover directory which now is the point where the image file is mounted.

Finally, the **cd /root/Desktop/** changes the directory to the Desktop for further digital forensic examination or analysis to be done.

3.4.7 INVESTIGATING THE DISK IMAGE

After the cloning the disk or creating the image of the disk, digital forensic investigation will be conducted on the image file to retrieve and analyze the deleted data. Investigation is preferably done on the image file to the actual device so as not to alter the original evidence.

To ensure the integrity of the image file, the image is hashed to get the checksum using the md5 hashing algorithm. To hash the image using the md5 hash algorithm, enter the code below at the terminal; **md5sum image.dd**

After entering the code, a checksum or a string of unique characters are displayed as output. This is done to check integrity in that, any change(s) done to the content of the image file will produce a different checksum as an indication of possible tempering when the **md5sum** command is invoked on the altered image file.

File carving

The process of recovering and investigating a deleted is referred to as file carving. In this experiment two forensic tools are used to perform the file carving, namely foremost and scalpel. This was done so that some comparative analysis could be done on the two forensic tools with respect to the rate of execution and the output of the tools.

Foremost

Foremost is a console – based forensic tool for the recovery of files and data based on the file or data's headers, footers and internal data structure. Foremost can work on image files, such as those generated by dd, dcfldd, etc or directly on a drive. The headers and footers can be specified by a configuration file or using a command line switches to specify built – in file types.

Scalpel

Scalpel is a fast file carver based on Foremost. The definition list for scalpel is at **/etc/scalpel.config**. Scalpel reads the configuration file on startup that defines the types of files that should be carved. The scalpel file carver detect many different file types. It does not matter which file system the disk has been formatted with; scalpel uses a database with headers and footers for various file type to trace files.

Using Foremost for file carving

Is not a Graphical User Interface (GUI) forensic tool, hence commands are used to undertake forensic investigation. Foremost has several options which may be combined to get a desired result. Perceive the foremost command as a function and the options as the arguments for the function.

The syntax for using the foremost command as well as brief descriptions for the options or attributes are shown below; **foremost** [-v | V | -h | -T | -Q | -q | -a | -w -d] [-t <type>] [-s <blocks>] [-k <size>] [-b <size>] [-c<file>] [-o <dir>] [-i <file>]

Table 3.1: Foremost command options and descriptions

Options	Description
---------	-------------

-V	Displays copyright information and exit
-t	Specify file type (-t jpeg, pdf, ...)
-d	Turn on indirect block detection (for UNIX file systems)
-i	Specify input file (default is stdin)
-a	Write all headers, perform no error detection (corrupted files)
-w	Only write the audit file, do not write and detected files to the disk
-o	Set output directory (defaults to output)
-c	Set configuration file to use (defaults to foremost.conf)
-q	Enables quick mode. Search are performed on 512 byte boundaries
-Q	Enables quiet mode. Suppress output messages Verbose mode. Logs all messages to screen.
-v	

With this brief insightful information on the foremost forensic tool, the code below demonstrates how to retrieve deleted information and undertake forensic investigation using foremost. Having launched the terminal, run the following code;

```
cd /root / Desktop/
```

```
foremost -t all -v i /root /Desktop/image.dd -o /root/Desktop/recover1
```

Executing this piece of code will take some reasonable amount of time depending on the size of the image file.

After the execution of the above foremost command, all the data retrieved are organized into a directory on the desktop named “recover1” as shown

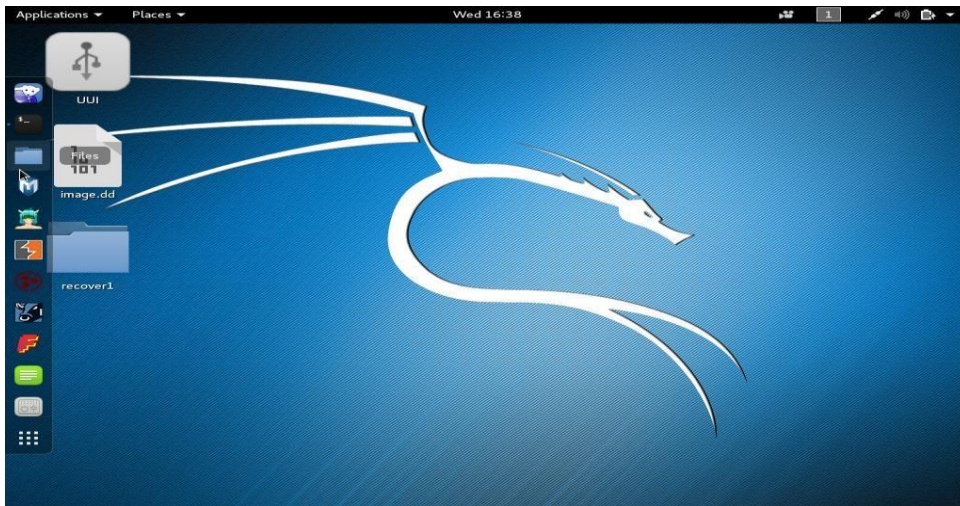


Figure 3.8: Screen showing the recover1 directory

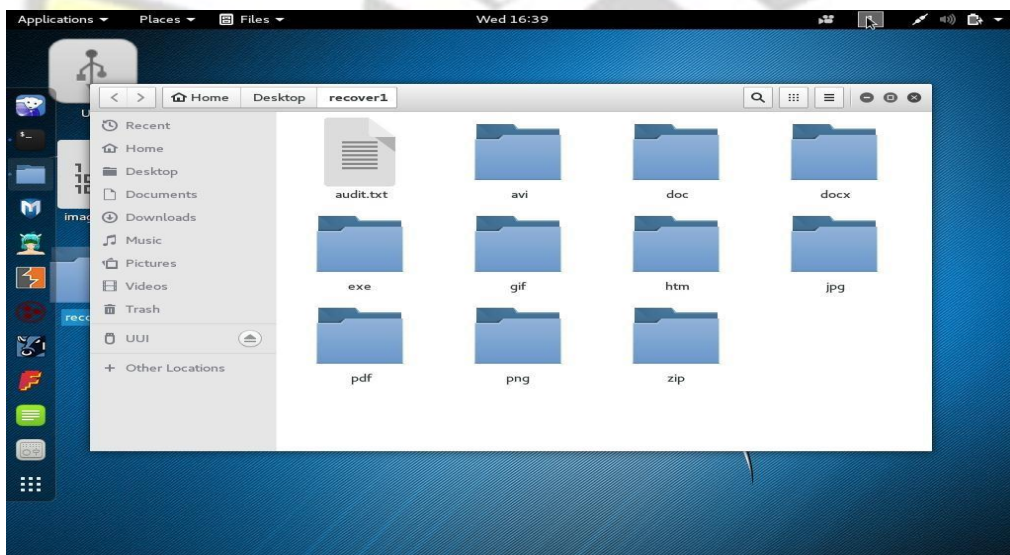


Figure 3.9: Screen showing the content of recover1 directory

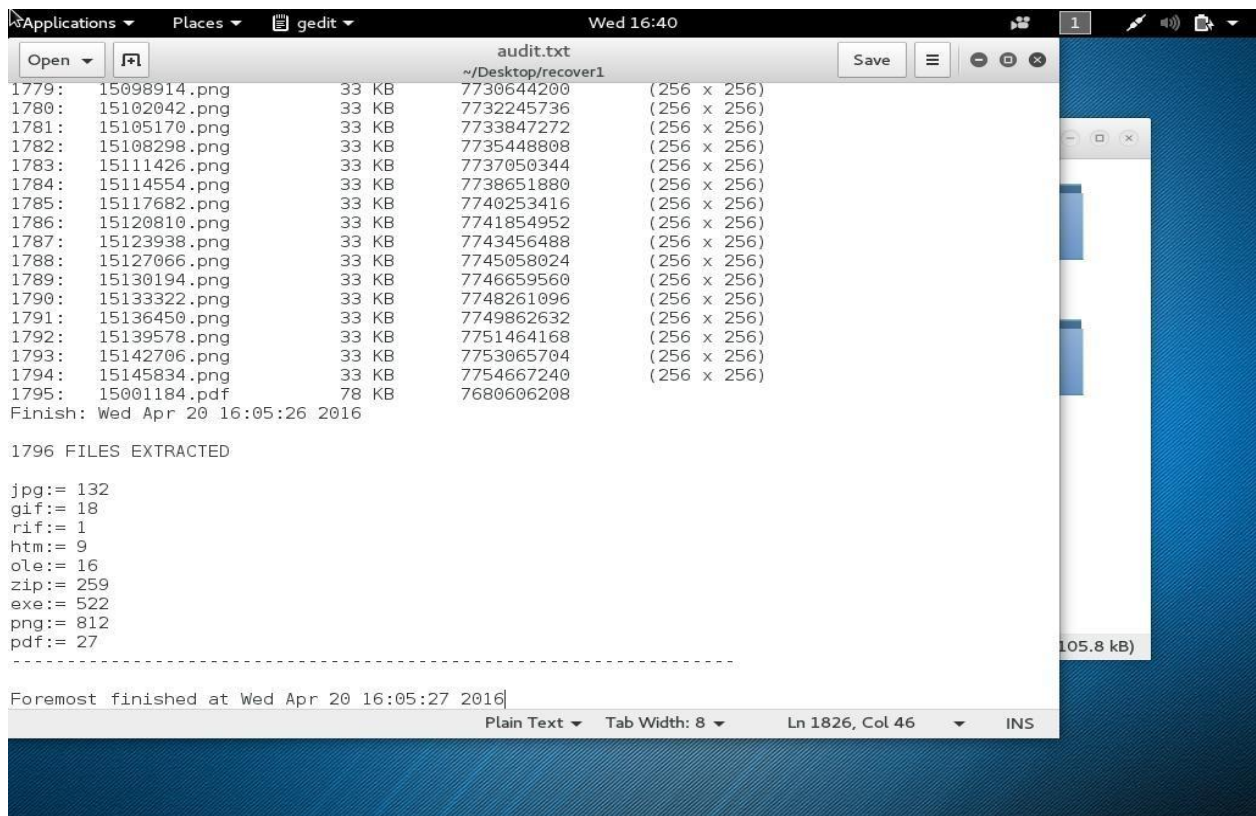


Figure 3.10: Foremost Audit File

Using scalpel for file carving

As stated above, since scalpel forensic tool was built on foremost, it does not have a Graphical User Interface (GUI) but rather console based. Before undertaking the forensic investigation using scalpel, let look at its syntax and the description of the available options that come with the scalpel command.

Scalpel [-b] [-c <config file>] [-d] [-h | V] [-i <file>] [-m blocksize] [-n] [-o <output dir>] [-O num] [-q clustersize] [-r] [-s num] [-t <blockmap file>] [-u] [-v] <imgfile>[<imgfile>]...

Table 3.2: Scalpel command options and descriptions

Option	Description
-b	Carve files even if defined footers aren't discovered within maximum carve size for file type.
-c	Choose configuration file
-d	Generate header / footer database, will bypass certain optimizations and discover all footers, so performance suffers. Doesn't affect the set of files carved.
-h	Print this help message and exits
-i	Read names of disk images from specified file
-m	Generate / update carve coverage blockmap file. The first 32 bit unsigned int in the file identifies the block size
-n	Don't add extensions to extracted files
-o	Set output directory for carved files
-p	Perform image file preview, audit log indicates which files should have been carved, but no files are actually carved.
-q	Carve only when header is cluster – aligned
-r	Find only first of overlapping headers / footers
-s	Skip n bytes in each disk image before carving
-t	Set directory for coverage blockmap
-u	Use carve coverage blockmap when carving
-V	Print copyright information and exit
-v	Verbose mode

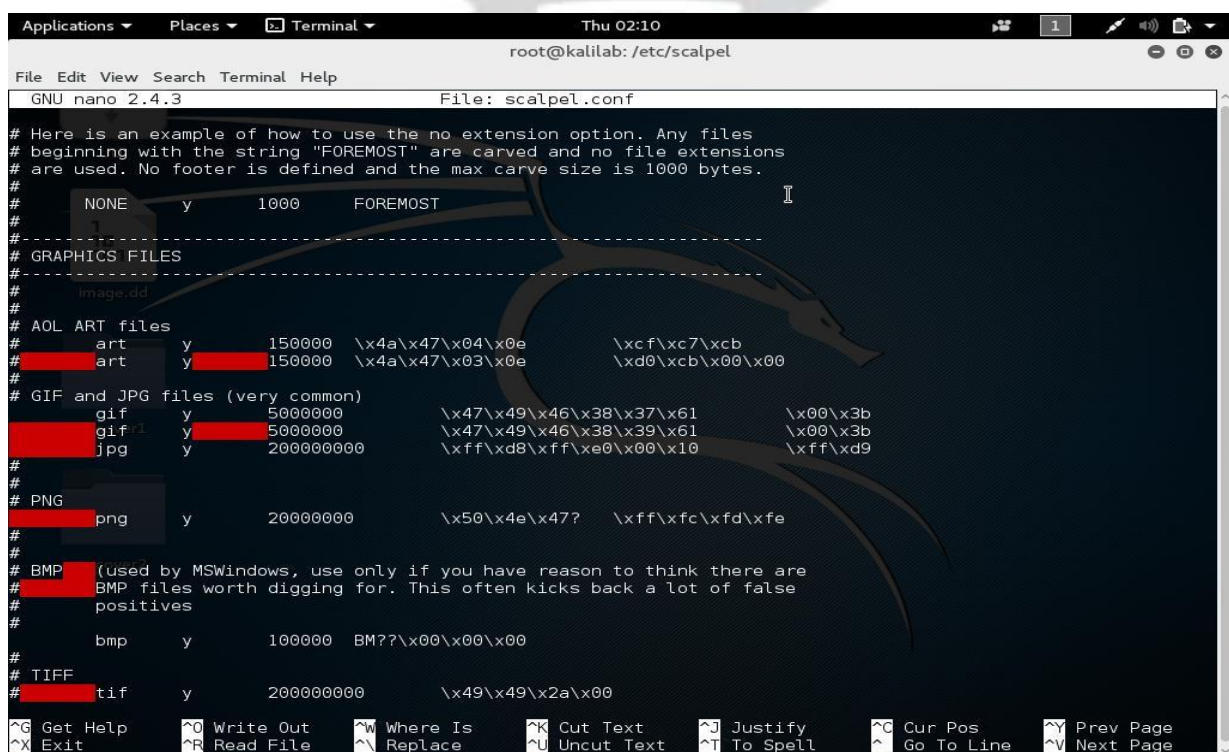
Now to conduct a forensic investigation with scalpel, changes must be made to the configuration file (scalpel.conf). The scalpel configuration file is located in the `/etc/scalpel/` directory. To configure the scalpel.conf file, run the follow code at the terminal;

```
cd /etc/scalpel/
```

```
ls
```

```
nano scalpel.conf
```

After entering the command **nano scalpel.conf** the content of the configuration file will be display as shown



```
Applications ▾ Places ▾ Terminal ▾ Thu 02:10
root@kalilab: /etc/scalpel

File Edit View Search Terminal Help
GNU nano 2.4.3 File: scalpel.conf

# Here is an example of how to use the no extension option. Any files
# beginning with the string "FOREMOST" are carved and no file extensions
# are used. No footer is defined and the max carve size is 1000 bytes.
#
# NONE y 1000 FOREMOST
#
#-----
# GRAPHICS FILES
#-----
# image.dd
#
# AOL ART files
# art y 150000 \x4a\x47\x04\x0e \xcf\xcb\xcb
# art y 150000 \x4a\x47\x03\x0e \xd0\xcb\x00\x00
#
# GIF and JPG files (very common)
# gif y 5000000 \x47\x49\x46\x38\x37\x61 \x00\x3b
# gif y 5000000 \x47\x49\x46\x38\x39\x61 \x00\x3b
# jpg y 200000000 \xff\xd8\xff\xe0\x00\x10 \xff\xd9
#
# PNG
# png y 20000000 \x50\x4e\x47? \xff\xfc\xfd\xfe
#
# BMP (used by MSWindows, use only if you have reason to think there are
# BMP files worth digging for. This often kicks back a lot of false
# positives
#
# bmp y 100000 BM??\x00\x00\x00
#
# TIFF
# tif y 200000000 \x49\x49\x2a\x00

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos ^Y Prev Page
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line ^V Next Page
```

Figure 3.11: Scalpel configuration file

After making the changes to the scalpel configuration file, press Ctrl + X keys to exit the configuration mode. To conduct the forensic investigation with the scalpel tool, run the following code;


```
cd /root/Desktop/
```

```
scalpel /root/Desktop/image.dd -o /root/Desktop/recover2
```

After running the `scalpel /root/Desktop/image.dd -o /root/Desktop/recover2` command, the analysis and file retrieval process take some time. After the investigation or file carving process, the results is displayed as shown

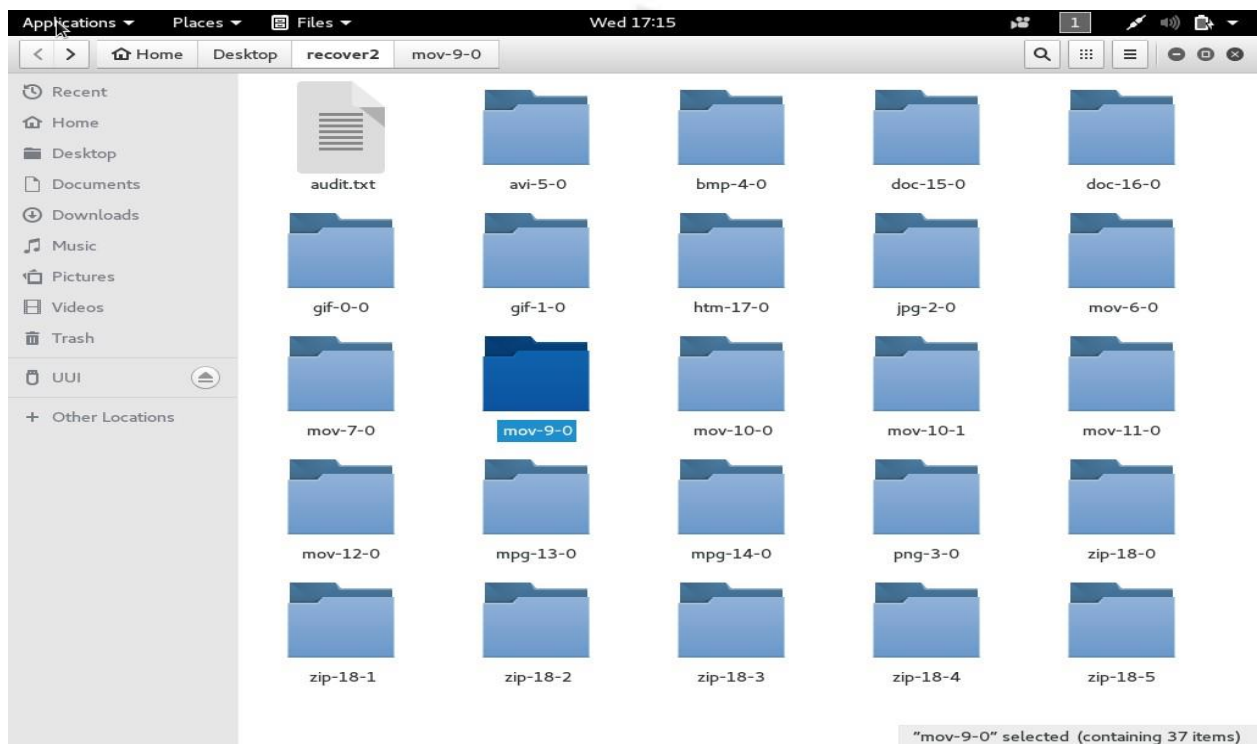


Figure 3.12: screen showing content of recover2 directory

CHAPTER FOUR

FINDINGS AND DISCUSSIONS

After reviewing previous knowledge in chapter two of this work, a critical analysis is presented on how to use desktop virtualization as a platform to conduct digital forensic investigation and the benefit derived from such technological advancement.

In this research work, the following were implemented; a virtual desktop environment was created using Oracle VirtualBox virtual machine monitor, the digital forensic platform was setup on the virtual desktop environment using a Debian – based OS integrated with forensics and security related tools. Forensic imaging was done to clone the suspected drive and investigations were done using forensics tools notably foremost and scalpel.

This chapter peruses the findings of the research methodologies and discusses the results. It also does some comparative analysis of the forensic tools and how to use the outcome to improve an existing digital forensic model.

4.0 Experiment

The Oracle VirtualBox was installed and used to setup the virtual desktop environment. This virtual environment provided an emulated platform to run a Debian – based OS tailored for forensic investigations and other security related tasks.

The virtual desktop used in the experimentation helped to attained the under listed benefits;

1. Successfully installing the Kali Linux OS without fear of messing up the file system of the host OS.
2. Easily reverting to a safe state when configuration did not produce expected results
3. Run the Guest OS irrespective of the underlying hardware architecture.

4.1 Repetitive Hashing

Guided by the ultimate goal of undertaking digital forensic research, which is to retrieve digital evidence admissible in court of law, hashing algorithm was used in the experiment. Thus, the **md5** hashing algorithm was evoked or used to encrypt the disk image in order to easily identify any alteration to the content of the disk image.

This was done to ensure the integrity of the image file under investigation. During the experiment, the **md5** hashing command and the result produced are shown below.

4.2 Code listing for hashing the image file using md5 hash

```
cd /root/Desktop/
```

```
md5sum /root/Desktop/image.dd
```

After the image file was hashed using the **md5** hashing algorithm, the forensic research was then conducted on the image file using the foremost forensic tool.



```
Applications ▾ Places ▾ Terminal ▾ Fri 10:53 1
root@kalilab: ~/Desktop
File Edit View Search Terminal Help
root@kalilab:~/Desktop# md5sum /root/Desktop/image.dd
90600322400788423fb302485e36878a /root/Desktop/image.dd
root@kalilab:~/Desktop#
```

Figure 4.1: The md5 hashing algorithm screen

The **md5** hashing algorithm was again applied to the image file to find its checksum. This was done in order to compare the value of the checksum in each instance to ascertain whether the content has been compromised or not.

The same hashing check of the image checksum is done for the image file after investigation was conducted on the image file by using the **scalpel** forensic tool as well.

4.3 Comparative study on the forensic tools

During the experiment, the original disk was cloned using the **dcfldd** tool. After the forensic imaging of the disk, forensic investigation was done using two popular file carving tools, namely; **foremost** and **scalpel**. Previous sections considered the forensic tools into details.

However, after using both digital forensics tools the following results or observations were made

- i. Considering the size of the image file which was examined the task was completed quickly using the **scalpel** forensic tool compared to the **foremost** given the same image file size and same platform.
- ii. Literally comparing the results of retrieved data by both forensic tools, it is obvious that the scalpel forensic tools retrieved enough data files compared to the foremost forensic tool.
- iii. In the usage of both forensic tools, it is obvious the scalpel forensic tool is relatively difficult than the usage of the foremost forensic tool. In that, in order to use the scalpel to get the acquired results, extra configuration first need to be done to the **scalpel.conf** file. This is not the case with the foremost tool whose configuration file comes already configured. The table shows a summary of the comparative analysis of the forensic tools.

Table 4.1: Comparative analysis of Foremost and Scalpel forensic tools

Forensic Tools	Foremost	Scalpel
Rate of Execution	Execution of the foremost command is fast	Execution of the scalpel command is faster than the foremost
Detailed of Retrieved Data	Quantity of data retrieved is less than scalpel	Extra data are retrieved depending on the configuration.
Difficulty of Usage	Relatively easier to be used	Some extra work need to be done during usage

4.4 Proposed Forensic Model

In this section, a model which improves or enhances an existing digital forensic investigation model called Computer Forensics Field Triage Process Model (CFFTPM) is proposed based

on the experimentation and the results obtained. The proposed model is called the **Enhanced Computer Forensics Field Triage Process Model (ECFFTPM)** which inculcates the concept of virtualization into the digital forensic investigation process.

The proposed model combines the benefits of Computer Forensics Field Triage Process Model (CFFTPM) with the need to undertake thorough investigation on the site or crime scene. This will enhance the initial goal or benefits of CFFTPM, which is the solicitation of usable evidence immediately, identification of victim at acute risk and identifying potential charges.

CFFTPM which has been reviewed in chapter two of this research project was proposed by Marcus K. Rogers et. al (2006). The existing model is needful in situations where quick information and investigation leads outweigh the need for an in – depth analysis of all the potential digital evidence back in a laboratory. The CFFTPM which is the existing model has six (6) main phases with two (2) of the phases having three (3) sub – phases each. The phases are, Planning, Triage, User Usage Profile (Home, File Properties, Registry), Chronology Timeline, Internet (Browser, Email, IM) and case Specific. After carefully reviewing the Computer Forensics Field Triage Process Model, some inherent challenges were identified which the proposed model seeks to solve using virtualization.

The proposed model appreciate the need to retrieve digital evidence in a timely manner which is one of the foci of the existing model. However, the Enhanced Computer Forensic Field Triage Process Model augment the existing model with the notion that, the need for quick information is not an implication for grossing over thorough search and forensically inclined experiments. Virtualization technology can help to provide and extension of the existing lab at the crime scene. This implies, through virtualization technology, a virtual forensic laboratory is created on site or the victim's crime scene. This research experiment provides the basis for the proposed model which seeks to improve the CFFTPM with the concept of virtual digital

forensic platform. The virtual digital forensic platform which was demonstrated in the experiment using Desktop virtualization will serve as an extended lab for further investigation right on the site.

Another inherent drawback realized from reviewing the CFFTPM model was that it seems incomplete. In that, this digital forensic investigation model focuses on gathering evidence from the crime scene. However, the digital forensic investigation normally extends beyond the crime scene hence the need to boost the extent of investigative work or activity carried on the crime scene. This may be greatly achieved by extending the investigative platform or environment on the scene using virtualization technology. Having demonstrated in this research experiment that forensic investigation can be conducted on the virtual desktop platform. The concept of desktop virtualization was then augmented to the Computer

Forensic Field Triage Process Model to define the proposed model which is the Enhanced Computer Forensic Field Triage Process Model.

4.5 Comparative Analysis

This section makes a comparative analysis of some existing digital forensic models and the proposed model. Table 4.2 looks at the number of phases in each of the models whilst table 4.3 looks at the functionalities of the forensic process models. Forensic process models were defined by different researchers to consist of multiple steps. Some process models had limited number of steps while others had elaborate number of steps. It is worthy to know that the number of steps in a forensic process model is not an implication of the usefulness or otherwise of the process model.

Table 4.2: Phases of some forensic process models

ADFM	IDIP	EDIP	CFFTPM	GCFIPM	PROPOSED MODEL
2002	2003	2004	2006	2011	2016

9 Phases	5 Phases	5 Phases	6 Phases	5 Phases	7 Phases
Identification	Readiness	Readiness	Planning	Pre – process	Planning
Preparation	Deployment	Deployment	Triage	Acquisition & Preservation	Triage
Approach Strategy	Physical Crime Scene Investigation	Trace back	User usage Profile	Analysis	Virtual Investigation
Preservation	Digital Crime Investigation Scene	Dynamite	Chronology Timeline	Presentation	User Usage Profile
Collection	Presentation	Review	Internet	Post – process	Chronology Timeline
Examination			Case specific		Internet
Analysis					Case specific
Presentation					
Returning evidence					

The next comparative analysis is done on the inherent features or attributes of the selected models shown reviewed in this research. From the table above, it is obvious different nomenclature is used for the various phases of the digital forensic model.

In view of that a more generic name which take in cognizance the task undertaken in each phase of the forensic model will be adapted to do the comparative studies. Table 4.3 compares the features of the selected forensic process model with the proposed model.

Table 4.3: Comparison of features of selected digital forensic models with the proposed

Features or Attributes	ADFM	IDIP	EDIP	CFFTP	GCFIP	PROPOSED MODEL

Planning & Scope Definition	Yes	Yes	Yes	Yes	Yes	Yes
Securing Crime Scene	No	Yes	Yes	Yes	No	Yes
Evidence Identification	Yes	Yes	Yes	Yes	Yes	Yes
Evidence Collection	Yes	Yes	Yes	Yes	Yes	Yes
Evidence Retrieval	Yes	Yes	Yes	Yes	No	Yes
Evidence Analysis	Yes	Yes	Yes	Yes	Yes	Yes
Results Presentation	No	Yes	Yes	Yes	Yes	Yes
Virtual Investigation	No	No	No	No	No	Yes

4.6 Conclusion

After successfully conducting an experiment by setting up a virtual desktop environment, installing and setting up a digital forensic investigative platform, and conducting forensic investigation in the virtual desktop environment. The experiment conducted showed that, virtualization technology can be used to enhance digital forensic investigations thereby improving the digital forensic process model.

The following conclusion was drawn from the observations

Since digital forensic platform and investigation was successfully done on the virtual desktop, it can serve as a means of allowing novice investigators or professionals to examine digital evidence without compromising on the integrity of the original evidence. Also, the forensic investigation undertaken in the virtual desktop environment buttress the fact that laboratory activities can be undertaken on site to assist in retrieving relevant and timely evidence. Hence the proposed model.

CHAPTER FIVE

CONCLUSION AND FUTURE WORK

5.0 Conclusion

Digital forensics investigation may be appropriately described as an evolving phenomenon rather than a new field of study due to the dynamism in relation to new threats and new practices encountered as a result of the increasing growth in the proliferation of technology and digital data representation. In – depth searching and fishing out for the “relevant” information in a forensic case is a vital aspect in digital forensics investigation. In line with this focus, investigations should be systematically guided, led by professional experts, customized for the particular case and forensically sound enough to make the investigative process or procedure to be executed in a short time frame resulting in the collection of enough essential information for further investigation.

The development of several forensics investigation models is therefore designed to provide a well-tailored, accurate and efficient means of acquiring, authenticating and analyzing digital evidence while ensuring the integrity and sanctity of the evidence to make it admissible in court of law. However, most of these models reviewed in a section of this research work revealed they were not focused to cater for virtualization which is one of the emerging technologies that can be used to enhance and improve the digital forensic investigation process. This research looked to integrate virtualization technology into the digital investigation process to enhance the existing process model.

Previous sections of this research have revealed some of the works that have been conducted in this area and this work happens to be in line with most of the research already conducted.

Objectives that were outlined for the research have also been met and thorough study and implementation of digital forensic investigation in a virtual environment to improve the process model also well established.

Observation made clearly indicates that, using virtualization to undertake digital forensic investigation is more efficient method in enhancing the digital investigation process as opposed to the conventional process model which normally does not target virtual environment. This goes a long way to sustain optimal performance with the rate of undertaking investigation.

To conclude, the functionality of inculcating or conducting digital forensic investigation in a virtual desktop environment has been introduced, and as well explored the ways in which these areas of research have begun to overlap over the last few years. It is observed that using desktop virtual environment offer tremendous potential benefits for both novice and professional investigators as well as enhancing the existing digital forensic process model.

5.1 Recommendations

Virtualization technology includes network virtualization, application virtualization, Storage virtualization, server virtualization and desktop virtualization. The capabilities of these virtualization technologies can be harnessed to augment the digital forensic investigation process.

Moreover, the need for thorough digital forensic investigation is necessary and urgent in this era of escalating digital related crimes. Such laboratory facilities could be setup to enhance further research and intense investigation.

5.2 Future Works

Attention must be paid to the exploration of better improvements in the areas of inculcating or harnessing the benefits of virtualization to improve and enhance digital forensic investigation and process models.

Secondly, the codes or commands in this research were run on a Linux based guest operating system or environment. Future works may be done to ascertain the viability of running the same code or its modifications on the different platforms to evaluate their performance.

Virtualization technology is being embraced in other computing areas such as network, storage, application, server and desktop. Future works could be done on how to put all these technologies together to build or establish a definition for setting up a virtual lab for virtual digital forensic investigation.

Lastly, digital forensic investigation in a virtual environment is a fascinating area and seems to have a promising future.



REFERENCES

- Ajjola, A., Pavol, Z. and Ron, R. (2012). A review and comparative evaluation of forensics guidelines of NIST SP 800101 Rev.1:2014 and ISO/IEC 27037:2012, World Congress on Internet Security (WorldCIS2014), 2014.
- Brian, C. and Eugene, H. S. (2003). Getting Physical with the Digital Investigation Process. International Journal of Digital Evidence, Fall 2003, Volume 2, Issue 2.
- Broad, J. and Andrew, B. (2014). Building a Penetration Testing Lab, Hacking with Kali.
- Casey, E. (2011). Digital evidence and computer crime: forensic science, computers, and the Internet, 3rd ed. London: Academic Press, 2011.
- Cisar, P. and Sanja, M. C. (2011). Methodological frameworks of digital forensics, 2011 IEEE 9th International Symposium on Intelligent Systems and Informatics.
- Chow, J., B. Plaff, T. Garfinkel, K. Christopher, and M. Rosenbleum. (2004). Understanding Data Lifetime via Whole System Simulation, Proceedings of the 13th USENIX Security Symposium.
- Derek, B., Francine, F., Ewa, H. and Oscar, B. (2008). Computer Forensics – Past, Present and Future. Journal of Information Science and Technology (JIST 5(3))
- Derek, B. and Ewa, H. (2007). Computer Forensic Analysis in a Virtual Environment. International Journal of Digital Evidence, Fall 2007, Volume 6, Issue 2
- Deqing, Z. (2009). Trusted Deployment of Virtual Execution Environment in Grid Systems. Lecture Notes in Computer Science.
- Diane, B. (2010). How Virtualization Happens, Virtualization and Forensics.
- Flores, C., Juan, C., and Travis, A. Digital forensics on a virtual machine, Proceedings of the 49th Annual Southeast Regional Conference on ACMSE 11 ACMSE November, 2011.

- Garfinkel, S. and Shelat, A. (2003). Remembrance of Data Passed: A Study of Disk Sanitization Practices, IEEE Security and Privacy
- Gary, L. P. (2001). A Road Map for Digital Forensic Research. Technical Report DTR – T0010-01, DFRWS. Report for the First Digital Forensic Science Communications, Vol. 2 No. 4
- Greg, D., Chris, M., Scott, C. and Philip, C. (2009). Analyzing the impact of a Virtual Machine on a host machine. International Federation for Information Processing.
- Gulsan, S., Kavita, S. and Akansha, D. (2012). Forensic Computing Models: Technical Overview.
- Guo, H., Daoli, H. and Ying, Z. (2011). Implication of Virtualization Technologies in Computer Forensics, Energy Procedia.
- Juan, C. F., and Travis, A. (2011). Digital Forensics on a Virtual Machine.
- Kent, K., Chevalier, S., Grance, T. and Dang, H. (2006). Guide to Integrating Forensics into Incident Response. Special Publication 800 – 86, Computer Security Division Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD.
- Kristin, F. and Catherine, A. T. (2008). Cybercrime: Conceptual Issues for Congress and U.S Law Enforcement Electronic CSI, A Guide for first responders, 2nd edition, National Institute of Justice.
- Kruse II, W., and Jay, G. H. (2002). Computer Forensics: Incident Response Essentials. Addison – Wesley.
- Lee, H., Palmbach, T. and Miller, M. (2001). Henry Lee's Crime scene Handbook. London: Academic Press

- Marcus, K. R., James, G., Rick, M., Timothy, W. and Steve, D. (2006). Computer Forensics Field Triage Process Model. *Journal of Digital Forensics, Security and Law*, Vol. 1 No. 2
- Mark, R., Clint, C., and Gregg, G. (2002). An Examination of Digital Forensic Models. *International Journal of Digital Evidence*, Fall 2002, Volume 1, Issue 3.
- Michael, N., Mark, M. P. and Lawrence, P. (2000). Recovering and Examining Computer Forensic Evidence, *Forensics Science Communications*, Vol. 2, No. 4
- Philip, C., Paul, B., Chris, M. and Mark, P. (2008). A Virtual Digital Forensics Laboratory, IFIP – The International Federation for Information Processing.
- Popek, G. J., and Goldberg, R. P., Formal requirements for virtualizable third generation architectures. Los Angeles: University of California, Honeywell Information Systems and Harvard University.
- Rebecca, G. and Jaqueline, R. (2004). Understanding Metadata. National Information Standards Organization.
- Ruan, K., Joe, C., Tahar, K. and Ibrahim, B. (2013). Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey result, *Digital Investigation*.
- Sabah, A. and Bashayer, A. (2012). Modeling the Forensics Process. *International Journal of Security and its Applications*, Vol. 6, No. 4.
- Shrivastava, G. and Gupta, B. B. (2014). An Encapsulated Approach of Forensic Model for digital investigation, 2014 IEEE 3rd Global Conference on Consumer Electronics (GCCE).
- Venansius, B. and Florence, T. (2004). The Enhanced Investigation Process Model, in proceeding of Digital Forensic Research Workshop, Baltimore, MD.

Wazid, M., Avita, K., Goudar, R. H. and Sreenivas, Rao. Hactivism trends, digital forensic tools and challenges: A survey. 2013 IEEE Conference on Information and Communication Technologies.

Yunus, Y., Roslan, I. and Zainuddin, H. (2011). Common Phases of Computer Forensics Investigative Models. International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No. 3.

