UNIVERSITY OF EAST LONDON

A Comprehensive Digital Forensic Investigation Model and Guidelines for Establishing Admissible Digital Evidence

A thesis submitted in partial fulfilment of the requirements of University of East London for the degree of Master of Philosophy (MPhil)

By

Inikpi Onechojo Ademu

School of Architecture, Computing and Engineering

University of East London

January, 2013

Director of Studies: Doctor Chris Imafidon

Supervisor: Doctor David Preston

Abstract

Information technology systems are attacked by offenders using digital devices and networks to facilitate their crimes and hide their identities, creating new challenges for digital investigators. Malicious programs that exploit vulnerabilities also serve as threats to digital investigators. Since digital devices such as computers and networks are used by organisations and digital investigators, malicious programs and risky practices that may contaminate the integrity of digital evidence can lead to loss of evidence. For some reasons, digital investigators face a major challenge in preserving the integrity of digital evidence. Not only is there no definitive comprehensive model of digital forensic investigation for ensuring the reliability of digital evidence, but there has to date been no intensive research into methods of doing so.

To address the issue of preserving the integrity of digital evidence, this research improves upon other digital forensic investigation model by creating a Comprehensive Digital Forensic Investigation Model (CDFIM), a model that results in an improvement in the investigation process, as well as security mechanism and guidelines during investigation. The improvement is also effected by implementing Proxy Mobile Internet Protocol version 6 (PMIPv6) with improved buffering based on Open Air Interface PIMIPv6 (OAI PMIPv6) implementation to provide reliable services during handover in Mobile Node (MN) and improve performance measures to minimize loss of data which this research identified as a factor affecting the integrity of digital evidence. The advantage of this is to present that the integrity of digital evidence can be preserved if loss of data is prevented.

This research supports the integration of security mechanism and intelligent software in digital forensic investigation which assist in preserving the integrity of digital evidence by conducting experiments which carried out two different attack experiment to test CDFIM. It found that when CDFIM used security mechanism and guidelines with the investigation process, it was able to identify the attack and also ensured that the integrity of the digital evidence was preserved. It was also found that the security mechanism and guidelines incorporated in the digital investigative process are useless when the security guidelines are ignored by digital investigators, thus posing a threat to the integrity of digital evidence.

PUBLICATIONS

These peer reviewed journal and conference papers have been published as a result of the research in this thesis:

Ademu, I. Imafidon, C. Preston, D. (2011a) 'Intelligent Software Agent applied to Digital Forensic and its Usefulness', Paper accepted and presented in the *International Journal of Computer Science and Informatics (IJCSI)* Issue 1,2 Volume 2, 7 September 2011, pp. 117-120 Available at http://interscience.in/IJCSI_Vol2Iss1/IJCSI_Paper_21.pdf (Accessed: 5 January 2014)

Ademu, I. Imafidon, C. Preston, D. (2011a) 'Intelligent Software Agent applied to Digital Forensic and its Usefulness', Paper accepted and presented in the proceedings of the *National Conference on Research Trends in Computing Science and Technology (NCRTCSA).* India. 7 July 2011

Ademu, I. Imafidon, C. Preston, D. (2011b) 'A New Approach of Digital Forensic Model for Digital Forensic Investigation', International *Journal of Advanced Computer Science and Applications (IJACSA)* Issue 12, Volume 2, 10 December 2011, pp. 175-178. Available at: http://thesai.org/Downloads/Volume2No12/Paper%2026-A%20New%20Approach%20of%20Digital%20Forensic%20Model%20for%20Digital%20Forensic%20Investigation.pdf (Accessed: 5 January 2014)

Ademu, I. Imafidon, C. Preston, D. (2012a) 'The Need for Digital Forensic Investigative Framework', *International Journal of Engineering Science and Advanced Technology (IJESAT)* Issue 3, Volume 2, 15 May 2012, pp. 388-392. Available at: http://ijesat.org/Volumes/2012_Vol_02_Iss_03/IJESAT_2012_02_03_01.pdf (Accessed: 10 January 2014)

Ademu, I. Imafidon, C. (2012b) 'The Need for a New Data Processing Interface for Digital Forensic Examination', *International Journal of Advanced Research in Artificial Intelligence* Issue 4, Volume 1, 4 July 2012, pp. 7-11. Available at: http://www.docstoc.com/docs/138237864/Paper-2-The-Need-for-a-New-Data-Processing-Interface-for-Digital-Forensic-Examination (Accessed: 5 January 2014)

Ademu, I. Imafidon, C. (2012c) 'Digital Forensic Acquisition and Analysis Tools and its Importance', Paper accepted and presented in the proceedings of *the 11th International Conference on e-Learning, e-Business, Enterprise Information System, and e-Government (EEE'12)* WORLDCOMP'12 Las Vegas, Nevada, USA, July 16-19, 2012. Available at: http://world-comp.org/p2012/EEE7656.pdf (Accessed: 12 January 2014)

Ademu, I. Imafidon, C. (2012d) 'Agent-Based Computing Application and its Importance to Digital Forensic Domain', Paper accepted and presented in the proceedings of the *14th International Conference on Artificial Intelligence (ICAI'12)* WORLDCOMP'12 Las Vegas, Nevada, USA, July 16-19 2012 Available at: http://world-comp.org/p2012/ICA7716.pdf (Accessed: 15th January 2014)

Ademu, I. Imafidon, C. (2012e) 'The Influence of Network on Digital Forensic', Paper accepted and presented in the proceedings of the *11th International Conference on Wireless Networks (ICWN'12)* WORLDCOMP'12 Las Vegas, Nevada, USA, July 16-19 2012 Available at: http://world-comp.org/p2012/ICW7717.pdf (Accessed: 12 January 2014)

Ademu, I. Imafidon, C. (2012f) 'Applying Security Mechanism to Digital Forensic Investigation Process', *International Journal of Emerging trends in Engineering and*

Development (IJETED) Issue 2, Volume 7, 10 November 2012, pp. 128-133. Available at: http://rspublication.com/ijeted/nov12/15.pdf (Accessed: 12 January 2014)

Ademu, I. Imafidon, C. (2012g) 'The Influence of Security Threats and Vulnerabilities on Digital Forensic Investigation', *International Journal of Computer Application* (IJCA) Issue 2, Volume 6 18 December 2012, pp. 1-6 Available at: http://rspublication.com/ijca/dec%2012/1.pdf (Accessed 10 January 2014)

Ademu, I. Imafidon, C. (2013) 'The Importance and Need for Digital Forensic Investigative Framework', Paper accepted and presented in the proceedings of the 2013 *International Conference on Artificial Intelligence (ICAI'13)* WORLDCOMP'1 3 Las Vegas, Nevada, USA, July 22-25 2013 Available at: http://world-comp.org/proc2013/icai/ICAI_Contents__Vol_II.pdf (Accessed: 10 January 2014)

Table of Contents

APPENDICES

LIST OF FIGURES

List of Tables

Definitions and Terminologies

For the purpose of this research, some definitions and terminologies are discussed as follows:

Digital Forensic Investigation

Digital forensic investigation is defined as the process of identifying, maintaining, analyzing, reconstructing and presenting digital evidence through the use of information technology to the investigation of digital attacks or incidents and preserving the digital evidence through the application of information security.

Digital Evidence

Digital evidence is defined as a data packet or digital information stored or transmitted by a digital device that support or rebut an assumption about digital incident or event that provides relationship between the cause of an incident and the victim.

Terminologies

During the review process, it was discovered that various authors used different terms such as 'model', 'procedure', 'process', 'phase, and 'task', etc. in order to describe their respective processes taken to perform an investigation. In this research of the thesis, for the purpose of standardisation the term 'model' was used to represent the entire set of activities performed in the digital forensic investigation process. The term 'phase' was used to represent the high-level components of the investigation model and the term 'activities' was used to represent task to be performed in each of the phases. The term digital object is used to represent digital devices. The term digital evidence was also used, as digital information, data and data packets.

ACKNOWLEDGEMENTS

The process of this thesis writing was a wonderful learning experience on my academic life which was filled with challenges and rewards. The completion of the present study leads a new beginning and a step forward towards my future.This preface provides a welcome opportunity and chance to appreciate God for his infinite mercy and guidance during this thesis and to acknowledge the help and assistance of the people who with their intellectual insights or constructive criticism, other times in the form of friendship have helped me to develop this research.

The dream of completing this research would not have been achieved without the support of God, who took my hands to step forward towards this dream. My gratitude goes to my Director of studies Dr Chris Imafidon for his support. I would also like to express my sincere gratitudeto my supervisor Dr David Preston I want to say thank you for your valuable supervision. I would like to thank the University of Cambridge Computer laboratory for providing support during this research.

I would like to express my sincere gratitude to my husband Mr Ojelemomu Ademu, my sons El-Favour and Ebenezar and my parent Mr and Mrs Agoh for their never-ending support and encouragement during this process. I am very grateful to my brother and sisters for their encouragement, to all my family, I want to say thank you. Without their understanding, this research would not have been achieved

Dedication

To God Almighty my Great Helper and Director who has helped me by His own hand to make this research an accomplished project. Thank you God for keeping to Your Word of strengthening, helping and upholding me with the right hand of Your Righteousness.

Chapter One: Introduction

1. Introduction

1.1 Background

The influence of information technology is pervasive in our private and professional lives. The use of the internet, email and chat groups has changed the ways in which interaction is carried out as a society. This important change is also apparent in organizations and the economy. The majority of organisations rely very much on computer systems and the Internet to operate and to enhance their businesses, relying on the system's ability to process, transmit, store and retrieve data. Sommer (2009) demonstrates that 98% of all documents in organizations are based on electronic form. A large amount of information is produced, accumulated, and distributed via electronic means. It is necessary for forensic experts to increase their abilities to gather evidence from digital devices. According to Healy (2008), approximately 85% of 66 million US dollars was lost by organizations due to digital related crimes, these were categorised as a computer related financial fraud. Panda Labs report (2009) shows that Ehud Tenenbaum was extradited from Canada on suspicion of stealing $1.5 million from a Canadian bank through stolen credentials and infiltrated computers.

The information technology has become the foundation for communications, banking, transformation etc. However, this has been capitalized on by the criminal in the society. Organisation's computers, servers and laptops have, therefore, increasingly become targets of crime and tools for committing crimes. The risk of terrorist organizations turning their attention to technology and cyberspace is very real (Rogers and Seigfried, 2004). The attention is also focused on using the technology to gather information on potential victims. Digital attacks or threats to information technology may have a

momentous impact on organisations. These threats usually lead to the disclosure of information, modification, denial of service (DoS), illegal use, identity theft or repudiation (Ciampa, 2007).

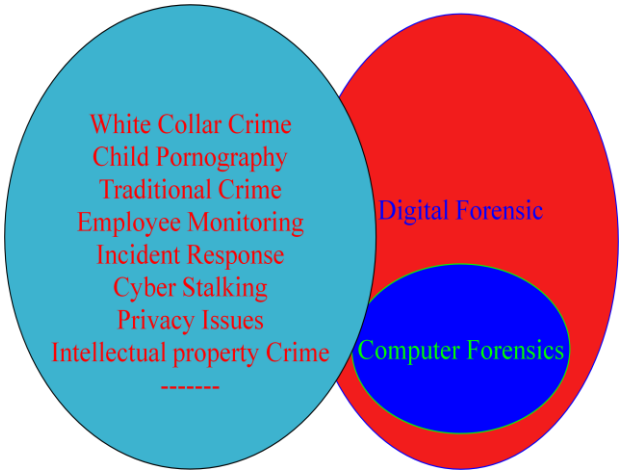


Figure 1: Contexts of Digital Forensics

Looking at the Dubai murder case reported on BBC News, Adler (2010) reports that the Dubai police believed 11 agents with six European passports were involved in the killing. In this case, there was fraudulent use of British passports. The then Prime Minister Gordon Brown was interested in carrying out forensic investigation, who said that evidence has to be collected about what actually happened, how it happened and why it happened. The Foreign Office also pledged to take actions that are necessary to protect British Nationals from identity fraud and said that the British embassy would ensure that a full investigation would be carried out into the fraudulent use of the passports. According to Adler (2010) the Serious Organised Crime Agency, who led the investigation, confirms that photographs and signatures on the passports used in Dubai did not match those passports issued by the UK. The alleged forgery raised a matter of great concern and raised the possibility that it could happen in terrorism cases.

Cole et al. (2007) believe that corporate security investigators are making increasing use of computer forensics in areas such as fraud, the accessing of pornography, and harassment and traditional criminal investigations need to be supported with digital collection and analysis tools and techniques. This need has led to the development of digital forensic science and specifically computer forensic (Rodgers and Seigfried, 2004). However, the increasing complexity of tools and techniques of digital investigation creates a new challenge for digital forensic investigators and corporate security investigators. A digital crime scene follows the same rules as for a physical crime scene, and it must be analysed and preserved in its original form. It is important to realise how imperative it is to use collection and analysis tools and follow a procedure when conducting digital evidence but the paramount need is to ensure that the integrity of the digital evidence is preserved.

According to Reith et al. (2002) digital forensics is a synonym for computer forensics as the use of scientific methods toward the preservation, 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.

For the purpose of this research, digital forensics can be defined as the use of scientifically derived and proven methods and techniques for the identification, preservation, reconstruction, and presentation of digital evidence derived from digital devices found to be an attack or incident. The definition is not just considering digital evidence recovered from the computer but it covers digital evidence recovered from any devices that are not traditionally considered a computer and any digital activity that is identified as an attack or incident.

This chapter aims to give an understanding of the need for digital forensics, research challenge, aims and objectives, hypothesis, questions, definitions and terminologies and the thesis structure.

1.2 Research Challenge

Palmer (2001) defined digital forensic investigation as the application of scientific, systematic and proven methods towards the preservation, collection, validation, identification, analysis, interpretation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or perceived to anticipate the unauthorised actions shown to be disruptive to planned operations. By this definition, it is important to demonstrate proofs of the integrity of digital crime object. Digital forensic investigators are constantly trying to find better and more efficient ways of uncovering evidence from digital sources. The challenge here is that beyond the presumptions of the occurrence of a crime, it is important to prove the integrity of the source of digital evidence. Law enforcement and corporate professionals require tools for effective digital evidence acquisition and analysis. According to (Rogers and Seigfried, 2004) cyber crime challenges are technical challenges that hinder law enforcement's ability to find and prosecute criminals operating online, legal challenges resulting from laws and legal tools needed to investigate cyber crime being unable to catch up with developing technological, structural, social changes and the resource challenge. Some of these tools already exist to capture, preserve and analyse data from hard drives, memory and network streams. They are available through commercial or open-source licences with their own unique user interface, features, and run on different operating systems. However, this presents a challenge to digital investigators because tools, systems and networks are vulnerable to threats or attacks.

According to Ashcroft (2001) the US National Institute of Justice (NIJ) conducted a study designed to identify the issues that the law enforcement community was experiencing in relation to computer crime and argued that most state and local law enforcement agencies report that they lack adequate training, equipment and staff to meet their present and future needs to fight digital or electronic crime and also mentioned that greater awareness of electronic crime should be promoted for all stakeholders, including prosecutors, judges, academia, industry and the general public. The study also identified the need for reliable digital evidence.

The present research addresses this issue through a proposed Comprehensive Digital Forensic Investigation Model (CDFIM), created by enhancing the current digital forensic investigation process. CDFIM identifies the need for the use of modern technologies to avoid security threats, when considering digital forensic investigation process in an attempt to present solution that contributes to a good security level and as a measure for integrity of digital evidence.

1.3 Motivation

Digital forensic techniques are used primarily by digital investigators, IT security officers and corporate security investigators etc to capture, preserve and analyse evidence on digital devices. Digital evidence collected at a crime scene has to be analysed, and the integrity of the digital evidence preserved. The search for digital evidence is thus a tedious task that consumes time. An extremely large amount of evidence needs to be processed in a very limited period, which leads to delay in processing schedules. Since it is the responsibility of the digital investigator to find what evidence exists and recover it in a sound manner, it is important for digital forensic investigators to be skilled and knowledgeable at pursuing cyber crimes to find related digital evidence on the private network, public internet, etc. A good

understanding of the technology entailed and security measures will allow digital investigators to recognise, collect, preserve, examine and analyse evidence related to crimes involving digital devices.

The task of the digital forensic investigator has grown harder due to the increase in the sizes of storage devices. Since the space is growing faster than corporate security investigator's ability to search, there is an opportunity for intelligent software to step in and assist law digital investigators. This thesis argues that security mechanism and guidelines can contribute positively to digital forensic investigation process and as a measure for integrity of digital evidence. Any admissible digital evidence should be able to proof that the integrity of the digital evidence is preserved. The presentation of digital evidence in the court of law is beyond the scope of this research.

1.4 Research Hypothesis

This research proposes that the integration of security mechanism and intelligent software when conducting digital forensic investigation can serve as a measurement tool for the integrity of digital evidence.

The research assumes that the necessary legal authorisation to search for and seize the suspected workstation is been obtained.

1.5 Aims and Objectives

The aim of this research is to explore the use of modern technologies to avoid security threats when considering digital forensic investigation process in an attempt to present solution that contributes to a good security level and as a measure for integrity of digital evidence. It will also create CDFIM in order to assist in conducting the digital investigation.

In order to obtain the research objectives of this thesis, it was necessary to consider the main aim of the thesis and the research hypothesis. These led to some specific research objectives that need to be addressed as follows:

- **Develop a Background Understanding of the Core Subject**

  To gain an extensive understanding of the fundamental digital forensic investigation framework/models, which are currently implemented. In order to investigate the various types of digital forensic investigation model, this analysis will help determine the shortcomings of existing models of digital investigation, as well as the requirements of CDFIM

- **Examine the Current Issues Around the Core Subject**

  To critically review the literature in order to identify the main problems in ensuring the integrity of digital evidence in digital forensic investigation.

- **Establish the Security Requirement for Digital forensic Investigation Process**

  The extensive literature review will assist in identifying the requirement for CDFIM

- **Develop Model for Evaluating the Security Level of Digital Forensic Investigation Process**

  To create a Comprehensive Digital Forensic Investigation Model based on the requirement.

- **Test the Model in Digital Investigation Context**

  To evaluate the model conducting experiment and a test case investigation

1.6 Research Question

A fundamental research question was posing to aid the development and refinement of research objectives.

The fundamental research question is:

- **What might constitute the requirement for utilizing security mechanism for digital forensic investigation process?**

1.7 Contribution to Knowledge

In the course of the research presented in this thesis, different contributions to knowledge have been made. The research has produced the following results:

Identifying issues that can influence the integrity of digital evidence when conducting digital investigation: The research identified that none of the current method of digital investigation initiated major concentration to attacks that can influence the integrity of digital evidence. Current models are concentrated on identifying collection and analysis method of digital evidence. As the reliability of digital evidence is important in any investigation, this research has been able to identify issues that can influence the integrity of digital evidence when conducting digital investigation. Therefore, CDFIM is advancement on existing models in its comprehensive nature to address the security threats faced in digital forensic investigation process. The model is easy to understand and used by even non-expert individuals with management responsibility for digital devices.

Creation of CDFIM as a Solution for the Problem of Altering the Integrity of Digital Evidence: This model is effective when investigating digital attack and ensuring the integrity of digital evidence. This is because most current digital investigation models are designed to deal with attacks such as those on systems and

networks. These models focus on translating the requirements of legal systems into those of IT systems in order to conduct proper digital forensic investigation. This is good; however, they do not address the issues faced in ensuring digital evidence integrity. It is in this cases that CDFIM helps in assisting digital investigation by employing its security mechanism and guidelines.

Implementation of IP as an Identifier and a Performance Measure to Solve Handover Latency and Loss of Data Packets: In the area of mobile network, the research proposed and implemented PMIPv6 with improved buffering to minimize performance issue on handover latency and loss of data which the research identified as able to assist in providing reliable services and in turn assist in digital investigation. This research conducted a network experimental test, which is based on comparing its proposed PMIPv6 with improved buffering to both standard PMIPv6 and buffering. It was set up, by analysing performance measures, which are handover latency and loss of data packet, which was identified in this research as an attack on the integrity of digital evidence. IP role as an identifier was also recognized in the research to identify the attacker of digital crime.

Improvement of the Investigative Process by Designing the Interaction Phase in CDFIM: This phase is a major advancement in the development of digital forensic models. In CDFIM interaction phase had been designed to deal with applying secure protocol (communication/internet) when conducting digital investigation to ensure the integrity of digital evidence collected.

1.8 Measure of Success

The success of the thesis is measured in two ways:

- **Evaluation:** Two different digital attacks were identified, and experiments were conducted to test the hypothesis.

- **Comparative Analysis:** CDFIM approach was compared with other approaches of digital forensic investigation.

1.9 Thesis Structure

Chapter 1: Introduction

In chapter 1, an introduction to the background of the core issue of the research is discussed. The aims and objectives, hypothesis, and approach of the thesis are presented. The fundamental research question mentioned in this chapter aims to develop and drive the research forward. The chapter identifies the research challenge and a possible solution that improves the research problem.

Chapter 2: Literature Review

In this chapter, the first part provide a holistic view of the background of digital forensic investigation process, digital evidence, characteristics of digital evidence, it's role, challenges and the procedures for digital evidence processing are addressed. The chapter also discusses the fundamental digital forensic investigation process and the need for framework/models. This section also covers the analysis conducted for existing investigation framework/model and the handling of different cases through these models. In this section, gaps in the existing models are identified giving a foundation of the need for a new model and then presents the conceptualised model. The second part of this chapter examines areas of application of digital forensic investigation process, security threats and vulnerabilities. This section explains adverse events and security incidents, and discussion on some different cases of digital forensic investigation such as computer forensic, network forensic and email forensics. The chapter also discussed digital forensics and investigative tools and techniques. Also, the security requirement for the new model was an output of this chapter.

Chapter 3: Research Methodology

This chapter discusses the implemented research process. The objectives of the research will be the backbone of the research methodology and the research process that was implemented to achieve them.

Chapter 4: The Comprehensive Digital Forensic Investigation Model

The chapter initially discussed the proposed model in a broad approach. In this chapter, the systematic design of the model was described presenting the Comprehensive Digital Forensic Investigation Model (CDFIM) that improves on previous digital forensic investigation process is created. In addition, the chapter examines the area of application of digital forensic investigation and impact of security threats and vulnerabilities.

Chapter 5: Experiments

This chapter conduct the experiments. The objective is to test the hypothesis and evaluate the requirements for the new model. It conducted a network experimental test, which compares its proposed PMIPv6 with improved buffering to both standard PMIPv6 and buffering. The experiment sets up by analysing performance measures, which are handover latency and loss of data packet, identified in this research as attacks on the integrity of digital evidence. In addition, this section conducts a test case investigation. The objective of this is to present the applicability of CDFIM.

Chapter 6: Validation

Two real cases used this model to identify whether incident/attacks was carried out and envisaged attacks during digital investigation, which can pose as a threat to the integrity

of digital evidence thereby applying precaution (security guidelines/measures) to avoid such threat.

Chapter 7: Discussion and Evaluation

This chapter discusses and evaluates CDFIM based on the experimental test results.

Chapter 8: Recommendations

This chapter suggest some recommendations that would assist in enhancing and improving digital investigation and the security level of digital information.

Chapter 9: Conclusion

This chapter of the thesis discusses the general conclusion. It presents this research findings and makes suggestions for future research.

1.10 Summary

This chapter discusses the aims, objectives, hypothesis, and approach of the research in the thesis. The fundamental research question mentioned in this chapter aims to develop and drive the research forward. The chapter identifies the research challenge and a possible solution that improves the research problem. This chapter also outlines the area of contributions of the research and the thesis structure. The research contributes to: (1) the theoretical knowledge of security threats faced in digital forensic investigation, (2) the new model can be turned into a measurement tool for the integrity of digital data.

Chapter Two: Literature review

Objectives:

- to define digital evidence
- to introduce the shortcomings of current digital investigation models
- to discuss digital attacks, security threats and vulnerabilities
- to identify digital forensic analysis and imaging tools and the application of intelligent software agent to digital investigation
- to identify the requirements of the new model

This chapter aims to give a detailed review of the existing literature concerning existing digital investigation models and framework and how they handled different cases through these models and the influence of digital attacks and threats is discussed. The gap in the existing models is being identified giving a foundation of the need for a new model, and then the conceptualised model is presented. This chapter provides a detailed overview on the evolution of digital forensics, literature review on the classification of an investigation process. The chapter discussed digital evidence characteristics and its challenges. The main aim of this chapter is to present the research that has been conducted until now and to introduce the shortcomings of current models of digital investigation and to identify the requirements for the new model.

2.1 Evolution of Digital Forensic

Computer crime is a huge criminal activity that continues to grow in its prevalence and frequency. This increase in criminal activity poses a strain on business organisation, law enforcement and government. Hence the need of shift from document based evidence to digital/electronic evidence has necessitated a rapid reformulation of standards and procedures (Casey, 2002). Digital forensic can be referred back to as early as 1984, when the FBI began developing programs to examine computer evidence (Noblett et al., 2000). The standard procedures from physical forensics are adopted into digital forensics, specific forensic software is created, and comprehensive knowledge is obtained by digital forensic specialists to defeat digital criminality (Furuseth, 2005). The procedures adopted in performing the digital forensic investigation have direct influence on the outcome of the investigation. Selecting inappropriate investigative processes may lead to incomplete, missing and inadmissible digital evidence. Skipping a step or procedure may lead to inconclusive results, and evidence captured in an unstructured manner may face the risk of not being admissible in the court of law or during internal hearing. The area of computer forensic is in its journey to become a recognised scientific discipline (Reith et al., 2002). To date, computer forensic has been primarily driven by vendors and applied technologies with very little consideration being given to establish a sound theoretical foundation (Farrell, 2009). Although this may have been sufficient in the past, it will not remain so for the near future. The judiciary system has already begun to question the scientific validity of many of the ad hoc procedures and methodologies and is demanding proof of some sort of a theoretical foundation and scientific rigor (Yasinsac et al., 1997).

Pollitt (2007) explains that one of the foundational ways in which researchers try to understand the scientific basis of the discipline is to construct models that reflect their observation. Even though digital forensic investigation paradigm is laborious and

requires significant expertise on the part of the investigator, computational intelligence is expected to offer more assistance in some aspect of the investigation procedures, and better knowledge reuse and sharing in computer forensics argued (Ruibin et al., 2005). Over the past years, there were numbers of investigation models proposed by different authors. The research observed that some of the models tend to be applicable to very specific scenario while others applied to a wider scope. Some of the models tend to be quite detail and others too general. This may lead to difficulty for forensic investigators to adopt the correct or appropriate investigation model. In this aspect of the thesis, the various available models are analysed, and common phases are extracted and grouped to propose a new comprehensive purpose model that would be applicable to any scenario.

In 1984 computer forensic investigative process was proposed for dealing with digital evidence investigation so that the results will be scientifically reliable and legally acceptable, it comprises four phases called Acquisition, Identification, Evaluation and Admission (Pollitt, 2007). In 2001, the first DFRWS investigative model proposed a general-purpose digital forensics investigation process that comprises of six phases (Palmer, 2001). Inspired by DFRWS investigative model, Reith et al. (2002) proposed an enhanced model, known as Abstract digital forensic model. In this model, the number of phases was expanded to nine, the three phases added to the model where Preparation, Approach Strategy and Returning Evidence. While majority of the authors and researchers have commented on the weaknesses, and strength in digital forensic, very few actual studies have been conducted. The National Institute of Justice in 1999 conducted a study designed to identify the issues that the law enforcement community was experiencing in relation to digital crime. The study identified ten issues such as investigative and forensic tools, public awareness, training and certification, data reporting, management assistance for onsite electronic crime task, updated laws, cooperation with the high-tech industry, research and publications, management

awareness and support and structuring a computer crime unit (Ashcroft, 2001). Carrier and Spafford (2003) proposed an investigation process known as integrated digital investigation process with the intention to combine various available investigative processes into one integrated model. The author introduced the concept of digital crime scene, which refers to the virtual environment created by software, and hardware where digital evidence of a crime or incident exists. In 2003, there was also End-to-End digital investigation model that consist of six phases. The model took into account the source of the incident (Stephenson, 2003). Baryamueeba and Tushaba (2004) introduced the Enhanced digital investigation process (EDIP). This model was based on the integrated digital investigation process in 2003. The EDIP introduces two significant phase known as Traceback Phase and the Dynamite Phase. Ciardhuain (2004) proposed a model for cybercrime investigation that combines the existing models, generalising them and extending them by addressing certain activities not included in them. Unlike previous models, this model explicitly represents the information flows in an investigation and captures the full scope of the investigation rather than only the processing of evidence. Beebe and Clark (2004) proposed a model known as a Hierarchical Objective-Based Framework for Digital Investigation and introduced the concept of objective-based tasks in which the investigative goals are used to select the analysis task. In a similar, study Ruibin et al. (2005) identified the need for computer intelligence technology in computer forensic framework. Rodger et al. (2006) proposed Computer Forensic Field Triage Process Model (CFFTPM) as an onsite approach to provide the identification analysis and interpretation of digital evidence in a relatively short period without the need to take back the devices or media back to the lab. Pilli et al. (2010) proposed a generic framework for network forensic analysis by specifically identifying the steps connected only to network forensic. Agawal et al. (2011) proposed the Systematic

Digital Forensic Investigation Model (SRDFIM) that focused on investigation cases of computer fraud and cybercrimes.

The increased development in the application of information technology in businesses, and the government has increased the value of information and influence on digital evidence. Information security science has evolved to be the main factor and supporting component of the use of information technology and which can be used to fight against cybercrime.

2.2 Digital Evidence

Cole et al. (2007, p. 444) defined evidence as information presented in court that attempts to prove a crime was committed. Carrier and Spafford (2006) define digital evidence as digital data that support or refute a hypothesis about digital events or the state of digital data. This definition includes evidence that is not only capable of entering into a court of law, but may have investigative value. Evidence can be gathered from theft or destruction of intellectual property, fraud or anything else related to the use of a digital device. Evidence, which is also referred to as digital evidence is any data that can provide a significant link between the cause of the crime and the victim (Perumal, 2009). Therefore, this current research defines digital evidence as a data packet or digital information stored or transmitted by a digital device that support or rebut an assumption about digital incident or event that provides relationship between the cause of an incident and the victim.

2.2.1 Characteristics of Digital Evidence

Digital evidence is by nature fragile. It can be altered, damaged or destroyed by improper handling or improper examination. It is easily copied and modified, and not easily kept in its original state. Precautions should be taken to document, collect, preserve and examine digital evidence (Carrier, 2003). Buttressing this point is research

carried out by Sommer (2009) which argued that data from computers can be accurately preserved and presented and, like all other evidences, digital evidence must be admissible, authentic, accurate, complete and convincing. Digital evidence is different from all other evidences in that it can change from moment to moment within a computer and along the transmission line, digital evidence can easily be altered without a trace and can be changed during evidence collection (Ademu and Imafidon, 2012g). The main problem is to determine how an expert can measure the reliability of digital evidence.

Digital evidence is data of investigative value that are stored on or transmitted by a digital device. Therefore, digital evidence is "hidden" evidence in the same way that deoxyribonucleic acid (DNA) or fingerprint evidence is hidden. In its natural state, digital evidence cannot be known by the content in the physical object that holds such evidence. Investigative reports may be required to explain the examination process and any limitations (Pollitt, 2007).

Figure 2: Different types of digital devices (Ademu et al., 2011b)

The digital devices such as those shown in figure 2 may contain potential evidence that relates to criminal activity. The majority of digital devices contain data that could be lost if not handled properly. Examples of other digital devices are audio recorders, answering machines, cables, GPS devices, telephones, pagers, chips, digital organisers, copy machines, scanners, dongles, wireless access points and fax machines. Potential evidence can also be found on multiple computers connected to each other or to the central server in a computer network.

2.2.2 Role of Digital Evidence

The major goal in an investigation is to relate the crime to its executor by uncovering compelling links between the offender, victim and crime scene. If the evidence suggests that the suspect committed a crime or violated an organization's policy the investigator begins a case, which is a collection of evidence that can be presented in the court or to interested parties, and for an internal hearing in an organisation (Ademu and Imafidon, 2012e). A witness may identify a suspect, but evidence of a person's involvement is usually more compelling and reliable. Previous scholars argue that anyone or anything penetrating a crime scene takes something of the scene with them and leaves something or a trace behind. In the physical world, a criminal might unconsciously leave fingerprints or hair at the scene and take a fibre from the scene. Similar to categories of evidence in the traditional forensic sense, digital equipments and their attributes can be grouped into class and individual groups. Printers, fax machines, scanners and all-in-one office devices may leave discernible artefacts that lead to common class characteristics allowing the identification of a particular device, e.g. Canon, Epson, etc. Even though individual characteristics could be sometimes rare, it should be possible to identify through detailed analysis (Ademu and Imafidon, 2012b). The investigator must evaluate the evidence thoroughly and document the chain of evidence, or chain of

custody, which is the route the evidence took from the time evidence was found until the case is presented.

2.2.3 Challenges in Digital Evidence

A huge number of organisations are faced with the need to collect evidence on their networks in response to incidents such as computer intrusions, intellectual property theft, fraud, child pornography, stalking, etc. The majority of organisations are taking into account legal solutions when criminals target them, emphasizes should also be given for more attention to handling digital evidence in a way that will be admissible. A lot of digital investigators deal with a huge number of crimes regularly, and there are fewer resources and less time to open a full investigation for each incident.

Digital evidence unlike physical evidence can be difficult to understand and handle. For instance, a hard drive contains a messy combination of data layered and mixed together over time. In most cases, only a small portion of this information can be relevant, making it necessary to extract useful pieces, fit them together and translate them into a form and language that can be interpreted.

Digital evidence is commonly an abstraction of some event or digital object (Casey, 2004). For instance in a situation where an email message is being sent by an individual, the resulting activities create data traces that give mainly an incomplete view of what occurred. Digital evidence can be influenced easily. Digital evidence can be altered either maliciously by criminals or accidentally during collection without leaving any noticeable signs of alteration (Ademu et al., 2011b). Digital evidence has different features that lessen this problem. For instance, digital evidence can be replicated exactly and a copy can be examined as if it were the original. With the right tools, it is very easy to know if digital evidence has been modified by comparing it with an original copy. Digital evidence can also be difficult to destroy; even when a file is deleted, or a hard

drive is formatted, the digital evidence can be recovered applying the correct tools. When criminals attempt to destroy digital evidence, copies and remain can still exist in places that they have no knowledge (Sommer, 2009). With digital evidence, it is difficult to attribute a digital activity to an individual. For instance if a case centres on a single form or source of digital evidence such as date-time stamps on computer files, such a case is very weak. Without additional information, it could be argued that someone else used the computer at the time.

The dynamic and distributed nature of the network makes it even more difficult to find and collect all relevant digital evidence. It is not realistic to take a snapshot of the entire network at a particular time. Also, network traffic is temporary and must be captured while it is in transit. Once network traffic is captured, only copies remain, and the original data are not available for comparison. The amount of data lost during the collection process can be documented, but the lost evidence cannot be recovered.

A network contains a large amount of data and sifting through for useful information can be more or less impossible and can prevent an investigation. Even when the important digital evidence is obtained, networks provide a degree of anonymity making it difficult to attribute online activities to an individual. The ultimate aim of the research in this thesis is to explore the use of modern technologies to avoid security threats when considering digital forensic investigation process in an attempt to present solution that contributes to a good security level and as a measure for integrity of digital evidence. This thesis provides methods of addressing these obstacles.

2.2.4 Digital Related Offenses

2.2.4.1 Cybercrime

According to Casey (2004) computer related offenses required special consideration, twenty six member countries signed the Council of Europe (COE) Convention on

Cybercrime to create a common criminal policy aimed at the protection of society against cybercrime, by implementing suitable legislation and fostering international co-operation. Even though the COE Convention on Cybercrime represents an aspirational policy document, a country that approves the Convention commits to putting in place a legislative framework that deals with cybercrime according to Convention requirements. Within this commitment, each country is given discretion in relation to the full scope. Despite the clear need for consistent legislation in Europe to facilitate cross-border investigations, there are major differences between the legal systems and cultures in European countries, making legislative consistency difficult. The COE Convention on Cybercrime has already been faulted by some for not taking due account of privacy rights. There are also differences between the Convention and existing laws in some European countries that will take time to resolve. To understand these differences, it is useful to compare categories of offences set out by the convention with related offences in English law.

2.2.4.2 Computer Exploitation

The United Kingdom was the first European country to enact a law to address computer crime specifically in 1990. The Computer Misuse Act introduced three new offences, which are unauthorised access to a computer , unauthorised access with intent to facilitate the commission of further offenses and unauthorised modification of computer material (Mobbs, 2003). The Council of Europe Convention introduces five offences against the confidentiality, integrity and availability of computer data and systems which are illegal access, illegal interception, data interference, system interference and misuse of devices.

2.2.4.3 Child Pornography

Offences relating to the possession and distribution of child pornography are most likely the major ones litigated and certainly the most notorious of cyber offences. The

associated law in England pre-dates the Convention and did not specifically mention computers. The Protection of Children Act Section 1 (1) , 1978 as amended by the Criminal Justice and Public Order Act, 1994 makes it an offence for a person to take or permit to be taken an indecent photograph of a child, to distribute or show such indecent photographs and to have in his possession such indecent photographs with a view to be distributed or shown to others. With the support of the amendment made by the 1994 Act, the term "photograph" includes data stored on a computer disk or by other electronic means that are capable of conversion into a photograph, including graphic images (Ademu and Imafidon, 2012c).

2.2.4.4 Forgery and Fraud

Forgery and fraud are traditional offences that may be assisted by the use of technology. The COE Convention describes computer related forgery offences as the intentional input, alteration or deletion of digital data resulting in inauthentic data with the intent that it is considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data are directly readable and intelligible. The COE Convention also describes computer related fraud as the intentional causing of a loss of property to another by any input, alteration or deletion of computer data or any interference with the functioning of a computer system with fraudulent intent of procuring, without the right to do so for the economic benefit for oneself or another (Mobbs, 2003).

2.2.5 Digital Evidence and its Application

When a digital device is seized, digital investigator's need to protect the system, its components and digital information. Digital investigators are careful to ensure that, no possible evidence is damaged, destroyed, or otherwise compromised by the procedures used to investigate the digital device extracted and possibly relevant evidence is properly handled and protected from later mechanical or electromagnetic damage and a

continuing chain of custody is established and maintained and if at all any information is inadvertently acquired during a forensic exploration it should be ethically and legally respected and not divulged (Ademu and Imafidon, 2012a).

One of the most important issues of digital evidence is the handling of data. The major aim of digital forensic investigation is to gather digital evidence in a manner that will preserve the integrity of digital evidence. In order for this to happen, there should be procedures that can minimise the chance of contamination of evidence. In handling digital evidence, the crime scene should be secure, preventing unauthorised access into the digital device or anyone from touching the computer and other related digital object. It is important to document information gathered at all times during the investigation; this will be useful when reconstructing the scene. On identifying the digital evidence, it is important to preserve such evidence. There is need for scientific validity of many procedures and methodologies used in digital investigation process (Carrier and Spafford, 2006). It is important to proof the theoretical foundation and scientific rigor of an investigation process.

A major error preventing digital evidence from being accepted is obtaining it and ignoring the preservative measures. In the case of exigency, a search can be made for any emergency without warrant needed. Digital examiners can also perform a search without a warrant by obtaining consent for the search in the case of purpose of internal hearing. Also in a situation where digital forensic examiners are authorised to search a computer, they must maintain a good level of security for the digital object, (Ademu and Imafidon, 2012f).

2.2.5.1 Types of Evidence

According to Casey (2004) when there is attack on a network or computer on the network, evidence can take several forms. For instances hardware devices such as hard

drives, keyboards, router, desktops, and servers are good sources of evidence gathering. These systems with their continuous increase in its amount of storage space can be rich sources of digital evidence. A simple file can contain incriminating information and can have related properties such as when and where the file was created, and by whom. The traditional telephones, mobiles, personal digital assistant, smart cards, log files, files on hard disk, database files, captures of a computer's state can also be a source of digital evidence.

Depending on the type of attack, in the case of a live system, the digital investigator might need to document the current state of the system. Some information known as volatile data, which identifies the activities on a computer, is lost when the digital investigator shut down or unplugs the system, but there is relevant information that needs to be gathered from a live system (Cole et al., 2007). The digital investigator can gather information from viewing information about listening ports and network connections. Information about listening ports and established network connections can be viewed by using special forensic tools available for gathering data. Evidence can also be gathered viewing information about the applications running on the computer.

2.2.5.2 Application of Digital Evidence

The following are example of the application and use of digital evidence.

• Criminal prosecutors use digital evidence in a variety of crimes where incriminating documents can be found such as homicides, financial fraud, drug and embezzlement recordkeeping, and child pornography (Sommer, 2009).

• Civil litigators can readily make use of personal and business records found on digital devices that bear on things such as fraud, divorce, discrimination, and harassment cases.

• Insurance companies may be able to mitigate costs by using discovered digital evidence of possible fraud in accident, arson, and workman's compensation cases.

• Corporations often hire computer forensics specialists to ascertain evidence relating to sexual harassment, embezzlement, theft or misappropriation of trade secrets and other internal/confidential information (Ademu at al., 2011b).

• Law enforcement officials frequently require assistance in pre-search warrant preparations and post-seizure handling of computer equipments (Sommer, 2009).

• Individuals sometimes hire computer forensics specialists in support of possible claims of wrongful termination, sexual harassment, or age discrimination (Ademu and Imafidon, 2012a).

2.2.6 Digital Evidence Processing Guidlines

When experts are ready to retrieve data they take careful steps to identify and attempt to retrieve data that exists on a computer. If the digital evidence is collected aimlessly then not only will there be an inefficient use of resources but the evidence could get compromised, thus liberating a criminal from all possible wrong doing. Before this evidence is submitted it must meet three basic requirements to maintain its reliability, It must be produced, maintained, used in a normal environment and be professionally authenticated and also meet the best evidence rule. This means that what is produced must be the best evidence available and not a substitute for the evidence offered (Icove et al., 1995).

There are also procedures that must be followed at the crime scene. Just like any other regular crime scene, in the case of computer forensic, a computer has to be kept in the same condition as it was found. Doing this prevents any evidence from being questioned. There are three methods recommended for handling evidence. Acquire the

evidence without altering or damaging the original, authenticate the recovered evidence as being the same as the originally seized data and analyse the data without modifying it (Yang, 2007).

There are some effective procedures on an investigation utilising digital forensics. First, digital forensic investigators must preserve the evidence. This step is followed after entering the scene of the crime. Digital evidence is fragile and can be changed at any time by just touching a key on the keyboard. Evidence that is damaged or handled improperly will be excluded from evidence and could result in criminals being vindicated (Kruse and Heiser, 2001). After this, evidence must be examined which means data are ready to be retrieved. Once all files are collected the unallocated disk space (free space) is checked and also compare and remove duplicate files (Casey, 2004). The empty space on the hard drive can contain previously deleted or formatted files. A bit-stream-copy method is used to find deleted files. Deleted files tend to be in strings, and the tool will help to rebuild documents. When someone deletes or formats, not all information is wiped; a special format is required for this to happen. When all files are retrieved, they need to be protected. Next, evidence is to be analysed. The analysis consists of the list of the digital device, any relevant data, and authorship information, and any indication to try and hide any revealing data. After this analysis, the data are taken to the appropriate place and prepared for presentation. Whenever needed, the forensics expert can provide consultation and/or testimony. Here they will be able to prove their theory of guilt or innocence based on their analysis of the evidence. If these procedures are followed correctly, criminals will be prosecuted thoroughly. These procedures should be followed by everyone involved in the collection of digital evidence. A digital crime scene follows the same rules as traditional crime scene, and it must be analysed and preserved in its original form. It is important to realise how imperative it is to follow the procedure.

According to Solomon and Lattimore (2006) one major problem of digital forensics today is the lack of a standard and consistent investigative process. Current procedures and tools should not be mistaken for a consistent investigative process; tools and procedures are built from the experience of law enforcement simply in an ad hoc fashion instead of coming from the scientific community where other traditional forensic sciences gets their methodologies. “This is a problem because evidence must be obtained using methods that are proven to reliably extract and analyse data without bias or modification”. (Reith et al., 2002).

According to Jennings and Barnard (2005) despite advances in automated technologies, human involvement is crucial. In agreement with the authors, the involvement of an investigator is important in digital investigation although it is possible for an investigator to make errors while performing specific actions or omitting facts while searching for digital evidence. To prevent such failures digital forensic tools and techniques in collaboration with good security guidelines are considered to achieve the goals of digital evidence searching, retrieval and recovery. The digital forensic investigator analyses a case and selects techniques to be used in the process of investigation. Carrying out a digital forensic investigation using a method manually could consume a huge amount of time, for example, searching all the clusters in a hard disk could take several years of work. Some specific tasks cannot be performed without the use of specific software tools. A large variety of software and hardware has been developed to help digital forensic investigators in performing digital forensic investigation.

In dealing with digital forensic investigation, digital related crime evidence is gathered, analysed, and presented to a court of law to prove that an illegal activity has occurred. It is important that when undertaking digital forensics investigation no alteration, damage or data corruption occur. In order to do a good analysis, the first step is to secure the

collection of evidence Ademu et al., 2011). This is important to guarantee the evidential integrity and security of information. Choosing and using the right tools and techniques are very important in digital forensic investigation. The digital forensic techniques mentioned in this thesis are as follows:

- **Imaging**

One of the first techniques used in a digital forensics investigation is to image, or copy the data to be examined. Without care, data can be modified, even though as little as the modification can be, the integrity of the evidence can be compromised. A digital forensic investigator is required to have good knowledge of different operating system behaviour so that residual data will not accidentally be overwritten. Both hardware and software solutions have been created to allow imaging that does not modify the drive. For most operating systems, there are procedures to follow to protect the media to be imaged. This involves disabling auto-mounting services and accessing the raw devices directly. There are also hardware solutions, in the form of write blockers that physically prevent the OS from modifying the media. According to (Bolt, 2011) write blockers are most common for hard drives, and provide several variations on implementation technique. Once the digital forensic investigator is certain that the original disk will not be modified, the data must be copied from the original disk for analysis, and this has important details that must be considered. A physical media device is normally made of blocks where data is stored. These blocks can be grouped into multiple partitions per device, with spaces between the partitions. Partitions are then formatted into file systems, with certain blocks containing metadata and control data for the file systems. To ensure all information is accurately copied from a system, the system must be imaged at the block level. To support law enforcement and industry alike, the National Institute of Standards and Technology (NIST), has created the Computer Forensic Tool

Testing (CFTT) Program. CFTT has set standards, created testing utilities, reviewed and certified disk imagers, file recovery software, hardware and software write blockers.

- **Hashing**

In order to demonstrate that an image or file was not modified, the forensic community has adopted cryptographic hashing. Modern hashing functions use one-way cryptographic functions to obtain the hash. The uniqueness of the hash depends on the cryptographic function used. According to Casey (2004) before copying data from a disk, it is advisable to calculate the MD5 values of the original disk. The hash value of the original disk can be compared with copies to demonstrate that they are identical. In 2004, MD5 was shown to be insecure by researchers. This research makes relying on MD5 hashes alone questionable in legal contexts. NIST collects software to hash for its National Software Reference Library project. NIST hashes the files collected with both MD5 and SHA-1 and plans additional functions in the future.

- **Carving**

Data carving is a technique used in digital forensics. Data files have certain identifiers in their coding structure such as text files and video files, etc. By carving through the lost pieces of data on a flash drive, common signatures can be found in order to reassemble the files. One category of tools in the digital forensic toolkit is called file carvers. These tools allow the scanning of disk blocks that do not belong to current files to find deleted data. An approach to recovering deleted files is to search unallocated space, swap files and other digital object for class characteristics such as headers and footers. This process is like carving files out of the combination of data in unallocated space (Casey, 2002). Recent advances in carving allow fragmented files to be recovered with more accuracy. Cohen (2008) described advanced JPEG carving as creating a jpeg

validation based on the open source lib jpeg and a distance function to find sudden image changes, indicative of an invalid reconstruction.

2.2.7 Backbone of Digital Forensic Investigation

The investigative process is structured to encourage a complete, accurate investigation, ensure proper evidence handling and reduce the chance of mistakes created by preconceived theories and other potential pitfalls. This process applies to criminal investigations as well as public and private inquiries dealing with policy violations or system intrusion. Digital investigators and examiners work hand-in-hand in a systematic and determined manner in an effort to present an accurate and reliable evidence to the court or the interested parties (Ademu and Imafidon, 2013). While in the court, evidence is handed over to the prosecutors who scrutinise the findings and decide whether to continue or discontinue the case. The stages in each process are often linked and there is need for digital investigators and examiners also to revisit steps after it is thought to be complete. The fundamental investigation processes are as follows:

2.2.7.1 Preparation

Every process of investigation has a starting point. In a digital forensic investigation, this step can be signalled by a system administrator reviewing firewall logs, questionable log entries on a server or some combination of indicators from multiple security sensors installed on networks and host (Sommer, 2009). In the case of an automated incident alert, it is necessary to consider the source and reliability of the information. An individual making a complaint due to repeated offensive messages appearing on his or her screen might be dealing with a computer worm or virus. Alert from an intrusion detection system may only indicate an attempted, unsuccessful intrusion or a false alarm. It is usually very important to weigh the strengths and weaknesses related to the sources and involve the human factor as well as the digital.

It is important to carry out a thorough preparation for assessing an event occurrence, there should be some preliminary fact gathering before carrying out a full or detailed investigation. To perform this fact gathering and preliminary assessment, it is usually important to enter a crime scene and carefully scan through a variety of data sources looking for items that may contain relevant information. There is need for careful handling at this stage in an investigation because every action in the crime scene may alter evidence. Carrying out an investigation without proper authorization can undermine the entire investigative process. Therefore it is necessary to perform only the minimum actions necessary to determine if further investigation is needed.

Documentation infuses all steps of the investigation process and is very important to all the steps of the investigation process. It is essential to record the details of each piece of digital evidence to help establish its authenticity and initiate a chain of custody. Investigators are usually busy with numerous cases or they have competing duties that require their attention. Putting in mind that investigative resources are limited, they must be applied where they are needed most. In civil, business and military operations, for instance, suspicious activity will be investigated but policy and continuity of operations often replace legalities as the primary concern, resources should be focused on the most severe problems or where they are most effective. Offenders and victims may deceive investigators intentionally claiming that something occurred or that they were somewhere at a particular time. By cross referencing such information with the digital traces left behind by an individual's activities, digital evidence may support or refute a statement (Casey, 2009). In one homicide investigation, the prime suspect claimed that he was out of town at the time of the crime but his computer experienced a bug that made most of the time-stamp dates on his computer useless; email messages sent and received by the suspect showed that he was at home when the murder occurred, opposing his original statement. Therefore because he was caught in a lie, the suspect

admitted to the crime. Proper action must be taken to ensure the integrity of potential evidence both physical and digital. The methods and tools employed to ensure the integrity are very important at this stage. Their accuracy and reliability and also professional acceptance may be subject to questioning if the case is prosecuted. This stage is generally the first stage in the process that employees commonly used tools of a particular type. This stage involves the duplicating of copies of all sources of digital data.

2.2.7.2 Collection

Once the crime scene is secured, possible evidence of the incident must be identified and seized. Clear procedures and understanding of necessary legal criteria are essential before the activity can begin properly. To avoid wasting time, the main goal here is for experienced digital investigators not to seize everything at a crime scene but to make informed decisions about what to seize, to document them and to be able to justify the action. Digital investigators are often asked to provide some insight into the origins of a particular item of digital evidence. In addition to determining the origin of an email message, different file formats have characteristics that may be associated with their source (Casey, 2004).

Comparing an item of evidence to an example can disclose investigative useful class characteristics or even individual characteristics. These embedded characteristics can be used to associate a piece of evidence with a specific computer. The earlier versions of Microsoft Office is also embedded with a unique identifier in files, called a Globally Unique Identifier (GUID), which can be used to identify the computer that was used to create a given document (Casey, 2009).

In the digital environment, like in traditional forensics, the seizure of material items occurs but all or part of the state and character of some material evidence may be lost

almost immediately upon seizure by virtue of the volatility of electronic devices and their designs. Recently most digital devices have a large amount of storage space where process context information, network state information, etc. are stored. Immediately a system is shut down the immediate contents of that memory is lost and can never be completely recovered, however, when dealing with digital evidence crime it may be necessary to perform operations on a system that contains evidence, especially in network connected environments.

2.2.7.3 Analysis

This step involves the detailed scrutiny of data identified by the preceding activities. The methods applied here will tend to involve review and study of specific internal attributes of the data such as text and narrative meaning of readable data Before performing a full analysis of preserved sources of digital evidence, it is possible to extract data that have been deleted, hidden and not available for viewing using the appropriate tools. Missing items are also important but their presence must be inferred from other events. For instance, if there is evidence that a certain program was used but the program cannot be found, it can be gathered that the program was removed after use. This can have important implications in the context of crime, since concealment behaviour is a major attribute of a criminal intent. The functionality of a piece of digital evidence can give a clue of what happened. Knowing what a program does is important for reconstruction.

2.2.7.4 Reporting

In order to provide a clear view of the investigative process, final reports should contain important details of each step, including reference to protocols followed and methods used to seize, document, collect, preserve, recover, reconstruct, organise and search key evidence. The major part of the report involves the analysis leading to each conclusion

and descriptions of supporting evidence. It is important that no conclusion should be written without a thorough description of the supporting evidence.

2.2.8 Why the Need for Investigative Framework/Model

Digital evidence is admissible as long as the process used to produce the evidence is known to produce reliable results. According to Kruse and Heiser (2001), the basic forensic methodology known as "the three 'A's" is evidence that must be acquired without altering or damaging the original. The investigator must authenticate that recovered evidence is the same as the originally seized data and data must be analysed without modification. Digital evidence must not be modified or damaged during any part of the investigation process (Ademu et al., 2012a). Hash sums should be calculated on collected digital evidence data and on the source of the evidence and compared to ensure the authenticity and integrity of the data.

An investigative framework should provide a process for conducting a digital forensic investigation. There are multiple factors complicating the investigative process. The more clearly the investigative process is defined, the more likely an investigation will be successful. An investigative framework, properly thought out and constructed would give a step-by-step process for conducting an investigation into a suspected digital device (Ademu and Imafidon, 2013). A clear and structured process will allow investigators and examiners determine early in the investigation that an attack has occurred and it can lead them to a conclusion (Casey, 2002). It is important to know that this does not imply that all such conclusions are successful. A worryingly large percentage of investigations end with the conclusion that the victim was attacked, but that the source of the attack cannot be determined.

Casey (2004) discussed that the US Supreme Court provides certain criteria in the Daubert vs. Merrel case that may be used as guidelines by courts to determine whether

evidence is admissible in court. Conventional applications therefore have to adhere to the requirements stipulated by the Daubert standard to allow the evidence they collect to be admissible in court. Few investigators have the time and skill to evaluate and analyse their chosen tools to determine whether they obey the rules of the criteria stated by the Daubert standard. Even though the tools obey the rules of the criteria and perform well in a trusted environment, they may give inconsistent results in an untrustworthy environment (Casey, 2004). This is because software applications rarely contain all the operating logic needed to perform basic functionality that can be supplied by external drivers or the operating system; the application relies rather on libraries and drivers and may be compromised to produce results that are inconsistent with the digital evidence.

Most commercial forensic tools seem to be very expensive to buy. This creates a problem because not every investigation team has the finance to invest in the very expensive toolkit and may have to use the available open source tools (Ademu and Imafidon., 2012b). It could be better to use the existing functionality supplied by commercial forensic tools, since their functionality has been tested and proven, but it is virtually impossible because the source code of these tools is not available to the public. A solution is needed to allow investigators to perform rapid digital forensic investigation on a consistent and structured framework in an attempt to speed up digital forensic investigation.

2.3 Existing Digital Forensic Investigation Framework/Models

With the increase in digital crime, lots of digital forensic investigation models already have been developed. One of the problems with digital forensics is that the procedures for accomplishing forensic investigation are not consistent. In the digital investigatory practices, there are hundreds of digital forensic investigation procedures developed, different countries and organizations tend to develop their own procedures, some

focused on the technology aspect, some on data analysis of the investigation. In conducting a digital investigation for impending criminal breach of the law the legal process depends on the local cyber law.

2.3.1 Computer Forensics Investigation Process

Pollitt (2007) proposed an approach where digital evidence can be investigated in a manner that the result will be scientifically reliable and legally acceptable. The author compared and mapped the computer forensic process to the admission of documentary evidence in a court of law. Four different steps are identified as a guide to the admission of any evidence into court. The steps are shown in figure 3.

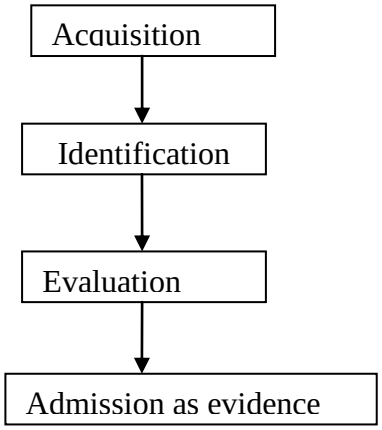


Figure 3: The digital investigative process (Pollitt, 1995)

2.3.2 DFRWS Investigative Model

Palmer (2001) discussed that the first Digital Forensic Research Workshop proposed a general-purpose digital forensic investigation. The goal of the workshop was to provide a forum for a newly formed community of academics and practitioners to share their knowledge on digital forensic science. The audience comprised military, civilian, and law enforcement professionals who use forensic techniques to uncover evidence from digital sources.

The group created a consensus document that drew out the state of digital forensics at that time. Among the group's conclusions was that digital forensics was a process with some agreed steps. The framework introduces digital investigation phases. The phases defined by the framework serve to categorise the activities of an investigation into groups which a list of techniques where provided. They outlined phases such as identification, preservation, collection, examination, analysis, presentation and decision. (Palmer, 2001). As shown in figure 4 below, the framework is represented as a table, the grey boxes at the top of their matrix, which is the column, is identify by the group as fundamental phases, and each row contains techniques although many will debate the forensic nature of each step of the process. This can be called an enhanced model of the DOJ model because it was able to cover stages that were not covered in any previous model, such as the presentation stage. The main advantage of DFRWS is that it is the first large-scale organisation that is led by academia rather than law enforcement; this is a good direction because it helps define and focus the direction of the scientific community towards the challenge of digital forensics, but the DFRWS model is just a basis for future work.

Identification	Preservation	Collection	Examination	Analysis	Presentation	Decision
Event/Crime Detection	Case Management	Preservation	Preservation	Preservation	Documentation	
Resolve Signture	Imaging Technologies	Approved Methods	Traceability	Traceability	Expert Testimony	
Profile Detection	Chain of Custody	Approved Software	Validation Techniques	Statistical	Clarification	
Anomalous Detection	Time Synch.	Approved Hardware	Filtering Techniques	Protocols	Mission Impact Statement	
Complaints		Legal Authority	Pattern Matching	Data Mining	Recommended Countermeasure	
System Monitoring		Lossless Compression	Hidden Data Discovery	Timeline	Statistical Interpretation	
Audit Analysis		Sampling	Hidden Data Extraction	Link		
Etc.		Data Reduction		Spacial		
		Recovery Techniques				

Figure 4: Digital Forensic Research Workshop (Palmer, 2001)

2.3.3 The Scientific Crime Scene Investigation Process Model

According to Ashcroft (2001) the US National Institute of Justice (NIJ) published a process model. The Technical Working Group for Scientific Crime Scene Investigation is completely design as a procedure for improving the collection process. The document serves as a guide for the first responders. The guide is intended for use by law enforcement and other responders who have the responsibility for protecting an electronic crime scene. The procedures involve recognition, collection, preservation, transportation and storage of digital evidence. The model consists of four phases, and started with the Collection phase, which involves the search for, recognition of, collection of, and documentation of electronic evidence. This follows by the Examination phase, which helps to make the evidence visible and explain its origin and significance. It includes revealing hidden and obscured information and the relevant documentation. This is followed by the Analysis, which involves studying the product of the examination for its importance and probative value of the case. Then finally, reporting which involves writing a report, outlining the examination process and information obtained from the whole investigation.

2.3.4 Abstract Digital Forensic Model

Reith et al. (2002) proposed a model known as the Abstract Digital Forensic model. The basis of this model is using the ideas from traditional (physical) forensic evidence collection strategy as practiced by law enforcement (e.g. FBI). The authors argued that the proposed model could be termed as an enhancement of the DFRWS model since it is inspired from it. The model adds supports for tool preparation and the dynamic formulation of investigative approaches. The model involves nine components:

- Identification – This recognises an incident from indicators and determines its type. This component is important because it has impact on other steps but it is not explicit within the field of forensics.
- Preparation – This involves the preparation of tools, techniques, search warrants and monitoring authorisation and management support.
- Approach strategy – This is formulating procedures and approach to use in order to maximise the collection of untainted evidence while minimising the impact to the victim.
- Preservation – This involves the isolation, securing and preservation of the state of physical and digital evidence.
- Collection – This is to record the physical scene and duplicate digital evidence using standardised and accepted procedures.
- Examination – This is an in-depth systematic search of evidence relating to the suspected crime. This focuses on identifying and locating potential evidence.
- Analysis – This determines importance and probative value to the case of the examined product.
- Presentation - This is where summary and explanation of conclusion.
- Returning Evidence – Physical and digital property returned to proper owner.

The three important phases introduced in this model were Preparation, Approach Strategy and Returning of Evidence. In Preparation, phase activities such as preparing tools, identifying techniques and getting management support were carried out. Approach Strategy was introduced with the objective to maximise the acquisition of unaltered evidence. In ensuring that evidence is safely returned to the rightful owner or property disposed, the Returning Evidence phase was introduced.

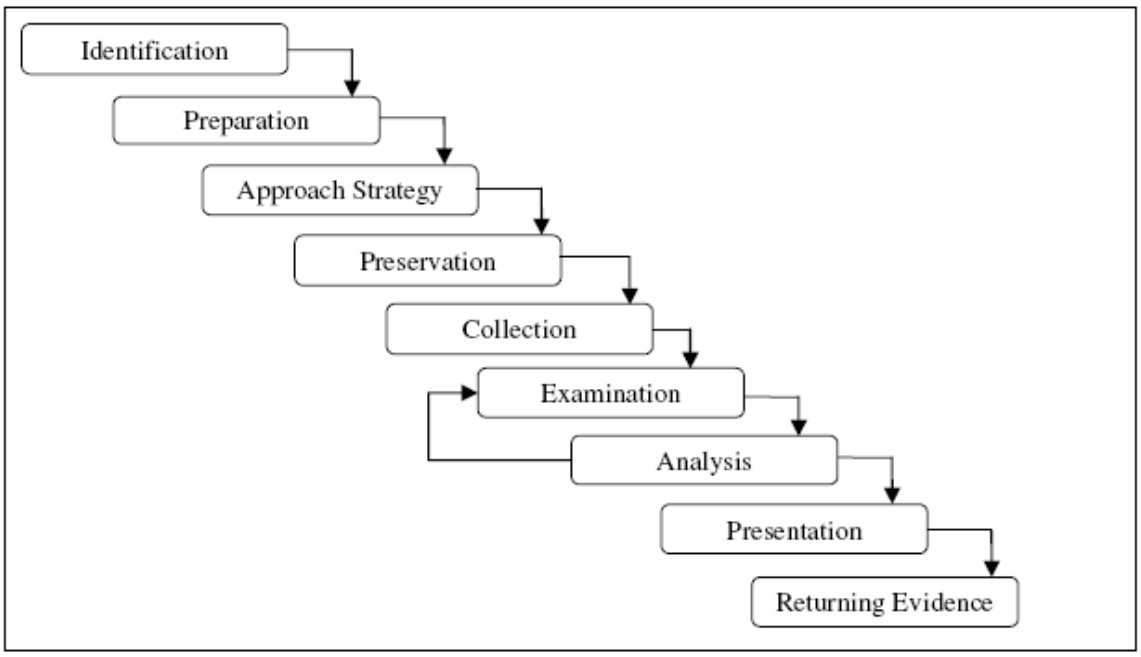


Figure 5: Abstract Digital Forensic Model (Reith et al., 2002)

Using this model shown in figure 5, future technologies and the technical details required to analyse them forensically can be instantiated to provide a standard methodology for providing electronic evidence (Reith et al., 2002). This will improve the science of forensics because it involves a basis for analysing new digital technology while at the same time providing a common framework for law enforcement and the judicial system to work feasibly within a court of law.

2.3.5 Integrated Digital Investigation Process Model (IDIP)

Carrier and Spafford (2003) proposed a model, which is based on previous work with the purpose of combining the different available investigative processes into one integrated model. They introduce the idea of digital crime scene which refers to the virtual environment developed by software and hardware where digital evidence of a crime or incident exits. The model known as the Integrated Digital Investigation Process was organised into 5 phases as shown in figure 6.

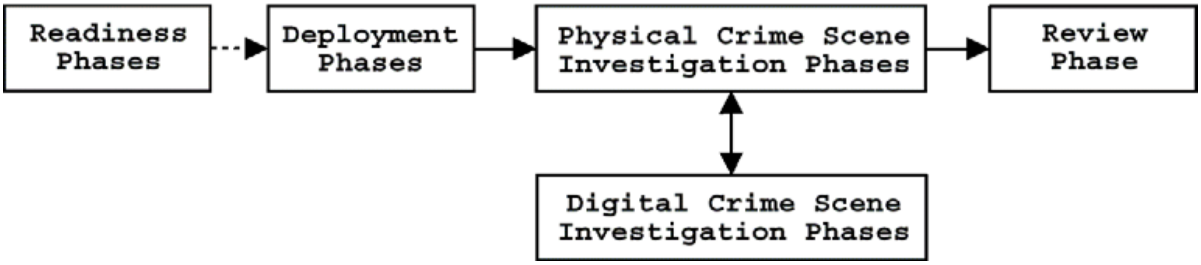


Figure 6: Integrated Digital Investigation Model (Carrier and Spafford, 2003)

The process started with a readiness phase that require the physical and operational infrastructure to be ready to support any future investigation. The phase is an ongoing phase in the entire life cycle of an organisation. After the Readiness phase is Deployment phase, which provides a mechanism for an incident to be detected and confirmed. The other phases introduced are Physical Crime Scene Investigation Phase, Digital Crime Scene Investigation Phase and finally Review Phase where the whole investigation processes are reviewed to identify areas of improvement that may result in new procedures or training requirement (Carrier and Spafford, 2003).

2.3.6 End-to-End Digital Investigation

End-to-end digital investigation consists of 6 phases as shown in figure 7. It combines an extended digital forensic investigation process. The model takes into account the source of the incident, where the incident happened (Stephenson, 2003).

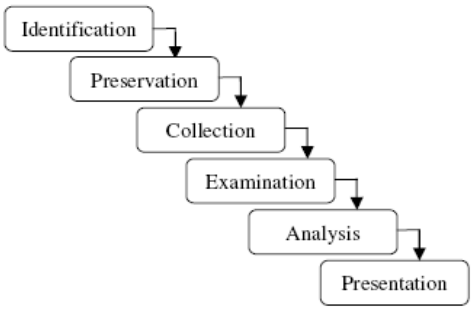


Figure 7: End to End-Digital Investigation (Stephenson, 2003)

2.3.7 Enhanced Digital Investigation Process

Baryamueeba and Tushaba (2004) investigative model is based on Integrated Digital Investigation Model. The Enhanced Digital Investigation Process mode as shown in figure 8, introduces two additional phases, traceback and dynamite, which seek to separate the investigation into primary crime scene (computer) and secondary crime scene (the physical crime scene). The goal is to reconstruct two crime scenes to avoid inconsistencies.

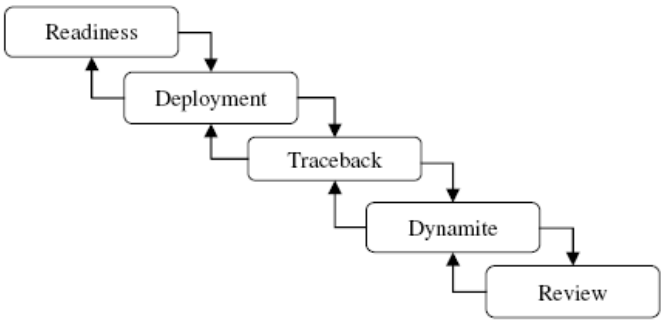


Figure 8: Enhanced Digital Investigation Process (Baryamueeba and Tushaba, 2004)

The Traceback Phase enables the investigator to trace back all the way to the actual device used by the criminal to perform the crime. In the Dynamite Phase, investigations are conducted at the primary crime scene with the purpose of identifying the potential attacker. In this model, the Deployment Phase provides a mechanism for an incident to be detected and confirmed. It consist of 5 sub-phases namely Detection and Notification, Physical Crime Scene Investigation, Digital Crime Scene Investigation and finally Submission (Baryamueeba and Tushaba, 2004). Unlike IDIP, this phase includes both physical and digital crime scene investigation and presentation of findings to legal entities through the submission phase.

2.3.8 Extended Model of Cybercrime Investigation

Ciardhuain (2004) argues that the existing models are general models of cybercrime investigation that concentrate only on the processing of evidence in cybercrime investigations. The author proposed an extended model for cybercrime.

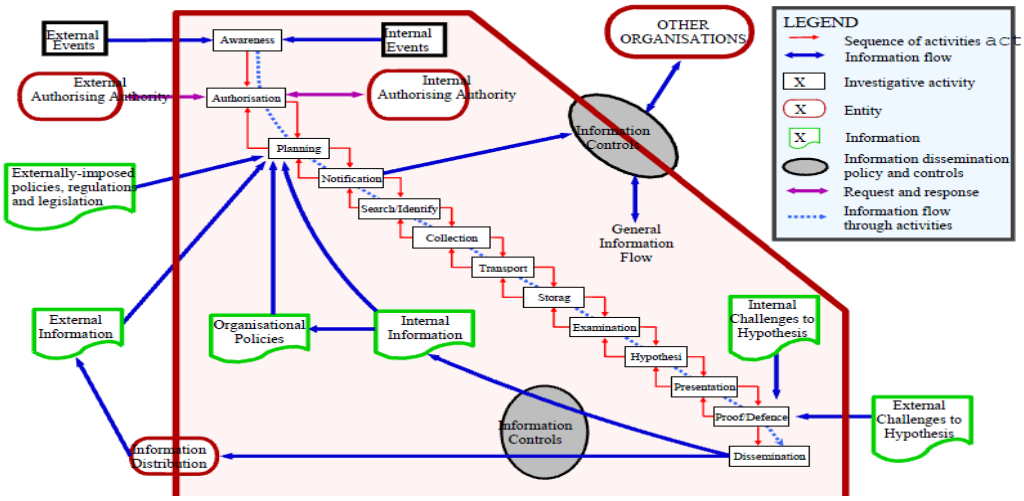


Figure 9: The extended model of cyber crime investigation (Ciardhuain, 2004)

The model shown in figure 9 above provides a good basis for understanding the process of cybercrime investigation, tackling certain activities such as presenting the information flow in an investigation for allowing deeper understanding of the source of evidentiary and other data. Even though the model is generic, it concentrates on the management aspect. The author argues that the available models are generic models of cybercrime investigation focusing on investigative processes such as gathering, analysing and presenting the evidence. This model is designed to assist public and corporate forensic investigations.

2.3.9 A Hierarchical Objective-Based Framework for Digital Investigation

Beebe and Clark (2004) provide an excellent review of the previous proposed digital forensic model and then propose that, why most of the previous models were single tier, the proposed one tends to be multi-tier as shown in figure 10. They introduced the

concept of objective-based tasks where the investigative goals for each sub-phases represent objectives rather than specific tasks. This is a significant and exceptional difference from the task-based models discussed so far. Objectives are goals that expect activities of a similar nature regardless of the specific case. Tasks directly relates to a specific case, type of case and platform.

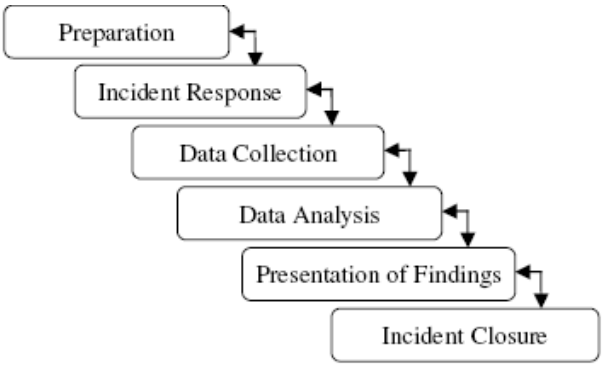


Figure 10: A Hierarchical Objective-Based Framework for the Digital Investigation (Beebe and Clarke, 2004)

2.3.10 Case-Relevance Information Investigation

Ruibin et al. (2005) identified the need for computer intelligence technology in the current computer forensic framework. It suggests an automatic and efficient framework to provide the case-relevance information by binding computer intelligence technology to the current computer forensic. The authors explained that computer intelligence expects to offer more assistance in the investigation procedures and better knowledge reuse within multiple cases and sharing in computer forensics. The first concept that the authors introduce is the notion of 'Seek Knowledge', and this is the investigative clues that drive the analysis of data. Another concept described by the authors is the notion of Case-Relevance. They used this notion to describe the distinctions between computer security and forensics, even defining degrees of case relevance.

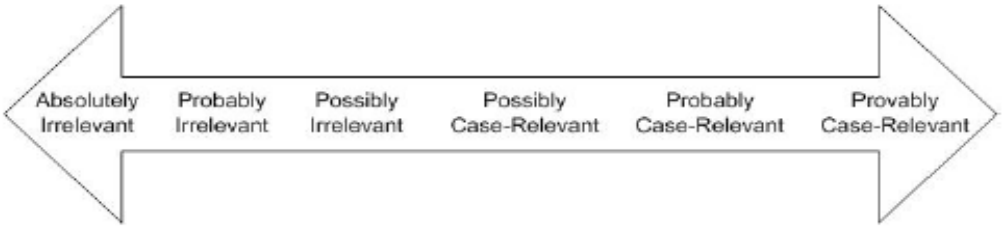


Figure 11: Case-Relevance Information Investigation (Ruibin et al., 2005)

The authors argued that the major problem faced for the deployment of computer intelligence in digital forensics is the lack of Standard Test Dataset and Evaluation Criteria. Some ideas have been given to the formalization of the test and evaluation activities of different product. It is very urgent to establish a formal and repeatable test dataset and evaluation environment for the data analysis phase. The authors emphasize that computer intelligence is extremely computational intensive and need large volume of data for training and testing.

2.3.11 Framework for a Digital Forensic Investigation

Kohn et al. (2006) clearly defined a framework that can be used in a forensic investigation and argue that the previous proposed framework revealed that a number of activities overlapped one another and that the differences were mainly terminological. The authors recommend a clear systematic approach for the collection of evidence suitable for a specific application framework for single computer. They stated that their required forensic investigation stages were preparation, investigation and presentation as shown in figure 12.

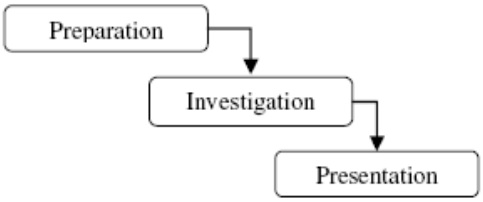


Figure 12: Framework for a Digital Forensic Investigation (Kohn et al., 2006)

2.3.12 Computer Forensic Field Triage Process Model

Rodger et al. (2006) proposed Computer Forensic Field Triage Process Model (CFFTPM) as an onsite approach providing identification, analysis, and interpretation of digital evidence in a relatively short period without the need to take the media back to the lab. The model consists of six phases that is further divided into six sub-phases as shown in figure 13.

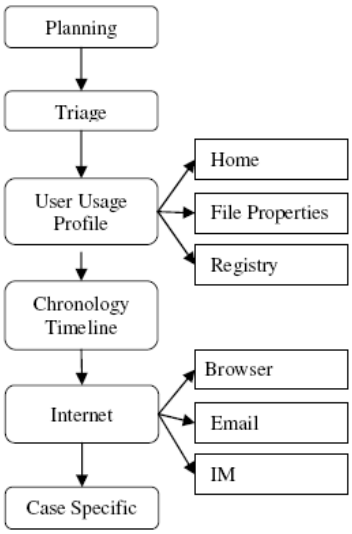


Figure 13: Computer Forensic Field Triage Process Model (Rodger et al., 2006)

CFFTPM started with planning phase where proper planning before conducting an investigation is done to ensure improving the success rate of the investigation. The next

phase is Triage phase, which is where the evidence are identified and ranked in terms of priority. Evidence with the most important and volatile need is processed first. Then the user usage profile phase which focus its attention to analyse user activity and profile with the objective of relating evidence to the suspect. Chronology Timeline phase aims at building the crime case from chronological perspective to sequence the probable crime activities. In the internet phase, the task of examining the artefacts of internet related services are performed. Finally, in Case Specific Evidence phase, the digital investigator can adjust the focus of the examination to the specifics of the case, for instance the focus in intellectual property would be different than that of the child pornography case.

2.3.13 Common Process Model for Incident and Computer Forensics

Freiling and Schwittany (2007) proposed a model for the purpose of introducing a new process framework to investigate computer security incidents, and its aim is to combine the two concepts of incident response and computer forensics to improve the overall process of investigation. The framework focuses generally on the analysis stage into Pre-Analysis, Analysis and Post-Analysis phases as shown in figure 14.

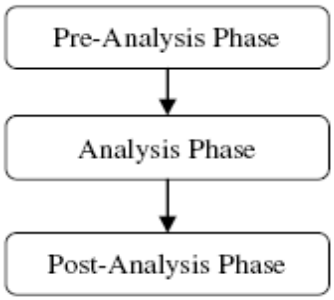


Figure 14: Common Process Model for Incident and Computer Forensic (Freiling and Schwittany, 2007)

2.3.14 Digital Forensic Model based on the Malaysian Investigation Process

Perumal (2009) proposed a model that clearly states that the investigation process will lead to better chances of successful prosecution, as the very most important stages such as live data acquisition and static data acquisition have been included in the model to focus on fragile evidence.

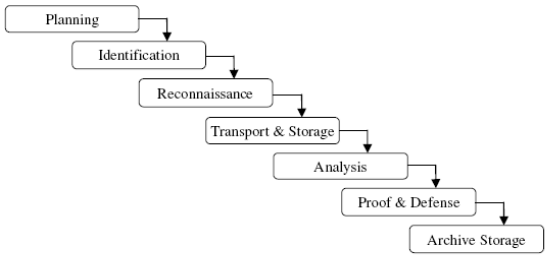


Figure 15: Digital Forensic Model based on the Malaysian Investigation Process (Perumal, 2009)

In this model as shown in figure 15, it started with the planning phase, and then followed by the identification phase. The third phase is the Reconnaissance phase, which deals with conducting the investigation while the devices are still running (live forensics). The author argued that the presence of live data acquisition that focuses on fragile evidence does increase the chances of positive prosecution. In order for the analysis of data, secure transportation of data to the investigation site and proper storage takes place in the Transport and Storage phase. As soon as the data is available, it is analyzed and examines using the relevant tools and techniques in the Analysis phase. In the Proof and Defence phase, the digital investigator is required to show the proof to support the case. Finally, in the Archive Storage phase, relevant evidence is properly stored.

2.3.15 Network Forensic Generic Process Model

Pilli et al. (2010) proposed a generic model for network forensic analysis based on various existing digital forensic models as shown in figure 16. This was specifically for the network-based investigation. It covers tools, process and framework implementation.

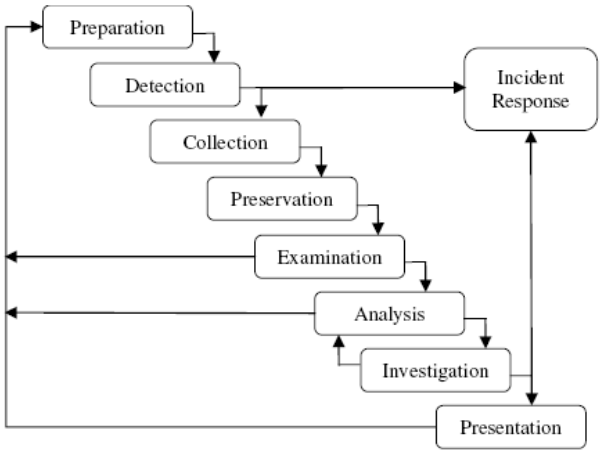


Figure 16: Network Forensic Generic Process Model (Pilli et al., 2010)

2.3.16 Systematic Digital Forensic Investigation Model (SRDFIM)

This model has been developed with the aim of helping forensic practitioners and organizations set up appropriate policies and procedures in a systematic manner. The proposed model as shown in figure 17 in this paper explores the different processes involved in the investigation of cybercrime and cyber fraud in the form of an 11-stage model (Agawal et al., 2011). The model focuses on investigation cases of computer frauds and cybercrimes. The application of the model is focused on computer frauds and cybercrimes, identifying various digital forensic processes but did not discuss on security measures on preserving the integrity of digital information.

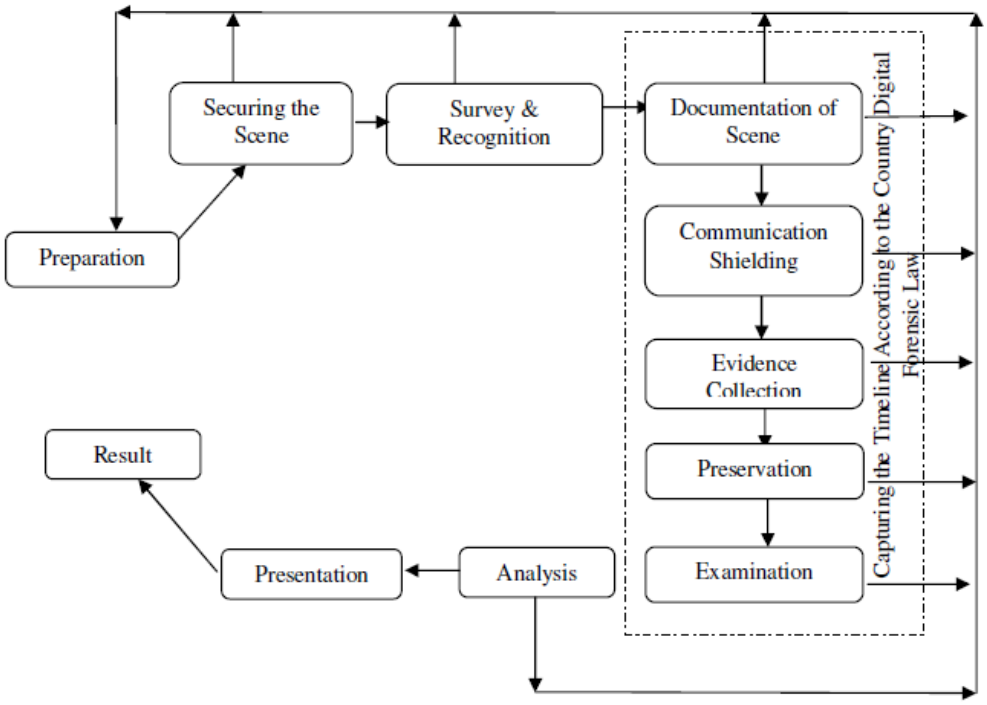


Figure 17: Systematic Digital Forensic Investigation Model (Agawal et al., 2011)

2.4. Investigative Models/Framework Analysis

The main objective of examining digital forensic investigation is to ensure that digital evidence is collected in a reliable way that can reconstruct an incident or event with an investigative value. Digital evidence is admissible in court or to interested parties as long as the processes used to produce the evidence are known to produce a reliable result. The literature reviewed in digital forensic investigation frameworks/models are analysed to discover the gap in the existing models by grouping the common phases of the existing investigation framework/model and then identifying the gap. The analysis is reported in tabular form. In order to identify the common phases with their activities shared by all of the existing models, codes were allocated to them. They were assigned with codes and sorted in chronological order. Using model as (M) and combining it with number (1) in accordance with the year proposed. For example the computer forensics process proposed by Pollitt (2007) is identified as M1. Table 1 below summarises the digital forensic frameworks/models explained in section 2.3

Table 1: The Existing Digital Investigation Frameworks/Models

Code	Name of Model	Originators	Years
M1	Computer forensic process	M. Pollitt	1995
M2	Generic Investigation process	DFRWS	2001
M3	Forensic Process Model	NIJ	2001
M4	Abstract model of the digital forensic process	Reith, Carr, &Gunsh	2002
M5	An integrated digital investigation	Carrier and Spafford	2003
M6	End-to-end digital investigation	Stephenson	2003
M7	Enhanced integrated digital investigation process	Baryamureeba & Tushabe	2004
M8	Extended model of cybercrime investigation	Ciardhuain	2004
M9	Hierarchical, objective based framework	Beebe and Clarke	2004
M10	Case-Relevance information investigation	Ruibin, Yun and Gaertner	2005

M11	Framework for a digital forensic investigation	Kohn, Eloff and Oliver	2006
M12	Computer forensic field triage process model	Rodger, Goldman, Mislan, Wedge and Debtota	2006
M13	Common process Model for Incident and Computer Forensic	Freiling and Schwittay	2007
M14	Digital Forensic Model Based on Malaysian Investigation Process	Perumal	2009
M15	Network Forensic Generic Process	Pilli, Joshi, Niyogi	2010
M16	The Systematic Digital Forensic Model	Agarwal, Gupta, M. Gupta, S and Gupta, C	2011

After identifying the investigation model, the phases with their activities are refined from the existing investigation model and assigned codes as shown in Table 2. This is done for the purpose of grouping similar tasks/activities together.

Table 2: The Identification of Phases

Code	Name of Phases
P1	Acquisition
P2	Admission
P3	Analysis
P4	Approach Strategy
P5	Archive Storage
P6	Authorization
P7	Awareness
P8	Case Specific Analysis
P9	Chronology Timeline Analysis
P10	Collection
P11	Communication Shielding
P12	Deployment
P13	Detection
P14	Digital Crime Investigation

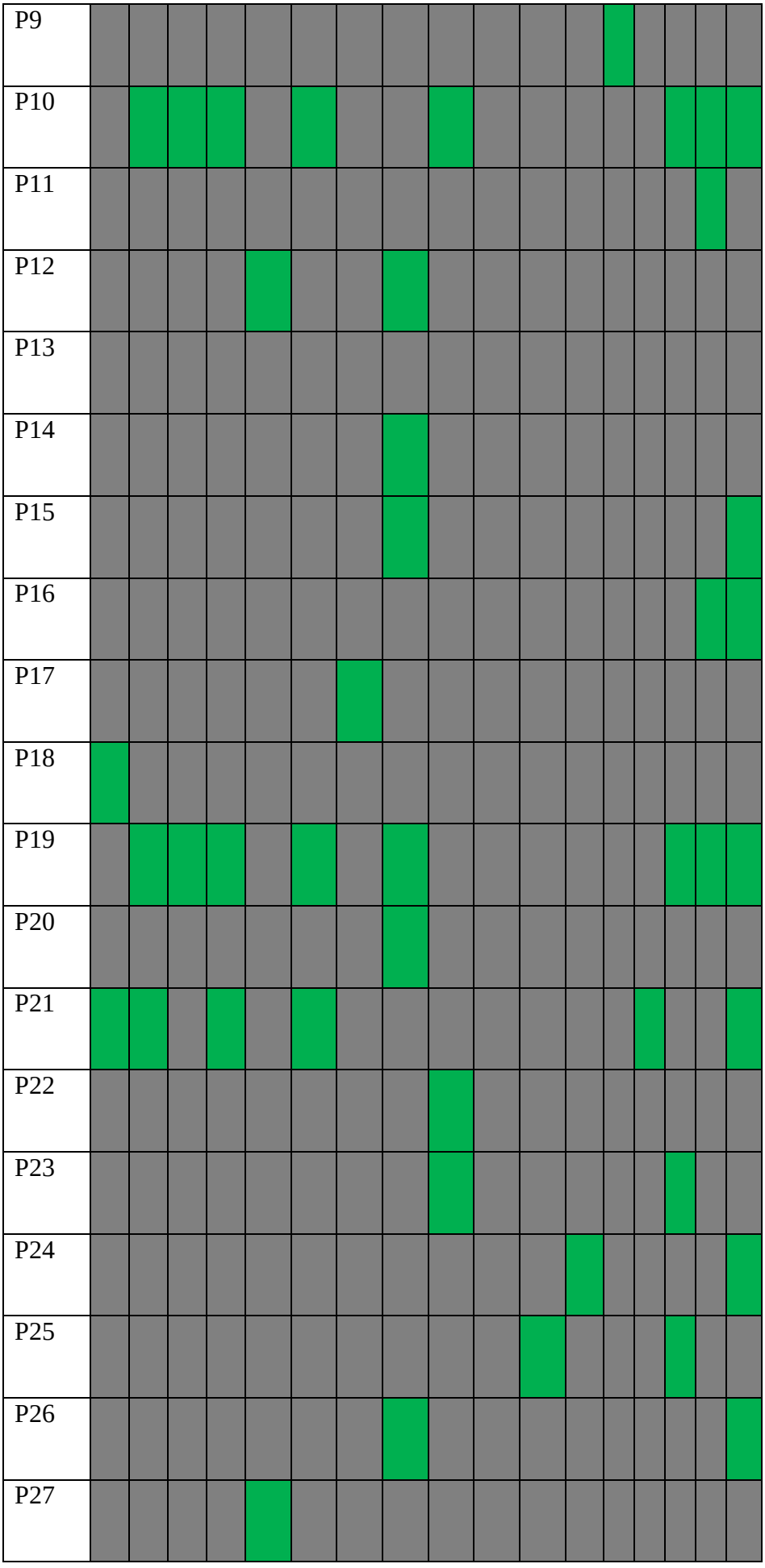
P15	Dissemination of Information
P16	Documentation
P17	Dynamite
P18	Evaluation
P19	Examination
P20	Hypothesis creation
P21	Identification
P22	Incident Closure
P23	Incident Response
P24	Internet
P25	Investigation
P26	Notification
P27	Physical Crime Investigation
P28	Planning
P29	Post-Analysis
P30	Pre-Analysis
P31	Preparation

P32	Presentation
P33	Preservation
P34	Proof & Defence
P35	Readiness
P36	Survey & Recognition
P37	Reconnaissance
P38	Report
P39	Result
P40	Returning Evidence
P41	Review
P42	Search & Identify
P43	Traceback
P44	Transport & Storage
P45	Triage
P46	User Usage Profile Investigation

The next step is refining all the phases with their activites within each investigation model. They are refined from the content of the papers. Each column represents a key paper explored. The cell in the table indicates if the paper addresses the activity in the role. Using the colour indicator shown in the table key, green shows that a particular phase in the cell was addressed in the particular model in the column and the grey shows that the particular phase in the cell was not addressed to the specific model. The objective of this, is to ensure accurate selection of the common phases with similar activities that are to be grouped together. The result is displayed in table 3 below:sss

Table 3: Models Discussed Showing Important Existing Phases

PHA-SES	***M MODEL***																
	M 1	***M 2***	***M 3***	***M 4***	***M 5***	***M 6***	***M 7***	***M 8***	***M 9***	***M 10***	***M 11***	***M 12***	***M 13***	***M 14***	***M 15***	***M 16***	***M 17***
P1																	
P2																	
P3																	
P4																	
P5																	
P6																	
P7																	
P8																	


P9
P10
P11
P12
P13
P14
P15
P16
P17
P18
P19
P20
P21
P22
P23
P24
P25
P26
P27

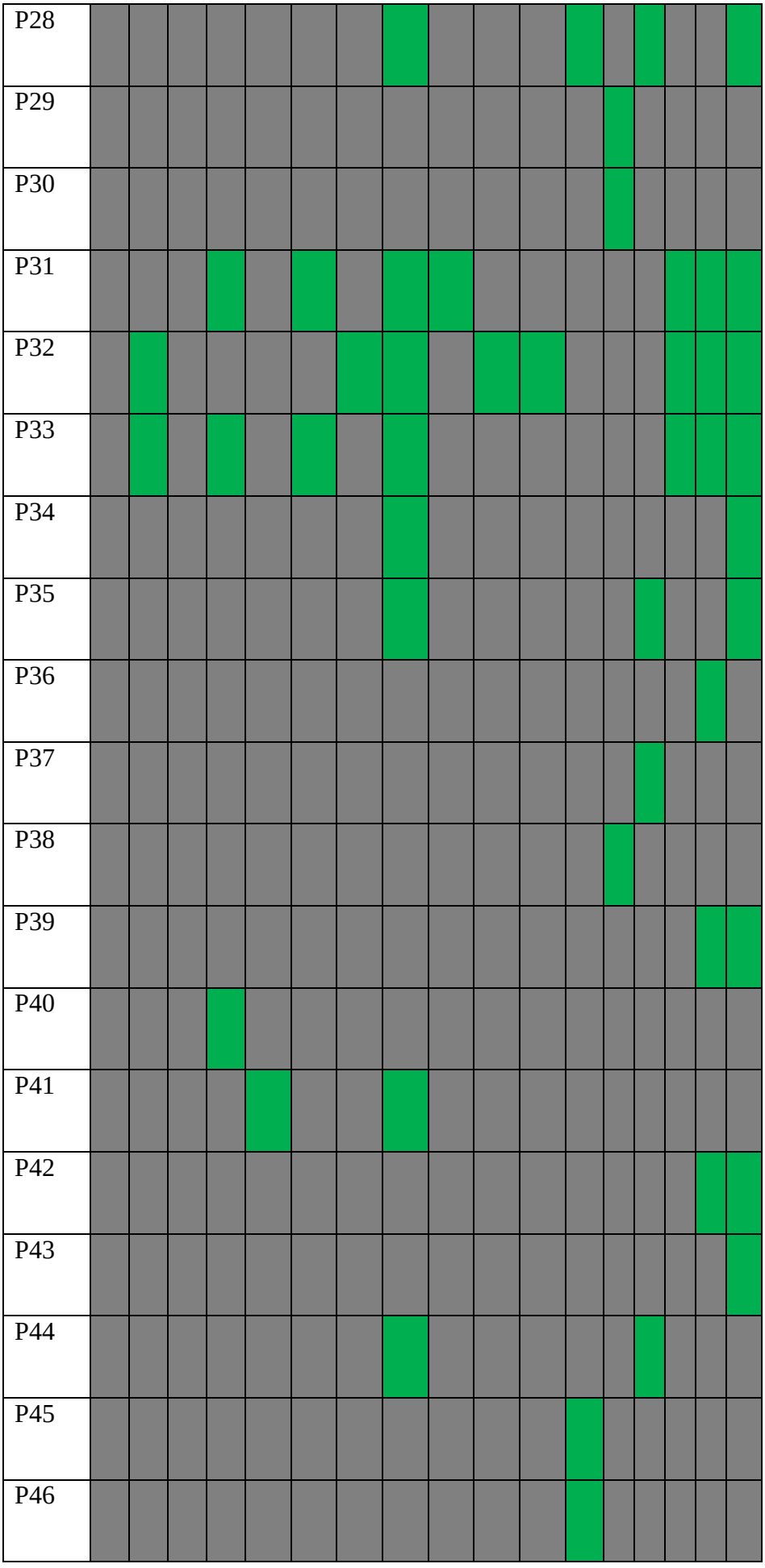
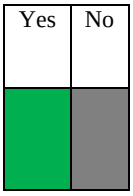

P28
P29
P30
P31
P32
P33
P34
P35
P36
P37
P38
P39
P40
P41
P42
P43
P44
P45
P46

Table Key:



Finally, phases with similar activities are grouped together using the different colour indicators in the table key. For the purpose of the research in this thesis, after exploring activities performed in each of the phases, observation was made, and it was identified that the phases could be grouped into four layers based on the methodology proposed by (Pollitt, 2007). The groupings identified in this research are namely, Preparation, Interaction, Reconstruction and Presentation (Ademu et al., 2011b) and as shown in table 4 below: With Interaction phase proposed as a new phase.

Table 4: The Four Layered Analysis

Layers	Available Phases
Preparation	P4, P6, P7, P11, P12, P13, P16, P23, P26, P28, P35, P36
Interaction	P8, P9, P10, P15, P16, P17, P19, P21, P24, P27, P30, P33, P42, P44, P46
Reconstruction	P1, P3, P5, P14, P16, P18, P20, P22, P25, P37, P39,P41, P43, P45

Presentation	P2, P29, P34. P38, P40

Based on the review of academic and industrial literature the following are the visual representation of essential phases required for an investigation process as observed in this chapter.

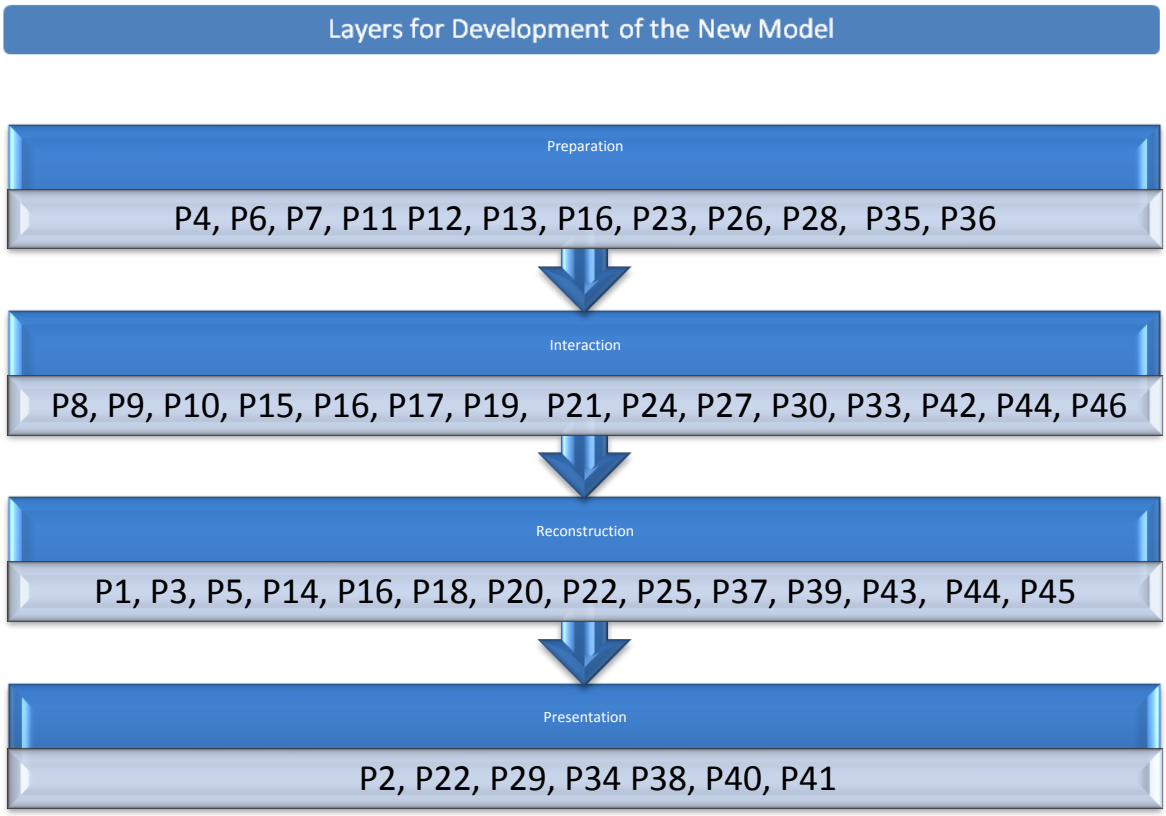


Figure 18: The layers towards building the new investigation process model (Ademu and Imafidon, 2012f)

2.4.1 Gap Analysis

Examining the result from the tables analysed, it was discovered that majority of the analysed models were addressing different phases of the investigation process either from one aspect or a few aspects. Given that a number of models already exist, what is the motivation for presenting yet another one?. The existing models do not cover a

major issue of cybercrime or the security threats that may affect digital investigation and influence the integrity of digital evidence. The existing models are concerned mainly on the processing (collection and analysis) of digital evidence. Although this is considered valuable, they are not enough to fully describe the investigative process in a way that assist the preservation of digital information. A comprehensive model can provide a common reference framework for conducting different digital investigation and for the development of future technology, it can support the development of tools, techniques, training and certification/accreditation of investigation and tools respectively, It can also provide a unified structure for case studies and lesson materials to be shared among student, digital investigators and for the development of standards, conformance testing and investigative best practice (Ciardhuain, 2004).

The largest gap in the existing models is that they do not identify digital attack or incident and security threat on the integrity of digital evidence. A few of the models were found focusing on the part of the process of investigation e.g. the collection and examination of the evidence. However, the earlier and later stages must also be considered and should be able to apply to any case if a comprehensive model is to be achieved, and in particular, as a relevant solution for digital based threats and attacks that are identified in digital investigation. The internal technical processes supporting the digital evidence processing is a dimension that need to be carefully examined (Selamat et al., 2008). There is need for integrating information security guidelines that support investigation processes.

Information technology has spread through businesses, the world and every operation in an organisation involves it to some extend. The importance of information security has increased in parallel with the uptake of technology, new system vulnerabilities such as poor security measures, inadequate virus protection and badly implemented software leaving organisations open to viruses, denial of service attacks, and industrial

espinoage. There are indeed different tools and techniques that assist digital forensic investigation process, but this tools may be opened to threats and vulnerabilities. There is concern in digital forensic investigation where digital evidence can be opened to threats and vulnerability that compromise the security objectives (Confidentiality, Availability and Integrity) of such evidence hence leading to damaged digital evidence (Ademu and Imafidon, 2012g). There is therefore need for security measures that can be integrated in investigation process. It is important to ensure the integrity of digital evidence is preserved. If the processes taken in gathering digital evidence followed a good security measures, it could be argued that the integrity of digital evidence is secured. With a good security mechanism, available, digital objects are secured. The workstations are secured including the digital information stored on it, hence any such digital evidence collected are secured.

In the research presented in this thesis, based on exploring the various investigation models, a model was conceptualised, which is known as the Comprehensive Digital Forensic Investigation Model (CDFIM) as illustrated in figure 18 below.

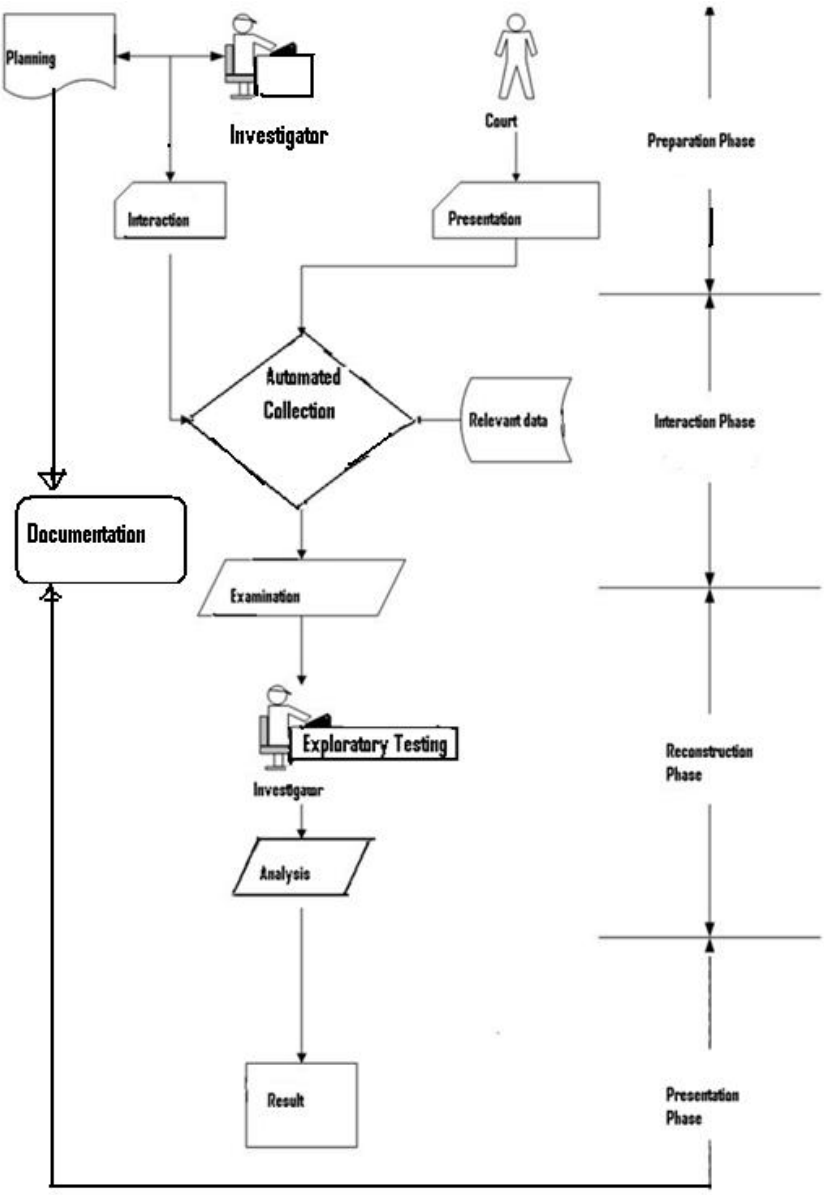


Figure 19: The Conceptualised Digital Forensic Model (Ademu et al., 2011b)

2.5 Digital Forensic Investigation and the Impact of Security Threats/Attacks and Vulnerabilities

Casey (2004) defined digital evidence as any data stored or transmitted using a digital device that support or refute the theory of how an offence occurred or which address critical element of the offence such as intent and reason. Nelson et al. (2004) explains that digital forensics involves scientific examination and analysis of data from digital

device storage media so the data can be used as evidence in court. Investigating digital devices typically includes securely collecting digital data, examining the suspect data to determine details such as origin and content, presenting reliable digitally based information. In this thesis, for the purpose of the research, digital forensics investigation is define as the process of identifying, maintaining, analyzing and presenting digital evidence through the use of information technology to the investigation of digital attacks or incidents and preserving such evidence through the application of information security. Digital forensics investigates stored or transmitted data from systems and networks. Digital evidence is characterised by its fragile nature, and it can be easily altered or destroyed, thus rendering it inadmissible in a court of law or to interested parties. Digital investigators should, therefore, take care to ensure that evidence is not destroyed. One of the major time consuming tasks in digital investigation is the search for digital evidence. Different toolkits have been developed that contain tools to support digital investigators in the process as much as possible in an attempt to increase the efficiency of a digital investigation.

The rapidly evolving age of information technology is changing our lives without our awareness. With the development of information communication technology and cybercrime, there is increase need for digital forensic investigation. The use of internet and software technologies has resulted in a few legal problems, and most existing investigation model/frameworks are inadequate to deal with them. A huge amount of activities are done through digital forms, and the major way a digital forensic investigator can prove that something happened or did not happen is through digital evidence. In as much as digital evidence can easily be compromised by poor handling, the value for digital evidence should not be undermined.

Chaikin (2007) raised the issue of reliability as a limitation of digital evidence. The author explained that cyber attackers are rarely held accountable for their illegal actions,

and one explanation for the lack of successful prosecution of cyber attackers is damage on digital evidence. Digital evidence is different from evidence created, stored, transferred and reproduced from a non-digital format. Digital evidence is temporary (short-lived) in nature and can easily be altered, and this characteristic of digital evidence raises issues as to its reliability. Since courts have become more familiar with the vulnerabilities of digital evidence, they scrutinise the reliability of digital evidence with specific emphasis on its content and processes of gathering the digital evidence. The defence counsels increasingly challenge both the admissibility and the weight of digital evidence. There is a need for improved competencies in handling digital evidence.

As the role of information technology expands, so has the importance of information security. The increase in the use of information technology has led to the appearance of new areas of vulnerability. Although more time and effort is being put into developing security products, the potential consequences of security failure are also growing. If an organisations computer network crashes, for instance certain parts of the organisation can effectively be paralyzed. Considering the alleged case of US v. Gary McKinnon in 2002; Gary McKinnon was alleged by American prosecutors of illegally accessing top-secret computer systems in what they claimed to be the biggest military computer hack of all times, McKinnon gained an unauthorised access into the US government network computer account causing damage that cost the USA some million dollars to repair. Having gained access to some of the government computers, he alledgely deleted data from them including critical operating system files, the deletion of which shut down the entire US Army's military district of Washington, network for 24 hours significantly disrupting government functions. On every system, he alledgely hacked he left messages but one of the messages came back to haunt him. Casey (2009) discussed that an offender encounters the crime scene, leaving something at the scene while also

taking something from the scene. People often leave their digital footprints behind from which their action and its reason can be inferred.

From the above discussion, it can be concluded that digital environments can be illustrated as a situation in which the executor of a crime may leave traces of the attack on the target system while also receiving traces of the actions or activities on the system that was used to perform the attack. Therefore, digital evidence may be found on both the compromised system as well as on the attacker's system. Forensic procedures can be used to acquire these traces from the targeted system and the attacker's system in an attempt to find or show a relationship in evidence that may help to convict the offender. This evidence if not handled carefully can be compromised. One of the negative impacts of technical progress has been an increase in new information threat.

2.5.1 Network Infrastructures

Digital investigators must understand and increase their knowledge with the infrastructure of private and public networks as well as the threats to components of the Internet and Local Area Networks (LANs), in order to understand potential digital crime scenes. It is necessary for investigators to understand the advanced methods of attack used by attackers to exploit the weaknesses of the Internet and thus create damage.

2.5.1.1. Internet

The internet is a huge public wide area internetwork that allows any computer to communicate with another computer using standard technologies and protocols (Tomsho et al., 2007). In order to understand threats to the security of the Internet, it is essential that the investigator first achieve a solid knowledge of the components of the Internet.

The internet has many groups involved in its infrastructure and management, such as the Internet Engineering Task Force (IETF) and the Internet Assigned Numbers Authority (IANA). The Network Service Providers (NSPs) provides national and international interconnecting Internet services to Regional Network Providers and large Internet Service Providers (ISPs).

1. Components of the Internet

The Internet is typically a high-speed connection of networks and it has three main components, as listed below:

- **Network Access Points (NAPs)**

These are the actual method by which ISPs and NSPs are connected. Wireless networks also require an access point. An access point acts as the base station for the wireless network (Ciampa, 2007 p. 171).

- **Internet Service Providers (ISPs)**

An ISP is responsible for connecting actual users to the Internet

- **Domain Name Systems (DNSs)**

This is responsible for translating Internet numbers (Internet Protocol (IP) addresses) to Web names. The organisation that keeps track of all the names and numbers associated with the DNS is IANA. IANA functions as the main controller for the assignment of IP addresses, and manages the Root Domain Name System.

2.5.1.2 Local Area Network (LAN)

LAN is a small network, limited to a single collection of machines and one or more cables and other peripheral equipment (Tomsho et al., 2007). Digital investigators can

use networks to access different types of digital evidence. For this reason, networks are regarded as a critical investigation source.

1. Components of a LAN

The main components of a LAN are as follows:

- **Network Hardware**

A main component of a LAN is the network hardware. The hardware is discussed as follows:

1. Network Interface Card (NIC)

Computers share access to a common network medium to ensure successful communication. In order to access any network, computers must attach to the network medium by using some kind of a physical interface. The hardware that connects a computer to a wired network is called a network interface card (Ciampa, 2009 p. 170). For instance, for personal computers the interface that connects it to a wired network is usually a network interface card (NIC) or network adapter. The function of the NIC is to transport data between a client or server and the shared network media and to listen to frame with their MAC address.

2. Repeaters

A repeater accepts a signal, cleans it and regenerates it, sending it down the line effectively and (Tomsho et al., 2007). Repeaters operate at the Physical layer of the OSI model, function only with bits, and cannot perform any filtering or translation on the actual data

3. Hubs

Tomsho et al. (2007) defines a hub as the centre of activity. The authors explains that hubs applied in network is classified as active hub, passive hub and repeating hub. Most of the hubs installed in networks are the active hubs also called multiport repeater because it has many ports and a repeating hub. A repeating hub is a type of active hub. Hubs assist as a connection point for network devices, which allows them to connect with each other physically on a LAN. A passive hub is just a central connection point and, is used as connection points between a long run of cable and between short runs of cable.

3. Bridges

It connects two network segments and can connect different physical media (Tomsho et al., 2007 p. 484). Bridges limit traffic on each segment reduces bottlenecks and connect network architecture. Bridges work with frames as the protocol data unit (PDU). Bridges operate in the Data Link layer and frames contain physical address information that is also defined in this layer.

4. Switches

Switches are multiport bridges as an intelligent device that maintains a switching table and keeps track of which hardware addresses are located on which network segment (Tomsho et al., 2007). It is a networking device that connects network nodes as network segments. A switch usually has a table that contains the MAC address for each node.

5. Router

A network device is responsible for moving data between different network segments and examining packet headers to determine the best routes for packets to travel. A

router directs packets towards their destination (Ciampa, 2007 p. 172). It recognises paths to all the segments on the network by accessing information stored in the routing table.

- **Network Software**

Another component of a LAN is network software. Computers need network software to issue the requests and responses services o f clients and servers (Ciampa, 2009). There are two types of network operating system (NOS) architecture in a LAN, which are peer-to- peer and client/server. Computers on the network run NOS that establishes what services a computer can offer. Although most operating systems can act as both clients and servers, competent of requesting network services (clients) and providing network services to clients (server). However, many operating systems have a workstation version and server version with the main difference being the number of services offered and the level of security that can be compelled on client accessing those services. Majority of LANs use client/server NOS because of scalability, centralised management and security issues. This research concentrates on client/server NOS because it has become a standard model for networking.

- **Network Communication Protocol**

Once a computer is connected to a network through an NIC or another interface, it must also be able to communicate with other computers by sharing a common set of rules known as network protocols (Stallings and Brown, 2008). In order to communicate successfully, computers must not only share a common network medium, but also have at least one protocol in common so that they understand each other. The protocol that all hosts on the network use is Transmission Control Protocol/ Internet Protocol (TCP/IP). (TCP/IP). TCP/IP has four layers. They are discussed as follows:

1. **TCP/IP Link Layer**

This is responsible for sending data into the physical network and receiving data from the physical network. The link layer protocol is also known as network layer protocols because it provides services called link services such as error checking, physical addressing and routing information and formatting of data for physical transmission and rules for communicating in a network environment (Tomsho et al., 2007) . The most commonly known network protocols are discussed as follows:

- **Internet Protocol version 4 (IPv4)**

It is mostly called as IP, and it provides addressing and routing information. IP provides unreliable service for connecting computers to form a network and it does not guarantee packet delivery (Cole et al., 2007 p. 36). Some security concerns are faced with IP. According to Stallings and Brown (2008) by implementing security with IP, organisation can ensure secure networking.

- **Internetwork Packet Exchange (IPX)**

It is the Novell's protocol for packet routing and forwarding

- **Internet Protocol version 6 (IPv6)**

It is a new version of IP, which addresses some weaknesses of IPv4. As a solution to this, the Internet Architecture Board (IAB) provided authentication and encryption as essential security features (IPSec) in IPv6 (Stallings and Brown, 2008). These security features are designed for use in both the current IPv4 and the future IPv6. IPSec is used to ensure data integrity, authentication and encryption and can also be used to perform packet filtering (Cole et al., 2007 p. 37). IPSec is a security protocol that provides authentication and encryption across the internet. IPSec is becoming a standard for

encrypting virtual private network and it is available on most network platforms and considered highly secure (Dulaney, 2009).

IPV6 will be discussed later in this thesis.

2. TCP/IP Internet Layer

It is responsible for encapsulating transport layer data into packets, and then addressing and routing them. The main types of Internet layer protocols are:

- **Internet Control Message Protocol (ICMP)**

It is responsible for sending error and control messages between systems (Cole et al., 2007). ICMP is used by the Ping utility to request a response from the system to verify its availability for communication.

- **Internet Protocol (IP)**

An internet layer protocol provides source and destination addresses, and routes packets between systems and networks as discussed earlier. IP is fast but unreliable protocol because it has no method for ensuring that data is delivered to the destination (Tomsho et al., 2007).

- **Address Resolution Protocol (ARP)**

It resolves and IP address to a MAC address of a system located on the physical network (Cole et al., 2007).

It is very important for digital investigators to identify and understand the structure of an IP address in order to find a particular digital device on a private/public network. Internet Protocols are logical addresses (numerical identifications) that are assigned to a particular computer. They are divided into two parts, which are networks and hosts. The

network part is what is used to identify the network that the host belongs to, whereas the host part is used to identify the specific system on the network.

3. TCP/IP Transport Layer

This layer is responsible for delivery of data between systems. There are two major types of transport protocols, which are discussed as follows:

- **Transmission Control Protocol (TCP)**

TCP provides connection oriented communication; therefore, it provides more reliable delivery than only IP (Ciampa, 2009). TCP uses a three-way handshake process in which the system initiating a communication sends a packet to the destination indicating its desire to create a connection with a specific network service on the destination computer; if the requested service is available, an acknowledgement is received. TCP is also responsible for message fragmentation and reassembly, by fragmenting large message into segments and using sequencing numbers to ensure that received segment are reassembled correctly.

- **User Datagram Protocol (UDP)**

UDP is a connectionless protocol, therefore, has no three-way handshake to begin communication and it transmits packets (Cole et al., 2007). It is faster and less reliable than the TCP. UDP also does not provide a method of breaking large amount of data into segment; it does not re-sequence packets that arrive out of order and it does not use acknowledgement to ensure that all the data arrived.

4. TCP/IP Application Layer

It is responsible for providing services and utilities that allow client and server applications to access network resources. Some application protocols are:

- **Hypertext Transport Protocol (HTTP)**

It is used to transfer web pages for a web server to a web browser (Tomsho et al., 2007).

- **Simple Mail Transfer Protocol**

It is responsible for transporting mail across the internet (Ciampa, 2007).

- **File Transfer Protocol (FTP)**

It is responsible for providing services for file transfer, directory and file manipulation functions (Cole et al., 2007).

- **Simple Network Management Protocol (SNMP)**

It is a TCP/IP protocol used for managing and monitoring network devices (Ciampa, 2009).

2.5.1.3 Network-Based Mobility Management Protocol

IP is designed to support communication in systems and networks. Also in the mobile networks, every device that is willing to connect to the internet should have an IP address that is used to identify it. This IP address is called Home Address (HA) and can be either IPv4 or IPv6. For the purpose of this research, IPv6 will be studied. Since a digital device obtains its IPv6 address from its home network, it roams with this address within other network known as the Foreign network (Gundavelli et al., 2013). The digital device can obtain a new temporary address known as Care-of-Address from the foreign network and the Correspondent node (CN) is still able to reach the Mobile Node using the HA.

Therefore, many IEFT standards were proposed. The current protocols are either host-based mobility management protocol or network-based localised mobility management protocol (NETLMM). The Proxy Mobile IPv6 (PMIPv6) protocol is a network-based

mobility management approach designed by the NETLMM working group of the IETF that provides effective mobility to mobile nodes regardless of whether they contain a mobility stack A lot of companies, such as Cisco, Nokia Siemens Networks etc. continuously implement PMIPv6. Since Proxy Mobile IPv6 (PMIPv6) is the most widely accepted NETLMM protocol, it will be discussed in this research.

PMIPv6 is faced with the problem long handover delay, as the new access network needs to register the connection of MN and grant it network access; this allows the mobile node to encounter a service disruption due to packet loss. Yokota et al. (2010) discussed fast handovers for proxy mobile in an attempt to reduce the impact of the issue of handover delay. OpenAirInterface PMIPv6 (OAI PMIPv6) an open-sourced under the GNU General Public Licence version 2 is an implementation of RFC 5213 and developed by EURECOM. Loureiro (2010) discussed localized routing in an attempt to solve the route optimization issue in PMIPv6.

The above literatures attempt to tackle the handover delay and route optimization, but there is a need for more effective method for minimizing the issue of handover delay, which result to loss of data packets and service disruption. This research proposes an attempt to implement PMIPv6 with improved buffering in order to solve the issue of handover latency and loss of data, this is discussed in detail in chapter 5.

2.5.1.4 Systems and Network Security Measures

Cole et al. (2007) explain that organisations have different best practices and control measures for securing systems and networks but in a situation where such control measures are not correctly implemented, this can pose a huge risk to an organisation's resources. Some types of security controls for systems and networks are discussed as follows:

1. **Secure Application and Content Based Technological Measures**

These are technical security controls such as tools and techniques responsible for protecting the system from attacks. Some examples are discussed below:

- **Antivirus**

This is a software security applications that scan documents and monitor computer activity for infections such as virus, if a virus is detected the file can be cleaned, quarantine or deleted (Ciampa, 2009). There is a need to update continuously for new viruses to be identified. This will be discussed later because it is one of the security mechanism implemented in the experiment conducted in this thesis

- **Firewalls**

This is a software or hardware that prevents malicious packets in and out of computers and networks. This will be discussed later.

- **Intrusion Detection Systems (IDS)**

These systems utilize different techniques to attempt the detection of intrusion into a computer or network by observing new actions with normal ones, security logs or auditing data. While an IDS is used mainly to identify incidents and raise alerts, if an incident occurs it can also be used as an evidence gathering and logging tool. The IDS attempts to monitor and possibly prevent attempts to intrude into the system.

- **Network Traffic**

This tool is able to analyse the header and content of network packets and is responsible for capturing the full communication stream. A protocol analyzer device or computer that runs protocol analyzer software can view network traffic (Ciampa, 2009). Protocol

analyzer will be discussed later in this thesis because a protocol analyzer was deployed for experiment to represent a good security mechanism

- **Cryptography**

Ciampa (2007) explains that cryptography is the science of transforming information for the purpose of securing it while it is transmitted or stored. This is done to ensure that unauthorised users do not view data. Cryptography can be used to ensure the integrity of the data, which is to ensure that data has not been modified or changed in any way. Cole et al. (2007) explains that cryptography is best understood by dividing it into different areas. The main areas of cryptography are:

i. Random Numbering

This is generating random numbers using algorithms that create pseudorandom numbers, which are numbers that appear to be random (Cole et al., 2007).

ii. Private Keys

A cryptographic key is a mathematical value used to encrypt and decrypt a message. Private Key is also known as symmetric or single key encryption where the same key is used to both encrypt and decrypt the message (Ciampa, 2007). One major benefit of using symmetric encryption is that it is fast, but with the symmetric encryption, the key remain secret by all users in order to get the best result else an attacker that discovers the key can read the messages sent. There is difficulty in transporting a private key to several users and ensuring its confidentiality.

iii. Public Keys

Public key is also known as asymmetric encryption, which requires the use of two keys, a public key and a private key to encrypt and decrypt the message respectively. The

public key, which encrypts the data, does not have to be kept secret, but the private key is kept confidential, therefore, avoiding the need to securely transport keys (Cole et al., 2007).

iv. Hash Functions

These are used to provide better performance when signing large blocks of data using asymmetric encryption, to ensure the integrity, in authentication protocols by ensuring message is not altered during transmission and to create pseudorandom data (Cole et al., 2007). A hash function takes a message of any size and computes smaller messages known as digest or hash. Message-Digest algorithm 5 (MD5) is an example of a hash function. A data always hashes to the same digest regardless of the amount of time computed. The only way a created digest is changed, is by changing the data itself. Therefore, these features ensure the integrity of the data.

2. Secured Policies

The network security measures are responsible for establishing a proper security policy to ensure that data integrity, confidentiality and availability are maintained. The security policy should include steps to secure the network.

3. Secure Operational Procedures

The secure operational procedures are responsible for establishing a proper security procedure to ensure that data integrity and availability are maintained. The security procedure should include steps to secure the network, equipment to be used and action to be taken in the event of incidents.

2.5.2 Attacks and Vulnerabilities

As indicated by the increase in internet usage, there is a great increase in computer networking. However, while internal and external networks such as the internet have increased productivity and profitability enormously, they have also increased system vulnerability. The threats faced by computer networks are obviously linked to vulnerabilities. For example, viruses can damage the system if there is inadequate protection, while improving security can prevent unauthorised access.

2.5.2.1 Taxonomy of Attacks

This section aims to identify suspicious activities that have been performed by attackers in order to harm systems and disrupt services. Any computer connected to the network is under threat from malicious attacks, such as viruses and attacks from crackers. Therefore, a digital forensic investigator and a corporate security investigator needs to understand the nature of these attacks in order to be able to determine which types of suspicious activity can be expected to occur. To understand how to mitigate the threat of malicious software and other threats there is a need to understand their different types. The classification of attacks is discussed below:

2.5.2.1.1 Desktop Attack

- **Malicious Software**

Malicious software or malware is a piece of software that is implemented for fraudulent reasons with the intention of causing damage on personal or corporate computers (Ciampa, 2007).

- **Virus**

A computer virus is a program that secretly attaches itself to a document or another program and executes when that document or program is opened (Ciampa, 2007). Computer virus replicates itself and attaches itself to a host file; this technique is known as self-propagation. The computer viruses infect executable programs. If the virus has attached itself to the application, the code in the virus is run every time the application runs (Nelson et al., 2004). Some viruses are able to attach to data files such as spreadsheet and word processor files. These viruses are scripts that execute when the file is loaded. A script is code written in a scripting language, so it does not need to be complied into an executable; instead, it is run by an application that supports such scripts (Cole et al., 2007).

A virus might be a simple message. Email viruses move from computer to computer as part of the body of the message. When the virus code is executed, a message with the virus embedded is sent to other mail clients. In addition to email, viruses can also be spread through instant messaging (IM). Using an IM program, such as MSM Messenger, AOL Instant Messenger, Yahoo Messenger etc, and users can receive the message immediately after they are sent. Like email viruses, IM viruses are malicious or annoying programs that travel through IM. For instance, IM viruses can be spread when a user opens an infected file that was sent in an instant message (Ciampa, 2007).

In a code attack, such as a virus attack, it is possible many computers are involved. It is important for investigators to be always on the alert for infection of the workstation by malicious code. The workstation should be automatically scanned all the time during the investigation for any code that has past the firewalls and server based antivirus programs (Anderson, 2001). Scan should even continue when an infection has been

detected. As soon as an infection has been detected, and the malicious code located it is important to remove it from the systems, correct all effects and reload backup where necessary.

- **Trojan Horses**

The Trojan horse is simply a program or application disguised as a useful and important program while performing a covert function (Cole et al., 2007). In most instances, users believe they are launching a legitimate application. Trojan horses can attempt to violate multilevel security by communicating important information to a process to allow an intruder gain access to information on the system. In contrast to viruses, Trojan horses are more difficult to distribute. A Trojan horse can operate with all the privileges of the user, so it is easy for the Trojan horse to obtain copies of information that the user processes. Trojan horses can give malicious users access to the system, allowing confidential or personal information to be compromised (Nelson et al., 2004).

An important source of Trojan horse programs is the frustrated programmer who has signed on with an organisation; such a programmer can implant in the code a Trojan horse that performs some malicious function. The routine to carry out the hidden function would be concealed in the legitimate code and might not be easily discovered. Trojan horses are very powerful threats to the security of a computer, network, and organization. They go around most security controls put in place to stop attacks. Trojan horses are not stopped by firewalls, intrusion detection systems (IDS), or access control lists (ACLs) because a user installs them just as they would any other application (Cole et al., 2007). A Trojan horse will be detected by antivirus software, if it is up to date (Anderson, 2001).

- **Logic Bomb**

Logic bomb is a type of Trojan horse that waits until some event occurs. It performs destructive acts based upon a trigger event. The most common trigger is a date, therefore, in most cases it is known as a time bomb (Cole et al., 2007). Logic bomb is a program that performs an action that violates the organisations security policy when some external event occurs (Reichenbach, 2007). A logic bomb is a malicious code, which executes and attacks the infected computers when a particular set of condition is met. Programmers who formerly worked for the victim create most logic bombs or Trojan horses.

- **Back Doors**

Back doors in software permit entry without detection. System designers use them for ease of entry, and people in a position of trust to permit these people to bypass the system's protective mechanisms insert the back doors in the system. Back doors are often rationalised as necessary to permit access when the system has gone into an undesirable error state, and all other means of access are blocked. Perhaps Back doors are necessary as a development tool, but when they are left in operational systems, it is relatively easy for penetrators to find and use them for an unsanctioned entry (Nelson et al., 2004).

- **Worms**

Worms are similar to viruses, but they have two differences. First a virus must attach itself to a computer document, such as an email message and is spread by travelling along with the document, a worm does not attach to a document to spread, but can spread on its own. Secondly, the virus needs the user to perform an action such as

starting a program or reading an email message to start the infection (Stephenson, 2000). If, for instance, a computer is infected with a worm, it may automatically send infected mail attachment to all of the addresses in the address book. A worm does not always require action by the computer user to begin its execution. Worms often replicate themselves until all available resources such as a hard disk drive, computer memory or the Internet network connection are infected.

- **Key Loggers**

User monitoring software existed in different forms prior to the personal computing age, in the 1970's programs designed to capture logon ID and password information on Mainframe dumb terminals were available. Some key loggers are marketed as legitimate tools for tracking employees or family members, For instance parents or employers monitoring their charges for appropriate internet use, but despite the putative legitimacy of some keystroke loggers, this form of spyware continues to be highly prevalent and threatening form of spyware, For instance the case of identity theft or outright spying (Stafford and Urbaczewski, 2004).

Key loggers are also used by hackers to capture passwords and infiltrate target networks. Often they are installed as part of Trojan Horse attacks. Keystroke loggers can also take the form of mechanical devices attached to the computer keyboard. Key loggers are used for recording data that a user may enter. They are invisible to the user and it is installed as an extension between the keyboard and the port (Pietro and Verde, 2010).

2.5.2.1.2 Network Attack

There are some attacks or threats that are conducted against networks:

1. **Denial of Service (DoS)**

Denial of Service (DoS) attack attempts to consume network resources so that the network or its devices cannot respond to genuine requests (Ciampa, 2009). DoS is an attempt to shut down an organisation's network by flooding it with automatically generated network traffic, the services that support the network eventually become overloaded and legitimate users are unable to use the services. In the worst case, network services may crash under the strain of such attack. There are many types of DoS, which are discussed as follows:

i. Distributed Denial of Service (DDoS)

One major type of DoS is the distributed denial of service (DDoS) attack, which is using normal computers that have been hijacked by attackers to carry out malicious network attacks. For instance an attacker breaks into a large computer called handler with huge disk space and fast internet connection, special software is loaded onto the handler computer to scan thousands of computers, looking for computer with vulnerable software in its operating system, immediately a vulnerable computer is found, the handler installs software on the computer turning it into a zombie, and then the handler looks for another computer to infect. The handler can also link all the zombie computers together to form a botnet and instructs it to flood a specific server with a request. A DoS may use hundreds or thousands of zombie computers in a botnet to flood a device with request making it practically impossible to identify and block the source of the attack. (Champlain, 2003).

ii. Teardrop attack

Teardrop is a program that sends IP fragments to machine connected to the internet or a network. Teardrop exploits an overlapping IP fragment bug present in machines. The bug causes the TCP/IP fragmentation re-assembly code to improperly handle overlapping IP fragments (Stallings and Brown, 2008). The main problem with teardrop attack is a loss of data. Configuring the ports on which the defence is enabled is a good option but because the CPU only examines a sample of the fragmented IP traffic on a port, there is no guarantee that the switch will prevent all occurrences of this attack, the switch will continue to forward fragmented traffic until an invalid fragment is detected (Cole et al., 2007).

iii. TCP SYN/ACK Attack

According to Ciampa (2009) in a normal network situation using TCP/IP, a system contacts a network server with a request, and this request uses a control message to initialize the connection called an SYN the server responds with its own SYN along with an acknowledgement (ACK) that it received the initial request, the server then waits for a reply ACK from the system that it received the server's SYN, in order to allow for a slow connection, the server might wait for sometimes for the reply and once the system replies, the data transfer begins. An attacker can send a number of connection requests very rapidly and then fail to respond to the replies. This leaves the first packet in the buffer so that other legitimate connection requests cannot be accommodated. The packet in the buffer is dropped after a short period without a reply. The effect of many such bogus connection requests is to make it difficult for legitimate requests for a session to be established.

iv. TCP/IP Hijacking

TCP/IP hijacking involves attacker gaining access to a system in the network and logically disconnecting it from the network, the attacker then includes another system with the same IP address giving the attacker access to the session and to all the information on the original system (Dulaney, 2009). TCP/IP hijacking takes advantage of a weakness in the TCP/IP protocol. In TCP/IP hijacking attack, the attacker creates spoofed TCP packets to take advantages of the weaknesses. TCP/IP hijacking is successful because some protocols, such as File Transfer Protocol (FTP) and Telnet, do not check the source IP addresses of the system from which they receive packets, therefore, when a system using these protocols receives a spoofed packet from an attacker; it is assumed that it has been received from a valid system (Ciampa, 2009).

v. UDP Attacks

A UDP attack is conducted on a maintenance protocol or a UDP service in order to overload services and initiate a DoS situation. UDP packets are not connection oriented and do not require synchronization process and are susceptible to interception. UPD like TCP does not check the validity of IP addresses. The most common UDP attacks involve UDP flooding in which services, networks and servers are overloaded (Stalling and Brown, 2008). For instance, large streams of UDP packets are focused at a target system, causing the UDP services on that system to shut down or UDP floods also overload the network bandwidth causing a DoS situation to occur.

vi. Smurf Attack

Smurf attacks can create damage in the network. A smurf attack uses IP spoofing and broadcasting to send a ping to a group of systems in the network (Dulaney, 2008). The effect of smurf attacks is utilizing IP broadcast addresses in order to create DoS. ICMP echo request packets can be directed to IP broadcast addresses in order to generate DoS

attack. The ping command is a common network utility used to test connectivity to the specified destination, it sends TCP/IP ICMP echo request packets to the destination and measures the time taken for the echo response packet to return (Stallings and Brown, 2008). In a smurf attack, a TCP/IP ping request is sent to all computers on the network, which shows that the server is requesting for a response. Therefore, each computer's response to the server, overwhelming it and causing the server to crash or be unavailable. Smurf attacks can be prevented by proper configuration of operating systems and routers (Ciampa, 2009).

vii. Buffer Overflow

According to Stallings and Brown (2008) a buffer overflow also known as a buffer overrun is a condition at the interface in which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Attackers exploit such a condition to crash the system or to insert specifically crafted code that allows them to gain control of the system. The program writes more data into the buffer than can be contained in the space that has been allocated in the memory. An attacker can overwrite the data, which controls the program execution path, and hijack control of the program in order to execute the malicious code instead of the process code.

2. Common Attacks

Majority of attacks are intended to utilize potential weaknesses, which can be either in the implementation of programs or the protocols used in networks. Many types of attacks require a high level of complexity, but there is a need for digital investigators to know about them so that in occurrence investigators can identify what has happened in the network. Some common attacks are discussed:

i. Social Engineering

The simplest way to attack a system requires no technical ability and is highly successful. Social engineering relies on tricking and deceiving someone to access a system (Ciampa, 2009). Social engineering is not limited to telephone calls, for instance digging through trash to find computer manuals, printouts, or password lists that have been thrown away are other ways.

ii. Data Loss

Attackers can attempt to break into a system to steal data; other times data can be simply lost and attacker can try to locate the lost data. According to Cole et al. (2008), Forensics is not limited to analysing evidence from a murder scene; it can also be applied to technology. As computers and networks are the foundation for communicating and recording information, a new area known as digital forensics can attempt to retrieve information, which can be used in the pursuit of an attacker. Digital forensics is also used to limit damage and loss of control of data.

iii. Spoofing

According to Dulaney (2008) spoofing attack is an attempt by someone or something to masquerade as someone else. Spoofing occurs when an attacker uses the identity of an organisation's resources such as network computer, in order to gain unauthorised access. Spoofing is impersonation that is pretending to be someone or something else by presenting false information. For instance, since most network systems keep logs of user activity, attackers may spoof their address so that their malicious actions would be attributed to a valid user, fake login screen asking for username and password is displayed, allowing the attacker to capture valid user credentials.

iv. Man-in-the-Middle

Man-in-the-middle attacks tend to be quite complex. The method used in these attacks secretly places a piece of software between a server and the user and the software intercepts data and then sends the information to the server as is nothing is wrong and the server response back to the software, thinking it is communicating with a legitimate client (Cole et al., 2008).

2.5.2.2 Network Vulnerabilities

There are weaknesses that can be found in networks that make them targets for attacks. Network vulnerabilities can be found in both network communication media and network devices themselves. Monitoring network traffic is an important task for a digital investigator. It helps to identify network attacks, for instance a network interface card (NIC) adapter that is faulty and is sending out distorted packets. Monitoring traffic can be done using a protocol analyzer, which helps to capture each packet to decode and analyze its content (Ciampa, 2009). Weaknesses in network devices can also be targets for attackers. One major network device vulnerability is weak passwords, which is unable to protect and prevent unauthorized users from accessing the device and altering data (Anderson, 2001). Although passwords are often the major method of security for a network device, passwords actually provide weak security. For a password to remain secure and prevent an attacker from discovering it, it should never be written down, and password must be of sufficient length and complex to avoid an attacker guessing it. A basic security measure is to require users accessing the internal computer network to have passwords of adequate strengths. Security can be improved by adding further levels of protection, such as biometric scans e.g. fingerprint and retinal scans for sensitive data (Champlain, 2003).

Network device vulnerability is a default account, which is a user account on a device that is created automatically by the device instead of by the administration. Default accounts are used to make the initial setup and installation of the device easier, without the need to create temporary individual accounts; they generally have full administrator privileges so as not to slow down the installation process. Although default accounts are intended to be deleted after the installation is completed, most of the time they are not (Ciampa, 2009). Default accounts are often the first targets that attackers seek. Default accounts usually have simple default passwords that are widely known, this makes it simple for an attacker to access the system and data. It is important default accounts be entirely disabled after the installation is completed.

In a normal situation, a network administrator would set up an account for a user on a network device and assign specific privileges to that account. A backdoor is an account that is secretly set up without the administrator's knowledge or permission that cannot be easily detected, and that allows for remote access to the devices (Tomsho et al., 2007). Back door created on the network device can be network vulnerability. For instance, an attacker using virus, worms or Trojan horse, that inserts a backdoor account, can infect the network device. Also, backdoor accounts are created to allow support personnel to connect remotely to a device for troubleshooting, or when creating a software program, developers sometimes leave a back door in the program that allows them to become the root user should they need to fix something during debugging phase, after debugging is done, and before the software goes live, these abilities are removed but in a situation where a developer forgets to remove the back door in the live version, it leaves the ability for an attacker to take advantage of the system.

2.5.3 Adverse Events and Security Incidents

An event in computer system terms is any discrete incident that can be observed (Champlain, 2003). For instance a user logging on, the file being created, an email being sent or changes being made to a database. An adverse event is simply an event that compromises information security such as an unauthorised user logging in with someone else password for instance, in the alleged case of US v. McKinnon (2002) alternatively, file being deleted accidentally. A computer security incident is an adverse event in which one of the main security objectives, which are availability, confidentiality and integrity, are being compromised (Anderson, 2001). The definition of a security incident includes event such as denial of service attacks, inappropriate usage, malicious software, etc. Security incident can be limited by adopting good security mechanism and guidelines. The need for organisations to employ a range of security mechanisms and procedures to protect their information cannot be ignored. In addition, it is important for digital forensic investigators, security investigators and other professionals to employ different security mechanism and procedures to protect digital evidence. If this is ignored, digital evidence can be vulnerable to be compromised and damaged. If digital evidence is compromised, the confidentiality, integrity and availability of the evidence are jeopardized.

In the alleged case of US v. Gary McKinnon (2002) this is a typical example of distributed denial of service attack (DDoS), alleged Gary intentionally and wilfully caused unavailability of the resource through the internet, accessing the installed RemotelyAnywhere software and using the stolen passwords, thereby causing damage without authorization to the organisation's computers.

According to Casey (2002) most intrusion cases are full of external events that may be used to gain further insight in a case. For instance, a system can be set up to log external

IP addresses that attempt to connect to the system or there is an Intrusion Detection System (IDS) located somewhere on the victim's network, and in some situations the system may contain a list of contacts or email addresses for users that have an account on the system. Any of these factors may allow digital forensic investigators to make connections between the system in question and external factors that may be of interest in the investigation. In intrusion cases, factors to consider could be:

- **Shell History Log:** This log recodes a number of commands issued in a shell environment. This can be very useful because it allows a digital investigator to track through exactly what commands the intruder issued to the compromised system.
- **IP Address:** One major type of information obtained in an intrusion analysis investigation is a log of IP transactions. For instance, the victim's system may keep a log of all systems that it interacts with. In this situation, any computer that uploads to or downloads from the victim's system may be logged. In a situation where the IP is gained, it is possible for the digital investigator to employ commands to find the registered authority for the IP address in question.
- **Classification:** This is identifying unknown data. Common examples would be deleted files or mass quantities of regular files. Mass quantities of files may be classified quickly using a combination of the commands such as find and file. The find and file command will send the file name of all files in a given file structure to the file command, which will try to resolve the file type.
- **Location:** In a relational sense, the physical location in which a network intrusion occurs is quickly becoming a non-factor but this is not to say that the physical location of a piece of evidence is of no importance. The increase or explosion of the internet and TCP/IP as a standard has made it unnecessary for an offender to be physically located in the same area as the victim's system.

According to Casey (2002) the location of the victim's system may be a factor in establishing a motive for an attack. If the victim's system is located in a large entity such as a military base, political entity, educational, or corporate organisation, there is much risk of attack because the information stored in such a system could be of greater value to the attacker. For instance if a corporate network is compromised, the attacker may very well be able to extract money from the victim.

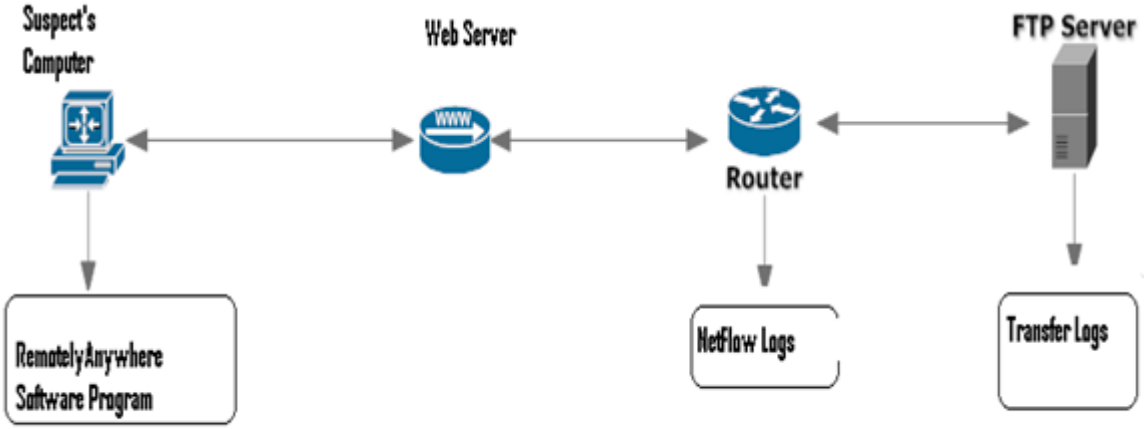


Figure 20: Possible sources of digital evidence for establishing crime

The alleged case of US v. Gary McKinnon presents the idea of a typical DDOS security attack and vulnerability that can be faced in an organisation. It can be recommended that businesses and organisation must follow a good security measures at all times in order to secure digital information.

2.5.4. The Network Security Approach

Schumacher and Gosh (1998) proposed a network security rating model which its objective is to set a rating for the network security across different areas. In this thesis, the network security rating approach is adopted to develop the security model that will

be incorporated i the new model. The initial step was to identify the characteristics of any secure network regardless of the area and independent of any specific threat. Some views adopted from the authors are, physical, communication, operational, personnel, application and performance. In this thesis, for the purpose of the research, the views where categorised into 4 steps such as Secure Application and Content based Technology, Secure Policies, Secure Operational Procedures and Performance (Ademu and Imafidon, 2012f). Each step was identified with threats and assigned codes and security measures as indicated in Table 5.

Table 5: Security requirement of the proposed model (Ademu and Imafidon, 2012f)

Code	**Attacks/Threats**	**Code**	**Security Measures**
S1	Virus	S1a	Anti Virus
	Gaining access to information	S1b	Firewall
	Denial of service	S1c	Protocol Analyzer
	Impersonation	S1d	Authentication and Password
	Altered integrity	S1e	Cryptography
S2	Impersonating	S2a	Password Management
	Loss of data	S2b	Administrative policies
	Denial of service	S2c	Internet connectivity
S3	Gaining access to information	S3a	Management tool

	Loss of data	S3b	Operational procedure
	Denial of service	S3c	Incident response process
	Loss of data		
S4	Loss of data packet	S4a	Performance monitor

The conceptualised digital forensic investigation model in chapter 2 presented 4 phases. There is no doubt that in digital forensic investigation, in order to acheive a successful prosecution, the integrity of digital evidence must be preserved. Therefore, secondly, attributes of an admissive digital evidence was defined such as integrity, availability, accountability and confidentiality. The relationship between the attributes and the identified steps determines a good secuirty level of digital evidence. Therefore each attributes is protected in each steps in order to provide a goood security level to digital evidence.

According to Dulaney (2009) security topology of a network identify the network design and implementation from a security view. Security topology have four main areas of concern:

- **Security Design Goals**

  The goal of setting any security design is concern with issues of confidentiality, integrity, availability, and accountability (Dulaney, 2009). This research in the thesis suggest that addressing these four concerns as a part of digital investigation will assist in ensuring a good level of secuirty. According to Cole et al. (2007, p. 97) confidentiality, integrity and availability is referred to as the CIA of network security. In this thesis, the accountability component is also

identified as a very important secuity design goal which must identify who is responsible for identifying the digital information and collecing digital evidence in a way that preserves the integrity of such evidence. It is important when dealing with digital investigation to be clear about who is responsible for making sure that data information is accurate in order to ensure its admissibility. There is also the need to fulfil the goal of confidentiality which is to prevent or minimize unauthorized access to and disclosure of data and information (Cole et al., 2007) . Digital forensic investigators must ensure that digital evidence is secured and ensures that such evidence do not fall into the wrong hands. Integrity involves making sure that the data or digital information identified, collected and examined for digital investigation is accurate and the integrity of the digital evidence preserved. Futhermore, data information must fulfil the goal of availability. Digital investigation must be able to to protect data and prevent its loss. Data that can't be accessed is of no investigative value.

- **Secure Security Zones**

  Establishing secuirty zones ensures isolating systems and network from unauthorsied users. The internet can be used by anybody with access to an internet portal or an ISP (Dulaney, 2009). Hence, digial forensic investigator must always safeguard the digital data with the extreme safety measure and guidelines. Any organization can create a secure digital environment, by implementing security zones such as intranet (private network implemented and maintained by an organization), extranet (an extended intranet to include outside connections to partner), and demilitarized zones (area where public server can be placed for access by people not trusted).

- **State-of-the-art Technologies**

  One of the main concern with technology is the continous change. The good thing about this, is that these new technologies have become available to assist a less vulnerable system. Vitualization technology which allows any single physical device hide its characteristics from users can improve security in the network. For instance multiple systems can be run one one device and make them appear as if they standalone. Virtualization can present security threats though, if an attacker override the physical layer protection (Dulaney, 2009). Another technology is a virtual local area network (VLAN) that allows creating groups of users and systems and segment them on the network, segmenting assit in hiding segments of the network from other divisions and thereby control access, this also improves security. Network address translation (NAT) server provides IP addresses to the hosts or systems in the network and tracks inbound and outbound traffic (Ciampa, 2009). NAT hides the IP addresses of network devices from attackers, this can improve security of the systems and network. Tunneling is a technology that creates a virtual connection between two systems or networks (Cole et al., 2007). Tunneling can be created between the two ends of a systems or network by encapsulating the data with a common protocol for transmission. Tunneling protocols usually include data security as well as encryption, this can assis in improving security in the systems and network.

2.6 Digital Forensic Analysis and Acquisition/Imaging Tools

Previously during digital forensic investigation, most digital evidence examinations were performed at the file system level neglecting data from the network and digital investigators widely used the evidential copy during analysis. The main risk of this method was that operating the evidential copy could alter the evidence in a way that is untraceable.

2.6.1 Analysis Tools

According to Palmer (2001) analysis tool refers to the actual media examination. The identification consists of locating items present in the device in question and then further reducing this set of items that are needed. These items are then subjected to the appropriate analysis. The type of analysis carried out can be file system analysis, file content examination, log analysis, statistical analysis, etc. The examiner then interprets the results of this analysis based on the examiners' training, expertise, experimentation and experience. As more people became aware of the value of digital evidence, the need for more advanced tools increased. In order to address this need, integrated tools such as Encase and FTK were created to make the digital investigator's work easier. These tools allow more efficient examination, by automating routine tasks and displaying data in a graphical user interface to help the user locate important information (Ademu and Imafidon, 2012c). Recently Linux has been used as a digital evidence examination platform and tools such as The Sleuth Kit and SMART have been developed providing a user-friendly interface.

More advanced tools are available for recovering data from hard drives, but one major concern is that these tools are expensive for most purposes. Regrettably, many people are still unaware of the need for these tools. Another issue is the training and certification in forensic science. According to Moore (2006) a vital problem of digital forensics is economics. This is the training of investigators. This places a financial weight on the agencies that carry out investigations. These agencies can only employ a limited number of investigators, therefore, leading to backlogs in digital forensics. In an attempt to solve these problems, some form of automated processing is introduced to lessen the problem faced by digital investigators. There are many digital evidence analysis tools that are commercially available, these are discussed:

1. Forensic Toolkit (FTK)

Forensic Toolkit is an easy to use computer forensic application. It is identified as the standard in computer forensic software. It is a court-validated digital investigation platform that delivers computer forensic analysis, decryption and password cracking software all within a spontaneous and customizable interface (Ademu and Imafidon, 2012c). FTK is a commercial forensic software product that supports both 32-bit and 64-bit Windows machines. FTK Toolkit is easy to use and understand; it has multiple data views that allow users to analyse files in a number of ways and create detailed report and output them into native format. According to Jones et al. (2005) recent versions of the FTK include acquisition functionality; a forensic information can be acquired using FTK imager with the same hardware devices. FTK has unique features that index text to produce instant search results, data recovery from a file system, email recovery from the leading email services and products along with the recovery of deleted messages and file filtering.

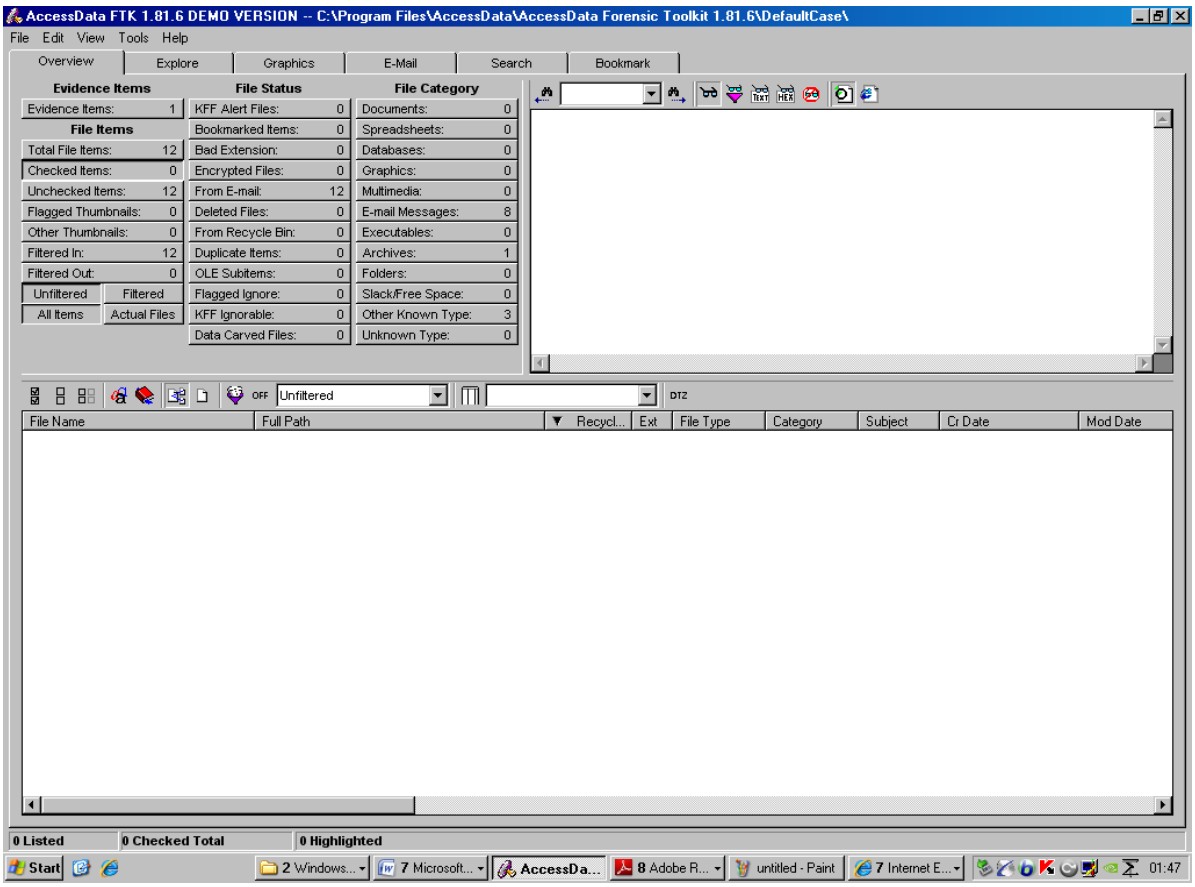


Figure 21: FTK User Interface

FTK supports Password cracking tools as follows:

- **Password Recovery Toolkit (PRTK)**

The Password Recovery Toolkit (PRTK) is an AccessData application, which is a Graphical User Interface application for Windows. This application helps to find and identify encrypted files on handheld, desktop and server computer systems. It can interpret the passwords or hashes of the password in applications such as Office 2000, WinZip, etc. Recently an advance in the encryption functions in Microsoft Office XP, Internet Explorer and Netscape Navigator have posed concerns. A new feature is added to PRTK known as the Distributed Network Attack (DNA) application (Aggarwal et al., 2008).

- **Distributed Network Attack (DNA)**

DNA is a password recovery tool with a twist. It uses multiple computers rather than a stand-alone system to recover a password encrypted file. DNA uses the concept of a network to allocate jobs to client machines to work on. DNA uses the power of multiple processors to make an exhaustive key space recovery. The larger the network, the greater the number of machines and password attempts per second that can be tried. With the help of DNA, investigators can crack the passwords of numbers of networked workstations, reducing the time needed to crack the most difficult passwords.

2. EnCase

EnCase is a commercial forensic investigation toolkit that is largely used within the law enforcement agencies (Nelson et al., 2004). According to Jones et al. (2005) EnCase is able to acquire data in a forensically sound way in which such data can be reviewed by other popular commercial forensic analysis tools. The software can manage a large volume of digital evidence, and transfer evidence files directly to law enforcement or legal representatives as necessary. It enables attorneys to review an evidence easily and also enables a quick report preparation to be made. The EnCase program has initiated Graphical User Interface tools for digital investigations.

A recent feature of DOS is a disk acquisition and preview tool called En.exe, which has been added toEnCase. The GUI EnCase and the DOS En.exe programs create images of a suspect's disk drive. EnCase can also acquire a suspect's disk drive on the network. Encase version 2.0 supports some Microsoft file system types such as FAT12, FAT16, FAT32, New Technology File System (NTFS), Universal Disk Format (UDF), etc. According to Casey (2002) EnCase provides an incredible amount of features and functionality but no one tool can do it all in forensic investigation. An important feature of the EnCase process is the integrated authentication and verification of evidence files.

Throughout the examination process, EnCase verifies the integrity of the evidence by recalculating the cyclical redundancy check (CRC) and the MD5 hash values and comparing them with the values recorded at the time of acquisition. This verification process is documented within the EnCase generated report. It is important to know that it is impossible for EnCase to write to the evidence file once it is created. Just like in other files, it is possible to alter EnCase evidence file with a disk-editing utility, although, if one bit of data on the collected evidentiary bit-stream image is altered after acquisition, EnCase will report a verification error in the report and identify the location of the registered error.

3. The Coroner's Toolkit (TCT)

The Coroner's Toolkit (TCT) is designed by Dan Farmer and Wietse Venema. TCT aims primarily at investigating a hacked Unix host. It offers tools with useful investigative capabilities that are available nowhere else (Kruse and Heiser, 2001). TCT is designed to help in reconstruction of events on a compromised network host. The most interesting feature of TCT is its ability to analyse activities on a live host and capture the current state of information that would be impractical to capture manually. TCT comprises a set of tools used to recover deleted Unix files. It contains a tool that attempts to reconstruct rational or logical data from a stream of bits, and it includes a tool for the Unix environment to create such a stream of bits from a file system. The Unix utility is a Unix tool that creates a single object containing everything that is within all the unallocated space on a file system, which can be a huge amount of data.

4. Sleuth Kit

The Sleuth Kit is an open-source forensic toolkit, which is a suite of file system forensic tools designed by Brian Carrier to perform forensic analysis or investigation in the Unix environment. The first version of Sleuth Kit was called the @stake Sleuth Kit (TASK),

which was based on The Coroner's Toolkit (TCT) and was distributed with similar command line tools (Kruse and Heiser, 2001). Although Sleuth Kit can be run from the command line, many practitioners find it easier to usegraphical user interface. TCT is a very powerful forensic analysis toolkit but its major challenge is the lack of portability between systems and lack of supports for non Unix-like file systems. Carrier developed the Sleuth Kit to provide a highly portable extensible and useful open source forensic toolkit. Since Sleuth Kit is open-sourced, support for any file system can be added. File system support may be added by users of the toolkit as required.

Table 6: Forensic tools, cost and their customisation ability

ToolKit	Scripting	Product cost
EnCase	Yes	£2450
Forensic ToolKit	No	£2700
Sleuth Kit	Yes	Free

The Sleuth Kit locally supports processing raw disk images, but it can also import the ability to process additional image formats from the LibEWF (Expert Witness Format) and AFFLib (Advanced Forensic Format) packages.

Commercial tools such as Carnivore, NetIntercept, NFR Security, NetWitness and SilentRunner have been developed with integrated search, visualisation and analysis features to help digital investigators collect information from network traffic. But this approach does not provide access to deleted data and may not be possible if the device is password protected. Tools such as ZERT, TULP and Cards4Labs have been developed to access password protected and deleted data. There has been a progression in the development of tools for collecting evidence on embedded computer systems.

They are frequently used by digital investigators to read information from pagers, mobile phones and personal digital assistants directly from the devices.

5. **Oxygen Forensic Suite**

Oxygen Forensic Suite is a mobile forensic software package for analysis of cell phones, smartphones and tablets. Oxygen Forensic Software supports Symbian OS, Nokia S60, Sony Ericsson UIQ, Windows Mobile 5/6, Blackberry, Android and Apple Smartphones, etc. Oxygen Software invented an advanced agent approach that allows Oxygen Forensic Suite to extract much more information from smartphones than other logical tools.

6. **Micro Systemation XRY Software**

XRY Software is a digital forensic tool designed by Micro Systemation used to analyse and recover information from mobile devices such as mobile phones, smartphones, GPS navigation tools and tablet computers. XRY software is developed to recover the contents of the device in a forensic manner acceptable by many users. The XRY is a complete digital forensic system for mobile devices that can be used on any Windows operating system.

2.6.2 Acquisition/Imaging Tools

The digital forensic field has created different opportunities for commercial enterprises and open-source alternatives. According to Farrell (2009) tools that perform specific functions are constantly being developed and distributed in the academic and open-source communities and these new functions are ultimately integrated into larger analysis suites. These suites are usually large graphical user interface-based programs that allow an analyst to explore and search for relevant data.

In digital forensics, experts or investigators are relied upon to interpret data and information retrieved by tools and provide findings by tools that can be trusted. According to Altheide and Carvey (2011) the process of digital forensics can break into acquisition, analysis and presentation. Acquisition refers to the imaging of digital devices to be examined, and these can be physical hard drives, optical media, storage cards from digital cameras, mobile phones, chips from embedded devices or single document files and network. The acquisition process should consist of creating a duplicate of the original data as well as maintaining good records of events carried out. The goal of digital evidence duplication is to image the original digital evidence that protects and preserves the evidence from destruction, damage, or alteration prior to analysis by the digital forensic practitioner.

Duplication is an accurate digital reproduction that maintains all contents and attributes. When duplicating or copying evidence, It is important to ensure that the examiner's storage device is forensically sterile. Write protection should be initiated to preserve and protect original evidence. The MD5 or SHA-1 hashing algorithm should be used prior to duplication or copying. The write protection can be performed via either hardware or software. The Hosted Protect Area (HPA) is defined as a reserved area for data storage outside the normal operating file system (Nelson et al., 2004). The Protected Area of Run-Time Interface Extension Services (PARTIE.S) is hidden from the operating system and file system, and that is normally used for specialised applications. It is important to image the digital evidence to the examiner's storage device using the appropriate software and hardware tools.

1. FTK Imager

Graphical User Interface (GUI) tools give an option for the investigator who wants to safely preview digital evidence prior to initiating the forensic process. An investigator

can have a quick scan of digital media using read-only tools without altering any data in the media. A few software developers have recently introduced digital investigation tools that work in Windows. Graphical User Interface forensic tools such as FTK Imager do not require a strong understanding of MS-DOS and the various file systems. They can simplify digital forensic investigations (Nelson et al., 2004). Some of the imaging tools are discussed as follows:

2. SafeBack

In the 1990s, tools such as SafeBack were created to allow digital investigators to collect all data on a computer disk without altering important data. SafeBack is used for bitstream backup. A bitstream backup is different from the regular copy operation. During the regular copying activities, files are simply copied from one medium such as a hard drive to another, e.g. a tape drive. When performing a bitstream backup of a hard drive, bit-by-bit copying of the hard drive is obtained and not just the files. Every bit that is on the hard drive is transferred to the backup medium (Carrier and Spafford, 2006).

3. GetTime

GetTime is used to document the time and date settings of a victim's computer system by reading the system date and time from the Complementary Metal Oxide Semiconductor (CMOS). Digital forensic examiners should compare the data/time from the CMOS to the current time before processing the evidence (Casey, 2004).

4. GetSlack

GetSlack is used to capture the data contained in the file slack of the hard drive. In the process of filling up clusters on the hard drive with files, the segment of a cluster that the file does not completely fill up is called slack space. Slack space is used by the

operating system for different things, but the ordinary computer user cannot view it. Special tools are required to view slack space. It is important to know that valuable information pertaining to an investigation can be found in the slack space (Casey, 2004).

5. Deleted Data (DD)

According to Jones et al. (2005) the most basic non-commercial forensic duplication tools are deleted data (DD). One reason examiners use forensic imaging is for completeness. In forensic examination, the idea of just examining an active file system as presented by the operating system is not sufficient enough. Most volumes contain potentially required evidence outside the viewable, allocated files on a mounted file system. Deleted files are files that have been unlinked, in which the file name entry is no longer present when a user views a directory and the file name, metadata structure, and data units are marked as free. However, the connections between these layers are still undamaged when forensic techniques are applied to the file system. Therefore recovering the files consists of recording the relevant file name and metadata structures and then extracting the data units.

Bugs have been found in different digital evidence processing tools, potentially causing evidence to be missed or misinterpreted. To avoid such errors, it is desirable to assess the reliability of commonly used tools. The National Institute of Standards and Testing (NIST) is making an effort to test some digital evidence processing tools. However, this could be time-intensive due to the advancement in tools. However, it looks impossible that only a single group such as NIST can test every tool in addition to those used to collect evidence from networks and embedded systems. An important approach suggested in this thesis such as following and utilizing simple security mechanism and guidelines can assist in improving security level and integrity of digital information. Studying the complexity of computer systems and the tools used to examine them, it is

not possible to eliminate or even quantify the errors, uncertainties and losses, therefore, digital investigators can proof the integrity of digital information using relevant security mechanism and guidelines (Ademu and Imafidon, 2012f).

2.7 Intelligent Software Agent

Russell and Norvig (2010) describe an agent as anything that can perceive its environment through sensors and act upon that environment through actuators. For instance, a human agent has eyes and ears for sensors and hands and legs for actuators; a robotic agent might have cameras and infrared range finders for sensors and various motor for actuators. A typical example is Letizia, an intelligent agent used for reading documents off the world wide web (WWW). Most of the time when the user is accessing the WWW, the computer is idle, waiting for instructions from the user to retrieve a new document. Letizia uses this otherwise idle time to look for other documents somehow related to the document being read, so that the user, after having read the document, will get suggestions for other documents that might be of interest. Letizia thus bases its search on the contents of relatively recently read documents (Lohani and Jeevan, 2007). Wallace (1997) defined an intelligent software agent as software that uses artificial intelligence (AI) in the pursuit of the goals for its clients. AI is the imitation of human intelligence by mechanical means. In the terms of this research, the word “agent” generally indicates intelligent agent (IA). The following features and properties are very important in defining an intelligent software agent:

According to Williams (2004) an agent is anything that can perceive its environment through sensors and act upon that environment through effectors. The criterion that is used to evaluate and draw a conclusion as to whether an agent is successful or not is performance measurement, and a critical success factor is based on how an agent could perform a particular task. The intrinsic part of an agent is being autonomous, adaptive

and cooperative in the environment in which it operates. The most desirable attribute of an agent is that it is autonomous, meaning the agent should not be under the control of another agent.

2.7.1 Properties of an Intelligent Agent

- **Autonomy:** The agent possesses the capacity to act independently from its user, both in chronological terms and in the sense of adding intelligence to the user's instructions. It needs to exercise control over its own actions (Williams, 2004).

- **Reactivity:** The agent senses and acts on its own surroundings. The agent also reacts to changes in the surroundings that are the result of its own actions (Bradshaw, 1997).

- **Proactivity:** This refers to the agent's ability to exhibit goal-directed behaviour and take initiatives by itself to get closer to the defined goal, out of an external instruction by its user (Russell and Norvig, 2010). It can predict, or at least make good guesses about the consequences of its own actions, and in this way use its reactivity to come closer to its goal. This should happen simultaneously, and on a periodic basis, which is an enormous help in saving time.

- **Adaptability:** The agent's capacity to learn and change according to the experiences accumulated. This has to do with the feature of having memory and learning. An agent learns from its user, from the external world and even from other agents, and progressively improves in performing its tasks, independently from external instructions (Lohani and Jeevan, 2007).

- **Continuity:** An agent does not necessarily work only when its owner is sitting by the computer; it can be active at all times. It is thus a temporally continuous process (Lohani and Jeevan, 2007).

- **Social Ability:** An agent is a piece of social software that interacts with other agents to do its job. It can be talking to other similar agents to exchange information, or it can talk to other kinds of agents to request and offer services. Communication with the owner is also important. It is through this that the agent is praised or punished for its work, and the owner can give further directions to the agent for how it can do its job better (Hermans, 1997).

- **Flexibility:** The agent works proactively; that is, directed by goals, but how it goes about reaching these goals may vary. As opposed to a script that performs the same sequence of commands each time it is run, an agent can do the same job in many different ways, depending on the situation and the surroundings (Lohani and Jeevan, 2007).

- **Cooperation:** The notion of cooperation with its user also seems to be fundamental in defining an agent, different from the one-way flow of information of ordinary software; intelligent agents are, therefore, true interactive tools (William, 2004).

2.7.2 Classification of Agent

According to Hermans (1997) a common classification of an agent is the weak and strong notion of agency. In the weak notion of agency, agents have their own will (autonomy); the agent operates without the direct intervention of humans or other agents; agents interact with other agents and humans (social ability), agents do not simply act in response to their environment (proactively), agents perceive their environment and respond to stimulus (reactivity). In the strong notion of agency, an agent has the ability to move around an electronic network (mobility), agents do not have conflicting goals (benevolence) and an agent will perform in an optimal manner to achieve goals (rationality). However no particular agent possesses all these abilities, but

these types of characteristics distinguish agents from ordinary programs (Ademu and Imafidon, 2012d).

According to Jennings and Wooldridge (1997) agents can be classified by the type of the agent, by the technology used to implement the agent, or by the application domain itself. For the purpose of this research, agent application will be classified as follows:

2.7.2.1 Classification by the Type of Agent

Nienaber and Barnard (2005) classified an agent into two, namely, stationary agents and mobile agents. A stationary agent can be seen as a piece of autonomous software that permanently resides on a particular host. An example of such an agent is one that performs a task on its host machine, such as accepting mobile agents, allocating resources, performing specific tasks, etc. A good example of a stationary agent is Clippit (Clippy), the Microsoft Office Assistant where its settings are for programs in the Microsoft Office Suite. A mobile agent is a software agent that has the ability to transport itself from one host to another in a network (Ademu and Imafidon, 2012d). The ability to travel allows a mobile agent to move to a host that contains an object with which the agent wants to interact, and then to take advantage of the computing resources of the object's host in order to interact with that object. An example of a mobile agent is a flight booking system where a logged request is transferred to a mobile agent that on its part negotiates the web, seeking suitable flight information quotations, as well as itineraries.

2.7.2.2 Classification by Agent Application Domain

- **Commercial Application:** Shopping Assistant uses intelligent agent technology to help the internet shopper to find the desired item quickly without having to browse from one page to another. A good example is the trading and negotiation

agent, which negotiates with other agents to buy or sell shares on behalf of their users and the auction agent at eBay (Patel et al., 2010).

- **Information Management Agents:** These agents help to selectively retrieve appropriate information (Bradshaw, 1997). For instance instead of hiring a help desk consultant to help customers search through the internet for an answer to a question, with an intelligent agent the customer describes the problem and the agent automatically searches the appropriate databases, e.g. CD-ROM, or internet, then presents a united answer with the most likely first. The diversity of information available to us has increased, and the need to manage this information has also grown. The large volume of information available through the internet and the World Wide Web (WWW) represents a very real problem. Even though the end user is required to constantly direct the management process, there is a need for such searches to be carried out by agents, acting autonomously to search the web on behalf of users, which is so important in the digital forensic investigation (Ademu et al., 2011a).

An intelligent agent has been proposed in some distributed applications as a useful mechanism. It is very applicable in digital forensic investigation. As Solomon and Lattimore (2006) mentioned, in many digital crimes, the procedures of accomplishing forensic science are neither consistent nor standardised, instead there are some elementary guidelines and need for automated tools for specific situations.

- **Web Browser Agent:** This is an intelligent agent that helps keep track of what website is visited and customises one's view of the web by automatically keeping a bookmark list, ordered by how often and how recent one visits the site. It also lets you know by notifying you when sites you like are updated, and it could also automatically download pages for browsing offline (Jennings and

Barnard, 2005). A good example is the IBM Web Browser Intelligent, a web spider that is used for collecting data to build indexes to be used by a search engine.

- **Data Mining –** This is where information-specific agents provide a context for data searches in vast databases or other information sources such as the web from which cooperating intelligent personal agents will extract a selection of useful information. This field is one of the fastest-evolving ones at the moment given the explosive growth of the amount of accessible information via networks and communications (Ralha, 2009).
- **Broker Agents:** Another type of agent that act as mediators or facilitators by matching user requests against information or known solutions in databases or provided by database agents (Lohani and Jeevan, 2007).

2.7.2.3 Classification by Technology used to Implement the Agent

- **Interface Agents:** Interface agents emphasise autonomy and learning in order to perform tasks for their owners (Ademu and Imafidon, 2012d). Interface agents support and provide proactive assistance to a user learning to use a particular application such as a spreadsheet or an operating system (Jennings and Wooldridge, 1997). The user's agent observes and monitors the actions taken by the user in the interface, learns new short-cuts and suggests better ways of doing the task.
- **Personal Assistant Agent:** This is an agent that contains personalised learning algorithms developed for a single, specialised application or task. Information filters for browsing tasks belong to this class of agents (Bradshaw, 1997).
- **Mobile Network Management Protocol:** This is where collaborative agents collect and exchange local information on network statistics in order to achieve

automation and optimization of decisions on network administration tasks such as routing, access, service provisions, monitoring and statistical evaluation, within a global view (Ralha, 2009). In MIPv6, which is a host-based mobility management protocol a Home Agent (HA) provides consistent network connectivity services for MN even during MN handover and manages the mobility of the MN (Gundavelliet al., 2013).

2.7.3 The Need for an Intelligent Agent and Programming Language Applied to Digital Forensics

An intelligent agent has been proposed in some distributed applications as a useful mechanism. The intelligent agent is very applicable in digital forensic investigations. As Solomon and Lattimore (2006) mentioned, in many digital crimes, the procedures for accomplishing forensic science are neither consistent nor standardised, instead there are some elementary guidelines and automated tools for specific situations. There are different intelligent agent-based frameworks, but none have brought all the important digital forensic processes together into a single consistent framework. Rekhis et al. (2009) mentioned that digital investigations should integrate the use of formal techniques that are useful to develop results and proof that cannot be disproved, and that can avoid errors. There is a need to consider the development of more enhanced automated tools for imaging and analysis and presentation of digital evidence.

The advancement of the digital forensic investigation requires a new design, improved security mechanism and investigative processes. Forensic experts are faced with growth in data. The amount of data has expanded hugely in recent years and attempts to consume the storage space available. The problem created by this trend is that our ability to analyse and filter data has not grown at nearly the same pace and also the loss in data. Roussev and Richard (2006) explains that computing and human resources are

incapable of accurately analysing that huge amount of data efficiently with present tools. Although computing resources are improving, the distributed computing field has made a major contribution for improvement. By coding tools with the use of intelligent agent programs that can harness the resources of computers, things such as searches can happen quicker, and loss data can be highly reduced.

During the early years of artificial intelligence (AI) development, there were no useful tools for developing AI applications and part of the reason was that the whole field of computer programming was itself a new concept, even object-oriented programming was not yet born (Kossiakkoff, 2003). Later new languages such as LISP and PROLOG were developed to assist AI developers. Although these languages are still in use, many programmers have turned to C++ or Java.

Visual Basic.Net and C# including C++ and Java are object-oriented. They share some of the essential features that have led developers to choose those languages. Visual Studio.NET has developed into a relatively robust tool and offers performance advantages not available in earlier versions. These advantages, along with the fact that many developers have already adopted .NET, and especially Visual Basic, make it an excellent choice for developing the applications applied in digital forensics. Visual Studio is a professional tool that provides a fully Integrated Development Environment (IDE) for visual C++, Visual C#, Visual J# and Visual Basic. IDE integrates all kinds of different codes written in C++, C#, J# or the Visual Basic programming language to create Windows applications. The IDE also provides a wide range of productivity enhancements, such as intelligence, code validation, an assortment of wizards that write code and elements to create and manage databases (Schneider, 2004).

Digital forensic investigators must also keep pace with new developments in areas such as .NET Framework. The .NET Framework can be considered as an operating system

within an operating system. It is an execution environment similar in concept to Java that is designed to run on Windows 98/ME/NT/2000/XP, etc. operating systems and to provide a common environment for programs. This enables programmers to write applications in their preferred language, such as visual Basic, C++, Perl, etc and compile them for the .NET environment, providing greater flexibility and functionality. Figure 22 shows an integrated development environment which provides greater flexibility and functionality, enabling programmers to write applications in their preferred languages and compile with ease and less time consumption. The integrated development environment can be a digital forensic suite for future development (Ademu and Imafidon, 2012b).

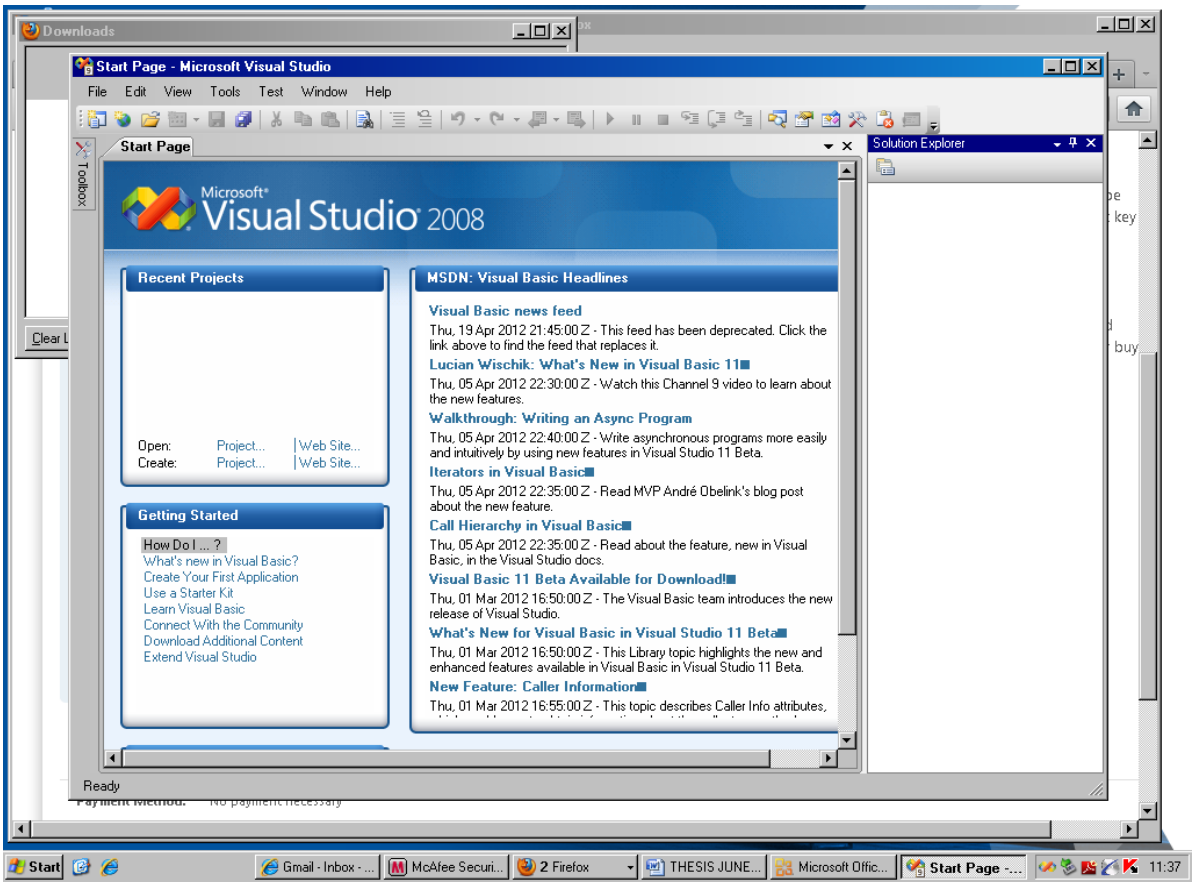


Figure 22: Visual Basic Express Edition

2.7.4 Current Status of the Intelligent Agent Application in Digital Forensics

According to Conotter (2011) the digital multimedia contents as a source for visual information has brought important technical and economical benefit and also problematic issues regarding their authenticity due to forger's ability to easily manipulate digital images or videos in area where sensitive data are dealt with such as digital forensic investigation. The author presented a forensic approach to authenticate photographs depicting text on sign and billboard. Applying forensic methods on the network is done by eavesdropping bit streams with tools called monitoring tools or sniffers. Network traffic can be viewed by a device or software known as protocol analyzer (Ciampa, 2009). A protocol analyzer captures each packet to decode and analyze its content. The analyzer is responsible for determining if an intrusion has occurred and the output of this device may include evidence supporting the conclusion that an intrusion occurred and the analyzer may provide guidance about what actions to take as a result of the intrusion (Stallings and Brown, 2008). The most common network protocol analyser is Wireshark formerly called Ethereal; it is used to filter data in the network . For instance website, email attachment and other activities that have been transmitted over the network can be reconstructed.

The New Technologies Inc. (NTI) developed an intelligent filter program known as the Filter_1, which has the ability to make binary data printable and to extract potentially useful data from a large volume of binary data (Middleton, 2004). The intelligent filter program or Filter_1 tool helps to reduce the size of the bitstream files without sacrificing useful information. IP Filter is an interesting and useful forensic utilities. It was developed by NTI to help law enforcement track down and investigate child pornography cases. It has a simple DOS user interface, and it is used in almost the same way as the Filter_1 (Stephenson, 2003). IP Filter, unlike Filter_1 is used for searching email addresses, Web URLs, and graphic or Zip file names. TextSearch Plus is another

utility for searching a disk for text strings. It can search both allocated space and unallocated space (slack space). When used to search the physical disk, it can be used on any file system. TextSearch Plus makes an excellent tool for parsing very large logs in an internet backtracing investigation. It uses fuzzy logic and is designed to process a large amount of data in a relatively short time.

The problem of consistency in the digital forensic process is a major weakness (Solomon and Lattimore, 2006). Biros et al. (2007) designed the National Repository of Digital Forensic Intelligence (NRDFI) to address the knowledge management issues across many law enforcement and intelligence agencies through an integrated system that allows investigators to access and share information with other agencies. Their research emphasize on the need for consistent security guidelines and investigative process that can improve digital investigation. Ralha (2009) proposed an application that integrated distributed multi-agent application and data mining which the author proposed that agents perform mining tasks locally and should merge their results into a global model. In order to achieve that, the research shows that agents cooperate by exchanging messages aimed to improve the process of knowledge discovered and generating accurate results. Another piece of research was carried out by Roussev and Richard (2004), which proposes the case for distributed digital forensics and presents some examples where they proposed a distributed framework that shows the advantages of distributed approach. The authors designed a prototype based on distributed processing and open protocol, where they presented a prototype where searches can be performed. Ruibin et al. (2005) proposes the application of a case-relevance indicator to the evidence. The research recommends a framework that provides the case relevance information from absolutely irrelevant to probably case-relevant by binding computer intelligence technology to the current computer forensic framework. Gonzalez and Javier (2009) developed a procedure to enable forensic police to extract metric data

from crime scenes using just a single photograph, and this is an improvement in documenting, analysing and visualising crime scene.

Rekhis et al. (2009) developed a system for digital investigation of network security incidents using techniques known as “intrusion response probabilistic cognitive maps” that are constructed to analyse the attacks performed against the network. In their work the authors emphasised that focusing merely on restoring the system is disadvantageous; valuable information and traces that allow understanding of the attack could be removed. If the compromised system is formatted or reinstalled, this weakness points up the need for conducting a post-incident digital forensic investigation. And in dealing with the problem faced with collecting and analysing of large amount of data, digital forensic investigation should reconcile both the expertise of the incident response team and the use of formal reasoning techniques. This allows the better filtering of the data to be analysed and the source of evidence to be explored and also validate the results of the formal techniques by the incident response team before presenting them. The recommendation by these authors relates to this present research where emphasis is placed on good standard security mechanism to be applied to digital investigative process.

2.8 Summary

This chapter reviewed existing digital forensic investigation model. The models were compared and analysed. The common investigative phases were initially grouped into four layers. A structured and consistent framework is vital for a comprehensive investigation model. There was a need to identify all the phases of existing investigation model/framework in a clear and logical manner that can assist in better understanding digital forensic investigation process. A review of the literature led to different ideas on how to pursue the construction of the new model. By Analysing the strength and

weakness of literature models, the conceptualised model was designed to address the impact of security threats and vulnerabilities in digital investigation process. Digital forensic analysis and acqusition tool and other investivative tools were discussed. Also the application of intelligent software agent to digital forensic were also discussed. The initial structure of the model and its four layers and the security requirement was the output of this chapter. The model evolved from the segmented process to a matrix view reflecting all the layers and sub layers of the investigation process.

Chapter Three: Research Methodology

Objectives:

- to discuss the research design
- to explain the implemented research process
- to discuss the various steps of the research process

This chapter begins by discussing the research design and explaining the implemented research process and its various steps. The objectives of the research as mentioned in chapter 1 were the backbone of the research methodology, and the research process was implemented to achieve them. The researcher provides recommendations and then concludes with a chapter summary highlighting all the key findings of the research methodology and future work.

3.1 Research Design

Research methodologies vary from qualitative to quantitative or both (Robson, 2002). Each method assists the researcher to achieve objectives and goals of the research with tools that enable the researcher to obtain data, analyse it, and present the output. Creswell (2003) discussed three main elements that will need to be addressed in order to come up with a structured and well-designed piece of research. The knowledge claim, the research strategy, and method of the data collection are strong pillars of good research. The researchers make claims about what the knowledge is (ontology), how we know it (epistemology), what values go into it (axiology), how we write about it (rhetoric), and the processes for studying it (methodology) (Creswell, 2003). In this research context, the knowledge is digital forensic investigation process and security

threats and vulnerabilities and the need to contribute to a good security level of. Through an extensive literature review and evaluation with modern technologies, the security requirement is established. The value of this research will be reflected through the new model developed and how the technologies assist in digital investigation process.

This chapter of the thesis reflects the overall research process and all the relevant research steps taken. The author adopted a methodological approach in reaching the final digital forensic investigation model. The methodology used in this research involves performing a literature study to identify a key aspect that affects the digital investigation process. An extensive search of the literature relating to digital forensics, particularly with impact of security threats and vulnerabilities has been undertaken. The data collection method of this research involves the use of journals, conference proceedings, books, websites, workshops and seminars understanding the issues on the digital forensic and security threats and vulnerabilities. A test image was created and populated with realistic data.

Some researchers follow the quantitative approach and use the post-positivism knowledge claim. The qualitative approach reflects the constructivism knowledge claim and it uses narrative, ethnographies, grounded theories, autobiography, participatory action research, phenomenology (each grounded in a specific discipline and philosophical assumption) and case studies as strategies of inquiries. The pragmatic approach is a mixed-method approach between the quantitative and qualitative (Robson, 2002). Data collection and analysis was conducted in a method that avoids any data bias. A case study is a method of choice when the phenomenon under study is not different from its context (Gray, 2004). The case study method is used for a wide variety of issues. Case studies can prove very useful in adding to the understanding, extending experience and increasing conviction about a subject. Case studies explore

subjects and issues where relationships may be ambiguous or uncertain (David and Sutton, 2004). The case study approach is considered valid for this research. Marshall and Rossman (2006) explain that the survey is a type of research strategy that collects the same set of information about all the cases in the same data. Survey involves systematic observation or systematic gathering.

Blaxter et al. (2006) argues that action research is a complex and dynamic activity involving the best effort of researchers and practitioners and placing emphasis on promoting change within an organisation. It involves the generation of new information and analysis together with actions aimed to transform the situation in question. Action research is a way of producing desired results for the people involved and it generates knowledge for both the researchers and the participants. Action research is carried out by individuals, professionals, and academia. It involves research, systematic, critical reflection and action. It aims to improve educational practice and is undertaken to evaluate change. The focus group is an example of a research technique that can be used in action research.

Experimental design is a situation in which an independent variable is carefully manipulated by the investigator under known controlled conditions. The experimental and control groups are investigated under the same conditions in order to minimise differences between them (Blaxer et al., 2006). According to Gray (2004), experimental design processes are divided into planning and operational stages. At the planning stage, research questions may be posed and the relevant literature and theories investigated. From this, it should be possible to formulate a hypothesis. The dependent variables are the subject of the research and the independent variables are variables that affect the dependent variables. In this research, experiments were conducted.

The field of forensic science is a convergence of different scientific and social sciences. Digital forensics is a branch of forensic science involving the recovery and investigation of material found in digital devices often in relation to computer crime. Digital forensics was originally used as a synonym for computer forensics but has developed to cover investigation of all devices capable of storing digital data (Casey, 2004). Digital forensic investigations have different applications, the technical aspect of investigation is divided into several sub-branches, relating to the type of digital devices involved, such as computers, networks, databases and mobile telephones.

The different parts of the most common three knowledge claims (post-positivism, constructivism, and pragmatism) were used. The post-positivism was used due to the reason that the theories, hypotheses, background knowledge of the researcher can affect and influence the observations of the research (Robson, 2002). In this research, knowledge background in the digital forensics and the impact of secuirty threats and vulnerabilities has helped to focus on the area needed for improvement in the digital investigation process.

The critical evaluation done in this research by establishing the requirement of the new model through the OAI PMIPv6 and the FTK follows the constructivism approach of the knowledge claim. This approach as stated above may be viewed as qualitative. It can also be argued that since the analysis of the data was based on both qualitative and quantitative approaches, the pragmatism school of thought was adopted during the research process. According to Bryman (2004) a qualitative approach was used when scenarios for applicability or confirming a phase in the model were required. The thematic analysis was practiced and results explained explicitly. A quantitative approach was used where numeric analysis was required for the correlation question relating to which requirements were needed to developing the new digital forensic investigation model.

This research is exploratory in nature. There are different ways of exploring research methodologies. The choice of methodology is determined by different factors, such as research questions asked, what the researcher thinks about the question asked and what the perspectives of people are about the research question. The outcome of exploratory research is not predictable and outcomes can sometimes be quite unexpected. There are different ways of exploring research methodologies. The choice of methodology is determined by different factors, such as research questions asked, what the researcher thinks about the question asked and what the outcome of experiment are about the research question. The research design is related to the fundamental research question. The research journey is mostly not straightforward, and a researcher always has to re-evaluate the first design and re-arrange it to fit current events during the research process. This research journey follows the same path as other research. The first intention was a rigorous approach, sketching a traditional picture of the general research work, literature review, collecting data, drawing conclusions and writing them in a thesis.

3.2 Implemented Research Methodology

There is need to summarise the steps used as the basis of the research process of this thesis. The following explains the steps:

Step 1: Formulate a Research Problem

The research problem was formulated in the initial stage of the research study for the thesis. The main objective of the research was to present a Comprehensive Digital Forensic Investigation model which can be used when conducting digital investigation and preserve the integrity of digital evidence by considering factors which can alter the integrity of digital evidence when conducting such investigation. The initial stage of the research problem was to address the important need of information technology and its

problems in organisations and private lives and then it was narrowed to address digital forensic investigation and digital incident and attacks faced that can alter integrity of evidence when conducting digital investigation. The research problem was thought of as a security challenge and the researcher started to analyze what would be the best model developed for such a challenge. The main output of this phase was the identification of the research challenge.

Step 2: Conceptualising, and the Research Design

During this stage, the researcher studied and reviewed the literature explaining the existing digital forensic investigation model addressing various activities carried out in digital investigation, and different types of the models were analyzed. The researcher searched for models, theories, journals, and previous research addressing the factors such as digital attacks and security threats which may have a direct or indirect effect in altering the integrity of digital evidence. The researcher then started to analyze the factors which can alter the integrity of digital evidence when conducting digital investigation. Literature and models reviewed are explicitly explained in Chapter 2. A review of the literature led to different ideas on how to pursue constructing the new model. It revealed several key requirements the new model will need to incorporate to be comprehensive such as the link between the security mechanisms and guidelines and the need to preserve digital evidence when conducting digital investigation. It was established that the existing models and frameworks address one or two aspects of the information security, not all, needed in digital investigation.

The majority of the literature was addressing approaches for collection and analysis of digital evidence. These approaches as solutions were presented as models required for digital investigation. The review presented the gap that there is no comprehensive model which addresses approaches to solve issues related to data integrity. Analysing

the strength and weakness of literature models, the structure of the new model was designed to address this issue. The initial structure of the model and its four phases was the output of this phase.

Step 3: Constructing Instrument for Data Collection and Collecting the Data

In the first experiment, a testbed was created to collect data packets based on the OAI PMIPv6 implementation. In the area of mobile network, the research proposed and implemented PMIPv6 with improved buffering to minimize performance issue which the research identified as able to assist in providing reliable services and in turn assist in digital investigation. The research identified that current approach of managing network-based IP mobility which is the standard PMIPv6 is identified with performance problem of handover latency and loss of data packet which can influence the integrity of data, therefore, the research proposed and implemented PMIPv6 with improved buffering in order to minimize this effect on data packets. A network experimental test was set up to carry out incident such as loss in data packets. This has led to creating an experimental network environment in which 3 nodes were connected to the same collision domain. Then packet traffic is transmitted between nodes for the purpose of comparing the PMIPv6 and PMIPv6 with improved buffering for solving handover latency and loss of data packet which are performance issue that can influence the integrity of the data as identified in the research. Also, another testbed was populated with real data and collection and analysis of data was carried out with the use of FTK. CDFIM was applied to conduct experimental test digital investigation to test the research hypothesis, and the applicability of the model. Related research papers such as journals, and industrial white papers were researched, collected, indexed. The objective of this step was to have a good repository of journals and conference proceeds addressing the topic of digital forensic investigation models and information security.

Step 4: Selecting a Sample

Based on the reviewed literature in chapter 2, the requirements for the model were identified. PMIPv6 with improved buffering was proposed and implemented based on the OAI PMIPv6 implementation. The PMIPv6 with improved buffering and the test case investigation conducted with Forensic Toolkit (FTK) will be explained in detail in chapter 5 and 7. The main objective of the experimental process were to the test the hypothesis of the research and the easiness applicability of the requirement of the new model.

Step 5: Processing the Data

The collected data for both experiments were analysed based on the real testbed environment. The data was examined against the model built in order to identify areas of support and areas that do not support the model. The correlation between the security measures and guidelines with investigative process were conducted between the different sections of the model in order to construct the final conclusion of the experimental results.

Step 6: Developing the Final Model

This stage of the research focused on processing the information which was collected from the real testbed, compare the results with the initial conceptual model developed in the initial stage of the research, and confirm the layers which are used to construct the final model. As a result of this stage, the final version of the model is presented in this thesis document.

Step 7: The Validation Phase

The validation was achieved based on the following:

- Observation from the collected data and the analysis results has shown the confirmation of the layers initially constructed as part of the conceptual model in the early stage of the research.
- The use of Open Air Interface PMIPv6 showed the strong interest of internet and security practitioners to have a common interest to have a secure protocol as reference which can identify the security level of data packet. This was observed from the experiment result of the standard PMIPv6 and the PMIPv6 with improved buffering. The PMIPv6 demonstration (PMIPv6D) was first developed and validated under Linux UBUNTU 10.04 by EURECOM.
- The final model was evaluated by conducting investigation on two real digital crime cases based on CDFIM

Step 7: Writing the Research Document

The research document was written in parallel to each step of the research process. The research document structure is explained in chapter 1, it covers the literature reviews, findings from the data analysis, the structure of the new model, an explanation of each layer in the new model, and the detailed validation process followed for this research.

3.3 Summary

The major aspect covered in the research methodology chapter is the scientific background of the research methodology, knowledge claims adopted, the implemented research processes, the methods of data collection, and the validation process followed during the construction of the thesis for the new model. The researcher used the post-positivism, constructivism, and the pragmatism knowledge claims. The research analysis of the data was using both qualitative and the quantitative research strategies. The qualitative and quantitative data analyses were applied on the data collected. The qualitative analysis was mostly interpretive using the researcher's intuition and it was mainly for the analysis of the human factors in selecting or rejecting security

technologies, committing computer crimes (creating of information threats), and interactions with security systems which include technologies and policies. On the other hand, the quantitative analysis was applied to study security technologies implemented in the areas, number of security incidents experienced.

Chapter Four: The Comprehensive Digital Forensic Investigation Model

Objectives:

- to discuss the different areas of digital forensic investigation model
- to explain the step by step process of developing CDFIM
- to provide a comprehensive model for digital investigation

The principle of digital forensics and investigation is to discover, obtain, analyse and preserve digital evidence as discussed in Chapter 2. The Chapter also mentioned that there is no model that identified security threats and provide security measures for the relevant digital forensic investigation process. This research argues that information security guidelines integrated in the digital investigation process can assist in establishing integrity of digital evidence.

In this chapter the step by step design of the investigative process for discovering, distributing, reconstructing and maintaining digital information by identifying factors that can influence the integrity of digital information will be described and a Comprehensive Digital Forensic Investigation Model (CDFIM) that improves on previous digital forensic investigation process is created. In addition, the chapter examines the area of application of digital forensic investigation and impact of security threats and vulnerabilities.

4.1 Digital Forensic Investigation

To relate the security technologies and guidelines proposed by the researcher with the digital forensic investigation process, different digital forensic investigation model and security threat and vulnerabilities has been reviewed. A good description was given in the literature about different digital forensic investigation model. Security requirement for digital forensic investigation was also found in the literature. Many cases were studied which are stressing on the need of applying the right technologies and guidelines in order to protect the digital information and digital evidence. The alleged case of US v.Gary McKinnon and how Gary McKinnon was alleged to intrude the computers indicated the effect of a technical and operational security issues on the corporate infrastructure. The implementation of security technologies and guidelines will play a major role in protecting and alleviating such risks. However, identifying the necessary technologies is not effective enough. The selection and implementation of the appropriate technology is important to the security plans of any organization and digital forensic investigation. The objective of the new approach is to turn the digital forensic investigation process into a comprehensive digital investigative process, which addresses the threats and vulnerabilities related to different digital technologies. The new approach can be considered as a tool to think about the threats of digital forensic investigation process and a method, which can be used by investigators to highlight a risk and manage its effect.

There are different aspects of digital forensic investigation, for the purpose of this research in this chapter, computer forensics, network forensics and Email forensics will be discussed:

4.1.1 Computer Forensics

Computer forensics is the science of computer crime investigation (Ruibin et al., 2005). The main purpose of digital investigation is to collect digital evidence without altering or damaging it (Kruse and Heiser, 2001). Computer systems and other electronic devices have been widely used in the past two decades and a large amount of information produced, accumulated, and distributed through electronic means. The majority of organizations interact with electronic devices every day for this purpose, there is a need to find digital evidence in computer systems and other electronic or digital devices.

Since digital devices such as computers are vulnerable to attack by criminals, digital forensics is very important. Understanding digital forensic procedures will help to capture vital information, which can be used to prosecute an intruder that compromises a digital device or network. Also, deciding on the specific tools for computers or other digital devices that is needed to correctly analyse evidence is crucial (Ademu et al., 2011b).

Data location is the process of finding relevant data stored in hard drive or other devices. Relevant information is often stored inside files, handled by the operating system of the computer that the mass storage devices are attached to, and there are still many cases in which information is stored on the hard drive without the recognition of the operating system. Storage devices are usually divided into one or more partitions, each of which has at most one file system associated with it (Nelson et al., 2004). Some of the locations data can be found are discussed as follows:

- **Log Files:** Operating systems and some applications and services store information about events in log files. Log files on the computer are important locations when searching for information about the potential attack (Cole at a.,

2007). For instance Windows Security log, identifies security events that have occurred, as long as the system is configured to log those events. Other log files can be viewed through Event Viewer and also the Application log is a log file used by a number of applications.

- **Cluster Tips:** Clusters are physical entities of a hard drive. Many operating systems, such as Linux and all Windows versions etc, share one rule known as "one cluster, one file", that is, each cluster will have information inserted belonging at most to a single file (Kruse and Heiser, 2001). The cluster tip technique involves reading clusters filled with data belonging to the RAM. Keeping in mind that the data are stored on a disk because of the operating system's limit to write a full block at once, they could be located by looking for an end-of-file character and then reading whatever follows. When a user deletes a file, such file will be moved to the Recycle Bin, however, even though the Recycle Bin is emptied, deleted files still remain on the hard disk. This is because a file is written to the hard disk in clusters For instance when a file is deleted, the area of the hard disk where the data was stored becomes available, some of the file contents remains available until the bits of the hard disk are over written with other data. The data left can be analyzed using some forensics and data recovery applications.
- **Hidden Files:** An attacker might try to hide their activities by hiding malicious files by changing the name or file extension of a file so that it looks like something genuine. Hidden files can be viewed using appropriate tools.
- **Free Space:** The operating system uses the free space only to store new data, since if there is no file associated with a block then there will be information to handle (Ademu and Imafidon, 2012e). Data contained in free space will be transparent to nearly all the applications. It is important to notice that operating

systems provide functionality to read arbitrary blocks from the file system, whether they are marked as free space or not, so data stored in free space are not transparent to the operating system. A skilled user could hide sensitive information inside blocks considered as free space by the file system and these data are not associated with any files, so they cannot be found by a common file searching utility (Pietro and Verde, 2010).

- **Registry:** System and application settings in the Windows operating system are usually stored in a database known as the system registry. Nearly all the operations in the Windows operating system involve reading from and writing to the system registry. Searching for data through the registry is a good way to reconstruct the history of actions taken by users of the computer system. The registry technique consists in reading sensitive data from the registry, even looking for deleted or undeleted data before they have been updated (Pietro and Verde, 2010).
- **History and Temporary Files:** Applications provide a special functionality to provide easy recovery of unsaved data after a boot crash by saving periodically. Such temporary file is created by some applications, such as Microsoft Word, although applications sometimes delete the temporary files they create but some do not. These type of files might contain valuable information. Also, temporary files are useful in internet applications, and users commonly visit some websites more frequently than others. Storing information from a website, such as images or a hypertext document, will speed up a browser since data are present locally and need not be requested from the website (Pietro and Verde, 2010). Some websites download temporary files to the user's hard disk to allow a web page to load more quickly on subsequent requests. Therefore, the temporary internet

files cache can be a possible location to look for digital evidence, mostly when examining a suspect computer where an attack was launched.

- **Swap File:** This is a Windows file used for virtual management. If a user is working on a file or document, Windows can copy all or part of it in an open unencrypted form to the swap file on a storage device. Encryption keys, passwords and other important information can be changed on the storage device, although, if a user uses all the security features in the updated versions of Windows, merely investigating the swap file in DOS mode with readily available tools may allow for important data protection.

4.1.2 Network Forensics

Digital forensic investigators need a basic understanding of networks to interpret digital evidence found onnetwork and system sources such as web browsers and file transfers. An understanding of fundamental network technologies is essential to track down unknown offenders through networks and related criminal activities to the networks (Ademu and Imafidon, 2013). For instance when digital investigators are not faced with attack launched on computer but faced with attack on the network, evidence can be reconstructed using digital information and digital evidence on the networks. The current state of the system might need to be documented. Victims may be persuaded to make available their live system, sources of evidence on the internet that may reveal with whom the victim was communicating, which involve log files on the victim's Internet Service Provider's system and backup tapes (Casey, 2004). Mobile telephone records may help verify with whom the victim was communicating and where the victim went.

4.1.2.1 Sources of Digital Evidence on the Network

The sources of digital evidence on the network may include the following:

- **Listening Ports**

Information can be viewed about listening ports using special application and command line utility,by displaying the protocol, the local address and the foreign address (Cole et al., 2007).

- **Network Connections**

Information on network connections can also be viewed using special applications and command line utilities which can assist in establishing whether the network connection is listening.

- **Live Applications**

Information can be saved on running applications on a computer. For instance in Windows, Task Manager allows viewing the processes running on the computer. The tasklist commnad line utility can assist in outputing a lsit of processes running on the computer (Dulaney, 2009).

- **Log Server**

The networked computers create log files that contain data or information on activities, connections and other transaction (Tomsho et al., 2007). Timestamping plays an important role in identifying the times at which activities were conducted (Kossiakoff, 2003). Log files for example use timestamps to indicate when an activity was added. A digital forensic or security system investigator should protect log files from misuse or alteration (Ademu and Imafidon, 2012e). These files should be kept locally by using a centralised log server. The log server prevents an attacker from altering the logs.

- **Contents of Network Devices**

A routers can be used to facilitate exchanging data between networks. When the router receives a packet, it analyzes the packet's destination network address and looks up that address in the routing table, routers are brilliant source of digital evidence (Casey, 2004). Firewalls can keep detailed logs of successful and unsuccessful attempts to reach hosts that they protect. Intrusion Detection Systems (IDS) are used to collect information from a variety of system and network sources, then analyse the information for signs of intrusion and misuse. In the network-based intrusion detection architecture, the system is used to analyse network packets (Anderson, 2001). Network-based architectures are used to detect access attempts and denial of service attempts originating outside the network. This architecture consists of sensors deployed throughout a network. These sensors then report to a central command console.

- **Traffic on Both Wired and Wireless Networks**

Peer-to-peer networking has been advanced by wireless technology that uses radio frequency, infrared, lasers and microwaves such as Bluetooth-enabled computers, personal digital assistants, mobile phones, etc. When a Bluetooth-enabled device is on, it attempts to communicate with other devices around it. The majority of the components of networked systems contain information about the activities of the people who use them. Routers are at high risk of attack and computer intruders target them to eavesdrop on traffic and disrupt or gain access to networks (Casey, 2002).

- **Network Communication Technologies**

A computer connected to a network is generally known as a host, and uses a modem or NIC to send and receive information over wires or through the air (Casey, 2004). In the past tap was used to connect a host to the network. But because this approach was difficult to maintain, devices called hubs were developed to reproduce the single

network cable configuration. In order to increase network security and efficiency, switches replaced hubs. Transport Control Protocol/Internet Protocol (TCP/IP) is used to communicate with computers connected to the internet. Routers are an important component of computer networks, essentially routing d data to the correct place, they are used to connect hosts to two or more networks and direct traffic between them. Firewalls are similar to routers in the way that they direct traffic from one network to another. These security devices are designed to block traffic by default and must be configured to permit traffic that meets certain criteria. The services that networks enable, such as sending and receiving emails, rely on the client/server model. Telnet provides client/server communication, enabling remote users to log into a server and execute commands. Two hosts using different network technologies cannot communicate directly. There are two methods of enabling communication between hosts using different network technologies: translators and common languages. When connecting different networks, it is more efficient to join them using devices with the necessary network interface cards and then use a common internet protocol such as TCP/IP that every host can understand (Tomsho et al., 2007).

The most widely used internet protocols are the Transport Control Protocol (TCP), the User Datagram Protocol (UDP), and the Internet Protocol (IP). These protocols, including a few supporting protocols, are collectively referred to as the TCP/IP internet protocol suite (Dulaney, 2009). In order to identify and deal with digital evidence on the internet, digital investigators need a concrete understanding of TCP/IP and identify method of avoiding data loss (Ademu and Imafidon, 2012f).

Mobile communications is in reality part of our daily lives. With the increase in PDA devices and ever-present availability of access network, IP Mobility is now a key aspect of mobile communications. Mobile IPv6 (MIPv6) protocol is a host-based mobility management protocol that has been developed by the Internet Engineering Task Force

(IETF), it requires the participation of the host in all aspects of mobility management (Gundavelli et al., 2013).

The Proxy Mobile Internet Protocol version 6 (PMIPv6) is designed to resolve the problems of MIPv6 and provide mobility management support to a mobile node without requiring its participation in any mobility related signaling (Gundavelli et al., 2013).

4.1.2.2 Network Technologies

Network technologies enable multiple hosts to share a single transmission medium such as wire or the air (Ciampa, 2009). In the process of the host sharing a transmission medium, only one host can use the medium at a particular time, but there would be an interference with each other if two hosts were allowed to use the transmission medium at the same time. There are many different network technologies but for the purpose of this research, three of them will be discussed (Ademu and Imafdon, 2012e) as follows:

- **Ethernet**

Ethernet is one of the most used network technologies because it is fast and inexpensive (Col et al., 2007). One of the most recent forms of Ethernet uses wires similar to the telephone cord. Ethernet uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) to synchronise communication.

- **Asynchronous Transfer Mode (ATM)**

ATM uses fibre optic cables and ATM switches to enable computers to communicate at very high rates (Tomsho et al., 2007). ATM uses technology similar to the telephone system to establish a connection between two hosts. The hosts are connected to a main ATM switch and these switches can be connected to form a larger network. One of the

hosts contacts the main switch when it wants to communicate with the other host. The switch contacts the other host and then establishes a connection between them.

- **Wireless**

According to Stallings and Brown (2008) hosts connected using one of the IEEE 802.11 standards do not require wires, and they transmit data through the air using radio signals. Commonly used standards and their spectrums are IEEE 802.11a (2.4) and IEEE 802.11b (5GHz). Computers, personal digital assistants, mobile devices and other devices with a compatible wireless NIC use access points to communicate with each other. Access points are also generally connected to a wired network, such as an Ethernet network, to enable communication with wired devices and the internet. The main limitation of 802.11 networks is that a computer must be within a certain distance of an access point to achieve reliable connectivity and, even then, data are only transmitted at a limited speed (Ademu and Imafidon, 2012f).

Most of the available mobile devices are equipped with multiple radio interfaces. These mobile nodes can possiblly attach to the network using one or more interfaces and be using all of those interfaces simultaneously for its data sessions. A mobile operator can also potentially be managing more than one access technology in their main network, these access networks can be running any IP protocol version such as IPv4, IPv6 or both (Gundavelli et al., 2013).

4.1.3 Email Forensics

There are no much difference in an email forensic investigation process from other areas of digital forensic investigations, except that email forensic may require different tools and techniques in its investigative process to achieve a convincing evidence. According to Palmer (2001) digital forensic investigation is the applciation of scientific, systematic and proven methods towards the preservation, collection, validation,

identification, analysis, interpretation, presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal. By this definition, it is important to demonstrate proofs of intergrity of digital crime objects beyond the presumptions of the occurence of a crime by employing consistent and methodical processes to establish the crime. Therefore, it is imperative to prove the integrity of digital evidence at any time in digital investigation (Ademu and Imafidon, 2012g). Since email crime can be as a result of forged and genuine messages with malicious purpose or even email messages sent in ways that can violate an organisation security policy.

Emails may be recognised by their header at the beginning of the message providing useful information of the IP address of the relaying mail servers, the names of any attachements included in the email, the time and date the email was sent (Ademu and Imafidon, 2012e). An email header can assist in viewing its path from its source to its destination. Email forensic investigation aims to identify details of the system that sent the email invloved in the crime, the authorship of the identified systems and to establish if the email messages are encoded according to some stardard, such as Multipurpose Internet Mail Extensionm (MIME), Binary to ASCII encoding scheme (Bin Hex), Unix-to-Unix encode (Uuencode), and transported through such protocol as Simple Mail Transfer Protpcol, Internet Massage Access Protocol (IMAP) and others (Ademu and Imafidon, 2012g). Hadjidi et al. (2009) argues that one limitation that exposes email communication to illegitimate uses is that the widely used email SMTP protocol, lacks a source authentication mechanism and that the data in the header of an email containing information about the sender and the path along which the message has travelled can easily be forged or anonymized. Information can be gathered through email if the attack was based on malware distributed through email, a spam and phishing attack. Also email can be used as evidence if the attacker is an employee. There is need also for

digital forensic investigation to be employed in a manner that can collect credible evidence by preserving information from email.

4.2 Threats Impact on Digital Forensic Investigation

Networks contain digital evidence that can establish that a crime has been committed, determine how a crime was committed, reveal links between an offender and the victim, disprove or support witness statements and identify likely suspects (Ademu and Imafidon, 2013). For instance child pornography on the internet has led digital investigators to the victim, an email of a missing person has created links between the victim and the offender.

In dealing with evidence on the internet, digital investigators are faced with some challenges. One major problem is that data on the networked systems are dynamic and volatile, making it difficult to take a snapshot of an entire network unlike with stand-alone computer systems and data are also easy to be lost (Dulaney, 2009). Shutting down a network will result in the destruction of most of the digital evidence it contains. An attacker can be in many places on the network at a particular time. This distribution of criminal activity and associated digital evidence makes it difficult to isolate a crime scene on the network. But having evidence distributed on numerous computers or networks can be an advantage in an investigation. The distribution of information makes it difficult to destroy digital evidence because if digital evidence is destroyed on a particular computer or network, a copy can be found on various computers on the network or on backup tapes. It is a good practice for organisations to back up their information regularly and store copies of all backups in a different location (Ademu and Imafidon, 2012e).

In some situations, digital evidence exists on networks that were not directly involved in a crime. There are always more sources of digital evidence on the network than even the

digital investigators realise. Therefore, to ensure that relevant data is located, digital investigators must use their understanding of networks in general. Collecting digital evidence from a large network requires significant preparation and planning. Planning is important in cases that involve digital devices. If possible, when generating a search warrant, care needs to be taken in researching the search site in order to determine what digital device to expect, what the system is used for and if it is a network environment or not. If the digital equipment is used for business purposes, this will influence the planning and preparation process. It is also important to know that without this information, it is difficult to know what expertise and evidence collection tools are required. At this stage proper preparation needs to be done for tools and storage capacities that will be used. In order for plans and procedures for investigation to be successful, it is important to provide an adequate acquisition process (Casey, 2004).

Digital evidence must be preserved as soon as it has been identified and collected and in a way that it preserves its integrity. The empirical law of digital collection and preservation states that if only one copy of the digital evidence is made, that evidence will be damaged or completely lost. Therefore, at least two copies of the evidence are taken. One of these is sealed and then placed in secured storage. This is the original copy and will only be opened for examination under instruction from the court in the event of a challenge to the evidence presented after forensic analysis on the second copy (Sommer, 2009). The main challenge of preserving digital evidence is collecting it in a way that does not alter it and also during the transmission process in the case of digital evidence from the network.

Most amount of digital evidence is a rich and often unexplored source of information. It can enable an investigator to create an incredibly detailed picture of events surrounding a crime. When an event happens, it is good practice to note the time it occurred, for example the time an individual logged on using a password, this can assist an

investigator in reconstrucitng the event. Digital devices can be useful for reconstructing the sequence of events or activities. The position of digital evidence in relation to other objects can be very informative. Determining where an object or individual was in relation to other objects or individuals is useful when investigating digital crimes mainly in a networked environment (Casey, 2004). In a large digital fraud case for example thousands of people and computers can be involved, making it difficult to keep track of the many relationships between objects. Creating a diagram visualising the associations between the objects and users can assist in analysing the activities. Analysing digital evidence from networks frequently needs specialised knowledge of tools and the underlying technology. There should be duplicates of digital evidence from a compromised systems, strict use of write-protection technology, and a positive legal chain of custody can be maintained. Hashes and checksums should also be maintained on duplicates and duplicate copies should be made and used during analysis. Presenting the findings to non-technical individuals can be challenging but remains one of the most important stages in a forensic examination because a digital forensic examiner's findings needs to be understood in order to be used (Ademu et al., 2011).

4.3 Towards a Comprehensive Model for Digital Forensic Investigation Process and its Security Guidelines

Based on the review of academic and industrial literature, a comprehensive approach that could be used to examine digital investigation process addressing security threat was not found. Most of the literature studied emphasized the collection and analysis of the evidence. There is no doubt that the process of evidence collection and analysis are major parts of the process of digital forensic investigation, but there is need to emphasize on the countermeasures of security threat of the process of digital forensic investigation. Digital forensic investigation processes are not in every steps supported by fully automated processes nor are offered through a common technological

infrastructure. Digital forensic investigators might have different levels of competencies, but there is need for them to follow appropriate security guidlines and measures and processes during digital investigation (Ademu and Imafidon., 2012f). The new Comprehensive Digital Forensic Investigation process includes two parts. Firstly, the new digital forensic investigation processes which are divided into four phases are discussed (Ademu et al., 2011b). Secondly, the security requirement layers and sublayers that are incorporated in the digital forensic processes are discussed (Ademu and Imafidon., 2012f).

4.3.1 Selection Criteria of the Layers of the New Model

The following criteria are used for the selection of the layers and sublayers in the model:

- The layer must address a security requirement in digital forensic investigation process
- The security sublayer must be recognised by information security service providers.

4.3.2 The New Digital Forensic Investigation Process

Having more than one layer of any model gives the model a robust structure. A literature review and an extensive research were conducted in order to prove the requirement and need of the layers discussed in this chapter. The literature review analysis indicates four main phases such as preparation, interaction, reconstruction and presentation of digital forensic investigation process (Ademu et al., 2011b). The proposed model contained different layers of digital forensic investigation process in four phases. The following are discussed below:

4.3.2.1 Preparation Phase

In order for a digital forensic investigator to acquire digital evidence, there are a number of things to consider. It is important for the investigator to ensure that the search will not violate any law, and all types of risk assessment needs to be carried out. For instance, in the case of stored email there are strict privacy laws protecting such digital evidence. If this law is violated, the evidence can be severely weakened. It is recommended as best practice for investigators to collect written instructions and authorisations from their legal representatives before conducting digital investigation (Ademu etal., 2011b). In this research, as mentioned in chapter 1 this area is beyond the scope and the research assumes that authorisation for investigation has been given.

As shown in Table 2 of chapter 2 where the phases refined from the existing investigation model were assigned an ID to identify the layers that will form the phases of the new model as shown below:

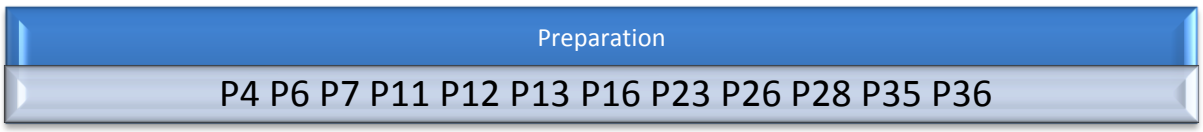


Figure 23: The Layer contains digital forensic investigation process of the preparation phase of the new model

The objective of the Layer shown above is to identify the different digital forensic investigative processes collected to make up the preparation phase. The activities shown in figure 23 making reference to the collated phases in Table 2 are discussed as follows:

- **Approach Strategy (P4)**

  This activity is introduce in order to maximize the acquisition of pure evidence and at the same time to minimize any negative impact to the victim and surrounding people (Reith et al., 2002)

- **Authorization (P6)**

  Ciardhuain, (2004) proposed authorization as where once the need for an investigation is identified; the next activity is to obtain authorization to carry it out. Authorization is interaction with both external and internal entities to obtain necessary authority. Depending on the type of investigation, in one extreme an IT security department or system administrator may require only a simple verbal approval from organization's management to carry out an investigation of the organization's computer system. At another extreme, law enforcement agencies require formal legal authorization, setting out in precise detail what is permitted in an investigation.

- **Awareness**

  This activity is the creation of awareness that investigation is needed, which is usually the first step in an investigation (Ciardhuain, 2004).

- **Communication Shielding (P11)**

  Agarwal (2011) proposed communication shielding. In this activity, all possible communication options or capabilities of the devices should be disabled. There is need for all unused port to be disabled. In a situation where the device appears to be in off state, some communication features like Wireless or Bluetooth may be enabled, resulting in overwriting the existing information. In other situations where the device is in the cradle

connected to a computer, synchronization mechanisms using ActiveSync might be enabled leading to corruption of evidence.

- **Deployment (P12)**

  This provides a mechanism to detect and confirm an incident or event (Carrier and Spafford, 2004).

- **Detection (P13)**

  This activity assists in detecting an incident (Pilli, et al., 2010)

- **Documentation (P16)**

  This phase involves proper documentation of the crime scene. Documentation is a continuous back and forth activity required in all the stages of the investigation and required for maintaining proper chain of custody.

- **Incident Response (P23)**

  Beebe and Clark (2004) explained that the incident response phase consists of the detection and initial pre-investigation response to a suspected computer crime related incident. For example, breach of computer security, using computer to view child pornography. The incident response activity detects, validate, assess and determine a response strategy for the suspected security incident.

- **Notification (P26)**

  According to Ciardhuain (2004) notification is an activity that informs the subject of an investigation or other concerned parties that the investigation is taking place. In some investigations where surprise is needed to prevent destruction of evidence, this activity may not be appropriate.

- **Planning (P28)**

  Planning is important in any investigation case that involve digital devices, what the systems are used for and if it is a network environment or not (Rodger et al., 2006). If the digital equipment is used for business purposes this will influence the planning and preparation process. At the preparation stage proper planning needs to be done for tools and storage capacities that will be used. The alert in a breach of security policy can show the importance of security measures in place in any organisation.

- **Readiness (P35)**

  Carrier and Spafford (2003) integrated digital investigation process started with readiness phase, which requires the physical and operational infrastructure to be ready to support any future investigation. In this phase, the equipment must be ever ready and the personnel must be capable to using it effectively. This activity is best identified in the preparation phase.

- **Survey and Recognition (P36)**

  This activity is recognising the need for an investigation (Agawal et al., 2011)

4.3.2.2 Interaction Phase

This is a major phase introduced in this research. Interaction is the distribution and maintaining of information during and after the investigation (Ademu et al., 2011b). The collection, transportation and maintaining the integrity of information is a major key aspect of supporting the work of investigators and it can be a fruitful area for the development of advanced applications involving techniques such as data mining and expert system (Harrison and Aucsmith, 2002). Interested logs, networks and computers involved in the incident or which hold investigative information are gathered.

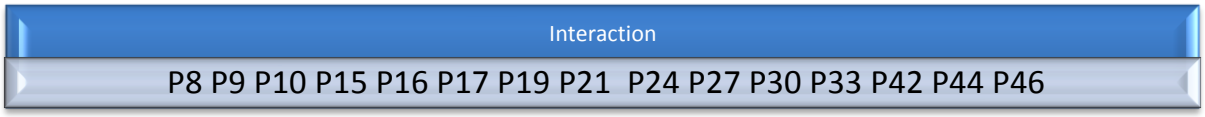


Figure 24: The digital forensic investigation process of the Interaction phase of the new model

The objective of the Layer shown above is to identify the different digital forensic investigative process that is collected to make up the Interaction phase. The activities shown in figure 24 are discussed as follows:

- **Case Specific Analysis (P8)**

  This enables the investigator to adjust the focus of the examination to the specifics of the case (Rodger et al., 2006). For instance, the focus of the case can be on email content investigation, child pornography, identity theft cases etc.

- **Chronology Timeline Analysis (P9)**

  This is building the crime case from chronological perspective to sequence the probable crime activities (Rodger et al., 2006). For instance using the computer time to identify the sequential order of crime activity

- **Collection (P10)**

  This is where digital investigator collects relevant data based on the approved methods utilizing various recovery techniques (Pilli et al., 2010).

- **Dissemination of Information (P15)**

  Some information may be made available only within the investigating organisation, while other information may be more widely distributed, this can be determined by the policies and procedures in place (Ciardhuain, 2004). This can assist good chain of custody. The

information will influence future investigations and may also influence the policies and procedures.

- **Documentation (P16)**

  Documentation is important at all the stages of handling and processing digital evidence (Agawal et al., 2011) Documenting every process of digital evidence handling is required to maintain the chain of custody. In the investigation every stage in the investigation was documented.

- **Dynamite (P17)**

  In this phase, digital investigator conducts investigations at the primary crime scene with the purpose of identifying the potential offender (Baryamueeba and Tushaba, 2004).

- **Examination**

  This activity involves identification and location of the potential evidence from the data collected (Reith et al., 2002).

- **Identification (P21)**

  This involves activity to identify the digital component from the acquired evidence and converting it to the format understood by human (Perumal, 2009)

- **Internet (P24)**

  In this phase, the activity of examining the artefacts of internet related services are performed (Rodger et al., 2006).

- **Physical Crime Investigation (P27)**

  This is where physical evidence is collected and analysed (Carrier and Spafford, 2003).

- **Pre-Analysis (P30)**

  This contains all the steps and activities that are performed before the actual analysis starts.

- **Preservation (P33)**

  After all potential evidence has been seized and is available to the digital investigator, duplicate copies of all data are made to ensure integrity of the original evidence (Pilli, et al., 2010)

- **Search and Identify (P42)**

  This activity deals with locating the evidence and identifying what it is for the next activity.

- **Transport and Storage (P44)**

  Data must be securely transported and properly stored (Perumal, 2009)

- **User Usage Profile (P46)**

  This focuses its attention to analyse user activity and profile with the objective of retaining evidence to suspect.

4.3.2.3 Reconstruction Phase

This phase involves bringing together the result of relevant information/activities from the earlier parts of the process and any other relevant information which investigators may have obtained to provide a detailed account of the events and actions at the crime scene (Ademu et al, 2011b). These activities are reviewed, and deleted hidden and protected data are retrieved. Investigator also ensures that data are not lost. In addition, the relationship between these activities and the offenders aim is ascertained in this phase.

Figure 25: The digital forensic investigation process of the Reconstruction phase of the new model

The objective of the Layer shown in figure 25 is to identify the different digital forensic investigative process that is collected to make up the Reconstruction phase. The activities shown above are discussed as follows:

- **Acquisition (P1)**

  In dealing with digital forensic investigation so that the results will be scientifically reliable and legally acceptable one phase of the computer forensic investigative process is known as Acquisition (Pollitt, 2007). In acquisition phase, evidence is acquired in acceptable manner with proper approval from authority.

- **Analysis (P3)**

  The process of determining the importance of evidence and drawing conclusion based on the evidence found is done in this phase (Perumal, 2009).

- **Archive Storage (P5)**

  This is where relevant evidence is properly stored for future references (Perumal, 2009)

- **Digital Crime Investigation (P14)**

  This focuses on collecting and analysing digital evidence in digital environment (Carrier and Spafford, 2003)

- **Documentation (P16)**

  As per discussed in previous phases, this stage involves proper documentation of the crime scene to assist in maintaining good chain of custody.

- **Evaluation (P18)**

  This involves task where the digital component identified is relevant to the case being investigated and can be considered as a legitimate evidence.

- **Hypothesis Creation (P20)**

  In hypothesis creation, based on the examination of the evidence the investigator must construct a hypothesis of what occurred (Ciardhuain, 2004). The creation of this hypothesis depends on the type of investigation. For example, an internal investigation by a company's systems administrator will result in a less formal report to management while a police investigation will result in the preparation of a detailed hypothesis with carefully documented supporting material from the examination suitable for use in court.

- **Investigation (P25)**

  During the investigation of the digital attack, different types of evidence relevant to the attack are gathered (Phlli et al., 2010). For instance, host or network based evidence are collected in order to reconstruct the events that comprise the digital crime committed. This reconstruction should provide explanations.

- **Reconnaissance (P37)**

  This phase involves conducting the investigation while the devices are still running; it is similar to performing live forensics (Perumal, 2009).

- **Result (P39)**

  This is the findings of the investigation. The findings or results are properly documented (Agawal et al., 2011).

- **Traceback (P43)**

  This is tracking down the source crime scene, including the devices and location (Baryamueeba and Tushaba, 2004)

- **Triage (P45)**

  This is a phase where evidence are identified and ranked in terms of importance or priority (Rodger et al., 2006). This process ensures that evidence with the most important and volatile need will be processed first.

4.3.2.4 Presentation Phase

In this phase analysed data are presented. Presentation is when the digital investigator or examiner shares results of the analysis with interested professionals (Ademu et al., 2011b). This involves generating a report of actions taken by the digital investigator, uncovered evidence and the meaning of the evidence.

Figure 26: The Layer contains digital forensic investigation process of the Presentation phase of the new model

The objective of the Layer shown in figure 26 is to identify the different digital forensic investigative processes that are collected to make up the presentation phase. The activities shown above are discussed as follows:

- **Admission (P2)**

  This activity involves presentation of the acquired and extracted evidence (Pollitt, 2007).

- **Incident Closure (P22)**

  The activities in this phase involves, to conduct a review of the entire process and investigation, makes and act upon decisions that result from the final findings, dispose the evidence and collect and preserve all information related to the incident (Beebe and Clark, 2004).

- **Post-Analysis (P29)**

  The first stage of post analysis phase is concerned with documentation of the whole activities during the investigation in a written report (Freiling and Schwittany, 2007). In this phase, all activities regarding the collection and analysis of digital evidence have ended, and the objectives set by the response strategy for the analysis phase have been fulfilled.

- **Proof/Defence (P34)**

  This activity enables the investigator to prove the validity of the hypothesis and defends it against any criticism and challenge (Reith et al., 2002).

- **Report (P38)**

  After the investigation of digital crime is finished, all the findings and results have to be documented in a written report. In the report, all investigative activities have to be written and conclusions drawn have to be explained.

- **Returning Evidence (P40)**

  This is to ensure that evidence are safely returned to the rightful owner or properly disposed.

- **Review (P41)**

  This activity involves reviewing the whole investigation processes to identify areas of improvement that may result in new procedures (Carrier and Spafford, 2003).

4.3.3 The Security Layers of the new Comprehensive Digital Forensic Investigation Model

As systems and network play an increasingly important role in businesses and for digital investigation, so have been the dangers of malicious software. In addition, as the computing industry has grown larger, the market has become dominated by a few

leading brands. A malicious program that exploits bugs or vulnerabilities in some market leaders is a threat to thousands of organisations (Champlain, 2003). Since digital investigators are using digital devices such as computers and networks there is need for investigators to understand the dangers of malicious code or the practices that carry a risk of digital evidence being contaminated and leading to unacceptability in the court or during internal hearings. Infection of a workstation by malicious code can usually be traced back to some instances of careless or risky behaviour, for instance a floppy disk or other storage device infected with a virus can infect an investigation workstation. Once the workstation such as system or network is infected, the virus can spread either by itself or with human assistance to other workstation in the network. If a computer is infected with a worm for example, it may automatically send infected mail attachment to all of the addresses in the address book. Malicious code is an increasing problem because the increasing complexity of programs has made more susceptible to attack. In addition, a few program suites dominate the market, so viruses can spread very quickly. Malicious code can enter the local network through a single workstation, but most attacks come through a network gateway. There are many different types of malicious code, including variety of vulnerability some of which have been discussed in chapter 2. The network can come under attack in different ways, but one common way is importation of executable code into the network. Digital devices connected to the internet are also vulnerable to attack through their internet connections.

One of the most important elements of information security is protecting the computer network and users from malicious code. The internet is infested with viruses and worms that can do a lot of damage to the computers and most importantly to the data, they store. Increasingly is the continuous experience of cybercrime threats. The growth of threats indicates that more types of threats will be faced in the near future. Also, there will be continuous need for countermeasures of security to control them. The nature of

these countermeasures might be technological, operational, personnel etc. Based on the review of academic and industrial literature, a model that integrates security measures in digital investigation process was not found. In this aspect of the research important security measures required for digital forensic investigation as observed from chapter 2 are discussed.

In this research, the security layer will identify the threats related to a digital forensic investigation process which can influence the integrity of digital information. The application and content based technology for example will address technological threats and the operational procedures will address the threats on digital forensic investigation process related to the human aspect. The aim of the research in this thesis is to explore the use of modern technologies and establish security threats in digital forensic investigation process in an attempt to present solution that contributes to a good security level and as a measure for integrity of digital evidence. There are four areas that this research argues that it contributes in building strong security mechanism. It can be observed that each area is a broad concept of the information secuirty field and can be broken to smaller sub layers which collectively contribute to the positive effect of the security plan or guidelines of digital forensics or any organisation. The security requirement/guidelines were considered in all the phases of the new model. The following are the important security requirement/guidelines needed for digital forensic investigation process as observed from the literatures reviewed in chapter two:

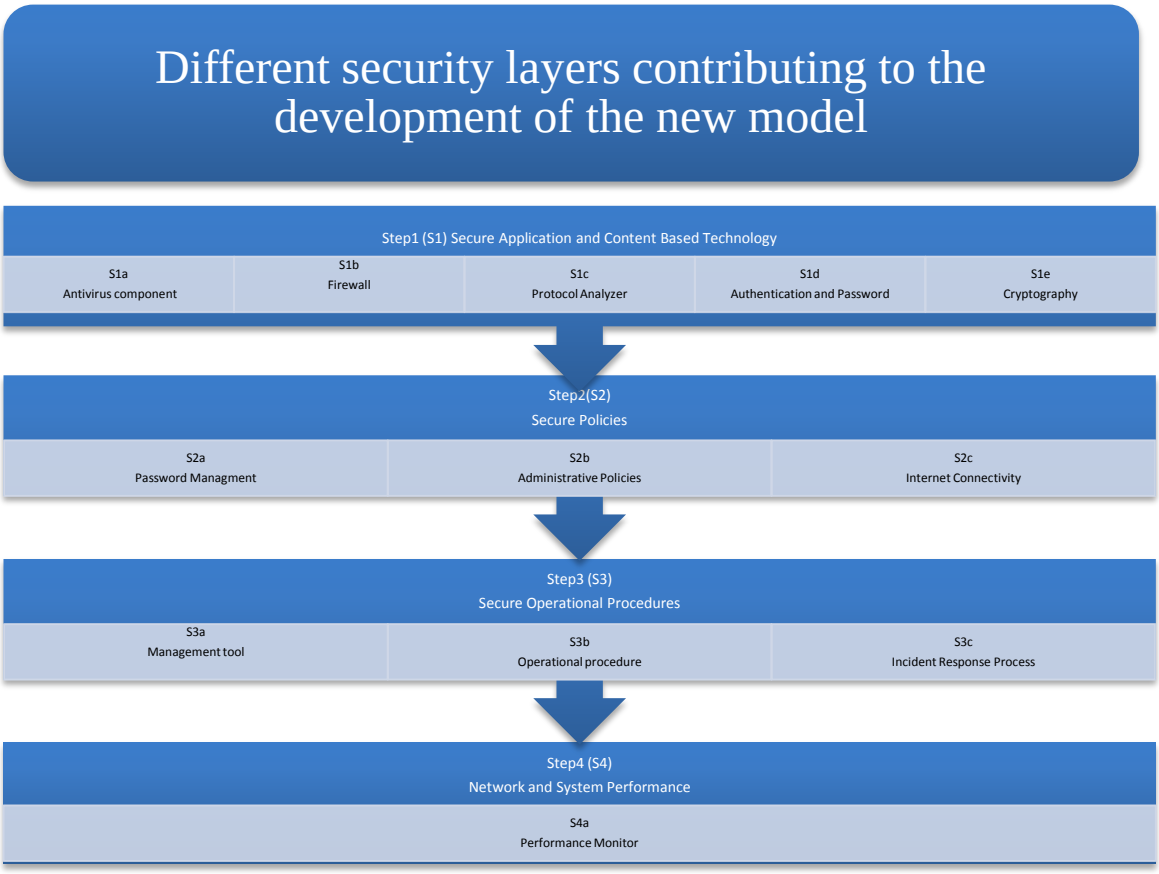


Figure 27: The security layer contributing to the development of the new model

4.3.3.1 Step1: Secure Application and Content Based Technology

Security technologies have important role in securing the systems and applications supporting the major aspect of digital forensic investigation processes. Technologies such as Antivirus, Firewalls, Cryptography, Security and Network Protocol (Anderson, 2001) contribute to the success of the digital forensic investigation process by providing those involve in digital investigation high trust for the digital evidence collected. In the case of not having all, some or any of the security measures will have a negative impact and can be considered a threat on the digital evidence (Ademu and Imafidon, 2012f). It is important all attachment for example email attachment be scanned before being opened. Attachment may contain code that will infect other files; care must be taken in working on attachment and executable files.

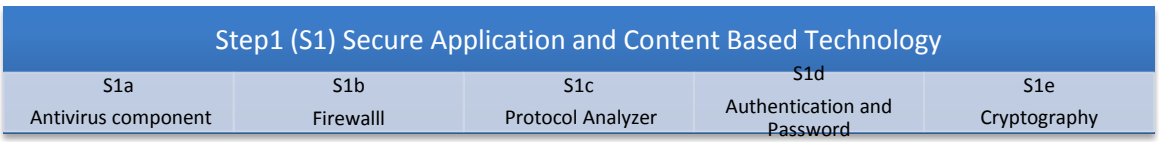


Figure 28: The layer of application and content based security requirement

A brief description is provided on the need of these technologies. The categorization of the technologies was derived from the literature reviewed for this layer. The main sub layers as shown in figure 28 found out of the review process are:

- **Step1a (S1a): Antivirus**

  Virus and worms can be used to infect a system and modify a system to allow an attacker to gain access, many viruses and worms carry Trojans and backdoors through this a virus or worm is a carrier and allows malicious code such as Trojans and backdoors to be transferred from one system to another and in turn affects the integrity of the data (Graves, 2010).

  Anti viruses are tools, which perform a health check of the technical body of the organisation and prevent viruses from being transferred through many channels that can cause harm to the organisation. Having antivirus systems distributed in the organisation will reduce the risk of huge damage or loss to digital information Ademu and Imafidon, 2012g).

- **Step1b (S1b) Firewall**

  A firewall also known as packet filter, is designed to prevent malicious packets from entering or leaving the computer (Dulaney, 2009). A firewall can be software or hardware. A personal software firewall runs as a program on a local system to protect it against attack. For instance, many operating systems now come with personal software firewalls or they can be installed as separate programs.

- **Step1c (S1c) Protocol Analyzer**

  Network protocols provide addressing and routing information, error checking, retransmission request and rules for communicating in the networking environment (Tomsho et al., 2007). The new version of IP is called the IPv6. The Internet Protocol version 6 (IPv6) is the network community's solution to resolving some of the issues in IPv4 such as lack of built-in security. IPv6 integrates the IP Security (IPSec) protocol that must be added to an existing IPv4 network (Tomsho et al., 2007). IPSec provides authentication and encryption in which authentication ensures that the sender and receiver of data packets are known to each other and have permission to send and receive data, while encryption makes the underlying data in packets unreadable except to the computers involved in the transmission.

  According to Ciampa (2009) protocol, analyzer can fully decode application-layer network protocols, such as Hypertext Transfer Protocol (HTTP) or file transfer protocol (FTP). When using protocol analyser technology, network intrusion detection system or network intrusion prevention system could detect any unusual activities that may be malicious.

- **Step1d (S1d) Authentication and Password**

  Authentication is the process of verifying that the sender is who they say they are (Dulaney, 2009). One of the methods of establishing authenticity is using secret words that have been agreed on in advance such as password.

- **Step1e (S1e) Cryptography**

  According to Dulaney (2009) cryptography is the art of concealing information. Cryptographic is a system, method, or process that is used to provide encryption and decryption. One major reason for implementing a cryptographic system in this research is that it provides data integrity, which is assurance that a message

was not modified during transmission. Modification can render digital evidence inaccurate.

4.3.3.2 Step2: Secure Policies

A secure policy determines what controls are required to implement and maintain the security of systems, users and networks (Ademu and Imafidon, 2012f). This policy can be used as a guide in system implementations and evaluations. As shown in figure 29 are the sub layers:

Figure 29: The layer of secure policies security requirement

- **Step2a (S2a) Password Management**

  A lot of attacking attempts are made with identifying a password to a target system. Passwords are the key piece of information needed to access a system and users often select passwords that are easy to guess. Many reuse passwords or select a simple one to help them remember it; because of this human factor, most passwords are easy to guess (Graves, 2010). Once a password is guessed or cracked, it can be a security threat such as escalating privileges, executing applications, hiding files etc. It is important for digital investigators to manage password securely.

- **Step2b (S2b) Administrative Policies**

  It is common for security flaws to be identified in software that has been released for sale to the public. Some of these flaws can leave the system open to attacks by malicious code (Champlain, 2003). Software vendors offer free patches to eliminate known flaws. Patches can also be installed against TCP SYN to avoid denial of service attack. Digital Investigators should ensure that

all relevant software is updated with patches as soon as they are made available. Occasionally, a number of patches may be issued together as a service pack.

- **Step2c (S2c) Internet Connectivity**

  The best solution for many of the vulnerabilities that exist on the internet is to implement secure internet connection. There are two common methods that provide secure connections between an internet client and server. Firstly, Secure Sockets Layer (SSL) and Transport Layer Security (TLS), the SSL protocol uses an encryption scheme between the two systems. TSL is a newer protocol that merges SSL with other protocols to provide encryption (Dulaney, 2009). Secondly, Hyper Text Transfer Protocol Secure (HTTP/S) is a protocol used for secure connections between two systems that use the internet, it protects the connection and all traffic between the two systems is encrypted. HTTP/S uses SSL or TLS for connection security.

4.3.3.3 Step3: Secure Operational Procedure

A good security guideline will have incident response process, security operational procedures (Ademu and Imafidon, 2012f).

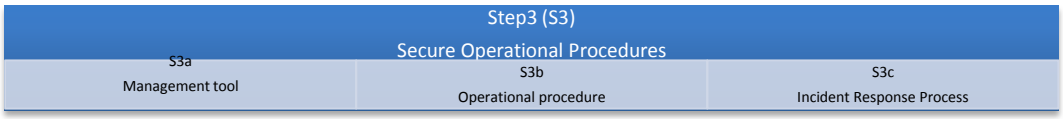


Figure 30: The layer of secure operational procedures security requirement

- **Step3a (S3a) Management Tool**

  There is need for investigators to be able to mange investigative tools properly and in a secured manner (Ademu and Imafidon, 2012g).

- **Step3b (S3b) Operational Procedure**

  There should be secure operational procedures in place. Operational procedures need to address authorisation, access and methods used to monitor organizational computer systems and applications. Due to the need of exchanging files and digital information between the investigators, the lack of having proper security plan/guidelines will increase the probability of having the digital information infected with viruses due to unsecure file exchange over the internet (Dulaney, 2009). The use of unsecured Windows shared folders should be avoided. Some worms for example can spread across the network through such unsecured shares, infecting all hosts that have unsecured shared folders.

- **Step3c (S3c) Incident Response Process**

  Incident response process is the process on how the digital investigator will respond to an incident such as an attempt to violate a security policy, any unauthorized access to information, a compromised system etc. Initial investigation must be carried out to eliminate any further damage.

4.3.3.4 Step4: Network and System Performance

The following sub layers as shown in figure 31 are:

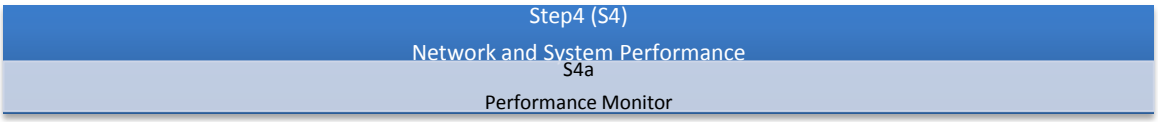


Figure 31: The layer of performance security requirement

- **Step4a (S4a) Network and System Performance**

  It is important to monitor networks and systems performance to ensure that the devices are operating normally (Tomsho et al., 2007). Some tools for monitoring system's performance are Event Viewer, Task Manager, Performance Monitor and Network Monitor. Performance monitor keeps track of activities by

monitoring performance on a server or system; this can assist in identifying any case of abnormality.

Table 7: The security measures and guidelines of the new model (Ademu and Imafidon, 2012f)

Steps	Measures	Threats
Secure Application and content-based technology Step 1 (S1)	Antivirus component	Viruses
	Personal Firewalls	Gaining access to information
	Protocol analyzer	Denial of Service
	Authentication and password	Impersonating
	Cryptography	Altered integrity
Secure Policies Step 2 (S2)	Password management	Impersonating
	Administrative policies	Loss of data
	Internet connectivity	Denial of service
Secure Operational procedure Step 3 (S3)	Management tool	Gaining access to information
	Operational procedures	Loss of data
	Incident response process	Denial of service
Network and System Performance Step 4 (S4)	Performance monitor	Denial of service
		Loss of data packet

Table 7 shows the security requirement and mechanism as security measures and guidelines incorporated with the investigation process in the new model.

4.4 The new Comprehensive Digital Forensic Investigation Model Incorporating the Security Mechanism

As seen in table 7 showing steps in the security guidelines with its measures and possible threats, each step will diminish group of threats related to a digital investigation process. A literature review and extensive research were conducted in order to prove the need of the measures discussed in this chapter.

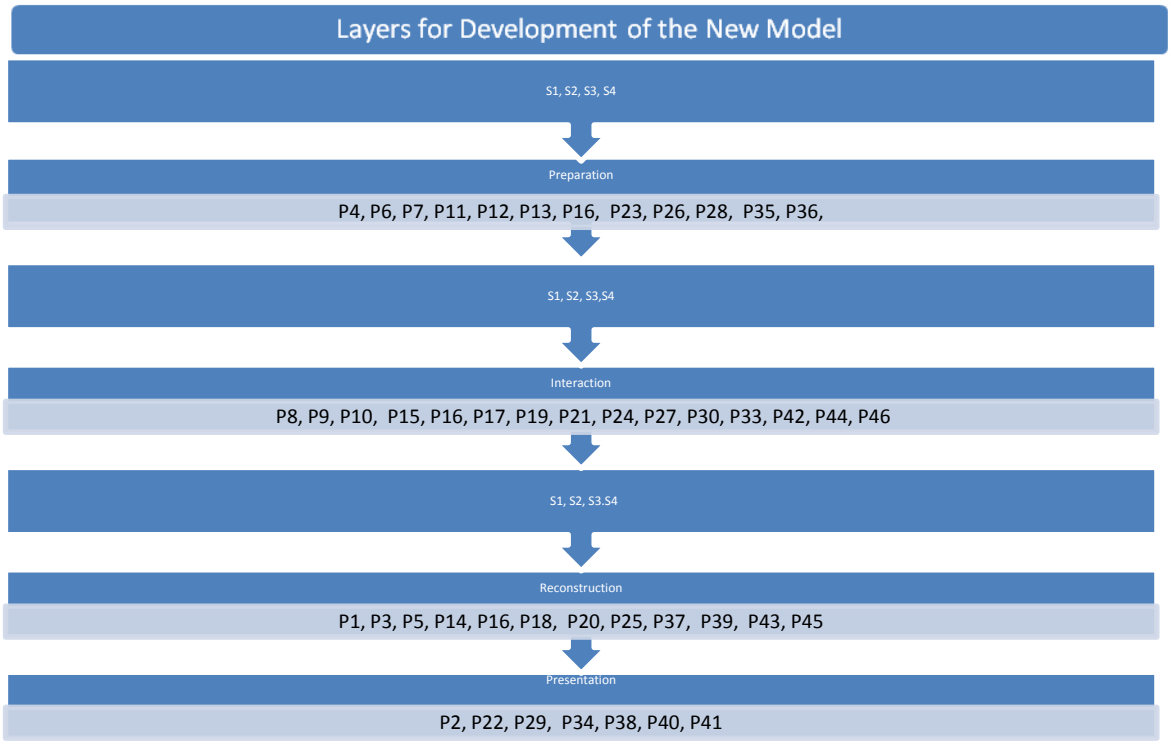


Figure 32: The layers of digital forensic investigation process integrating security measures for development of new model (Ademu and Imafidon, 2012f)

The idea of the model is to come up with a solution that contributes to the security level of digital investigation process by integrating security mechanism that assist reviewing the security needs and requirements for any digital investigation process. For simple visual representation, the model is represented in a matrix view as illustrated below:

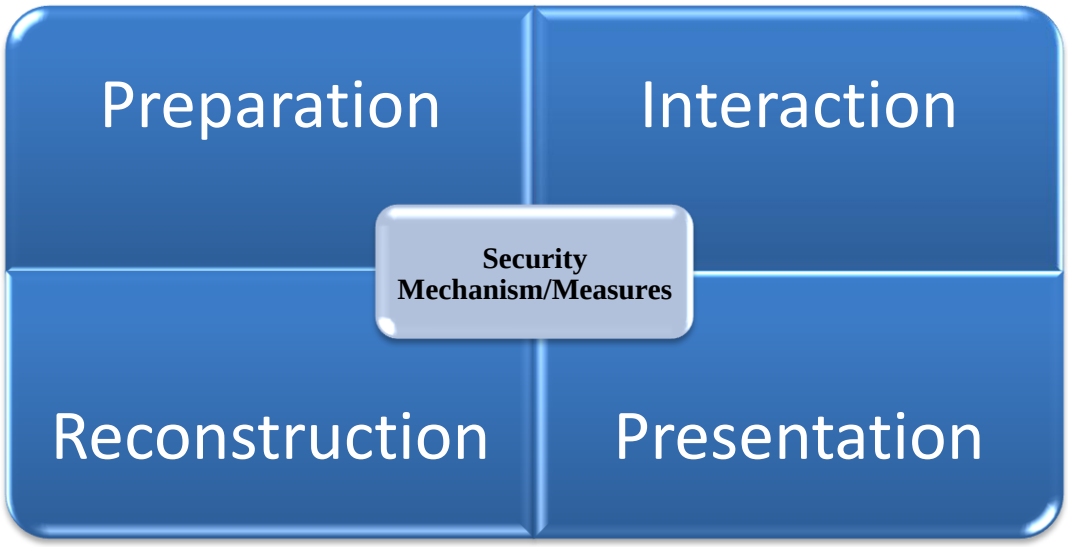


Figure 33: The Comprehensive Digital Forensic Investigation Model (Ademu and Imafidon, 2012f)

4.5 Summary

This chapter presents the concern of security threats in digital forensic investigation process, the need of having a model addressing these threats and an application of this concept. This security threat concerns is considered as the foundation of the need of a new comprehensive digital forensic model. The chapter discussed the systematic approach for the development of the new model.

Chapter Five: Experiments

Objectives:

- to test the hypothesis
- to conduct experiments
- to discuss the result of experiments

This chapter aims at testing the hypothesis by conducting experiments, which will either support or refute the hypothesis. It also evaluates the results of the experiment. Digital devices are becoming more technologically advanced and specifically the area of mobile network require support for IP mobility in order to maintain its connectivity with its peers while they move across networks and to minimize their service disruption.

In this section of the research, the CDFIM is applied to two different areas of digital investigation. The area of mobile networking and email content. It has been recognised in the research that loss of data/packets can be a threat to the integrity of digital evidence. Therefore, the recent localized mobility protocol known as PMIPv6 is explored. In this section, in order to minimize handover latency and provide reliable service buffering function is implemented to minimize packet loss during mobile node handover. Furthermore, an experiment is conducted in a real testbed environment to compare and analyze standard PMIPv6, the buffering scheme and the improved buffering scheme applied to PMIPv6. In addition, an experiment on digital investigation is conducted using Comprehensive Digital Forensic Investigation Model (CDFIM) with FTK in investigating email content.

5.1 Hypothesis

This research proposes that the integration of security mechanism and intelligent software in digital forensic investigative process can serve as a measurement tool for the integrity of digital evidence.

5.2 Data Integrity

Data integrity ensures providing guarantee that data was not altered in storage or during transmission. Data integrity can be achieved by adding information such as checksums that can be used as part of the decryption process and using cryptographic approach. Another way of establishing data integrity identified in this research is the use of PMIPv6 with buffering function.

5.3 Experiment 1

Ruibin et al., (2005) explains that obtaining or simulating real case data for a stand-alone system is not difficult but fetching data from network of a large organisation or a large volume of legal cases is very complex and not applicable in many situations. Law enforcement agencies have the best-maintained document systems but for reasons of security and privacy protection, these documents are not usually accessible to researchers. Researchers in Intrusion Detection areas are also face with the issue of protecting the sensitive data, but they have already worked out some standard datasets and test beds and are still working to improve this. In order to support research and implementation, in both digital forensic and computer intelligence, the authors suggests adopting the method from information technology to build and publish a standard datasets for digital forensic where raw data from selected cases are reorganised and filtered, adding some manually created events if the need arise in order to carefully examine, locate and categorise events and private and sensitive information removed.

5.3.1 Experiment Design

This section covers a possibility of digital attack investigation. The possibility of data/packets loss during handover in a mobile node, which is an attack that can influence the integrity of digital information (evidence). An experiment was designed to conduct a digital investigation into integrating security mechanism and intelligent software in digital forensic investigation process in order to preserve the integrity of digital evidence.

5.3.1.1 Type of Attack

This experiment considers packet loss during handover, resulting in lost packets with longer handover latency. MN handovers delay can lead to more packets lost. This is common attack during handover, resulting to lack of integrity on digital information.

5.3.1.2 Collection of Data

The Wireshark is used to collect packets. The libipq library is provided as part of the IP6Table and it is used to store the packets for the investigation. The aim of carrying out this investigation is to establish how preventing packet loss can assist the integrity of Digital evidence.

5.3.1.3 Method of Investigation

The investigation is conducted based on the Comprehensive Digital Forensic Investigation Model (CDFIM). The objective of this is to test the hypothesis and to present the applicability of CDFIM.

5.3.2 Experiment Component

This section discusses the network infrastructure, software and tools used in the experiment. This experiment is designed in order to minimize MN handover latency, and provide reliable service, fast handover schemes have been proposed and implemented. These schemes apply buffering function to prevent packet loss during MN handover. The integrity of digital evidence can be preserved by implementing security mechanism and intelligent software to prevent data loss. Thus, the research hypothesis will be tested. Table 8 summaries the component of the experiment's infrastructure.

Table 8: Component of the Experiment's infrastructure

Infrastructure	**Description**
Linux-Ubuntu 10.04	Operating system
OAIPMIPv6 version 0.3.1	OpenAirInterface
C	Language
Wireshark 1.10.3	Network Protocol analyzer

Table 9: Component of Buffering Function Implementation

No.	**Infrastructure**
1	Netfilter Framework
2	Libipq
3	Hash and List Library
4	IP6 Tables Utility

5.3.3 Implementation of Buffering

This section presents the implementation of buffering function to minimize packet loss, basic buffering operation, buffering function design, and implementation is explained then proposed an improved buffering function. Table 9 shows the component of implementing the buffering function.

5.3.3.1 Fundamental Buffering Operating Principles

During MN handover, handover latency is caused by the connection in a wireless setting, the authentication procedure with an authentication, authorization, and accounting (AAA) server, and binding update in Mobile Access Gateway (MAG) and Local Mobility Anchor (LMA). It is impossible to prevent packet loss during MN handover in standard PMIPv6 (Rasem, 2011). Therefore, a buffering function is necessary to prevent packet loss during MN handover. There is also a problem when applying route optimization without a buffering function. The out-of- sequence problem occur, in which packets arrive out of order because of the gap of transmitting time through existing and optimized paths (Filipe and Santos, 2011). This problem increases network load and service delay or setback with packet retransmission in TCP. It also provides unreliable services because of out-of-sequence data in User Datagram Protocol (UDP). In PMIPv6, the buffering function must be implemented to provide reliable mobility to MNs.

In order to perform buffering in PMIPv6, either MAG or LMA should support a buffering function (Egli, 2013). If the buffering is performed in the MAG, the previous MAG (pMAG) should perform buffering during the MN handover. When the MN attaches to a new MAG (nMAG), pMAG should forward all the packets stored in the buffer to the nMAG so that it can prevent packet loss. If the LMA performs buffering, it

stores packets in the buffer during the MN's handover and forwards all the buffered packets to the nMAG after the handover. Most of the schemes, which use the buffering function, provide reliable services with these procedures.

In this research, a PMIPv6 buffering function is implemented based on the open -source OpenAirInterface (OAI) PMIPv6. OAI PMIPv6 has recently been developed most actively out of the PMIPv6 open - source codes. Before implementation of the buffering function, a test bed was established using OAI PMIPv6. OAI PMIPv6 version 0.3.1 was used and referred to the method of establishment provided by OAI. The operating system is Ubuntu 10.04, and C language is used. To implement the buffering function, Netfilter framework, Libipq, Hash &List library, and the IP6Tables utility were used. The implemented buffering function can be applied to LMA and/or MAG. An experimental environment was established in which LMA performs buffering.

5.3.3.2 Function Design

In the testbed in this research at LMA, the NF_IP_PRE_ROUTING hook point is provided a hook handler from IP6Tables in the user space to buffer the packets. To provide a hook handler to the NF_IP_PRE_ROUTING hook point of Netfilter in the kernel space, IP6Tables adds a rule that includes the IP information of the roaming MN. The Libipq library is used to store the packets, which is provided as part of IP6Tables. This library provides an Application Programming Interface (API) set that can assist in communicating with the IP6_Queue module in the kernel space, so that it can push and pop packets from the queue during buffering and forwarding, respectively.

5.3.3.3 Packet Buffering Module

In this research a new module, Packet Buffering, is added to the existing OAI PMIPv6 in Figure 34. The Netfilter framework and IPTables tool are used to hook and buffer the packets. The Libipq library is included in the IPTables tool, so that the Netfilter can

push the hooked packets to the queue in the Packet Buffering module. A NETLINK socket is used for transferring information between the Netfilter in the kernel space and IPTables tool in the user space. Some few existing modules, such as the Handler, Finite State Machine, and Message modules, are also modified to add functions to evaluate whether or not forwarding and buffering occur. The Finite State Machine calls the buffering module by obtaining the event from the handler when an MN roams. The buffering module inserts the hook rule, as a hook handler for a hook point of Netfilter, into the IP6Tables using the IPTables tool, and controls the address information of the packets, which should be buffered. Then, the Netfilter refers to the data in IP6Tables and hooks the packets in the kernel space.

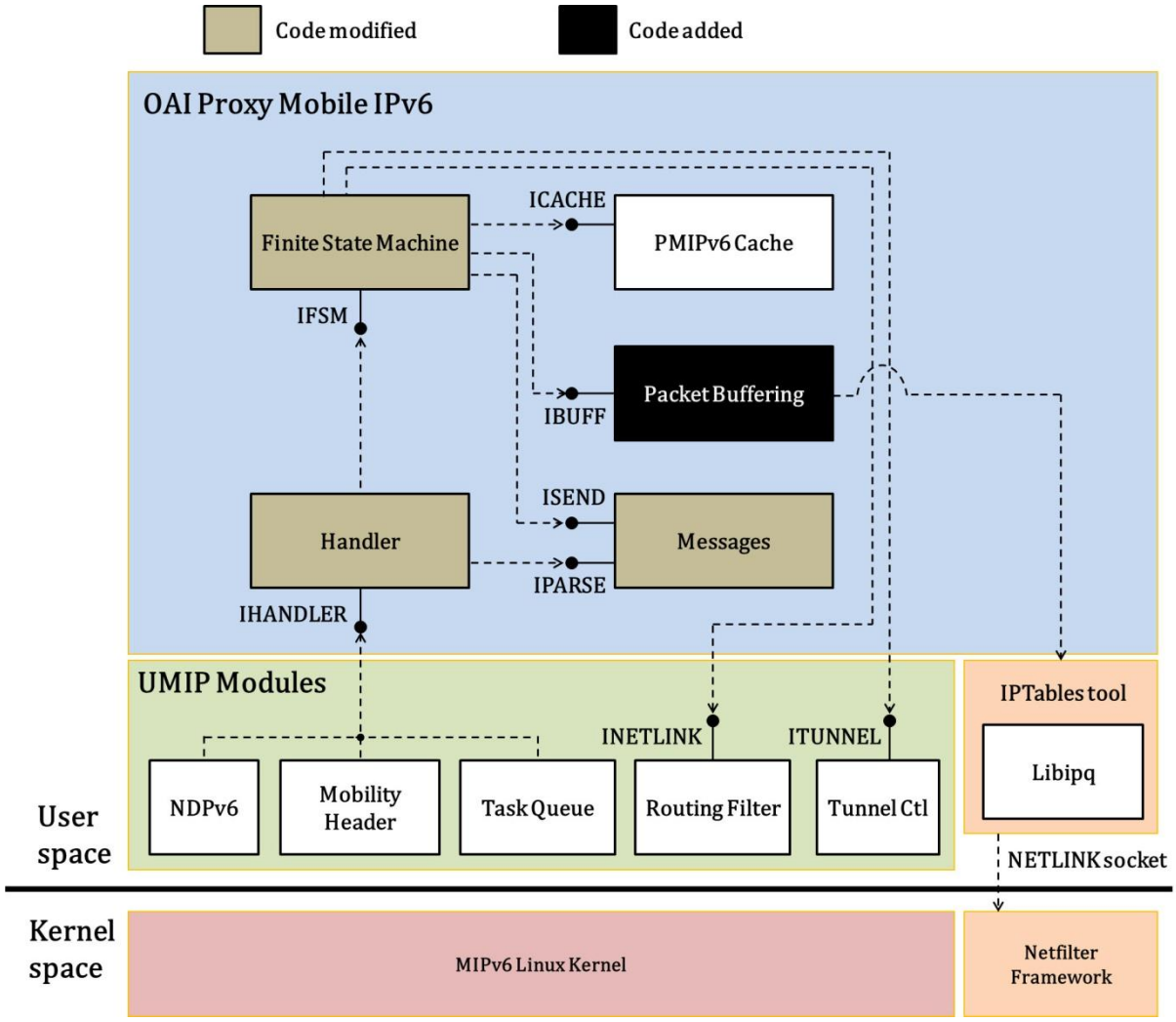


Figure 34: OAI PMIPv6 including buffering module

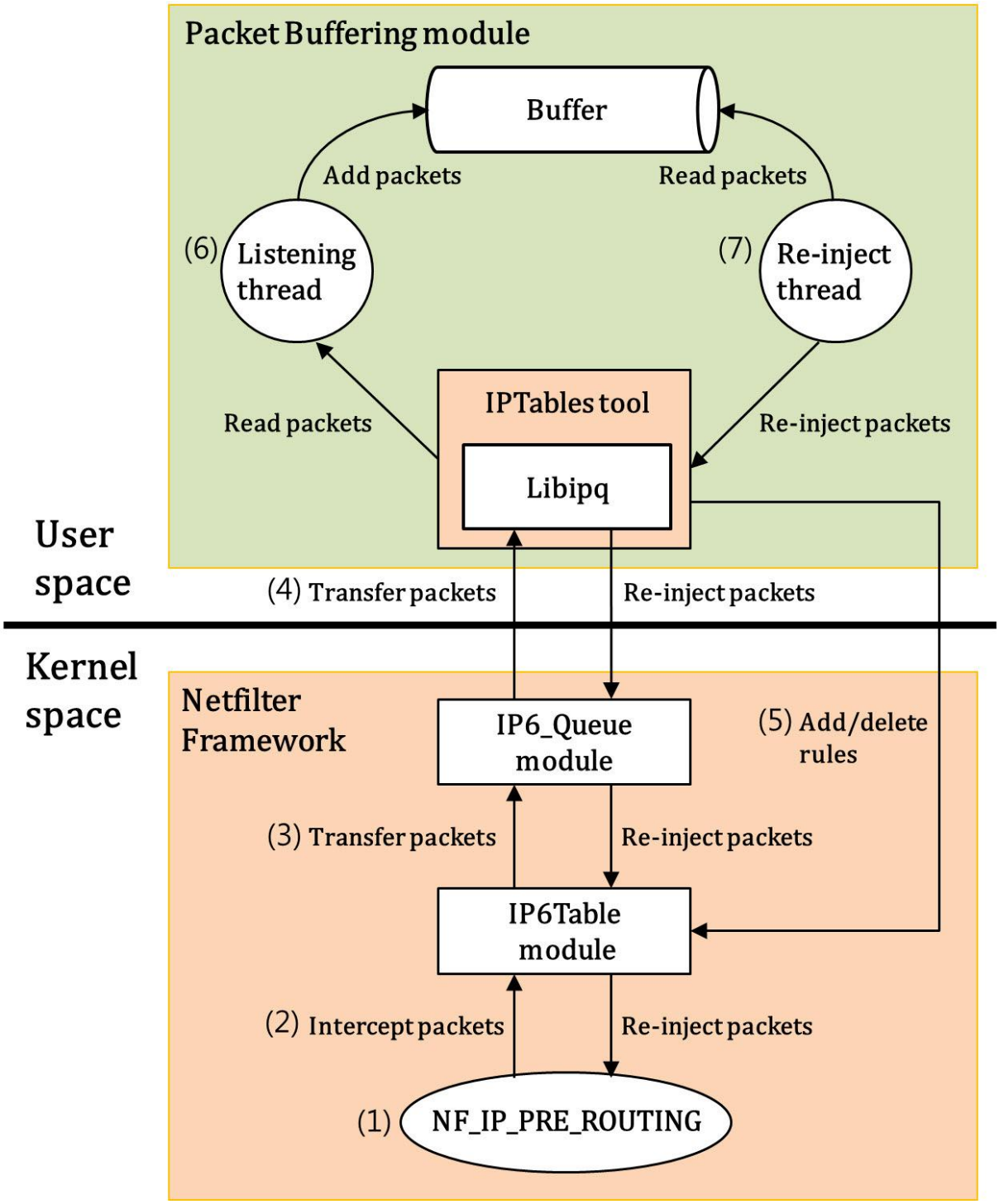


Figure 35: Operation of Packet Buffering Module

Figure 35 represents the Packet Buffering module, which is the heart of buffering implementation. The Packet Buffering module is classified into two parts:

- Kernel space,
- User space.

The part in the kernel space is responsible for hooking packets and passing them to the user space (Egli, 2013). The packets, which should be buffered, are hooked at the NF_IP_PRE_ROUTING hook point in the Netfilter (line1). The IP6Table module controlled by the IPTables tool in the user space contains the handler for the hook point. The hooked packets are passed to the user space through the IP6_Queue module (line2 - line4). The other part in the user space stores the packets received from the kernel space to the buffer, and passes the buffered packets to the kernel space. The IPTables tool in the user space adds other rules to the IP6Table module to hook packets (line5). The Packet Buffering module stores the packets received from the kernel space in the buffer using the Libipq library. It pushes and pops the packets from the buffer by using a Listening thread and a Re-inject thread (line6 - line7).

If the LMA performs buffering, the start time of the buffering is the time when the LMA receives a De-Registration Proxy Binding Update (DeReg PBU) from pMAG after the MN's detachment (Egli, 2013). If the pMAG cannot communicate with the MN nor transmit packets to the MN for a certain time during an MN handover, the pMAG sends a DeReg PBU to LMA to notify that the MN has been detached. On receiving the message, the LMA identifies that the MN is undergoing handover and buffers all the packets for the MN. When the LMA receives the DeReg PBU, the Handler module detects it and sends the result of detection to the Finite State Machine module. The Finite State Machine module passes the message using the Message module, and then sends the MN's information by calling the Packet Buffering module. The Packet Buffering module calls the IPTables tool to include the MN's address information to the IP6Tables rule, and the Netfilter refers to the information to buffer the packets for the MN. After the MN attaches to the nMAG and the LMA receives the

PBU message, LMA sends the PBA message and all the buffered packets to the nMAG. In this way, the packet loss that can occur during the MN handover is prevented.

5.3.3.4 Buffering Function Implementation

The implemented buffering is operated in the LMA. Therefore, when pmip_lma_init() is executed for LMA initialization, it calls pmip_buffering_init() to initialize the buffering function. Figure 36 shows the main lines of the pmip_buffering_init() function. The function pmip_buffering_init(), that initializes the buffering function, creates a queue to store packets(line 1), defines the mode(line 4), and creates a thread that performs packet buffering(line 10). In this research in order to buffer the payload of the packets as well as the metadata, the mode was defined with IPQ_COPY_PACKET. The thread calls pkt_bufering_listener() to buffer the packets hooked in the kernel space and passed to the user space(line 10). After the initialization, if the Handler in the LMA receives the PBU message, pmip_lma_recv_pbu(), that is existing in OAI PMIPv6 , is called. The function, pmip_lma_recv_pbu(), calls the lma_fsm() function, that is the Finite State Machine of LMA. Then, the Finite State Machine finds out whether or not the MN is attached, and calls pmip_buffering_start() to start buffering if the MN has detached, or calls pmip_buffering_reinject() to start forwarding if the MN has attached.

```
int pmip_buffering_init()
{
 1:    h = ipq_create_handle(0, PF_INET6);  // create a queue for the buffer
 2:    if (!h)
 3:            return -1;  // return error if the queue is not created
 4:    ret = ipq_set_mode(h, IPQ_COPY_PACKET, BUFSIZE);  // set up the size of the queue and storage method
 5:    if (ret < 0)
 6:            return -1;  // return error if the set up has failed
 7:    if (pthread_rwlock_init(&buffer_lock, NULL))  // inialization to lock read/wirte function of buffer_rock
 8:            return -1;

 9:    buff_hash_init(&hash_pool);  // initialization of buffer hash
10:    pthread_create(&pb_listener, NULL, pkt_buffering_listener, NULL); // create the thread for storing packet
11:    return 0;
}
```

Figure 36: Main lines of pmip_buffering_init() function

If the Finite State Machine in the LMA receives a DeReg PBU from the pMAG, it checks the MN 's IP address in the message and prepares packet buffering for the MN . Figure 37 shows the main lines of the pmip_buffering_start() function. This function get ready to start packet buffering during the MN handover. It includes two parts, firstly, to include a rule that carries the MN 's address to the IP6Tables to hook the packets for the MN (line 8, line 11), secondly, to assign the memory to store the packets in the hash table (line 2 - line 7, line 10). The function, pkt_buffering_add_rule(), is made to include a rule adding the MN 's address to the IP6Tables. The Netfilter hooks packets for the MN by using this rule as a handler in the kernel space and passes the packets to the user space. The passed packets are buffered by the thread that the pkt_buffering_listener() function calls.

```
int pmip_buffering_start(struct in6_addr* mn_addr)
{
 1:    pthread_rwlock_wrlock(&buffer_lock);  // lock the thread for packet buffering

 2:    hash_item = (packet_hash_entry_t *)malloc(sizeof(packet_hash_entry_t));
 3:    // dynamic memory allocation to create hash entry for packet buffering
 4:    head = (packet_list_t *)malloc(sizeof(packet_list_t));  // dynamic memory allocation to create linked list header
 5:    memset(hash_item, 0, sizeof(packet_hash_entry_t));  // initialization of the hash entry

 6:    hash_item->packet_list = head;  // storing header address to connect the list
 7:    INIT_LIST_HEAD(&hash_item->packet_list->list);  // initialization of the hash list
 8:    memcpy(&hash_item->mn_address, mn_addr, sizeof(struct in6_addr));
 9:    // storing the MN's address related to the buffered packets
10:    ret = buff_hash_add(&hash_pool, hash_item);  // put the hash item into buffer pool

11:    pkt_buffering_add_rule(mn_addr);  // register the MN's address into IP6Tables rule

12:    pthread_rwlock_unlock(&buffer_lock);  // unlock thread unlock for buffering
13:    return ret;
}
```

Figure 37: Main lines of pmip_buffering_start() function

When the MN attaches to the nMAG, the nMAG sends PBU to the LMA. The Finite State Machine in the LMA that has received the PBU checks the MN 's address from the message and prepares to forward the packets for the MN. Figure 38 represents part of the function source code, pmip_buffering_reinject(), which searches for the hash item related to the MN, and calls the function for packet forwarding. It searches the hash tables where the packets for the MN are stored by using the MN 's address(line 2). After

that, it creates a thread that performs the pkt_reinject() function and forwards the packets to the MN until the buffer is emptied(line 5). Figure 39 shows the part of pkt_reinject() where the packets are forwarded to the MN from the hash table(line 1-line 9), and the MN 's address is erased from the IP6Tables after the buffer is emptied(line 10). It forwards all the packets for the MN that has roamed using the ipq_set_verdict() function in the libipq library. The ipq_set_verict() function forwards the packet to the kernel space repeatedly until the table gets empty. Therefore all the buffered packets are forwarded to the MN after the MN handover.

```
void pmip_buffering_reinject(struct in6_addr* mn_addr)
{
1:    pthread_rwlock_wrlock(&buffer_lock);  // lock buffer_lock thread
2:    hash_item = buff_hash_get(&hash_pool, mn_addr);  // load the hash item related to the MN from the buffer pool
3:    if (hash_item != NULL) {  //  if the hash item is found
4:            if (hash_item->is_reinject == 0) {
5:                    pthread_create(&thread, NULL, _pkt_reinject, (void*)mn_addr);  // create pkt_reinject thread
6:            }
7:    }
8:    else {
9:            dbg("Hash item is null. \n");  // if the hash item is not found, print error
10:   }
11:   pthread_rwlock_unlock(&buffer_lock);  // unlock buffer_lock thread
}
```

Figure. 38 Main lines of pmip_buffering_reinject() function

```
void * _pkt_reinject(void* data)
{
1:    mn_addr = (struct in6_addr*) data;  // storing the MN's address for forwarding
2:    hash_item = buff_hash_get(&hash_pool, mn_addr);  // load the hash list from the hash pool by usng the MN's address
3:    if (hash_item != NULL) {  // if the hash item is not empty
4:            list_for_each(pos, &hash_item->packet_list->list) {  // load the packets until the hash list gets empty
5:                    element = list_entry(pos, packet_list_t, list);  // pass the pointer of packet_list_t
6:                    ipq_set_verdict(h, element->pmsg->packet_id, NF_ACCEPT, 0, NULL);
7:                    // pass the packets to kernel
8:            }
9:    }
10:   pkt_buffering_del_rule(mn_addr);  // delete the MN's address from IP6Tables after the forwarding is done
11:   pkt_buffering_clean(mn_addr);  // delete the buffer related to the MN's address
}
```

Figure. 39 Main lines of pkt_reinject() function

The implemented packet buffering function prevents packet loss during the MN 's handover so that it can provide a reliable service. However, an MN that moves quickly may roam before all the packets are forwarded to the MN. In this case, the LMA does not forward the buffered packets and holds them, because the MN is not connected. In

addition, since the packets for the MN are buffered during the MN ’s hand over, more memory space in the LMA is required, which increases the load in the LMA. In order to resolve this problem and perform buffering effectively, this research proposes an improved forwarding scheme.

5.3.3.5 Performance Improvement Implementation

Most of the schemes that use buffering functions, packets buffered during the MN handover are flushed to the MN (Rasem, 2011). Packet flushing, that does not consider network bandwidth is the reason behind rapid network load and packet loss. Therefore, in this research a method is used in which the packet forwarding rate is adjusted according to the packet arrival rate, and the packets are forwarded to the MN instead of packet flushing. However, if the packet arrival rate and forwarding rate are the same in the LMA, the load of LMA is increased, because the amount of the packets in the buffer is increased when the MN moves quickly. In order to prevent the buffer from keeping packets longer, the packet forwarding rate is adjusted in order to be faster than the packet arrival rate in the LMA. So, the LMA increases the packet forwarding rate by the given rate of increment according to the calculated packet arrival rate, and forwards the packets. In this way, the LMA empties out its buffer, forwarding the packets more quickly than receiving them.

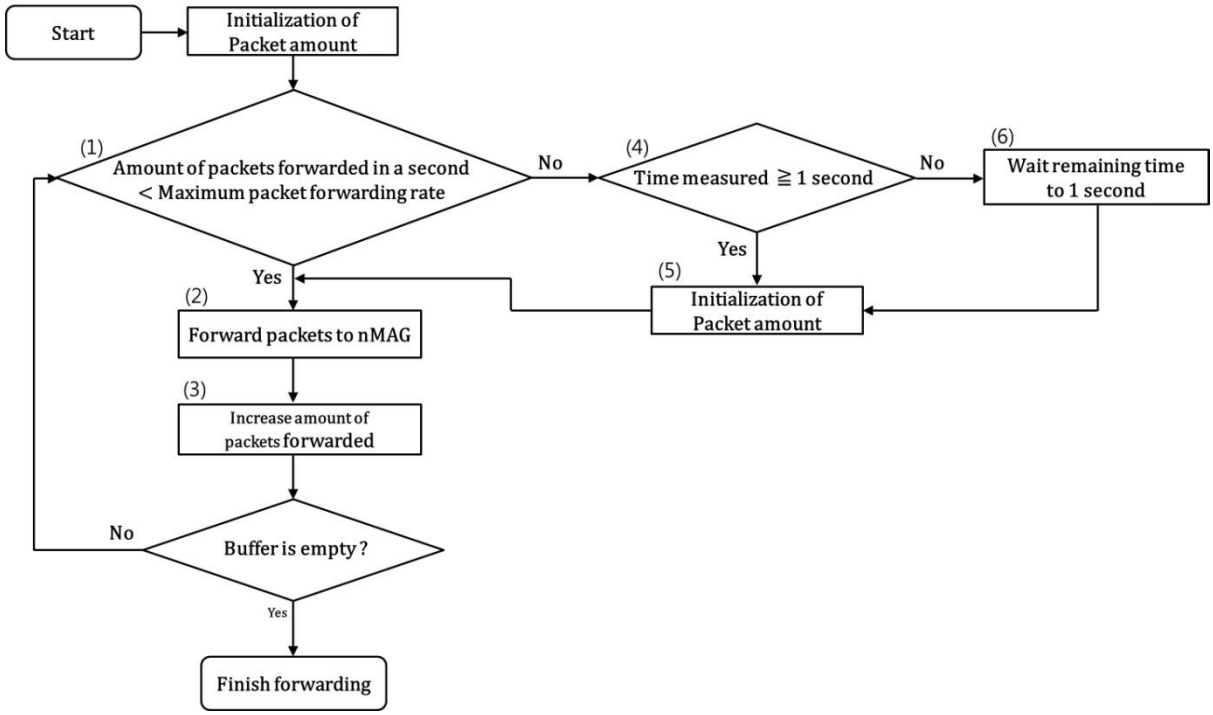


Figure 40: Flow chart of the improved buffering scheme

Figure 40 is a flow chart of the proposed buffering scheme to improve the buffering performance. The LMA calculates the packet arrival rate by using the interval of received packets during the MN handover. In order to make the packet forwarding rate higher than the packet arrival rate, the packet arrival rate is multiplied by a constant between 1 and 2 and obtain the maximum packet forwarding rate. After the MN handover, the LMA forwards the buffered packets to the MN. As packets are forwarded to the MN, the amount of the forwarded packets is increased. If the amount of the forwarded packets does not exceed the maximum packet forwarding rate (bps), the LMA continually forwards packets to the nMAG(line1 - line3). If the amount of the forwarded packets exceeds the maximum packet forwarding rate, the LMA checks if the measured time for the packet forwarding exceeds 1 second(line1, line4). If it exceeds 1 second, which means the LMA forwards packets within the limit of maximum packet forwarding rate, the amount of the forwarded packets is initializes and packet forwarding is continued(line4, line5). If it does not exceed 1 second, which means it reaches to the limit of the maximum packet forwarding rate, it stops the packet

forwarding and waits(line4, line6). Figure 41 shows a part of the control_bytesrate() function for performance enhancement of the implemented buffering function. Figure 42 shows a part of the modified pmip_buffering_reinject() function called when the packets in the buffer are forwarded. The packet arrival rate is multiplied by 1.2 to forward packets 20% more quickly to prevent excessive network load due to the increment of the packet forwarding rate(line 13).

```
void control_bytesrate(packet_hash_entry_t* hash_item)
{
1:    if (hash_item->sending_ctl.size_sent >= hash_item->sending_ctl.bytesrate) {
2:    // if the amount of the forwarded packets is larger than the maximum packet forwarding rate
3:            gettimeofday(&now, NULL);
4:            elapse = ts2usec(now) - ts2usec(hash_item->sending_ctl.date);  // measure the time of packet forwarding
5:            if (elapse < TIME_SEC_USEC)  // if the time is less than 1 second
6:                    usleep(TIME_SEC_USEC-elapse);  // wait remaining time to 1second
7:            gettimeofday(&hash_item->sending_ctl.date, NULL);
8:            hash_item->sending_ctl.size_sent = 0;
9:    }
}
```

Figure 41: Main lines of Control_bytesrate() function

```
#define INCREASE 1.2  // the constant to calculate the packet forwarding rate

void pmip_buffering_reinject(struct in6_addr* mn_addr)
{
1:    pthread_rwlock_wrlock(&buffer_lock);  // lock buffer_lock thread
2:    hash_item = buff_hash_get(&hash_pool, mn_addr);
3:    // load the hash item from the hash pool by using the MN's address
4:    if (hash_item != NULL) {  // if the hash item is found
5:            if (hash_item->is_reinject == 0) {
6:                    hash_item->is_reinject = 1;
7:                    elapse = ts2dsec(hash_item->time_end) - ts2dsec(hash_item->time_start);
8:                    // measure the time of packet buffering in LMA
9:                    if (elapse != 0)
10:                           hash_item->sending_ctl.bytesrate = hash_item->total_packets_size/elapse;
11:                           // calculate the average packet arrival rate by using the amount of the buffered packets and
12:                           // the time of buffering
13:                   hash_item->sending_ctl.bytesrate = hash_item->sending_ctl.bytesrate * INCREASE;
14:                   // calculate the maximum packet forwarding rate by multiplying the packet arrival rate by ICREASE
15:                   pthread_create(&thread, NULL, _pkt_reinject, (void*)mn_addr);  // create pkt_reinject thread
16:           }
17:   }
18:   pthread_rwlock_unlock(&buffer_lock);  // unlock buffer_lock thread
}
```

Figure 42: Main lines of modified pmip_buffering_reinject() function

In this research the buffering function was used to provide reliable service in PMIPv6. However, when the MN moves more quickly, handovers occur regularly and the LMA performs packet buffering before it forwards all the packets in the buffer to the MN.

This research proposes and implements a buffering scheme to resolve this problem and manages the buffer in the LMA more effectively. After the MN handover, the LMA forwards the packets to the MN more quickly than the packet arrival rate. The packet forwarding rate can be obtained by multiplying the packet arrival rate by a constant between 1 and 2. Packets can be sent more quickly to the frequently roaming MN by implementing the proposed buffering scheme, and reduce the load of the LMA by managing the buffer effectively.

5.4 Conducting the Experiment

The literature review analysis indicates four main investigative phases such as preparation, interaction, reconstruction and presentation of digital forensic investigation process, and the incorporation of security requirement/guidelines were considered in all the phases of the new model. The investigation was based on CDFIM.

In this aspect of this research, an experiment of a real testbed environment is performed to compare and analyze standard PMIPv6, the buffering scheme and the improved buffering scheme applied to PMIPv6. Packet loss during the MN handover are performed in each case, also the performance of the buffering and improved buffering schemes when the MN moves quickly.

5.4.1 Preparation Phase

At this stage, the strategy of approach on how to conduct the investigation was established. During the investigation Wireshark was used for data collect and to detect and confirm potential incident that can alter the data. Proper planning is conducted on the use of tools. The physical and operational infrastructure where made ready to support investigation. While conducting the investigation, consistent use of antivirus was in place and firewalls configured to ensure minimized risk of security threat to digital information. Authorization and authentication was established by applying

methods such as using username and passwords when using the systems and when the MAG detects mobile nodes, it checks for the host authorization. Secure policies were in place to implement and maintain the security of systems and digital information. The password used was securely managed to avoid any attampts of attack on the digital device and information. Proper check was made to ensure that software used was not identified with any security flaws. Secure internet connection was implemented each time there was need to connect to the internet. The security guidelines were demonstrated as applicable in the four phases.

The PMIPv6 testbed was established and experiment conducted to observe the performance of the implemented buffering scheme. Figure 43 represents the topology of the PMIPv6 testbed. The testbed is based on OAL PMIPv6 v0.3. The experiment was conducted by establishing an OAI PMIPv6 v0.3 testbed for standard PMIPv6, and including the buffering function. The testbed consists of an LMA and two MAGs. A free RADUIS was installed in the LMA and an AAA server rather than using a separate AAA server. A hub was used instead of an Acess Point (AP) for the wireless link, and connect the MN to an MAG with a cable. Although the same results can be obtained in a wireless environment as a wired environment, a cable was used in order to minimize signal interference and the effect of signalling size in a wireless environment. Unified handover time was also regarded by clarifying the start and end points of the handover in each cases and provide the same environmental conditions. The performance was evaluated with the testbed to obtain more reliable results from any performance evaluation.

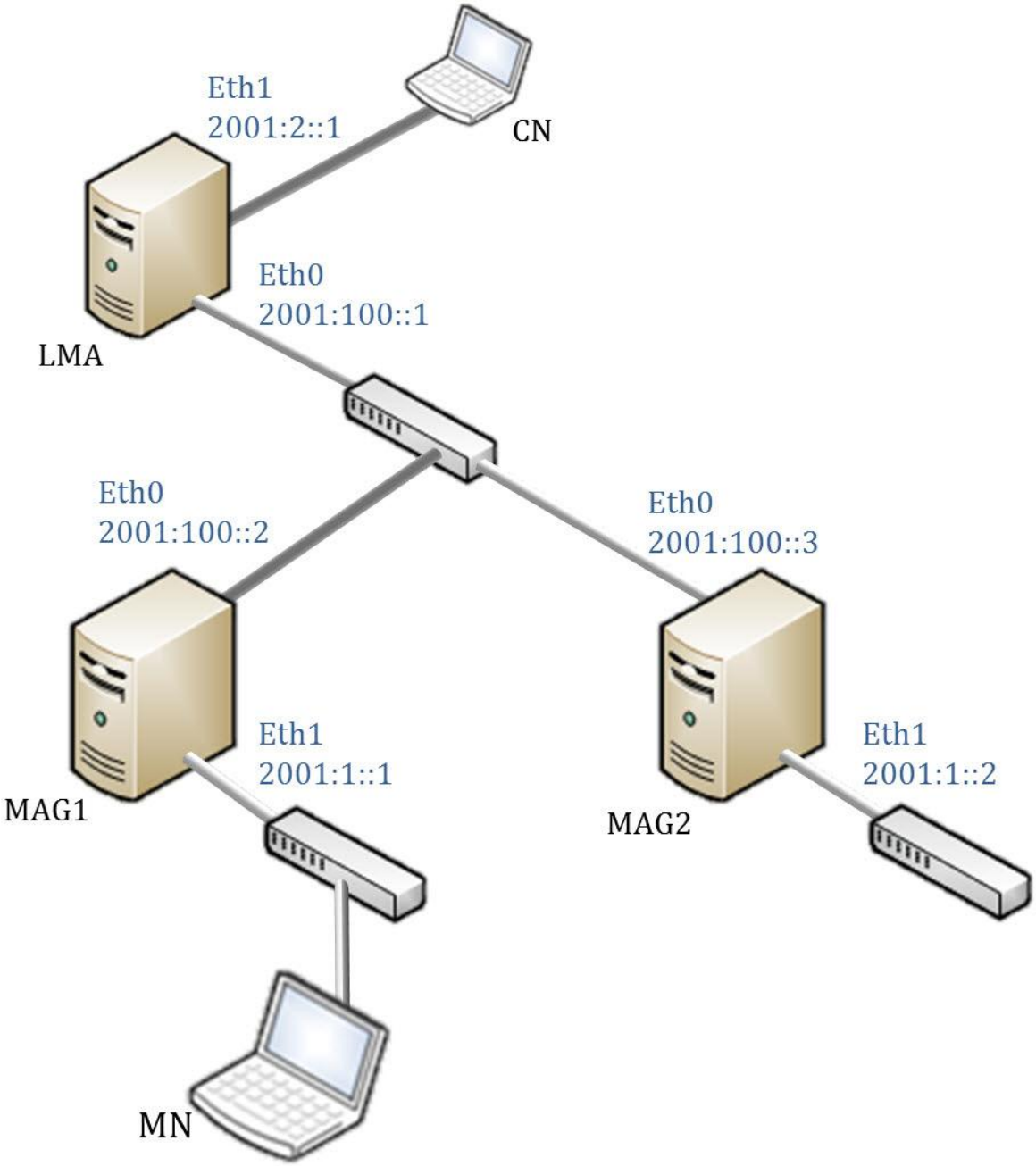


Figure 43: The topology of PMIPv6 test bed

5.4.2 Interaction Phase

The focus of the investigation was adjusted to the specifics of the case which is loss of data packets. The main goal of all activities carried out at this stage ensures the discovering, distributing of digital information and maintaing the integrity of the data. The performance of standard PMIPv6, and PMIPv6 with buffering and the improved

buffering scheme applied was evaluated. In this performance evaluation, the MN moves from MAG1 to MAG2 . A program written in python for packet transmission between the MN and Correspondent Node (CN) was used. The packet transmission program uses UDP protocol and consists of a server and client. The client transmits packets with the amount the user has set in the given data rate. Upon receiving the packets, the server checks the information in the data received. In the experiment, the CN is the client and transmit data to the server, the MN. The MN moves to MAG2 to MAG1 while receiving data, and the performance is evaluated by measuring packet loss.

The most important performance improvement of applying the buffering function is to prevent packet loss during the MN handover. In this performance evaluation, packet loss is compared in standard PMIPv6 and PMIPv6 with buffering applied, and show the superiority of the implemented buffering scheme by observing the packet sequence number change. The amount of packet in LMA is also compared in PMIPv6 with buffering and the improved buffering applied for performance comparison. Through this comparisons, this research proves the provision of reliable service by applying the buffering scheme, and the decrease in load of the LMA by applying the improved buffering scheme thus assisting in the integrity of digital data. Hence proving the integrity of digital evidence.

5.4.3 Reconstruction Phase

This phase involves bringing together the result of relevant digital information (data) from the earlier part of the process and any other relevant information which investigator may have obtained to provide a detailed account of the events or incident. Figure 44 shows the results of the MN handover in the standard PMIPv6, and PMIPv6 with buffering and improved buffering applied. The horizontal and vertical axes are time and packet sequence number that the MN has received, respectively. The MN

begins and finishes handover at 2 seconds and 4 seconds, respectively. The handover latencies are 2 seconds in each case. In the standard PMIPv6, about 250 packets are lost during the MN handover, as was observed during the experiment through the packet sequence number. However, in PMIPv6 with the buffering and improved buffering applied, packet loss does not occur, because the MN receives all the packets buffered in the LMA. In addition, the slope of the PMIPv6 with improved buffering applied is steeper than that of the PMIPv6 with buffering applied, because the packets are transmitted more quickly. Through Figure 44, it was observed that packet loss is prevented during the MN handover if a buffering function was used. It was also observed that if the improved buffering scheme was used, the buffered packets arrive in the MN more quickly.

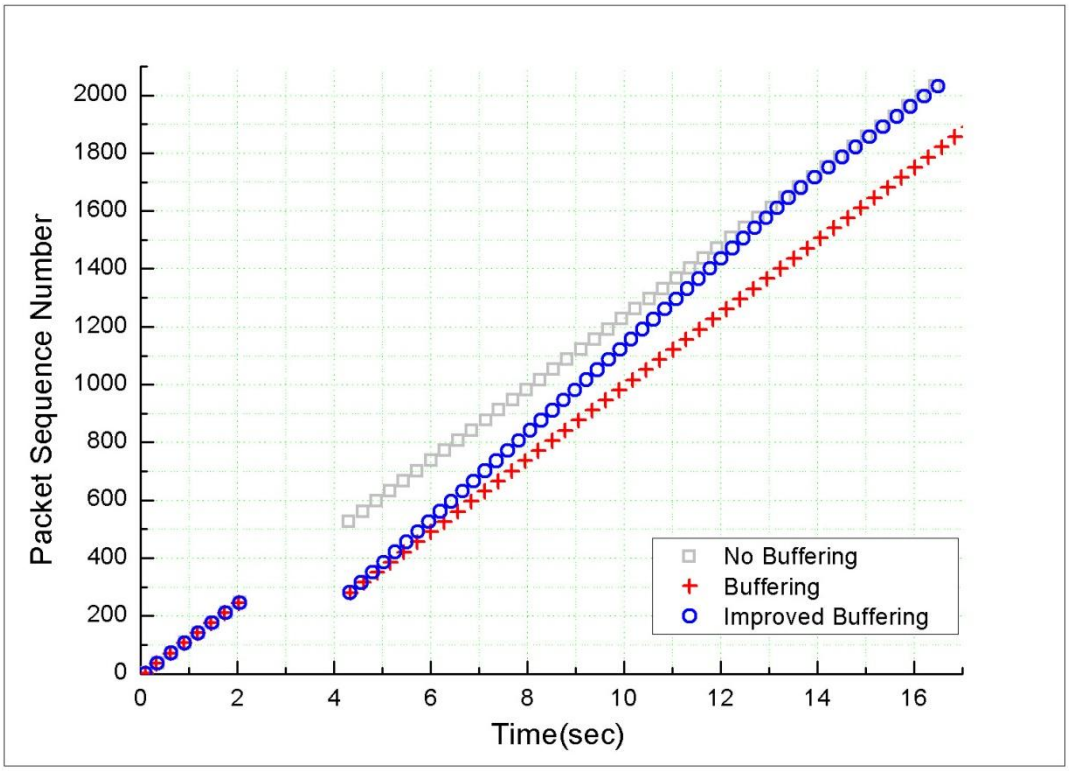


Figure 44: Handover results

5.4.4 Presentation Phase

In the presentation phase, the results of the case analysis are presented and the documentation of the whole activities during the investigation in a written report is conducted.

The packet loss in the standard PMIPv6 and that with buffering applied was checked to determine the differences in packet loss. In the experiment of this research, the client transmits 5 Megabytes of data to the server at 32~512Kbps. The number of packets was measured and sent from the CN to the MN. Figure 45 shows the amount of packets that the MN receives, depending on the handover latency. If the handover latency is longer, fewer packets arrive at the destination in the standard PMIPv6. If the data rate is higher, fewer packets arrive at the destination as well, because the amount of packets sent during the MN handover is larger. In the PMIPv6 with the buffering function, the amount of packets arriving at the destination is constant, depending on handover latency, although it is decreased as the data rate becomes higher. Figure 46 shows the packet loss depending on the handover latency.

The packet loss is in reverse proportional to the amount of packets arriving at the destination. When the data rate is 512 Kbps and the handover latency is 5 seconds, packet loss is prevented by 98.16%. It can be expected that if the handover latency is longer, it will prevent more packet loss. After the MN detaches from the pMAG, the pMAG sends a DeReg. PBU to the LMA and the LMA prepares packet buffering. During that time, the packets sent to the MN are lost, and the buffering function cannot prevent it. In Figures 45 and 46, it was observed that packet loss can be minimized during the MN handover using the buffering function, and it is effective if the handover latency is long.

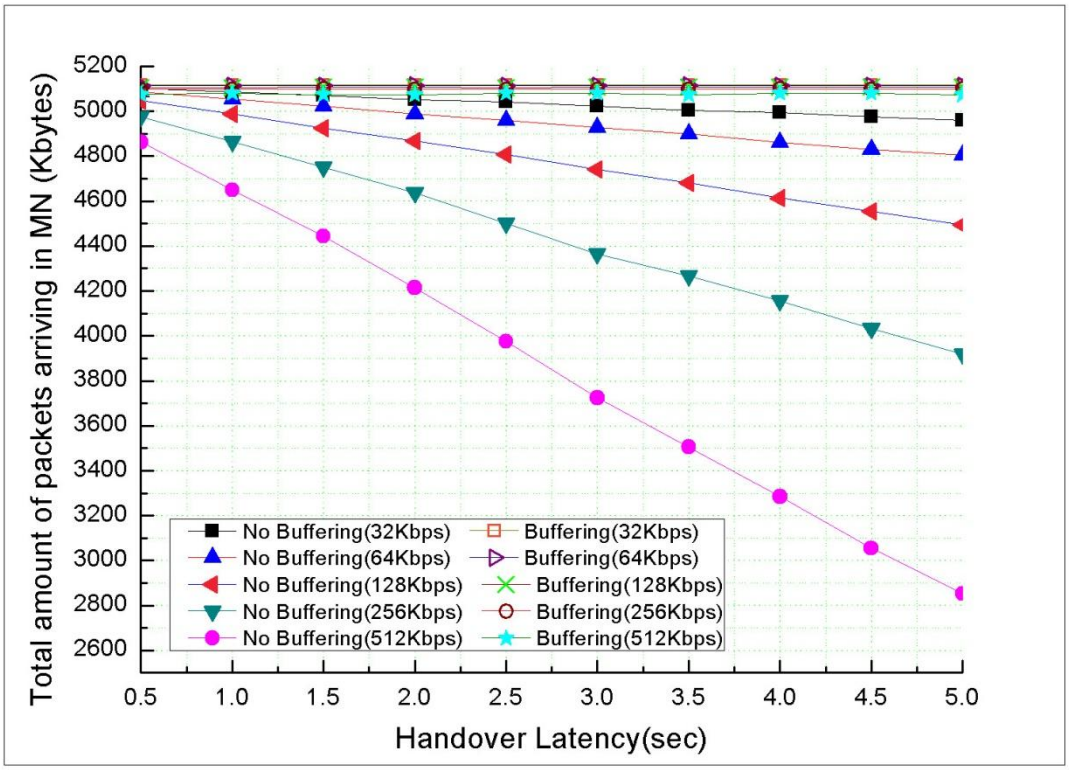


Figure 45: Total amount of packets arriving in MN

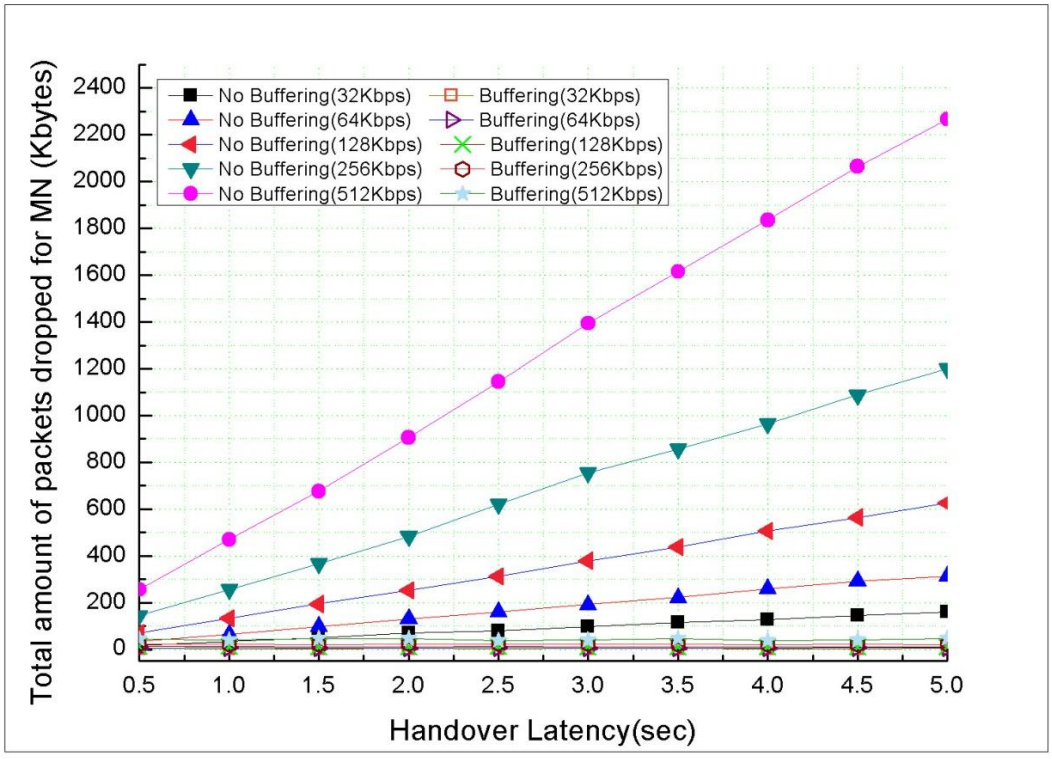


Figure 46: Total amount of packets dropped for MN

If the buffering scheme is used, packets are left in the buffer after the MN handover. If the packet arrival rate and forwarding rate at the LMA are the same, the amount of remaining packets in the buffer is constant. But if the packet forwarding rate at the LMA to the MN is higher than the arrival rate, the amount of packets gradually decreases, and the buffer will be empty after the MN handover. Figure 47 shows a comparison between two schemes, firstly, where the packet forwarding and arrival rate are the same, secondly, where the packet forwarding rate is higher than the arrival rate. After the handover latency for 2 seconds, the amount of packets in the buffer is constant in the buffering scheme. After that, it is increased again during the next handover for 2 seconds. However, in the improved buffering scheme, the amount of packets in the buffer is gradually decreased after the MN handover. Figures 47, 48, and 49 shows how the amount of packets in the buffer is changed when the packet forwarding rates are 1.05, 1.1, and 1.2 times the packet arrival rate, respectively. The times required to empty the buffer are 32 seconds, 16 seconds, and 9 seconds for each case, respectively. In the improved buffering scheme, the amount of forwarded packets is higher than the amount of received packets at the LMA for a while. Therefore, the amount of packets in the buffer and the load of the LMA can be reduced, but the required time depends on the packet forwarding rate.

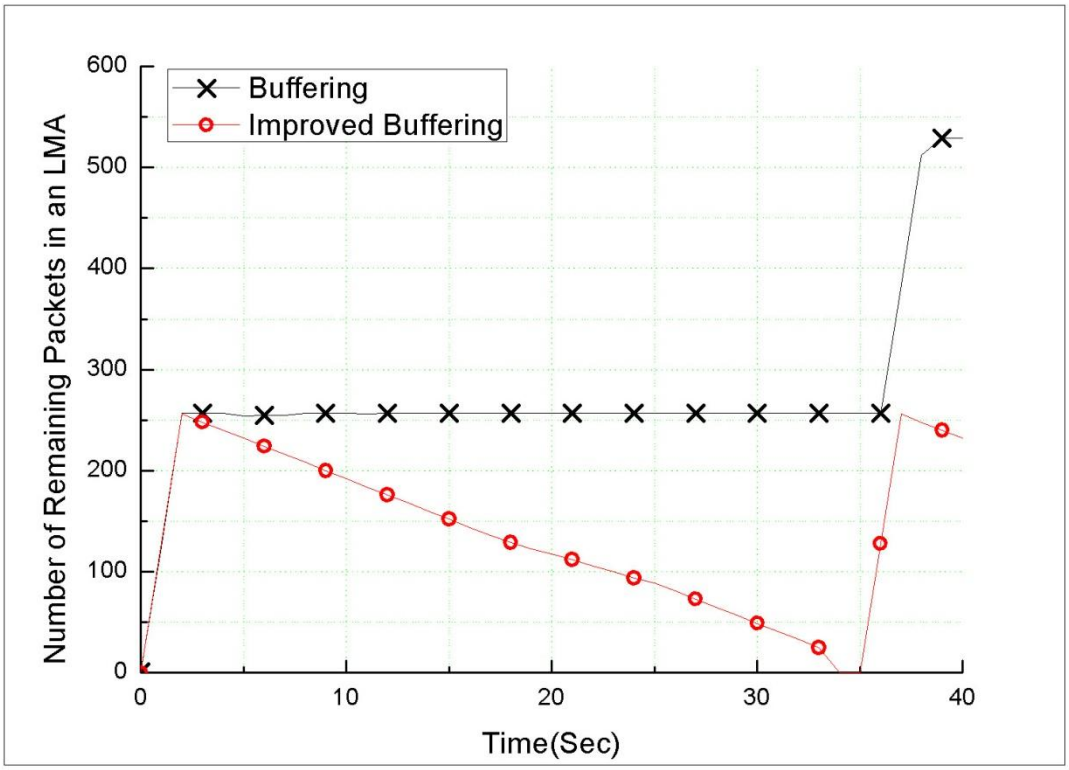


Figure 47: The amount of remaining packets in the buffer (5% improvement)

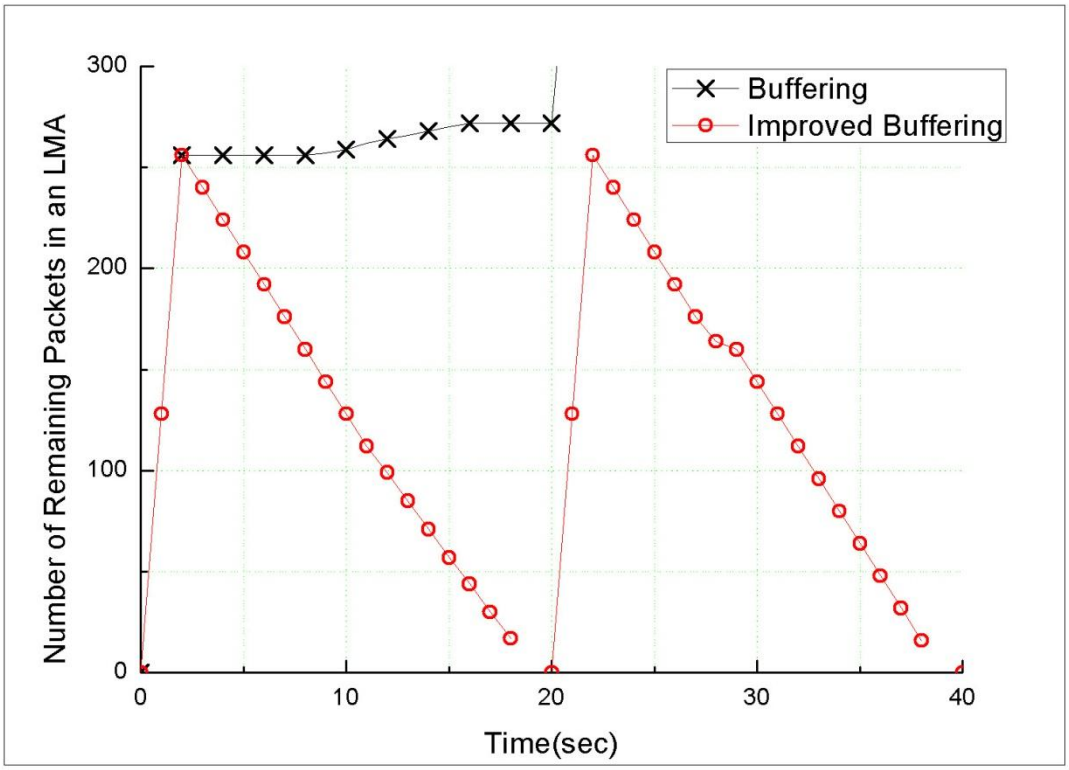


Figure 48: The amount of remaining packets in the buffer (10% improvement)

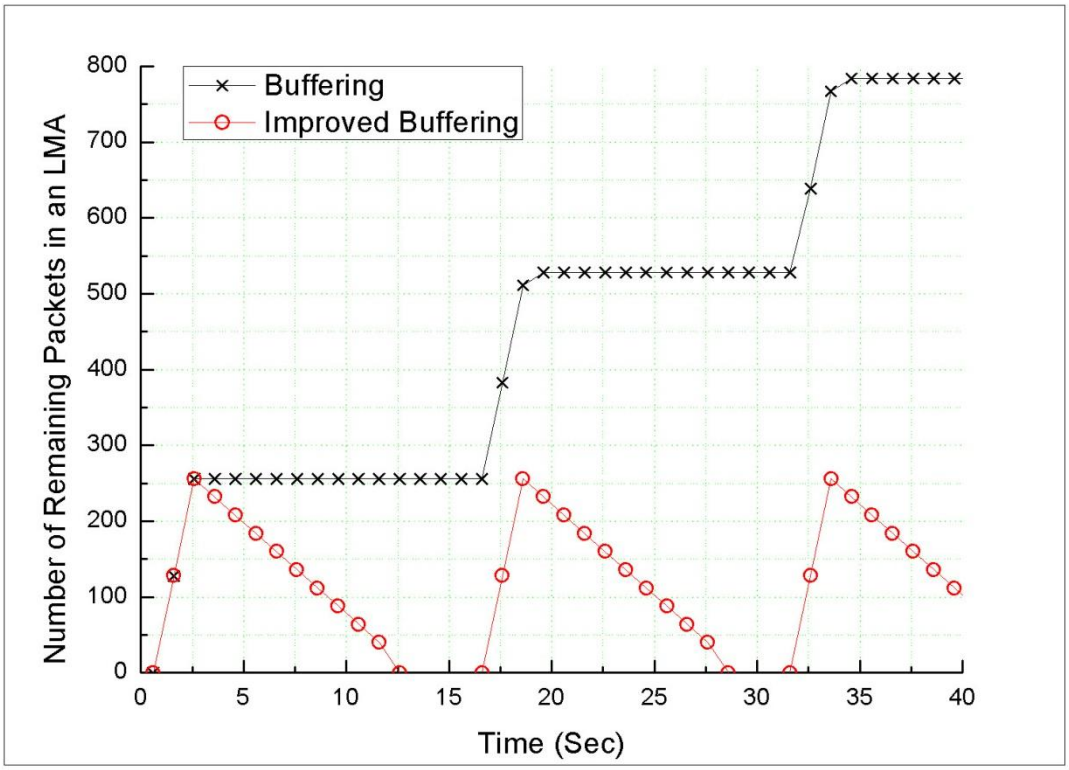


Figure 49: The amount of remaining packets in the buffer (20% improvement)

PMIPv6 with improved buffering function, provides a solution that can reduce the latency in IP handovers by limiting the mobility management within the PMIPv6 domain, therefore, it can largely avoid remote service which not only cause long service delays but consume more network resources which can cause DoS attack.

5.5 Experiment 2

5.5.1 Experiment Design

This section covers another possibility of digital attack investigation.

5.5.1.1 Type of Attack

This is a case of violation of an organisation's IT policies. The IT security discovers that an employee violated the organization's IT policy by illegally using his personal email account during office hours. A digital investigation needs to be conducted in order to identify the activities of the employee, there was need to collect evidence of activity by the employee from the employee's email box. This activities were then examined to provide the interaction and reconstruction process with information about the employee's activities. This examination also demonstrates the applicability of the investigative process proposed in this research.

5.5.1.2 Collection of Data

To examine the case in order to confirm the need of proposed security requirement and digital forensic investigation process of the new model, a test image with realistic data was created. In a hypothetical scenario, an email message is sent in a way that breaches a security policy, the computer is acquired and there is need to investigate the case to confirm the use of the personal email box during office hours. The test image is a Virtual Machine (VM) running Microsoft Windows XP with messaging and communication applications installed. The image has a user labelled dommyuser1. The user account was created with a default administrator account and labelled dommyuser1 with no administrator privileges. Once the user account was created, communication software was installed. A gmail account was created with the same username. Outlook was configured using IMAP and synchronised for the account. The dommyuser1 sent email to the account. To capture the initial state of the source data to ensure that copy that can be used for data processing is available when needed. The copy of email

content (gmail account) from Outlook was saved in a folder called "U" and kept safely to be used when needed for data processing.

5.5.1.3 Method of Investigation

In this case, security violation is established therefore, a systematic and scientific model of investigation is employed to examine and analyse the crime. Using the Comprehensive Digital Forensic Investigation Model (CDFIM) an investigation is conducted. The objective of this is to test the hypothesis and to present the applicability of CDFIM.

5.5.2 Experiment Component

- Windows XP
- Internet Explorer
- Firefox
- Google Chrome
- Internet Massage Access Protocol (IMAP)
- Outlook
- Google Mail
- Wireshark

5.5.2.1 Toolkits

The Forensic Toolkits (FTK) was used in this investigation. FTK establishes the perception of relationship of the security requirement with digital forensic investigation process. The analysis will show how the phases of the comprehensive model address cases during digital investigation.

The protocol analyzer known as Wireshark was deployed and used to detect and confirm any incident that may disrupt the investigation and influence the integrity of digital evidence while conducting the investigation.

5.5.2.2 System Requirement

- Windows XP 32/64-bit
- Minimum RAM of 2GB
- Hard disk space 6GB
- FTK Version 1.81.6

5.5.3 FTK Interface

The FTK interface is divided into a number of tabs. Each tab is filled with individual panes that can be defined by the user. Each tab in FTK is a customizable frame in which individual panes can be moved, added or deleted.

Every tab contains only one tree pane such as Explorer, Graphics, Overview, Email, or Bookmark. It can also contain other panes such as File List, File Content, Properties, Hex Value Interpreter or Thumbnails. The report can be extracted and presented constructively at the end of the case analysis. The following are:

Search Tab

In AccessData FTK 1.81.6 Version the Search tab is a specific tab that, once tabbed, is divided into Index Search Tab and Live Search Tab. The Index Search allows for fast searching based on keywords. The evidence must be indexed in order to perform indexed searches. The Live Search tab allows searching of any word, hex value, or number entry throughout the case.

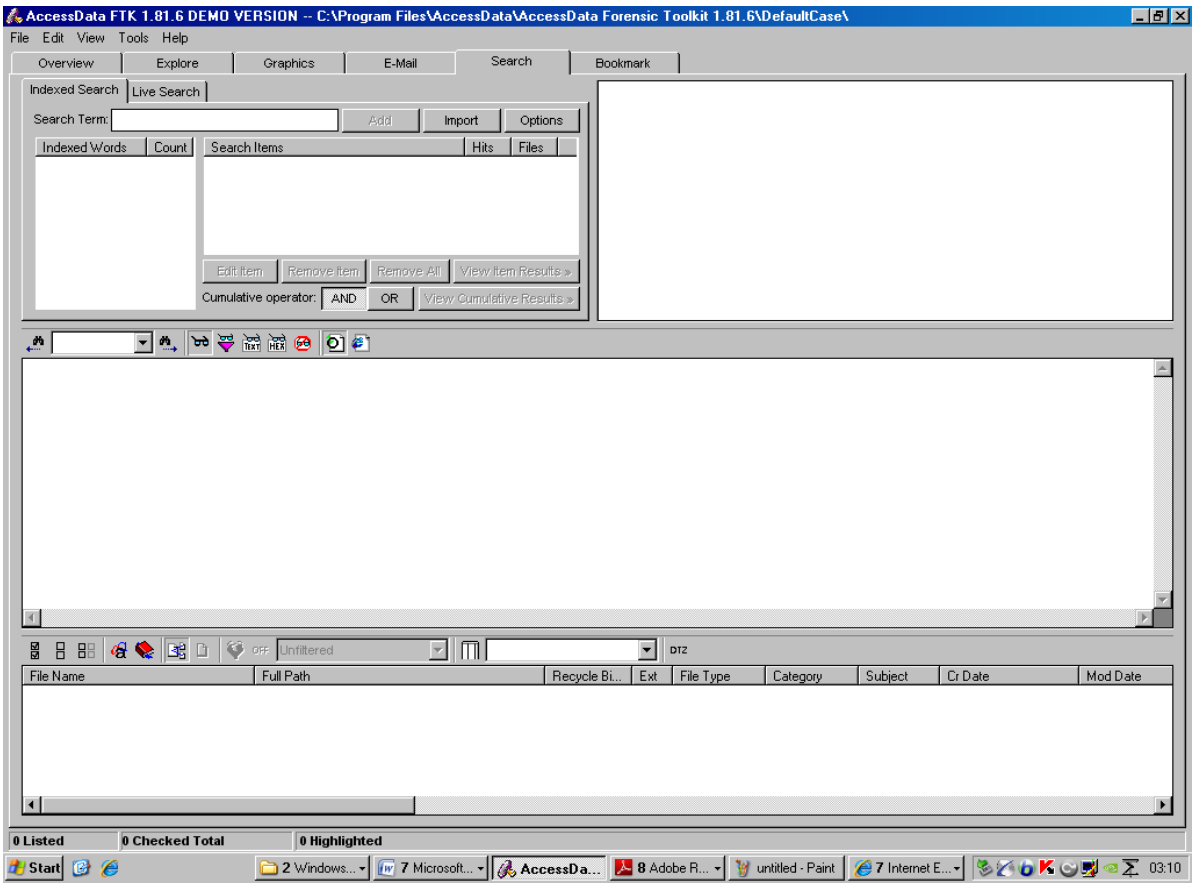


Figure 50: The search tab

Overview Tab

The overview tab provides a general view of a case. From the test conducted as shown in Figure 51, it can be confirmed the items that exist in the various categories, view lists of items and look at individual files. FTK categorises file types based on the file header. File types are organised in a tree structure rather than containers, FTK can categorise file types on a granular level. As confimed during the test at the root level, the overview tab groups case items in the categories of File Items, File Extension, File Category, File Status and Bookmarks.

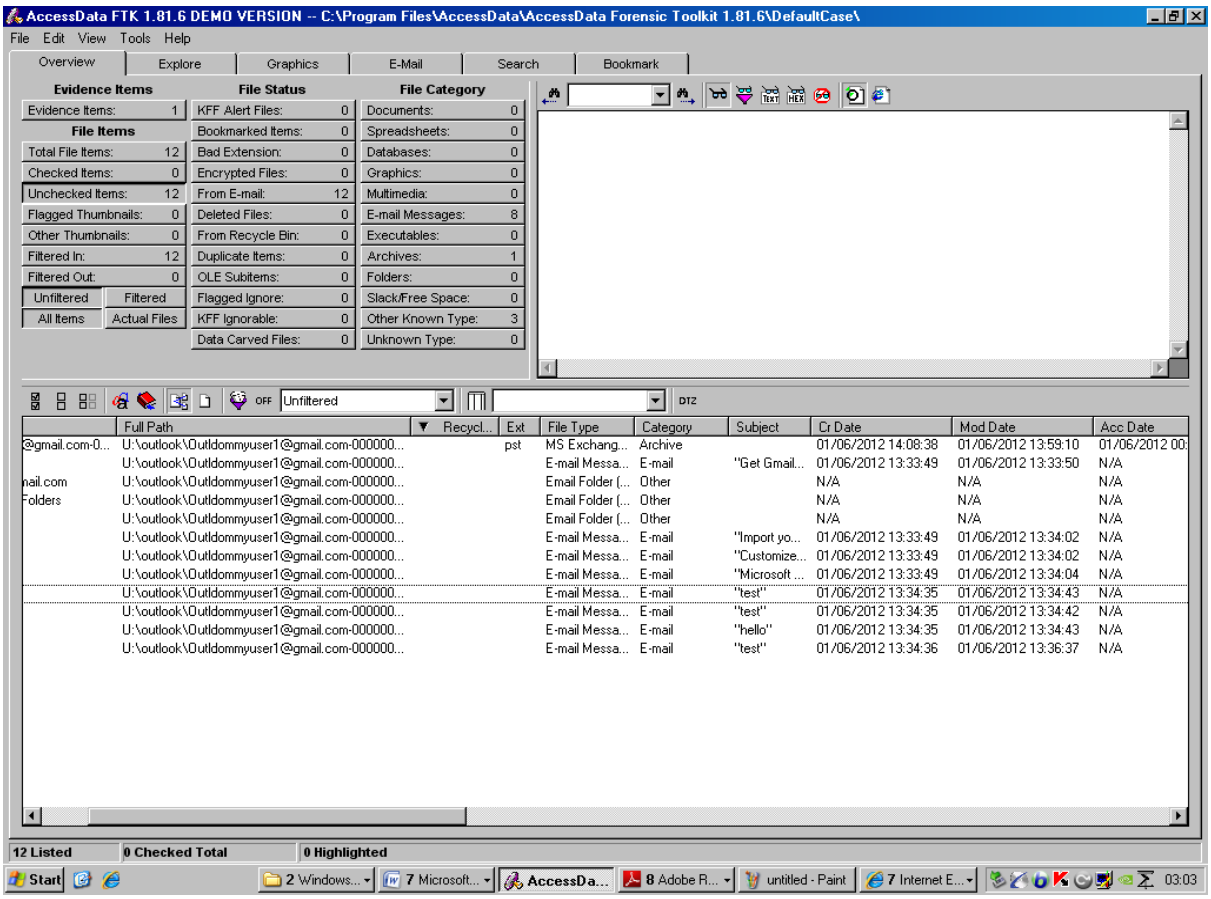


Figure 51: Overview of the case

Explore Tab

The Explore tab gives access to the evidence item's original directory structure. From the test result as shown in figure 52 the Explore tab viewed folders in specific locations and perform searches based on the layout created by the user.

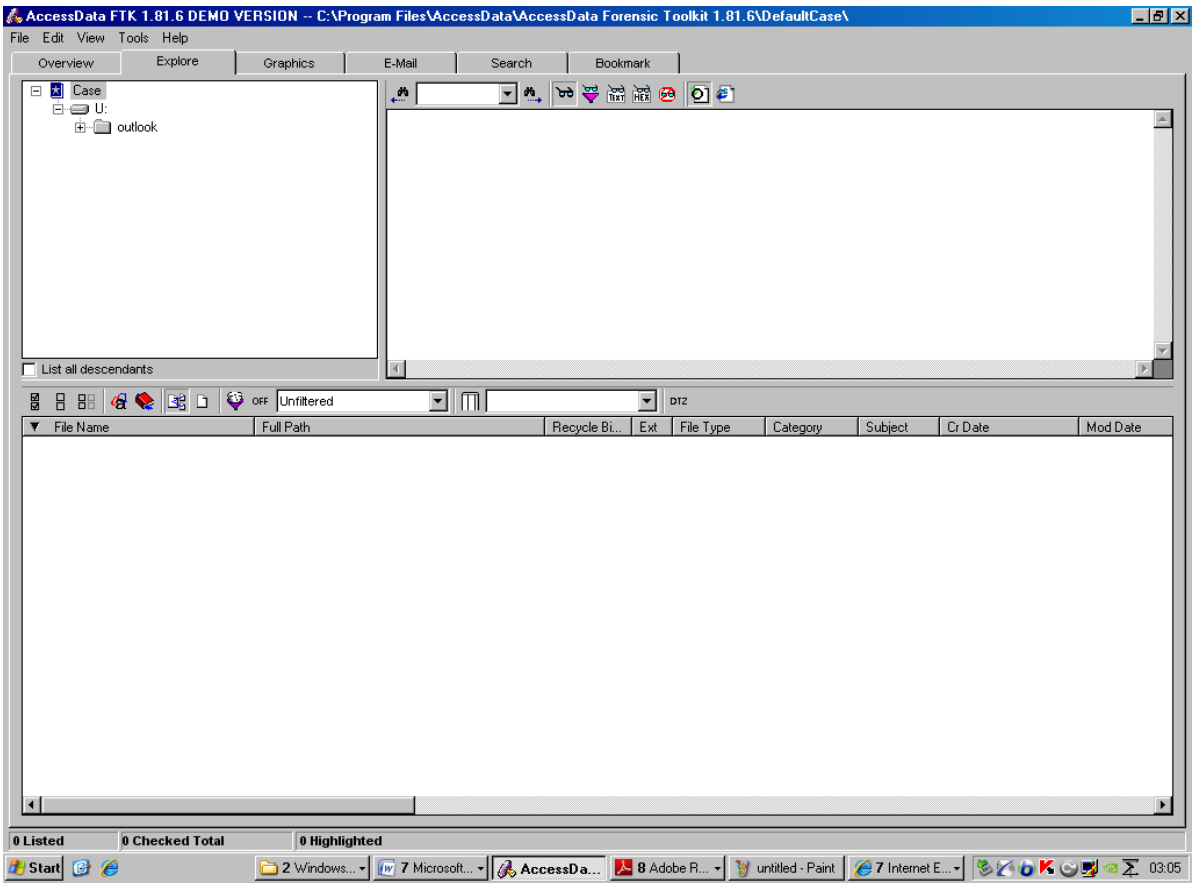


Figure 52: The Explore tab

Graphic Tab

The Graphic tab is a variation of the Explore tab with an emphasis on graphics files. Like the Explorer tab, it includes the Evidence tree but during the test conducted, filtering is applied so that the Graphic tab shows only graphics files.

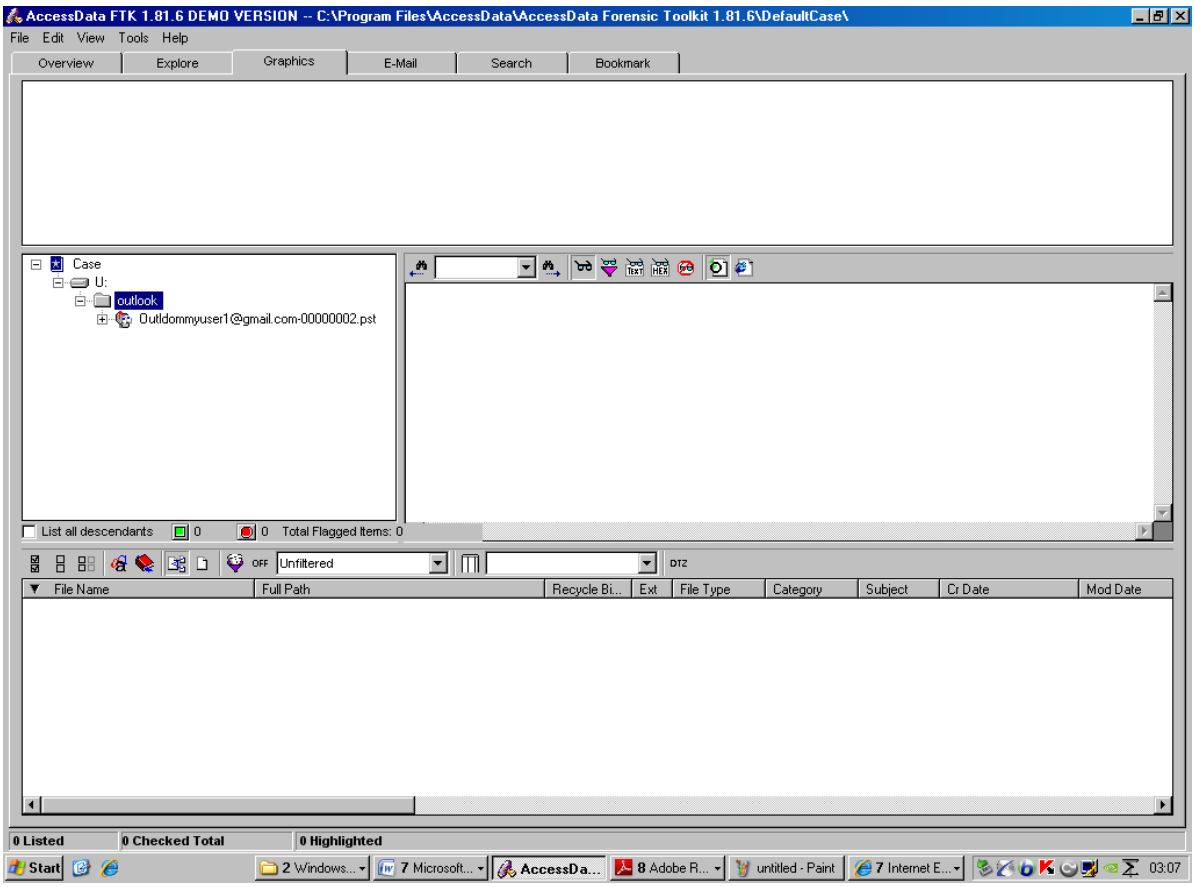


Figure 53: The Graphic tab

Bookmark Tab

The FTK bookmark features provide an excellent way to organise and track items of interest. After an item is bookmarked, it was indicated that the bookmark and their associated files/items in the bookmark tab as shown in figure 54 can be viewed. Bookmark can also be used to generate case reports.

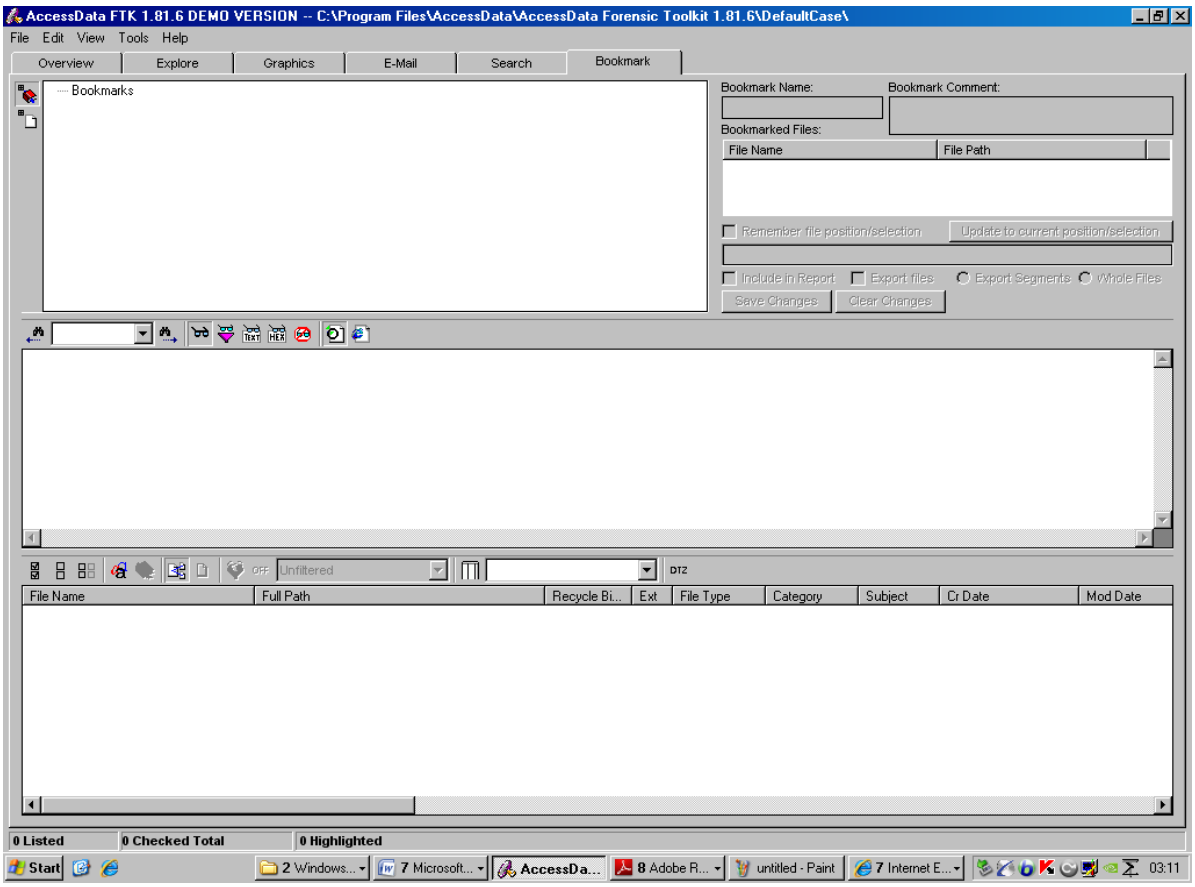


Figure 54: the Bookmark tab

Evidence Processing

In FTK options can be selected to calculate file hashes and perform the Known File Filter (KFF). FTK provides a number of filtering options, including a Slack/Free space button on the main screen that will provide a list of file slack, file system slack, and unallocated space. The File slack and drive free space (unallocated space) are located on the Overview tab, then File Status and then Slack/Free Space. They can also be found on the Explore tab under the appropriate tree node.

In FTK Evidence Processing defines the default processing options for all evidence items added to the current case as shown in figure 55. These processes can shape the scope of the analysis and the outcome of the case.

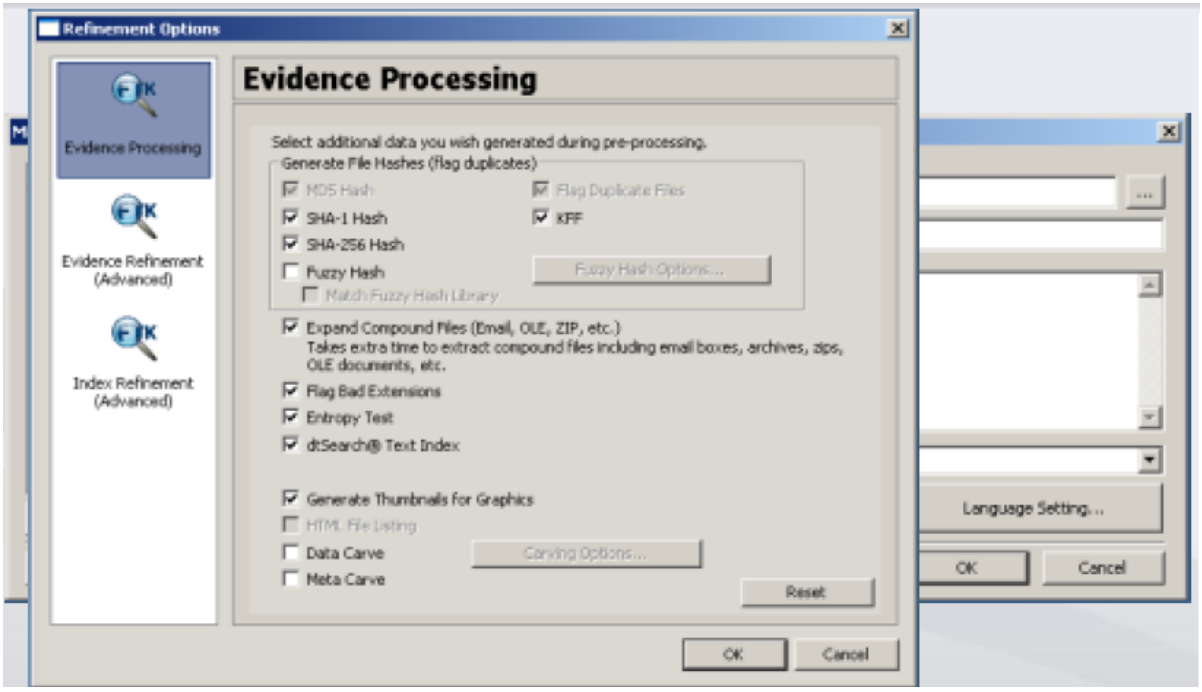


Figure 55: Case processing option

Filtering capabilities are built into FTK in the form of a File Filter Manager, enabling to select which types of files to exclude. For instance in ignoring duplicate files, click on the Filtered button on the main FTK screen and then uncheck file system artefacts that are unwanted or have been exported. In FTK File Duplicate Files Option helps to generate an MD5 hash for each file and identifies duplicate files based on a comparison of MD5 hash values.

Evidence processing shows the default processing options for all evidence items added to the current case. These processes can shape the scope of an analysis and the outcome of the case.

5.5.4 Conducting the Experiment

The digital investigation is conducted based on CDFIM

5.5.4.1Preparation Phase

The first step taken to examine this case was to ensure that the search will not violate any law and risk assessment was conducted. As identified in this research, it is recommended for investigators to collect written instructions and authorisations from their legal representatives before conducting digital investigation. As mentioned previously this is beyond the area of scope and the research assumes that authorisation for investigation has been given.

The preliminary investigation showed that the employee had used a personal email during office hours but denied the allegation of using personal email. In this case, an incident was detected and confirmed and there was need for an investigation. Therefore, further step was to collect evidence of suspicious activity from the employer's computer. This activity was then examined in order to provide the reconstruction process with information about the employer's activities. All possible communication capabilities of the system were disabled to avoid corruption of evidence. To maintain chain of custody, there was proper documentation of the processes.

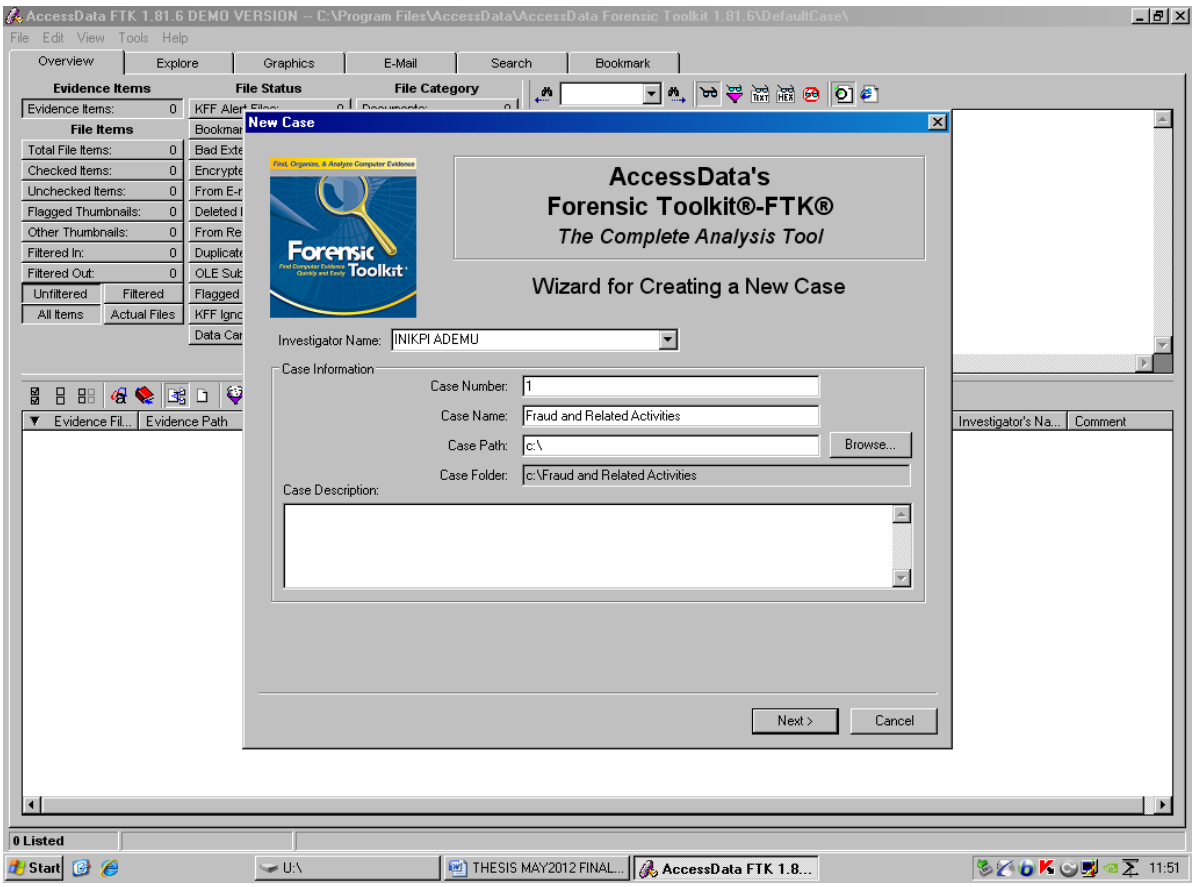


Figure 56: Creating a New Case

In this test phase, the equipment was ready and used effectively for the investigation.

For the test, a new case within FTK with the following steps are:

- Log into FTK Case Database Manager with a user account that has administrative rights to create a case.
- Click on File and then New Case
- Complete the New Case Option dialog as shown in Figure 56.

The FTK deployed contains security component that was not ignored but considered during the investigation. Authorization and authentication were established while conducting the investigation. Identification and Passwords were properly managed. Cryptographic options were considered and applied in order to ensure the integrity of the duplicate files of the digital evidence. Operational procedures was followed on how to use and manage tools, also security procedures on how to protect tools from threats

and vulnerabilities were also considered. Security component such as antivirus, personal firewalls and secured protocol were made available. Antivirus software was implemented in order to detect any known malicious code and stop them from infecting a workstation . The Antivirus software's virus definition files was kept up to date, so that it can detect the most recent viruses. A personal firewall protected the workstation from intruders. An intrusion detection system known as wireshark was made available for port sanning to detect signal of imminent attack and alert during investigation. Care was also taken to ensure that software flaws are identified and relevant update with patches are applied.

5.5.4.2 Interaction Phase

This is a major phase introduced in this research. The Interaction phase ensured the following:

The gathered evidence is added to the case for analysis.

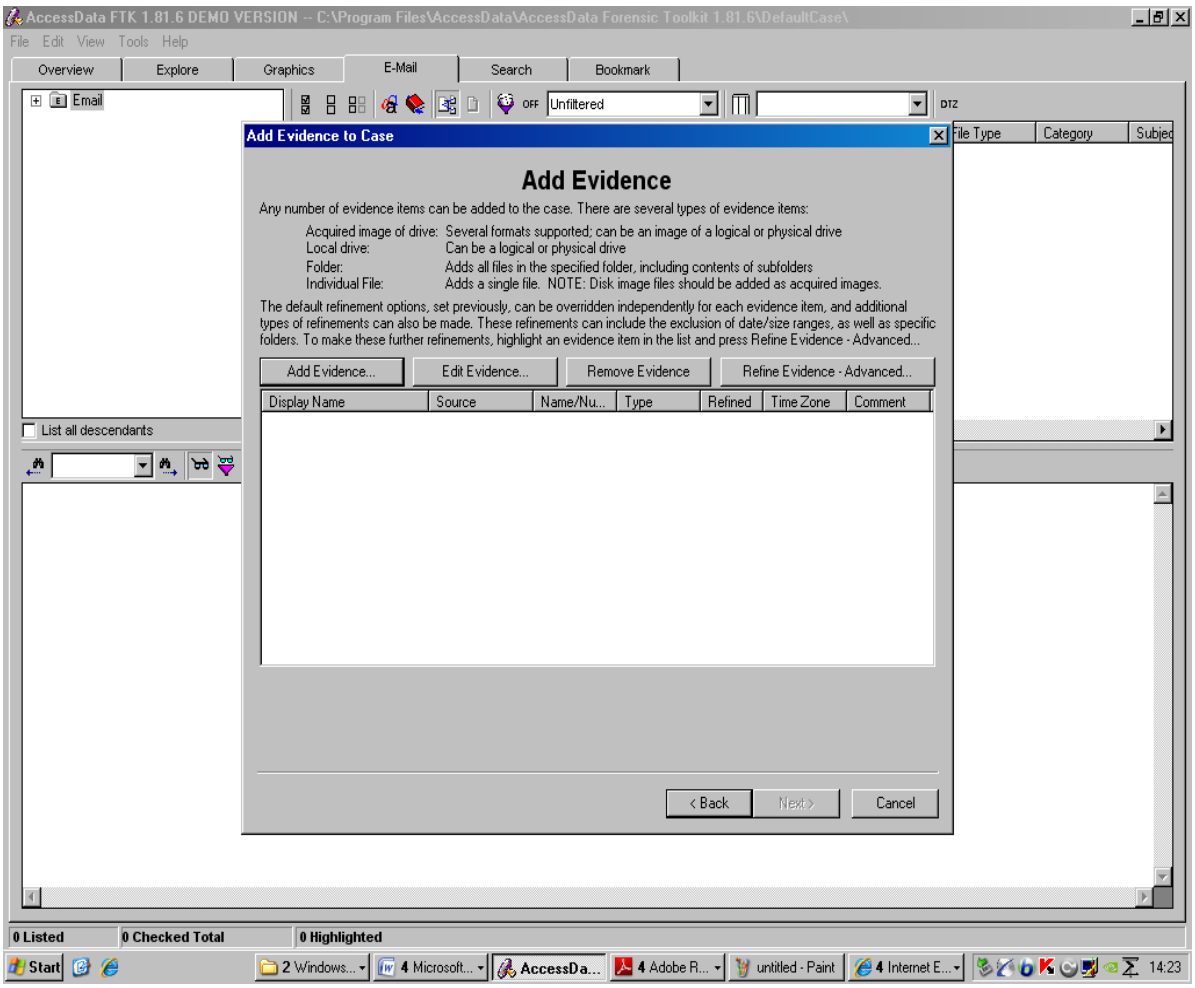


Figure 57: Adding Evidence in FTK

In order to add an evidence, a dialogue box will pop up as shown in Figure 57.

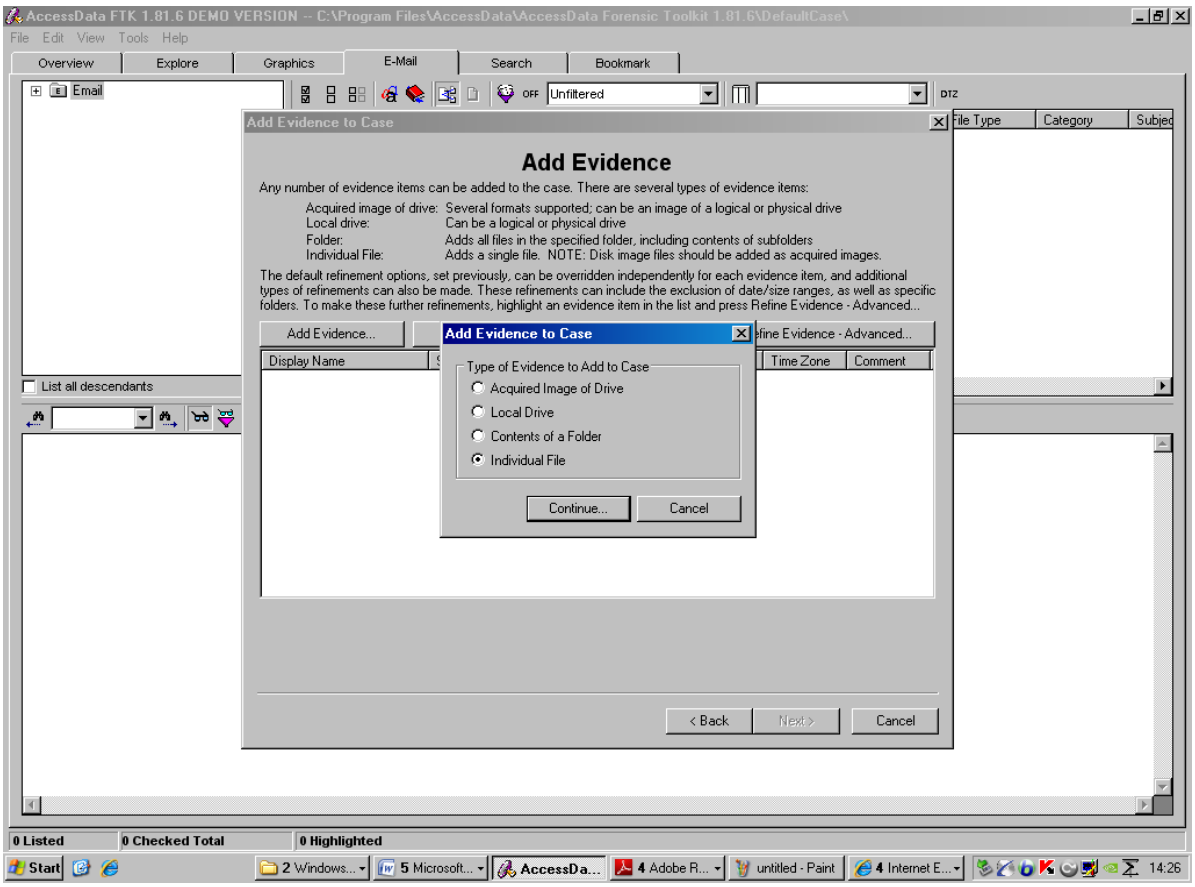


Figure 58: Selecting an image destination

The Evidence dialogue box allows the adding and removal of evidence items from the case.

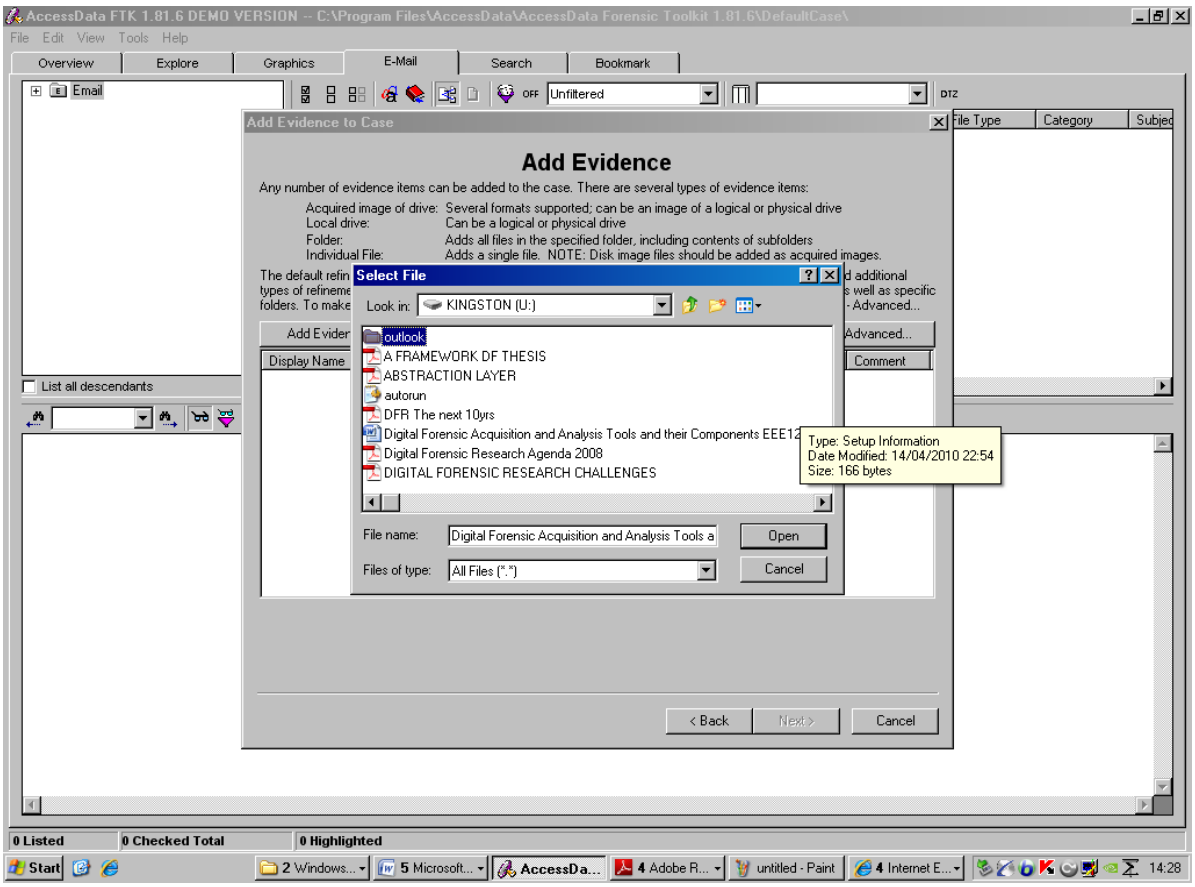


Figure 59: Selecting the image folder

As shown above, FTK works with different evidence source types.

- Acquired image of a drive: Any supported forensic image
- All images in the directory: all supported forensic images located in the specific folder
- Content of a folder: A specific folder and accompanying subfolders and files
- Individual files: A specific file or files
- Mobile Phone: for a mobile phone to appear as an evidence source, the Mobile Phone Examiner Software (MPE) must be installed and the MPE licence must be present on the CodeMeter dongle.

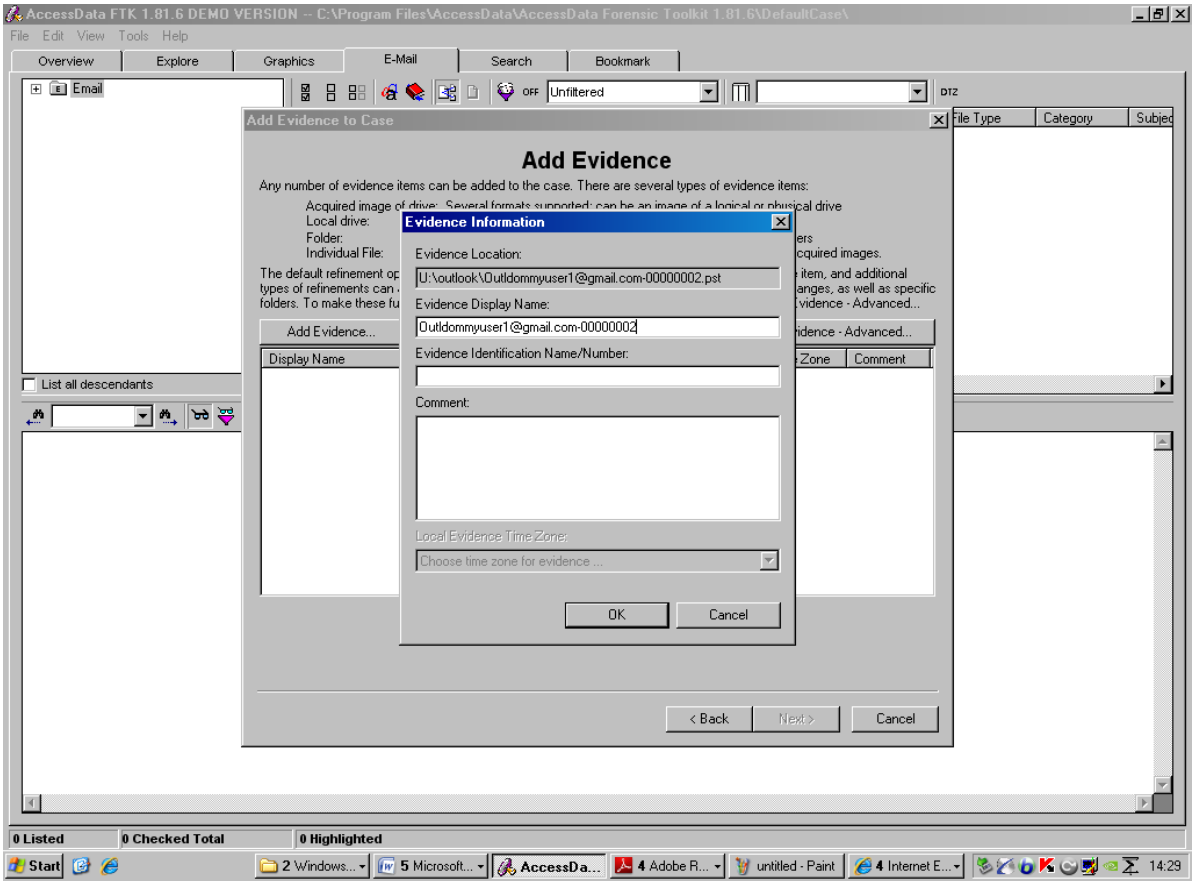


Figure 60: Identifying the evidence

Figure 61 shows that the test focused on the specific of the case. The digital investigation focused on email content. The relevant data was collected. At every stage of handling and processing the digital evidence documentation was a continuous process, which was required to maintain a good chain of custody.

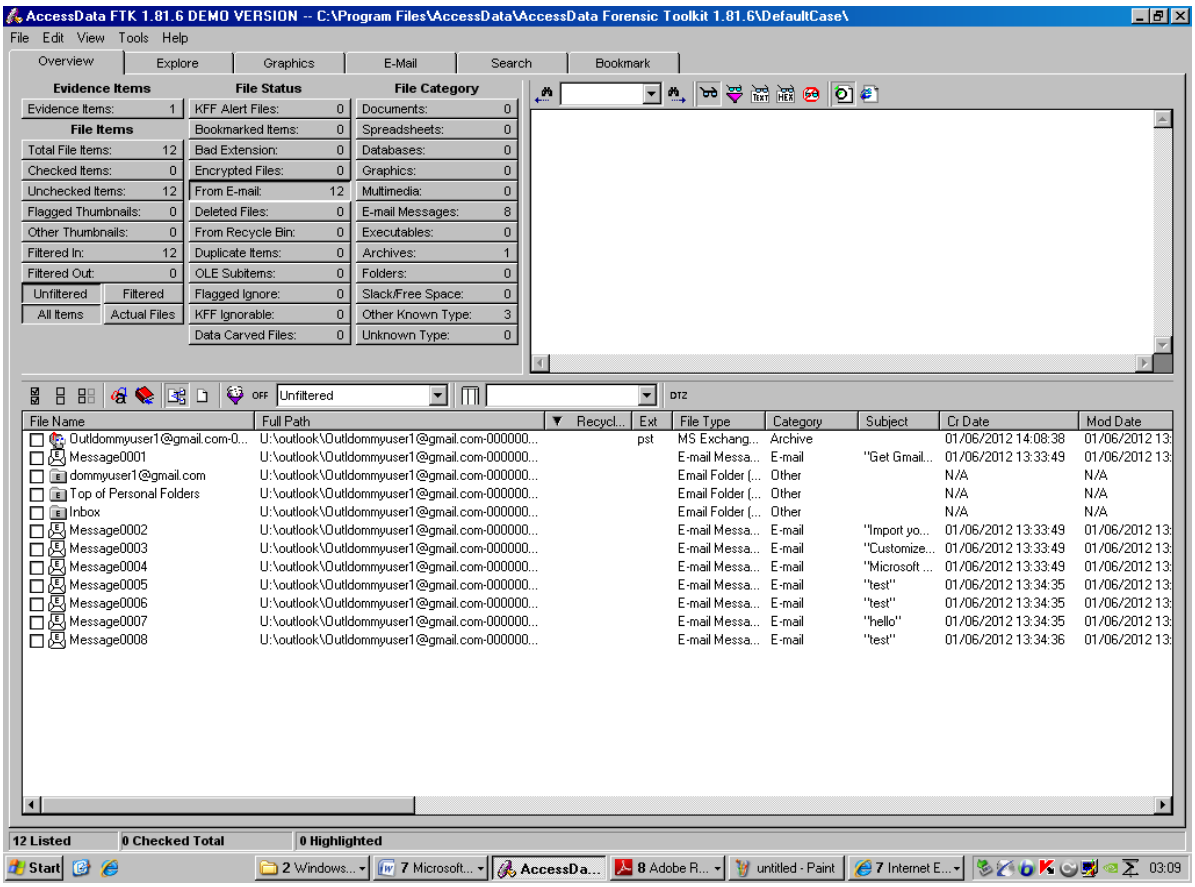


Figure 61: Viewing the Email messages

In the test conducted the Email tab helps narrow the focus to display only email-related files. The Case overview pane displays email-related containers to give quick access to email databases within the evidence. From the test conducted when an email file was selected from the file list, it indicated that the File Content Viewer displays the email message in HTML format and the Email Attachments pane displays email attachments associated with the current message as shown in Figure 61.

Baesed on the result shown above, a chronological timeline analysis was conducted in order to identify the employer's activities, it was confirmed that the employee used his personal email from 13:34pm until 14:08pm. This time confirmed that the employee used his personal email during office hours. The digital evidence is securely transported and properly stored.

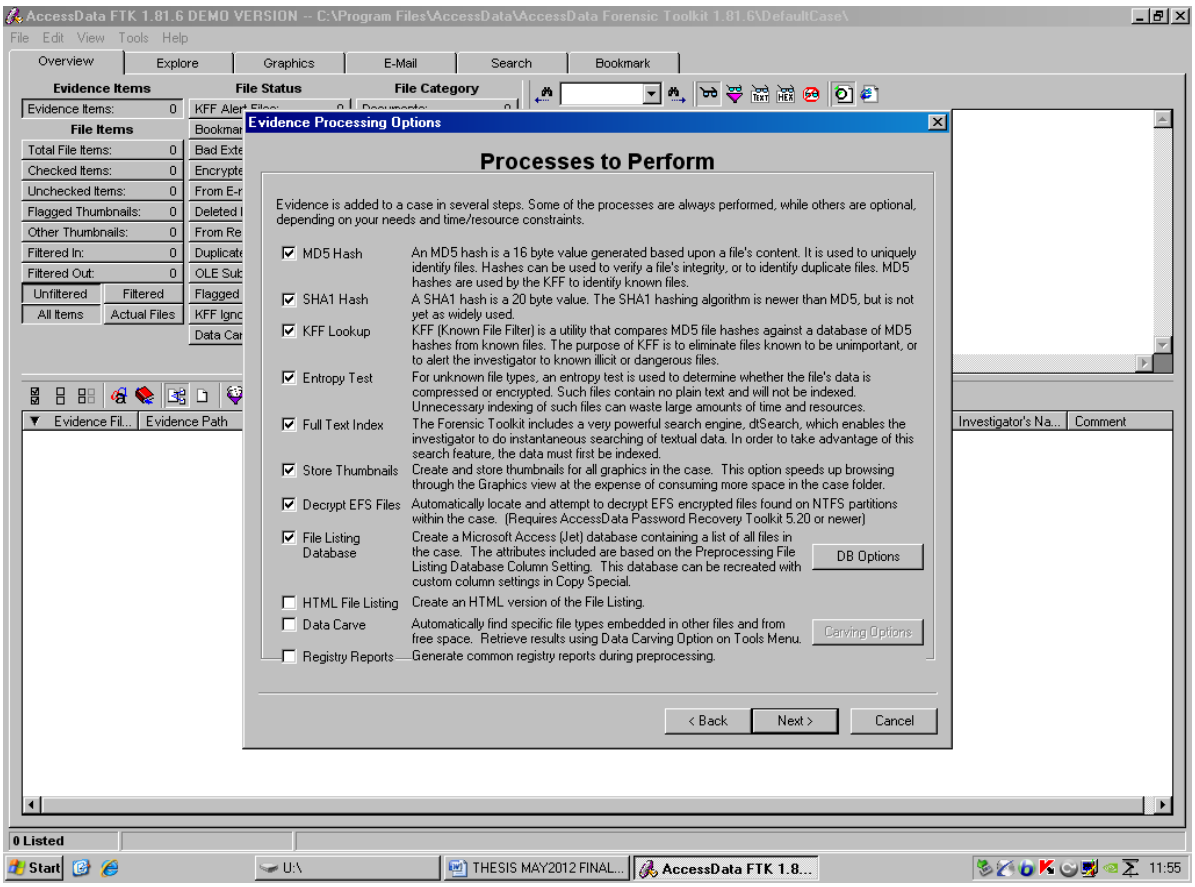


Figure 62: Case processing options

Figure 62 shows the preservation of the evidence conducted by applying the evidence processing options. This assist in verifying the integrity of files which contains evidence.

In the Interaction phase all the security giudelines also needed to be considered and ensured its continous availability. In the investigation, security guidelines such as using a secure protocol and ensuring that all available unused network ports were closed to avoid external communication that may lead to vulnurability. An important step when collecting evidence is to image the data in a way that will not alter the integrity of the data. Adequate process was in place for making available safe media on which to image the data to be processed. The FTK used to examine the case in the test is able to recover a lot of raw data, files, folders, streams and metadata. Without doubt identifying the data on its own generates value in an investigation. There are pages and pages of file

names, attributes and other details, but none of this information is enough to ensure the integrity of the evidence though. It is important that data is analysed in a step by step approach that ensures the integrity of the information collected.

5.5.4.3 Reconstruction Phase

In this phase, the result of relevant information from the earlier part (interaction phase) of the analysis process were gathered with other relevant information which have been obtained to provide a detailed account of the activities of the employee.

Based on the evidence found, more analysis is made and conclusion is drawn. When an evidence item is selected in FTK, relevant information about the item can be displayed. To view the properties of any file item, select the item in the File List pane, and the file properties will show as seen in Figure 63.

The digital component identified is evaluated and ensures that it is relevant to the case being investigated and can be considered as a legitimate evidence. The findings or results are properly documented.

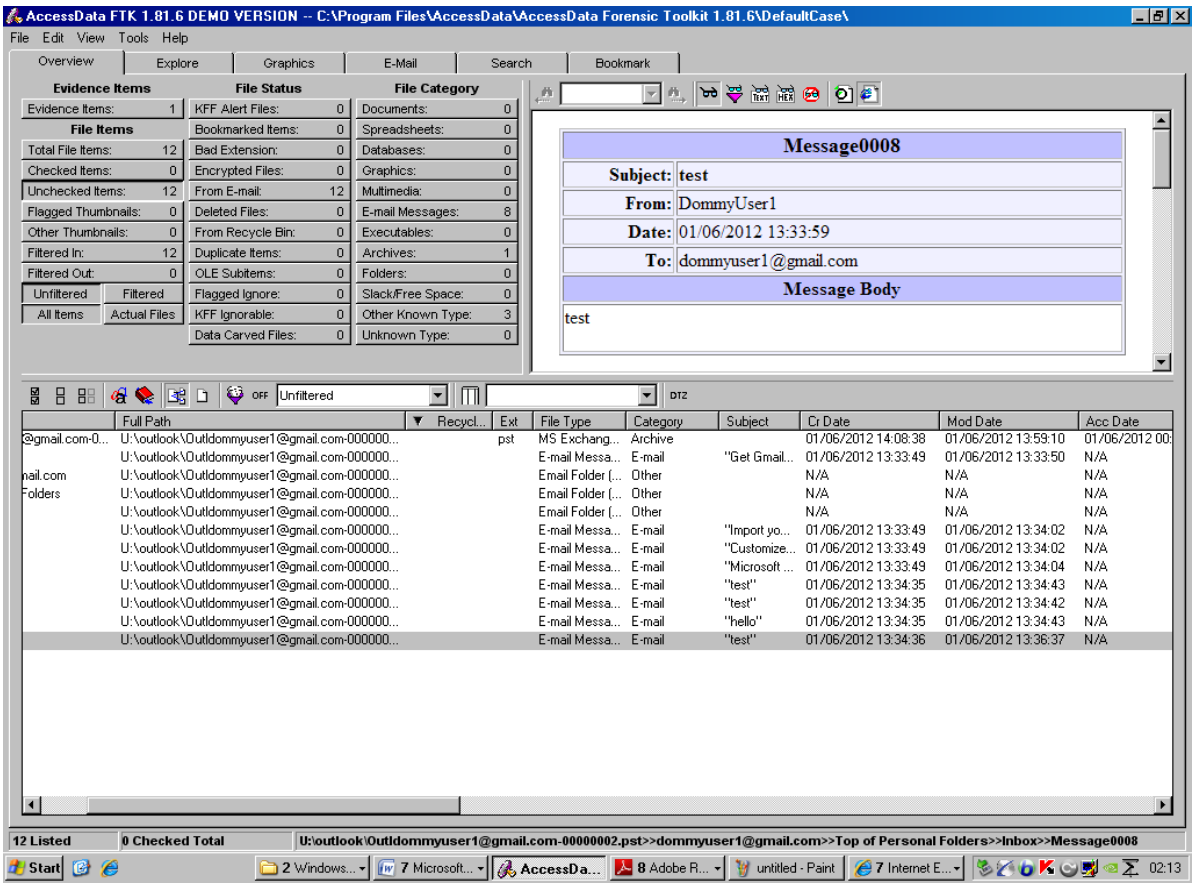


Figure 63: Viewing the file properties

This is where relevant evidence is properly stored for future references

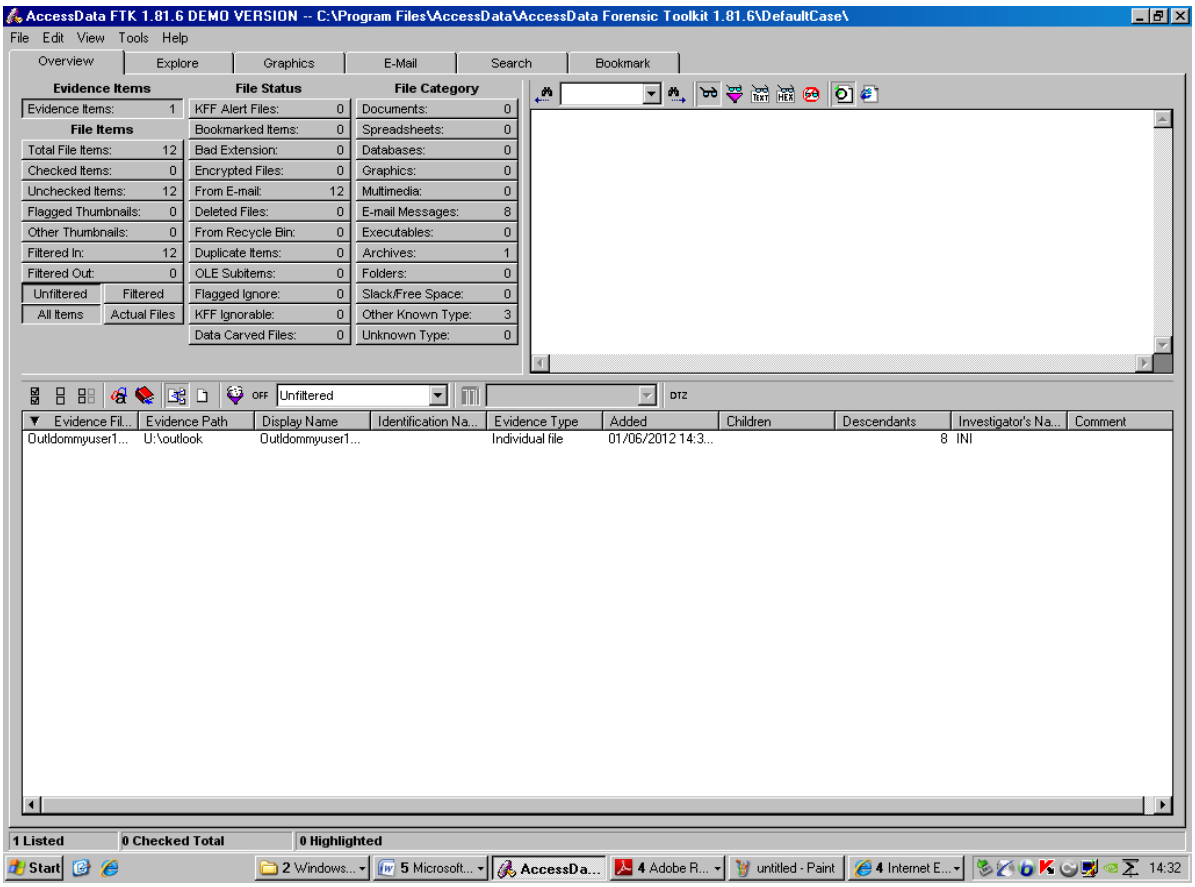


Figure 64: FTK Evidence item overview

During the examination process, the security component were made available. In the email content examination, there ensured the availability of antivirus software which automatically scan system and files at times to avoid the the infection of security threats and vulnerabilities.

5.5.4.4 Presentation Phase

After completing the digital investigation, all the findings and results is documented as a report. In the report, all investigative activities have to be written and conclusions drawn have to be explained. In this investigation FTK presented a good documentation process by generating a custom formatted report that shows the content of the case including the relevant email content as shown in the Appendix.

5.6 Summary

This chapter discussed security threats and vulnerability impact on investigation process, and the step by step approach of developing the new model. The chapter aimed to test the hypothesis by running two digital attacks investigation on different areas such as mobile network and emails using CDFIM to demonstrate the digital investigation. The researcher found that the integration of security mechanism and intelligent software when conducting digital forensic investigation could preserve the integrity of digital evidence.

In the area of mobile network, the research proposed and implemented PMIPv6 with improved buffering to minimize performance issue on handover latency and loss of data which the experiment's result identified, as able to assist in providing reliable services and in turn assist in digital investigation.

Loss of data/packet and violation of organisation's IT policy were used as methods of attack, in both cases, data were collected. The resulting data were analysed and examined using CDFIM. The researcher also found that when CDFIM was applied, regardless of the digital envioronment, the digital investigation could be conducted based on CDFIM

Chapter Six: Validation

Objectives:

- to comparatively analyse CDFIM
- to present case studies that used CDFIM in real digital devices attack
- to discuss the limitations of CDFIM

In chapter 2 and 4 the conceptualised model was introduced. The objective was to establish the digital forensic investigation process and security requirments needed in the new model. The main purpose of this chapter is to justify the digital forensic investigation process and its security requirement as a good model for digital investigation process and as a measurement for ensuring the integrity of digital evidence. It is important to demonstrate not just that a crime has been committed, but to demonstrate proofs of the intergrity of digital evidence (Pilli et al., 2010). By employing a consistent and methodical processes to establish the crime, it is important to prove the integrity of the originality of the digital information.

The conceptualised model derived from the literature review and analysis is used as a measure to identify good security level applicable to the different digital investigation. The validation process was part of the research methodology used.

6.1 Comparative Analysis

The proposed model is compared with other digital forensic models; the research finds that the main differences between CDFIM and others are as follows:

6.1.1 Preparation

CDFIM is designed for dealing with security attacks and vulnerabilities identified when conducting digital investigation, which poses threat to the integrity of digital evidence, where as other models, are general model that do not take adequate cognisance of possible threats on the integrity of digital evidence in the conduct of investigation. In the preparation phase, an organised working environment is in pace before and during digital investigation. While conducting the investigation, proper security components are made available that can avoid the occurence of security incident which can alter the integrity of digital evidence.

6.1.2 Interaction

This phase is a major advancement in the developement of digital forensic models. In CDFIM interaction phase has been designed to deal with digital information when conducting digital investigation to ensure the integrity of digital evidence collected. In this phase, the digital information is identified, maintained and distribution in a secure manner. The network protocol analyser known as Wireshark applied in the research is used as a security mechanism to monitor the network in order to ensure that, there are no abnormal activites that can distrupt the investigation and cause damage to digital evidence. Also in the area of mobile communication network, the research proposed a network-based mobility management known as the PMIPv6 with buffering function in order to deal with performance issues of handover latency and loss of data packet which can affect the integrity of digital evidence.

6.1.3 Reconstruction

CDFIM has employed reconstruction as a method of further analysis to examine the digital information collected in the previous phase (interaction) in order to identify the relationship between these pieces of digital information. Also it ensured that the

transport and storage approach to the digital evidence are conducted in a way that will secure the integrity of digital evidence. However other models do not prescribe how to securely analyse collected digital information in a way that will ensure its integrity.

6.1.4 Presentation

CDFIM emphasized on consistent documentation of the various activities conducted during digital investigation. More emphasis was made to providing detailed report which are gathered from the initial stage of the investigation to the finish. While other models do not identify at this phase presenting standard and consistent documentation of the whole process of the investigation.

6.2 Criteria of Success

The proposed model was derived from the extensive research and literature review, and result of the experiment and analysis. The development of the layers was done based on a scientific approach and each layer and sub layer was justified and backed with an academic literature. The critical success factors considered during the development of the model are:

- **Applicability:** The model must be applicable to any organisation for its information sharing. It can be observed that the model presented in this thesis is applicable to any organization. Any digital investigator can apply this model.
- **Simplicity:** The model must be clear to the intended users such as digital forensic investigators, security investigators, system administrators or individuals. The layers of the model must be explicit to non-digital forensic or security expert.
- **Flexibility**

  The model must be flexible and can be implemented in phases.

- **Doable**

  The model must be doable to the intended users.

6.3 Case Study

Since the case studies used in this research are life case scenarios the validation process was crucial to confirm model applicability.

6.3.1 Case Study 1

6.3.1.1 Background

A company relies on computer systems to perform, process, transmit, store and retrieve data. The company uses a client/server operating system. The company's IT security is responsible for securing IT resources and conducting computer forensic investiagtions.

6.3.1.2 A case of Teardrop Denial of Service Attack

A system administrator of a server in a company identified that the server was suddenly generating a large amount of network traffic, consuming considerable bandwidth. The company therefore isolated the server's portion of the network until the situation was resolved.

The initial findings of the IT security, which conducted an analysis of its system found that there was initiated teardrop denial of service attack. Figure 65 demonstrates the result of the electronic evidence using wireshark to sniff and monitor the packet on the network as shown below:

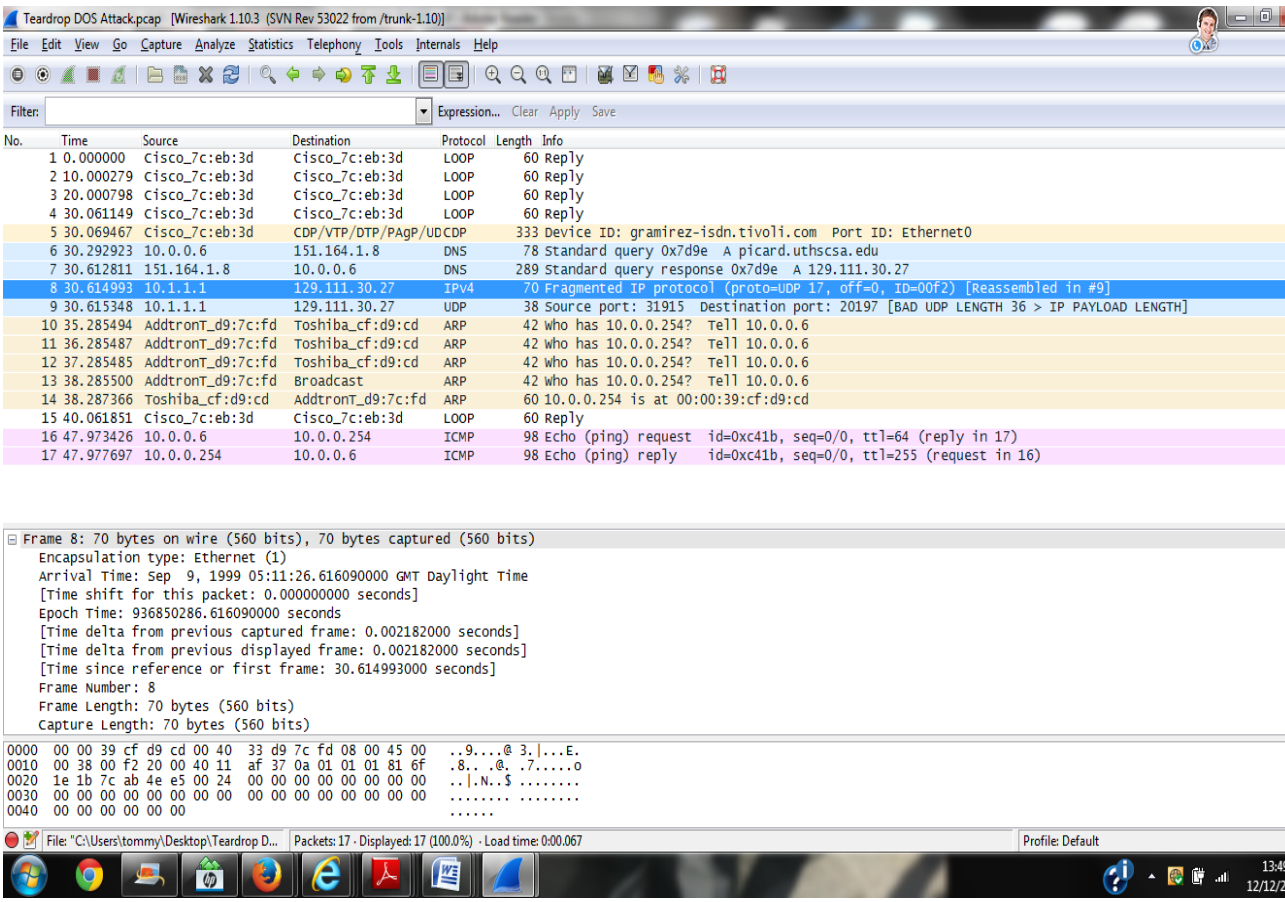


Figure 65: The result of the electronic evidence of the teardrop denial of service attack

6.3.1.3 CDFIM Findings

The CDFIM was used to conduct the investigation. The researcher identified the need for an investigation and then investigated the situation. The initial activity that was conducted by the researcher is deploying a security mechanism (protocol analyzer) called wireshark which is a packet sniffer software on the network. The wireshark was used to look at all traffic coming from or going to the suspect machine and it was also used to detect and confim incident while conducting the investigation. The digital evidence was collected using wireshark.

Proper planning is conducted on the use of tools. The physical and operational infrastructure where prepared to support the investigation. The investigative tools were properly managed and in a secured manner. While conducting the investigation,

consistent and steady use of antivirus was in place and firewalls configured to ensure minimized risk of security threat to digital information. Authorization and authentication was established by applying methods such as using username and passwords when using the systems. Secure policies were in place to implement and maintain the security of systems and digital information. The password used was securely managed to avoid any attampts of attack on the digital device and information. Proper check was made to ensure that software used was not identified with any security flaws. Secure internet connection was implemented each time there was need to connect to the internet. In order to minimize the risk of having the digital information infected with digital attacks and threats unsecure file exchange and opening of unsecure shared folders were avoided. The security guidelines were demonstrated as applicable while conducting the investigation.

The investigation revealed that packet 8 and packet 9 shows the overlapping IP Fragments in a teardrop attack. In packet 8 as seen in figure 66, result shows that a machine with the IP address source 10.1.1.1 was sending packets to the IP address 129.111.30.27. The result also shows the time rate at which these packets were being sent. A more detailed look at the contents of the packets showed the following:

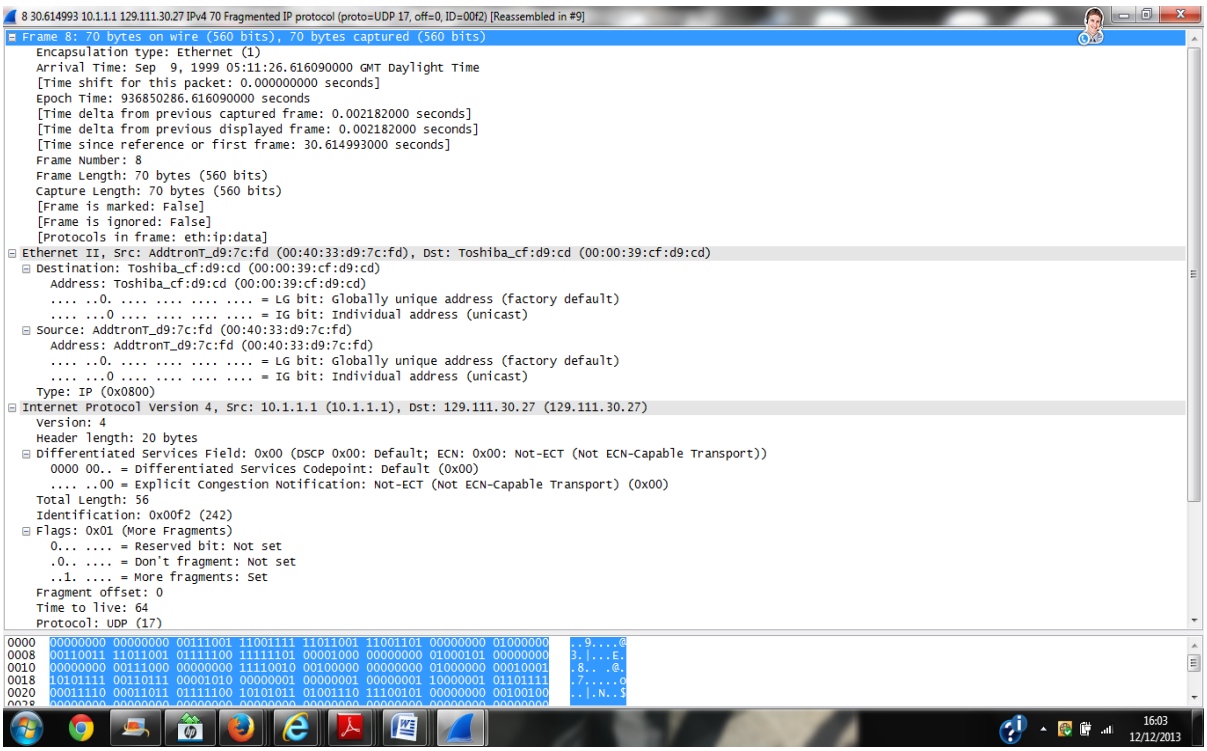


Figure 66: Packet 8 analysis result

Breaking down the packet shows that these are valid IP packet, but inside the long string of zeroes is the hexadecimal string which shows the reassemblying of the data.

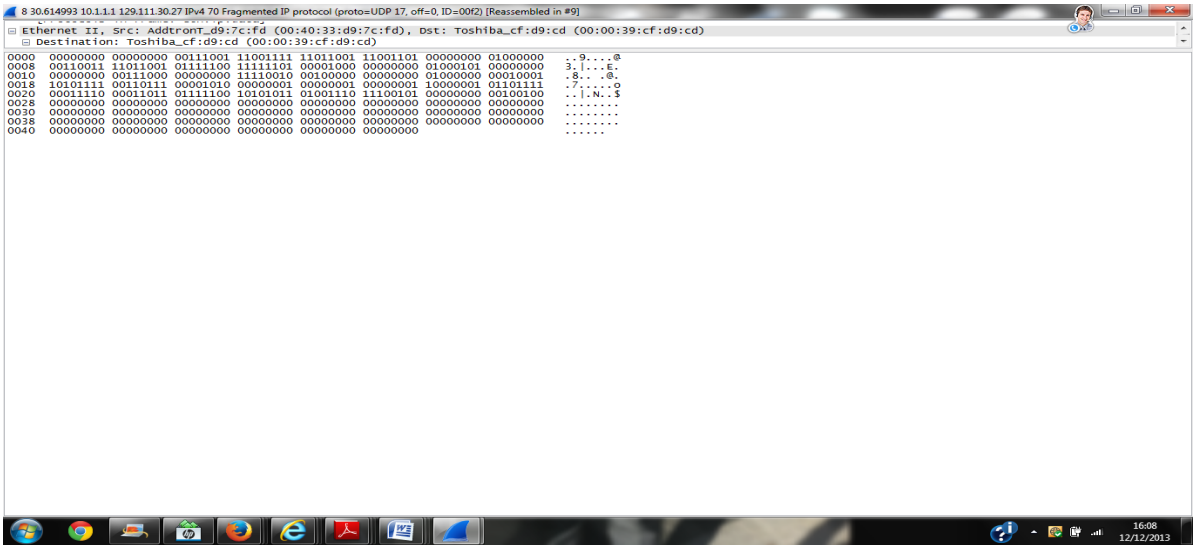


Figure 67: A detailed bit view of analysis result

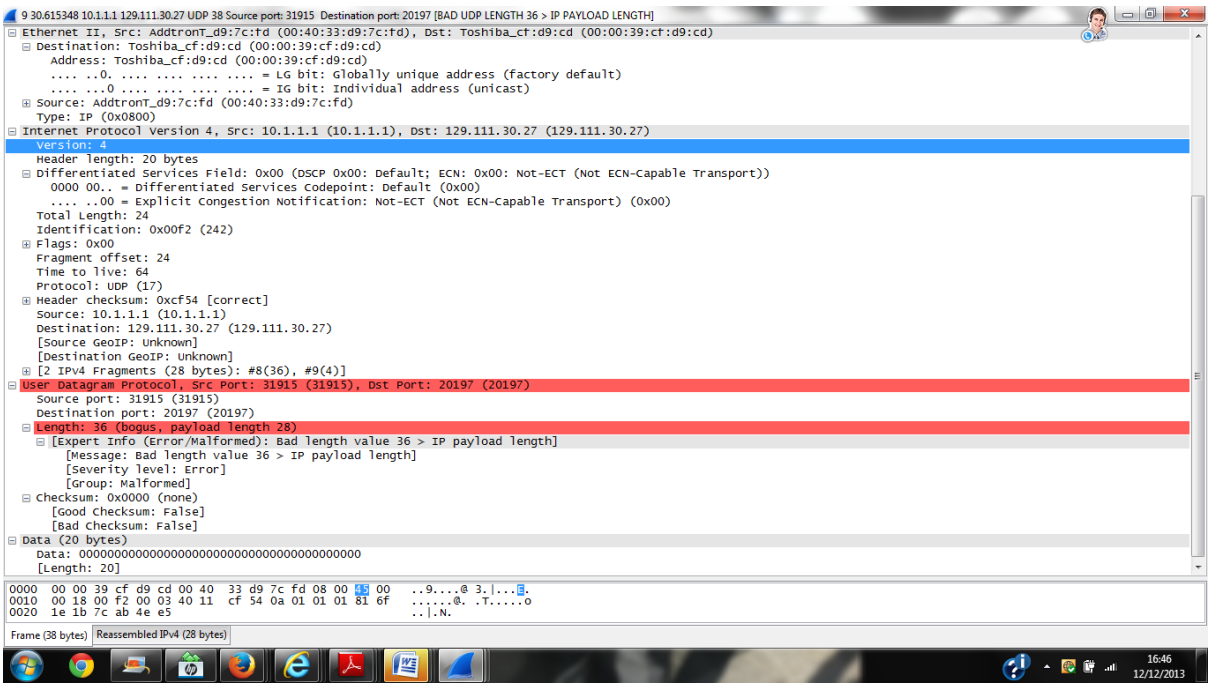


Figure 68: Using details to show security issue Teardrop DoS attack in packet 9

Figure 68 shows that in packet 9, data packets are reassembled with confusing OFFSET fields and a malformed payload sizes or length. Further analysis showed confused data fragment occurring at different sizes, this is potentially problematic to the target system. Subsequent examination of the server showed the protocol as user datagram protocol (UDP) source port as 31915 and destination port as 20197.

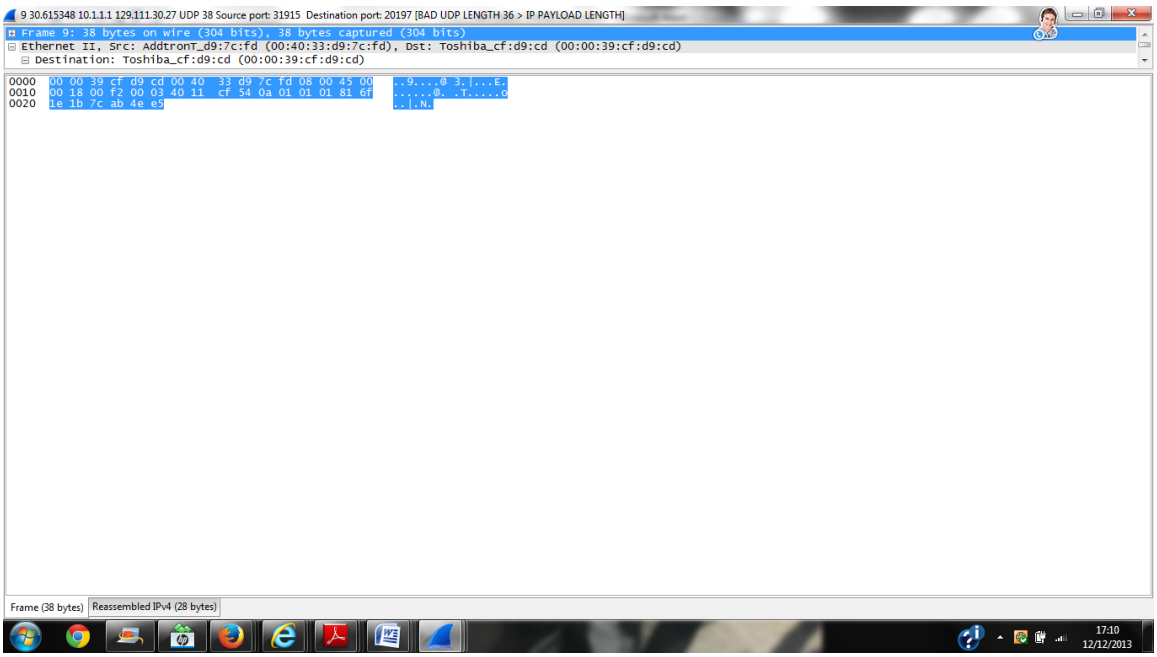


Figure 69: A detailed hexadecimal view of the reassembled packet 9

The result in this investigation identified that the target system will have no idea as how to handle this kind of data packets and reassembling the data packets according to TCP/IP or IPv4 will result in system crash or reboot. Based on the result of a reassembled packet showed in figure 69, in this research it was concluded that if a system has been exploited there is no way to know how badly it has been compromised, once the exploit is discovered, it should be assumed that the best option for the system is to be rebuilt rather than merely cleaning the server. For instance simply using "remote sysadmin" to clean the server of the known rootkit is not enough; more malware can be left in the system. With the use of a secure communication protocol, which is the IPv6, the digital evidence from this investigation, was safely transported and securely stored.

6.3.2 Case Study 2

6.3.2.1 Background

An organisation relies on computer systems to perform, process, transmit, store and retrieve data. The organisation uses a client/server operating system and performs huge daily operations on the system.

6.3.2.2 A Case of Unauthorised Access

An individual was allegly accused by an organization of illegally accessing top secret computer systems in what they claimed as the biggest military computer hack of all times. The alleged individual using his home computer, through the internet identfied the organisation's network computers with an open Microsoft windows connection and extracted the identities of certain administrative accounts and password. Having gained access to those accounts he installed unauthorised remote access and administrative software called "Remotely Anywhere" that enabled him to access and alter data upon from the organisation's computers at any time and without detection by virtue of the programme masquerading as a Windows operating system. He installed software facilitating both further compromises to the computers and concealment of his activities. Using this software, he scanned the organisation's computers for other computers and network susceptible to similar compromise. He was able to move from network to network in different location. Due alleged individual's actions, data were delected from the organisation's databases, including critical operating system files, this lead to system shut down in the organisation, disrupting the organisattion's functions.

6.3.2.3 CDFIM Findings

The CDFIM was used to conduct the investigation. Upon having knowledge of this case, the researcher identified the need for an investigation and then investigated the situation. The initial activity that was conducted by the researcher was applying the Wireshark in order to look at all traffic coming from or going to the workstation and it was also used to detect and confim incident on the workspace while conducting the investigation. Proper planning is conducted on the use of tools. The physical and operational infrastructure where made ready to support investigation. While conducting the investigation, consistent use of antivirus was in place and firewalls configured to ensure minimized risk of security threat to digital information. Secure policies were in place to implement and maintain the security of systems and digital information. The password used was securely managed to avoid any attampts of attack on the digital device and information. Proper check was made to ensure that software used was not identified with any security flaws. Secure internet connection was implemented each time there was need to connect to the internet. Also to minimize the risk of having the digital information infected with digital attacks and threats unsecure file exchange and opening of unsecure shared folders were avoided.

It can be observed that the log entry showed the downloading of files containing username and password, deleting of approximately 300 user accounts, and deleted files necessary for the operation of the computer from an FTP server with IP address 160.168.10.45 from a remote directory on the FTP server named "/home/GaryM". Timeline analysis conducted shows one of such activity carried out on the 22 February 2002 at 1600 hours as shown:

Feb 22 16:00:00 2002 160.168.10.45 780800/home/GaryM/uname.pdf a_o r user

Modem logs on the computer may show that the computer was connected to the internet at the time in question. The server logs at the alleged individual Internet Service

Provider (ISP) may show that a specific address was assigned to the alleged individual user account.

Routers connecting to the alleged individual's computer to the internet may have related NetFlow logs containing additional information about the alleged individual's connection to the FTP server logs on the FTP server may confirm that files were downloaded to the slleged individual’s IP address. For instance the following FTP server transfer log entry shows a file with the same name and size as that found on the alleged individual’s computer being downloaded to the IP address that was assigned to his computer account at the time in question. CDFIM also observed that the IP address as an identifier can be used to identify the attacker in this case. In dealing with this case, during investigation it was identified that security measures were needed to be properly followed and care was taken to ensure that digital evidence was not altered. The documentation is shown in the Appendix.

6.4 Comprehensive Digital Forensic Investigation Model (CDFIM) Limitation

It is not possible to always guarantee the success of CDFIM, because digital analysis usually depends upon output from protective security components. The basic issues confronting digital investigators in ensuring the preservation of the digital evidence is therefore as follows:

6.4.1 Mis-Configured Security Components

Security components such as firewalls or Intrusion Detection Systems (IDS) are hardware or software used to protect an organisation's system by filtering out unwanted network traffic and recording suspicious computer events. This record is essential if one is to comprehend the computer incident and the behaviour of the attacker. For example, if an IDS cannot correctly detect Trojans or any tools of hacking a loss of evidence of an attempt to attack access will result.

6.4.2 The Model's Inability to Enforce Human Intervention

Even though CDFIM can sufficiently combat security threats and vulnerabilities in its investigative process, human intervention can hugely influence the integrity of digital information. Digital investigators that ignore security guidelines and policies can affect the integrity of digital evidence.

6.4.3 Lack of Preservation of the Log Files

Digital investigators sometimes face a problem if the log files are not preserved correctly done, because the integrity of log files is affected. Attackers alter these logs upon gaining unauthorised access, thereby hiding the evidence of their crimes. In this case, it is very difficult to ensure the integrity of digital evidence. These log files should be preserved in a separate server to protect the integrity of these files.

6.5 Summary

The chapter aimed to conducts a comparative analysis by comparing current method of digital investigation and the proposed model. The researcher also discussed the challenges of this model. The researcher found that the security mechanism and guidelines incorporated in the digital investigative process are useless when digital investigator ignores the security guidelines.

This chapter also discussed this model use in the real world. The first case was the case of teardrop denial of service attack where a system administrator of a server in a company identified that the server was suddenly generating a large amount of network traffic, consuming large bandwidth. This model was able to apply the investigative process and identified that the attack took place and the incorporated security measures and guidelines ensured the integrity of the digital evidence is preserved. In the second case, an individual violates the IT policy of an organisation by gaining unauthorized access to its systems and network. The model was able to identify the attack occurred

by providing relevant information. CDFIM was also used to ensure that the integrity of the digital information is preserved.

Chapter Seven: Discussion and Evaluation

Objectives:

- to discuss the results of the experiments and case studies
- to evaluate CDFIM

This chapter of the thesis aims to discuss the result of experiment and test investigation of CDFIM. The aim of this research is to explore the use of modern technologies to avoid security threats, when considering digital forensic investigation process in an attempt to present solution that contributes to a good security level and as a measure for integrity of digital evidence.

7.1 Experiments and Case study Analysis

Due to the increased development in the communication area and various technologies involved in the delivery of information from source to destination, IP mobility is faced with increased research ideas. Also due to the increase in communication devices and different technologies, digital investigators are recently faced with increasing cases for investigation. In mobile networking, users are attracted to the requirement of roaming while maintaining the ability of having a network communications preferably without service interruption. A mobile communicating device should have the ability to move from one network to another while maintaining its normal communication and active sessions with its Correspondent mobile device. The Internet Engineering Task Force

(IETF) developed a protocol of Mobile IPv6, which is a host-based approach. Mobility IPv6 solves the issue of IP mobility. With the drive in assisting in a shift in IP mobility protocol, IETF proposed a network-based localized mobility management known as the PMIPv6. Standard PMIPv6 is faced with critical performance issues such as handover latency and packet loss.

It was observed that all the layers of the model were required after the experiment analysis. The selection was based on understanding the needs and requirement of different aspects of protection and relationship between the threats and the security measures required during digital investigation. The main target of digital investigators is to be able to present accurate and reliable digital evidence. In the area of mobile network, digital devices require support for IP mobility in order to maintain its connectivity with its peers while they move across networks and to minimize their service disruption. In this research, it has been identified that loss of data packets can be a threat to the integrity of digital evidence. Therefore, the performance issue of handover latency of mobile node and packet loss can affect the successful sending or transporting of packet therefore, influence the integrity of data packet.

Thus in this research PMIPv6 with improved buffering function is identified to minimize packet loss during mobile node handover. The purpose of the PMIPv6 with improved buffering is to assist in providing reliable service as a solution the performance issues, which not only cause long service delays but also consume more networks and system resources. This is identified in the research as able to assist digital investigation, since the network will have reliable service. It was observed in the result of the experiment conducted in chapter 5 that in the standard PMIPv6 250 packets were lost during the mobile node handover while with the PMIPv6 with improved buffering all the data packets buffered in the LMA were received by the mobile node. Furthermore, PMIPv6 with improved buffering transmitted packets quicker than the

standard PMIPv6. The result has also identified that if data are transmitted quickly it avoid the situation where system resources is used that can lead to denial of service attack. The result of the experiment also found that the use of security mechanism and guidelines with the investiagtion process based on CDFIM, enables the ability to identify the attack or incident and also ensured that the integrity of the digital evidence was preserved.

In this research, the second test examined in chapter 5 contains the realistic data used in conducting the email content investigation. In the hypothetical scenario in which a personal email account is used in a way that breaches the IT security policy of an organisation, the computer is acquired and there is need to determine the user's activities. By examining the emails and log files, it was able to confirm the activities of the user. The digital evidence was collected and FTK was used for analysis. Using the FTK, copies of the email and relevant information was found. A protocol analyser known as Wireshark was also deployed for the purpose of monitoring the network for any abnormality of the system during the investigation. The Wireshark and other security mechanism and FTK, were effectively used and managed. The investigative tools were securely protected from threats and vulnerabilities. one of the test experiment of digital investigation conducted based on CDFIM is discussed as folows:

7.1.1 Preparation

The test conducted identified the need to begin an investigation, therfore, an approach strategy was applied on how to conduct the investigation as discusse:

- **Step 1 (S1): Secure Application and Content Based Tecnology**

An organised working environment was prepared. The physical and operational infrastructures was ready to be used. Tools and applications were properly prepared and managed. During the investigation, there was need for proper security component to be

available. Security component such as antivirus, personal firewalls and secured protocol analyzer were made available and configured.

It was ensured that consistent availability of antivirus software which will detect any malicious code and stop them from infecting the workstation. The objective of this was to ensure that the risk of systems being infested with viruses and other malicious program were minimized. Since there is a huge risk of data loss when the workstation is infested with malicious programs. The Antivirus software's virus definition files was kept up to date, so that it can detect the most recent viruses. Also firewall was implemented to prevent malicious packet from entering the system or workstation. The objective of this was to prevent gaining access to digital information. In order to monitor the network traffic, a Protocol analyzer known as Wireshark was deployed in order to detect and confirm incident, event or any unusual activities that may be malicious and that can influence the integrity of digital evidence in the digital investigation. All unused port where disabled to avoid any unauthorized access that can cause disruption. For instance in monitoring the system and network, it can avoid any damaged that can be caused by denial of service. In order to ensure the integrity of the digital information, crytographic techniques were applied.

- **Step 2 (S2): Secure Policies**

The systems, tools and applications that were used during the digital investigation were authenticated using password in order to ensure that only authorized investigators had access to the digital information. The objective of this, is to avoid impersonating that can cause damage to the digital information.

- **Step 3 (S3): Secure Operational Procedures**

The investigative tools where managed properly and correctly used. Passwords were managed securely in order to avoid access to the system by unauthorized individuals

and thus, tempering with the digital information. Regular check was conducted on the security mechanism such as Antivirus to ensure that they were up to date for the purpose of accurately securing the network and systems. In the need for accessing the internet, only secure connections were made.

Step 4 (S4): Network and System Performance

The digital forensic and investigation tools were managed properly and in a secure manner. Secure operational procedures such as authorization access and methods used to monitor systems and tools were enabled during the digital investigation. Performance monitor was used to keep track of activities by monitoring performance on the server or system.

It can be observed that all the security measures or guidelines were followed to ensure a good security level of digital information. The result of the experiment shows that the use of security mechanism and guidelines with the investigation process, based on CDFIM was able to identify the attack and also ensured that the integrity of the digital evidence was preserved.

The preparation stage is where the actual reasoned examination begins, which is where concrete facts begin to take shape that support or falsify hypotheses built during the investigation. The ability to know the technologies and tools used, in addition to an understanding of the underlying mechanisms and technical principles involved are of great importance in digital investigation at this phase.

The nature and extent of a digital evidence examination depends on the known circumstances of the crime and the limitation placed on the digital investigator. In the test scenario since the crime committed was carried out in a digital scene, it was ensured that both the physical and digital environment were secured to avoid further damage done.

7.1.2 Interaction

In this phase, the digital information was identified (identification), and the location of the potential evidence from the data collected (collection) was converted to an understandable language (examination). The focus of the examination was on the specific of the case (case specific analysis). A chronological time line analysis was conducted. Duplicate copies of the data are made to ensure integrity. In the investigation, working with the recovered source information, descriptive material about the content were gathered. After the preliminary investigation, important steps that were considered in the interaction phase was the imaging of the digital information and preserving the integrity of digital evidence. This was conducted in a way that will not alter the integrity of the data. Adequate process was in place for making available safe media on which to image the data to be processed. Also the preservation of the evidence was conducted by applying the evidence processing options for indicating the cryptographic options that will be considered for ensuring the integrity of the duplicate files of the digital evidence. In the test experiment, the cryptographic options were applied as follows:

- **MD5 HASH:** This option generates an MD5 hash for all evidence files. An MD5 hash is a 128-bit generated value based upon a file's content. It is used to identify files uniquely. Hashes can be used to verify file integrity or to identify duplicates files. MD5 are used by the Known File Filter (KFF) to identify files.
- **SHA-1 HAH**: It generates a SHA-1 hash for all evidence files. A SHA1 hash is a 160-bit value. The SHA-1 hashing algorithm is newer than MD5, but has not yet been widely used. This algorithm is not used in the KFF comparison and cannot be added to the KFF hash database but can still be used to identify a file uniquely through a manual comparison.

- **SHA-256:** Generates a SHA-256 hash (newer than sha-1) for all evidence files. SHA-256 hash values are not used in the KFF comparison and cannot be added to the KFF hash database but can still be used to identify a file uniquely through a manual comparison.
- **Fuzzy Hash:** This generates Fuzzy Hash for all evidence items.
- **KFF:** The KFF is a utility that compares file hashes against a database of hashes for known files.

All the security measures and guidelines from Step 1 - 4 were followed to ensure proper distribution, examinaing and preserving the integrity of digital evidence. The PMIPv6 proposed and implemented in this research to address handover latency and loss of data can provide reliable services. This can asssit digital investigation.

7.1.3 Reconstruction

In the reconstruction phase, the security guidelines were consistently applied. This phase involves bringing together the result of relevant information/activities from the earlier parts of the process and any other relevant information which investigators may have obtained to provide a detailed account of the events and actions at the crime scene. This phase ensures that all activities conducted in collecting the relevant digital information properly adhere to the security measures. Also the secure transportation and storage of the digital evidence was paramount in this phase. Therefore proving the integrity of the digital evidence. The protocol analyser was used as the security mechansim which enusres consistent monitoring of the network of the workstation to detect and confirm any incident that can affect or influence the integrity of the digital evidence.

Considering the case example of the indiviudal that gained unauthorized access to an organization's systems, the IP mobility identified in this research was applied as a

solution to the case. IP addresses has two roles as locators and identifiers. IP addresses are locators that specify by means of the routing system, how to reach the mobile mode such as communication device or network interface which is using a specific destination address. The routing system keeps information about how to reach different sets of addresses that have a common network prefix. On the other hand IP addresses are also identifiers used by protocol such as the TCP to identify the endpoints of a communication channel, also names of mobile nodes are translated by the Domain Name System to IP addresses therefore playing the role of node identifiers.

Mobility involves separating the identifier role from the location one. From the identification view, the IP addess of a mobile mode should never change but from the location point of view the IP address should change each time the mobile node moves, showing its current location. The IP mobility solution identified in this research provide mobile nodes with a permanent address known as the Home Address (HA) to be used as identifier and the and a temporal address known as the Care-of Address (CoA) to be used as locator. Therefore in the above mentioned case the IP addresses can be used to identify the offender. In order to overcome the performance issue of handover latency and packet loss in Mobile IPv6, as shown in the result of the experiment, PMIPv6 with impoved buffering was implemented to minimize handover delays and packet loss. Therefore, this can assist as a solution to avoid a situation of denial of service which can be caused by handover latency in mobile devices leading to utilization of network resouces which can cause data packet loss by this, affecting the integrity of digial information.

7.1.4 Presentation

In the test investigation, while all the necessary security measures were still in place. All findings in the course of the investigation where carefully outlined and documented. Documenting established digital evidence requires integrating all findings and

conclusions into a final report that explains the findings to others, in some cases the investigator may have to present in court, but this is beyond the scope of this research. Report writing is an important stages of the digital forensic process because it is the only view that others have of the entire process. In this investigation FTK presented a good documentation process by generating a custom formatted report that shows the content of the case including the relevant email content as shown in the Appendix.

7.2 Summary

This chapter discussed the experiments results and evaluate the Comprehensive Digital Forensic Investigation Model. During the investigation, it was important to ensure that all the investigation processes were conducted ensuring that the security mechanism were available and all neccessary security guidelines followed. The model discussed can be used to define tools for supporting investigations. It is important for any digital investigation to be able to prove the integrity of digital evidence. One way that this can be achieved is for investigators to ensure that security mechanism and policies were followed during the invesitgation. And also the security mechanisms must be integrated in the investigation process to ensure that digital information are secured from security threats and vulnurabilities that can alter digital object such as the computer and its information hence altering the digital evidence.

Chapter Eight: Recommendations

Objectives:

- to enhance security mechanism to assist digital investigation
- to improve the preservation process of digital investigation

This chapter provides a number of recommendations as methods to enhance the performance of a system, prevent data loss therefore assisting digital investigation, and improve the process by which digital investigators apply authentication techniques for securing digital data. This chapter also improves the process of digital investigation by recommending preservation methods. These recommendations will lead to improvements in the process of digital investigation.

8.1 Recommendation for Enhancing Systems and Tools Authentication

Passwords are the most used method for authentication. Although, there are lots of problems faced with password authentication such as password guessing, cracking, eavesdropping and users writing down password in an open place. There is need for digital investigators to enhance their authentication techniques in order to prevent attackers gaining their passwords applied to systems and tools used during investigation. In order to enhance the password used, the following should be considered:

8.1.1 Implementation of Multifactor Authentication

The use of simple and easy passwords makes the password vulnerable to attack. Hence, in multifactor authentication, passwords depend on something the user know (PIN),

have (smart card), and are (biometrics) in order to enhance authentication. The researcher believes that the use of multifactor authentication can prevent attackers from gaining investigators credentials, accessing the gathered digital evidence and then altering the evidence thereby endangering the integrity of such evidence.

8.1.2 Password Salting

Users often apply simple authentication methods such as user-name and passwords. This assumes only a reduced security requirement because these passwords are easy and not difficult to guess. In order to prevent password cracking or guessing, password is randomly salted before it is hashed which is the addition of pseudorandom data to a message before it is hashed, so that dictionary attack cannot be conducted. Hashing is a fast computation; therefore computing a few extra thousand digest for all the words in the dictionary makes a brute force attack more difficult to carry out.

8.1.3 Implementing Password Complexity

This is applying passwords and ensuring that they are strong and complex. For instance, passwords should not be the user's pet name, full name or dictionary word but it must contain characters, digits and symbols. A password should consist of at least a specific number of characters and numbers, enforcing password length.

8.2 Ensuring Integrity of Digital Evidence using Keyed Hash Functions

A data hashes to the same digest no matter how many times it is computed. The only way to change a created digest is by changing the message; this feature provides the proof of data integrity. Digital investigator must be able to verify that data was not altered in any way. Most hash functions do not require any type of key to create their digests but there are hash functions designed to require keys. The reason for this is that even though they have all of the same principles as a normal hash function they also

have additional property of the digest not able to be created without the proper key. Being able to create a data key combination that hashes to the same digest should be computationally corresponding to counting through all the keys.

8.3 Implementing Intrusion Prevention Systems

Firewall filters incoming packets while intrusion detection system monitors the packets and activity on a network and sends alerts if there is malicious activity. There is need for a more proactive approach for providing good level of security. Unlike intrusion detection systems, an intrusion prevention system (IPS) monitors the packet and activity, and in the case of malicious traffic, IPS deals with it immediately. A host intrusion prevention systems (HIPS) can be installed on the systems that needs to be protected. In addition, network intrusion prevention systems (NIPS) can be installed to protect the entire network and all devices that are connected to it, which monitors network traffic and immediately react to block a malicious attack or incident. The researcher believes that the use of IPS during digital investigation can assist in dealing with malicious activity that can disrupt the investigation and alter the integrity of digital evidence.

8.4 Recommendation for Enhancing Digital Resource Performance

An enhanced network and system performance can assist in digital investigation. When the performance of a system and network is normal, there is a minimise risk of incident that can cause loss of data. For instance, when there is high rate in usage of network bandwidth, this can be a DoS attack.

8.4.1 Enhancing Digital Resource Performance

PMIPv6 with buffering function can be used to improve service reliability. PMIPv6 with buffering function can assist in minimising packet loss during mobile node

handover. When applying route optimization without a buffering function, the out-of-sequence problem occur, which is packets arriving out of order because of the gap of transmitting time through optimized paths. Thus, causing increased network load and service delay, providing unreliable services. In implementing PMIPv6 with improved buffering function, this provides reliable services and minimise loss of data packets. Therefore, it can improve digital investigation since the loss of data affects the integrity of digital evidence.

8.4.2 Enabling IPv6 Traffic using 6to4 for Encapsulation

Most organizations use a client/server network environment and they rely on computer systems to perform process, transmit, store and retrieve data. Packet flushing that does not consider network bandwidth is the reason behind rapid network load and packet loss. In an organisation, this could result to performance issues and loss in data while in digital forensic investigation it could cause the issue of loss in data leading to compromise in the integrity of digital evidence. Every organisation or individual that makes use of the network including digital investigators are interested in high performance of the network. Therefore there is consistent need of analysing the response times in a network, this can assist in ruling out latency issues.

There is need for more internet traffic to be carried through tunnel as the internet infrastructure migrates from IPv4 to IPv6. Envisaging this, figure 69 shows the use of IPv6 traffic with 6to4 for encapsulation.

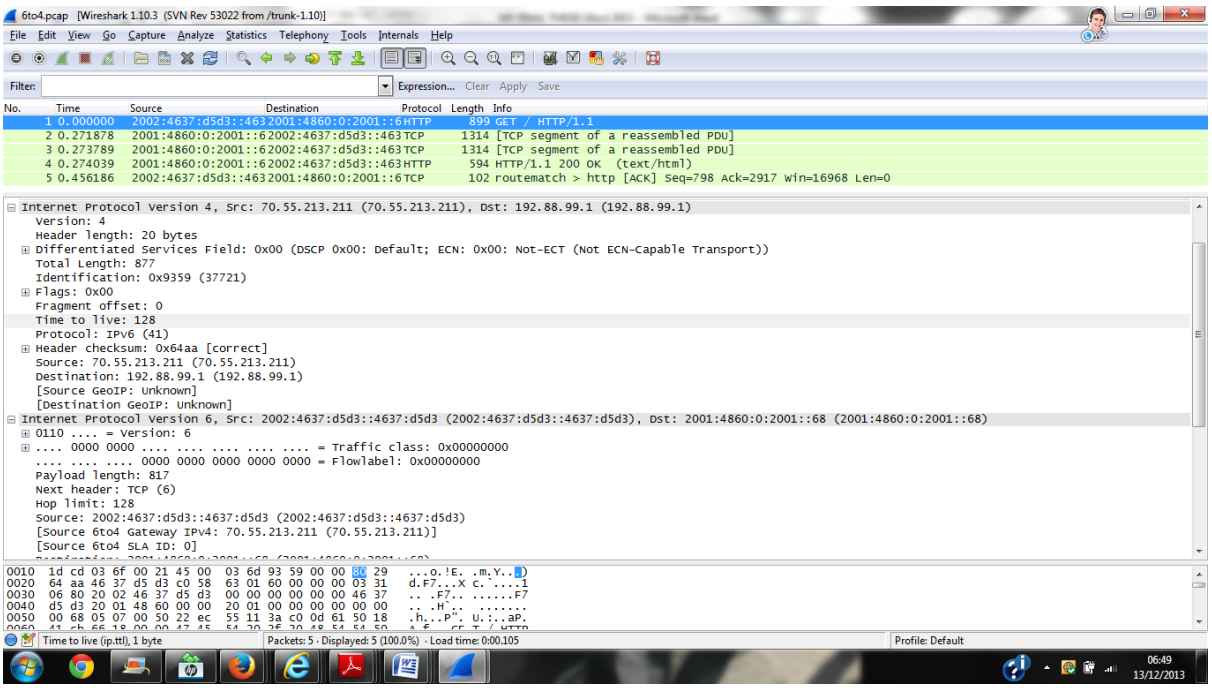


Figure 70: Using IPv6 with 6to4 for Encapsulation

Figure 70 shows that packets were sent to the IP address 192.88.99.1. The 6to4 global address used is 2002:4637:d5d3::4637:d5d3. Further analysis shows that IPv4 uses 32-bit addresses and can support many devices connected directly to the internet while IPv6 uses 128-bit addresses and supports a virtually unlimited number of devices. This can be of great assistance in the area of digital forensic investigation where the need for investigating digital devices on the network is growing tremendously.

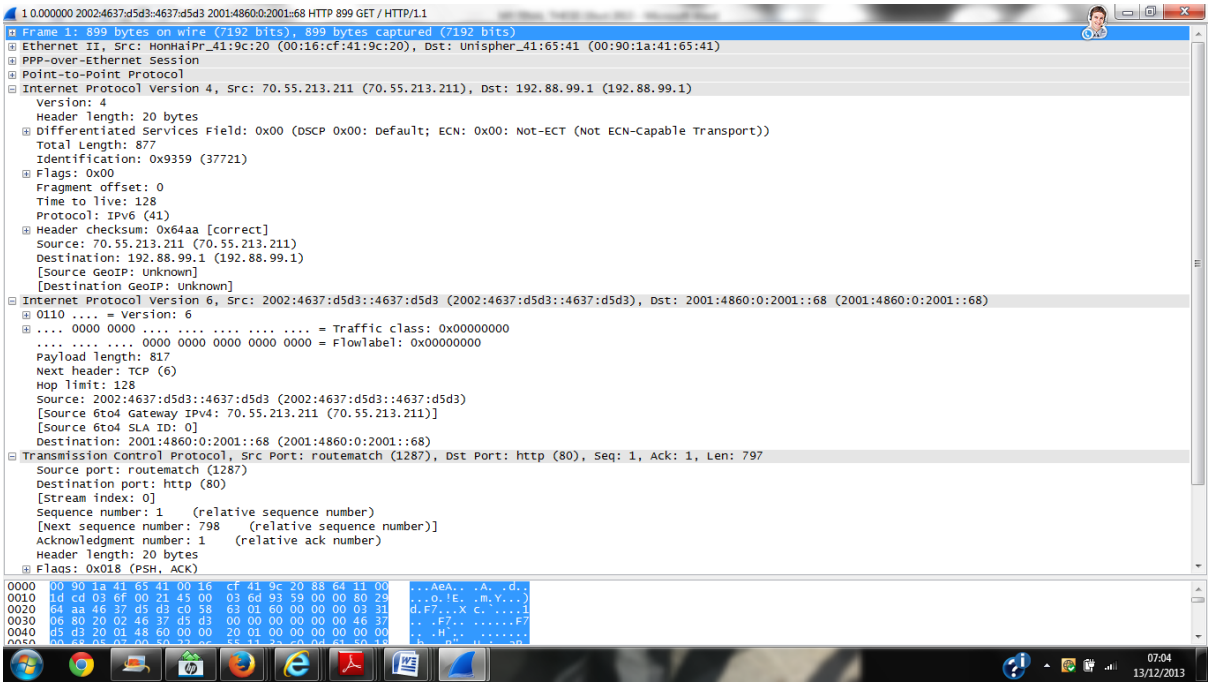


Figure 71: Using 6to4 techniques by encapsulating IPv6 in IPv4 header

As shown in figure 71 6to4 is a tunnelling technique for connecting IPv6 host or networks to each other over an IPV4 backbone. The networks can connect to the IPv6 internet using an IPV4 connection in 6to4 methods. A major benefit of 6to4 is that it does not require configured tunnels; it can be implemented in border routers without a great deal of router configuration.

8.5 Summary

This chapter has identified some recommendations. These recommendations would improve the digital systems and tools authentication such as enhancing password policy and enabling muitifactor password and password salting. They would also improve the performance for digital resources which in turn assist digital investigation. Furthermore, the researcher suggests the implementation of keyed hash function in order to ensure that the integrity of digital evidence is preserved. Also the researcher recommends the inplementation of intrusion prevention systems which can assist in monitoring traffic

and immediatly react to block malicious attack or incident that can alter the intergrity of digital evidence.

The researcher also suggests implmenting PMIPv6 with improved buffering function and IPv6 traffic using 6to4 for encapsulation in order to improve performance, minimise data loss and ensure service reliability. These recommendations will assist and improve the process of digital investigation.

Chapter Nine: Conclusion

9.1 Conclusion

This research has established the importance of the use of modern technologies, identifying security threats when conducting digital forensic investigations in order to present solution that correctly identify suspect, also solution that contributes to a good security level and as a measure for integrity of digital evidence.The need for a security mechanism that contributes to a good security level of digital forensic investigation process and as a measurement tool for the intergrity of digital evidence should not be ignored . Due to the fragile nature of digital evidence, it must be handled properly, carefully and accurately to be able to prove its integrity. Once digital evidence is established, its integrity is assessed to determine its probative value. If there is concern that the evidence was tampered with prior to collection, during and after collection, these doubts may reduce the weight assigned to the evidence.

The research reflects on the importance of integrating system mechanism and intelligent software in conducting digital investigation, also serving as a measurement tool for the integrity of digital evidence. A model was then constructed, CDFIM, that builds on current models in order to fulfil this function.

The research identified the main issues facing digital investigators involved in conducting digital investigation. Firstly, the need to be able to attain and maintain the integrity of digital evidence. Secondly, security attacks and vulnerabilities on digital resources such as system, mobile communication devices and networks may affect the integrity of digital evidence. Thirdly, there is no comprehensive model for digital

forensic investigation that identifies mobility IP as an approach to assist in the integrity of digital evidence.

The research collectively identified the major activities of the investigative process conducted during digital investigation in four phases. It was also understood in the research that successful digital investigation should depend not only on the investigative process but also on the integration of security mechanism, which assist in the integrity of digital evidence.

The Comprehensive Digital Forensic Investigation Model (CDFIM) was therefore created by developing upon the investigative process used by other models. The model is an advancement on existing models in its comprehensive nature to address security issues faced in digital investigation. CDFIM includes preparation, interaction, reconstruction and presentation phase. The interaction phase is a major phase introduced in this research which assist in the distribution and maintaining of information during and after the investigation. The collection, transportation and maintaining the integrity of information is a major key aspect of supporting the work of investigators and it can be a fruitful area for the development of advanced applications The model is easy to understand and can be used by even non-expert individuals with management responsibility for digital devices. The CDFIM presented in this thesis can be used for multiple real cases such as computer forensics, network forensics and email forensics.

The test of the hypothesis was by conducting experiment, and test case investigation covering possible attacks that can affect the integrity of digital evidence. In the area of mobile network, PMIPv6 with improved buffering was proposed and implemented to address performance issue to provide reliable services, which can assist digital investigation. The experiment results based on current approach of managing network-

based IP mobility, which is the standard PMIPv6, and the proposed method of PMIPv6 with improved buffering are compared, the results identified that during handover in mobile node the application of PMIPv6 with improved buffering assisted in minimizing handover latency and loss of data packets. In addition, a case of violation of an organisation's IT policies was examined and used to test the research hypothesis and the applicability of the model. The model was used to deal with and investigate two real cases.

The success of research presented in this thesis has been measured according to the following criteria:

1. **Evaluation:** This research conducted a network experimental test which is based on standard PMIPv6, buffering and PMIPv6 with improved buffering set up to carry out attacks by analysing performance measures which are handover latency and loss of data packet. Current method of network-based IP mobility management (PMIPv6) was compared to PMIPv6 with improved buffering. In addition, a test case was investigated evaluating the proposed investigative process of CDFIM.
2. **Comparative Analysis:** The investigative process approach used in CDFIM was compared with methods of other models.
3. **Case Study:** Two real cases used this model to identify whether incident/attacks were carried out and envisage attack during digital investigation that can pose as threat to the integrity of digital evidence thereby applying precaution (security guidelines/measures) to avoid such threat. The first case concerned the system administrator of a server in a company who identified that the server was suddenly generating a large amount of network traffic, consuming increased bandwidth. CDFIM was used to determine whether this attack occurred. CDFIM

indeed found that the attack occurred and followed security guidelines/measures that ensure the integrity of the digital evidence.

In the second case, it was alleged that an unauthorised access was gained into a network by using a piece of software retrieving stolen username and passwords and a number of files were accessed and downloaded, data was deleted from the organisation's database and there was system shutdown causing disruption and damage to the organisation. However, CDFIM revealed that there were links between the activities carried out by the individual. CDFIM also revealed the use of internet protocol to create a relationship between an activity and the attacker. CDFIM also followed security measures that ensure the integrity of digital evidence.

The researcher also discussed the limitations of CDFIM. One of these is the model's inability to enforce human intervention, digital investigators that ignore security guidelines and policies can affect the integrity of digital evidence. Another limitation of the model is mis-configured security components. Security components such as firewalls or Intrusion Detection Systems (IDS) are hardware or software used to protect an organisation's system by filtering out unwanted network traffic and recording suspicious computer events. This record is essential if one is to comprehend the computer incident and the behaviour of the attacker. However, if the IDS is not deployed correctly in a way that it can detect attack, a loss of digital evidence can occur. In addition, another difficulty faced by the model is lack of preservation of the log files, if log files are not preserved correctly, the integrity of log files is affected.

9.2 Future Work

Implementation of improved cryptographic systems/techniques

Based on the experimental results, it is important to apply cryptographic techniques available with the forensic investigative tools in order to preserve the integrity of the digital data. The researcher believes that studies should be conducted to identify more improved cryptographic systems or techniques that should be applied in order to improve the process of preserving digital data.

Developing CDFIM

Another task for future research is the development of CDFIM to work automatically as an investigation tool that will lead to the preparation, interaction and reconstruction of digital evidence, ensuring that the integrity of the evidence is preserved and presenting the digital evidence in a way that is easily understood and admissible.

The researcher believes that CDFIM can be applied to investigations into various types of attack/incidents such as data loss, information theft, email abuse and denial of service. The researcher suggests improving this model by using it to conduct investigation into different future digital attacks and preserve the integrity of the digital evidence.

A major task for future research is the development of CDFIM to work automatically as an investigative and security tool that will support in digital investigation and assist in preserving the digital evidence. The researcher believes that CDFIM can be applied to investigations into various types of attacks or offence.

References

Ademu, I. Imafidon, C. Preston, D. (2011a) 'Intelligent Software Agent Applied to Digital Forensic and its Usefulness', *National Conference on Research Trends in Computing Science and Technology* 2 (1,2) 7 September 2011, pp. 117-120. Available at: http://interscience.in/IJCSI_Vol2Iss1/IJCSI_Paper_21.pdf (Accessed: 10 April 2012)

Ademu, I. Imafidon, C. I. Preston, D. (2011b) 'A New Approach of Digital Forensic Model for Digital Forensic Investigation', *International Journal of Advanced Computer Science and Applications (IJACSA)* 2(12) 10 December 2011, pp. 175-178. Available at: http://thesai.org/Downloads/Volume2No12/Paper%2026-A%20New%20Approach%20of%20Digital%20Forensic%20Model%20for%20Digital%20Forensic%20Investigation.pdf (Accessed: 28 April 2012)

Ademu, I. Imafidon, C. Preston, D. (2012a) 'The Need for Digital forensic Investigative Framework', *International Journal of Engineering Science and Advanced Technology (IJESAT)* 2 (3) 15 May 2012 pp. 388-392. Available at: http://www.ijesat.org/Volumes/2012_Vol_02_Iss_03/IJESAT_2012_02_03_01.pdf (Accessed: 25 May 2012)

Ademu, I. Imafidon, C. (2012b) 'The Need for a New Data Processing Interface for Digital Forensic Examination', *International Journal of Advanced Research in Artificial Intelligence (IJARAI)* 4 July 2012 1(4), pp. 7-11. Available at: http://www.docstoc.com/docs/138237864/Paper-2-The-Need-for-a-New-Data-Processing-Interface-for-Digital-Forensic-Examination (Accessed: 5 January 2014)

Ademu, I. Imafidon, C. (2012c) 'Digital Forensic Acquisition and Analysis Tools and its Importance', *11th International* Conference *on e-Learning, e-Business, Enterprise*

Information System, and e-Government (EEE'12) Las Vegas, Nevada, USA, July 16-19, 2012 Las Vegas: WORLDCOMP

Available at: http://world-comp.org/p2012/EEE7656.pdf (Accessed: 12 January 2014)

Ademu, I. Imafidon, C. (2012d) 'Agent-Based Computing Application and its Importance to Digital Forensic Domain', *14th International Conference on Artificial Intelligence (ICAI'12)* Las Vegas, Nevada, USA, July 16-19, 2012 Las Vegas: WORLDCOMP Available at: http://world-comp.org/p2012/ICA7716.pdf (Accessed: 15th January 2014)

Ademu, I. Imafidon, C. (2012e) 'The Influence of Network on Digital Forensic' *11th International Conference on Wireless Networks (ICWN'12)* Las Vegas, Nevada, USA, July 16-19, 2012 Las Vegas: WORLDCOMP Available at: http://world-comp.org/p2012/ICW7717.pdf (Accessed: 12 January 2014)

Ademu, I. Imafidon, C. (2012f) 'Applying Security Mechanism to Digital Forensic Investigation Process', *International Journal of Emerging trends in Engineering and Development (IJETED)* 7(2) 10 November 2012 pp. 128-133. Available at: http://rspublication.com/ijeted/nov12/15.pdf (Accessed: 12 January 2014)

Ademu, I. Imafidon, C. (2012g) 'The Influence of Security Threats and Vulnerabilities on Digital Forensic Investigation', *International Journal of Computer Application* (IJCA) 6(2) pp. 1-6 18 December 2012, Available at: http://rspublication.com/ijca/dec%2012/1.pdf (Accessed 10 January 2014)

Ademu, I. Imafidon, C. (2013) 'The Importance and Need for Digital Forensic Investigative Framework', *International Conference on Artificial Intelligence (ICAI'13)* Las Vegas, Nevada, USA, July 22-25, 2013 Las Vegas: WORLDCOMP Available at:

http://world-comp.org/proc2013/icai/ICAI_Contents__Vol_II.pdf (Accessed: 10 January 2014)

Adler, K. (2010) *Dubai Hamas Murder: 'Fake Passport' Inquiry Launched.* London: BBC News. Available at: http://news.bbc.co.uk/1/hi/world/middle_east/8520227.stm (Accessed: 24 August 2011)

Agawal, A. Gupta, M. Gupta, S. and Gupta, C. (2011) '*Systematic Digital Forensic Investigation Model'*, 5(1) Available at: http://www.cscjournals.org/csc/manuscript/Journals/IJCSS/volume5/Issue1/IJCSS-438.pdf (Accessed: 30 June 2011)

Aggarwal, S. Duan, Z. Kermes, L.and Medeiros, B (2008) *E-Crime Investigative Technologies* Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04439186 (Accessed: 5 April 2012)

Altheide, C. Carvey, H. (2011) *Digital forensics with Open Source Tools* pp 26–27 Waltham: Elsevier

Anderson, R. (2001) *Security Engineering: A Guide to Building Dependable Distributed Systems.* New York: Wiley

Ashcroft, J. (2001) *'Electronic Crime Scene Investigation: A Guide for First Responders'*, Available at: https://www.ncjrs.gov/pdffiles1/nij/187736.pdf (Accessed: 20 October 2011)

Baryamureeba, V. Tushabe, F. (2004) *'The Enhanced Digital Investigation Process'*, Available at: http://www.dfrws.org/2004/bios/day1/tushabeEIDIP.pdf (Accessed: 15 June 2011)

Beebe, N. Clark, J (2004) '*A Hierarchical Objectives-Based Framework for the Digital Investigation Process'*, Available at: http://www.dfrws.org/2004/bios/day1/BeebeOjiFrameworkforDI.pdf

(Accessed: 18 August 2011)

Biros, D. Weiser, M. Witfield, J. (2007) *'Managing Digital Forensic Knowledge: An Applied Approach'*, Available at: http://ro.ecu.au/adf/11 (Accessed: 5 April 2011)

Blaxter, L. Hughes, C. Tight, M. (2006) *How To Research* 3rd edn. Berkshire: McGraw Hill House.

Bolt, S. (2011) XBOX 360 Forensics: *A Digital Forensic Guide to Examining Artefacts* Burlington: Elsevier

Bradshaw, J. (1997) *Software Agent*. London: MIT Press

Bryman, A. (2004) *Social Research Methods*. 2nd edn. Oxford: Oxford University Press

Carrier, B. Spafford, H. (2003) *'Getting Physical with Digital Forensic Process'*, 2(2) Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.76..pdf (Accessed: 20 August 2013)

Carrier, B. Spafford, H. (2006), *Categories of Digital Investigation Analysis Techniques Based on the Computer History Mode* Available at: http://dfrws.org/2006/proceedings/16-carrier.pdf (Accessed: 12 September 2013)

Carrier, B. (2003) *'Defining Digital Forensic Examination and Analysis Tools using Abstraction Layers'*, 1(4)

Available at: http://www.cerias.purdue.edu/homes/carrier/forensics (Accessed: 20 September 2013)

Casey, E. (2002) *Handbook of Computer Crime and Investigation: Forensic Tools and Technology. London*: Elsevier Academic Press

Casey, E. (2004) *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet.* 2nd edn. London: Elsevier Academic Press.

Casey, E. (2009) *Handbook of digital forensics and investigation.* London: Elsevier

Chaikin, D. (2007) '*Network Investigation of Cyber Attacks: The Limits of Digital Evidence'*, Available at: http://www.springerlink.com/content/g002057l01381lgw/ (Accessed: 18 March 2011)

Champlain, J. (2003) *Auditing Information Systems. 2nd edn.* New York: Wiley

Ciampa, M. (2007) *Security Awareness: Applying Practical Security in Your World.* 2nd end. Boston: GEX

Ciampa, M. (2009) *Security + Guide to Network Security Fundamentals.* 3rd edn. Boston: Course Technology

Ciardhuain, S. (2004) '*An Extended Model of Cybercrime Investigation*' Available at: www.ijde.org/citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.80...

(Accessed: 11 August 2011)

Cohen, F. (2008) '*Challenges to Digital Forensic Evidence'*, Available at: http://experts.all.net/Talks/CyberCrimeSummit06.pdf (Accessed 13th August 2010)

Cole, E. Krutz, R. Conley, J. Reisman, B. Ruebush, M. Gollman, D. Reese, R. (2007) *Network Security Fundamentals.* USA: Wiley

Conotter, V. (2011) '*Active and Passive Multimedia Forensic'*, International Doctorate School in Information and Communication (PhD). University of Trendo. Available at:

http://eprints-phd.biblio.unitn.it/575/1/Conotter_PhD-Thesis.pdf (Accessed: 15 September 2013)

Creswell, J. (2003) *Research Design: Qualitative, Quantitative and Mixed Methods Approaches.* 2nd edn. Thousand Oaks: SAGE

David, M. Sutton, C. (2004) *Social Research.* London: SAGE

Dulaney, E. (2009) *CompTIA Security + Study Guide.* 4th edn. Indiana: Wiley

Egli, P. (2013) '*PMIPv6 Proxy Mobile IPv6 RFC5213'*, Available at: www.indigoo.com/dox/itdp/12_MobileWireless/PMIPv6.pdf (Accessed: 15 June 2013)

Farrell, P. (2009) *A Framework for Automated Digital Forensic Reporting*, Naval postgraduate School California. Available at: http://cisr.nps.edu/downloads/theses/09thesis_farrell.pdf (Accessed: 20 March 2012)

Freiling, F. Schwittany, B. (2007) '*A Common Process Model for Incident Response and Computer Forensic'*, Available at: http://whitepapers.hackerjournals.com/wp-content/uploads/2010/06/A-Common-Process-Model-for-Incident-Response-and-Computer-Forensics.pdf (Accessed: 17 April 2010)

Filipe, B. Santos, S. (2011) '*Localised Mobility Management Protocol Implementation using PMIPv6'*, Available at: http://ria.ua.pt/bitstream/10773/7198/1/5456.pdf (Accessed: 20th March 2013)

Furuseth, A. (2005) '*Digital Forensic: Methods and Tools for Retrieval and Analysis of Security Credentials and Hidden Data'*, Available at: http://www.diva-portal.org/diva-1342-1_fulltext.pdf (Accessed: 20 February 2012)

Gonzalez, A. Javier, G. (2009) '*Crime Scene Measurements can be taken from a Single Image'*, Available at: http://www.sciencedaily.com/releases/2009/12/091201102338.htm (Accessed: 13 February 2011)

Gordon Brown (2010) *Dubai Hamas Murder: 'Fake Passport' Inquiry Launched.* London: BBC News Channels Available at: http://news.bbc.co.uk/1/hi/8520227.stm (Accessed: 20 August 2011)

Gray, D. (2004) *Doing Research in the Real World.* New Delhi: SAGE

Graves, K. (2010) *Certified Ethical Hacker Study Guide.* Indiana: Wiley

Gundavelli, S. Pularikkal, B. Koodli, R. (2013) '*Applicability of Proxy Mobile IPv6 for Service Provider Wi-Fi Deployment;*, Available at: http://www.potaroo.net/ietf/all-ids/draft-gundavelli-netext-pmipv6-wlan-applicability-06.txt (Accessed: 25 October 2013)

Gupta, G. Mazumdar, C. Rao, M. (2004) *Digital Forensic Analysis of Emails: A Trusted Email Prototype*, 2 (4) Available at: http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B4342D-E76E-F8F2-AC926AB64EC719B8.pdf (Accessed: 20 April 2013)

Hadjidj, R. Debbabi, M. Lounis, H, Iqbal, F. Szporer, A. and Benredjem, D. (2009) '*Towards an integrated email analysis framework'*, Available at: www.sciencedirect.com (Accessed: 20 May 2012)

Healy, L. (2008) *Increasing the Likelihood of Admissible Electronic Evidence: Digital Log Handling Excellence and a Forensically Aware Corporate Culture* Available at: http://www.emich.edu/ia/pdf/phdresearch/Increasing%20the%20Likelihood%20of%20Admissible%20Electronic%20Evidence,%20Larry%20Healy%20COT%20704.pdf

(Accessed: 20 August 2013)

Hermans, B. (1997). '*Intelligent software agents on the internet: An inventory of currently offered functionality in the information society and a prediction of (near) future developed*', Available at: http://www.firstmonday.dk/issues/issues2_3/ch_123/ (Accessed: 17 August 2010)

Icove, D. Seger, K. VonStorch, W. (1995) *Computer Crime: A Crime fighter's Handbook.* O'Rielly & Associates: Sebastapol, CA

Jennings, N. Wooldridge, M. (1997) *Agent Technology: Foundations, Applications and Markets.* Berlin: Springer

Jennings , N.R. Barnard, A. (2005) '*Software Quality Management Supported by Software Agent Technology*', Available at: http://www.informingscience.org/proceedings/InSITE2005/I53f40Nien.pdf (Accessed 13 April 2012)

Jones, K. Bejtlich, R. Rose, C. (2005) *Real Digital Forensics: Computer Security and Incident Response.* Upper Saddle River: Addison-Wesley

Kohn, M. Eloff, J. Olivier, M. (2006) '*Framework for a Digital Forensic Investigation*', Available at: http://icsa.cs.up.ac.za/issa/2006/proceedings/full/101_paper.pdf (Accessed: 12 August 2011)

Kossiakkoff, A. Sweet, W. (2003) *Systems Engineering Principles and Practice.* New York: Wiley

Kruse, W. Heiser, J. (2001) *Computer Forensics: Incident Response Essentials.* Indianapolis: Addison-Wesley

Lohani, M. Jeevan, V. (2007) '*Intelligent Software Agents for Library Applications*', 28(3). Available at: www.emeraldinsight.com/0143-5124.htm (Accessed: 18 April 2013)

Marshall, C. Rossman, G. (2006) *Designing Qualitative Research.* 4th edn. London: SAGE

Middleton, B. (2004) *Cyber Crime Investigator's Field Guide.* 2nd edn. Florida: Auerbach

Mobbs, P. (2003) *Computer crime: The law on the Misuse of Computers and Networks.* GreenNet Civil Society Internet Rights Project.

Available at: http://www.internetrights.org.uk/briefings/irtb08-rev1-draft.pdf

(Accessed: 20 July 2012)

Moore, T. (2006) '*The Economics of Digital Forensic*', Available at: http://people.seas.harvard.edu/~tmoore/weis06-moore.pdf (Accessed: 30 April 2012)

Nelson, B. Phillips, A. Enfinger, F. and Steuart. C (2004) *Guide to Computer Forensics and Investigation*. Boston: Thomson/Course Technology

Nienaber, R. Barnard, A. (2005) *Software Quality Management Supported by Software Agent Technology*, Available at: http://www.informingscience.org/proceedings/InSITE2005/I53f40Nien.pdf (Accessed: 13 April 2011)

Nikkel, B. (2006) *'The Role of Digital Forensic with a Corporate Organisation'*, Available at: www.digitalforensics.ch/nikkel/06a.pdf (Accessed: 25 February 2010)

Noblett, M. Pollitt, M. Presley, L (2000) *Recovering and Examining Computer Forensic evidence.* Forensic Science Communications. 2(4) Available at:

http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/oct2000/index.htm/computer.htm (Accessed: 5th December 2012)

Palmer, G. (2001) *'A Road Map to Digital Forensic Research'*, Available at: http://www.dfrws.org/2001/dfrws-rm-final.pdf (Accessed: 25 October 2011)

Panda Security (2009) *Annual Report PandaLabs* Available at: http://www.pandasecurity.com/img/enc/Annual_Report_Pandalabs_2009.pdf (Accessed: 16th August 2011)

Patel, A. Qi, W. Wills, C. (2010) '*A Review and Future Research Directions of Secure and Trustworthy Mobile Agent-Based E-Marketplace Systems'*, 28(3) Available at: www.emeraldinsight.com/0968-5227.htm (Accessed: 15 April 2012)

Perumal, S. (2009) *'Digital Forensic Model Based on Malaysian Investigation Process'*, 9(8) Available at: http://paper.ijcsns.org/07_book/200908/20080805.pdf (Accessed: 7 August 2012)

Pietro, D. Verde, N. (2010) *Handbook of Electronic Security and Digital Forensic World.* Singapore: Scientific

Pilli, E. Joshi, R. Niyosi, R. (2010) '*Network Forensic Frameworks: Survey and research Challenges'*, Available at: http://www.sciencedirect.com/science?_ob=MiamiImageURL&_cid=273059&_user=132444&_pii=S1742287610000113&_check=y&_origin=&_coverDate=31-Oct-2010&view=c&wchp=dGLzVlt-zSkzS&md5=f0345fa37fdcbc76113b1d98c9a83367/1-s2.0-S1742287610000113-main.pdf (Accessed: 28 July 2013)

Pollitt, M. (2007) '*An Ad Hoc Review of Digital Forensic Models'*, 10(12)

Available at: http://www.ieeexplore.ieee.org/ie15/4155337/4155338/04155349.pdf (Accessed: 17 September 2012)

Ralha, C. (2009) *'Towards the Integration of Multi-Agent Application and Data Mining'*,

Available at: http://www.springer.com/cda/content/9781441905215.ci.pdf (Accessed: 22 April 2011)

Rasem, A. (2011) '*O-PMIPv6: Optimized Proxy Mobile IPv6'*, Master of Applied Science in Electrical and Engineering. Carleton University. Available at: www.csit.carleton.ca/~msthilaire/.../Ahmad%20Rasem%20-%20Thesis.pdf (Accessed: 15 June 2013)

Reichenbach, M. (2008) *'Lecture 9: Computer System Security'*, Information and Communication Security (WS 2008/2009). Johann Wolfgang Goethe University Frankfurt. Available at: http://www.web-portal system.de/wps/wse/dl/down/open/rannenberg/53a433b8e84b7f766b29f03d9d85227d4343dec952607e10dfdc4b243ad68e924970146ca18bb17ad9f947befdd9a3c9/SEC-WS08-9-CSS.pdf (Accessed: 6 July 2012)

Reith, M. Carr. C. Gunsch, G. (2002) '*An Examination of Digital Forensic Models'*, 1(3) Available at: http://people.emich.edu/pstephen/other_papers/Digital_Forensic_Models.pdf (Accessed: 7 October 2011).

Rekhis, S. Krichene, J. Boudriga, N. (2009) *Forensic Investigation in Communication Networks Using Incomplete Digital Evidence*, 2(9) Available at: http://www.sciRP.org/journal/ijens/ (Accessed: 20 April 2011)

Robson, C. (2002) *Real world research: A Resource for Social Scientists and Practitioner-Researchers.* New York: Wiley

Rogers, M. Siegfried, K. (2004) '*The Future of Computer Forensics: A Need Analysis Survey Computer and Security*', 23(1) Available at: http://www2.tech.purdue.edu/cpt/courses/TECH581A/Rogers.pdf (Accessed: 7th May 2012)

Rodgers, M. Goldman, J. Mislan, R. and Wedge, T. (2006) *Computer Forensic Field Triage Process* Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.99...pdf (Accessed: 29 September 2011)

Roussev, V. Richard, G. (2006) *Next-Generation Digital Forensics.* Available at: http://portal.acm.org/citation.cfm?id=1113074 (Accessed: 30 May 2010)

Roussev, V. Richard, G. (2004) *Breaking the Performance Wall: The case of distributed digital forensics.* Available at: http://www.dfrws.org/2004/day2/Golden-Perfromance (Accessed: 25 August 2010)

Ruibin, G. Tony, C. Gaertner, M. (2005) '*Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework*', 4(1) Available at: http://www.utica.edu/academic/institutes/ecii/publications/articles/B4A6A102-A93D-85B1-95C575D5E35F3764.pdf (Accessed: 15 September 2011)

Russell, S. Norvig, P. (2010) *Artificial Intelligence: A Modern Approach.* 3rd edn. New Jersey: Prentice Hall

Schneider, D (2004) *An Introduction to Programming using Visual Basic 6.0* 4th edn. New Jersey: Prentice Hall

Schumacher, H. Gosh, S. (1998) '*Fundamental Framework for Network Security Towards Enabling Security on Demand in an ATM Networks*, Computers and Security, 17(6), pp. 527-542.

Selamat, S. Yusof, R. Sahib, S. (2008) '*Mapping Process of Digital Forensic Investigation Framework'*, 8(10) Available at: http://paper.ijcsns.org/07_book/200810/20081025.pdf (Accessed: 18 October 2011)

Solomon, J. Lattimore, E. (2006) '*Computer Forensics'*, Available at: http://citeseerx.ist.psu.edu/ (Accessed: 20 February 2011)

Sommer, P. (2009) *'Directors' and Corporate Advisors' Guide to Digital Investigations and Evidence'*, 2nd edn. London: Information Assurance Advisory Council. Available at: http://www.iaac.org.uk/_media/DigitalInvestigations2009.pdf (Accessed: 3 September 2011).

Stafford, T. Urbaczewski, A. (2004) *'SPYWARE: The Ghost in the Machine'*, 14, p. 293 Communications of the Association for Information System. Available at: http://citeseerx.ist.psu.edu10.1.1.145.8618.pdf (Accessed: 3 July 2012)

Stallings, W. Brown, L. (2008) *Computer Security: Principles and Practice.* Upper Saddle River: Pearson Prentice Hall

Stamm, M. (2012) *'Digital Multimedia Forensics and Anti-Forensics'*, Doctor of Philosophy (PhD). University of Maryland, College Park. Available at: http://sig.umd.edu/alumni/thesis/Stamm_Thesis.pdf (Accessed: 10 June 2013)

Stephenson, P. (2000) *Investigating Computer-Related Crime: A Handbook for Corporate Investigators.* Florida: CRC

Stephenson, P. (2003) *'A Comprehensive Approach to Digital Incident Investigation'*, Elsevier Information Security Technical Report. 8(1) Available at: http://www.emich.edu/cerns/downloads/pstephen/Comprehensive-Approach-to-Digital-Investigation.pdf (Accessed: 20 April 2013)

Tomsho, G. Tittel, E. Johnson, D. (2007) *Guide to Networking Essentials* 5th edn. USA: Thomson

US v. McKinnon (2002) *Bill of Indictment.* Available at: http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/cyberlaw/usmck1102vaind.pdf (Accessed: 10 May 2013)

Wallace, D. (1997) *'Intelligent Software Agents: Definitions and Applications'*, Available at: http://alumnus.caltech.edu/~croft/research/agent/definition/ (Accessed: 25 August 2011).

Williams, G. (2004) *Synchronizing E-Security* London: Kluwer

Yang, T. Li, T. Liu, S. Wang, T. Wang, D. and Liang, D. (2007) '*Computer Forensics System Based on Artificial Immune Systems*', 13(9) Available at: citeseerx.ist.psu.edu/viewdoc/download? doi=10.1.1.96.1008.pdf (Accessed: 20 June 2012)

Yasinsac, A. Erbacher, R. Marks, D. Pollitt, M and Sommer, P. (1997) '*Computer Forensics Education'*,

Available at: http://www.pmsommer.com/csdspaper.pdf (Accessed: 25 December 2012)

APPENDIX 1: Building the Testbed

1.1 Ubuntu

In order to implement the buffering function, a testbed was established using OAI PMIPv6 version 0.3.1 and reference was made to the method of establishment provided by OAI. The operating system used is Ubuntu 10.04.

Ubuntu Requirement:

The minimum system requirements of Ubuntu Desktop are as illustrated in Table 10 shown below:

Table 10: Minimum System Requirements of Ubuntu

	Minimum System Requirements	**Recommended minimum Requirements**
Processor	300 MHz	700 MHz
Memory	256 MB	384 MB
Hard drive	4 GB	8 GB

1.2 Setting the Network

Network was set up between the machines. The PMIP domain is created that contains 3 nodes which are 1LMA and 2MAG's.The 3 nodes were connected to the same collision domain.

To test the network connection between the machines to ensure machines can reach each other. ping 192.168.1.4. Figure 72 shows the experiment's network connection reach other.

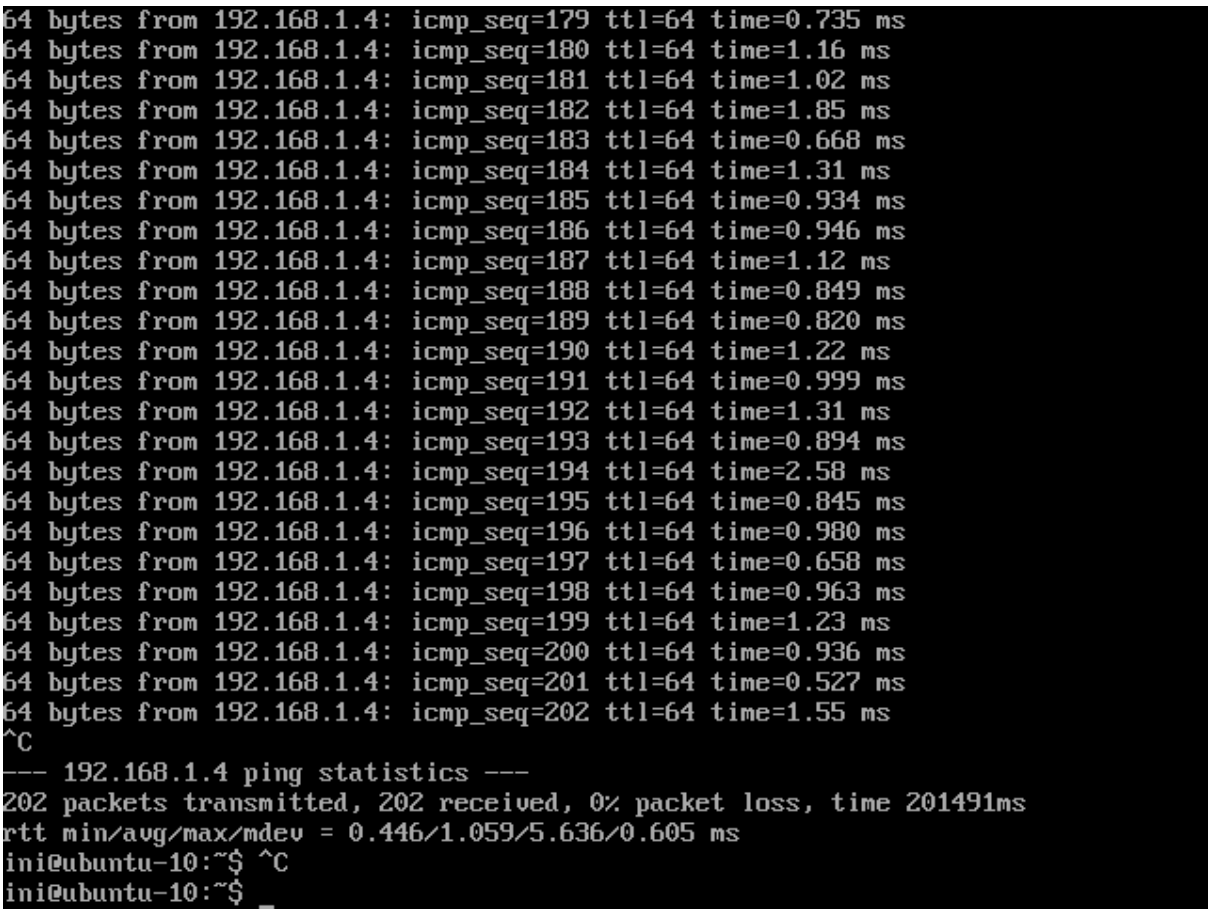


Figure 72: Using ping for testing experiment's network connection

The rest of the machines are configured the same way but the IP addresses for the rest machines are shown in Table 11

Table 11: IP address for experimental machines

Machine Name	IP Address
LMA	192.168.1.4
MAG1	192.168.1.5
MAG2	192.168.1.6

1.3 Netfilter Operations

In order to implement the buffering function, the Netfilter and IP6Tables by Linux were used:

- Once a packet is entered into the system, some simple consistency checks are carried out, and the packet is passed to the NF_IP_PRE_ROUTING hook point (line 1-3).
- Next, the routing code decides whether the packet is intended for another machine or higher layers(line 4)
- If it is intended for higher layers, it navigates through the NF_IP_LOCAL_IN hook point before being passed to the local process of the higher layers (line 5)
- If the packet is intended to pass to another machine, the packet navigates through the NF_IP_FORWARD hook point (line 6).
- A packet sent from higher layers navigates through the NF_IP_LOCAL_OUT hook point and enters the routing code (line7-9).

The packet then passes a final Netfilter hook point, NF_IP_POST_ROUTING, and is sent to the device driver (10-11). Figure 72 Netfilter framework operation

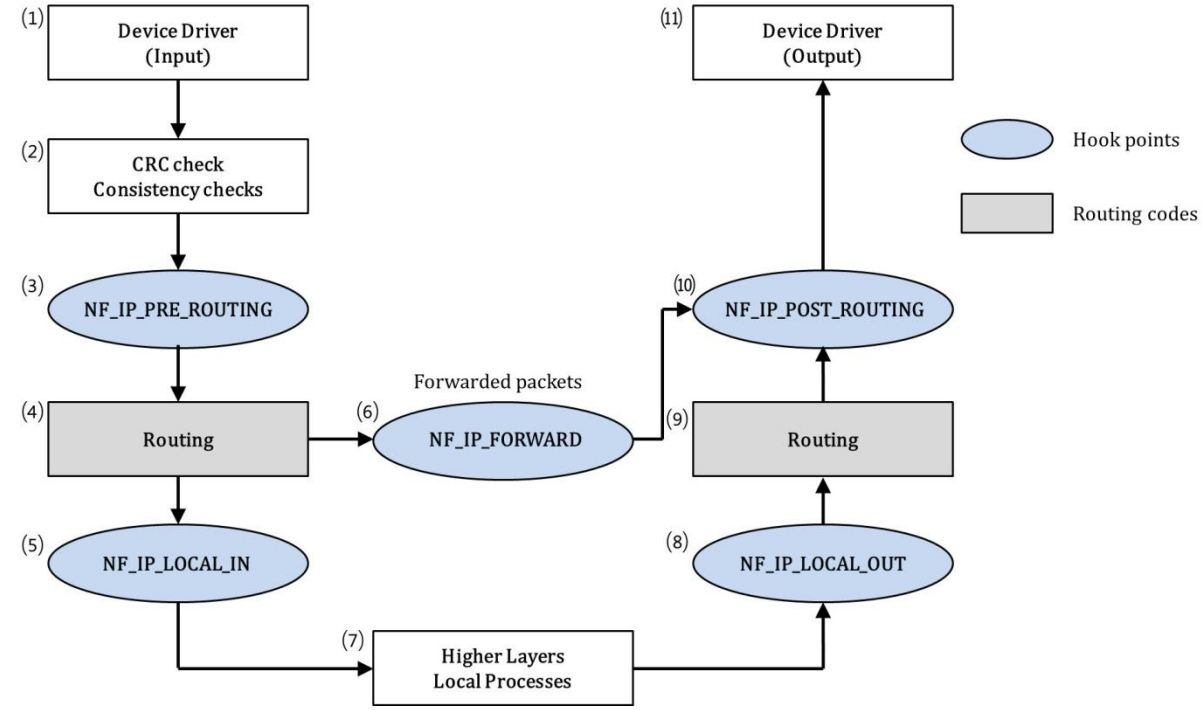


Figure. 72 Netfilter framework operations

1.4 Testbed

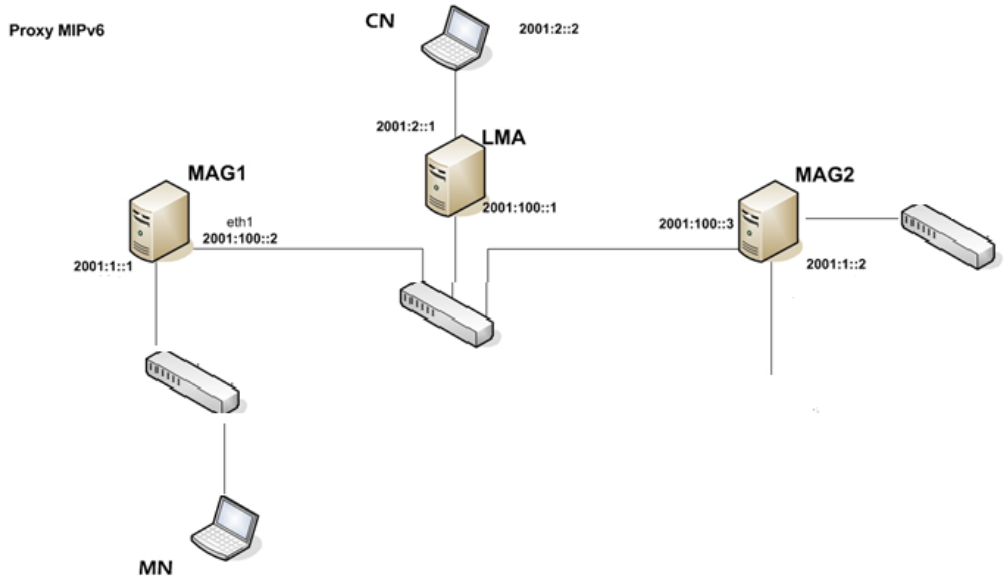


Figure 73: The real testbed of Proxy MIPv6 representation

To conduct the experiment, an OAI PMIPv6 v0.3 testbed was established for standard PMIPv6. The testbed consist of an LMA and 2MAGs. Hubs were used rather than Access Point for the wireless link.

All the network entities in the test-bed are running Ubuntu 10.04 LTS with its generic Linux kernel. The functionalities for LMA and MAG have been developed above UMIP and discussed as follows:

- An unmodified MN, which does not have any specific software for mobility, uses its wireless card to attach to one of the hub.
- Each hub is directly connected to a MAG.
- The implementation of MAG functionalities contains additional features and modifications of UMIP to handle PBU and PBA messages and mobility options, and a modified Router Advertisement daemon (RADVD), which unicasts RAs with a specific HNP per MN.
- Each MAG is connected to the LMA.
- The LMA is configured as a modified HA in UMIP, which stores the HNP in the BCE for each MN, and it is able to handle PBU and PBA messages.
- Finally, an unmodified CN is connected to the LMA.

1.5. Message flow demonstration

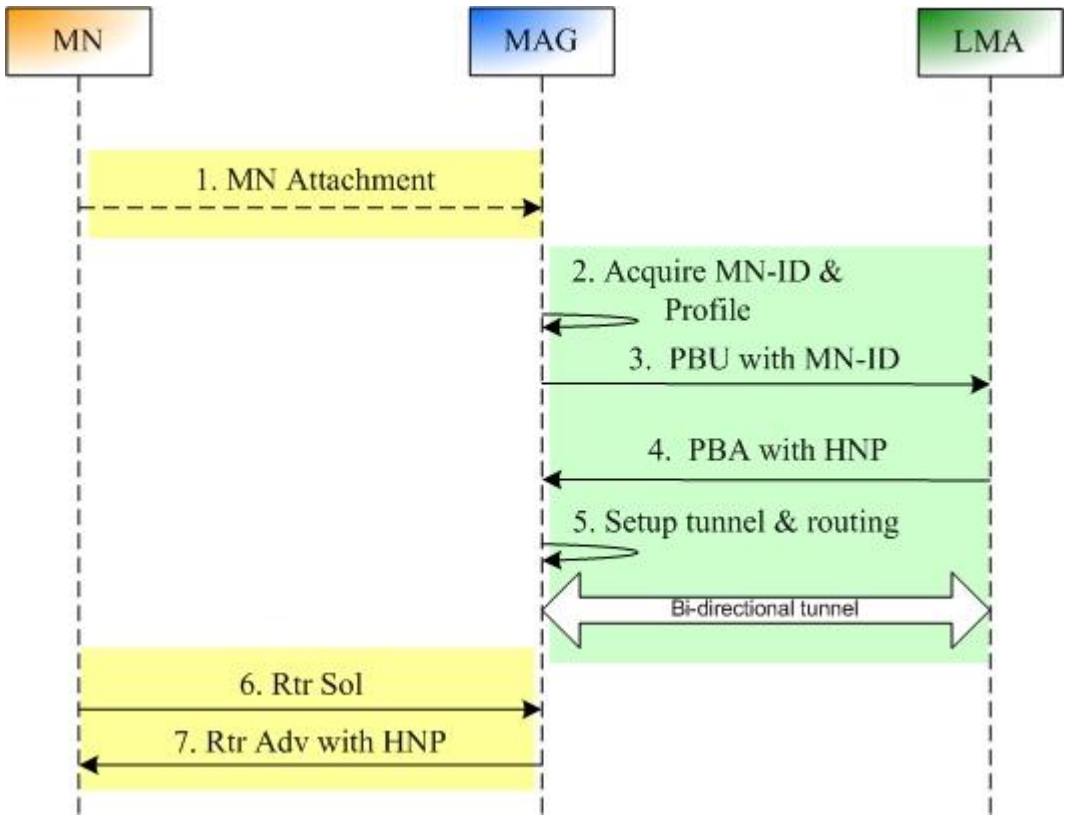


Figure 74: Message flow demonstration

The message flow demonstration is as follows:

- The Mobile Node enters the PMIP domain for the first time and connects to Mobile Access Gateway ‘s hub
- MAG1 detects the MN and checks for host authorization
- MAG1 updates then the Local Mobility Anchor about the current location of the mobile node
- Both MAG1 and LMA create an IP in IP bi-directional tunnel
- MAG1 sends a Router Advertisement message to MN with its specific Home Network Prefix
- The MN auto-configures itself according to the HNP. An unlimited ICMP traffic (ping6 command) is started between the MN and CN
- While MN keeps pinging CN, the Mobile Node moves. It connects now to MAG2 via the second hub and loses connection with MAG1.

- After a while, MN leaves MAG2 and goes back to MAG1 area.
- After a while, MN leaves again MAG1 and return to MAG2

1.6 Proxy Mobile Internet Protocol Version 6 (PMIPv6) domain

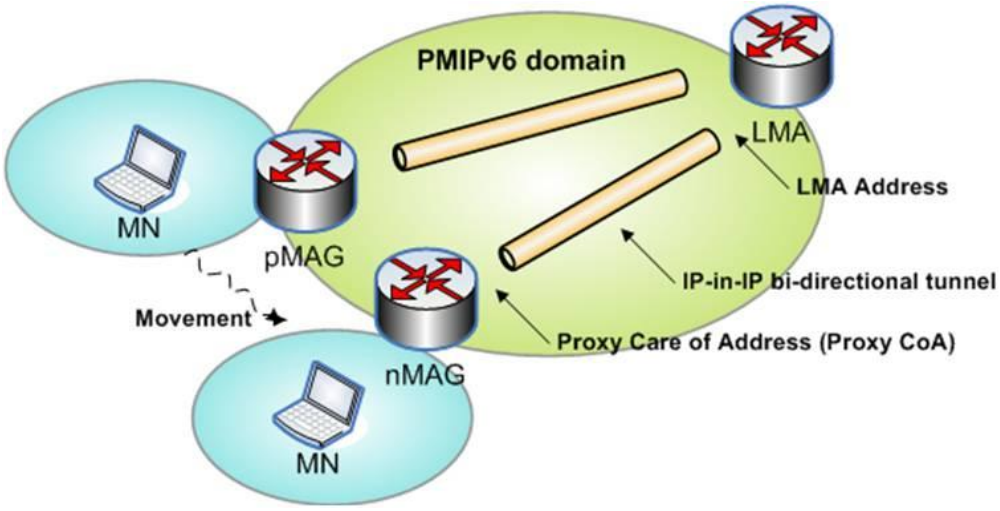


Figure 75: the PMIPv6 domain

1.7 Packet Collection

The Libipq library is provided as part of the IP6Tables. It is used to store the packets. Figure 76 and 77 shows the packets stored for buffering and forwarding.

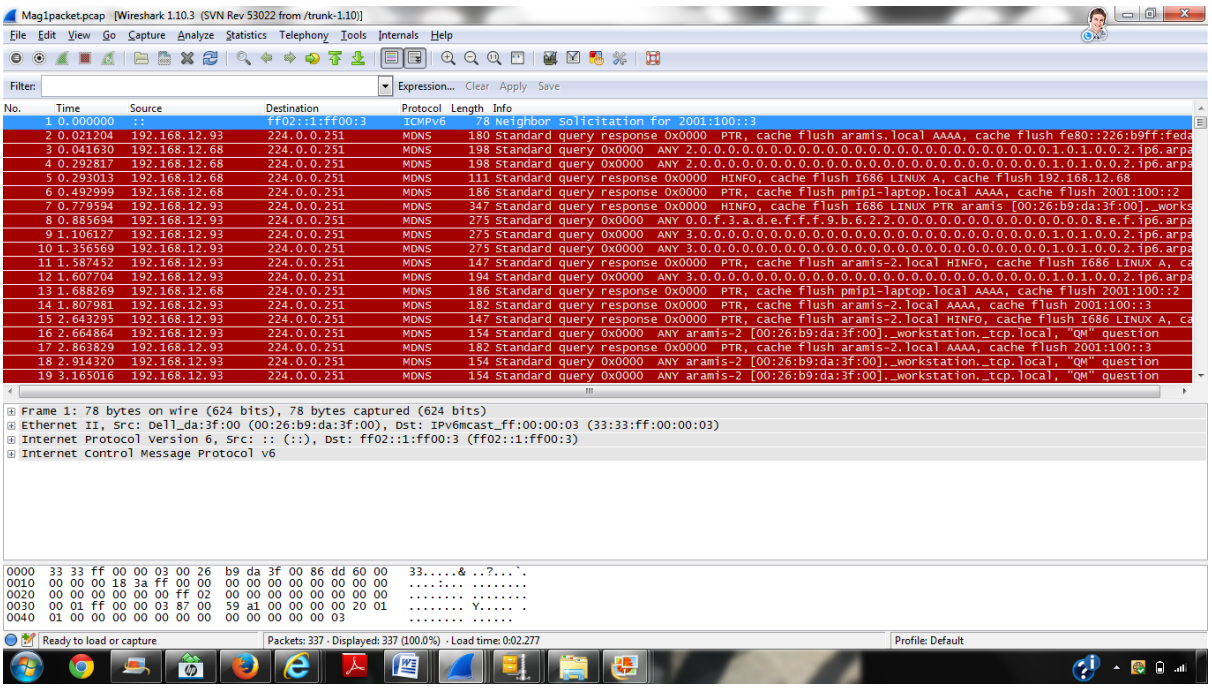


Figure 76: Packets for Mag1

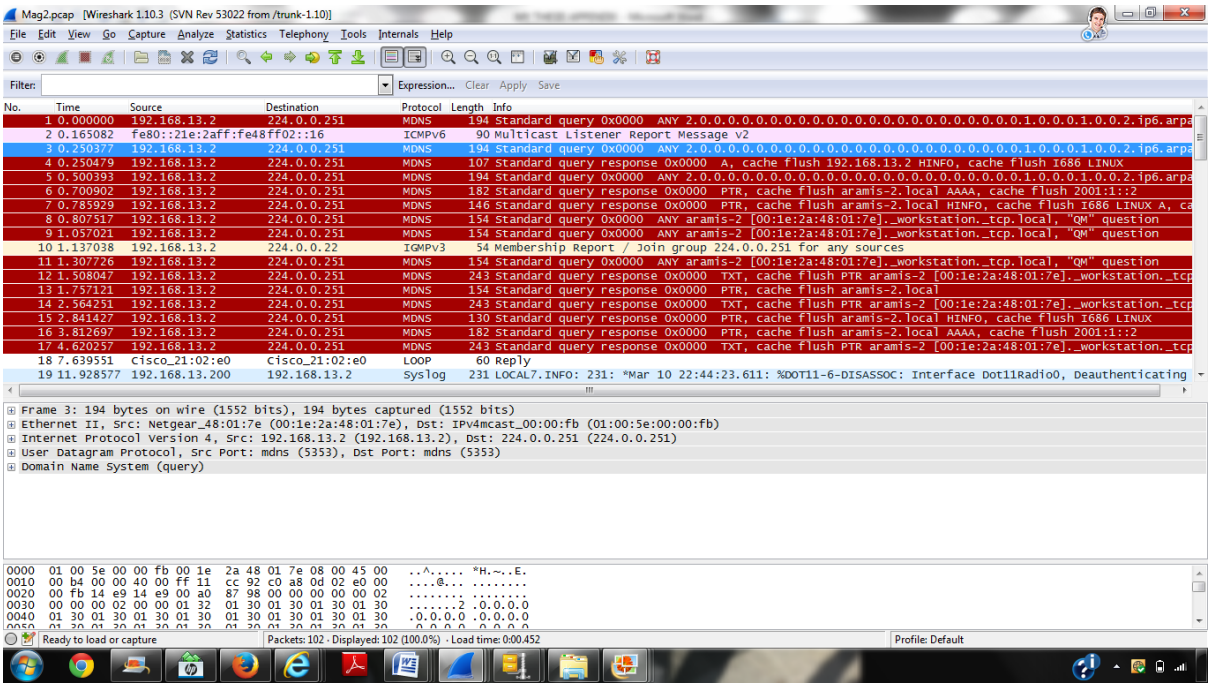


Figure 77: Packets for Mag2

Appendix 2:

Digital Investigation with Comprehensive Digital Forensic Investigation Model (CDFIM) using FTK

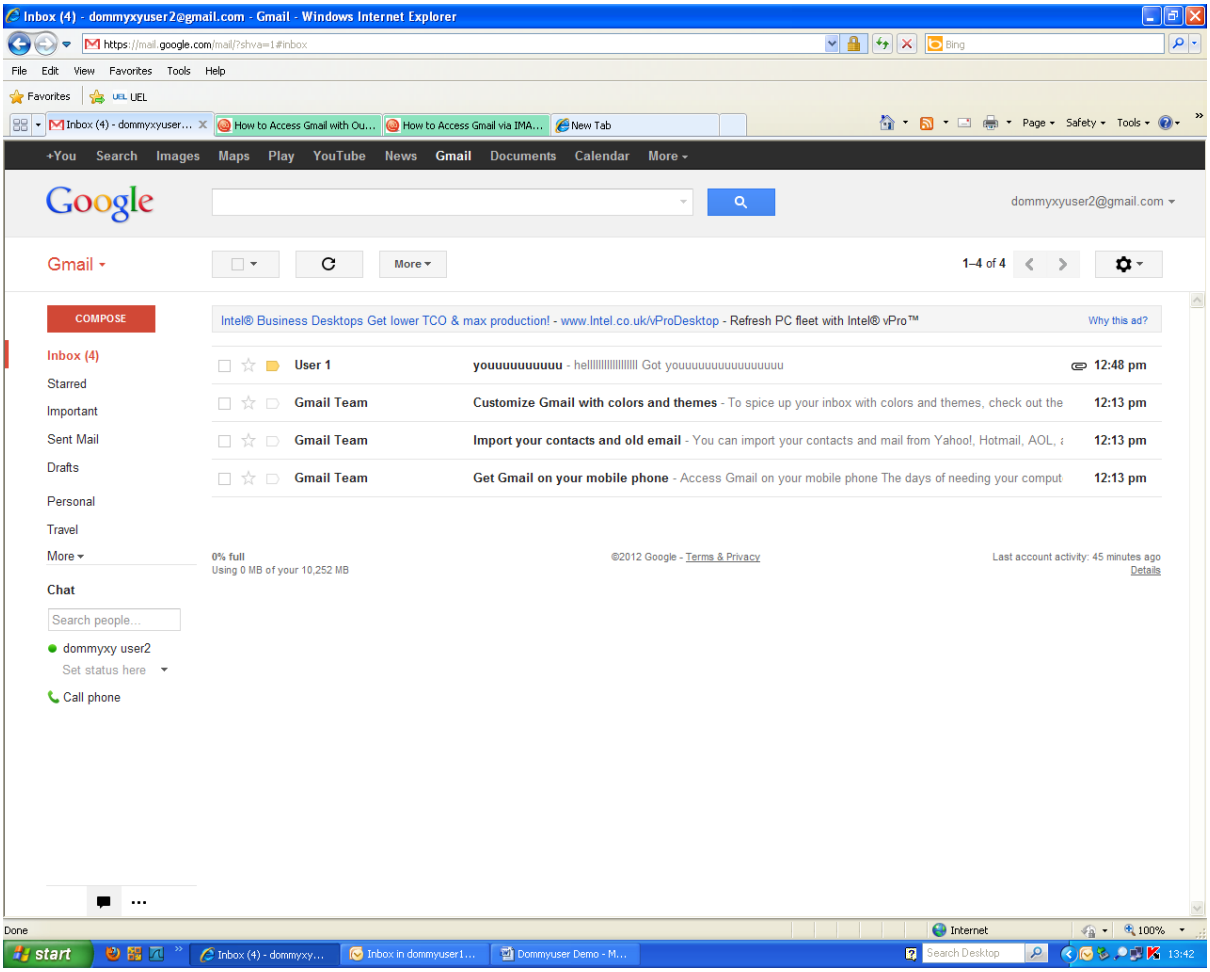


Figure 78: test email box

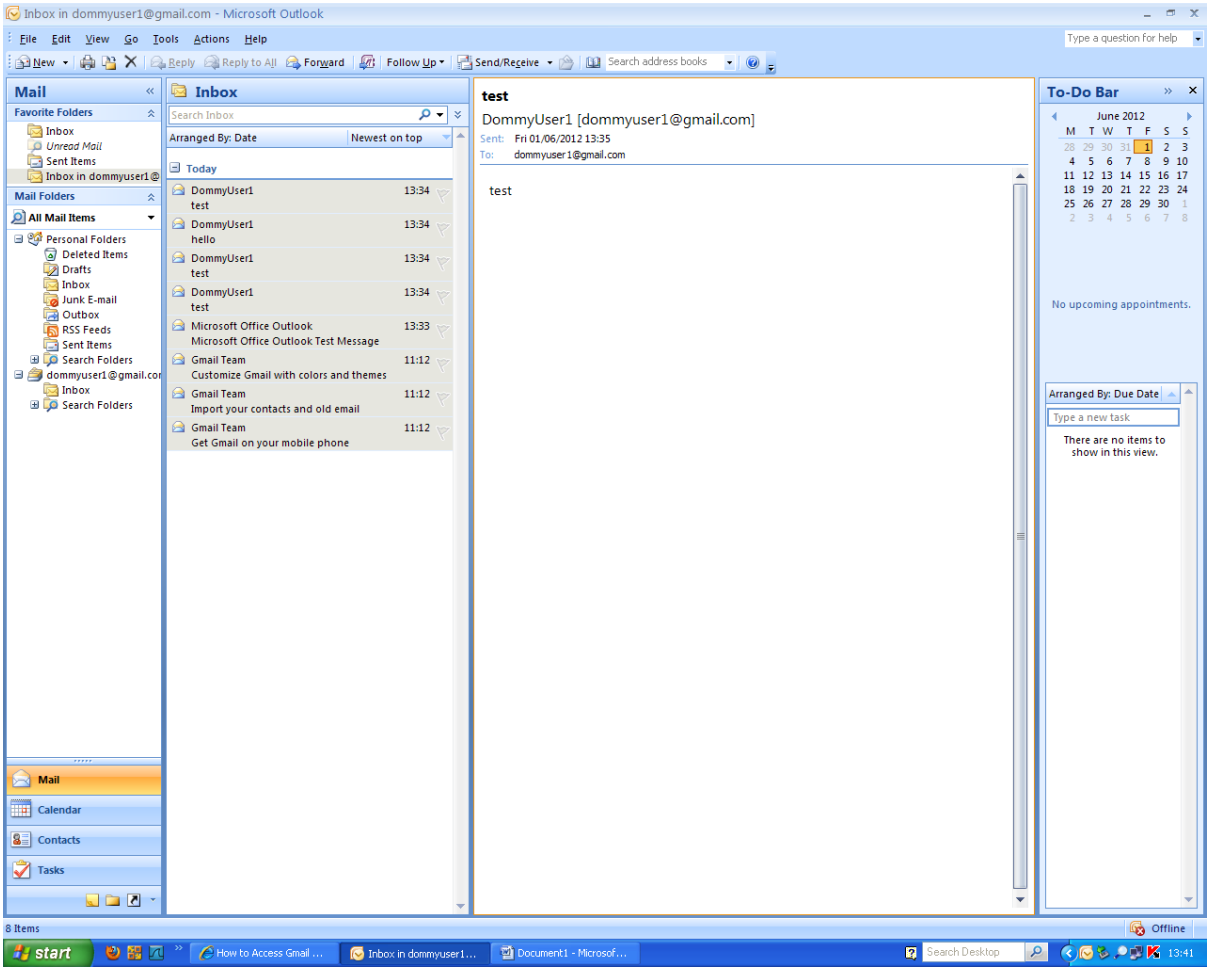


Figure 79: test email box with incoming messages

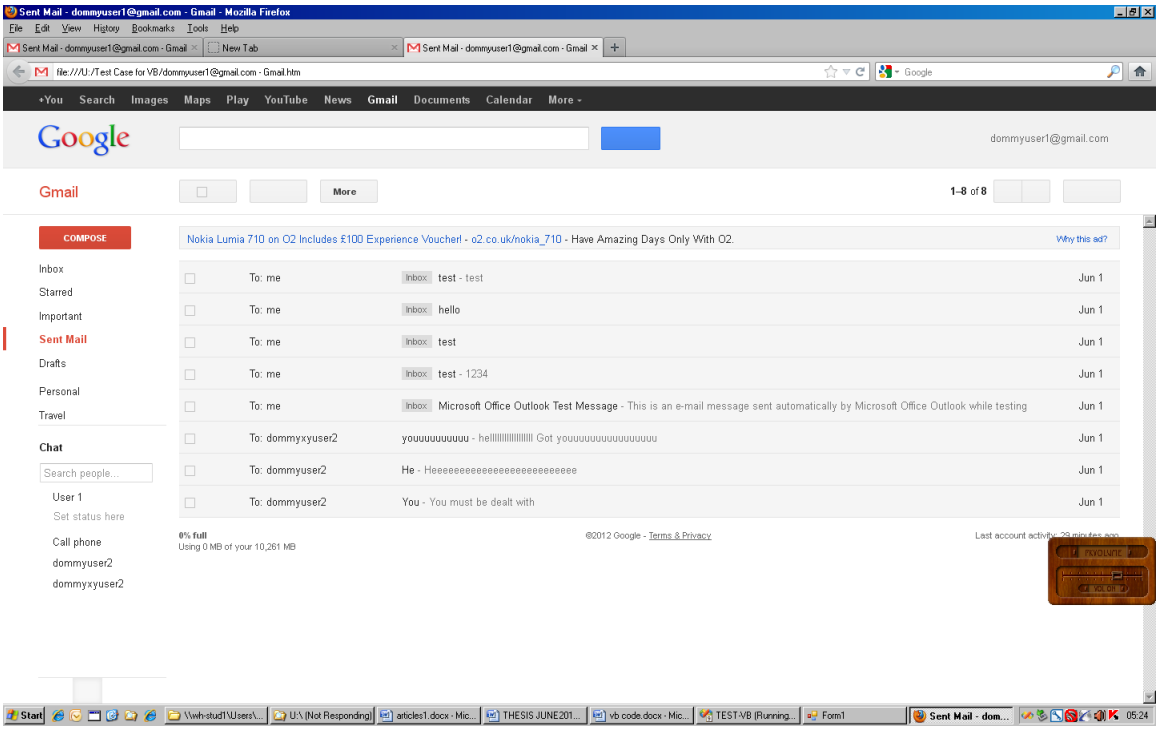


Figure 80: the Email folder and its content

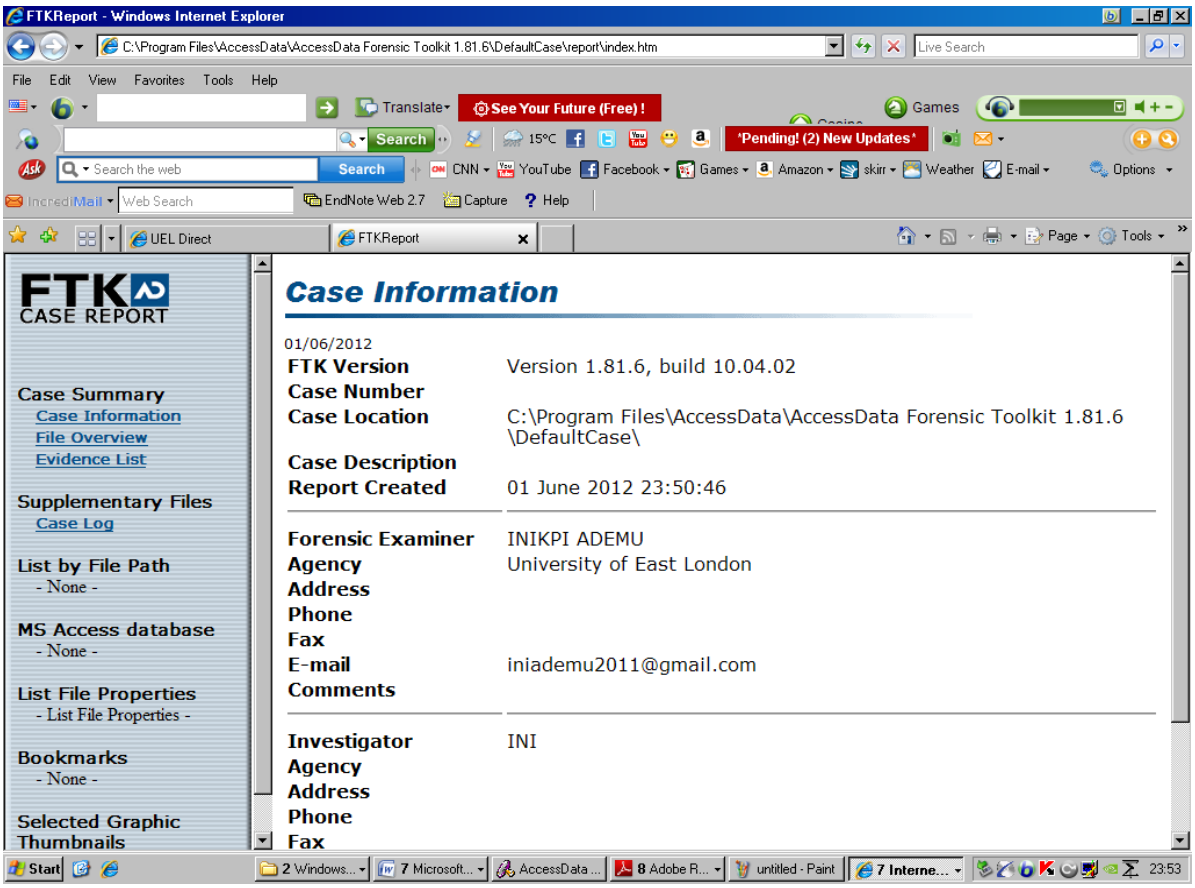


Figure 81: FTK case log information

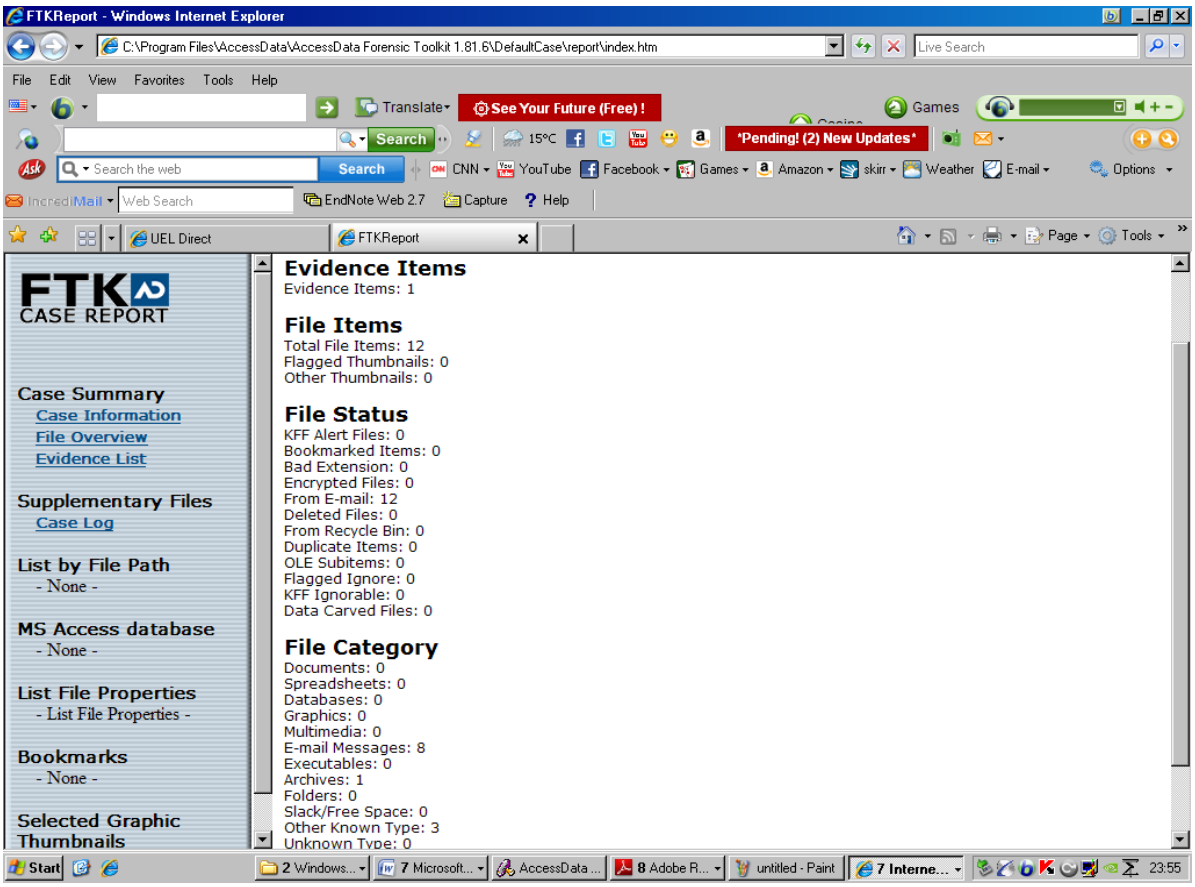


Figure 82: FTK File overview

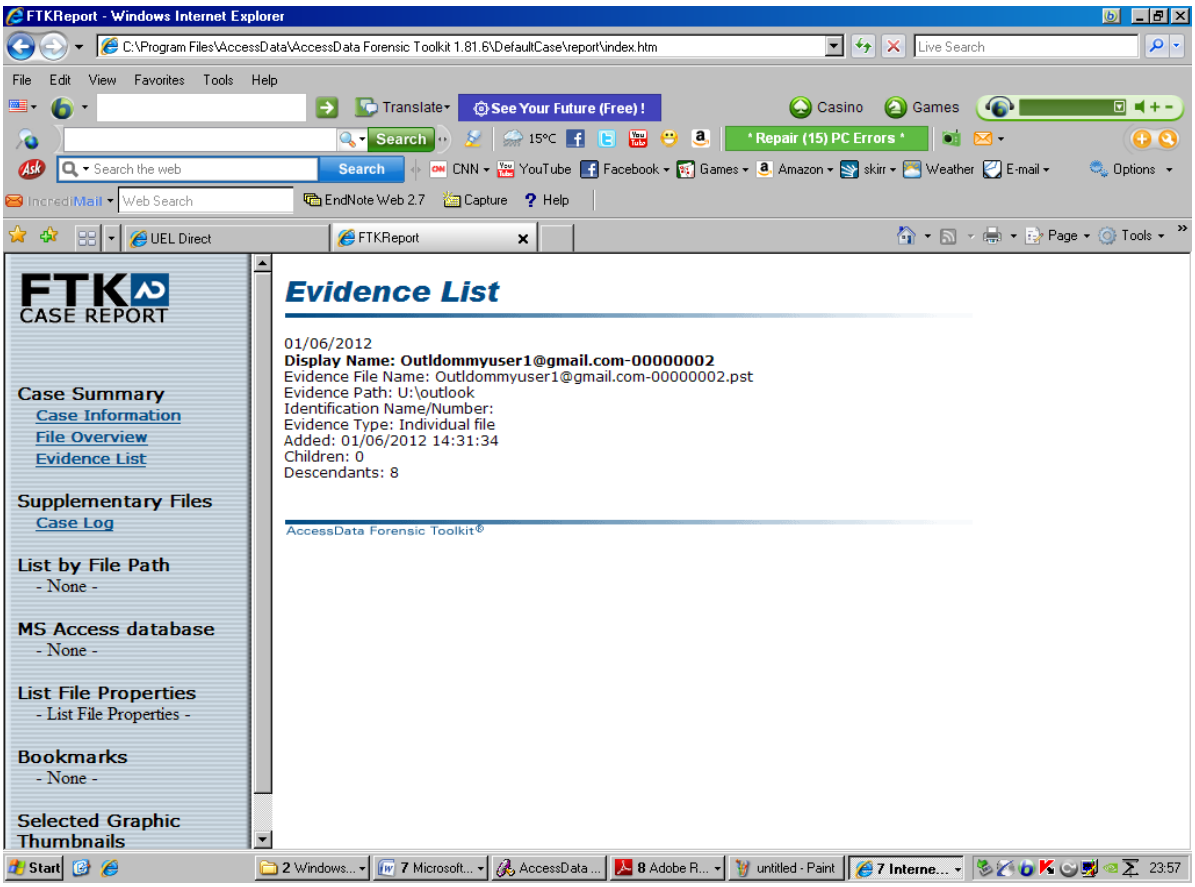


Figure 83: FTK Evidence list

CASE LOG RECORD

31/05/2012 11:40:43 -- FTK Version 1.81.6 build 10.04.02

FTK Exe Path: C:\Program Files\AccessData\AccessData Forensic Toolkit 1.81.6\Program\ftk.exe

Examiner's Machine:

Phys Mem: Total: 2,128,252,928 Available: 1,496,666,112 Used: 631,586,816

Virt Mem: Total: 2,147,352,576 Available: 1,927,348,224 Used 220,004,352

Page File Available: 3,592,515,584

31/05/2012 11:40:43 -- KFF database being used: none

31/05/2012 11:40:43 -- Examiner's Local Machine Setting is time zone used for file times (create, modify, accessed) in file display and reports.

31/05/2012 11:40:57 -- Warning: unable to open Examiner information file C:\Program Files\AccessData\AccessData Forensic Toolkit 1.81.6\DefaultCase\FtkExaminer.dat. Data not loaded.

31/05/2012 11:47:07 -- Loading case

31/05/2012 11:47:07 -- Updating Overview Cache

31/05/2012 11:47:07 -- Filtering file list

31/05/2012 11:47:07 -- Initializing thumbnail view

31/05/2012 11:47:07 -- Resetting search terms list

31/05/2012 11:47:07 -- Building the indexed search results tree...

31/05/2012 11:47:07 -- Building the live search results tree...

31/05/2012 11:47:07 -- Building the bookmark tree

31/05/2012 11:48:14 -- Warning: unable to open Examiner information file C:\Program Files\AccessData\AccessData Forensic Toolkit 1.81.6\DefaultCase\FtkExaminer.dat. Data not loaded.

31/05/2012 11:48:25 -- Loading case

31/05/2012 11:48:25 -- Updating Overview Cache

31/05/2012 11:48:25 -- Filtering file list

31/05/2012 11:48:25 -- Initializing thumbnail view

31/05/2012 11:48:25 -- Resetting search terms list

31/05/2012 11:48:25 -- Building the indexed search results tree...

31/05/2012 11:48:25 -- Building the live search results tree...

31/05/2012 11:48:25 -- Building the bookmark tree

31/05/2012 11:49:22 -- Warning: unable to open Examiner information file C:\Program Files\AccessData\AccessData Forensic Toolkit 1.81.6\DefaultCase\FtkExaminer.dat. Data not loaded.

31/05/2012 12:42:06 -- Loading case

31/05/2012 12:42:06 -- Updating Overview Cache

31/05/2012 12:42:06 -- Filtering file list

31/05/2012 12:42:06 -- Initializing thumbnail view

31/05/2012 12:42:06 -- Resetting search terms list

31/05/2012 12:42:06 -- Building the indexed search results tree...

31/05/2012 12:42:06 -- Building the live search results tree...

31/05/2012 12:42:06 -- Building the bookmark tree

01/06/2012 14:31:34 -- Evidence added by investigator INI using FTK version 1.81.6 build 10.04.02

Processes to be performed:

File Extraction: Yes

File Identification: Yes

MD5 Hash: Yes

SHA1 Hash: Yes

KFF (Known File Filter): Yes

Entropy Test: Yes

Full Text Index: Yes

Prerender Thumbnails: No

File Listing Database: No

HTML File Listing: No

Data Carving: No

Preprocess Registry Files: No

Decrypt EFS Files: No

Default Case Refinement Settings:

Add files only if they satisfy BOTH the file status and the file type criteria as follows:

File Status Criteria:

Deletion status: any

Encryption status: any

From email status: any

Duplicate status: any

OLE stream status: any

File Type Criteria:

documents: yes

spreadsheets: yes

databases: yes

graphics: yes

email messages: yes

executables: yes

archives: yes

folders: yes

other recognized: yes

unknown: yes

Default Index Refinement Settings:

Index files only if they satisfy BOTH the file status and the file type criteria as follows:

File Status Criteria:

Deletion status: any

Encryption status: any

From email status: any

Duplicate status: any

OLE stream status: any

File Type Criteria:

documents: yes

spreadsheets: yes

databases: yes

graphics: yes

email messages: yes

executables: yes

archives: yes

folders: yes

other recognized: yes

unknown: yes

-- Evidence 1 --

Name/Number:

Location: U:\outlook\Outldommyuser1@gmail.com-00000002.pst

Display name: Outldommyuser1@gmail.com-00000002

Type: Individual file

Comment:

Evidence-specific Case Refinement Settings:

Add files only if they satisfy BOTH the file status and the file type criteria as follows:

File Status Criteria:

Deletion status: any

Encryption status: any

From email status: any

Duplicate status: any

OLE stream status: any

File Type Criteria:

documents: yes

spreadsheets: yes

databases: yes

graphics: yes

email messages: yes

executables: yes

archives: yes

folders: yes

other recognized: yes

unknown: yes

Evidence-specific Index Refinement Settings:

Index files only if they satisfy BOTH the file status and the file type criteria as follows:

File Status Criteria:

Deletion status: any

Encryption status: any

From email status: any

Duplicate status: any

OLE stream status: any

File Type Criteria:

documents: yes

spreadsheets: yes

databases: yes

graphics: yes

email messages: yes

executables: yes

archives: yes

folders: yes

other recognized: yes

unknown: yes

01/06/2012 14:31:34 -- Starting to add evidence items...

01/06/2012 14:31:35 -- Completed adding Outldommyuser1@gmail.com-00000002

01/06/2012 14:31:35 -- Updating Overview Cache

01/06/2012 14:31:35 -- Filtering the list

01/06/2012 14:31:35 -- Updating counts

01/06/2012 14:31:35 -- Flushing case data to disk

01/06/2012 14:31:36 -- Loading case

01/06/2012 14:31:36 -- Building explore path tree

```
01/06/2012 14:31:36 -- Building explore, graphic and email path tree
01/06/2012 14:31:36 -- Updating Overview Cache
01/06/2012 14:31:36 -- Filtering file list
01/06/2012 14:31:36 -- Initializing thumbnail view
01/06/2012 14:31:36 -- Resetting search terms list
01/06/2012 14:31:36 -- Building the indexed search results tree...
01/06/2012 14:31:36 -- Building the live search results tree...
01/06/2012 14:31:36 -- Building the bookmark tree
01/06/2012 14:31:36 -- Final Status Update:
        Total Elapsed Time:    0.00:00:02
        Total Items Examined:   9
        Total Items Added:     9
        Total Indexing Completed:
          Items Indexed:     9
          Index Time:      0.00:00:00
          Data Indexed:     287,864
          Data Indexed (filt):  16,504
          Index granularity set at: 4
        Indexing completed since last update:
          Items Indexed:     10
          Index Time:      0.00:00:00
          Data Indexed:     287,864
```

APPENDIX 3

Bill of Indictment

```
  Data Indexed (filt):  16,504
Total Bytes Processed:   16,504
Physical Memory Available: 825,784KB of 2,078,372KB
Virtual Memory Available: 1,717,816KB of 2,097,024KB
```

Page File Available: 2,331

IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	)	
	)	Criminal No.
v.	)	
	)	18 U.S.C. § 1030
GARY MCKINNON,	)	Fraud and Related Activity in
	)	Connection with Computers
Defendant	)	(Counts 1 through 7)
	)	

INDICTMENT

NOVEMBER 2002 Term - At Alexandria

Introduction

THE GRAND JURY CHARGES THAT:

1. At all times material to this Indictment:

a. The United States Army is a military department of the United States Government, which provides military forces to defend the United States and any occupied territory and to overcome any aggressor that imperils the peace and security of the United States.

b. The Department of the Navy is a military department of the United States Government, which provides naval forces that defend the United States and are capable of winning wars, deterring aggression and maintaining the freedom of the seas.

c. The Department of the Air Force is a military department of the United States Government, which provides military forces that defend the United States through the control and exploitation of air and space.

d. The Department of Defense is a department of the United States Government and is responsible for providing military forces that defend the United States and any occupied area, and overcome any aggressor that imperils peace and security of the United States.

e. The National Aeronautics and Space Administration ("NASA") is an agency of the United States Government, which conducts research into flight within and outside the Earth's atmosphere, including the exploration of space.

f. RemotelyAnywhere is a software program that provides a remote access and remote administration package for computers on the Internet and can be downloaded over the Internet from 03AM Laboratories PL, Hungary. Once installed on a host computer, RemotelyAnywhere allows the user to remotely control the host computer and access the host computer from any other computer connected to the Internet. RemotelyAnywhere provides the user with the ability to transfer and delete files or data, and the ability to access almost every administrative function available on the host computer.

g. Defendant GARY MCKINNON was an unemployed computer system administrator living in London, England.

h. The above introductory allegations are realleged and incorporated in Counts One through Seven of this indictment as though fully set out in Counts One through Seven.

COUNT 1

(Fraud and Related Activity in Connection with Computers)

THE GRAND JURY FURTHER CHARGES THAT:

2. Between on or about February 1, 2002, and on or about February 22, 2002, within the Eastern District of Virginia, and elsewhere, the defendant GARY MCKINNON did knowingly cause the transmission of codes, information and commands, and as a result of such conduct, intentionally caused damage without authorization to a protected computer, belonging to the United States Army.

3. Specifically, the defendant intentionally accessed a computer belonging to and used exclusively by the United States Army, Fort Myer, Virginia, with the Internet Protocol address of 160.145.40.25, which computer was used in interstate and foreign commerce and communication. The defendant then obtained administrator privileges and transmitted codes, information and commands that: (1) deleted approximately 1300 user accounts; (2) installed RemotelyAnywhere; (3) deleted critical system files necessary for the operation of the computer; (4) copied a file containing usernames and encrypted passwords for the computer; and (5) installed tools used for obtaining unauthorized access to computers. As a result of such conduct, the defendant intentionally caused damage without authorization by impairing the integrity and availability of data, programs, a system and information, and that damage: (a) caused loss aggregating more than $5,000 in value during a one-year period to the United States Army; and (b) affected the use of the computer system used by a government entity, the United States Army, in furtherance of the administration of national defense and national security.

(All in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(i), 1030(a)(5)(B)(i) and 1030(a)(5)(B)(v)).

COUNT 2

(Fraud and Related Activity in Connection with Computers)

THE GRAND JURY FURTHER CHARGES THAT:

4. From in or about September 2001, through on or about March 19, 2002, within the Eastern District of Virginia, and elsewhere, the defendant GARY MCKINNON did knowingly cause the transmission of codes, information and commands, and as a result of such conduct, intentionally caused damage without authorization to protected computers, belonging to the United States Army.

5. Specifically, the defendant intentionally accessed computers exclusively used by the United States Army, which computers were used in interstate and foreign commerce and communication. Then, the

defendant obtained administrator privileges on these computers and installed RemotelyAnywhere. On several of the computers, the defendant installed tools used for obtaining unauthorized access to computers, deleted critical system files necessary for the operation of the computers and copied files containing unclassified information to his own computer. The computers accessed and damaged by the defendant included the following:

IP Address	Location
160.145.18.111	Fort Myer, VA
160.145.30.89	Fort Myer, VA
160.145.33.52	Fort Myer, VA
160.145.40.22	Fort Myer, VA
160.145.40.31	Fort Myer, VA
160.145.40.51	Fort Myer, VA
160.145.214.25	Fort McNair, Washington, DC
160.145.214.26	Fort McNair, Washington, DC
160.145.214.27	Fort McNair, Washington, DC
160.145.214.31	Fort McNair, Washington, DC
160.145.214.202	Fort McNair, Washington, DC
160.145.214.204	Fort McNair, Washington, DC
160.145.214.205	Fort McNair, Washington, DC
128.190.84.39	Alexandria, VA
128.190.130.16	Fort Belvoir, VA
128.190.178.21	Fort Belvoir, VA
128.190.224.22	Alexandria, VA
128.190.253.68	Fort A.P. Hill, VA
134.11.65.17	Arlington, VA
134.11.65.33	Alexandria, VA
134.11.237.129	Arlington, VA
134.66.12.64	Fort Irwin, CA
140.153.67.5	Fort Polk, LA
140.153.61.133	Hinton, WV

140.183.2.14 Fort Belvoir, VA

140.183.220.75 Fort Belvoir, VA

141.116.58.63 Arlington, VA

141.116.204.150 Pentagon, Arlington, VA

141.116.230.88 Pentagon, Arlington, VA

150.177.124.5 Fort Meade, MD

150.177.193.130 Fort Meade, MD

150.177.193.248 Fort Meade, MD

155.213.1.201 Fort Benning, GA

155.213.4.100 Fort Benning, GA

155.213.11.46 Fort Benning, GA

160.145.28.84 Fort Myer, VA

160.145.102.216 Fort McNair, DC

160.147.41.166 Fort Belvoir, VA

160.147.126.16 Fort Belvoir, VA

160.147.126.180 Fort Belvoir, VA

160.147.131.150 Alexandria, VA

160.151.76.10 Arlington, VA

160.151.76.56 Arlington, VA

160.151.77.78 Arlington, VA

160.151.77.118 Arlington, VA

(160.151.76.128)

199.114.42.111 Rosslyn, VA

199.122.33.10 Alexandria, VA

199.122.33.24 Alexandria, VA

199.122.41.3 Fort Meade, MD

199.122.45.7 Alexandria, VA

204.34.24.217 Great Lakes, MI

214.3.73.14 Alexandria, VA

As a result of such conduct, the defendant intentionally caused damage without authorization by impairing the integrity and availability of data, programs, systems and information, and that damage caused loss

aggregating more than $5,000 in value during a one-year period to the United States Army.

(All in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(i) and 1030(a)(5)(B)(i)).

COUNT 3

(Fraud and Related Activity in Connection with Computers)

THE GRAND JURY FURTHER CHARGES THAT:

6. From in or about March 2001, through on or about March 19, 2002, within the Eastern District of Virginia, and elsewhere, the defendant GARY MCKINNON did knowingly cause the transmission of codes, information and commands, and as a result of such conduct, intentionally caused damage without authorization to protected computers, belonging to the United States Navy.

7. Specifically, the defendant intentionally accessed computers exclusively used by the United States Navy, which computers were used in interstate and foreign commerce and communication. Then, the defendant obtained administrator privileges on these computers and installed RemotelyAnywhere. On several of the computers, the defendant installed tools used for obtaining unauthorized access to computers and deleted system logs. The computers accessed and damaged by the defendant included the following:

IP Address	Location
144.247.5.1	Groton, CT
144.247.5.22	Groton, CT
144.247.5.6	Groton, CT
144.247.5.14	Groton, CT
144.247.5.17	Groton, CT
144.247.5.11	Groton, CT
144.247.5.5	Groton, CT
144.247.5.40	Groton, CT
144.247.5.29	Groton, CT
144.247.5.4	Groton, CT

144.247.5.10 Groton, CT

144.247.5.8 Groton, CT

144.247.5.3 Groton, CT

144.247.5.7 Groton, CT

198.97.72.252 Patuxent River, MD

199.211.89.77 Crystal City, VA

(199.211.89.146)

131.158.84.161 Patuxent River, MD

131.158.65.9 Bethesda, MD

204.34.154.59 Pearl Harbor, HI

199.211.163.7 Wayne, PA

As a result of such conduct, the defendant intentionally caused damage without authorization by impairing the integrity and availability of data, programs, systems and information, and that damage caused loss aggregating more than $5,000 in value during a one-year period to the United States Navy.

(All in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(i) and 1030(a)(5)(B)(i)).

COUNT 4

(Fraud and Related Activity in Connection with Computers)

THE GRAND JURY FURTHER CHARGES THAT:

8. From in or about September 2001, through on or about March 19, 2002, within the Eastern District of Virginia, and elsewhere, the defendant GARY MCKINNON did knowingly cause the transmission of codes, information and commands, and as a result of such conduct, intentionally caused damage without authorization to protected computers, belonging to NASA.

9. Specifically, the defendant intentionally accessed computers exclusively used by NASA, which computers were used in interstate and foreign commerce and communication. Then, the defendant obtained administrator privileges on these computers and installed RemotelyAnywhere. On several of the computers, the defendant installed

tools used for obtaining unauthorized access to computers, deleted system log files and copied a file containing usernames and encrypted passwords. The computers accessed and damaged by the defendant included the following:

IP Address	Location
192.42.75.135	Hampton, VA
128.157.55.97	Houston, TX
198.122.128.114	Houston, TX
139.169.118.33	Houston, TX
139.169.118.28	Houston, TX
139.169.18.77	Houston, TX
128.183.158.148	Greenbelt, MD
198.116.200.1	Huntsville, AL
198.119.37.16	Greenbelt, MD
128.155.18.249	Hampton, VA
192.150.38.45	Moffett Field, CA
192.150.38.14	Moffett Field, CA
192.150.38.51	Moffett Field, CA
192.150.38.125	Moffett Field, CA
128.183.144.73	Greenbelt, MD
198.116.36.16	Herndon, VA

As a result of such conduct, the defendant intentionally caused damage without authorization by impairing the integrity and availability of data, programs, systems and information, and that damage caused loss aggregating more than $5,000 in value during a one-year period to NASA.

(All in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(i) and 1030(a)(5)(B)(i)).

COUNT 5

(Fraud and Related Activity in Connection with Computers)

THE GRAND JURY FURTHER CHARGES THAT:

10. Between in or about February 2001, and on or about March 19, 2002, within the Eastern District of Virginia, and elsewhere, the defendant GARY MCKINNON did knowingly cause the transmission of codes, information and commands, and as a result of such conduct, intentionally caused damage without authorization to protected computers, belonging to the United States Department of Defense.

11. Specifically, the defendant intentionally accessed computers exclusively used by the United States Department of Defense, which computes were used in interstate and foreign commerce and communication. Then, the defendant obtained administrator privileges on this computer and installed RemotelyAnywhere. The defendant accessed and damaged the following computers:

IP Address	Location
150.177.2.192	Fort Meade, MD
150.177.178.130	Fort Meade, MD

As a result of such conduct, the defendant intentionally caused damage without authorization by impairing the integrity and availability of data, programs, a system and information, and that damage caused loss aggregating more than $5,000 in value during a one-year period to the United States Department of Defense.

(All in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(i) and 1030(a)(5)(B)(i)).

COUNT 6

(Fraud and Related Activity in Connection with Computers)

THE GRAND JURY FURTHER CHARGES THAT:

12. Between in or about February 2001, and on or about March 19, 2002, within the Eastern District of Virginia, and elsewhere, the defendant GARY MCKINNON did knowingly cause the transmission of codes, information and commands, and as a result of such conduct, intentionally caused damage without authorization to a protected computer, belonging to the United States Air Force.

13. Specifically, the defendant intentionally accessed a computer exclusively used by the United States Air Force, which computer was used in interstate and foreign commerce and communication. Then, the defendant obtained administrator privileges on this computer and installed RemotelyAnywhere. The defendant accessed and damaged the following computer:

IP Address	Location
209.22.51.6	Crystal City, VA

As a result of such conduct, the defendant intentionally caused damage without authorization by impairing the integrity and availability of data, programs, a system and information, and that damage caused loss aggregating more than $5,000 in value during a one-year period to the United States Air Force.

(All in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(i) and 1030(a)(5)(B)(i)).

COUNT 7

(Fraud and Related Activity in Connection with Computers)

THE GRAND JURY FURTHER CHARGES THAT:

14. From in or about September 2001 through on or about March 19, 2002, within the Eastern District of Virginia, and elsewhere, the defendant GARY MCKINNON did knowingly cause the transmission of codes, information and commands, and as a result of such conduct, intentionally caused damage without authorization to protected computers, belonging to the companies identified in paragraph 15.

15. Specifically, the defendant intentionally accessed computers belonging to the companies identified below, with the Internet Protocol addresses and locations described below, which computers were used in interstate and foreign commerce and communication.

IP Address	Location	Company
204.2.33.22	Houston, TX	Tobin International
128.169.32.181	Knoxville, TN	University of Tennessee
206.245.175.40	Wayne, PA	Frontline Solutions

206.218.158.90 LaFourche, LA Louisiana Technical College

206.166.40.243 Colfax, IL Martin Township Library

206.245.141.46 Bethlehem, PA Bethlehem Public Library

Then, the defendant obtained administrator privileges and installed RemotelyAnywhere. On some of the computers, the defendant installed tools used for obtaining unauthorized access to computers. As a result of such conduct, the defendant intentionally caused damage without authorization by impairing the integrity and availability of data, programs, systems and information, and that damage caused loss aggregating more than $5,000 in value during a one-year period to the identified companies.

(All in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(i) and 1030(a)(5)(B)(i)).

A TRUE BILL

FOREPERSON

Paul J. McNulty

United States Attorney

By:

Justin W. Williams

Assistant United States Attorney

Chief, Criminal Division

Scott J. Stein

Michael J. Elston

Assistant United States Attorneys

Appendix 4

Federal Rules of Evidence (2012)

Article IX.

Authentication and Identification

Rule 901. Authenticating or Identifying Evidence

(a) In General. To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.

(b) Examples. The following are examples only — not a complete list — of evidence that satisfies the requirement:

(1) *Testimony of a Witness with Knowledge.* Testimony that an item is what it is claimed to be.

(2) *Non-expert Opinion about Handwriting.* A non-expert's opinion that handwriting is genuine based on a familiarity with it that was not acquired for the current litigation.

(3) *Comparison by an Expert Witness or the Trier of Fact.* A comparison with an authenticated specimen by an expert witness or the trier of fact.

(4) *Distinctive Characteristics and the Like.* The appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances.

(5) *Opinion about a Voice.* An opinion identifying a person's voice — whether heard firsthand or through mechanical or electronic transmission or recording — based on hearing the voice at any time under circumstances that connect it with the alleged speaker.

(6) *Evidence about a Telephone Conversation.* For a telephone conversation, evidence that a call was made to the number assigned at the time to:
(A) a particular person, if circumstances, including self-identification, show that the person answering was the one called; or
(B) a particular business, if the call was made to a business and the call related to business reasonably transacted over the telephone.

(7) *Evidence About Public Records.* Evidence that:
(A) a document was recorded or filed in a public office as authorized by law; or
(B) a purported public record or statement is from the office where items of this kind are kept.

(8) *Evidence about Ancient Documents or Data Compilations.* For a document or data compilation, evidence that it:
(A) is in a condition that creates no suspicion about its authenticity;
(B) was in a place where, if authentic, it would likely be; and
(C) is at least 20 years old when offered.

(9) *Evidence about a Process or System.* Evidence describing a process or system and showing that it produces an accurate result.

(10) *Methods Provided by a Statute or Rule.* Any method of authentication or identification allowed by a federal statute or a rule prescribed by the Supreme Court.