UNIVERSITY OF NAIROBI
COLLEGE OF BIOLOGICAL AND PHYSICAL SCIENCES
SCHOOL OF COMPUTING AND INFORMATICS

An Investigation of Digital Forensic Models Applicable in the Public Sector

(A case of Kenya National Audit Office)

MARTIN KIOKO KILUNGU

Registration: P53/64908/2013

Supervisor

Dr. Elisha Abade

This Research Project is submitted as Partial Fulfillment for the Award of Master of Science Degree in Distributed Computing Technologies of the University of Nairobi.

March 2015

Student Declaration

This research project being presented is my original work and has not been presented for the award of any university degree.

Sign …………………………….. **Date ………………**

P53/64908/2013

Martin Kioko Kilungu

This research project is submitted as partial fulfillment for the award of Master of Science Degree in Distributed Computing Technologies with my approval as the university supervisor.

Sign ………………………………. **Date …………………**

Elisha Abade

Supervisor

DEDICATION

I dedicate this research project to my loving mum for her providence, inspiration and love.

ACKNOWLEDGEMENT

I thank my supervisor for the dedicated guidance in undertaking and writing this research project. I also wish to express my sincere gratitude to my colleague, Jeremy, for proofreading the report, and Fredrick my research assistant for his contribution. Last but not least, I would like to appreciate my family members for their continued love and support.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBREVIATIONS

CD – Compact Disk

CDMA – Code Division Multiple Access

CFE – Certified Forensics Examiner

CISA – Certified Information Systems Auditor

DOS – Disk operating System

FBI – Federal Bureau of Investigations

FTK – Forensic Toolkit

GSM – Global System for Mobile Communications

GUI – Graphical User Interface

HTML – Hypertext Markup Language

ICT – Information and Communication Technology

IM – Instant Message

LAN – Local Area Network

NIST – National Institute of Standards and Technology

PDA – Personal Digital Assistant

PIN – Personal Identification Number

ROM – Read Only Memory

SIM – Subscriber Identity Module

SMS – Short Message Service

TDMA – Time Division Multiple Access

TSK – The Sleuth Kit

USB – Universal Service Bus

WAN – Wide Area Network

ABSTRACT

Digital forensics is a relatively new field in technology which deals with investigation of computer related crimes. The rapid technological growth poses a serious challenge to traditional paper-based forensic investigations. The use of computer systems and the emergence of youthful and technology savvy employees in the public sector are two challenges faced by forensic investigators. This research project reviewed the current state of computer-related crimes and the need for digital forensics in the public sector. Similarly, several digital forensic models used in computer and mobile phone forensics were reviewed. This study took a descriptive approach. The research covered Kenya National Audit Office which has branches spread across the country. Two types of data were collected. Level 1 data collection involved administering questionnaires to a random sample of KENAO staff. This data was then analyzed using both SPSS and Microsoft Excel. Level 2 data collection involved extracting computer images using Linux Mint. This data was analyzed using Microsoft Excel in level one, and using Pro Discover Basic and the Sleuth Kit, in level two. The results from both Level 1 and Level 2 data analysis were presented in a comparative format using tables, pie charts, and bar graphs and interpreted in form of notes. Finally, limitations and conclusions of the study were drawn and recommendations made based on the results obtained.

CHAPTER ONE

1.0 INTRODUCTION

1.1 Background to the Problem

The use of computers in personal, industrial, academia, governmental and other areas of life has changed the world positively (Reith et al. 2002). Contrary, technological advancement has led to increased numbers of computer related incidences and crimes. Digital forensics is used to describe the process of investigating and analyzing evidence, data or information magnetically stored in electronic format. According to Sansurooah (2008), computer forensic analysts should follow clear, well defined methodologies and procedures with expectation of being flexible in case of unusual circumstances. Wilson (2006) argues that employees are turning to the computer to commit crimes for various reasons thus posing a threat to the computer systems in an organization. This is made more complex by the fact that blocking insider attacks is even harder. According to Vasudevan (2004), the aim of forensic investigation is legal determination whether fraud has actually occurred and naming the person(s) involved, with a view to take legal action. The same author states that, the techniques and procedures used for forensic investigation should produce evidence that proves beyond reasonable doubt that somebody has either committed a crime or not. The use of manual techniques by public fraud investigators is becoming outdated due to adoption of technology (Kenya National Audit Office 2013). The high rate of technology evolution in Kenya has led to more complicated computer related crimes according to the GOK Cyber Security Strategy (2013). The Kenya Cyber Security Report released in June 2014 by the Telecommunications Service Providers Association indicates that the country is losing KShs.5 Billion annually to cybercrime. According to the report, top attacks originate from Germany and Kenya itself. Top issues noted in the report include insider threats by employees, telecommunication threats, social media, mobile banking and cyber espionage, respectively. With current employees topping the list of threats according to the report, much has to be done to address computer-related crimes.

1.2 Problem Statement

According to the forensic audit guide by KENAO (2013), public forensic investigators from the office use paper oriented techniques in their investigations, and only use their computers to prepare reports. While evidence can be found in paper files and documents saved in the computers of suspects, the complexity of computer systems renders the forensic investigation difficult to undertake. Some of the fraudulent files are deleted, encrypted or hidden by the suspect to avoid detection. Using manual techniques, it is difficult to get relevant evidence and adequate facts about the suspected crime and thus the evidence produced cannot sustain a case against the accused person before a court of law. This in itself defeats the purpose of forensic investigation. The application of a reliable digital forensic model in forensic investigations and the use of suitable digital forensic tools can seal the holes that would have otherwise emerged in the acquired evidence. The purpose of this research is therefore to review some of the existing digital forensic models, then adopt the most suitable that can be used to conduct investigations in the public sector. The expected outcome will be the adoption of the most suitable digital forensics model for use in the public sector and the proposal of a suitable tool that can work well with the said model. The findings will also be used to make recommendations for future research.

1.3 Objectives of the Study

The research project aims to achieve the following objectives:

1.3.1 Overall Objective

To review various models used in digital forensics that can be used in the public sector in Kenya, adopt the most suitable model, and test its applicability.

1.3.2 Specific Objectives of the Study

1. To establish the adequateness of the current forensics methodology used in the public sector.
2. To review digital forensic models that can be used in the public sector, and propose the most suitable for adoption.
3. To test the applicability of the selected digital forensic model for adoption.
4. To identify and verify an effective and efficient forensic tool usable with the model.

1.4 Research Questions

The study aims to answer the following questions:

1. How adequate is the current methodology used for forensic investigations in the public sector?
2. Which digital forensic models can be used in the public sector and which is the most suitable for adoption?
3. Is the adopted digital forensics model applicable and able to produce valid results?
4. Which is the most effective and efficient forensic tool that can be used with the model?

1.5 Justification of the Research Study

The continuous adoption of technology by government implies that in coming years, most of the government processes and services will be computerized. The mobile phone is also becoming a crucial tool not only for personal use, but also for office use. This means that fraud and crimes committed using these devices will continue to increase. This study will be useful in that it will adopt a model that can be applied to ensure forensic investigations produce more detailed and reliable findings that can be used to reveal whether crime was committed, how it was committed, when it was committed and the person (s) responsible for it. Since adoption of a forensic report by court has serious consequences, it is only fair that effort is put to determine whether fraud occurred. By adopting digital forensics, hiring and training forensic professionals and applying a proper model and tools, KENAO will be able to produce more valuable forensic reports.

1.6 Assumptions and Limitations of the Study

1. Research would be intended to propose implementation of a digital forensics model applicable in the entire public sector. It may not be possible to carry out the study on entire sector due to time and cost constraints, and therefore sampling will be used.
2. Since the research will involve government officers and resources, it is assumed that there will be cooperation from the information providers and the organization targeted.

1.7 Significance of the Study

The application of a proper approach in forensic investigations in the public sector will lead to more reliable findings and sustainable evidence. This is because it will be possible to recover data and files deleted or hidden which will lead to more concrete evidence. Digital forensics in government will discourage crimes and corruption committed using modern technologies. Once employees know that it is possible to engage in corruption using a mobile phone or computer and get caught even after deleting all related files and other related communication, corruption in the public sector will reduce. In addition, lessons learned during investigations on how crime is committed through, and around the computer will be useful in implementing effective and reliable computer security controls. Lastly, the study will make recommendations for future areas of research.

1.8 Scope of the Study

The research will be carried out in Kenya National Audit Office (KENAO) offices across the country. It will include offices under central government, county governments, state corporations, and independent commissions.

CHAPTER TWO

2.0 LITERATURE REVIEW

2.1 Introduction

This chapter will focus on review of existing literature related to digital forensics, the techniques used as well as existing methodologies. It will specifically narrow down to computer forensics on Windows environment and Android mobile phone forensics due to their popularity in Kenya. The literature review will also capture the current state of cybercrime and digital forensics in Kenya.

2.2 Overview of Digital Forensics

Reith et al. (2002) defines digital forensic as, "the use of scientifically derived and proven 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, or helping to anticipate unauthorized actions shown to be disruptive to planned operations."

Rogers et al. (2006) says that with the cyber criminals growing their tactics and changing with technological advancement to adopt more sophisticated methods, the field of computer forensics is expected to continue to grow. As new innovations continue to hit the market, and the use of computers and other technology devices continue to expand, the need for computer forensics will become more vital. In their research, Bashir and Khan (2013) indicated that malicious tools and software are being designed and implemented in an equal measure to technological growth to exploit the networks and data storage associated with them to extract private information with an objective of committing crime. People are using computers and mobile phones to deal with their relationships, family issues, business matters, family among other issues. This has been a key motivator to the increase in cybercrime. In the last two decades, the use of smart phones specifically android mobile phones has become one of the main methods of communication.

With continuous advancement in technology, smart phones are becoming more popular due to their many functionalities and features (Lessard and Kessler 2010). This has led to conviction that these devices contain evidence that can be helpful in investigating and determining crimes.

2.3 Current State of Cybercrime and Digital Forensics

According to Dezfoli et al. (2013), in the previous decades investigators gathered digital evidence from monolithic, stand-alone mainframes. Nowadays, we have personal computers, super computers, client-server networks, mobile phones, laptops, LANs and WANs conveying information across the globe. The rapid change in technology involving computers and mobile devices has led to wide use of such devices in criminal activities and putting in place adequate and efficient security measures has proven to be a difficult endeavor. There has also been the emergence of a trend whereby every existing device is being interconnected into a network of other devices, both household and office devices Lammle (2011). This has made investigations relating to such devices even more difficult.

The 2014 US report on Cyber Security indicates that most organizations cannot match the persistence, skills, and technological prowess of their potential attackers. The report goes on to state that common criminals, organized groups, and even nations leverage sophisticated techniques to make attacks that are very targeted and complex to detect. Most attackers target valuable, sensitive and confidential information. The Kenyan cyber security landscape is changing fast as more and more organizations are becoming victims to intrusion and exploitation. According to Serianu Cyber Security report 2014, the fast growing digitally enabled operating ecosystem in Kenya is characterized by increasingly sophisticated insiders and outsiders launching more frequent and targeted attacks.

2.4 The Need for Digital Forensics

Imtiaz (2004), states that, “A single security breach or attack can cause great financial and reputation loss, which can be devastating for a well-known organization. As security experts are trying their best to defend against the latest forms of attacks, attackers are moving on devising plans and potentials for more sophisticated attacks. ”

The author explains that most security attacks leave behind some trails which can be used by forensic investigators to track down the attacker.

In the modern society, the adoption of technology as the method of choice for communication has made computer-based information a primary source of evidence in many legal investigations. People of different races, culture and age are spending many hours of their day hooked to one form of technology device or another whether at home, school or work place. According to Gartner, a global research firm, “worldwide sales of smart phones to end users totalled 968 million units in 2013, an increase of 42.3% from 2012.” According to the research, smartphone sales accounted for 53.6% of mobile phones sold during the year 2013, with Android mobile phones leading in sales at 66.4%. Also, a research conducted by World Bank in Kenya and South Africa in 2013, indicated that Kenya was among the leading countries in Africa in terms of mobile phone penetration at 75.4%. This was a 4% increase from the previous year going by iHub Kenya 2012 report that indicated there were 28 million mobile phone subscribers in Kenya estimated to be 71% of the population. Mohtasebi and Dehghantanha (2013), notes that the advancement in smartphone capabilities has enabled users to store and manage large amounts of information about their lives, both personal and professional. Sansurooah (2006) argues that, due to technological improvement, 93% of all organizations’ communication in Australia was created electronically, with the remaining being communication ever printed as at 2006. This has led to increased risk and computer misuse related incidences raising awareness in both public and private sectors of the need to develop defensive and offensive responses. The Kenya Cyber Security Report 2014, released by Serium Consultants, indicates that technology adoption is driving business innovation and growth in Kenya, and at the same time, it is exposing the country to new and emerging threats. Cyber-terrorists, spies, hackers, and fraudsters are increasingly motivated to target ICT infrastructure due to the increasing value of information held within it, driven by the perceived lower risk of detection and capture as compared to traditional crime. With the increasing adoption of technology, the nation faces evolving cyber threat landscape. In view of the above pointers, computers and mobile phones may become the most reliable sources of accurate and reliable evidence for prosecuting criminal cases and thus digital forensics will be critical in investigating such crimes.

2.5 Digital Forensic Models

In line with the scope described earlier, we review some of the models used in computer and mobile phone forensics.

2.5.1 Mobile Phone Forensics Models

We review the following two models:

1. Smartphone forensic investigation process model
2. CDCD-5 an improved mobile forensics model

Smartphone Forensic Investigation Process Model

According to Goel et al. (2012), this model consists of the following subsequent steps:

Phase 1: Preparation

This phase entails understanding the crime committed and the activities surrounding the suspected crime. The relevant tools and materials that may be needed are assembled, the right team combination is assembled and roles assigned. A systematic approach is mapped out considering technical, legal and business matters. Legal constraints and jurisdictions must be factored. Search warrants, management support, rights of suspect and authorizations must not be overlooked. Notification to all parties and also any relevant team training are done at this stage.

Phase 2: Securing the scene

This involves preventing contamination of evidence and ensuring the security of the scene of crime from unauthorized access. Systematic and secure custody of evidence is a major concern and thus the number of people involved must be decreased and no unauthorized people should be allowed. Safety of the investigators must also be ensured.

Phase 3: Documenting the scene

Documentation involves recording all actions at every stage. The state of the mobile phone immediately after the crime and any visible data must be recorded to help reconstruct the crime. Sketches, maps, and photographs may also be useful at this stage. A log of all the people in the crime scene, grouped according to their roles along with a summary of their actions and any tools used must be maintained.

Phase 4: PDA mode

i) Active mode: When the device is running, it has to first be shielded from network and no communication should be done with it to avoid volatile evidence contamination.

ii) In-active mode: When the device is off, it should be left in that state to avoid overwriting old data.

Phase 5: Communication shielding

This step emphasizes the need to block further communication from the device. This is important to avoid overwriting existing information. All communication avenues including any USB or serial cable connections must be disabled.

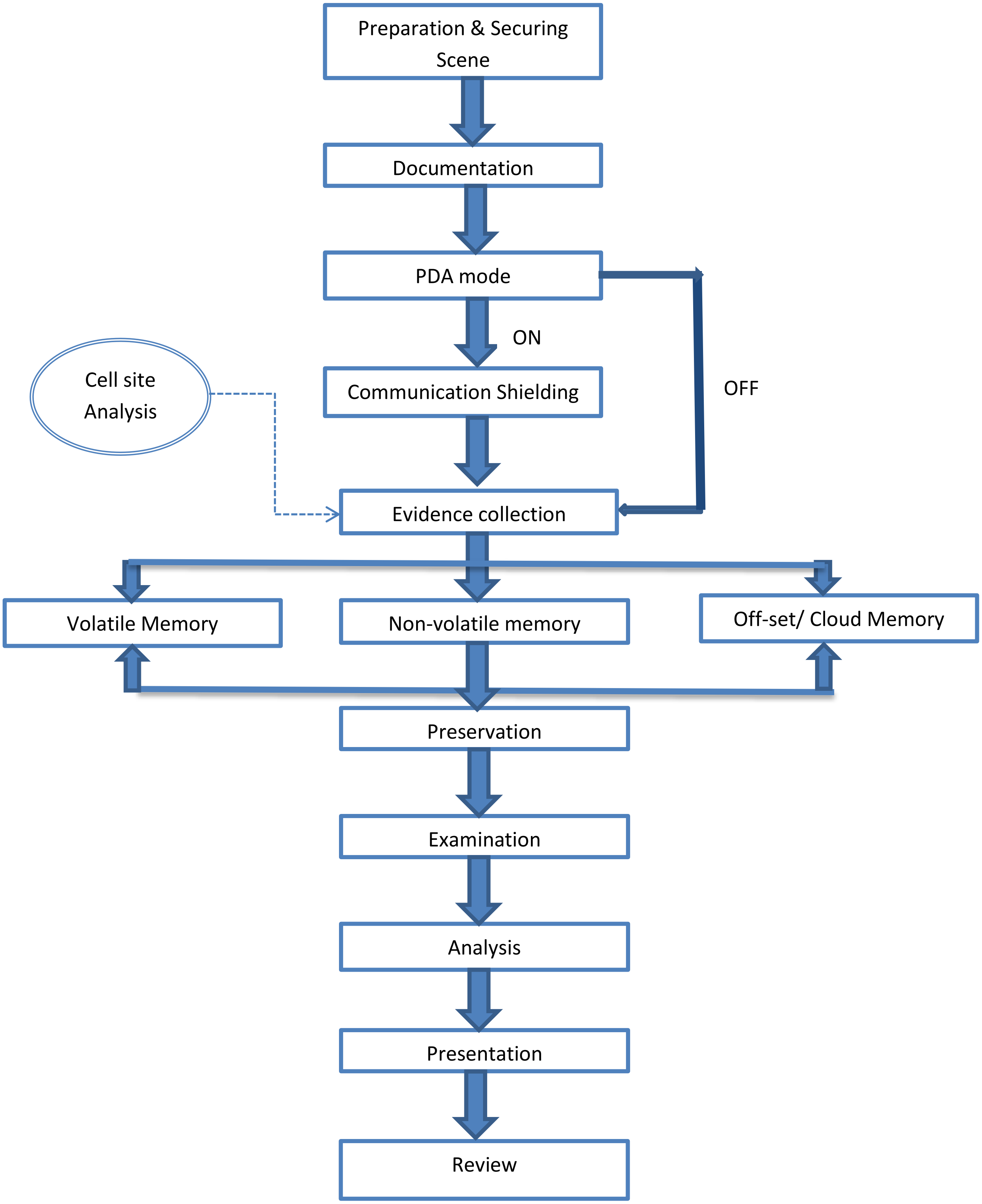


Figure 2.5.1: Smartphone forensic investigation process model

Source: Goel et al. (2012)

Phase 6: Volatile evidence collection

Volatile information is easily contaminated especially should the device change state. Also in case of device losing power, volatile data will be lost thus effort must be made to sustain it. Alternatively, the volatile memory can be imaged using available acquisition tools.

Phase 7: Non-volatile evidence collection

This involves extraction of data from external storage devices like Compact Flash (CF) cards, Secure Digital (SD) cards, and USB memory stick. Evidence from computers synchronized to the device in question must be acquired. Other related items like passwords on paper and user manuals are also collected. Lastly, hashing and write protection of the device are done to ensure integrity and authenticity.

Phase 8: Off-set

This involves searching for evidence that could be stored in the cloud using the suspected smart phone.

Phase 9: Cell-site Analysis

This deals with establishing specific positions where mobile phone has been or where it is currently. It gives record of location for both the sending and receiving device. It identifies the geographical location of the originating and terminating device of any communication and can be used to support the fact that a suspect was at the alleged location at the time of crime.

Phase 10: Preservation

This step involves packaging, transportation and storage of evidence. Once evidence is identified and labeled, it is packaged in non-static bag to avoid damage. Precaution should be taken to avoid excessive pressures, humidity and temperatures during transportation and storage. Throughout the entire process, proper chain of custody must be maintained and unauthorized people should not gain access to the evidence.

Phase 11: Examination

This involves data filtering, validation, pattern matching and searching for particular key words with regard to nature of crime. Items like address book, appointments, calendars, schedulers, text messages and voice messages, documents and emails are examined in detail. Evidence is also sought for system tampering, data hiding or deleting utilities and unauthorized system modifications. Recovery of hidden or obscured information is a tedious but critical exercise that should be carried out. At this stage collected volatile and non-volatile evidence is analyzed and backups taken. Everything done and the person doing it must be documented. Hashing functions should be used for mathematical authentication of the data.

Phase 12: Analysis

This phase involves analyzing hidden data, determining significance of information collected, reconstructing the event data and arriving at proper conclusions. The analysis should be done in a manner to ensure that chain of evidence and timeline of events are consistent. The use of a combination of tools can lead to better results. According to the National Institute of Justice Guidelines (2004), timeline analysis, hidden data analysis, application analysis, and file analysis should be carried out at this stage.

Phase 13: Presentation

This entails presenting findings of the investigation before the relevant authority. The alleged crimes are either confirmed or discarded. The report must contain a detailed summary of the events that took place and a complete description of all the steps taken during the investigation. Other things presented along the report are items found at the crime scene, chain of custody documents, print outs and photographs of various items of evidence. Complex terminology, methodologies and tools used must be explained in writing.

Phase 14: Review

In this phase, the steps followed during the investigation and areas of improvements are reviewed. Results of the investigation can be used together with their interpretations to guide similar exercises in future. It should be noted that iteration is usually repeated several times between examination and analysis to get a clear picture of the incident. This can be applied in future to establish better procedures and policies.

An Improved Mobile Forensics Model

As Shah and Bansal (2012) have demonstrated, the improved mobile forensics model, commonly known as the CDCD model, consists of the following 5 steps:

1. Hypothesis
2. Condition of the cell phone
3. Data extraction
4. Collection of evidence
5. Documentation

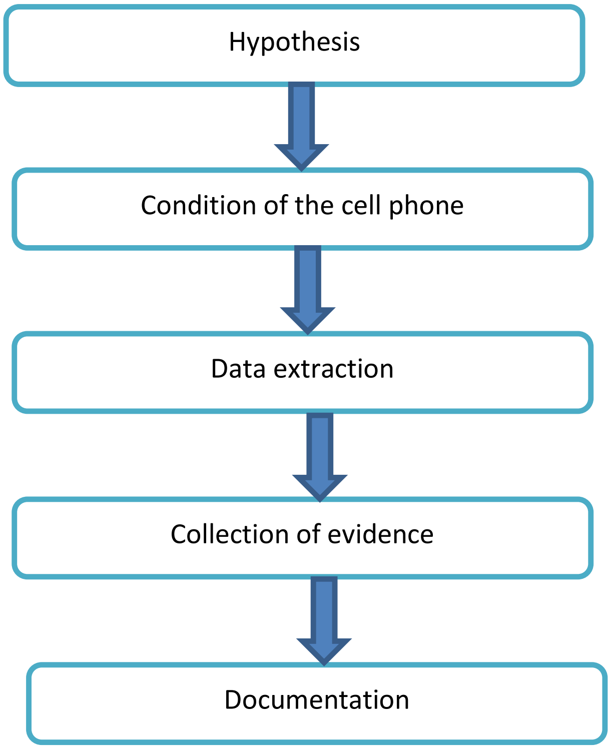


Figure 2.5.2: An improved mobile forensics model

Source: Shah and Bansal (2012)

Phase 1: Hypothesis

This is a logical approach in an effort to address a crime case. Before preparations, the examiner must first understand the crime scene and then prepare a hypothetical evidence list. After the hypothesis, investigator must visualize the scene of crime and then try to relate the evidence. This step is purely based on experience. It enables him to decide whether evidence has to be collected and the type of tools to use depending on the expected situation.

Phase 2: Condition of the cell phone

Here the examiner verifies whether the phone is operational or not which determines the method selected for purposes of data collection.

The key thing here is whether the mobile phone is ON or OFF. If it is OFF, it must never be turned on to avoid evidence contamination especially volatile data.

Phase 3: Data extraction

This is the most important phase where examiner interacts with the phone via software or hardware. The right tools may at this stage be used to extract data depending on the type of mobile phone. Some of the evidence that could be found include: SMS, Call logs, contacts, stored drafts, notes, reminders, internet history, images and installed applications.

Phase 4: Collection of evidence

Evidence refers to the physical prove of crime and its type depends on the nature of crime at hand. Different crimes need different evidence. The investigator creates a table of all extracted evidence.

Phase 5: Documentation

The extracted evidence is arranged logically in form of a document ready to be presented to the relevant authorities. The document produced is a summary of the case and evidence obtained indicating whether crime was committed by the suspect or not.

2.5.2 Computer Forensic Models

The following five models on computer forensics investigation process are reviewed in this study with an aim to extract the major phases that can be applied in a forensic audit environment.

1. First Digital forensics research workshop model - 2001
2. Computer forensics field triage process model - 2006
3. Cyber tools online search for evidence model - 2006
4. Digital forensic model based on Malaysian investigation process - 2009
5. The generic computer forensic investigation model - 2011

1. First Digital Forensic Research Workshop Model

During the First Digital Forensic Research Workshop (DFRWS) in the year 2001, a forensics model called the DFRWS model was proposed (Palmer 2001). It consists of six phases as shown in figure 2.5.3:

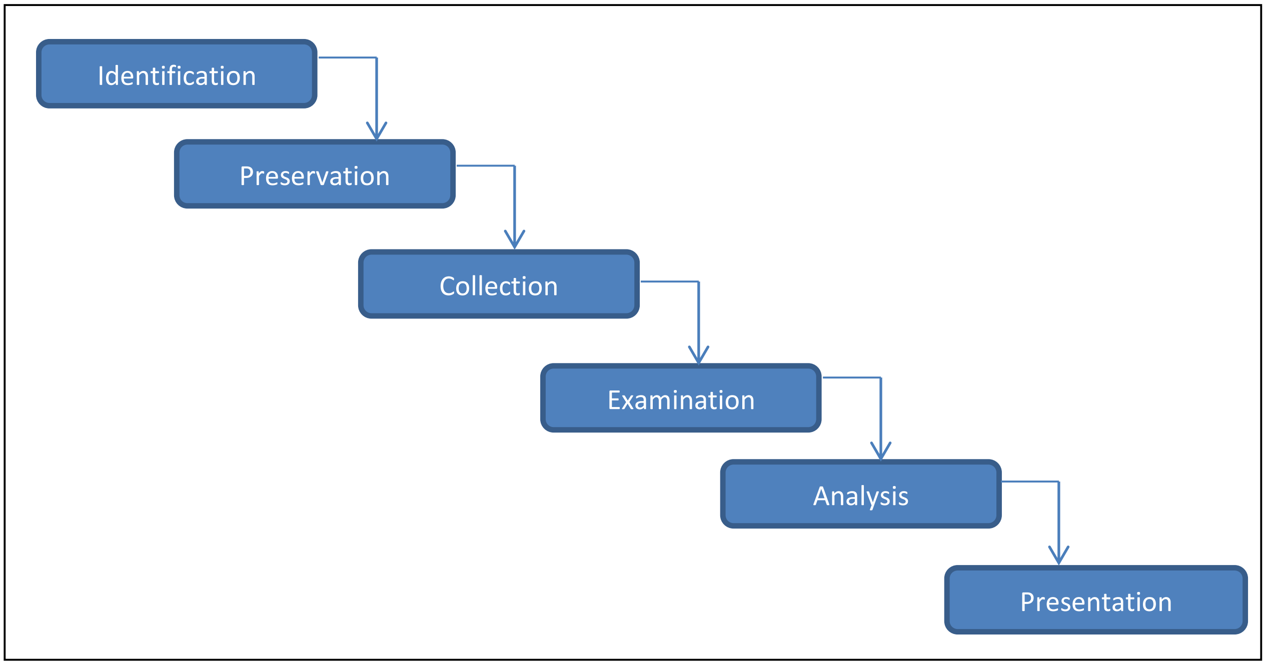


Figure 2.5.3: First Digital forensics research workshop model

Source: Palmer (2001)

This model is not comprehensive but rather basic and meant to be a basis for more comprehensive models and as a basis framework for future research. It only mentions the few tasks under each step without giving full details on how to perform them.

The model also gives room to go backwards from one step to another during the investigation process though it is presented as a linear method.

2. Cyber Tools Online Search for Evidence (CTOSE) Model

This model was devised by a research funded by the European Union. The methodology, as described by Sansurooah (2006), aims at providing a consistent approach for identifying, preserving, analyzing and presenting digital evidence.

The purpose of that model is based on the acquisition of digital evidence and how it is to be collected, conserved and analyzed in such a way that the source will not be subject to tampering and that it will be legally admissible should court proceedings be instigated.

The Investigation Process

The basic inherent process to computer forensics can be outlined as shown below:

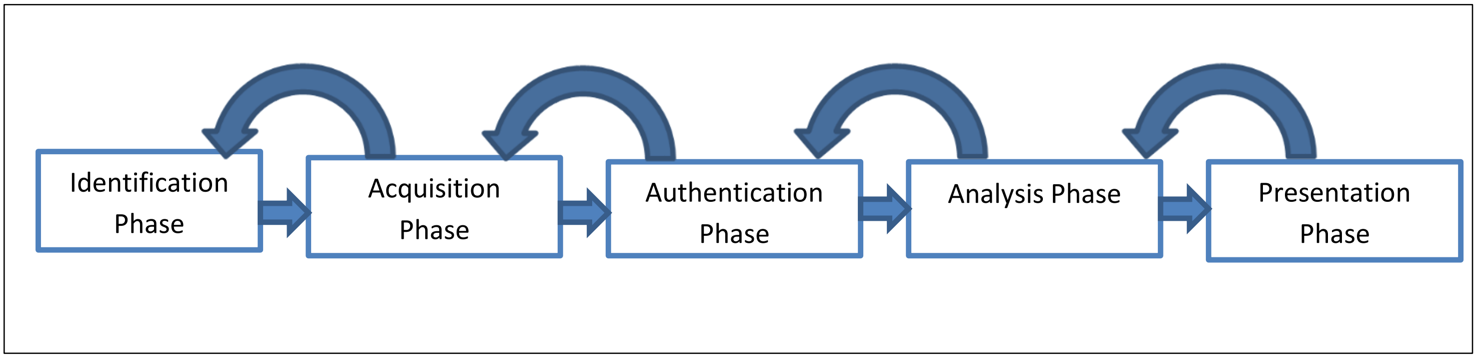


Figure 2.5.4: the Cyber Tools Online Search for Evidence Model

Source: Sansurooah (2006)

These phases are described below:

a. Identification Phase

Identification deals with intelligence gathering of information. At this stage, the examiner needs information about the evidence being sought.

Critical issues here are the possible sources to target, how to go about the information collection, acquisition actions that will be needed, and the order in which the information should be seized. The examiner is able to foresee the challenges that will be encountered during analysis and presentation phases and try to provide for them.

b. Acquisition of Evidence Phase

The aim of this phase is to obtain copies of all digital evidence that will be required during the analysis stage. Special forensic tool should be used since the act of simply booting the computer changes the nature of data on disks drives connected to the computer. This may result in vast amounts of data being destroyed or altered before it can be imaged. This acquisition of digital evidence would be snapshots and live datasets. All snapshot data sources are to be seized or forensically imaged and live data is acquired in a valid way and the chain of custody should be maintained. During acquisition, procedures used must ensure that acquired evidence is acceptable in a legal proceeding and can be duplicated and if necessary should be done by an independent third party.

c. Authentication Phase

It is difficult to show that evidence that was gathered during seizure is the same as the one left behind by the criminal. Digital forensics allows investigator to prove that the evidence did not change or get altered after it was collected. By using timestamps, it is possible to demonstrate that the evidence did not change after collection.

Simple techniques enable investigator to demonstrate that the evidence was in existence at the specific time it is claimed to have been collected.

The investigator must create a hash value after collection to help in this task. When data is initially collected, investigator should create a hash value and record it as it is. The investigator can still prove that the acquired evidence is still identical to the original source by comparing the hash values of both the image and the original source.

d. Analysis Phase

This stage consists of two steps:

Preparation – Preparing the working directories on separate media to which evidentiary files and data can be recovered or extracted.

Extraction – Two types of data extraction exist for this model as shown:

-Physical extraction – This is extraction of data from the drive at the physical level regardless of the file systems present on the drive. It includes keyword searches and file curving.

-Logical extraction – This is extraction of data from the drive based on the file system(s) present on the drive such as deleted files, file slack and un allocated file space.

Analysis of extracted data – This deals with timeline analysis, data hiding analysis, application and file analysis.

e. Presentation Phase

This phase entails creating a report to present the final digital evidence obtained. The report must be a self-contained, self-explanatory written document in which all relevant details and actions taken during all the above phases are recorded. Documentation must be complete, accurate and comprehensive.

3. Digital Forensic Model Based on Malaysian Investigation Process

Perumal (2009) proposes a digital forensic investigation model from the Malaysian investigation process flow. The model consists of seven phases as shown in figure 2.5.5. As shown in the diagram, the first two phases, that is, planning and, identification are common in most digital forensic models. The Reconnaissance phase is concerned with collection of evidence from running systems commonly called live forensics. According to the author, acquiring live data which focuses on volatile evidence improves the probability of successful investigation. In the next two steps, data is securely moved and stored safely waiting for analysis. Next, the data is then examined with the right methods and tools. In presentation, just like in the other previous models, the investigator has to prove his or her findings. The last step deals with proper keeping of evidence for future.

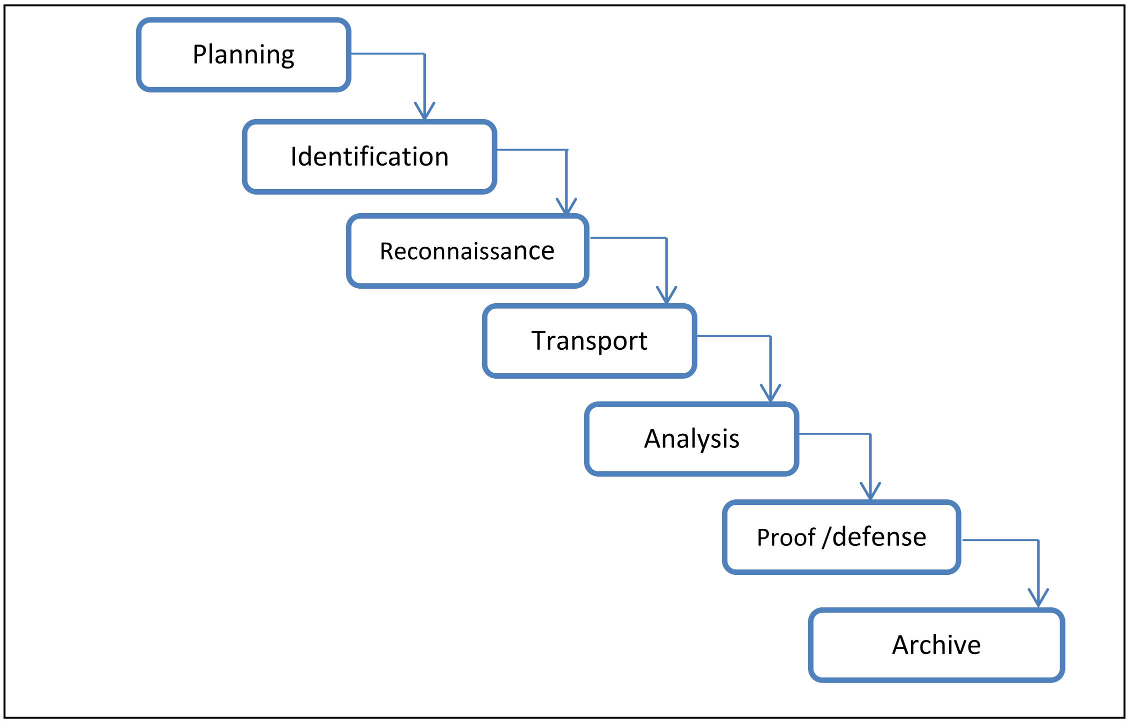


Figure 2.5.5: Digital forensic model based on Malaysian investigation process
Source: Perumal (2009)

4. Computer Forensics Field Triage Process Model – CFFTPM

Rogers et al. (2006) proposes a method of carrying out identification, analysis and interpretation of computer-based evidence within a short time without having to go to the laboratory. It is rather a quick method and again does not require taking complete images. This model has the following areas of focus:

1. To be able to get concrete evidence immediately
2. To identify any victims at further risk
3. To give direction to ongoing investigation
4. To ascertain any potential charges and accurately classify the culprit's ability

The CFFTPM model consists of six phases as shown in figure 2.5.6 below:

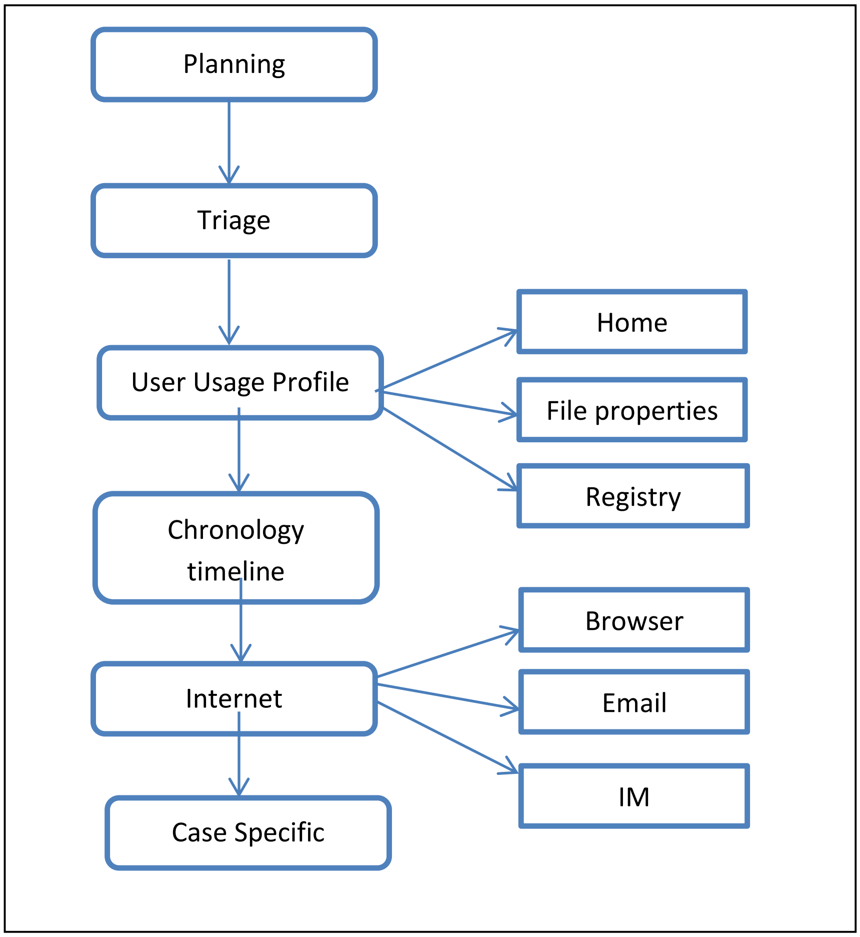


Figure 2.5.6: Computer forensics field triage process model
Source: Rogers et al. (2006)

Computer forensics field triage process model begins with the Planning Phase which is critical to improve the chances of successful investigation. The investigator is concerned about capabilities of the suspect, their activities, location, time and types of machines.

Second is the Triage Phase under which examiner identifies evidence and things are arranged according to importance and probably priorities. Of concern here are potential places in the systems where evidence could be located like volatile memory, temporary files among others. Information from the suspect is very critical in supporting the above revelations. Next is the Usage Profile Phase where the examiner focuses on the user's profile and activities and information found in home directory, system registries and file properties. After usage profile analysis, the investigator needs to build the case in a chronological order under the Chronology Timeline Phase which deals with issues to do with when a file was accessed, modified or created. In Internet Phase, examinations of relevant artifacts like instant message logs, web browsers and e-mails are done. It should be noted that e-mails require a lot of time to analyze but can yield very substantial evidence. The last phase in this model is Case Specific Evidence Phase**.** It is required that the investigator adjusts and focuses his attention to the case at hand depending on the type of crime. The approach is different for issues like child phonography, drug activity or financial crimes.

5. The Generic Computer Forensic Investigation Model (GCFIM)

The Generic Computer Forensic Investigation Model (GCFIM) was developed in 2011 and it is based on the study of more than ten preceding models developed between 1984 and 2010. According to Yusoff, Ismail and Hassan (2011), this model was arrived at after investigating the common phases in previous models. By grouping together overlapping phases in different models, regardless of the sub-steps and details of each phase, a high level forensic investigation model was derived. This model is shown in figure 2.5.7 below:

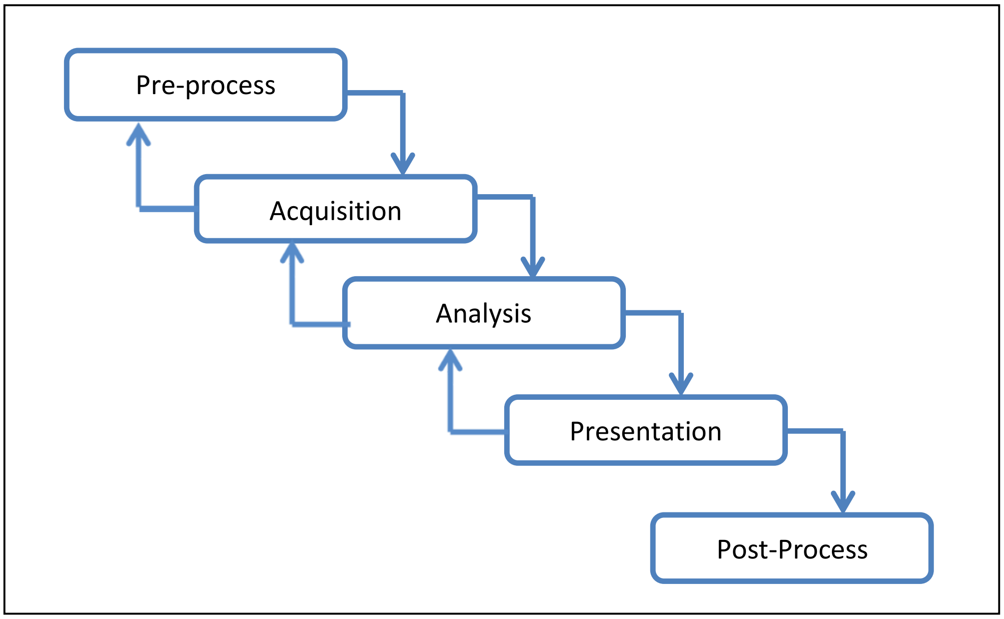


Figure 2.5.7: Generic computer forensic investigation model

Source: Yusoff, Ismail & Hassan (2011)

As shown in figure 2.5.7, the generic computer forensics investigation model consists of the following five steps:

1. Pre-process

Under this phase, all the tasks carried out prior to the real investigation and actual data collection is included. These include getting the necessary approvals and permissions from the authorities, preparing teams, techniques and tools to be used among other related tasks.

2. Acquisition and preservation

The tasks undertaken here include identification, acquisition, transportation, storage and preservation of data. It is in this stage where required data is captured and kept for analysis.

3. Analysis

Analysis is the core step in digital forensics. It is the step under which real detailed examination of collected data takes place. Various tools and techniques are used to analyze the data with an aim to identify crime details and the culprits responsible for it.

4.Presentation

In presentation, the documented findings are given to the relevant authority. Such reports and documentation must be understood by the target audience and must be supported with sufficient and admissible evidence. The aim here is for the examiner to uphold or dismiss the crime alleged to have been committed.

5. Post-process

This is the final stage in the investigation process and deals with conclusion of the investigation. All necessary evidence collected, both digital and physical, need to be returned to owners or kept safely. The investigator also requires a review of the investigative process with an objective to learn some lessons and probably make future adjustments and improvements.

2.6 Digital Forensics Tools

Digital forensics tools can be viewed as any technology which assists the forensic examiner in completing his/her forensic duties, for example, data extraction, data presentation and report processing like word processors and spreadsheets. However, the term is often used in digital forensics to refer only to those tools and techniques which extract and analyze data during a digital forensic exercise (Kleber and Galvao 2004). Bashir and Khan (2013) describe the various digital forensic tools used during the various phases of investigation process. These include Forensic toolkit, OS forensics, Autopsy, The sleuth kit, Wire shark, CAINE (Computer Aided Investigative Environment), COFEE (Computer Online Forensic Evidence Extractor) and DFF (Digital Forensic Framework). We review some of the tools that can be applied in the public sector.

a. The Sleuth Kit (TSK)

This is a UNIX systems open source tool kit for computer forensics. It is a command line based collection of executable commands. Kleber and Galvao (2004) explain that the user can use it to examine the computer file systems through a non-intrusive approach not depended on the operating system of the machine. TSK is able to recover hidden, deleted, and or compressed files. The results generated by TSK are used by another analysis tool called the Autopsy Forensic Browser which presents the user with a user-friendly graphical interface to analyze the results.

Features of the Sleuth Kit

TSK analyzes the file system images generated by the disk dump (dd) command, available in both UNIX and Windows. According to Kleber and Galvao (2004), the data format of the investigated partition does not depend on the operating system of the machine on which TSK is run.

Capabilities of the sleuth kit

1. It shows all the details and content of NTFS files attributed data streams.
2. It shows file system details and metadata structure.
3. It is used to create timelines of file activities exportable as report in excel.
4. It can visualize hash files in a hash database to customize databases that can be formed using the MD5sum tool.

b. Autopsy Forensic Browser

This is a HTML-based forensics tool that provides a graphical interface for Sleuth Kit that looks like a file manager, and shows deleted data information and file structures, and display the results on a HTML browser. Autopsy can work directly over image files and mounted partitions and is considered an interface for Sleuth Kit.

c. EnCase Toolkit

Encase can be used in a wide variety of digital investigations environments. It can be used on smartphones, removable media and hard drives and generates various reports.

According to the Encase Certified Examiner's study guide, Encase offers different options that can be used to acquire digital evidence. Each case in digital forensics is a unique endeavor, with its own set of challenges and encounters thus it requires the use of various acquisition methods.

EnCase requires a forensic boot disk which is required in booting the computer and to launch the operating system in a safe manner to ensure the media is not tampered with in any way.

d. Forensic Toolkit (FTK)

This is a commercial multipurpose tool which is commonly used to index digital evidence as described by Bashir and Khan (2013). It takes a snapshot of the disk drive and then makes a bit-to-bit copy for use in the analysis phase. This tool has many features and it is user-friendly. It offers various capabilities including registry view, easy-to-read logging, standalone disk imaging and direct e-mail analysis plus zip file analysis. It is an efficient all-inclusive tool that can be used at a reasonable cost.

2.6.1 Review of Some Tools used in Mobile Phone Forensics

The National Institute of Standards and Technology, (NIST, 2004) describes the following mobile phone forensic tools:

a. Cell Seizure

This is a forensic toolkit that allows investigators to search, examine and generate report on data available in a mobile phone. It is used in CDMA, TDMA and GSM networks.

It entails connecting a cable chosen from those available in the Cell Seizure toolbox which can be used as a link between the phone and a workstation. It could be USB or serial cable depending on the type of phone. It has extra features allowing investigator to bookmark files of interest for filtering.

Cell Seizure can produce reports with the following types of data.

1. Messages (inbox and outbox)
2. All numbers stored in phonebook
3. Call history (dialed numbers, received calls, missed calls)
4. Reminders and memos
5. Phone logos e.g. welcome note
6. Phone graphics like photos in camera among other details.

b. Oxygen Forensics Tool

Oxygen forensic suite is software used in digital forensics. This tool is used for extraction and analysis of data from cell phones, smartphones and tablets. It uses some advanced proprietary protocols that allow extraction of more data from smartphones than that extracted using logical forensic tools. Oxygen forensics tool offers capabilities for timeline analysis, social graph depiction and geo-location.

c. Open Source Android Forensics Toolkit

This is an all-inclusive solution to carry out forensics on Android OS devices. It uses sophisticated methods for collecting, analyzing and presenting information from Android devices in a format that meets most legal requirements. By use of this tool, the investigator can create new case or open an existing case, each being assigned a unique number. It has capabilities to extract and harsh data for safe storage. It enables investigator to see links to detailed criminal connections made through the Android device. This tool is able to categorize extracted information in an intuitive format.

2.7 Current Methodology used in Forensic Investigations

According to the Forensic audit manual developed by Kenya National Audit Office, the forensic audit investigation can be summarized as follows:

1. **Receipt of complaints**

At step one, all the complaints regarding fraud in the public sector are received and recorded for monitoring and tracking purposes.

2. **Complains analysis and prioritization**

All the received complaints are analyzed, the results are prioritized, documented and recommendations for further action are made.

3. **Planning**

For the complaints which require investigation, the team determines the required resources, personnel, scope, time and criteria to execute the investigation.

4. **Evidence gathering**

This step involves interviews, inspection, analysis and review of documents.

5. **Analysis**

Under this step, reasoned argument, re-performance of contested issues, and re-computations are carried out.

6. **Communication and reporting**

This component entails obtaining statements from the management, preparing investigation reports, and finally issuing the forensic audit report to the relevant authorities.

7. **Follow-up**

This deals with tracking and making follow-ups on the recommendations made.

2.8 Digital Forensics Conceptual Framework

2.8.1 Basis of the Framework

The Perumal (2009) digital forensic model based on Malaysian investigation process will be adopted in this study. This model is more relevant for use in public sector forensic investigations because three of its seven phases are found in the current model used in manual forensic investigations, i.e. planning, identification, and analysis. The model has a second benefit in that it is concerned with acquisition and analysis of digital devices while they are still operating. This is important in a forensic investigation environment where computers do not have to be taken away and therefore suitable for application to replace manual forensic investigation methodology. The digital forensic model based on Malaysian investigation process has been adopted because of the following reasons:

1. It allows on-site analysis of digital devices
2. It is time conscious in that less time is required to handle the computer in question thus no much interruption to organization's operations.
3. It offers convenience since no computers need to be carried to a laboratory.

Therefore the above features satisfy the requirements for the intended digital forensics model that can be used in the public sector in Kenya.

The adopted model consists of the following 7 steps:

1. Planning Phase

This is the first step and consists of two sub steps; authorization and obtaining search warrant.

It involves getting authority from local enforcement team and securing a search warrant to seize items needed for evidence. It is a compulsory procedure in every legal cybercrime investigation, though sometimes it can just be inform of verbal authorization before the investigator proceeds to investigate an organization's computer systems.

The detailed adopted digital forensic model is shown below:

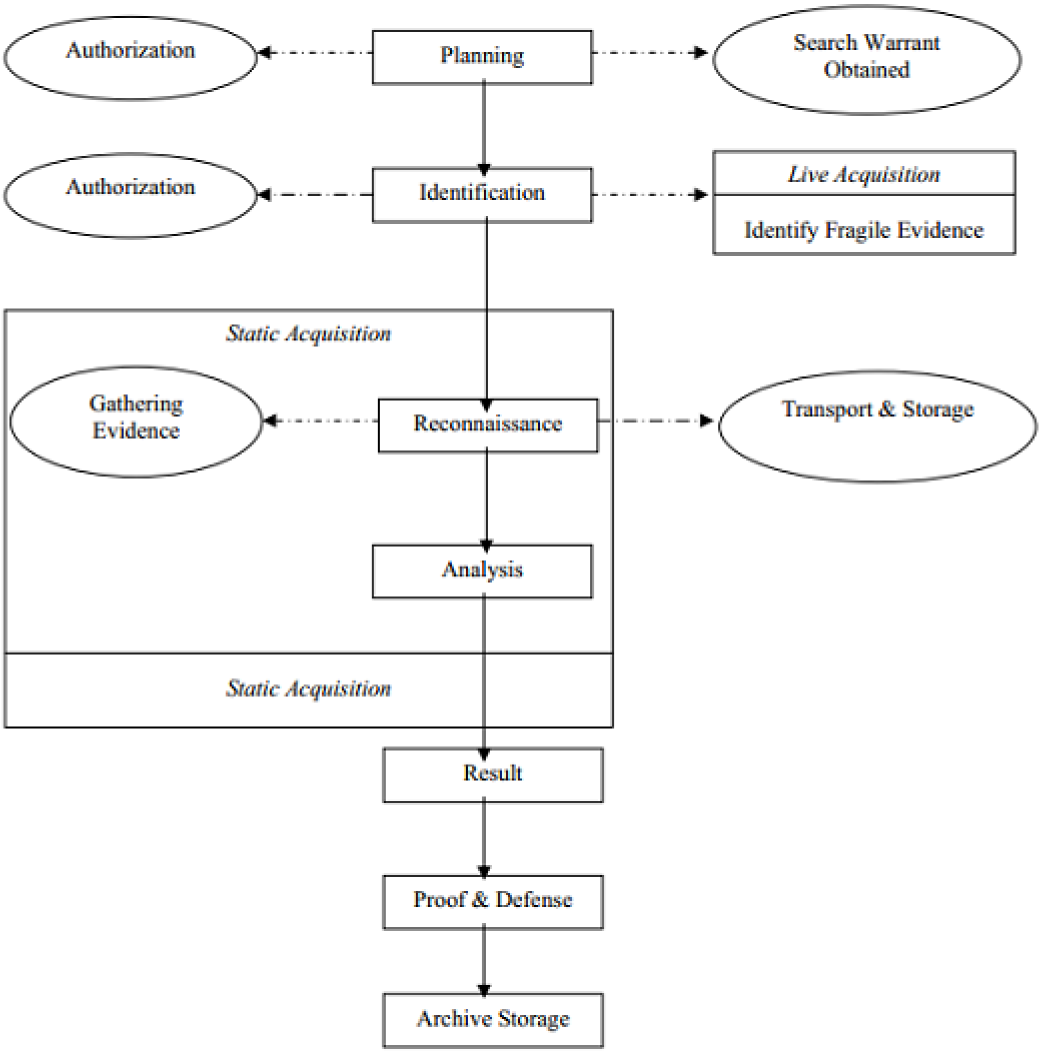


Figure 2.7.1: The Adopted digital forensic model

Source: Perumal (2009)

2. Identification Phase

This step consists of two sub procedures which aim to identify relevant items, and to identify fragile evidence. To begin with, all the computer systems used by suspect need to be identified. Next, the investigator needs to carryout live forensics on any running computer identified as part of the investigation. Under live acquisition, file time stamp, registry key, swap files and memory details are retrieved. These items can reveal very critical evidence that would otherwise have been lost should the system have been shut down.

3. Reconnaissance Phase

This is the stage in which the investigating team gathers only the relevant evidence on specific running machines rather than removing them from the network which can interfere with other company operations, for instance in case of servers. Also, the volume of storage needs to be considered to evaluate the best option to use in selecting the most appropriate target, and also choosing the best tools.

Caution needs to be taken to avoid damaging crucial evidence (Rogers et al. 2006). Since time is an important factor in this model, effective prioritization is required. Digital devices and their storage accessories which contain most important evidence and the ones which contain volatile evidence need to be handled first (Rogers et al. 2006).

Computer systems, external storage disks, mobile phones and other devices are arranged depending on their importance and relevance to the investigation. Information from the suspects is very important at this stage to help in the analysis phase.

4. Transport and Storage Phase

Acquired evidence need to be kept safely and care must be taken to avoid any type of contamination which may interfere with its integrity.

5. Analysis Phase

According to Perumal (2009), live acquisition needs to be carried out especially on all the running computers. Since some systems could be playing critical roles on a network, it is advisable that evidence is gathered without disconnecting them.

The items to be examined include:

-User profiles - This is important to help link a particular individual to a certain piece of evidence found in a computer or other storage media. Thorough understanding of the user profiles and associated artifacts relating to usage are critical in this stage. Use of dates and times associated with the artifacts found need to be put into context of the times and dates a particular user accessed the computer. All the files, folders, registry keys and file properties associated with a particular user account need to be carefully classified.

-Home directory - Presence of incriminating files in a certain user's home directory indicates it is either the user or anyone else who could logon to that account who had access to the said files.

-Chronological/Timeline - This entails examining the dates and times when a particular file was created, modified or accessed. The time the system was used, identification and analysis of software applications and data files the user accessed, recent shortcuts and stored information is also conducted.

-Internet - The examiner evaluates the internet activities of the suspect believed to have been utilized to see if and how they relate to the case at hand. Web browsing, instant messaging and e-mail are some of the things examiner may wish to go through. These contain lots of information and time factor may be a hindrance to do all of them. The examiner should only concentrate on what may be relevant to the case.

-Browser artifacts - Dates and times of a cookie can be used to determine when the user accessed a certain site and help the investigator in creating a timeline of activities. Things like user information and preferences stored by a web browser may give the examiner important evidence. Once prioritization and examination have been properly carried out, the analysis phase is fairly easy though it can still be complicated. As Perumal (2009) argues, the analyst needs to analyze and correlate data so as to build a clear picture of the committed crime. Each piece of evidence depends on the other one in creating a bigger picture of events. Planning and obtaining information prior to this step is very important and can save a lot of time. For instance getting to know the type of computers or mobile phones, suspect's activities, operating systems in use, applications in use, and nature of environment, can be very helpful for a speedy investigation.

6. Proof and Defense Phase

All the evidence found either upholding or against the suspected crime is properly documented. The investigator has to proof the validity of the findings beyond reasonable doubt. A report has to be tabled and this should be in a format and language that can be understood by the target audience. According to Goel (2012), the report must summarize the actions of the suspect during the crime, a full description of the investigation process and the conclusions made. Copies of digital evidence, photographs taken, and methodology used, expertise of the examiner and the chain of custody documents must accompany the report.

7. Archive and Storage Phase

The challenges and issues encountered during the investigation can be used to make improvements for future investigations (Goel, 2012). The results and their interpretations may be used in future to refine image gathering, analysis and examination of evidence, and also for purposes of future training.

CHAPTER THREE

3.0 RESEARCH METHODOLOGY

3.1 Introduction

This chapter explains the method used to carry out the research. It encompasses a description of the type of research and the nature of research design. It also covers the procedures, tools and techniques used in data collection, data analysis and interpretation, together with justifications for the techniques used. It also gives a review of target population, the sampling techniques applied and the justifications for their selection.

3.2 Research Design and Approach

Quantitative type of research was followed in this study. The aim was to collect and analyze quantitative data using various data collection tools. Similarly, the research design applied in this research was a descriptive survey. “A research design is the arrangement of conditions for collection and analysis of data in a manner that aims to combine relevance to the research purpose with economy in procedure” (Kothari, 2004). The choice of this research design was informed by the fact that it provides an accurate description of beliefs, opinions and knowledge of the respondents. It also assisted in attaining the third objective of the study, that is, to test the applicability of the adopted model in the public sector. It involved collecting data from sampled population with an aim to establish applicability of the adopted model by asking the selected members of the population about various aspects including current forensic methodology in use, reasons for current state, and various aspects of the computer forensics model to be adopted. Descriptive research ensured a well-organized and systematic description that was accurate and reliable regarding digital forensic investigation in public entities. Through descriptive research design, the researcher was able to link the data collected to the original problem, and again to the conclusions drawn at the end.

3.3 Research Setting

The research was conducted in Kenya National Audit Office (KENAO). KENAO is an independent office enshrined in article 229 of the Kenya constitution and established through an Act of Parliament. The office is mandated to audit all government entities and ensure accountability in the use of government resources. It has over 500 auditors and has offices in 44 government departments in Nairobi, and 10 county headquarters used as regional hubs to audit neighboring counties and government entities outside Nairobi.

3.4 Research Strategy

The research was aimed at establishing a suitable digital forensics model for use in public sector. It explored existing models as proposed by various authors with an objective of identifying and adopting the most suitable for use in the public sector. Extensive study of the current state in cyber security and the need for digital forensics was carried out to guide the identification of a suitable model. Literature on the progressive development of digital forensic models for various digital environments especially those applicable in the public sector was discussed. Publications, Journals, conference proceedings and books were reviewed to get the required literature. Data was then collected and analysed in an effort to get input and opinions of respondents on the identified model. The model was then applied in the field by the researcher to collect and analyse computer images using selected tools with an aim to evaluate and identify the most suitable for use alongside the model.

3.5 Research Population

The target population consisted of KENAO auditors working in various departments including forensic department, central government, county governments, state corporations, commissions and independent offices who met the set sample criteria. Random sampling was applied to get respondents based on representativeness and the feasibility of obtaining the required data and information.

All the 21 forensic auditors in KENAO were deliberately selected, while random sampling was applied to sample 167 auditors, which is 30% of the total 501 auditors working in different branches across the public sector and across the 11 hubs as shown in table 3.5.1:

	Countrywide Distribution of Offices	**Total Number**	**Sampled Respondents**
1	Headquarters	51	17
2	Forensic Department	21	21
3	Nairobi Hub	21	7
4	Mombasa Hub	43	14
5	Garissa Hub	10	3
6	Nyeri Hub	24	8
7	Embu Hub	19	6
8	Nakuru Hub	24	8
9	Eldoret Hub	30	10
10	Kakamega Hub	33	11
11	Kisumu Hub	33	11
12	National Government	151	50
13	Specialized Audit	44	14
	Total	**502**	**167**

Table 3.5.1: Distribution of sampled population

3.6 Sampling Criteria

Subjects included in the sample had to meet the following criteria:

1. Be 18 years and above.
2. Be of sound mind.
3. Be willing to participate.
4. Working in main stream audit.

3.7 Collection Procedures

3.7.1 Level 1 Data Collection

1. Questionnaire

A questionnaire was chosen as the instrument for Level 1 data collection. According to Cooper and Schindler (2009), a questionnaire can be described as a research instrument consisting a series of questions for the purpose of gathering information from respondents. A Questionnaire was chosen as the tool for data collection because of the following advantages compared to other methods of data collection like interviews, according to Cohen et al (2011):

1. Questionnaires require less time and resources to administer.
2. Administering questionnaires consistently ensures less opportunity for bias.
3. Questionnaires gives anonymity to respondents since no name is required.

Despite the above benefits, the questionnaires have the demerit of the question of respondents answering what they think would please the researcher. Both mailed survey through postal services and office drop-off survey were combined in an effort to get a higher response rate in the survey.

The five point scale shown in figure 3.1 below was used.

Scale	Meaning
5	Strongly agree
4	Agree
3	Don’t know
2	Disagree
1	Strongly disagree

Figure 3.1: Questionnaire scale

The questionnaires were issued to all forensic auditors through deliberate sampling while audit managers, heads of sectors and operational auditors were randomly selected.

2. Observation

Observation method was applied by going into the real work environment and witnessing the exact techniques and actions taken by forensic auditors in their work. This served as a complement to the questionnaires in gaining deeper understanding of the current forensic audit methodology and its shortcomings.

3.7.2 Level 2 Data Collection

The second part of the research study entailed the application of the adopted model in the field to collect and analyze computer images using selected tools. The objective here was to establish the most suitable tool that can be used alongside the adopted model. It involved the acquisition of computer images using Linux Mint, and analysis of the images using two computer forensic tools, Pro Discover Basic and the Sleuth Kit which were selected on basis of the fact that they are Open Source. Linux Mint produces images which can be analyzed using most types of forensic tools. The procedures of the digital forensic model based on Malaysian investigation process were followed to test whether the model could be applied in real life and also to evaluate the tools. The resulting data was then tabulated for the respective tools to evaluate their performance based on various metrics.

Level 2 Data Collection Procedure

Planning Phase and Authorization

Planning was done in advance to ensure successful acquisition, analysis and storage of images. Planning entailed obtaining image acquisition tool, in this case, Linux Mint for imaging purposes, and Pro Discover Basic and the Sleuth Kit for analysis purpose. Two USB storage disks were also acquired for image storage. Relevant authority was then sought from the management regarding the computers to be imaged, in addition to self-study to learn the use of the image acquisition and analysis tools.

Computer Image Acquisition and Evidence Gathering

After the Imaging authority was given, the researcher identified the authorized computers for imaging. The computers were selected through deliberate sampling as per the authority given. The choice of sampling technique was informed by the concern by KENAO management about the sensitivity and security of office data. The selected computers were as follows:

Type	**Serial number**	**Location**
HP	CZC9234XQT	Administration
HP	CZC9234LHB	Legal Department
Lenovo	LMWZKX8	Specialized Audit
Lenovo	LM28844	Value for Money Audit
HP	CZC9234MLB	ICT Section

Table 3.7.1: Sampled computers

After identification of the computers, the computer type, serial number and the department were properly documented. The computers were then imaged using Linux Mint. The choice of Linux was motivated by the fact that it is effective in imaging and it is easy to learn and use in addition to being Open Source. Additionally, image acquired can be accessed by most digital forensic tools. The image from each computer was then stored in a labelled external USB disk. Next, analysis of the gathered images was carried out using Pro Discover basic and the Sleuth Kit. During the analysis, the following metrics were used to evaluate the performance of the two tools, as described by Frandrin et. al (2013):

1. **Accuracy rate:** The proportion of correct results, as per the original Hash value.
2. **Precision rate:** The number of extracted files from a known list of files in the image.
3. **Absolute speed:** The total time required by a tool to complete a task.
4. **Relative speed:** The time a tool takes to complete analysis compared to the time taken to transfer the same data in the image from original media.
5. **Reliability:** A measure of how often the tool is likely to fail during an investigation.

The results obtained from each computer image were tabulated for further analysis as per the above metrics as follows:

	Artifact	**The Sleuth Kit**		**Pro Discover Basic**	
1	User profiles	1		1	
2	Email addresses/messages	1		0	
3	Activity timeline	1		0	
4	Hidden files	0		0	
5	Deleted files	1		1	
6	Recent documents	1		0	
7	Pictures and videos	1		1	
8	Downloads	1		1	
9	Web history	1		1	
10	Cookies	1		1	
	Precision rate (P)	9	90%	6	60%
		Out of 10	**Out of 100%**	**Out of 10**	**Out of 100%**
	Absolute speed (T) in Mins	80		103	
	Relative speed (R)	0.63		0.82	
	Reliability (Q) - No. of times the tool did not fail during entire analysis of the above 10 artifacts.	8	80%	6	60%
		Out of 10	**Out of 100%**	**Out of 10**	**Out of 100%**
	Accuracy rate (A)	100%		N/A	

Table 3.7.2 (a): Image 1 analysis Key**: 1** - means **present** **0** - means **absent**

	Artifact	**The Sleuth Kit**		**Pro Discover Basic**	
1	User profiles	1		1	
2	Email addresses/messages	1		0	
3	Activity timeline	1		0	
4	Hidden files	0		0	
5	Deleted files	1		1	
6	Recent documents	1		0	
7	Pictures and videos	1		1	
8	Downloads	1		1	
9	Web history	1		1	
10	Cookies	1		1	
	Precision rate (P)	9	90%	6	60%
		Out of 10	**Out of 100%**	**Out of 10**	**Out of 100%**
	Absolute speed (T) (Mins)	63		75	
	Relative speed (R)	0.59		0.71	
	Reliability (Q) - No. of times the tool did not fail during entire analysis of the above 10 artifacts.	10	0%	8	80%
		Out of 10	**Out of 100%**	**Out of 10**	**Out of 100%**
	Accuracy rate (A)	100%		N/A	

Table 3.7.2 (b): Image 2 analysis Key**: 1** - means **present** **0** - means **absent**

	Artifact	**The Sleuth Kit**		**Pro Discover Basic**	
1	User profiles	1		1	
2	Email addresses/messages	1		0	
3	Activity timeline	1		0	
4	Hidden files	0		0	
5	Deleted files	1		1	
6	Recent documents	1		0	
7	Pictures and videos	1		1	
8	Downloads	1		1	
9	Web history	1		1	
10	Cookies	1		1	
	Precision rate (P)	9	90%	6	60%
		Out of 10	**Out of 100%**	**Out of 10**	**Out of 100%**
	Absolute speed (T) in Mins	41		57	
	Relative speed (R)	0.53		0.73	
	Reliability (Q) - No. of times the tool did not fail during entire analysis of the above 10 artifacts	9	90%	7	70%
		Out of 10	**Out of 100%**	**10**	**Out of 100%**
	Accuracy rate (A)	100%		N/A	

Table 3.7.2 (c): Image 3 analysis Key**: 1** - means **present 0** - means **absent**

CHAPTER FOUR

4.0 ANALYSIS, PRESENTATION AND INTERPRETATION OF FINDINGS

This chapter presents the results and data analysis as set in the study objectives. According to Alasuutari et al (2009), data analysis is the process of packaging the collected information, evaluating it, putting it in order and structuring its main component in a way that findings can be easily interpreted. In this study, the researcher used quantitative data analysis. Quantitative data analysis involved data entry, coding, tabulating, interpreting and expressing the numerical data in terms of frequencies and percentages representing them in tables and figures. The collected data was analyzed using a software called Statistical Package for Social Sciences (SPSS) and presented using tables, pie charts and figures. Data interpretation was by the use of notes. Just like the data collection, data analysis was split into two levels as follows:

Level 1 Data Analysis: This involved the analysis of the quantitative data collected using questionnaires with an aim of testing the applicability of the adopted model.

Level 2 Data Analysis: This involved practical analysis of computer images by applying the procedures of the digital forensic model based on Malaysian investigation process.

4.1 Level 1 Data Analysis

The results of Level 1 data analysis were presented in eight sections. The first and second sections describe the response rate and background characteristics of the respondents, respectively. The other sections are the major steps in the digital forensic model based on Malaysian investigation process, and overall opinion section as follows:

1. Pre-investigation (planning and authorization);
2. Evidence identification and acquisition;
3. Evidence transportation and storage;
4. Evidence Analysis (timelines and user profiles);
5. Results, documentation and reporting;
6. Post-investigation and archiving in the digital forensic model based on Malaysian investigation process;

7. Adoption of digital forensics, and current methodology problem**.**

The purpose of the data analyzed at this level was to aid in evaluating the applicability of the adopted digital forensics model in the public sector. Since a small but representative sample was used, descriptive statistics techniques were utilized to analyze the data as follows:

4.1.1 Response Rate Analysis

Category	**Frequency**	**Percentage**
Response	120	71%
Non-response	47	295
Total	**167**	**100**

Table 4.1.1: Response rate

The research was conducted at Kenya National Audit Offices across the country, where the questionnaires returned were used for analysis. All the questionnaires initially issued were at this stage grouped into two categories; response and non-response. As shown in table 4.1.1, the response rate was 71%. With response rate above two-thirds of all respondents, it was evident that the response was adequate for the study to continue.

4.1.2 Background Characteristics

The researcher took into consideration the background of the participants in the research study.

4.1.2.1 Gender

Both male and female auditors took part in the research study.

The distribution of those who successfully participated was as shown in figure 4.1.2 below:

	Frequency	**Percent**
Male	78	65%
Female	42	35%
Total	120	100%

Table 4.1.2: Gender distribution

Figure 4.1.2 shows a majority of successful respondents in the study, 65%, were male whereas 35 % were female.

4.1.2.2: Age

The age of the participants in the research study was also determined. Figure 4.1.1 below illustrates their age brackets:

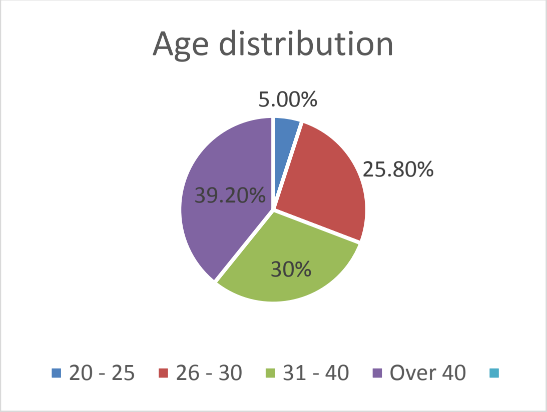


Figure 4.1.1: Age distribution

The figure above shows that majority of the respondents, 39.2% , were above 40 years, 30% were between 31 and 40, 25.8% were between 26 and 30, while 5% were between 20 and 25 years. This implies that the respondents were all mature and capable of providing reliable information for the study.

4.1.2.2 Level of Education

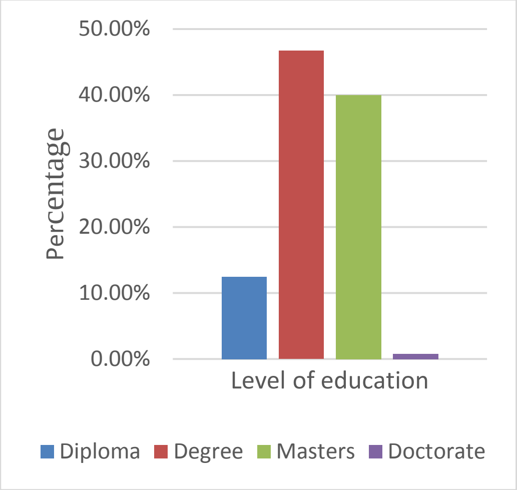


Figure 4.1.2: Level of education

Figure 4.1.2 shows that from the number of respondents who participated in the study, 12.5 % had Diploma, 46.7% had Bachelors degree, 40.0% had Masters degree and 0.8 % had Doctorate degree. These levels of education were adequate proof that the respondents were informed enough to give reliable responses.

4.1.3 Planning in the Malaysian Investigation Process Model

Response	**Strongly agree**	**Agree**	**Don't Know**	**Disagree**	**Strongly Disagree**	**Total**
Frequency	62	56	2	0	0	120
Percentage	51.7%	46.7%	1.7%	0%	0%	100%

Table 4.1.3: Lack of planning affects the quality of audit evidence

Response	**Strongly agree**	**Agree**	**Don't Know**	**Disagree**	**Strongly Disagree**	**Total**
Frequency	48	57	7	8	0	120
Percentage	40%	47.5%	5.8%	6.7%	0%	100%

Table 4.1.4: Relevant authority is required to do forensic investigation in any public entity

Table 4.1.3 above shows how the respondents rated the extent to which they agree with importance of planning as the backbone of achieving good results in investigations.

The statistics clearly show that majority of the respondents, 51.7%, strongly agreed that lack of planning affects the quality of evidence obtained during forensic investigations. 46.7% of the respondents agreed that lack of planning affects the quality of digital forensic evidence, while 1.7% of the respondents were indifferent on the fact that lack of planning affects the quality of audit evidence obtained during forensic investigation. On the other hand, no respondent disagreed nor strongly disagreed that lack of planning affects the quality of audit evidence. About seeking relevant authority to carry out digital forensics, as shown in table 4.1.4, 40% of the respondents strongly agreed that relevant authority is required to carry out digital forensic investigation in any public entity. 47.5% of the respondents agreed that relevant authority is required to carry out digital forensic investigations, while 5.8% of the respondents were indifferent on the need for relevant authority to carry out digital forensic investigations. On the other hand, 6.7% of respondents disagreed that relevant authority is required to carry out digital forensic investigations. These statistics show the importance of proper planning and seeking relevant authority at planning stage as emphasized in the digital forensic model based on Malaysian investigation process.

4.1.4 Identification and Acquisition of Evidence

Response	**Strongly agree**	**Agree**	**Don't Know**	**Disagree**	**Strongly disagree**	**Total**
Frequency	5	32	4	53	26	120
Percentage	4.2%	26.7%	3.3%	44.2%	21.7%	100%

Table 4.1.5: Most sources of evidence found during audits have equal importance

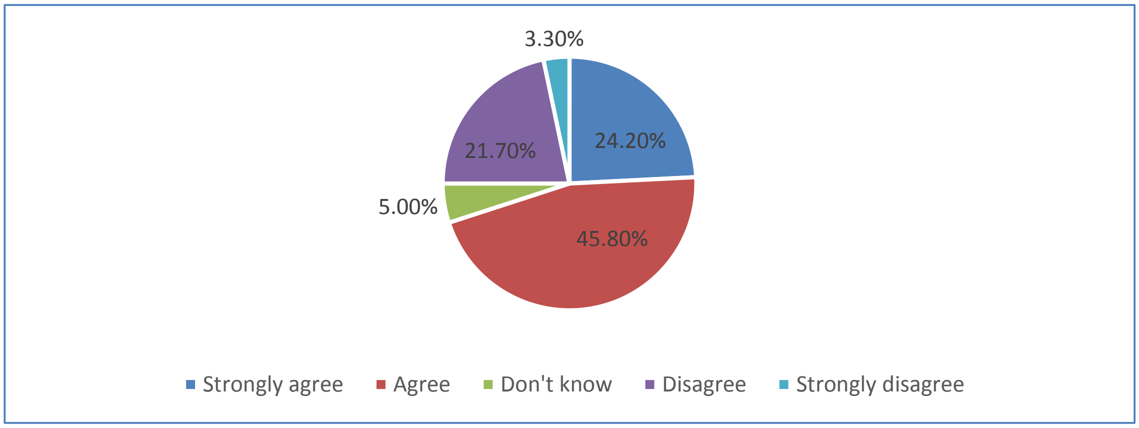


Figure 4.1.3: Extracting evidence from computers during audit is not easy

Table 4.1.5 above shows how the respondents rated the extent to which they agree with importance of identifying and classifying various sources of evidence during digital forensic investigations and figure 4.1.3, the ease with which evidence may be extracted from computers. From table 4.1.5, the statistics clearly indicate that majority of the respondents 44.2% disagreed that most sources evidence found during investigations have equal importance. 21.7% of the respondents strongly disagreed that most sources of evidence found during investigations have equal importance, while 3.3% of the respondents were indifferent on whether most sources of evidence found during investigations have equal importance. On the other hand, only 26.7% of respondents agreed that most sources evidence found during investigations have equal importance, while 4.2% of respondents strongly agreed that most sources of evidence found during investigations have equal importance. Similarly, from figure 4.1.3, the statistics show that majority of the respondents 45.8% agreed that extracting evidence from computers is not easy. 24.2% of the respondents strongly agreed that extracting evidence from computers is not easy, while 5.0% of the respondents were indifferent on whether extracting evidence from computers is not easy. On the other hand, 21.7% of respondents disagreed, and 3.3% strongly disagreed that extracting evidence from computers is not easy.

These statistics clearly indicate the importance of identifying the most important sources of evidence from the investigation site, and using the right tools and procedures to acquire the digital evidence as envisioned in the digital forensic model based on the Malaysian investigation process.

4.1.5 Evidence Analysis

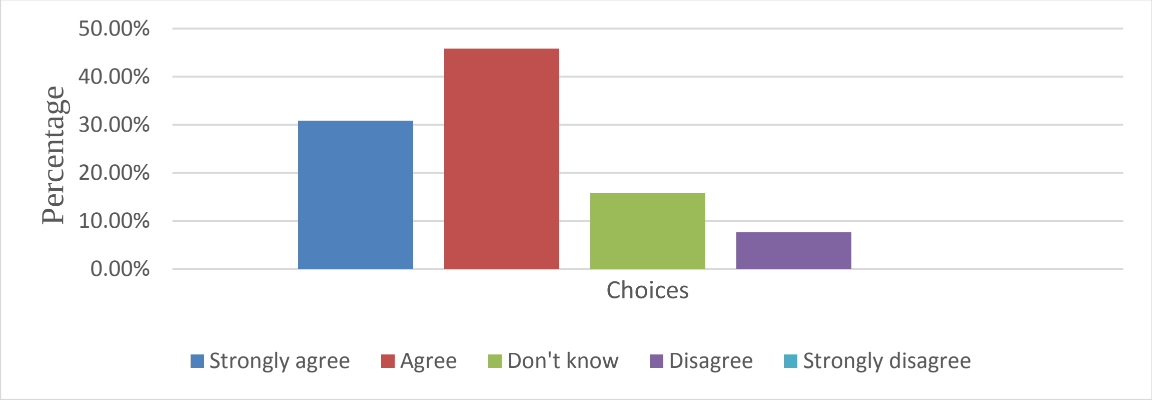


Figure 4.1.4: Files are hidden by institutions being investigated to avoid fraud exposure

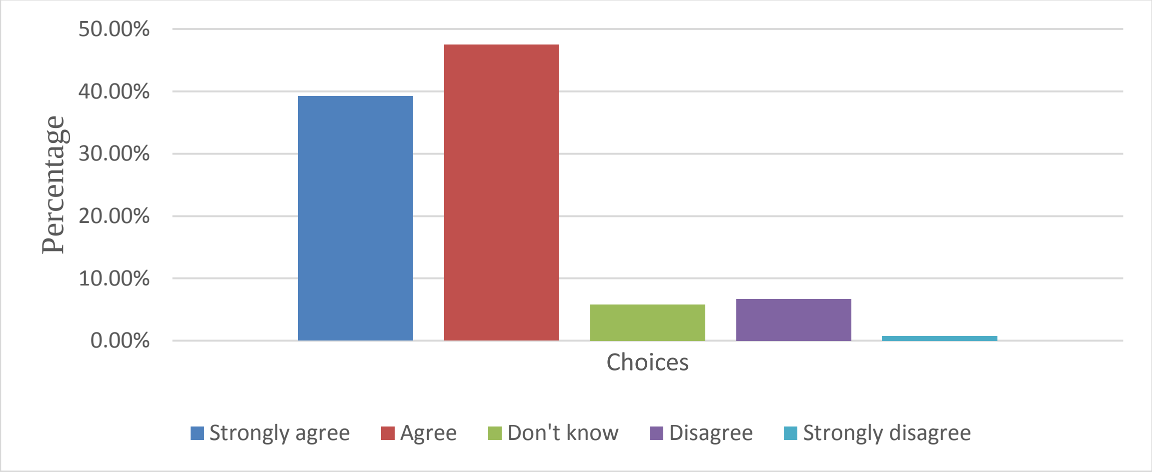


Figure 4.1.5: Technology has been used to hide fraud and related evidence

Figure 4.1.4 above shows how the respondents rated the extent to which they agree with the statement that files are hidden by institutions being investigated to avoid fraud exposure. The statistics clearly show that majority of the respondents, 45.8% agreed with the statement that files are hidden by institutions being investigated to avoid fraud exposure. 30.8% of the respondents strongly agreed that files are hidden by institutions being investigated to avoid fraud exposure, while 15.8% of the respondents were indifferent on the statement that files are hidden by institutions being investigated to avoid fraud exposure. On the other hand, 7.5% of the respondents disagreed that files are hidden by institutions being investigated to avoid fraud exposure. About the question on whether technology has been used to hide fraud and related evidence, as shown in figure 4.1.5, 47.5% of the respondents agreed that technology has been used to hide fraud and related evidence. 39.2% of the respondents strongly agreed that technology has been used to hide fraud and related evidence, while 5.8% of the respondents were indifferent on the question whether technology has been used to hide fraud and related evidence. On the other hand, 6.7% of respondents disagreed that technology has been used to hide fraud and related evidence while only 0.8% strongly disagreed that technology has been used to hide fraud and related evidence. These statistics show the importance of detailed image analysis to extract deleted or hidden evidence using various digital forensic tools, as emphasized in the analysis stage of the digital forensic model based on Malaysian investigation process.

Timeline analysis and user profile analysis

Response	**Strongly agree**	**Agree**	**Don't know**	**Disagree**	**Strongly disagree**	**Total**
Frequency	60	54	2	4	0	120
Percentage	50%	45%	1.7%	3.3%	0%	100%

Table 4.1.6: The time a crime was committed is important in forensic investigations

Response	**Strongly agree**	**Agree**	**Don't Know**	**Disagree**	**Strongly disagree**	**Total**
Frequency	35	49	1	31	4	120
Percentage	29.2%	40.8%	0.8%	25.8%	3.3%	100%

Table 4.1.7: Identifying the person who committed fraud is the most important aspect of forensic investigation

Table 4.1.6 above shows how the respondents rated the extent to which they agree with importance of the time at which a crime was committed to the investigator. The statistics clearly show that majority of the respondents, 50% strongly agreed that the time a crime was committed is important during forensic investigations. 45% of the respondents agreed that the time a crime was committed is important during forensic investigations, while 1.7% of the respondents were indifferent on the fact that the time a crime was committed is important during forensic investigations. On the other hand, 3.3% of the respondents disagreed that the time a crime was committed is important during forensic investigations. About identifying the person who committed fraud being the most important aspect of forensic investigations, as shown in table 4.1.7, 40.8% of the respondents agreed that identifying the person who committed fraud is the most important aspect of forensic investigation. 29.2% of the respondents strongly agreed that identifying the person who committed fraud is the most important aspect of forensic investigation, while 0.8% of the respondents were indifferent on the need for identifying the person who committed fraud. On the other hand, 25.8% of respondents disagreed that identifying the person who committed fraud is the most important aspect of forensic investigation while only 3.3% strongly disagreed that identifying the person who committed fraud is the most important aspect of forensic investigation. These statistics show the importance of timeline analysis and detailed image analysis to identify the culprit who committed the alleged crime, as emphasized in the Analysis stage of the digital forensic model based on Malaysian investigation process.

4.1.6 Results, Documentation and Reporting

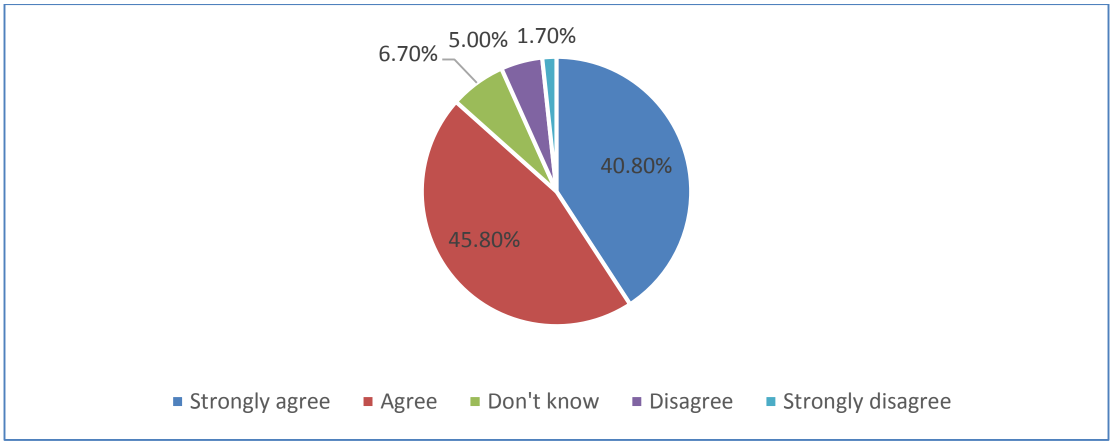


Figure 4.1.6: Documentation is the most important task in computer forensic investigations

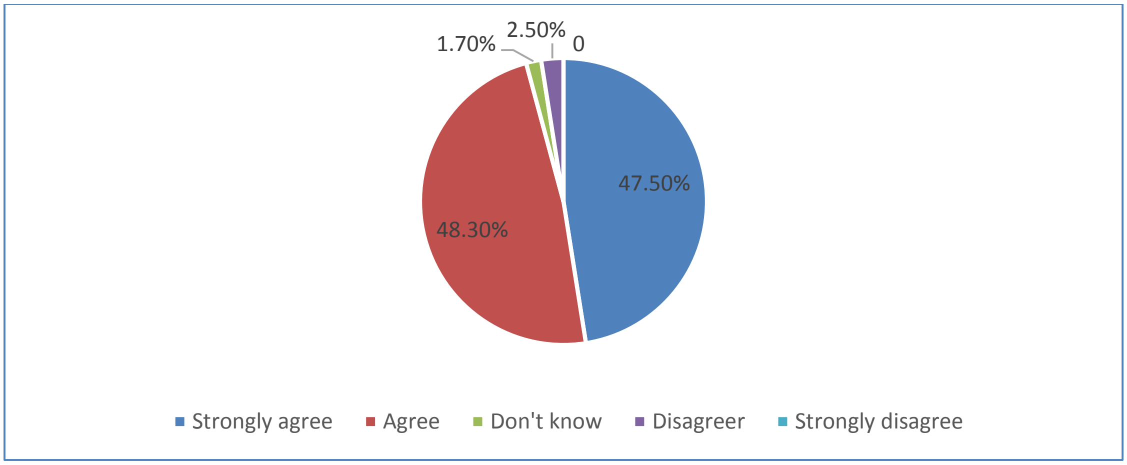


Figure 4.1.7: Investigating computer systems could enhance the quality and reliability of evidence

As shown in figure 4.1.6 above, majority of the respondents, 45.8%, agreed that documentation is the most important task in computer forensics. 40.8 % of the respondents strongly agreed that documentation is the most important task in computer forensics, while 6.7% of the respondents were indifferent on the fact that documentation is the most important task in computer forensics. On the other hand, only 5.0% of respondents disagreed that documentation is the most important task in computer forensics while only 1.7% of respondents strongly disagreed that documentation is the most important task in computer forensics. Similarly, figure 4.1.7 above shows that majority of the respondents, 48.3% agreed that investigating computer systems could enhance the quality and reliability of evidence. 47.5% of the respondents strongly agreed that investigating computer systems could enhance the quality and reliability of evidence, while 1.7% of the respondents were indifferent on whether investigating computer systems could enhance the quality and reliability of evidence. On the other hand, only 2.5% of respondents disagreed that investigating computer systems could enhance the quality and reliability of evidence. These results emphasize the importance of the evidence analysis step in the digital forensic model based on the Malaysian investigation process.

4.1.7 Post-Investigation (Defense and Proof of Evidence, and Archiving)

Response	Strongly agree	Agree	Don't know	Disagree	Strongly disagree	Total
Frequency	69	38	3	8	2	120
Percentage	57.5%	31.7%	2.5%	6.7%	1.7%	100%

Table 4.1.8: Evidence is useful after the closure of an investigation

Table 4.1.8 above shows how the respondents rated the extent to which they agree with usefulness of evidence material at the closure of an investigation exercise. The statistics clearly show that majority of the respondents, 57.5%, strongly agreed that evidence obtained during a forensic investigation was useful even after the closure of the investigation. 31.7% of the respondents agreed that evidence obtained during a forensic investigation was useful even after the closure of the investigation, while 2.5 % of the respondents were indifferent on the fact that evidence obtained during a forensic investigation was useful even after the closure of the investigation.

On the other hand, 6.7% of respondents disagreed that evidence obtained during a forensic investigation was useful even after the closure of the investigation, while only 1.7% of the respondents strongly disagreed that evidence obtained during a forensic investigation was useful after the closure of the investigation. These statistics show the usefulness of evidence obtained during a forensic investigation even after the closure of the investigation, as emphasized in the Defense and Proof step and the Archiving step of the digital forensic model based on Malaysian investigation process.

	Planning	Authority	Identification	Acquisition	Analysis	Archiving	Average
Agree	47.6%	47.5%	26.7%	45.8%	45.8%	31.7%	40.8%
Strongly Agree	51.7%	40.0%	4.2%	24.2%	30.8%	57.5%	34.7%
Sub total	**99.3%**	**87.5%**	**30.9%**	**70%**	**76.6%**	**89.2%**	**75.5%**
Others	0.7%	12.5%	69.1%	30%	23.4%	10.8%	24.5%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Table 4.1.9 Summary of responses on the Malaysian Investigation Process Model

4.1.8 Adoption of digital forensics and methodology problem in KENAO.

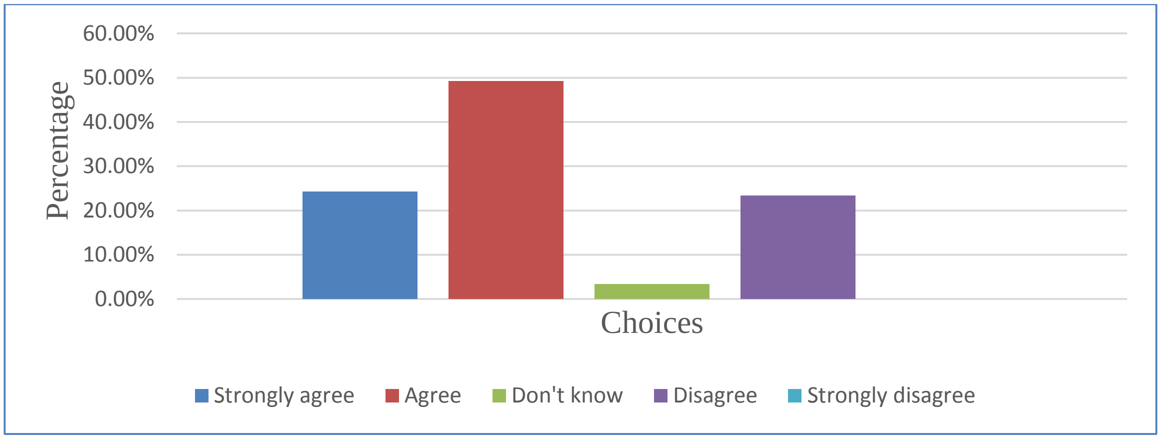


Figure 4.1.8: Lack of appropriate methodology

Response	**Strongly agree**	**Agree**	**Don't know**	**Disagree**	**Strongly disagree**	**Total**
Frequency	73	39	1	7	0	120
Percentage	60.8%	32.5%	0.8%	5.8%	0%	100%
Total	93.3%		6.7%			100%

Table 4.1.10: Need for KENAO to adopt computer forensics

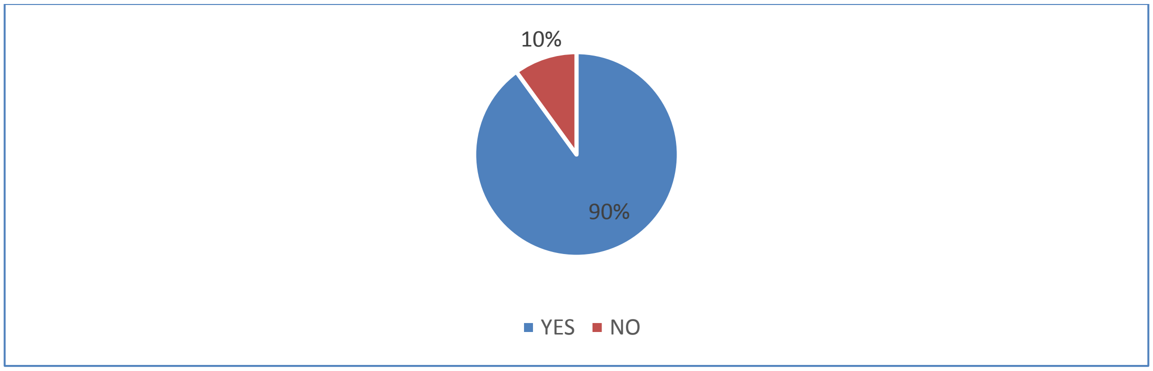


Figure 4.1.9: Should KENAO carry out computer forensics

Response	YES	NO	Total
Frequency	38	82	120
Percentage	31.7%	68.3%	100%

Table 4.1.11: Adequateness of the current methodology used by KENAO

The tables above shows how the respondents rated the extent to which they agree with the fact that KENAO lacked an appropriate methodology to carry out digital forensics, the adequateness of the current methodology used by KENAO to carry out forensic investigations, and finally the need for KENAO to carry out digital forensics in its fight against corruption in the public sector. From figure 4.1.8 above, the statistics show that majority of the respondents 49.2% agreed that KENAO lacked an appropriate methodology to carry out digital forensics. 24.2% of the respondents strongly agreed that KENAO lacked an appropriate methodology to carry out digital forensics, while 3.3% of the respondents were indifferent on the fact that KENAO lacked an appropriate methodology to carry out digital forensics. On the other hand, 23.3% of respondents disagreed that KENAO lacked an appropriate methodology to carry out digital forensics.

About the adequateness of the current methodology used by KENAO to carry out forensic investigations, as shown in table 4.1.11, 68.3% of the respondents said that the methodology used by KENAO to carry out forensic investigations was inadequate, while 31.7% of the respondents said that the methodology used by KENAO to carry out forensic investigations was adequate.

On whether KENAO should adopt digital forensics table 4.1.10, 60.8% of the respondents strongly agreed that KENAO should adopt digital forensics, 32.5% agreed that KENAO should adopt digital forensics, while 0.8% were indifferent on the need for KENAO to adopt digital forensics. On the other hand, 5.8% of the respondents disagreed on the need for KENAO to adopt digital forensics. Similarly, in figure 4.1.9, 90% of respondents said that KENAO should adopt digital forensics while only 10% of the respondents where against adoption of digital forensics by KENAO.

The statistics shown in the above tables and figures show the magnitude of the need for KENAO to adopt a modern digital forensic investigation model in its forensic methodology, and to fully adopt digital forensics in its quest to promote accountability and counter fraud in the public sector. The digital forensic model based on the Malaysian investigation process offers a solution to the methodology problem currently encountered.

The following tables show how participants responded on whether KENAO lacked computer forensic tools and the relevant skills for adoption of digital forensics:

Response	Frequency	Percentage
Strongly disagree	19	15.8%
Disagree	4	3.3%
Don’t know	0	0%
Agree	50	41.7%
Strongly agree	47	39.2%

Table 4.1.12(a) Lack of computer forensic tools

Response	Frequency	Percentage
Strongly disagree	3	2.5%
Disagree	35	29.2%
Don’t know	8	6.7%
Agree	54	45%
Strongly agree	20	16.7%

Table 4.1.12 (b) Lack of technical skills

These results indicate the need for KENAO to acquire the relevant computer forensic tools and equally hire and train forensic professionals for the office to be able to introduce and sustain digital forensics as part of the investigations carried out by the office.

4.2 Level 2 Data Analysis

By using the image analysis data tabulated in table 3.7.3 (a) to 3.7.3 (c), percentages and other measures of central tendency were calculated to show the time comparisons between the two tools used. Microsoft Excel was used to analyze the data. The choice of Microsoft Excel as the analysis tool was motivated by the fact that it is excellent in descriptive statistics, in which measures of central tendency need to be calculated. For further analysis, the data from table 3.7.3 (a) to 3.7.3 (c) were summarized as shown in table 4.2.1 (a) to 4.2.1 (c) as follows:

Key: Tool A – The Sleuth Kit **Tool B** – Pro Discover

Tool	**Image 1**				
	Precision rate in %	Abs. speed	Relative speed	Reliability in %	Accuracy rate in %
Tool A	$P_1 = 90$	$T_1 = 80$	$R_1 = 0.63$	$Q_1 = 80$	$A_1 = 100$
Tool B	$P_2 = 60$	$T_2 = 103$	$R_2 = 0.82$	$Q_2 = 60$	$A_2 =$ N/A

Table 4.2.1 (a): Further analysis of computer images - Image 1

Tool	**Image 2**				
	Precision rate in %	Abs. speed	Relative speed	Reliability in %	Accuracy rate in %
Tool A	$P_3 = 90$	$T_3 = 63$	$R_3 = 0.59$	$Q_3 = 100$	$A_3 = 100$
Tool B	$P_4 = 60$	$T_4 = 75$	$R_4 = 0.71$	$Q_4 = 80$	$A_4 =$ N/A

Table 4.2.1 (b): Further analysis of computer images - Image 2

Tool	**Image 3**				
	Precision rate in %	Abs. speed	Relative speed	Reliability in %	Accuracy rate
Tool A	$P_5 = 90$	$T_5 = 41$	$R_5 = 0.53$	$Q_5 = 90$	$A_5 = 100$
Tool B	$P_6 = 60$	$T_6 = 57$	$R_6 = 0.73$	$Q_6 = 70$	$A_6 =$ N/A

Table 4.2.1 (c): Further analysis of computer images – Image 3

Metric Analysis:

Average Precision rate for tool A, P_A in % = $(P_1+P_3+P_5)/3$

= (90+90+90)/3

= 90%

Average Precision rate for tool B, P_B in % = $(P_2+P_4+ P_6)/3$

= (60+60+60)/3

= 60%

Average Absolute speed of Tool A, A_T in Mins = $(T_1+T_3+T_5)/3$

= (80+63+41)/3

= 61.3 Minutes

Average Absolute speed of Tool B, B_T in Mins = $(T_2+ T_4+T_5)/3$

= (103+75+57)/3

= 78.3 Minutes

Average Relative Speed of Tool A, R_A = $(R_1+R_3+R_5)/3$

= (0.63+0.59+0.53)/3

= 0.58

Average Absolute Speed of Tool B, R_B = $(R_2+ R_4+R_6)/3$

= (0.82+0.71+0.73)/3

= 0.75

Average Reliability of Tool A, Q_A in % = $(Q_1+Q_3+Q_5)/3$

= (80+100+90)/3

= 90% Reliable.

Average Reliability of Tool B, Q_B in % = $(Q_2+ Q_4+Q_6)/3$

= (60+80+70)/3

= 70% Reliable.

Accuracy Rate of Tool A in % = (100+ 100+ 100)/3

= **100% Accurate.**

Accuracy Rate of Tool B in %: Could not be determined, accuracy metric not available.

	Average Precision rate	Average Absolute speed	Average Relative speed	Average Reliability	Average Accuracy
The Sleuth Kit	90%	61.3 Minutes	0.58	90%	100%
Pro Discover	60%	78.3 Minutes	0.75	70%	N/A

Table 4.2.1 (d) Summary of Tools Performance Analysis

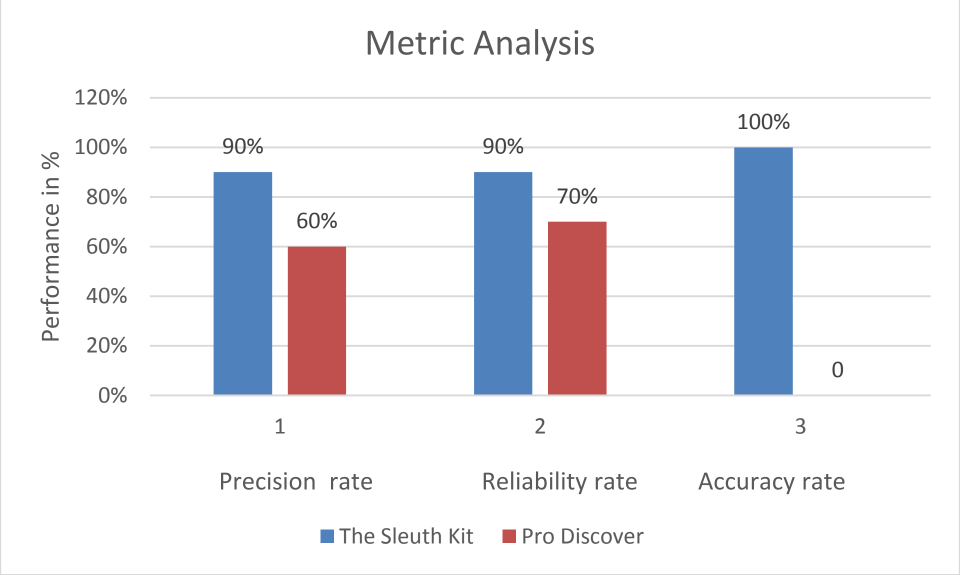


Figure 4.1.10: Summary of tools performance analysis

The results in table 4.2.1 (d) and figure 4.1.10 above, clearly indicate that the Sleuth Kit had a higher precision rate and reliability, all at 90%, compared to the same metrics in Pro Discover at 60% and 70% respectively. In terms of time taken to analyze the images, the Sleuth Kit was faster completing file analysis in an average time of 61.3 minutes compared to Pro Discover at 78.3 minutes. The same is reflected in their relative speeds in copying data from original media, with the Sleuth Kit taking 0.58 and Pro Discover taking 0.75 of the time taken to copy the images from the original media. On accuracy rate, the Hashing function available in the Sleuth Kit confirmed that all the images analyzed by the tool had the same Hash value as the one taken on the image before the analysis. This facility was not available in Pro Discover and therefore its accuracy rate could not be determined.

These results clearly indicate that the Sleuth Kit had an overall better performance compared to Pro Discover considering the four metrics analyzed and the Hash value calculation function it offered to ascertain the integrity of images analyzed. This implies the Sleuth Kit is more suitable for use alongside the proposed digital forensic model based on the Malaysian investigation process.

CHAPTER FIVE

5.0 SUMMARY OF FINDINGS, RECOMMENDATIONS, AND CONCLUSIONS

5.1 Introduction

This chapter summarizes the findings of the research therefore forming a basis for recommendations and conclusions with an aim of answering the research questions. It also covers the challenges experienced and the limitations of the study.

5.2 Summary of Findings

The study aimed to establish the adequacy of the current forensics methodology used by KENAO, to review digital forensics models that can be used in the public sector, and to propose the most suitable model for adoption in the public sector forensic investigations. Additionally, the study aimed to test the applicability of the identified digital forensics model for adoption and finally to establish and verify an effective and efficient forensic tool usable with the model. From data analysis, 93.3% of respondents supported the view that KENAO should adopt digital forensic techniques in its forensic investigations. Similarly, 68.3% of the respondents felt that KENAO lacked adequate methodology to carry out digital forensics. Regarding the applicability of the adopted digital forensic model based on Malaysian investigation process, 99.3% of the respondents supported the view that planning was an important step as envisioned in the digital forensic model based on Malaysian investigation process. Similarly, a total of 87.5% of respondents supported the need to seek authority before commencing a forensic investigation exercise, while 69.1% agreed on the importance to identify the most important sources of evidence before beginning the evidence acquisition. 70% of respondents supported the need to computerize evidence acquisition, with 76.6% of all respondents supporting detailed analysis of computer images to extract all relevant evidence, while a total of 89.2% of all the respondents supported the need to archive evidence and reports after completion of investigations for future reference. Averagely, across all the steps of the digital forensic model based on Malaysian investigation process, 75.5% of respondents agreed with the procedures proposed by the model and their importance. On digital forensic tools that can be usable with the model, the Sleuth Kit had an overall better performance in all the evaluated metrics.

5.3 Limitations of the Study

The major limitation of this study is the fact that it was not possible to image many computers as KENAO could not authorize access to as many computers in the production environment due to data security concerns. Similarly, storage space for images was a big challenge since most computers had 500 GB hard disks which were not partitioned. In view of these two challenges, only a few computer images were used for the research. Since the objective was to evaluate the suitability of the tool to be adopted alongside the model, in a real life environment after testing the applicability of the model through a survey, this change in number of computers imaged had no major effect on the outcome of the research. Nevertheless, the accuracy of the calculated absolute speed and relative speed, precision rate and reliability would have improved had many images been used. To add on, Open Source forensic tools were used to go round the cost of commercial tools since they are free and were able to meet the objectives of the study. Finally, self-study was applied to counter the challenge of training costs on forensic tools. The challenge of learning and applying the knowledge gained to use the digital forensic tools was also experienced though it created an opportunity to gain useful hands-on experience. The negative impact was that some functions of the digital forensic tools like image hashing for integrity check could not be undertaken, thus that component of the digital forensic could not be practically applied.

5.4 Conclusions

The application of digital forensics in identifying, extracting, analyzing and presenting electronic evidence in an automated fashion is a challenging task. While it was possible to ascertain that the digital forensic model based on the Malaysian investigation process is applicable in the public sector, it should be noted that this is only most suitable where digital images are to be acquired and carried from site for later analysis. Similarly, the Sleuth Kit which was verified as an effective and efficient tool to use alongside the model can only work best when the image has already been acquired, and it requires significant amount of time to be able to analyze the image and generate the forensic reports.

5.5 Recommendations

1. **KENAO should adopt modern digital forensics**

In view of the challenges encountered by use of manual forensic methodology due to problems related to technology, there is need for the office to adopt modern digital forensics to solve them. Problems like issues of deleted data, data hiding and encryption can easily be resolved through digital forensics. Similarly, KENAO should invest in modern digital forensic tools that can work well with different types of digital devices including mobile phones and computers and carry out intense hands-on training on the use of such tools to optimize their utilization.

2. Adoption of the digital forensic model based on Malaysian investigation process

According to the study, majority of respondents agreed that KENAO should adopt the digital forensic model based on Malaysian investigation process. The study recommends KENAO to adopt the digital forensic model based on Malaysian investigation process to carry out detailed investigations and strengthen the value of findings and reports from the investigations. Through this model, the overall evidence gathered will be of higher quality and adequate, and therefore able to stand any challenge before a court of law. Additionally, in the meantime, KENAO should adopt the use of the Open Source tool, the Sleuth Kit, which is widely accepted across the world and quite adequate for use in the public sector. Nevertheless, KENAO should also consider the acquisition of modern commercial forensic tools, and further hire and train qualified staff in digital forensics to reap maximum benefits from this model and tools.

3. Recommendation for future research

The study recommends further research in the area of digital forensic models to build on the existing models in order to stay ahead of the ever changing cybercrime landscape and to be able to adequately investigate computer related crimes and produce concrete evidence.

REFERENCES

Alasuutari, P., Bickman, L., & Brannen, J. (2009). *Social Research Methods*. London: Sage Publications Ltd.

Bashir, M.S., Khan, N.A., 2013, 'Triage in Live Digital Forensics Analysis', *The International Journal of Forensic Computer Science,* 36-44. viewed 14 June 2014, from http://www.ijofcs.org/V08N1-PP05-TRIAGE-IN-LIVE-DIGITAL.pdf

Broadhurst, R., Grabosky, P., ALazab, M., Chon, S., 2014, 'Organizations and Cybercrime: An Analysis of the Nature of Groups engaged in Cyber Crime', *International Journal of Cyber Criminology* 8(1), 1-20. viewed 11 March 2014, from http://www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf

Ciardhuain, N., 2004, An Extended Model of Cybercrime Investigation", *International Journal of* Digital Evidence, (3)1, 1-22. viewed from https://utica.edu/academic/institutes/ecii/publications/articles/A0B70121-FD6C-3DBA-0EA5C3E93CC575FA.pdf

Cohen, L. Manion, L. and Morrison, K. (2011).*Research methods in education,* 6th Edition.Routledge.

Cooper, D. and Schindler, P. (2009).*Business Research Method*. 9th Edition. Boston: McGraw-Hill Irwin.

Dezfoli, F, N., Dehghantanha, A., Mahmoud, R., Sani, N.F., Daryabar, F., 2013, 'Digital Forensic Trends and Future', *International Journal of Cyber-Security and Digital Forensics,* 2(2), 48-76. viewed 10 June 2014, from http://sdiwc.net/security-journal/Browse-Archive.php?ptid=1&ptsid=66&vnum=2&inum=2

Goel, A., Tyagi, A., Agarwal, A., 2012, 'Smartphone Forensic Investigation Process Model', International Journal of Computer Science & Security (IJCSS), 6(5), 322-341. viewed 17 May 2014, from http://cscjournals.org/csc/manuscript/Journals/IJCSS/volume6/Issue5/IJCSS-719.pdf

Government of Kenya, Ministry of Information, Communication and Technology, *Cyber Security Strategy*, February 2014, viewed 19 June 2014, from http://www.icta.go.ke/wp-content/uploads/2014/03/GOK-national-cybersecurity-strategy.pdf

Imtiaz, F., 2006, 'Enterprise Computer Forensics: A defensive and offensive strategy to fight computer crime', Paper presented at the 4th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, 4th December.

World Bank, 2013, *Mobile Usage at the Base of the Pyramid: Research Findings from Kenya and South Africa*, Washington, DC. viewed 17 June 2014, from http://www.infodev.org/mbopsummary.

Information Assurance Advisory Council (IAAC), 2013, *Digital Evidence*, Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organizations, Security Advisers and Lawyers, United Kingdom.
viewed 12 June 2014, from
http://www.iaac.org.uk/itemfiles/DigitalInvestigations2013.pdf

Kenya National Audit Office, 2013, *Forensic Audit Manual*, Nairobi.

Kothari, C. R., 2004, *Research Methodology, Methods and Techniques*, 2nd edn., viewed 21 June 2014, from
http://www2.hcmuaf.edu.vn/data/quoctuan/Research%20Methodology%20-%20Methods%20and%20Techniques%202004.pdf

Lammle, T., 2011, *Cisco Certified Network Associate: Study Guide*, Wiley Publishing, Indiana.

Mohtasebi, S.H., Dehghantanha, A., 2013, 'Towards a Unified Forensic Investigation Framework of Smartphones', *International Journal of Computer Theory and Engineering,* 5(2), 351-355. viewed 29 June 2014, from http://www.ijcte.org/papers/708-A241.pdf

Mohiri, T., Kumar, S.A., Nitesh, G., 2013, 'Review on Android and Smartphone Security', *Research Journal of Computer and Information Technology Sciences* 1(6), 12-1. viewed 13 June 2014, from http://www.isca.in/COM_IT_SCI/Archive/v1/i6/3.ISCA-RJCITS-2013-030.pdf

National Institute of Standards and Technology (2004b) *PDA Forensic Tools: An Overview and Analysis*. viewed 14 July 2014, US, from
http://www.csrc.nist.gov/publications/nistir/nistir-7100-PDAForensics.pdf

Perumal, S. (2009), 'Digital Forensic Model Based on Malaysian Investigation Process', *International Journal of Computer Science &Network Security*, (9)8, 38-44. viewed 28 June 2014, from http://paper.ijcsns.org/07_book/200908/20090805.pdf

Reith, M., Carr, C., Gunsh, G., 2002, 'An Examination of Digital Forensics Models', *International Journal of Digital Evidence*, 1, (3), viewed 11 June 2014, from
From http://www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf

Rogers, M.K., Goldman, J., Mislan, R., Wedge, T., Debrota, S., 2006 'Computer Forensic Field Triage Process Model', paper presented at ADFSL Conference on Digital Forensics, Security and Law, Las Vegas, Nevada, 20-21, April.

Shah, V., Bansal, P., 2012, ‘CDCD-5 an Improved Mobile Forensics Model’, *International Journal of Computer Science and Information Technology & Security*, 2(4), 739-741. viewed 20 June 2014, from http://www.ijcsits.org/papers/vol2no42012/6vol2no4.pdf

Vasudevan, S., 2004, Forensic Auditing, *The Chattered Accountant*, 53(3), 359-36. viewed 17 June 2014, from http://www.icai.org/post.html?post_id=2804

Wilson, R., 2006, Understanding the Perpetration of Employee Computer Crime in the Organizational Context Information and Organization, *Information and Organization*, 6(4), 304-324. viewed 10 May 2014, from http://www.sciencedirect.com/science/journal/14717727/16/4

Yusoff, Y., Ismail, R., Hassan, Z., 2011, ‘Common Phases OF Computer Forensics Investigation Models’, *International Journal of Computer Science & Information Technology*, 3(3), 17-31. viewed 22 June 2014, from http://airccse.org/journal/jcsit/0611csit02.pdf

APPENDICES

Appendix 1: Research budget

Item	Estimated Cost in Kshs.
Storage	13,000
Travelling	9,000
Data analysis	15,000
Airtime and internet charges	3,000
Printing and binding reports	2,000
Courier services	2,000
Totals	**44,000**

Appendix 2: Definition of Terms

Artifact - The result arising from preparatory or investigative procedures.

Cookie - A message, or segment of data, containing information about a user, exchanged between the web server and the client browser each time the browser makes a web page request.

Cybercrime - Criminal activity or a crime that involves the Internet, a computer system, or computer technology.

Digital forensics - The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources.

Hypothesis - A suggestion, or set of suggestions, set forth as a description for the occurrence of some specified group of phenomena, asserted merely as a provisional assumption to guide investigation.

Kenya National Audit Office (KENAO) - A body corporate established by an Act of parliament and refers to the Auditor-General and his/her staff.

Model - a representation to show the appearance or construction of something.

Appendix 2: Questionnaire

Martin Kilungu,

P.O. Box 30084 – 00100,

Nairobi.

E-mail: kilungu@hotmail.com

Phone no. 0726 776 593

06/09/2014

Dear Participant,

RE: Invitation to participate in a Survey entitled: "An Investigation of Digital Forensic Models Applicable in the Public Sector: A Case of Kenya National Audit Office"

You are invited to participate in the aforementioned study. This study is being conducted by Martin Kilungu and his research committee from the School of Computer Science and Informatics, at the University of Nairobi. The research concerns models used in digital forensics. The purpose of this study is to establish a suitable model for digital forensics in an audit environment.

In this study, you will be asked to complete a questionnaire. Your participation in this study is purely voluntary and the questionnaire should take only 10 minutes to complete. The responses given will be confidential and you will not be required to identify yourself. Collected data will be used purely for research purposes.

Any questions with regard to this questionnaire can be directed to Martin Kilungu through the E-mail address and phone number provided above. By completing and submitting this questionnaire, you are indicating your consent to participate in the study. Your participation is highly appreciated.

Student: Martin Kilungu, MSc – Distributed Computing Technologies

Supervisor: Dr. Elisha Abade,

School of Computing and Informatics,

University of Nairobi.

Questionnaire

Instructions

In the given spaces, give your opinion using the following 5 point scale:

Scale	**Meaning**
5	Strongly agree
4	Agree
3	Don’t know
2	Disagree
1	Strongly disagree

Tick **ONLY one answer** per question.

Section I: Demographic Details

1. Gender Male □ Female □
2. Age 20 -25 □ 26 -30 □ 31- 40 □ over 40 □
3. Level of Education Phd. □ Masters □ Bachelors □ Diploma □
4. Years Worked in Audit Below 1 □ 1- 4 □ 5-8 □ 9 -12 □ Over 12 □

Section 1: Overview questions

To what extent do you agree with the following statements regarding forensic investigations in public sector.

		5 Strongly Agree	**4 Agree**	**3 Don’t know**	**2 Disagree**	**1 Strongly Disagree**
1	Mandate of KENAO allows for detailed					

	investigation of fraud in the public sector					
2	Currently the fraud investigations done by KENAO is advanced					
3	Fraud investigating entities need to adopt new technologies					

Section 2: Computer forensics investigations

To what extent do you agree with the following statements regarding investigation of computer systems during forensic investigations by KENAO

		5 Strongly Agree	**4 Agree**	**3 Don't know**	**2 Disagree**	**1 Strongly Disagree**
1	Lack of planning affects the quality of audit evidence.					
2	Relevant authority is required to do forensic audit in any public entity.					
3	Most sources of evidence found during audits have equal importance					
4	Extracting evidence from computers during audit is not easy					

5	Files are hidden by institutions being audited to avoid fraud exposure.					
6	Documentation is the most important task in computer fraud auditing					
7	Audit evidence is useful after the closure of an audit investigation.					

Section 3: Factors affecting forensic auditing in the public sector

To what extent do you agree with the following statements regarding investigation of computer systems during fraud investigations conducted by KENAO

		5 Strongly Agree	**4 Agree**	**3 Don't know**	**2 Disagree**	**1 Strongly Disagree**
1	Lack of financial resources					
2	Lack of appropriate methodology					
3	Lack of Initiative					
4	Lack of technical skills					
5	Lack of computer forensic tools					

Section 4: Benefits of forensic auditing of computer systems in public institutions

To what extent do you agree with the following statements regarding the benefits of investigating computer systems during forensic audits by KENAO

		5 Strongly Agree	**4 Agree**	**3 Don't know**	**2 Disagree**	**1 Strongly Disagree**
1	Investigating computer systems can detect and prevent fraud					
2	Investigating computer systems could enhance the quality and reliability evidence					
3	Technology has been used to hide fraud and evidence					
4	Computer forensics can speedup forensic investigations					
5	The time a crime was committed is important in fraud investigations					
6	Identifying the person who committed fraud is the most important					

	aspect of forensic investigation					

		5 Strongly Agree	**4 Agree**	**3 Don’t know**	**2 Disagree**	**1 Strongly Disagree**
1	This questionnaire was complex and difficult to answer					
2	Relevant audit aspects are captured in this questionnaire					
3	All the phases of an audit are reflected in this questionnaire					
4	This questionnaire does not reflect true picture of a forensic investigation					
5	KENAO should adopt computer forensics					

Section 5: Closing questions

To what extent do you agree with the following statements regarding this questionnaire?

Section 6: Your Comments

In your own opinion, does KENAO need to carry out computer forensics in response to fraud in the public sector?

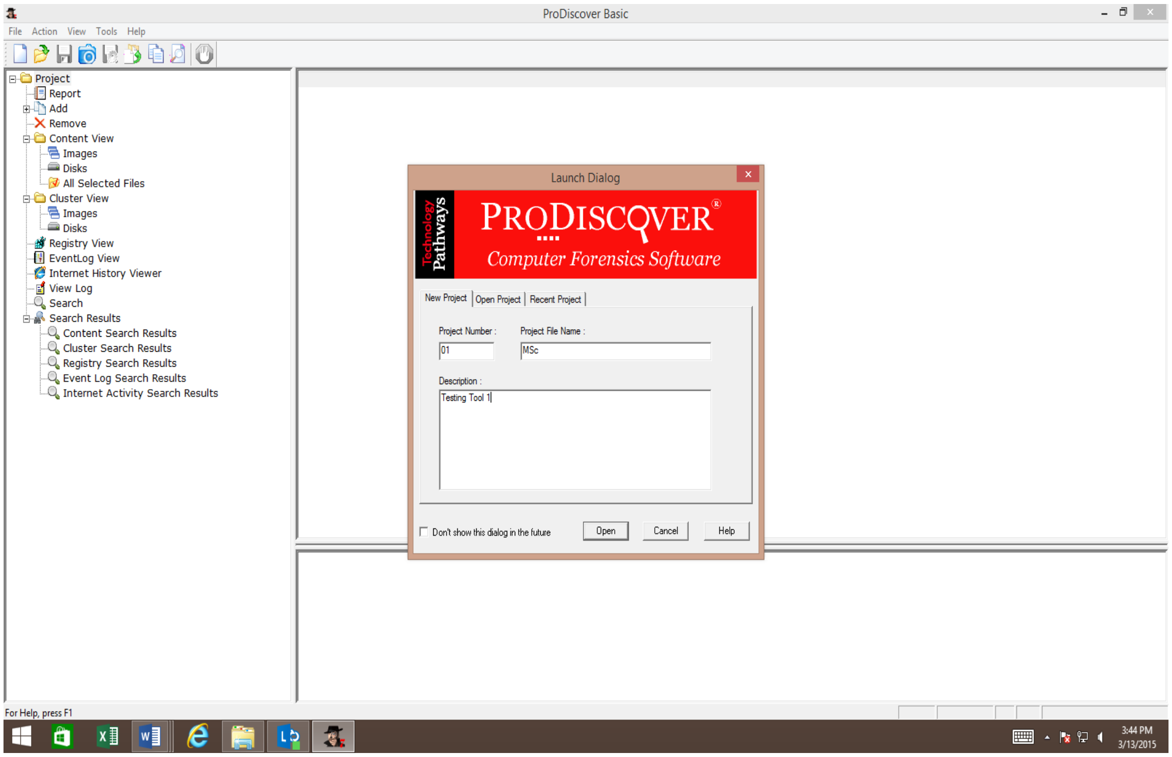
□ YES □ NO

In your own opinion, is the auditing methodology followed by KENAO adequate to be applied in forensic investigation of computer systems in the public sector?

□ YES □ NO

Appendix 3: Sample Output of Running Two Forensic Tools

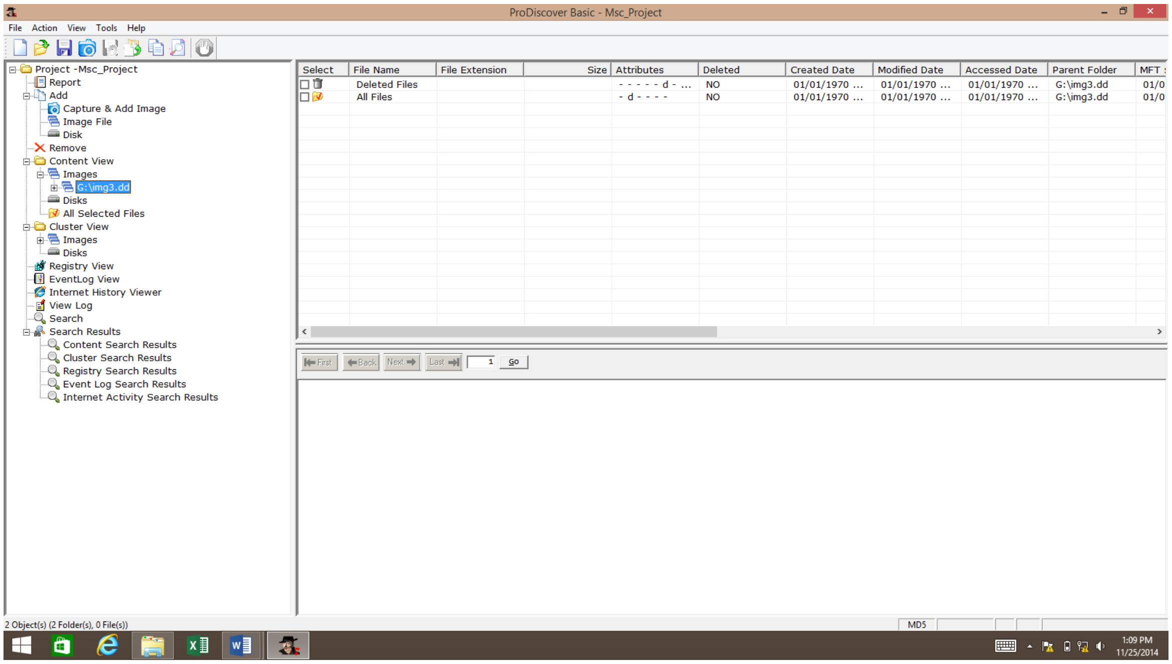
1. Prodiscover Progress Results



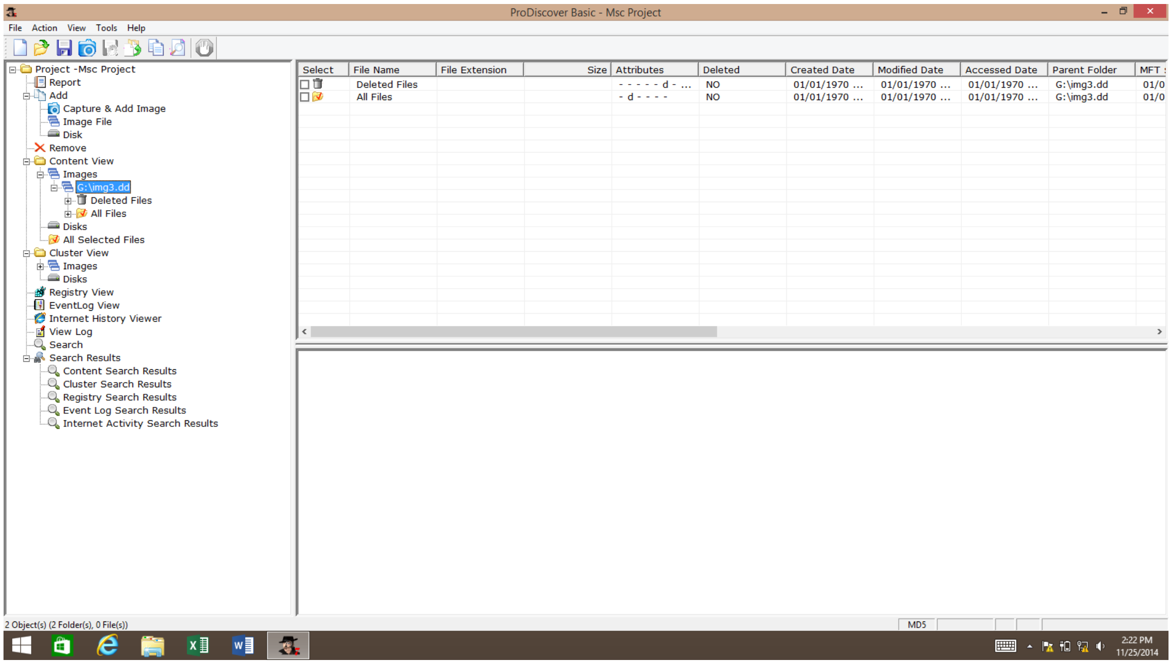
Project Number : 01

Project File Name : MSc

Description : Testing Tool 1

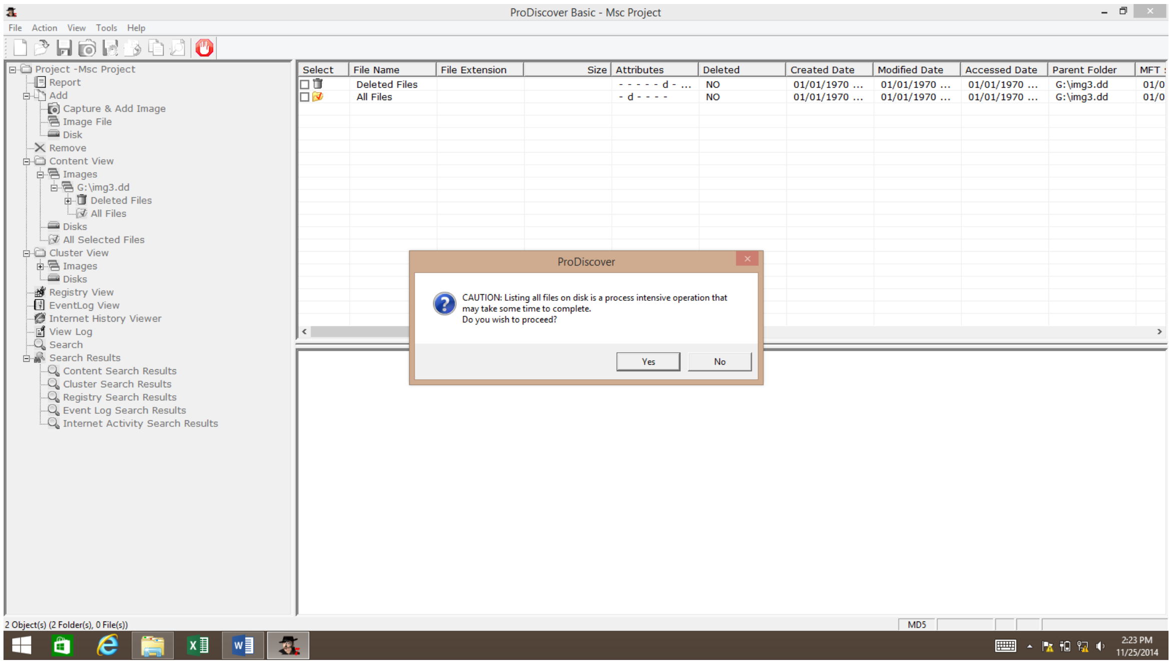


Select	File Name	File Extension	Size	Attributes	Deleted	Created Date	Modified Date	Accessed Date	Parent Folder	MFT :
☐	Deleted Files			- - - - - d - ...	NO	01/01/1970 ...	01/01/1970 ...	01/01/1970 ...	G:\img3.dd	01/0
☐	All Files			- d - - - -	NO	01/01/1970 ...	01/01/1970 ...	01/01/1970 ...	G:\img3.dd	01/0



Select	File Name	File Extension	Size	Attributes	Deleted	Created Date	Modified Date	Accessed Date	Parent Folder	MFT :
□	Deleted Files			- - - - - d - ...	NO	01/01/1970 ...	01/01/1970 ...	01/01/1970 ...	G:\img3.dd	01/0
□	All Files			- d - - - -	NO	01/01/1970 ...	01/01/1970 ...	01/01/1970 ...	G:\img3.dd	01/0

2 Object(s) (2 Folder(s), 0 File(s))

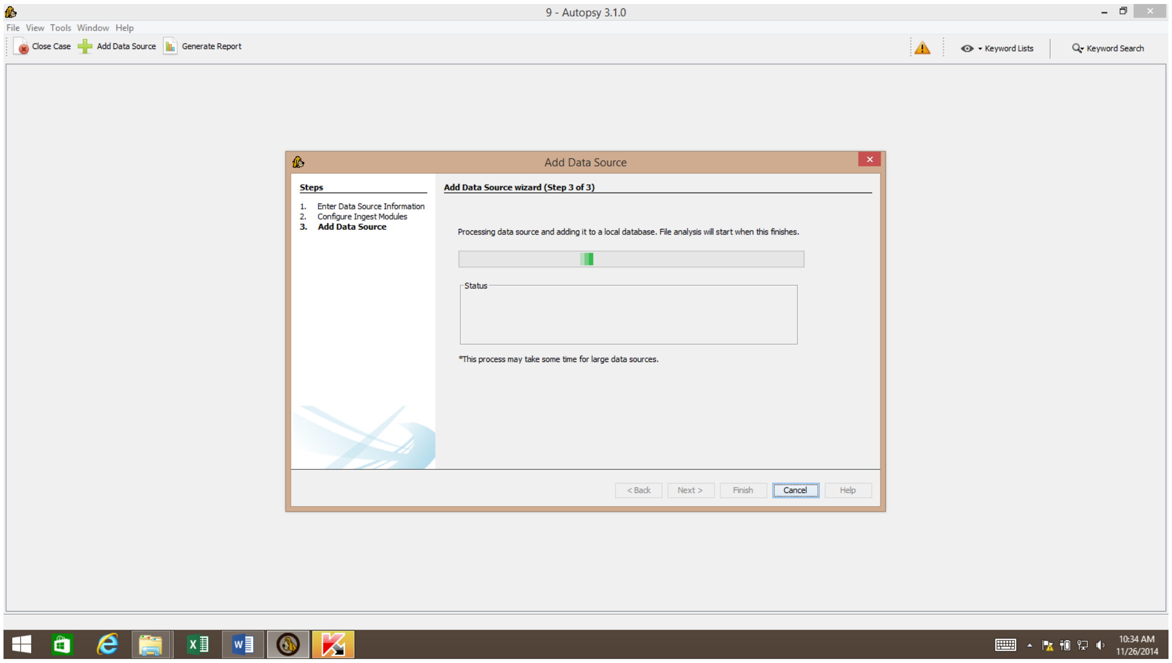


Select	File Name	File Extension	Size	Attributes	Deleted	Created Date	Modified Date	Accessed Date	Parent Folder	MFT :
□	Deleted Files			- - - - - d - ...	NO	01/01/1970 ...	01/01/1970 ...	01/01/1970 ...	G:\img3.dd	01/0
□	All Files			- d - - - -	NO	01/01/1970 ...	01/01/1970 ...	01/01/1970 ...	G:\img3.dd	01/0

CAUTION: Listing all files on disk is a process intensive operation that may take some time to complete.
Do you wish to proceed?

2 Object(s) (2 Folder(s), 0 File(s))

2. Autopsy Progress Results



Add Data Source

Steps

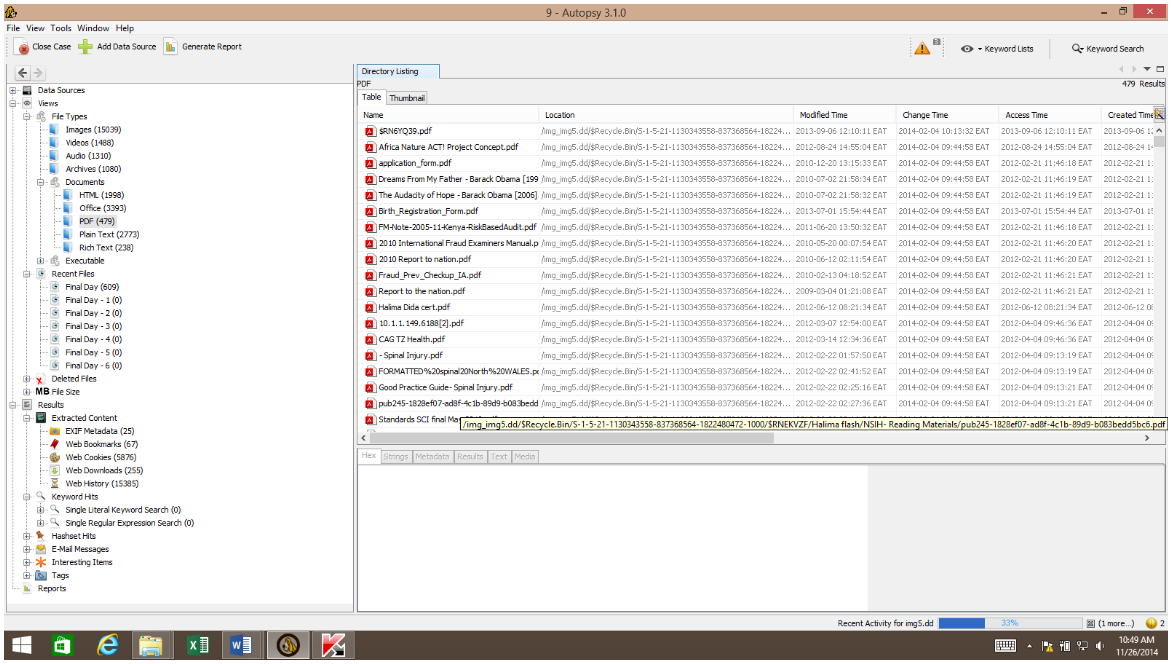
1. Enter Data Source Information
2. Configure Ingest Modules
3. **Add Data Source**

Add Data Source wizard (Step 3 of 3)

Processing data source and adding it to a local database. File analysis will start when this finishes.

Status

*This process may take some time for large data sources.



- Data Sources
- Views
  - File Types
    - Images (15039)
    - Videos (1488)
    - Audio (1310)
    - Archives (1080)
    - Documents
      - HTML (1998)
      - Office (3393)
      - PDF (479)
      - Plain Text (2773)
      - Rich Text (238)
    - Executable
  - Recent Files
    - Final Day (609)
    - Final Day - 1 (0)
    - Final Day - 2 (0)
    - Final Day - 3 (0)
    - Final Day - 4 (0)
    - Final Day - 5 (0)
    - Final Day - 6 (0)
  - Deleted Files
  - MB File Size
- Results
  - Extracted Content
    - EXIF Metadata (25)
    - Web Bookmarks (67)
    - Web Cookies (5876)
    - Web Downloads (255)
    - Web History (15385)
  - Keyword Hits
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (0)
  - Hashset Hits
  - E-Mail Messages
  - Interesting Items
  - Tags
- Reports

Directory Listing

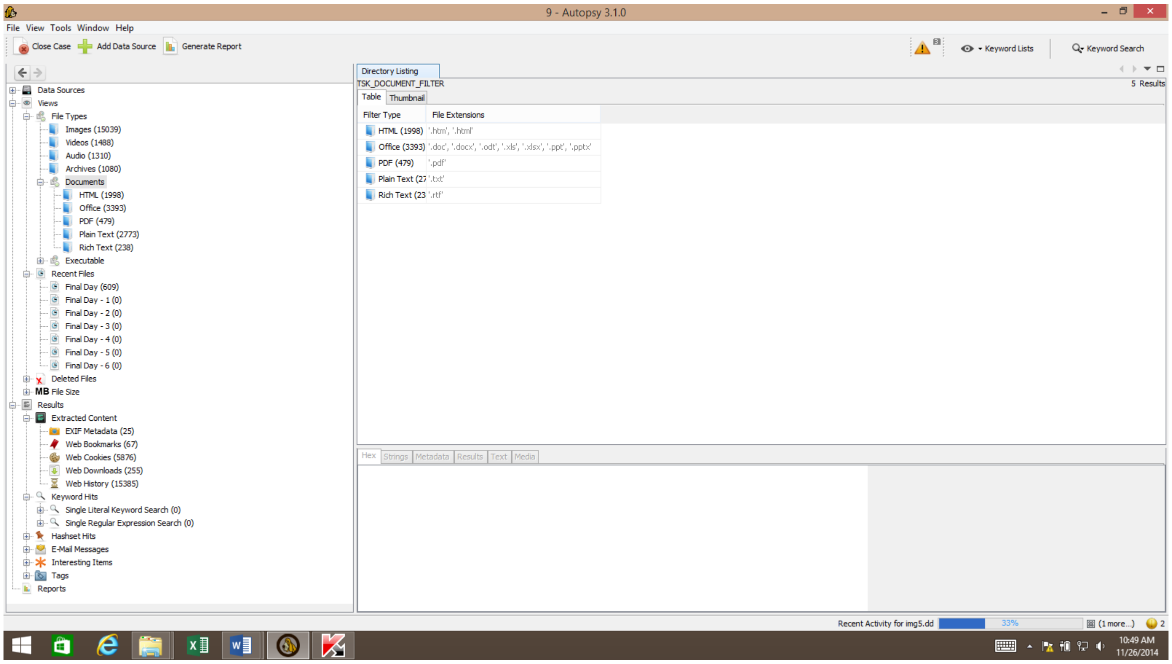
PDF

479 Results

Table | Thumbnail

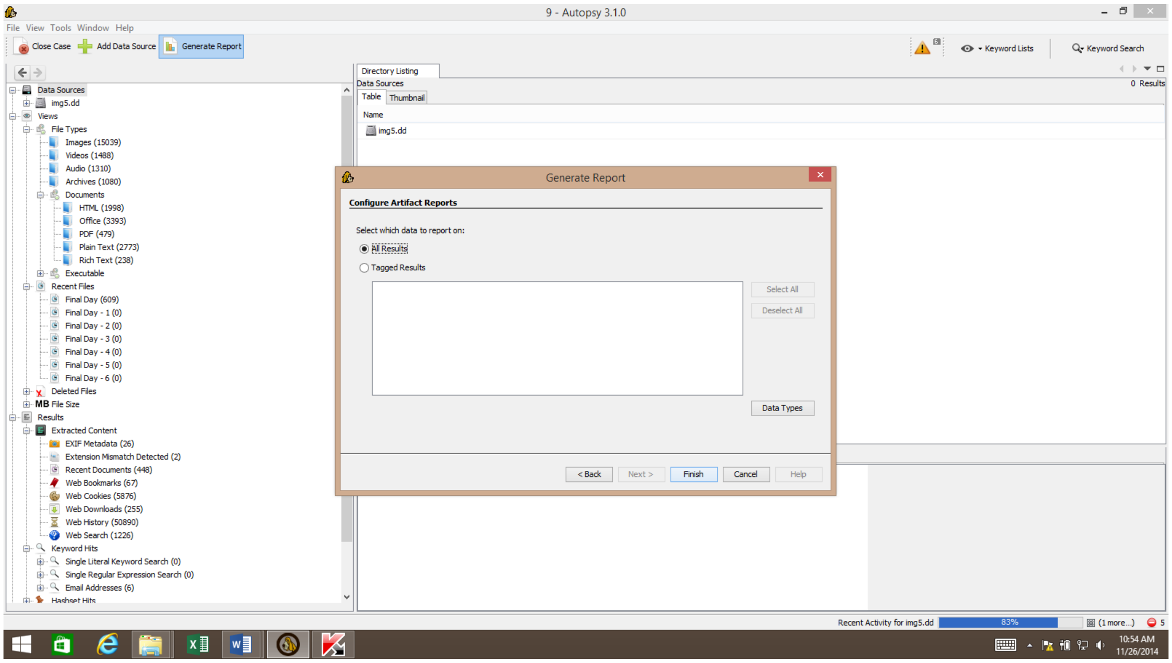
Name	Location	Modified Time	Change Time	Access Time	Created Time
$RN6YQ39.pdf	/img_img5.dd/$Recycle.Bin/S-1-5-21-1130343558-837368564-18224...	2013-09-06 12:10:11 EAT	2014-02-04 10:13:32 EAT	2013-09-06 12:10:11 EAT	2013-09-06 1
Africa Nature ACT! Project Concept.pdf	/img_img5.dd/$Recycle.Bin/S-1-5-21-1130343558-837368564-18224...	2012-08-24 14:55:04 EAT	2014-02-04 09:44:58 EAT	2012-08-24 14:55:04 EAT	2012-08-24 1
application_form.pdf	/img_img5.dd/$Recycle.Bin/S-1-5-21-1130343558-837368564-18224...	2010-12-20 13:15:33 EAT	2014-02-04 09:44:58 EAT	2012-02-21 11:46:18 EAT	2012-02-21 1
Dreams From My Father - Barack Obama [199	/img_img5.dd/$Recycle.Bin/S-1-5-21-1130343558-837368564-18224...	2010-07-02 21:58:34 EAT	2014-02-04 09:44:58 EAT	2012-02-21 11:46:19 EAT	2012-02-21 1
The Audacity of Hope - Barack Obama [2006]	/img_img5.dd/$Recycle.Bin/S-1-5-21-1130343558-837368564-18224...	2010-07-02 21:58:32 EAT	2014-02-04 09:44:58 EAT	2012-02-21 11:46:19 EAT	2012-02-21 1
Birth_Registration_Form.pdf	/img_img5.dd/$Recycle.Bin/S-1-5-21-1130343558-837368564-18224...	2013-07-01 15:54:44 EAT	2014-02-04 09:44:58 EAT	2013-07-01 15:54:44 EAT	2013-07-01 1
FM-Note-2005-11-Kenya-RiskBasedAudit.pdf	/img_img5.dd/$Recycle.Bin/S-1-5-21-1130343558-837368564-18224...	2011-06-20 13:50:32 EAT	2014-02-04 09:44:58 EAT	2012-02-21 11:46:18 EAT	2012-02-21 1
2010 International Fraud Examiners Manual.p	/img_img5.dd/$Recycle.Bin/S-1-5-21-1130343558-837368564-18224...	2010-05-20 00:07:54 EAT	2014-02-04 09:44:58 EAT	2012-02-21 11:46:20 EAT	2012-02-21 1
2010 Report to nation.pdf	/img_img5.dd/$Recycle.Bin/S-1-5-21-1130343558-837368564-18224...	2010-06-12 02:11:54 EAT	2014-02-04 09:44:58 EAT	2012-02-21 11:46:20 EAT	2012-02-21 1
Fraud_Prev_Checkup_IA.pdf	/img_img5.dd/$Recycle.Bin/S-1-5-21-1130343558-837368564-18224...	2010-02-13 04:18:52 EAT	2014-02-04 09:44:58 EAT	2012-02-21 11:46:21 EAT	2012-02-21 1
Report to the nation.pdf	/img_img5.dd/$Recycle.Bin/S-1-5-21-1130343558-837368564-18224...	2009-03-04 01:21:08 EAT	2014-02-04 09:44:58 EAT	2012-02-21 11:46:21 EAT	2012-02-21 1
Halima Dida cert.pdf	/img_img5.dd/$Recycle.Bin/S-1-5-21-1130343558-837368564-18224...	2012-06-12 08:21:34 EAT	2014-02-04 09:44:58 EAT	2012-06-12 08:21:34 EAT	2012-06-12 0
10.1.1.149.6188[2].pdf	/img_img5.dd/$Recycle.Bin/S-1-5-21-1130343558-837368564-18224...	2012-03-07 12:54:00 EAT	2014-02-04 09:44:58 EAT	2012-04-04 09:46:36 EAT	2012-04-04 0
CAG TZ Health.pdf	/img_img5.dd/$Recycle.Bin/S-1-5-21-1130343558-837368564-18224...	2012-03-14 12:34:36 EAT	2014-02-04 09:44:58 EAT	2012-04-04 09:46:36 EAT	2012-04-04 0
- Spinal Injury.pdf	/img_img5.dd/$Recycle.Bin/S-1-5-21-1130343558-837368564-18224...	2012-02-22 01:57:50 EAT	2014-02-04 09:44:58 EAT	2012-04-04 09:13:19 EAT	2012-04-04 0
FORMATTED%20spinal20North%20WALES.pc	/img_img5.dd/$Recycle.Bin/S-1-5-21-1130343558-837368564-18224...	2012-02-22 02:41:52 EAT	2014-02-04 09:44:58 EAT	2012-04-04 09:13:19 EAT	2012-04-04 0
Good Practice Guide- Spinal Injury.pdf	/img_img5.dd/$Recycle.Bin/S-1-5-21-1130343558-837368564-18224...	2012-02-22 02:25:16 EAT	2014-02-04 09:44:58 EAT	2012-04-04 09:13:21 EAT	2012-04-04 0
pub245-1828ef07-ad8f-4c1b-89d9-b083bedd	/img_img5.dd/$Recycle.Bin/S-1-5-21-1130343558-837368564-18224...	2012-02-22 02:27:36 EAT	2014-02-04 09:44:58 EAT	2012-04-04 09:13:21 EAT	2012-04-04 0
Standards SCI final Ma	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

/img_img5.dd/$Recycle.Bin/S-1-5-21-1130343558-837368564-1822480472-1000/$RNEKVZF/Halima flash/NSIH- Reading Materials/pub245-1828ef07-ad8f-4c1b-89d9-b083bedd5bc6.pdf



TSK_DOCUMENT_FILTER

Filter Type	File Extensions
HTML (1998)	'.htm', '.html'
Office (3393)	'.doc', '.docx', '.odt', '.xls', '.xlsx', '.ppt', '.pptx'
PDF (479)	'.pdf'
Plain Text (27	'.txt'
Rich Text (23	'.rtf'



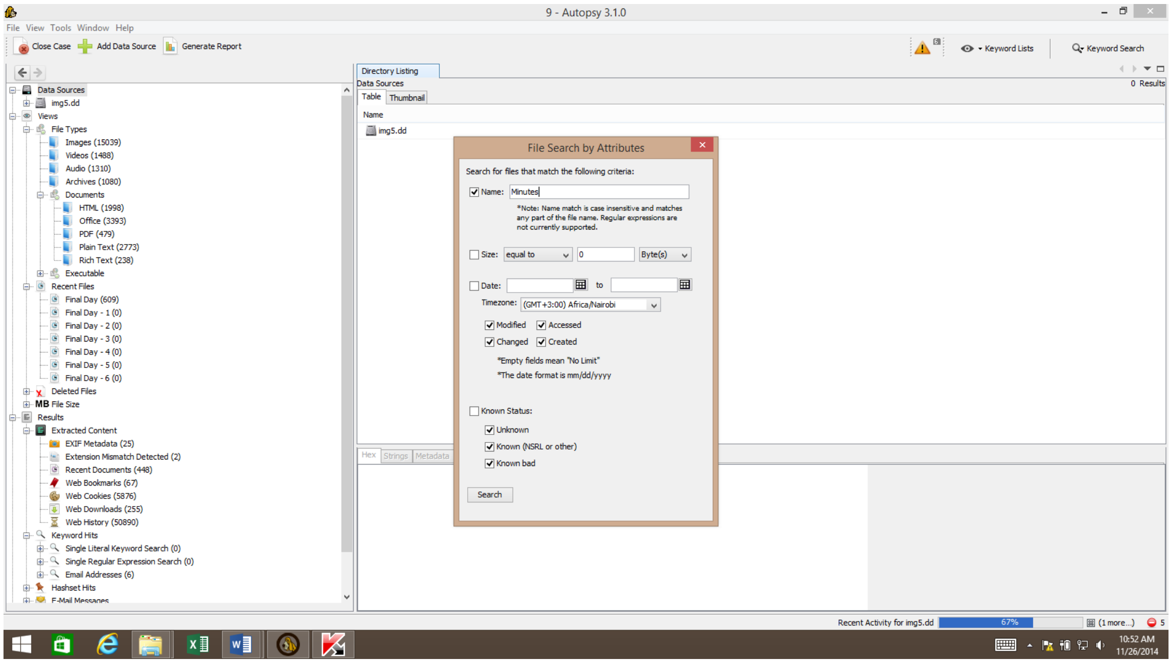
Generate Report

Configure Artifact Reports

Select which data to report on:

● All Results

○ Tagged Results



File Search by Attributes

Search for files that match the following criteria:

☑ Name: Minutes

*Note: Name match is case insensitive and matches any part of the file name. Regular expressions are not currently supported.

☐ Size: equal to 0 Byte(s)

☐ Date: to

Timezone: (GMT+3:00) Africa/Nairobi

☑ Modified ☑ Accessed

☑ Changed ☑ Created

*Empty fields mean "No Limit"

*The date format is mm/dd/yyyy

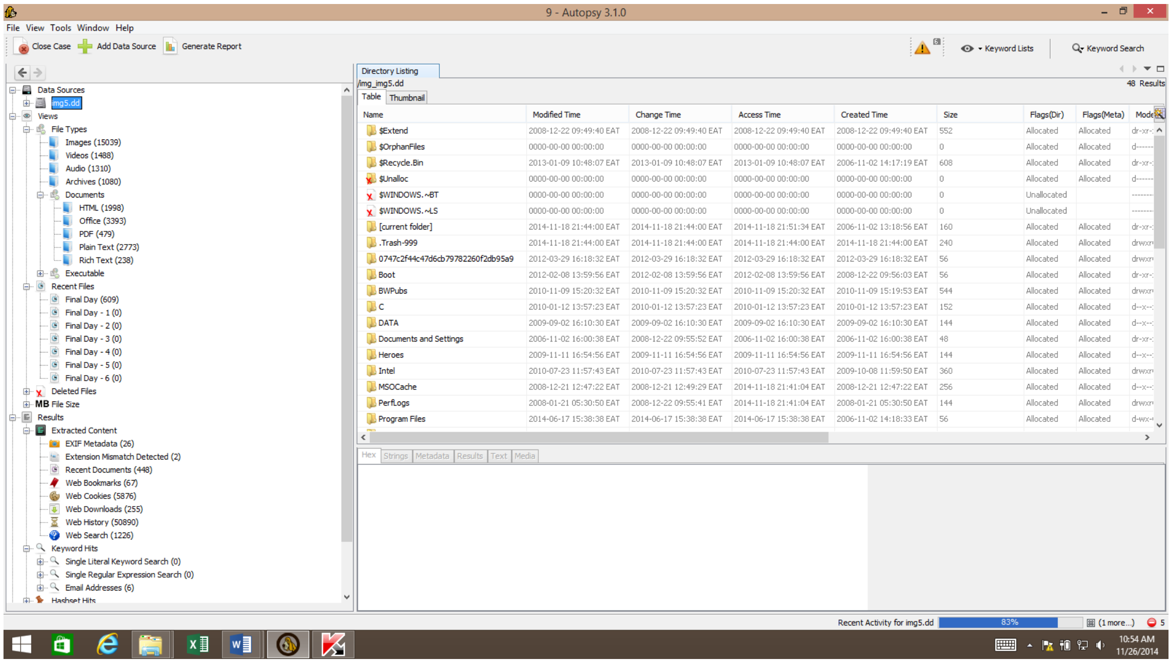
☐ Known Status:

☑ Unknown

☑ Known (NSRL or other)

☑ Known bad

Search



/img_img5.dd

48 Results

Name	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Mode
$Extend	2008-12-22 09:49:40 EAT	2008-12-22 09:49:40 EAT	2008-12-22 09:49:40 EAT	2008-12-22 09:49:40 EAT	552	Allocated	Allocated	dr-xr-
$OrphanFiles	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	d------
$Recycle.Bin	2013-01-09 10:48:07 EAT	2013-01-09 10:48:07 EAT	2013-01-09 10:48:07 EAT	2006-11-02 14:17:19 EAT	608	Allocated	Allocated	dr-xr-
$Unalloc	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	d------
$WINDOWS.~BT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		-------
$WINDOWS.~LS	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		-------
[current folder]	2014-11-18 21:44:00 EAT	2014-11-18 21:44:00 EAT	2014-11-18 21:51:34 EAT	2006-11-02 13:18:56 EAT	160	Allocated	Allocated	dr-xr-
.Trash-999	2014-11-18 21:44:00 EAT	2014-11-18 21:44:00 EAT	2014-11-18 21:44:00 EAT	2014-11-18 21:44:00 EAT	240	Allocated	Allocated	drwxr
0747c2f44c47d6cb79782260f2db95a9	2012-03-29 16:18:32 EAT	2012-03-29 16:18:32 EAT	2012-03-29 16:18:32 EAT	2012-03-29 16:18:32 EAT	56	Allocated	Allocated	drwxr
Boot	2012-02-08 13:59:56 EAT	2012-02-08 13:59:56 EAT	2012-02-08 13:59:56 EAT	2008-12-22 09:56:03 EAT	56	Allocated	Allocated	dr-xr-
BWPubs	2010-11-09 15:20:32 EAT	2010-11-09 15:20:32 EAT	2010-11-09 15:20:32 EAT	2010-11-09 15:19:53 EAT	544	Allocated	Allocated	drwxr
C	2010-01-12 13:57:23 EAT	2010-01-12 13:57:23 EAT	2010-01-12 13:57:23 EAT	2010-01-12 13:57:23 EAT	152	Allocated	Allocated	d--x--
DATA	2009-09-02 16:10:30 EAT	2009-09-02 16:10:30 EAT	2009-09-02 16:10:30 EAT	2009-09-02 16:10:30 EAT	144	Allocated	Allocated	d--x--
Documents and Settings	2006-11-02 16:00:38 EAT	2008-12-22 09:55:52 EAT	2006-11-02 16:00:38 EAT	2006-11-02 16:00:38 EAT	48	Allocated	Allocated	dr-xr-
Heroes	2009-11-11 16:54:56 EAT	2009-11-11 16:54:56 EAT	2009-11-11 16:54:56 EAT	2009-11-11 16:54:56 EAT	144	Allocated	Allocated	d--x--
Intel	2010-07-23 11:57:43 EAT	2010-07-23 11:57:43 EAT	2010-07-23 11:57:43 EAT	2009-10-08 11:59:50 EAT	360	Allocated	Allocated	drwxr
MSOCache	2008-12-21 12:47:22 EAT	2008-12-21 12:49:29 EAT	2014-11-18 21:41:04 EAT	2008-12-21 12:47:22 EAT	256	Allocated	Allocated	d--x--
PerfLogs	2008-01-21 05:30:50 EAT	2008-12-22 09:55:41 EAT	2014-11-18 21:41:04 EAT	2008-01-21 05:30:50 EAT	144	Allocated	Allocated	drwxr
Program Files	2014-06-17 15:38:38 EAT	2014-06-17 15:38:38 EAT	2014-06-17 15:38:38 EAT	2006-11-02 14:18:33 EAT	56	Allocated	Allocated	d-wx-

Appendix 4: The Sleuthkit/Autopsy User Guide for Windows

The Sleuth Kit/Autopsy User Guide for Windows

Sleuthkit and Autopsy Installation

1. Step I: Install Cygwin

Browse www.cygwin.com and download Cygwin

When the file download window pops up, click open and then Next

Confirm that, "Install from Internet" is selected, then Click Next Again.

Set your Cygwin root directory and set the Package directory in the Root directory as follows:

C:\Cygwin\Package, then Click Next.

Make sure "Direct Connection" is selected then click Next.

Click on the word, "Devel". Under Devel, select all the desired packages (All) and then click Next. Setup will download all desired packages and install them, when it is finished, click "Finish" to create Desktop and Start menu icons.

2. Step II: Compile Sleuth Kit

Browse to **http://www.sleuthkit.org/sleuthkit**

Click on "Download", then click "Source code"

When the "File Download" window pops up, click Save then move to C:\cygwin\usr\local then click "Save" to save the file in this directory.

Double click on the Cygwin icon on your desktop to open a Cygwin Bash shell

Type cd /usr/local to change to /usr/local and enter the command "tar xvfz sleuthkit-1.70.tar.gz " to uncompress the file. Do "cd /sleuthkit" to change to the sleuthkit directory then type "make".

The compilation should complete successfully. Lastly, make a copy of the DLL in the same directory as the Sleuthkit command-line binaries. To do this, close the current Bash shell window and open a new one. Enter the command, ‘cp /bin/Cygwin/.dll /usr/local/sleuthkit/bin’ to copy the DLL.

3. Step III: Install Autopsy

Browse to http://www.sleuthkit.org/autopsy
Click on the “Download link”, then on the “Source Code” link.

When the “File Download” window pops up, click on “Save” then move to C:/Cygwin/usr/local if not already there then click on “Save”

Open a new Bash shell with the Cygwin icon on your desktop. Change back to C:/Cygwin/usr/local and uncompress autopsy by entering the command, “tar xvfz Autopsy-2.01.tar.gz”

Create an “Evidence directory” using the command, “mkdir Evidence”

Change into Autopsy’s directory by entering the command, “cd /Autopsy-2.01” and then enter the “make” command to begin the configuration process. When it prompts you whether you have purchased copy of the NSRL, enter “no”

The script will then ask you for the “Evidence-locker directory”. You should enter the command, “/usr/local/Evidence”

The script should complete with the statement, “Execute the ./Autopsy” command to start with the default settings. It starts its own service on port 9999. Copy the URL address it displays and paste it on your browser then press “Enter”. You should see the sleuthdog graphic and options to open a new case, start a new case, etc. Autopsy is now running, Congratulations!

How to use Autopsy

Adding a data source (image, local disk, logical files)

Data sources are added to a case. A case can have a single data source or it can have multiple data source if they are related. Currently, a single report is generated for an entire case, so if you need to report on individual data sources, then you should use one data source per case.

Creating a Case

Use either the "Create New Case" option on the Welcome screen or from the "File" menu to create a Case. This will start the New Case Wizard. The Wizard will prompt you to supply it with the name of the case and a directory to store the case results into. You can optionally provide other details.

Adding a Data Source

The next step is to add input data source to the case. The Add Data Source Wizard will start automatically after the case is created or you can manually start it from the "File" menu or toolbar. You will need to choose the type of input data source to add (image, local disk or logical files and folders). Next, supply it with the location of the source to add.

For a disk image, browse to the first file in the set (Autopsy will find the rest of the files). Autopsy currently supports E01 and raw (dd) files.

For local disk, select one of the detected disks. Autopsy will add the current view of the disk to the case (i.e. snapshot of the meta-data). However, the individual file content (not meta-data) does get updated with the changes made to the disk. You need to run Autopsy as an Administrator to detect all disks.

For logical files (a single file or folder of files), use the "Add" button to add one or more files or folders on your system to the case. Folders will be recursively added to the case.

There are a couple of options in the wizard that will allow you to make the ingest process faster. These typically deal with deleted files. It will take longer if unallocated space is analyzed and the entire drive is searched for deleted files. In some scenarios, these recovery steps must be performed and in other scenarios these steps are not needed and instead fast results on the allocated files are needed. Use these options to control how long the analysis will take.

Autopsy will start to analyze these data sources and add them to the case and internal database. While it is doing that, it will prompt you to configure the Ingest Modules.

Ingest Modules

You will be prompted to configure the Ingest Modules. Ingest modules will run in the background and perform specific tasks. The Ingest Modules analyze files in a prioritized order so that files in a user's directory are analyzed before files in other folders. Ingest modules can be developed by third-parties and here are some of the standard ingest modules that come with Autopsy:

Recent Activity extracts user activity as saved by web browsers and the OS.

Hash Lookup uses hash databases to ignore known files from the NIST NSRL and flag known bad files. Use the "Advanced" button to add and configure the hash databases to use during this process. You will get updates on known bad file hits as the ingest occurs. You can later add hash databases via the Tools -> Options menu in the main UI.

Keyword Search uses keyword lists to identify files with specific words in them. You can select the keyword lists to search for automatically and you can create new lists using the "Advanced" button. Note that with keyword search, you can always conduct searches after ingest has finished. The keyword lists that you select during ingest will be searched for at periodic intervals and you will get the results in real-time. You do not need to wait for all files to be indexed.

When you select a module, you will have the option to change its settings. For example, you can configure which keyword search lists to use during ingest and which hash databases to use. While ingest modules are running in the background, you will see a progress bar in the lower right. You can use the GUI to review incoming results and perform other tasks while ingest is running at that time. The Data Sources root node shows all data in the case.

The individual image nodes show the file system structure of the disk images or local disks in the case.

The Logical File Set nodes show the logical files in the case.

The Views node shows the same data from a file type or timeline perspective.

The Results node shows the output from the ingest modules.

When you select a node from the tree on the left, a list of files will be shown in the upper right. You can use the Thumbnail view in the upper right to view the pictures. When you select a file from the upper right, its contents will be shown in the lower right. You can use the tabs in the lower right to view the text of the file, an image, or the hex data.

If you are viewing files from the Views and Results nodes, you can right-click on a file to go to its file system location. This feature is useful to see what else the user stored in the same folder as the file that you are currently looking at. You can also right click on a file to extract it.

If you want to search for single keywords, then you can use the search box in the upper right. You can tag (or bookmark) arbitrary files so that you can more quickly find them later.

Ingest Inbox

The Ingest Inbox receives messages from the ingest modules as they find results. You can open the inbox to see what has been recently found. It keeps track of what messages you have read.

The intended use of this inbox is that you can focus on some data for a while and then check back on the inbox at a time that is convenient for them. You can then see what else was found while you were focused on the previous task. You may learn that a known bad file was found or that a file was found with a relevant keyword and then decide to focus on that for a while.

When you select a message, you can then jump to the Results tree where more details can be found or jump to the file's location in the file system.

Timeline (Beta)

There is a basic timeline view that you can access via the Tools -> Make Timeline feature. This will take a few minutes to create the timeline for analysis. Its features are still in development.

Some of the Common analysis tasks are illustrated below:

Web Artifacts

If you want to view the user's recent web activity, make sure that the Recent Activity ingest module was enabled. You can then go to the "Results" node in the tree on the left and then into the "Extracted Data" node. There, you can find bookmarks, cookies, downloads, and history.

Known Bad Hash Files

If you want to see if the data source had known bad files, make sure that the Hash Lookup ingest module was enabled. You can then view the "Hashset Hits" section in the "Results" area of the tree on the left. Note that hash lookup can take a long time. When you find a known bad file in this interface, you may want to right click on the file to also view the file's original location.

Media: Images and Videos

If you want to see all images and video on the disk image, then go to the "Views" section in the tree on the left and then "File Types". Select either "Images" or "Videos". You can use the thumbnail option in the upper right to view thumbnails of all images. Also, you can select an image or video from the upper right and view the video or image in the lower right. The Video will be played with sound.

Reporting

A final report can be generated that will include all analysis results. Use the "Generate Report" button to create this. It will create an HTML or XLS report in the Reports folder of the case folder. If you forgot the location of your case folder, you can determine it using the "Case Properties" option in the "File" menu. There is also an option to export report files to a separate folder outside of the case folder.