University of Nairobi

College of Biological and Physical sciences

School of Computing and Informatics

Comparative evaluation of the effectiveness of Smartphone forensics tools.

Onditi Reagan Johns

P53/6576/2017

Supervisor: Dr.Elisha Odira Abade

Research Project Report Submitted in Partial Fulfillment of the requirement for the Award of the Degree of Master of Science in Distributed Computing Technology.

December 2019.

Declaration

I Onditi Reagan Johns, do hereby declare that this research project is entirely my own work and where there are work or contributions of other individuals, it has been duly referenced as acknowledgement.

To the best of my knowledge, similar research has not been carried out before or previously presented to any other University.

Sign: ___________________ Date: ______________________

Onditi Reagan Johns

This project has been submitted in partial fulfillment of the requirement for the Master of Science degree in Distributed Computing Technology of the University of Nairobi with my approval as the University supervisor.

Sign: ______________________ Date: ______________________

Dr.Elisha Odira Abade.

School of Computing and Informatics, University Of Nairobi.

Dedication

I dedicate this research to Digital forensics organizations in Kenya, The Communication Authority of Kenya and Forensics Software companies around the world specifically the once who accepted to send me the trial versions of the software which allowed me to carry out the research successfully.

Acknowledgment

First and foremost, I would like to give thanks to the Almighty God for enabling me to conduct this research, My Parents Mr. and Mrs. Onditi for continues encouragement to work hard and achieve the best in education.

To my family Linet, Radley, and Ramone who are always around me wondering what I am always doing with Laptops and the Mobile Phones during this journey.

Great appreciation to my Supervisor Dr.Elisha Abade for his relentless support with his much wealth of knowledge in computer security that he shared in the form of ideas and reviews that helped in the completion of this research. I am thankful to the school of Computing and Informatics fraternity at the University of Nairobi for support while conducting this research.

Extremely grateful to my Parents for their love, Understanding, financial support and encouragement to soldier on and see this work to completion. Their prayers and goodwill helped me put in more effort to achieve this.

Finally, I would like to thank my wonderful friends, colleagues and all the people that directly or indirectly supported and contributed to the realization of this research.

Abstract

Technological growth in mobile phones and the development of smart phones has led to increased use and dependence on the mobile phone. The explosion use of mobile phones has led to fraud, cyber stalking, Harassment, Child pornography and other criminal incidents linked with mobile phones. There is a need for suitable mobile phone forensic tools that can be used to conduct a proper investigation by retrieving relevant artifacts that can be presented and hold a case before a jury in Kenya. Smartphone forensics which is part of digital forensics requires tools that are capable of recovering what is important for the forensic examiner or investigator. During the Evaluation of the tools used in Kenya, Most of the Investigative organizations preferred Oxygen suite and Cellebrite to acquire and Analyze the data but our research also looked at what the Open source tool can retrieve from the images acquired. Total of five smartphones were imaged and analyzed, Oxygen suite retrieved more WhatsApp messages on iPhone compare to Cellebrite and Autopsy this means that it is the best tool that can be used for acquisition of WhatsApp artifacts from iPhone phones, when it comes to acquisition of Contacts, Pictures, Text Messages and call logs from smartphone, Cellebrite Touch is the best.T-tool (Autopsy) is an open source software for forensic which can run on Linux and Windows but could not retrieve many artifacts from all the five phones used in the experiment. Other software's like MOBILedit, Moblyze, and Elcomsoft for iPhones where also used by some Few organizations.

Contents

List of Tables

List of figures

List of Charts

CHAPTER ONE

INTRODUCTION

1.1 Background

Kenya is the world leader in mobile overtaking Nigeria's share of Internet traffic in 2017, at 83 percent. (Standard Newspaper March 17, 2018).

According to the latest sector statistics from the Communications Authority, as of 30th September, 2018 stood at 46.6 million active phone subscriptions in the nation.

This marked a growth of 2.4 percent when compared to 45.5 million subscriptions recorded as at 30th June 2018. Subsequently, mobile penetration rose by 2.3 percentage points to stand at 100.1 percent from 97.8 percent reported last quarter. According to (*Global Cybersecurity Index (GCI) 2017*, 2017) Kenya is ranked third after Mauritius and Rwanda on cybersecurity-related crimes. Kenya lost around 17.7 billion to cyber-crimes (*Governance in focus Cyber risk reporting in the UK Cyber reporting survey Contents*, 2017). However as technology develops so does the vulnerabilities of smartphones to Frauds, phone misuse, cyberstalking, forgery, harassment, etc. In civil, illegal and even high profile instances, data obtained from mobile phones continue to be used as proof (Aljazeera, 2015). The fast advances in technology and procedures and the growing popularity of mobile devices present major difficulties for researchers and law enforcement officials around the globe (Yadav, Ahmad and Shekhar, 2011).

Forensic file and system assessment is a helpful way to characterize big Digital data quantities. It is essential to be able to evaluate digital data within these systems with the increase of mobile technologies and the quantity of information that mobile phone systems now retain. Additionally, it has become increasingly useful to derive metadata from bulk mobile data since most communications now happen via mobile devices. To extract and evaluate information content, digital forensic tools such as Cellebrite are needed. These instruments served their purpose well and enhanced over time. (Martin, 2017).

1.2 Problem Statement

Based on a literature review, a comparative study of different Smartphone forensic tools (Namrata R, 2013), found that there is no generic forensic methodology available that can acquire, analyze, and recover evidence from most Smartphones.

Other studies have investigated some forensic tools for their effectiveness, they have used more than one tool which of course can be constraining, and resource-intensive(Osho, 2016)

Besides, these studies conducted in Nigeria, Australia and Saudi Arabia (Kausar, 2014). Little or scanty information is available in determining the effectiveness of these forensic tools. This research focus on assessing of the effectiveness of smartphone forensic tools used in Kenya from images acquired from different phones using Oxygen suite, Cellebrite software (UFED Touch) and T-tool (Autopsy) Smartphone forensics tools with the same tools used for imaging and addressing the analytical and presentation of digital evidence that can stand a jury process.

1.3 Research Objectives

1.3.0 General Objective

- The primary aim of this research is to comparatively analyze and evaluate the effectiveness and performance of forensics tools on Smartphone

1.3.1 Specific Objectives

- To identify Smartphone forensics tools used in Kenya
- To determine the performance of the forensic tools based on usability.
- To evaluate the effectiveness of the forensic tools on imaging and detection of evidential information.

1.4 Scope

The scope of this study was restricted to evaluating and comparison of raw artifacts acquired from five mobile devices using Cellebrite Touch, an oxygen suite and analyzed using the same tools with one additional open source forensics tool 'T' tool (Autopsy).

1.5 Research Questions

Through this research, we aim to answer the following research questions:

- What are the mobile phone forensics tools used in Kenya
- Mobile forensic tools are preferred by Investigators and Why?
- Are there differences among Cellebrite Touch, Oxygen suite and 'T' Tool (Autopsy) concerning mobile device Imaging and analytical capabilities?
- The number of files found by one tool that is not found by the other?

Mobile forensics is unlike computer forensics that provides forensic examiners with distinctive difficulties. Law enforcement and forensic examiners often struggle with mobile devices to acquire digital evidence.

1.6 Assumptions and Limitations of the Study

Research would be intended to propose the implementation of a mobile phone digital forensics tool applicable in Kenya. It may not be possible to carry out the study on all the Organization doing mobile phone forensic due to time and cost constraints, therefore sampling was used in some areas.

Since the research involved the government and private sector, it was assumed that there will be cooperation from the information providers and the organization targeted.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This section demonstrates a review of literature on digital forensics, forensics models and instruments of forensics. It started with the definition of the digital forensics and the smartphone forensics overview. The section then provides an in-depth look at the ongoing cybercrime and Kenya's need for a forensic smartphone. Mobile digital forensic tools are then explored as critical facets of this research. Mobile forensic tools are integrated into the process of digital forensics,
their function and role in the development of a smartphone forensic manual must be studied.

2.2 Digital Forensics

Digital forensics is a forensics element that has evolved to tackle computers and other digital devices ' legal proof characteristics. Digital forensics also involve computer forensics in some instances and may include subdivisions such as mobile forensics, cloud forensics, information forensics, and cyber forensics. The method of gathering proof, recovering lost information, determining how the entry was created into a scheme, including what was accomplished and a sequence with the supposed device. (Wright, 2001).

This is an investigative procedure mainly used to detect and collect evidence of computer-related crimes like hacking, computer fraud, and identity theft. Digital phones have increased in the last two centuries, both for the traditional perpetrators, and a new form of the crime scene has been developed. Increasingly digital devices are used to commit a crime or as a supplement to crime. While proof from such a crime can be physical and readily available to criminals, other officials in the digital field may be more challenging than ever. (Zareen and Baig, 2010).Digital forensics has become widespread as law enforcement acknowledges that modern-day life involves a range of digital tools that can be used for criminal activity, not just computer systems. Unfortunately, a normal or coherent digital forensic methodology does not exist, but rather a set of processes and instruments based on the experiences of law enforcement, system administrators, and hackers. Palmer indicates that the development of digital forensics has been based on ad hoc instruments and methods rather than on the scientific community, where many of the other traditional forensic sciences have come from (Palmer, 2001). This is difficult as proof must be acquired using techniques that prove to obtain and evaluate proof reliably without bias or alteration. The processes for carrying out forensics are neither coherent nor standardized in many digital crimes. Over the past few years, a number of authors have tried to create guidelines, but they have been written with a focus on technology details and without consideration for a widespread process.

2.3 Overview of Mobile phone Forensics

Forensics is the law-based science of researching and presenting in court concepts or digital proof (Sridhar 2011). Forensics includes effective investigation procedures, steps, stages or processes. The stages of forensics include preparation and planning, accessing crime scene, collecting, preserving, transporting, analyzing, documenting and presenting. These stages also apply to forensics on the phone.

A mobile phone is a digital instrument that is specifically used today to commit various offences (Vishal et al 2012) as a communication instrument that can be used to support traditional offences. Mobile devices, on the other side, can also be a destination or rightly used for cybercrimes. The devices would contain information on proof in all instances. A typical smartphone, for instance, includes prospective evidence data including user-created information such as contacts, audio, video, and files; internet-related information, including email texts and web browser history; and third-party apps installed (Casey E et al 2011).

2.4 Current State of Cybercrime, Digital and Mobile 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, supercomputers, client-server networks, mobile phones, laptops, cloud, LANs and WANs conveying information across the globe. The rapid changes in technologies involving computers, Cloud storage, and mobile devices have led to the wide use of such in criminal activities and putting in place adequate and efficient security measures have 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. As more and more organizations become victims of intrusion and exploitation, the Kenyan Cybersecurity landscape is evolving rapidly. The fast-growing digitally-enabled working ecosystem in

Kenya is defined by increasingly advanced insiders and outsiders launching more frequent and targeted attacks, according to the Serianu Cyber Security Report 2016.

2.5 The Need for Mobile phone Forensics

(Imtiaz 2004), says that a single safety violation or attack can cause major economic and reputational losses that can devastate a well-known organization.

As safety specialists try their utmost to protect themselves against the recent types of assaults, attack ers are developing plans and potential for more advanced assaults. The author explains that most security attacks leave behind some trails which can be used by forensic investigators to track down the attacker. In 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. The Kenya Cyber Security Report 2014, released by Serianu Consultants, It shows that implementation of technology is driving Kenya's business innovation and development while exposing the nation to fresh and emerging threats. Due to the growing importance of data held within it, caber-terrorists, spies, hackers, and fraudsters are increasingly motivated to target ICT infrastructure, driven by the perceived reduced detection and capture danger relative to traditional crime. With the increasing adoption of technology, the nation faces an evolving cyber threat landscape. Given 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.

2.6 Process of Digital Forensics

Digital forensic examiners rely on interpreting data and information collected through instruments and providing results through instruments that can be trusted. The digital forensic process can be split into procurement, evaluation, and presentation according to (Altheide and Carvey 2011). Acquisition relates to digital device collection to be reviewed. These may include a physical hard drive, optical media, and digital cameras, mobile phones, embedded device chips, memory cards or single document files. The acquisition process should consist of creating a duplicate of the original data and keeping good records of the performed event (Ademu et al, 2011). The purpose of digital evidence duplication is to copy the initial digital evidence that protects and maintains the evidence before the digital forensic professional analyzes it from destruction, harm, or modification.

According to the 2001 Digital Forensic Research Workshop (DFRWS) Analysis related to the actual medi a examination, the identification comprises
discovering objects present in the device involved and then reducing this set of items needed further

(Palmer, 2001). These items are then analyzed accordingly. File system analysis, file content review, log analysis, statistical analysis, etc. can be the kinds of analysis performed. Then the examiner interprets the outcomes of this assessment based on the training, knowledge, experimentation, and experience of the examiner.

The presentation is when the examiner shares with interested professionals the results of the analytical phase. This involves generating a report of the examiner's actions, uncovered evidence and the evidence's meaning.

2.7 Mobile Forensic Models

It provides a review of important literature on mobile forensics issues and trends as well as the digital evidence generated from the method. Included in this review is literature produced for the digital forensics method concerning various models, methodologies, and frameworks (terms used mutually in the field). In this job, the references made to methodology and structure are particularly important as it offers a dual scheme with a structure of values and a step-by-step methodology for carrying out the particular process.

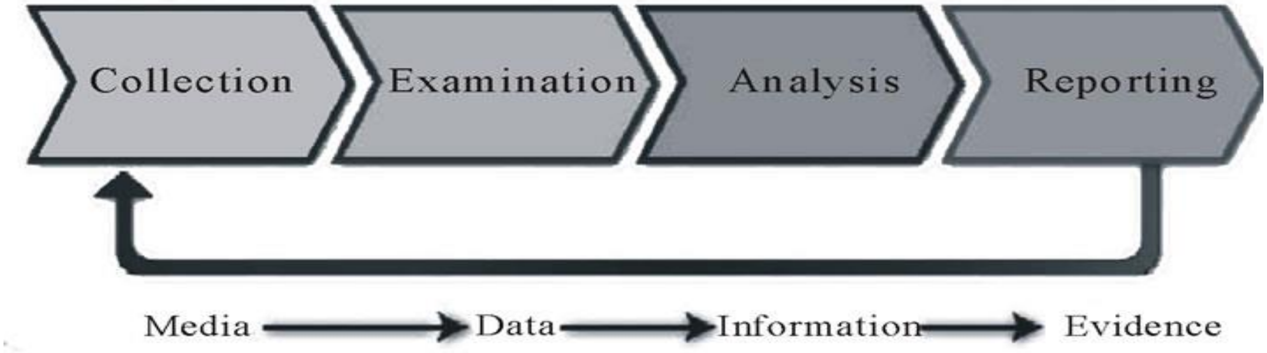
There are countless current mobile forensic models, methodologies and frameworks, some of which have been established for their own use by organizations or law enforcement staff for their own nations and even by other people depending on their background, personal goals or the needs of their employers (Salemat et al, 2008) and (Perumal, 2009). There are some models that concentrate solely on acquiring proof that ignores all other procedures that are critical to investigating forensics. The models to be discussed are some of the most common ones that scholars and professionals have highlighted in the sector and all have beneficial and negative characteristics that will be highlighted in this chapter.

2.8 Existing Mobile phone Forensic Models

2.8.1 Forensic Process Model

In the Digital Crime Scene Investigation,

the United States Department of Justice developed a protocol model: a four-phase guide for the first respondents:-



Collection: involves searching for evidence, identification of facts, collection of evidence and records.

Examination: This is designed to make the proof more apparent and to clarify the origin and meaning of the evidence. It involves revealing information and documentation that is hidden and obscured.

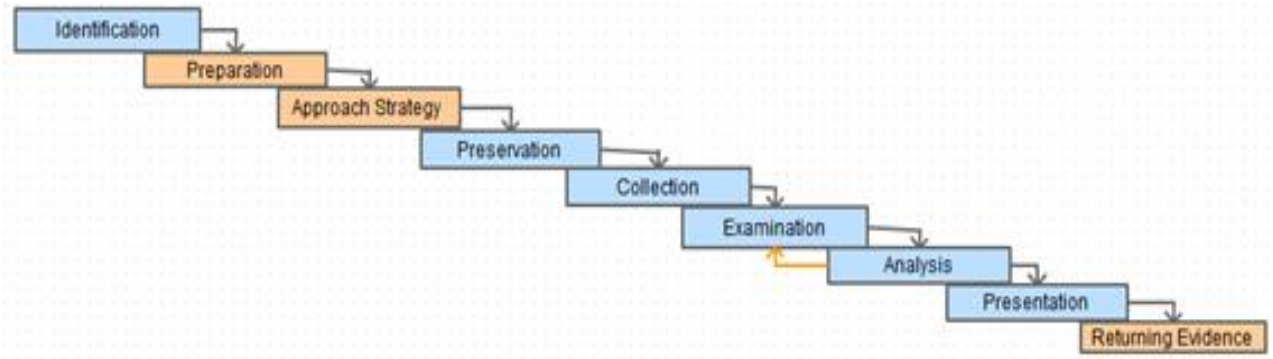
Analysis: The research item looks at its validity and proof for the case.

Reporting: It requires a document detailing the review process and the relevant data gathered from the entire study.

2.8.2 Digital Forensic Research Workshop (DFRWS) Model

At the first Digital Forensic Research Workshop held in Utica, NY in 2001, (Reith, Carr and Gunsch 2002) derived the model, the state of digital forensics was discussed and it was concluded the DFRWS Model was a process with a number of fairly agreed measures.

DFRWS model proposes a standardized forensics process that consists of nine components:

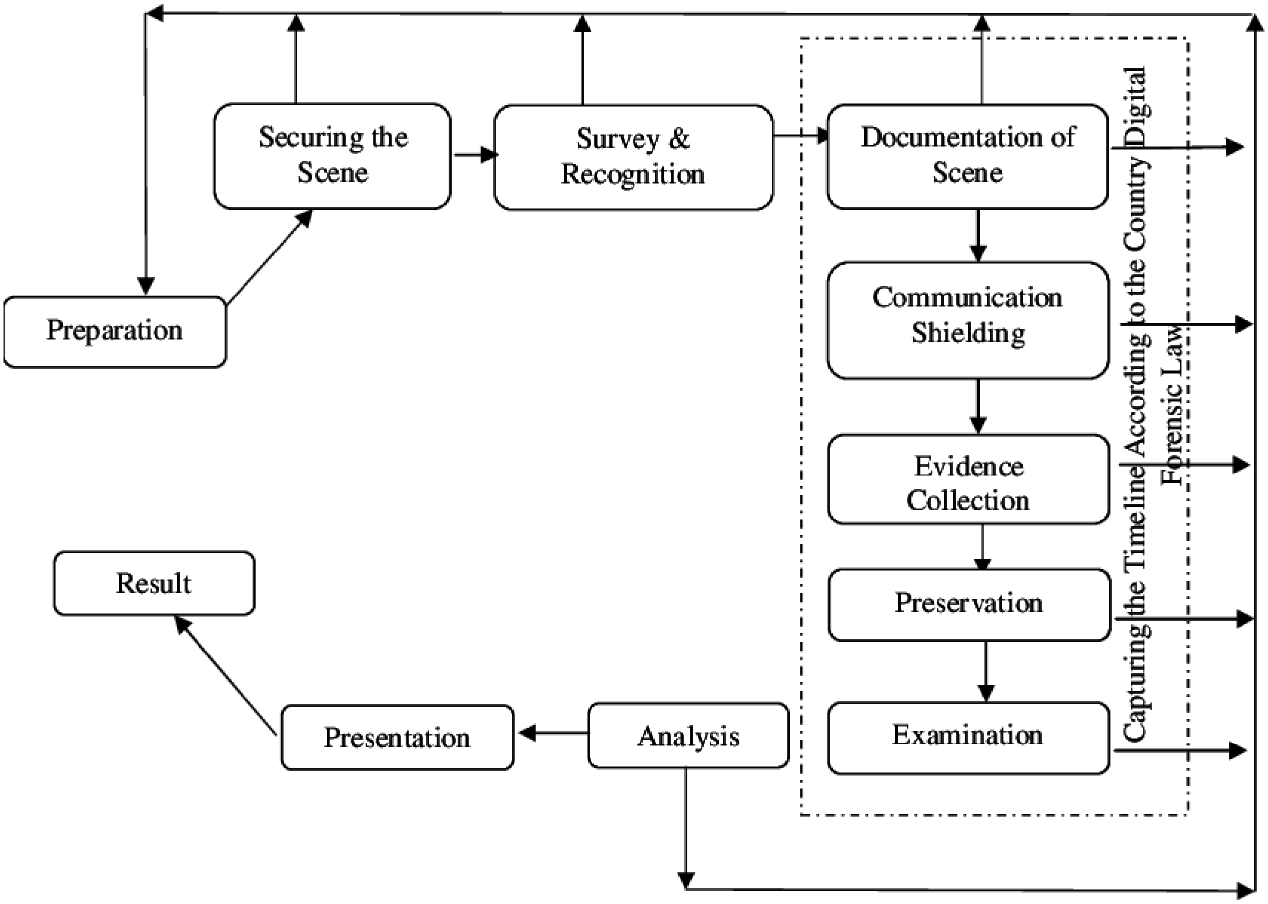


This model is based on concepts drawn from conventional forensic evidence processing techniques (e.g. the FBI).

1. **Identification:** Recognition of an incident indicator and determination of its type.
2. **Preparation:** This includes the preparation of tools, methods, search warrants, and authorizations for supervision and leadership support.
3. **Approach strategy:** develop a procedure to maximize the collection of untapped evidence while minimizing the impact on the victim.
4. **Preservation:** This includes the isolation, protection, and preservation of the state of physical and digital evidence.
5. **Collection:** this involves recording physical scenes using standardized and accepted processes and duplicating digital evidence. Examination: This involves a systematic in-depth search of proof concerning the alleged crime.
6. **Analysis**: This involves the determination of meaning, the reconstruction of information fragments and the drawing of conclusions based on the discovery of evidence.
7. **Presentation:** It provides a summary and clarification of the conclusion.
8. **Returning proof:** Ensures a return to the right owner of the physical and digital property.

2.8.3 Systematic Digital Forensic Investigation Model (SRDFIM)

This model involved the investigation of Cybercrime and Cyber fraud in the form of an eleven-stage model. The Systematic digital forensic investigation model (SRDFIM) has been developed to help forensic practitioners and organizations for setting up appropriate policies and procedures in a systematic manner (Ankit Agarwal et al, 2011).



First Phase: The preparation stage is prepared prior to the actual study. The first awareness of the nature of the crime and activities, and preparation for the collection of materials for packaging sources of evidence.

Second phase: The main objective of securing the scene in this phase is to prevent unauthorized access from the crime scene and to prevent contamination of evidence.

Phase Three: This phase involves an initial survey of the scene evaluators to identify potential evidence sources and to draw up an appropriate search plan.

Phase four: This phase includes proper documentation of a crime scene, as well as video, drawing, and visualization of the criminal scene.

Phase five: Protection of communication is a step before the collection of evidence. All further communication possibilities of the devices should be blocked at this point.

Phase Six: Evidence Collection The collection of evidence for digital or mobile appliances is an important step and a proper procedure or guideline is required.

The list of evidence digital devices can be divided into two categories:

• Volatile Evidence Collection

The majority of evidence for mobile devices will be volatile and present in the ROM.

Volatile evidence collection.

• Non-Volatile Evidence Collection

This stage includes collecting evidence from external storage media supported by these devices,

Including MMC cards, compact flash cards, memory sticks, safe digital (SD) cards,

USB memory sticks, etc.

Phase Seven: This phase is preserved for packaging, transport and storage purposes. Appropriate procedures to ensure that the obtained digital evidence is not changed or lost should be implemented and recorded.

Phase Eight: This phase is examined by forensic experts to look at the contents of the evidence collected and to extract information which is critical for the case to be proved.

Stage Nine: Review In this phase, the investigative team is more engaged in a technical review based on the findings of the evidence test.

Phase Ten: Presentation the results may be presented to a broad audience including legal enforcement officials, technical experts, lawyer experts, and corporate administration after collection and analysis of the evidence collected.

Eleven. The final stage of the design is the assessment phase. Phase Eleven: Test & Assessment all the investigation steps are reviewed and areas of improvement are identified. In order to refine further evidence gathering, evaluation, and analysis of future research, the findings and subsequent interpretations may be used as part of the review process.

2.8.4 Comparison of major forensic models with the Smartphone Forensic Investigation process model.

Smartphone Forensic Investigation Process Model	**Abstract Digital Forensic Model**	**DFRWS Model**	**Systematic Digital Forensic Investigation Model**
Preparation	✓		✓
Securing the scene		✓	✓
Survey and Recognition	✓	✓	✓
Documenting the scene			✓
Mode Selection/ Shielding			
Volatile Evidence Collection			✓
Non-volatile Evidence Collection	✓	✓	✓
Off-Set/ Online Storage			
Cell Site Analysis			
Preservation	✓	✓	✓
Examination Analysis	✓	✓	✓
Presentation	✓	✓	✓
Review			✓

2.9 Mobile Forensic Tools

Mobile forensic tools are the real variables in the digital forensics sector as it is impossible to carry out a Cybercrime or computer crime investigation without them. For the most part, the tools were reliable and yielded results that were used in law courts. Despite the fact that there is no proof that the physician using them provides in-depth data about how the instrument actually operates or the techniques they use to enable them (practitioner) to check the authenticity of the obtained proof.

Practitioners in the field of digital forensics need to be conscious of how the instruments they use in their job as well as methods of verification to ensure that the resulting proof is accurate and meaningful.

Mobile forensic tools are classified based on their position in the process of digital forensics, the particular instrument for which they are designed or a particular operating scheme (Sriram and Raghavan, 2013). The roles include instruments to acquire proof, instruments to examine proof, instruments to analyze proof and embedded instruments. The following is a description of examples given by the various groups of instruments.

2.10 Acquisition tools

Mobile forensics procurement instruments are a kind of tool used to create what is referred to as the suspect device's mirror copy or picture. Usually produced at the moment of purchase, this cryptographic hash is one of the intrinsic actions engaged in keeping the chain of evidence custody. This aspect of the digital inquiry method is very crucial and the ultimate goal here is to maintain the suspicious device's integrity. In turn, it also helps to preserve the integrity of the proof as it preserves the physical evidence from which the digital evidence will be obtained, thus preserving the custody chain. Usually, mobile forensics procurement instruments are used in cooperation with write blockers to guarantee that during the process nothing is written to the drive. Despite all good intentions and intent, it is important to consider that questions will arise about the integrity of the copy being produced. How do you prove that the copy is a complete copy of the original and how do you know that the original and the copy are the same for a fact? For the most part, the response lies in the virtue of the instruments being used as well as the practitioner's integrity.

The work that this study presents deals with these problems, as it discusses the ethical principles and presents t he full chapter on ethics.

2.10.1 Cellebrite Physical Analyzer

Cellebrite UFED Touch ® has been used as one of the leading forensic mobile telephone devices for these studies. The UFED Touch ® is a Cellebrite mobile variant that can be examined. The graphic user interface (GUI) is simple to use and informs an individual how to operate it correctly. It describes how to use a write block cord on a particular phone and where to place it, together with where to connect a receiving place device. Three kinds of extractions are possible: physical, file system and logical. The UFED Touch ® also allows you to capture phone pictures and display shots. Each phone has various extractions and artifacts that can be imaged. Each phone is different. Upon the UFED Touch, ® phone is acknowledged or opened manually, a list of activities can be displayed. From then on, the help in the imaging phase will be guided. The UFED Touch of Cellebrite was combined with the Physical Analyzer of Cellebrite (2018), which was also available in German. The software was both used to extract the information from the phones and to view the contents when they were extracted.

2.10.2 T Analyzer (Autopsy)

T is the name we have provided an Official Use Only or FOUO portable forensics tool. T is an Autopsy version with some other characteristics. "Autopsy is a digital forensic platform and graphical interface to The Sleuth Kit and other digital forensic instruments. The Sluithkit tool is examined by law enforcement authorities, army, and corporate examiners."

2.11 Examination and Analysis Tools

The exam and analysis instruments are occasionally rolling into one instrument. You can collect, search, browse, examine and analyze information together with reporting or two or more of these procedures. These instruments are generally created for particular devices or interfaces. For example, Encase (Guidance), Oxygen, FTK (access data); T-tool and Cellebrites Physical Analyzer (CPA) are the instruments incorporated. Examples of these are embedded instruments. For the imaging and review of the current analysis process, the respective tools will be compared and evaluated at various levels in the acquisition, examination, and analysis of the smartphone Forensics process. Analytic Platforms: T, oxygen suite, Cellebrites Physical analyzer (CPA). In the research, we will discuss the benefits and constraints of all levels. These instruments are used for digital proof extraction and analysis. Extraction can be physical or logical of two kinds. Physically, physically extraction being the recovery of data all across the entire drive regardless of the type of file system while logical extraction recovers files based on the devices operating and file systems as well as its application.

2.12 Evaluation of Mobile forensic tools

Most of them are effective and common when it comes to precise digital evidence acquisition, investigation, and evaluation. There are many portable forensic techniques and the associated instruments to counter mobile forensic investigation. The effectiveness of any digital instrument relies on how much the digital forensic investigation and assessment contributes to every step. Different tool-kits have been created which contain instruments to help digital researchers in their efforts to improve the effectiveness of portable research.

The present aim of the analysis platform – the T tool Oxygen Suite and Cellebrites Physical analyzer (CP

A) are used both for imaging and analysis, as they are used for the comparison and assessment of their results. The analysis platform also provides the results of multiple forensic smartphones
Systems.

2.12.0 Encase

EnCase is a toolkit for commercial forensic investigations used mainly by law enforcement authorities. Accorder information can be obtained forensically by other common forensic business assessment instruments, according to Nelson et al (2004), in which the information can be analyzed. The software can handle a huge quantity of digital evidence and, where needed, transfer files directly to legal officers. It allows lawyers to readily review the proof and also to prepare rapid reports. EnCase has launched digital research graphical user interface instruments. EnCase is a toolkit for commercial forensic investigations used mainly by law enforcement authorities. Accorder information can be obtained forensically by other common forensic business assessment instruments, according to Nelson et al (2004), in which the information can be analyzed. The software can handle a huge quantity of digital evidence and, where needed, transfer files directly to legal officers. It allows lawyers to readily review the proof and also to prepare rapid reports. EnCase has launched digital research graphical user interface instruments. It is important to know that after creation, EnCase cannot write to the proof file. Just like in other documents, with a disk-editing utility, it is feasible to change the EnCase proof file. However, if one bit of information on the collected evidence bit-stream picture is modified after the purchase, Encase will report a verification mistake in the document and recognize the place of the registered mistake.

2.12.1 Oxygen Forensic Suite.

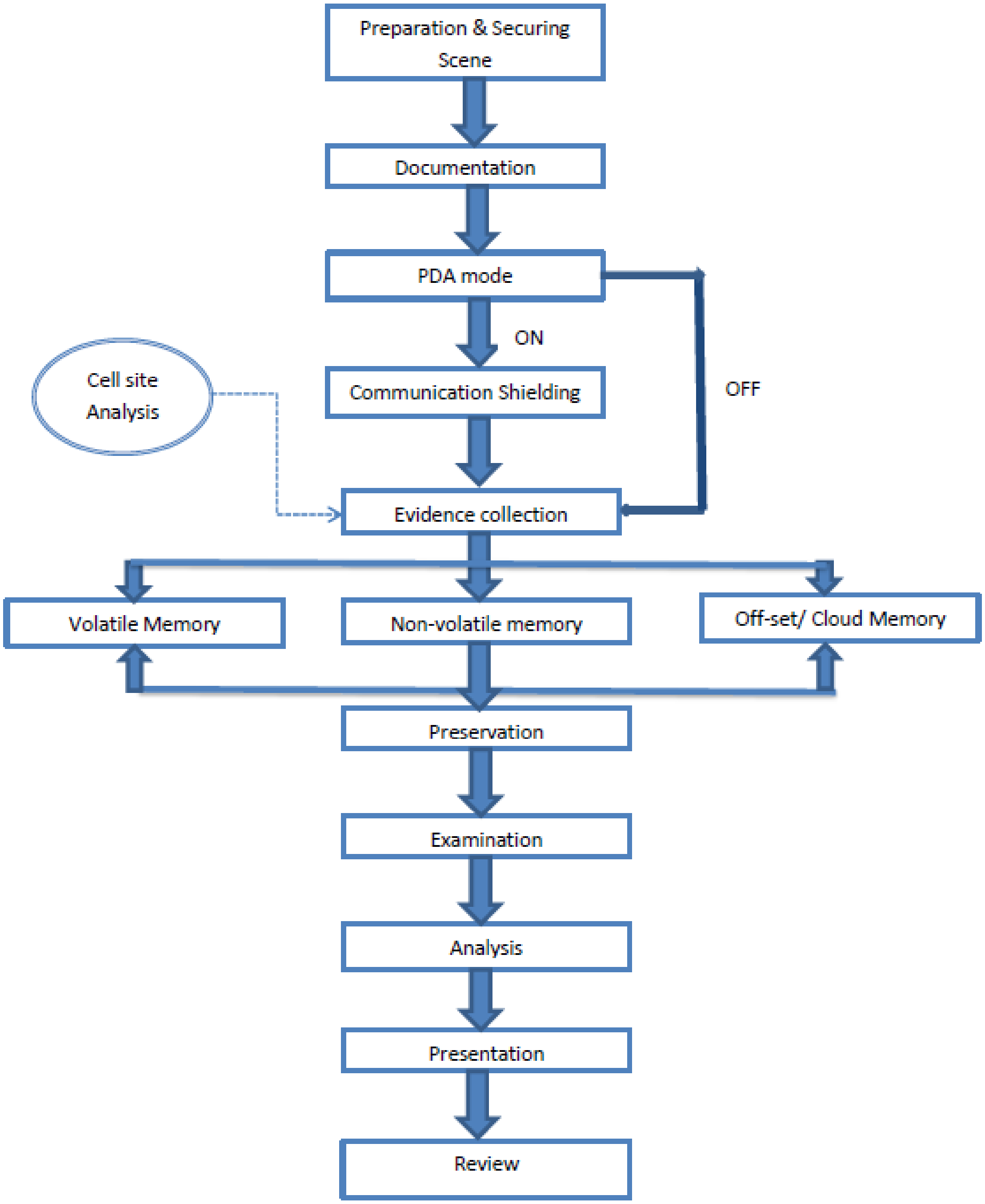
This instrument is the preferred forensic mobile instrument in Europe. Oxygen forensic suite is a digital forensic software. Software. This instrument can be used in cellphones, smartphones, and tablet data extraction and analysis. It utilizes sophisticated proprietary protocols that enable more information from smartphones than extracted using logical forensic instruments. The oxygen forensics instrument provides timeline assessment, social graphic representation, and geographical location as well as Nokia phones information. Not many other instruments can do so, so they are outstanding.

2.12.2 Mobilyze

Mobilyze is a black bag technologies product which is a mobile acquisition tool designed to give users immediate access to data from iOS and Android™ devices. The Mobilyze application runs on either Mac or Windows and can be effectively deployed in the field or within a forensics lab. Once Mobilyze has been installed, simply plug the smartphone or tablet into an associated USB port, and Mobilyze will begin collecting all relevant user data. The data is available for viewing, searching, and filtering within minutes. A user can even detach a device while data is being collected without losing the acquired data. Items of interest can be tagged in Mobilyze cases, and professional, customizable reports can be generated within seconds. Through its incredibly simple and intuitive user experience, Mobilyze allows users of all technical abilities to quickly ascertain whether a device contains relevant forensic evidence, whether immediate action needs to be taken, and/or whether the device needs to be sent to a forensics lab for a comprehensive analysis. Once the relevant data is discovered, Mobilyze provides users one-click reporting in a clean and easily readable format.

2.13 The Conceptual Mobile phone Forensics Model

Smartphone Forensic Investigation Process Model According to Goel et al. (2012), this model consists of the following subsequent steps:



Smartphone forensic investigation process model Goel et al. (2012).

Phase 1: Preparation of 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 is done at this stage.

Phase 2: Securing the scene involves preventing contamination of evidence and ensuring the security of the scene of the 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. The 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 Active mode: When the device is running, it has to first be shielded from the network and no communication should be done with it to avoid volatile evidence contamination. **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.

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 involves the 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 smartphone.

Phase 9: Cell-site Analysis this deals with establishing specific positions where the mobile phone has been or where it is currently. It gives a 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 the crime.

Phase 10: Preservation This step involves packaging, transportation, and storage of evidence. Once evidence is identified and labeled, it is packaged in a 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, a proper chain of custody must be maintained and unauthorized people should not gain access to the evidence.

Phase 11: Examination this involves filtering, validating, matching patterns and searching for specific keywords about the nature of the crime. Items such as address books, appointments, calendars, schedulers, text messages and voice messages, documents and emails are examined in detail. Evidence is also sought for system tampering, data concealing or deleting utilities and unauthorized system modifications. Recovery of hidden or obscured information is a time-consuming but critical exercise that should be carried out. Volatile and non-volatile evidence is analyzed at this stage and backups are taken. Everything has been done and the person doing it has to be documented. Hashing functions should be used for mathematical purposes authentication of the data.

Phase 12: Analysis of this phase involves analyzing hidden data, determining the significance of information collected, reconstructing the event data and arriving at proper conclusions. The analysis should be done in a manner to ensure that the 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, a 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 improvement are reviewed. The results of the investigation can be used together with their interpretations to guide similar exercises in the future. It should be noted that iteration is usually repeated several times 14 between examination and analysis to get a clear picture of the incident. This can be applied in the future to establish better procedures and policies.

2.14 Challenges of mobile phone Forensics

2.14.1 Selection of the appropriate toolkit

The biggest challenge in mobile forensics is to know which tool is the best in different situations, and which tool ensures the extraction of the most data possible. There are a lot of tools in the mobile forensics market, but the one that suits the investigation best is sometimes very hard to find. There is in fact not a single tool that meets all the needs of an investigator, so the perfect mix of the various mobile forensics toolboxes is very important to use.

Another legal challenge is that data cannot be accessed, stored and synchronized across multiple devices when it comes to the mobile platform. Due to the volatility of data and the remote transformation or deletion of data, more effort is required to maintain this information.

2.14.2 Extraction of all relevant data

Data extraction from all relevant Apps may be difficult, particularly on Android phones. Acquiring physical removal is increasingly difficult and for many devices on the market at the moment is not feasible. Therefore, the use of an Android backup was the safest way to extract information from those devices. The device producers can, however, choose to remove their app information from Android backups or to encrypt their app servers. So additional steps have to be taken to secure those kinds of data. For iPhones, the main extraction method is a device backup too also some data not included in those backups (e.g. emails or frequent locations) and has to be acquired with additional steps T3K Forensics (2018).

2.15 Justification of the study

This research will evaluate and compare the performance of various Smartphone forensic tools across various cases and scenarios concerning the Association of Chief Police officers (ACPO) good practice guidelines (2012).

In assisting forensic researchers to determine adequate instruments to carry out smartphone forensic examination, the study contributes significantly to the existing literature. The assessment can save time through the selection of the correct tool in the investigation and thus eliminate the necessity for repeated tests to gain evidence. The methods used must be known and the extent of interference should be understood so as to prevent potential evidence from being contaminated.

It may also be useful for people who may mistakenly need to recover deleted data.

CHAPTER THREE

RESEARCH DESIGN AND METHODOLOGY

Mobile forensics is the mobile phone testing method of finding and collecting evidence for the crime. The process used to conduct research is explained in this section. It offers a description of the research design, method of gathering data, techniques, and methods for smartphone imaging. The main focus of the approach is to analyze the internal, external memory and SIM card for mobile telephones and test them using the proposed methods.

3.0 Research Philosophy

The research philosophy and importance of a research philosophy should be understood by researchers, which is characterized as knowledge creation and knowledge nature (Saunders, Lewis & Thornhill, 2009). Epistemology, ontology, and methods are part of the research theory. Research philosophies can be grouped in Positivism, Realism, Interpretation, and Pragmatism following the suggestions of research onions.

3.1 Positivism

The theory of objectivism is positivism where an investigator is independent of the research subject and influences it (Remenyi, 1998). (Positivism, 1998) Positivism is employed to describe a research approach on the premise that the data collection and analysis to establish truths can be discovered by data collection (Somekh & Lewín, 2005). "Positivist studies are based on a prior fixed the relationship between phenomena usually explored by organized instruments. These research mainly test theory to improve predictive phenomenon comprehension "(Baroudi & Orlikowski, 1990:5). Positivism is generally aimed at discovering the social phenomena by starting from a series of assumptions. Usually, this form of theory uses experiments, calculation methods, and evaluation. The result is causal (Easterby-Smith et al., 2006). Quantitative analysis and a deductive approach usually apply to a positivist theory (Saunders et al., 2009). The research is based on the philosophy of positivism based on existing pieces of literature, and studies in the area of mobile forensics explaining major issues related to smartphone forensics and evidence acquired. Neo positivism and post severity are other philosophies based on positivists on mobile devices. The research hypothesis is developed from theory and the secondary data collected will be used to test and analyses the hypothesis.

3.2 Research Design

The different types of research methods are usually linked to various philosophies of science.

The two main methods are inference and deduction. A deduction is mainly linked to positive and interpretative induction. This deduction approach involves the development of theory and a research strategy that tested some hypotheses and examined the relationship between the causal-comparative layouts of variables (Saunders et.al 2012). This research is deductive and follows the process of deduction. The data is collected and evaluated to determine the relationships between variables based on the foundation of existing theory and literature in the digital forensics field.

In terms of smartphone forensics, the overall concept is mobile forensics, characterized by the use of techniques closely related to the mining of mobile digital data (Mumba E. R et al, 2014), which is mobile digital data. This study deals with data collection from smartphones using the Open Source Autopsy (Sleuth Kit) Tool and the patented Oxygen Forensic Suite program. Three specific extractions can be performed: physical, file system and logical by Cellebrite. Physical extraction takes all data from the unallocated / deleted space, including data.

The extraction of a filesystem is like physical extraction, but it does not check unassigned / deleted spa ce even when extracting secret files. The logical abstraction is basically what the client sees when the u ses the device. In this type of research, experimental research methodology was also applied. A qualitative type of research was followed in this study. The aim was to collect the images from Smartphones using Oxygen Forensic Suite and Cellebrites Physical analyzer (CPA) software and analyze data using additional tools namely: Analysis platform Autopsy (Sleuth kit) tool. "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, 2014).

The choice of this research design is informed by the fact that it provided an accurate description of the tools. It also assisted in attaining the second and the third objectives of the study, that is, to test the performance and effectiveness of each tool using the adopted model.

3.3 Target population

Digital forensics Investigation is a new phenomenon, the sample size is relatively small and 10 institutions were sampled and only 8 out of 10 gave their responses.

3.4 Sampling frames and techniques

Purposive sampling was employed in this research. According to Kombo and Tromp (2015), purposive sampling enables a researcher to select information-rich cases for in-depth analysis related to the central issues being studied. In this case, purposive sampling was applied to institutions that offer mobile forensics.

The research required input from respondents who use mobile forensic tools and in particular tools that support smartphone imaging and analysis.

3.4.1 Data Acquiring Techniques

There are two main physical and theoretical approaches to mobile extraction. A physical replacement is a portion of the memory copy. This contains a flash memory that allows access to missing or deleted data and files. Corporation Cellebrite (2016). Logical extraction is more of a data request than a bit-by-bit copy. The API of the app is used for interaction and live and viewable information can be requested on the computer. The machine responds and transmits information over a network. There are much fewer data to gather for Cellebrite Corporation (2016). There is a much faster logical extraction. Some devices did not permit physical exhaust, so we decided to make a logical extraction for those devices. Physical extractions were carried out for this study

3.5 Data Collection

Mobile data often appears in the phone's internal memory on a number of mobile devices. It includes contacts, SMS, saved the audio recording, photos, inbound and number logs, calendar and events, settings (languages, hours, tones and volumes, GPRS, WAPs, and the Internet), Bluetooth content and IMEI. Many mobile data that often reside in SIM memory, on the other hand, include text messages, Identification and call logs of a service provider, touch, IMSI and the Integrated Circuit Card ID (ICCID). In this research deleted text messages, text messages on the smart-phone, call logs, Documents and Internet logs were retrieve from the SIM memory, Phone memory, and External memory.

Data are collected from five different smartphones with the assumption that this was the most used phones in Kenya, using three imaging tools and the tools are subjected to the same test environment then analyzed by the same tools, This form primary data source. Secondary data will include a literature survey of internet sources, frameworks, methodologies, models, past research projects, reports as well as books.

According to Douglas and Montgomery (1997), it is important to follow the data collection protocol exactly as data are collected. Before the collection of data, all the tools were checked to ensure that they are valid, reliable, and calibrated.

This study utilized both primary and secondary data sources. The primary sources are interviews, more specifically expert review. The results collected from different tools subjected to the same test environment. This formed the primary data source. Secondary data included a literature survey of internet sources, frameworks, methodologies, models, past research projects and reports as well as books. Data collection plan considered how four important variables: background, constant, Uncontrollable and primary, fitted into the study. Inconclusive results are likely if any of these classifications are not adequately defined. It is important to consider.

3.6 Collection Procedure

3.6.1 Level 1 Data Collection Procedure

3.6.2 Questionnaire

According to Mugenda (2008), the purpose of a tool or research instrument is to measure the variables of the study. The researchers used questionnaires and interviews for data collection. The questionnaire had both closed-ended and opened ended variables.

3.6.3 Level 2 Data collection Procedure

The second part of data collections involved testing mobile phone forensics tools in an unbiased environment. The comparative analysis cannot yield satisfactory results if global variables we allowed to manipulate. This was done in a constant environment. The phones were put into airplane mode, not connected to the Wi-Fi, the display was put onto the longest time possible, and developer options were made available (when applicable) and stay awake and USB debugging was turned on.

3.7 The Test Environment

The test environment consists of the following:-

High powerful Computer with 16GB RAM, 1 TB storage with Oxygen Suite, Autopsy 3.4.0, and Celebrate Touch installed.

3.7.1 Images Source Drive

These are previous images which have been used to carry out Mobile forensics by other mobile forensics researcher and will be a user across all tools as a secondary data source.

3.7.2 Test Parameters

Some of the parameters to be tested while evaluating digital forensics tools are Accuracy, the depth of artifacts extraction and Analysis.

3.7.3 Test Processes

This is the most critical stage in this research. Any interference by a global environment shall render the results inaccurate and irrelevant. At this point, every mobile forensic tool shall be run in a controlled environment. It is important to note that no interruption is accepted at this stage.

The forensics computer was loaded with four mobile phone forensics tools namely: Cellebrite UFED, Oxygen Suite, Autopsy 3.4.0 and Axiom Magnet, each forensics image was loaded and analyzed using the four tools.

3.8 Data Capture

The accuracy of the results of an experiment is highly dependent on the accuracy of the data captured. Although observation for critical changes is acceptable in scientific experimental research, the mobile forensics experiment is unique. Its uniqueness is brought by the fact that all forensic tools are built with their timers and a summary of their processing evidence.

3.9 Data Analysis

During the data analysis process, the Shannon index (H') methodology is used. Shannon analysis requires data review, transmission, are used to identify systematic relationships between specific attributes and variables, It also enables data to reveal their underlying structure. Gaussian distribution

of the curve was used to determine the proportion and determinant of the artifacts where p=0.05. Here are the main reasons for using the Shannon index (H') method; the identification of data changes, hypotheses for tests, provisional models of the corresponding models and the relations between the variables. During analysis an Examination is done using the three tools namely Analysis platform –T tool (Autopsy) and Cellebrites Physical analyzer (CPA) software and specialist tool Oxygen, to aid with a viewing, recovering data and recording of variable parameter then comparison and contrast of the output of each tool are drawn. Different types of methods are used to retrieve proof that usually involves some kind of keyword search within a picture archive, either finding matches with the phrases in question or searching the types of known data. Most files (such as visual images) have a sequence of bytes that can mark the start and end of a file when a deleted file is identified. Many forensic software use hash signatures to identify remarkably or exclude (benign) detected files and have hacked the data obtained and compared lists such as the National Computer Reference Library Reference Data Set (RDS).

CHAPTER 4

RESULTS

4.0 Introduction

In each part of our daily life, smartphones have penetrated from directions, sending photos or emailing. Most people use their smartphones for previous activities, but people use their smartphones for unpleasant purposes (Marcie 2017).

In this section, we compared the mobile device analysis with Cellebrite UFED, Oxygen Suite and Autopsy, and looked for content differences based on the tools ' results. We wanted to know whether a tool subsequently reported more or less information about these specific types of files and summarize the results of mobile forensics tools ' performance. After gathering, the results from both tools were compared and the differences were measured.

4.2 Return Questionnaire

A tested and approved questionnaire was provided to respondents and below are the status of the filled questionnaires.

Respondents were required to provide feedback on how many Forensic Experts do they have in their organization. Most of the organizations had between 1 to 10 Forensics Experts doing both digital and Mobile Forensics.

Respondents were required to provide feedback on what are the core Activity of the Organization. The results below show that the core Activities of the Organizations sampled.

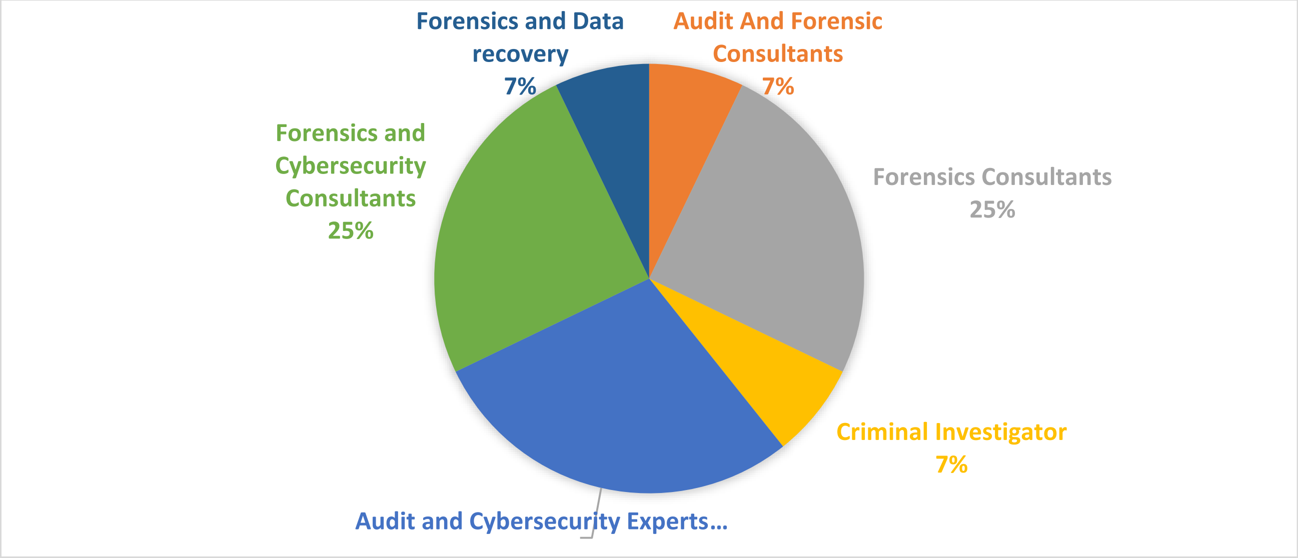


Chart 1.0

Chart 1.0 1

Forensic Consultancy (25%), Audit and Cybersecurity Experts (29%), Forensics and Cybersecurity Consultancy (25%), were the core activities carried out by most organizations, above chart shows the percentages of all the activities carried out by the Forensic Organizations.

Respondents were required to provide feedback on what are the major forensics cases their organization handled and out of the eight organizations sampled, all of the organization handles hard drive formatted cases and Retrieval of Information.

what are the major forensics cases your organization has ever handled

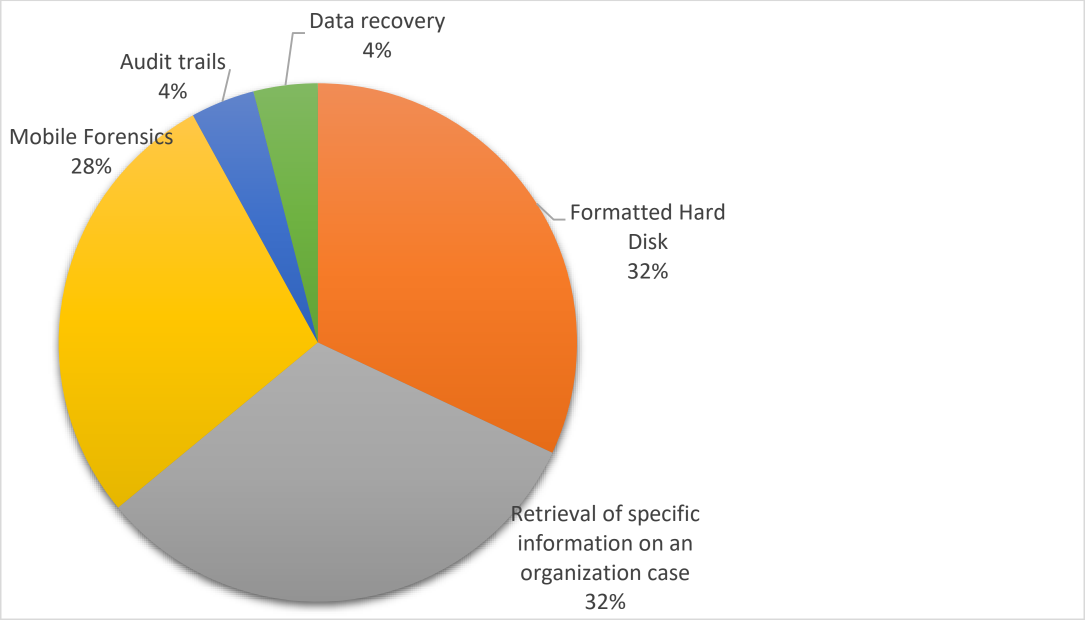


Chart 1.0 2

(32%) of the organizations handles hard drive formatted cases and Retrieval of Information followed by (28%) of the organizations handled mobile phone forensics and (4%) handles Data recovery and Audit trails.

Respondents were required to provide feedback on what are some of the limitations the organization face during forensic investigations. The results show that it is expensive to carry out a digital investigation (20%), Variety of tools to Accommodate (20%), Cost of mobile phone forensic tools (20%) and lack of common tools to carry out digital forensics (18%) on different devices are the major limitation most organization face during forensic investigations

what are some of the limitations your Organization face during forensics

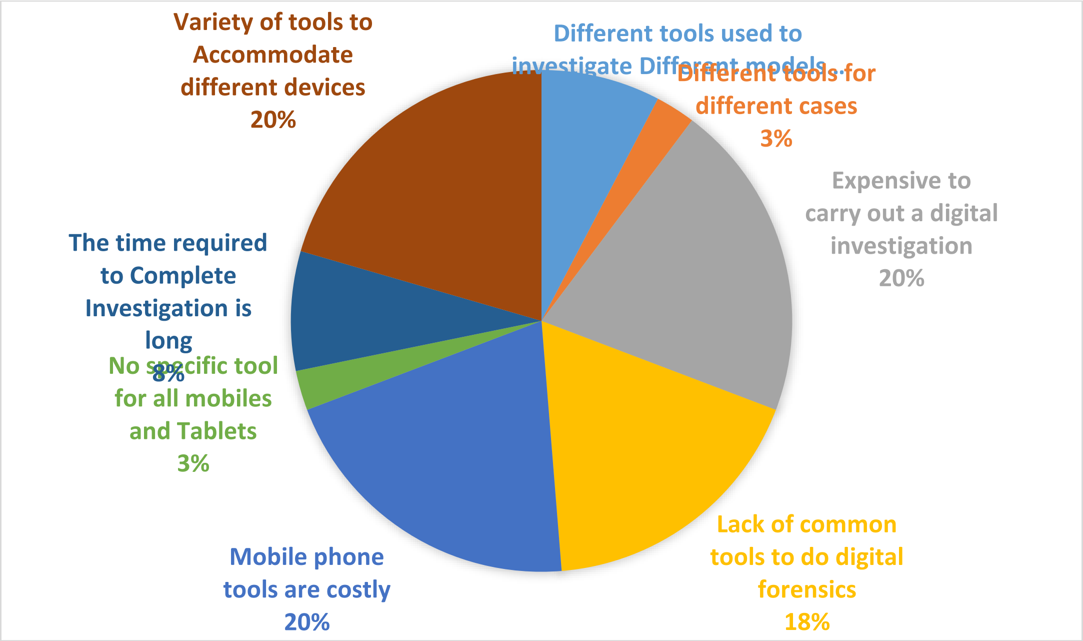


Chart 1.0 3

Respondents were required to provide feedback on what are some of the main tools used to carry out digital forensics in there Organization. The results are shown in the tables below:

What are the main tools used by your organization to carry out digital Forensics

FTK, Open source were the major tools used by the forensics Expert and this is because FTK has a free version.

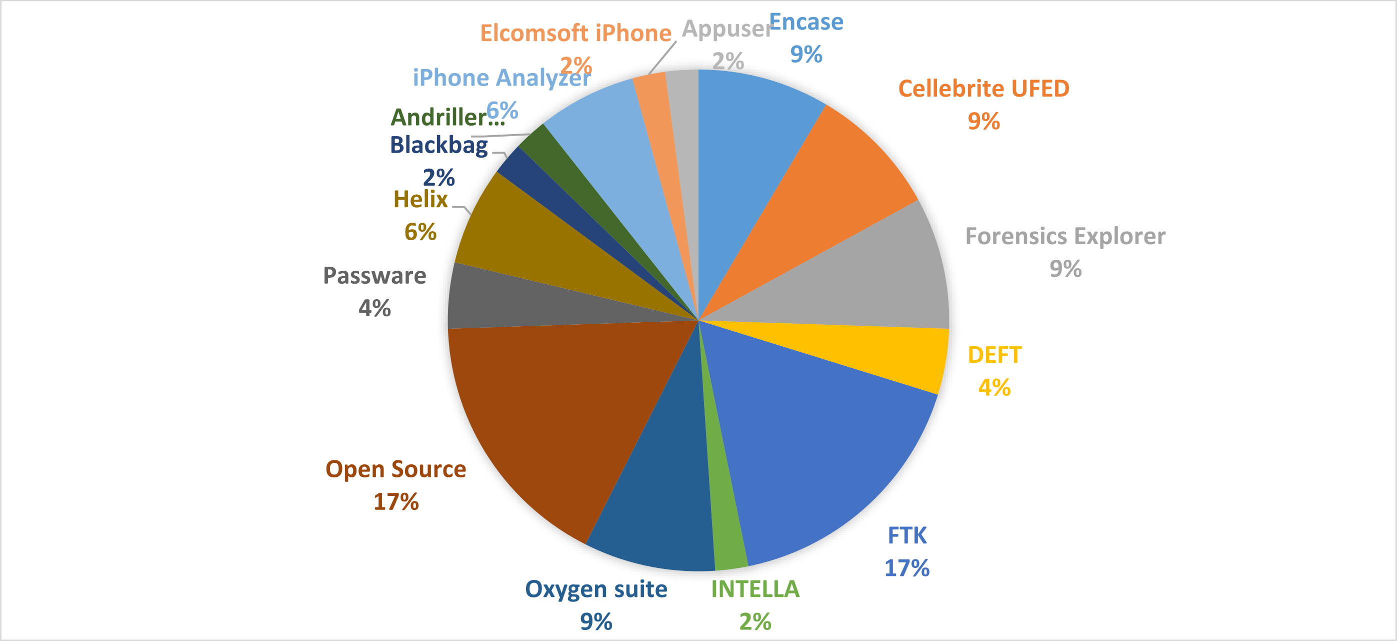


Chart 1.0 4

Respondents were required to provide feedback on how effective the digital forensic tools are and the results show that the tools are effective with 62% believes the tools are excellent while 38% responded that the tools are good.

How Effective are the digital forensic tools

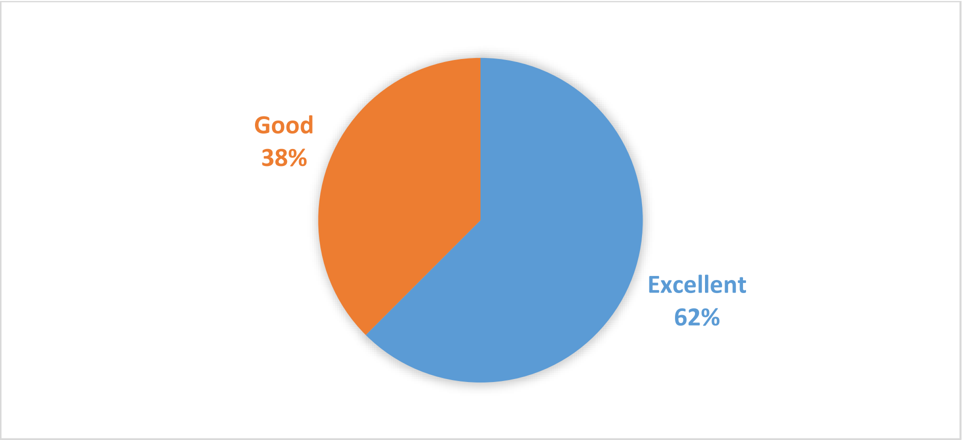


Chart 1.0 5

Respondents were required to provide feedback on whether they use the same tools for imaging and analysis. The results show that 25% say they use the same tools, 25% said they don't use the same tools and 50% say they use the same tools in some cases.

Do your Organization use the same tools for imaging and analysis

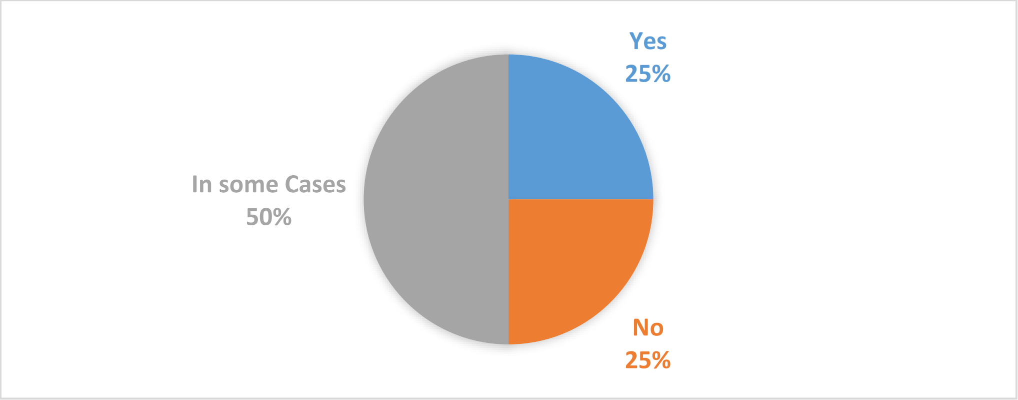


Chart 1.5

Respondents were required to provide feedback on what the cost of forensics tools have on the operation of the Organization. The results show that All the Organizations stated that the high cost of Forensic tools as a greater effect on the operations of the Organization.

Does the cost of Digital forensics tools affect the operation of your Organization?

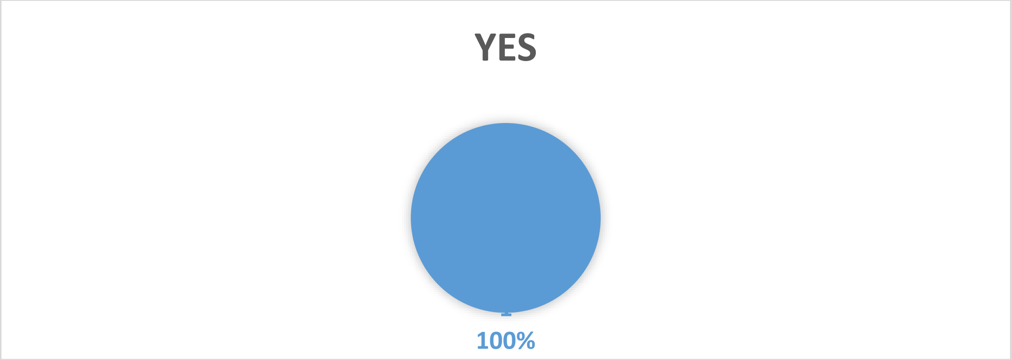


Chart 1.0 6

Respondents were required to provide feedback on what are the Tools used to Image mobile phones during the investigation. The results show that 50% of the organizations sampled use Celebrate UFED Software while the other 50% uses other forensics tools.

What are the tools used to image mobile phones during investigation?

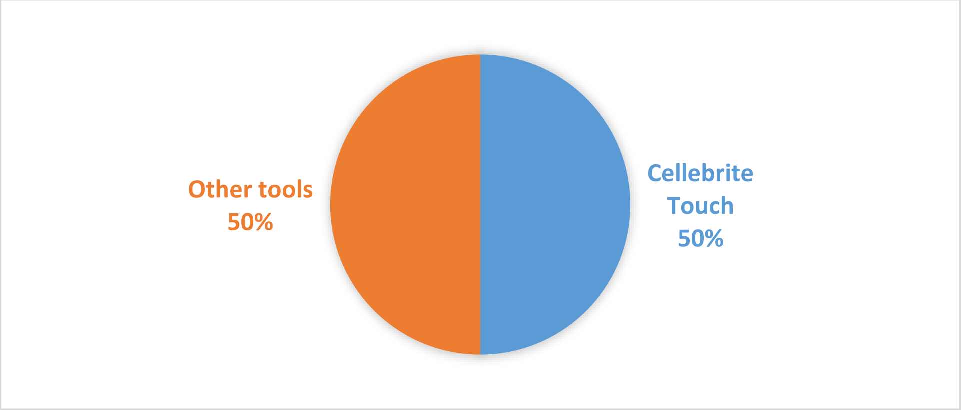


Chart 1.0 7

Respondents were required to provide feedback on whether the organization does mobile forensics. The results show that all the sampled organization does mobile forensics.

Do your Organization handle mobile forensics?

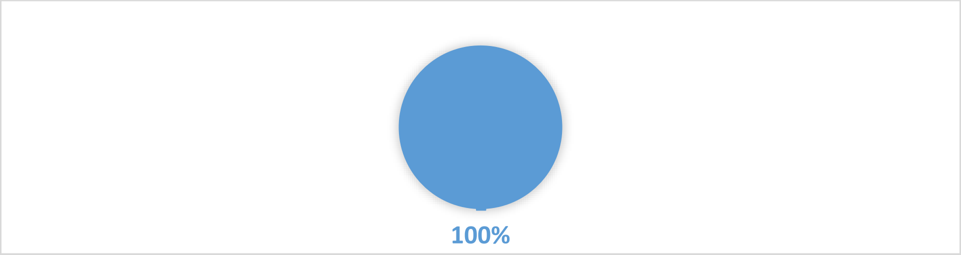


Chart 1.0 8

Respondents were required to provide feedback on the effectiveness of the forensic tools used by the organization to handle mobile phone cases. The results show that 62% of the organizations said tools used are Excellent and 38% say the tools are good.

How effective are the tools provided by the Organization when handling mobile phone cases?

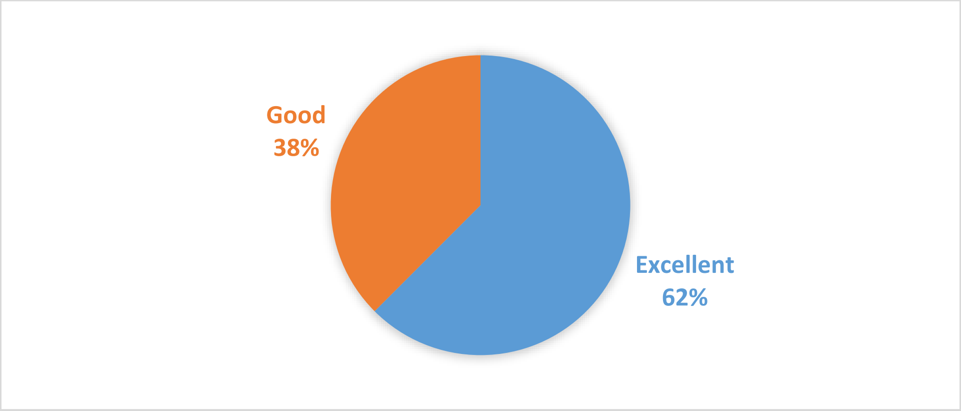


Chart 1.0 9

Respondents were required to provide feedback on the tools used to image phones during an investigation. The results show that 22% uses the iPhone Analyzer 18% of the organizations use Cellibrite UFED,17% Oxygen Suite, 13% uses MOBILedit and XRY,9% uses Andriller and 4% uses Elcomsoft and Mobilyzer.

What are the tools used for the analysis of mobile phones during investigation?

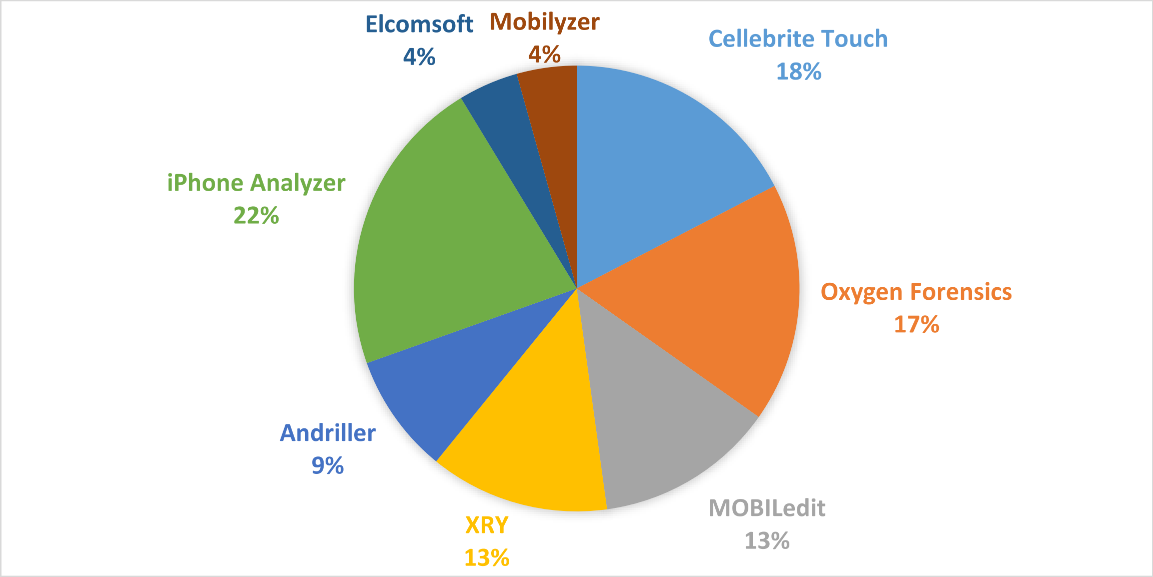


Chart 1.0 10

Respondents were required to provide feedback on the number of tools used to investigate mobile phone cases. The results show that 25% of the investigators use a single tool, 37% use at least 2 tools and the other 38% use At least 3 tools.

How many tools are used to investigate each mobile phone case?

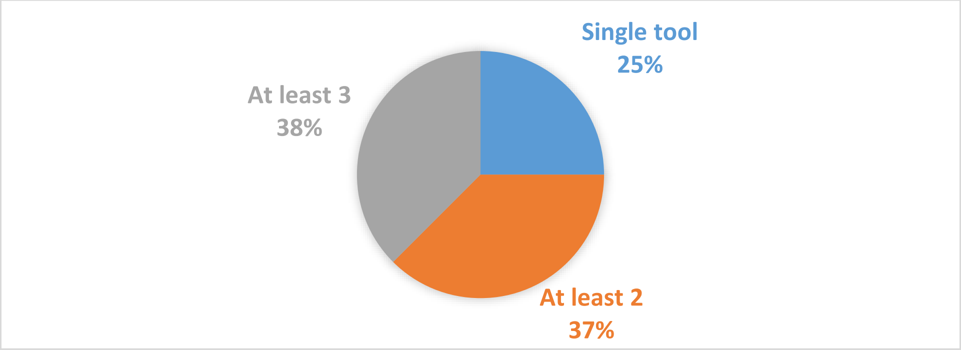


Chart 1.0 11

Respondents were required to provide feedback on whether the organization use licensed or Open source forensics tool, 87% of the respondents' uses the open-source and 13% use open source in some cases.

Do your Organization Use Open Source forensics tools?

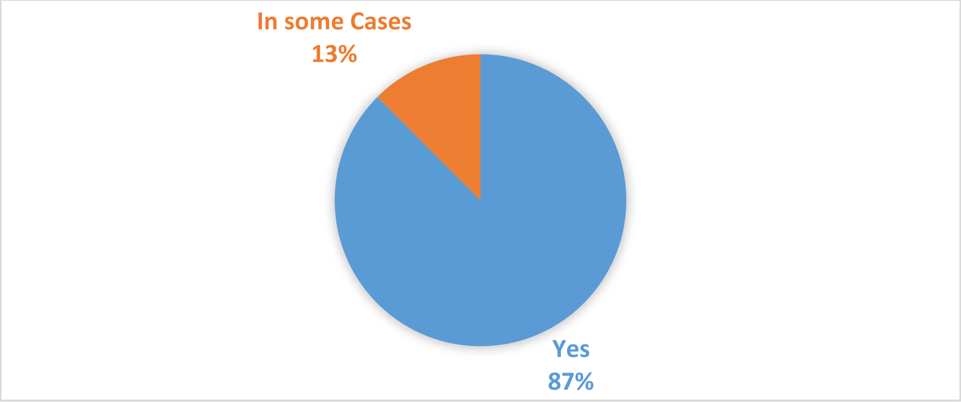


Chart 1.0 12

Respondents were required to provide feedback on how effective are the Open source tools compared to licensed forensics tools. Results show that 50% of the organizations believe they are good while the other 50% believe the results of the Investigations are Acceptable.

If you Use open source forensics tools, how effective are they compared to licensed forensics tools?

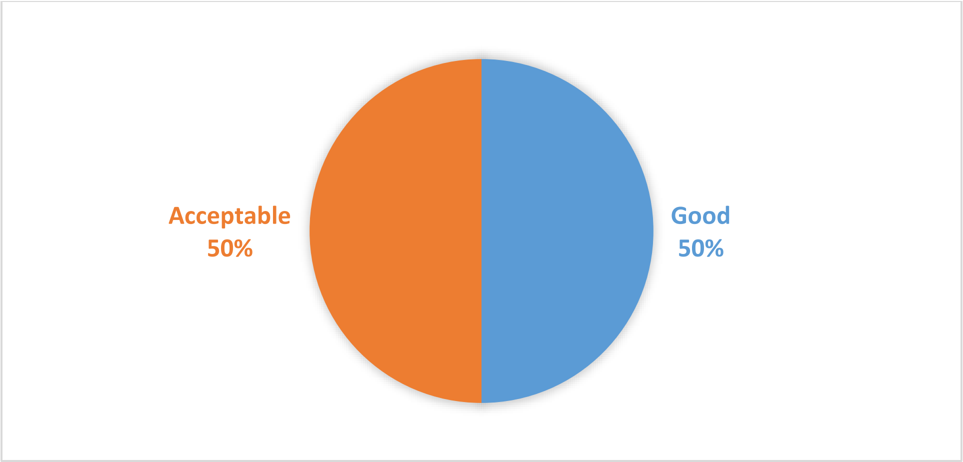


Chart 1.0 13

Respondents were required to provide feedback on how long it takes to investigate a case. The result shows that 50% of the investigator takes 2 to 4 days while 50% takes 4 days and above.

How long does it take to investigate a given mobile phone case?

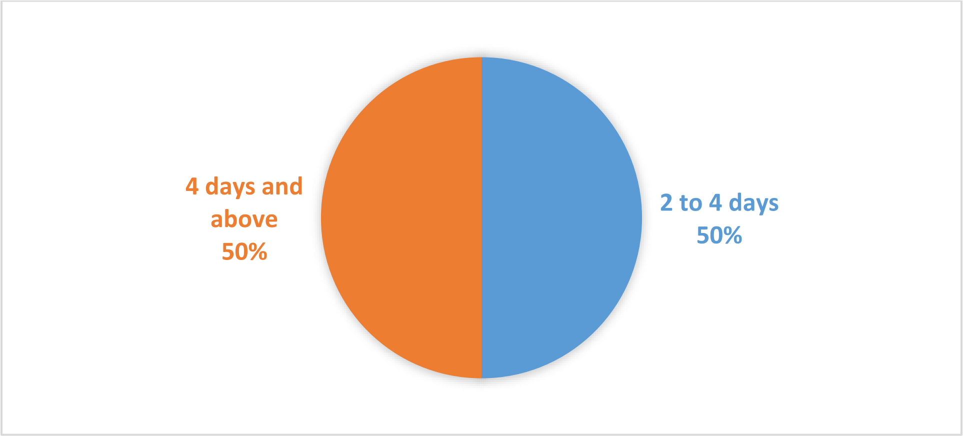


Chart 1.0 14

4.3 Phone Corpus

The research data set consisted of five different smartphones used in Kenya today. The real Data set was imaged using an Oxygen forensic suite and Cellebrite phone detective (UFED).

Five of those smartphones were iPhones, Samsung, HTC, Techno, and Infinix. The table below shows the details of the phones that were imaged.

Phone ID	Vender	Name	Model	Extraction Type	OS	Version
001	Apple	iPhone	6	Physical	iOS	5
002	HTC	Desire	D626	Physical	Android	4.4.2
003	Samsung	Galaxy	S6	Physical	Android	5.2.0
004	Infinix		X601	Physical	Android	7.0
005	Techno	Camon CX	CX air	Physical	Android	7.0

Table 1 Phones used for the study.

4.4 Mobile Imagine Inspection and Content

All device Images were analyzed using Autopsy (Sleuth) tool for mobile, Cellebrite's Physical Analyzer as well as Oxygen. We compared and contrasted the outputs of each tool. We focused on E-mail, Call logs, Photos, Contacts, Web history, WhatsApp messages, and Text messages.

4.5 Initial Phone Extraction

The Oxygen and Cellebrite Touch were used to render mobile forensic pictures and to stay awake with a USB debugging. A physical removal was performed on each mobile by Cellebrite Touch, Oxygen and Autopsy. If a physical removal for a mobile phone was not usable, a file system and/or logical removal was performed. Physical extractions have been favored as most information from a device is available compared to the theoretical extraction or a file system. Extracts were saved for later analysis on an external hard drive.

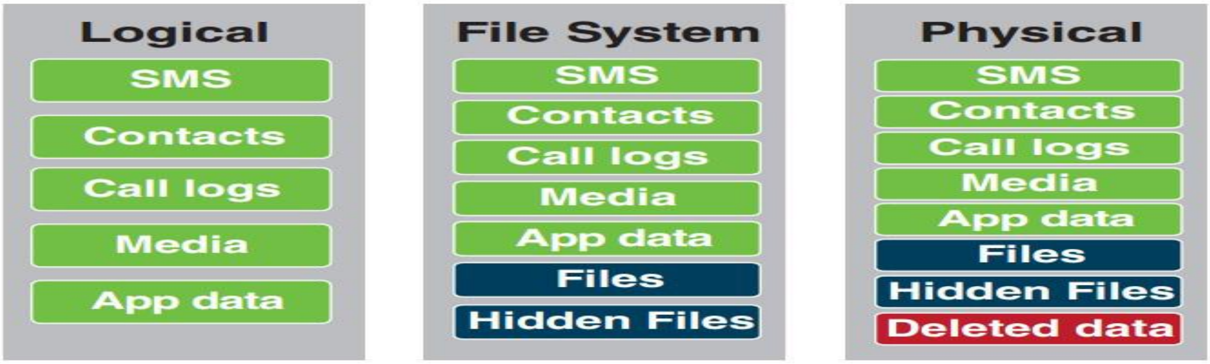


Figure 1 Cellebrite's® types of extractions and the artifacts each one supports.

4.6 Data creation

Each phone was given an identity to identify the Phone during the Experiment as shown in the above table. After the identities on each phone were connected to a computer running Cellebrite and Oxygen, artifacts were produced on each phone.

Artifacts to be retrieved from the Experiment	
Call logs	Taken Pictures
E-mails	Deleted pictures
Contacts	WhatsApp Messages
Text messages	Web History

Table 2 A list of artifacts extracted for evaluation from each phone.

4.6.1 Data Extraction Process

The method of physical removal differs between mobile phones. The imagery process was usually the following except for iPhones:

1. Allow debugging, if necessary, by hand.

2. Turn off your device and connect it to on USB port on computer or Laptop running Cellebrite Touch and Oxygen Suite.

4. Monitor the Software (Cellebrite Touch, Oxygen Suite) prompt to begin the extraction process via the computer-based software.

Following these steps, the extraction process started and a bit-by-bit memory copy was extracted to a directory of choice as an image.

4.7 Mobile Image Analysis Tools

Our goal was to determine the efficiency of the Autopsy Open Source Tool (’T’tool), Cellebrite, and Oxygen. In order to accomplish this, we used the three tools to image the smartphones looking specifically for discrepancies across call logs, e-mails, WhatsApp messages, text messages, and images and deleted text information.

4.8 Images results

The results were collected from the Images of the five phones, the imaging was done on the same experimental environment with all phones set on airplane mode and the following results were recorded from the analysis of the three tools.

Artifacts	iPhone	HTC Desire	Infinix	Techno	Samsung
Call logs	34	305	209	56	103
E-mails	15	56	31	12	34
Contacts	21	45	26	36	67
Text messages	18	219	145	83	108
Pictures	13	87	63	13	71
Deleted Text	8	102	181	71	90
WhatsApp Messages	142	567	669	105	206
Taxa_S	7	7	7	7	7
Individuals	251	1381	1324	376	679
Shannon_H	1.421	1.599	1.461	1.739	1.823
Berger-Parker	0.5657	0.4106	0.5053	0.2793	0.3034

Table 3 Artifacts analysis from the image created using Cellebrite touch software.

The Berger parker from the Shannon Index was used to give the proportion of the amount of artifacts retrieved from each phone and since WhatsApp was the most dominant with the highest(57 %) and lowest(28%) from iPhone as shown on *table 3*, The Diversity index (H') shows that there was no significantly different between HTC Desire and iPhone ($t_{df=}$ 2.6371, p= 0.00879), iPhone and Infinix ($t_{df=}$ 0.57357, p= 0.56666) but there was significant different between HTC Desire and Infinix ($t_{df=}$1.61E-05, p= 1.61E-05),infinix and Techno ($t_{df=}$ -7.4187, p= 2.55E-13),Techno and Samsung ($t_{df=}$2.4535,p= 0.014389) iPhone and Techno($t_{df=}$4.5224,p= 8.38E-06),iPhone and Samsung ($t_{df=}$ 5.9945,p= 5.94E-09),HTC Desire and Techno ($t_{df=}$ -3.9722,p= 7.75E-05),infinix and Samsung ($t_{df=}$ 11.703,p= 1.21E-30) and HTC Desire and Samsung ($t_{df=}$ -2.6371,p= 0.00879) when using Cellebrite touch to perform analysis. Individuals from the table above shows that Cellebrite Touch retrieved more artifacts from all the phones better than Oxygen Forensics Suite and open source Autopsy.

Artifacts	iPhone	HTC Desire	Infinix	Techno	Samsung
Call logs	30	223	173	43	78
E-mails	9	49	27	8	29
Contacts	19	32	23	31	60
Text messages	23	187	133	67	101
Pictures	10	79	55	9	59

Deleted Text	5	91	173	69	74
WhatsApp Messages	154	485	527	99	191
Taxa_S	7	7	7	7	7
Individuals	250	1146	1111	326	592
Shannon_H	1.295	1.598	1.506	1.697	1.803
Berger-Parker	0.616	0.4232	0.4743	0.3037	0.3226

Table 4 Artifacts analysis from the image created using Oxygen Suite Software.

The Berger parker from the Shannon Index was used to give the proportion of the amount of artifacts retrieved from each phone and since WhatsApp was the most dominant with the highest of (62 %) and lowest of (30%) from iPhone as shown on *table 4*, The Diversity index (H') shows that there was no significantly different between Techno and Samsung (t_{df} = 2.7026, p=0.007067) and HTC Desire and Infinix (t_{df} = 2.6975, p= 0.007038) but there was significant different between, infinix and Techno (t t_{df} = 4.6132, p=4.66E-06) , iPhone and Techno(t_{df} = -5.3093, p=1.92E-07),iPhone and Samsung (t_{df} =7.0823, p=9.91E-12), HTC Desire and Samsung (t_{df} = 6.4323, p= 1.66E-10),HTC Desire and Techno (t_{df} = 2.4644, p=0.013971),infinix and Samsung (t_{df} = 8.8512, p=2.18E-18) and HTC Desire and iPhone (t_{df}= 4.2134, p= 3.31E-05),iPhone and Infinix (t_{df} = 2.9054, p= 0.0039217) when using Oxygen suite to perform analysis.

Artifacts	iPhone	HTC Desire	Infinix	Techno	Samsung
Call logs	0	0	0	0	0
E-mails	3	7	5	1	3
Contacts	2	0	0	0	0
Text messages	1	17	12	0	0
Pictures	5	23	31	5	12
Deleted Text	0	0	0	0	1
WhatsApp Messages	0	0	0	0	0
Taxa(S)	4	3	3	2	3
Individuals(n)	11	47	48	6	16
Shannon(H)	1.24	1	0.86	0.45	0.7
Berger-Parker(d)	0.45	0.49	0.65	0.83	0.75

Table 5 Artifacts analysis from the image created using Autopsy Open source Software.

The Berger parker from the Shannon Index was used to give the proportion of the number of artifacts retrieved from each phone and since pictures was the most dominant with the highest of (83 %) and lowest of (45%) from Techno phone as shown on *table 5*, The Diversity index (H') shows that there was no significantly different between iPhone and Infinix (t_{df} = 1.9747, p= 0.091055), iPhone and Samsung (t_{df} = 1.9593, p= 0.060656) and HTC Desire and Techno (t_{df} = 1.9747, p= 0.091055) but there was significant different between, iPhone and HTC Desire(t_{df} = 1.2059, p= 0.24857),HTC Desire and Infinix (t_{df} = 1.2059, p= 0.24857),infinix and Techno (t_{df} = 1.4422, p= 0.1899),Techno and Samsung (t_{df} = 0.74867, p= 0.46758), HTC Desire and Samsung (t_{df} = 1.4273, p= 0.16955),Infinix and Samsung (t_{df} = 0.73528, p= 0.46952) when using Autopsy to perform analysis.

CHAPTER 5

DISCUSSION, CONCLUSION, AND RECOMMENDATIONS

5.0 Introduction

This chapter presents a discussion on the summary of findings, challenges, and limitations encountered during research, conclusions reached and finally recommendations on findings of the research.

5.1 Discussion

The selected forensics configuration of tools where the best and available during the study.

In order to meet the general study objective of *comparatively analyze and evaluate the effectiveness and performance of forensics tools on smartphones*. We formulated two research questions that we use to organise the results. These questions, used to determine the order the results are presented, are as follows: -

RQ3 and **RQ4:** Are there differences among Cellebrite Touch, Oxygen suite and 'T' Tool (Autopsy) concerning mobile device Imaging and analytical capabilities? And the number of files found by one tool that is not found by the other?

This is handled in *Table 3, Table 4 and Table 5* Artifacts analysis from the image created using Cellebrite touch software, Oxygen Suite and Autopsy. The ability of some of these tools to acquire data demonstrates significant progress in the development of quality and effective forensic procedures but the findings as shown that no single tool can be used complete an investigation on smartphone, one tool was able to get more artifacts from one phone more than what could be retrieved from the other phones.

The aim of the study was also to know, which tools are used in Kenya to carry out mobile forensics.

RQ1: and we found out that different organizations used different tools to image and Analyze but in some cases same tools where used for both, FTK and Open source forensics software's we common in all the organization but Cellebrite touch and Oxygen suite were the best tools since they were used for imaging and analysis.

The study concentrated on observation of the performance of Cellebrite Touch, Oxygen Suite, and Autopsy. The tools were subjected to the same test environment for examination.

The need for forensics tools capable of extracting evidentiary data cannot be overemphasized. Being able to provide adequate and no-refutable evidence of data would be crucial to the success of prosecuting the suspect in a court of law. It is evident to say that different tools present different strengths and weaknesses.

The benefit of this study can, therefore, be related to the benefits of testing tool which include:

- Being assured of what the tool's capabilities are.
- Know the limitations of each tool and have a head start on validating the tool for use in a forensics laboratory.

It is noticed that Autopsy was the weakest in mobile Analysis and may not be the right tool for mobile phone Investigation. Cellebtrite was the best-suited tool for mobile Investigation. The amount of individuals artifacts retrieved was very high compared to the other two tools, but for quick investigation on the mobile phone, the Oxygen suite is the best since it takes a short time to image and analyses compared to Cellebrite but the amount of artifacts retrieved are less.

5.2 Challenges

The study was done biased in one operating system environment, windows. This was the first limitation in that other operating systems are not very popular in mobile forensics and digital forensics. Only the Autopsy tool can work both on windows and Linux platforms.

Another key issue is getting the mobile phone forensics tools for this research was very difficult since most institutions could not afford the cost of licensing the two major tools (Cellebrite and Oxygen suite). Lastly, the working knowledge of how to use the tools took me a long time to understand and implement.

5.3 Conclusion

After critically analyzing the findings, it is evident that every forensics tool has its unique strengths and weakness. The identifiable and evaluated strengths and weaknesses in mobile and digital forensic at large are that the results should be reliable before the presentation of evidence a jury.

The finding from this research also shown that each forensic tool has its capability in terms of Effectiveness and Performance and all the tools used in this research varies.

Major forensics organizations can borrow heavily on this finding to help select the best tool to investigate a case and get enough artifacts that can be produced in court during the adjudication of a case involving smartphones.

The research will contribute to the evaluation of other mobile phone forensics tools used in Kenya since the forensic industry has a strong demand for well configure forensics tools and a comprehensive evaluation methodology. The study also summarized the relevant literature related to the evaluation, performance, and effectiveness of mobile forensics tools.

5.4 Future work and Recommendation

Considering that both digital and mobile forensics is a major requirement in any state, all tools whose effectiveness has been evaluated and certified should be deployed in a forensic laboratory within the investigative institution. This shall promote the acceptability and admissibility of evidence before a jury or any other equivalent institution.

The researchers propose a generic methodology for Smartphone forensic tools. A methodology that can allow several tools to share their databases and file extensions.

Future work should include a wide variety of mobile phones and the phones should be new and given to the users, monitored on the usage and later imaged and analyzed to get the accuracy on the number of Artifacts recovered from each brand new mobile phone.

BIBLIOGRAPHY

Global Cybersecurity Index (GCI) 2017 (2017).

Governance in focus Cyber risk reporting in the UK Cyber reporting survey Contents (2017).

Kausar, F. (2014) 'New Research Directions In The Area Of Smart Phone Forensic Analysis', *International journal of Computer Networks & Communications*, 6(4), pp. 99–106. doi: 10.5121/ijcnc.2014.6409.

Martin, C. M. (2017) 'Comparing Two Tools for Mobile-Device Forensics'. Available at: https://apps.dtic.mil/dtic/tr/fulltext/u2/1046880.pdf.

Osho, O. (2016) 'Comparative Evaluation of Mobile Forensic Tools', (January), pp. 74–83. doi: 10.5815/ijitcs.2016.01.09.

Yadav, S., Ahmad, K. and Shekhar, J. (2011) 'Analysis of digital forensic tools and investigation process', *Communications in Computer and Information Science*, 169 CCIS, pp. 435–441. doi: 10.1007/978-3-642-22577-2_59.

Zareen, A. and Baig, S. (2010) 'Mobile phone forensics challenges, analysis and tools classification', *5th International Workshop on Systematic Approaches to Digital Forensic Engineering, SADFE 2010*, (May 2009), pp. 47–55. doi: 10.1109/SADFE.2010.24.

Wright. Jon. "High-tech Holmes". Security Management. Arlington: July 2001. Vol. 45, Issue 7; pg. 44, Wright-Patterson. Available (Online).

==

A SAGE Company, 2455 Teller Road Thousand Oaks, California, USA.

A. Zareen, & S. Bai," Mobile Phone Forensics Challenges, Analysis and Tools Classification".

Altheide, C. Carvey, H (2011) Digital forensics with open source tools Pp 26 – 27 Waltham: Elsevier.

Altinay, L. and Paraskevas, A., 2008, planning research in hospitality and tourism. Butterworth-Heinemann, Linacre House, Jordan Hill, Oxford OX2 8DP, UK.

Ankit Agarwal, Megha Gupta, Saurabh Gupta & Prof. (Dr.) S.C. Gupta "Systematic Digital Forensic

Casey E, and Turnbull B. Digital evidence on mobile devices. Computers, and the Internet, Academic Press (2011).

Crime', Paper presented at the 4th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, and 4th December.

Dasari Manendra Sai et al, "International Journal of Computer Science and Information Digital Forensic Research Workshop (DFRWS) Utica: Research Road Map, 2001

Electrical and Computer Engineering Air force institute of technology.

Eoghan Casey, Digital Evidence and Computer Crime. Third Edition. Forensic Science,

Firdous Kausar "New research directions in the area of smartphone forensic analysis" IJCNC Vol.6, No.4, July 2014.

Gael et al. (2012) Smartphone forensic investigation process model

http://www.dfrws.org/2001/dfrws-rm-final.pdf.

http://www.t3k-forensics.com/allgemein-en/10-main-challenges-in-mobile-forensics2.

http://www.utica.edu/academic/institudes/ecii/ijde/articles.cfm?action.

https://www.cellebrite.com/en/products/ufed-ultimate/

https://www.standardmedia.co.ke/business/article/2001235820.

Imtiaz, F., 2006, 'Enterprise Computer Forensics: A defensive and offensive strategy to fight computer

International Journal of Advanced Computer Science and Applications, 2011, (11), 110 –114.

Investigation model.

Investigation Model" Volume5, Issue1, IJCSS-438.

Jones, K. Bejtlich, R. Rose, C. (2005) real digital forensics: Computer security and incident response P-172.

Kaur and Amandeep Kaur, 2012, Digital Forensics (Vol. 50) Guru Nanak Dev University.

Kenya-worst-hit-in-east-africa-by-cyber-crime.

Kothari, C. R., 2004, Research Methodology, Methods and Techniques, 2nd Edition.

Martin, Casandra M." Comparing two tools for mobile-device forensics''2017.

Namrata R. Agrawal ''Mobile Forensics – A Literature Review'' IJFEAT 2013.

Neha Kishore, Cheta Gupta, and Dhvani Dawar, 2014, an insight into digital forensics.

Oluwafemi Osho, Sefiyat Oyiza Ohida '' Comparative Evaluation of Mobile Forensic Tools '' IJITCS, 2016.

Palmer, G. (2001) a road map to digital forensic research Available (online):

pg. 6.

Reith, M. Carr. C. Gunsch, G. (2002). An examination of a digital forensic model. Department of

Serianu KenyaCyberSecurityReport 2017.

Sridhar N, Bhaskari DL, and Avadhani P. Plethora of Cyber Forensics.

Sriram Raghavan and V Raghavan, "A Study of Forensic & Analysis Tools", IEEE, 978-1-4799-4061-5/13, 2013.

Technologies", IJCSIT, Vol. 6 (5), 2015, 4847-4850.

Vishal R A, and Meshram B B. Digital Forensic Tools.IOSR Journal of Engineering, 2012, 2(3), 392-398.

Wright. Jon. "High-tech Holmes". Security Management. Arlington: July 2001. Vol. 45, Issue 7; pg. 44, Wright-Patterson. Available (Online):

Yadav S. "Analysis of Digital Forensic and Investigation". VSRD-IJCSIT, Vol. 1 (3), 2011, 171178p.

Yunus Yusoff, Roslan Ismail and Zainuddin Hassan, 2011, Common phrases of computer forensics

Questionnaire –Pre Implementation

Comparative evaluation of the effectiveness of Smartphone forensics tools.

The survey is to get feedback on the forensics organizations in Kenya and the tools use to carry out smartphone forensics and which tools are preferred when it comes to smartphone forensics imaging and analysis of the artifacts to form a case that can be presented before a court.

1. How many forensics experts do your organization have?

○ 1 - 10

○ 10 - 50

○ 50 - 100

○ 100 - 200

○ Above 200

2. What does your organization do?

3. What are the major forensic cases your organization has ever handled?

○ Formatted hard disk

○ Retrieval of specific information on an organization case

○ Mobile forensics

○ Specific Case (indicate)

4. What are some of the limitation your organization face during forensic investigations?

5. What are the main tools used by your organization to carry out digital forensic?

6. How effective are the digital forensic tools?

○ Excellent

○ Good

○ Acceptable

○ Fair

○ Poor

7. Does your organization use the same tools for imaging and analysis?

○ Yes

○ No

8. Does the cost of digital forensic tools affect the operation of your organization?

○ Yes

○ No

9. Does your organization handle mobile phone forensic?

○ Yes

○ No

10. How effective are the tools provided by the organization when handling mobile phone cases?

○ Excellent

○ Good

○ Acceptable

○ Fair

○ Poor

11. What are the tools used to image mobile phones during investigation?

12. What are the tools used to analyze mobile phones in your organization?

1.

2.

3.

4.

5.

13. How many tools are used to investigate each mobile phone case?

14. Do your organization use (Indicate the tool)

Licensed forensic tools?

Open Source forensic tools?

Others

15. If you use open source forensic tools how effective are they compared to licensed forensic tools?

○ Excellent

○ Good

○ Acceptable

○ Fair

○ Poor

16. How long does it take to investigate a given mobile phone case?

○ Less than a day

○ 1 day

○ 2 to 3 days

○ 3 to 4 days

○ 4 days and above

17. Does your organization use the same forensic tools to image and analyze?

○ Yes

○ No

18. Which are the forensic tools available for use in your organization when investigating mobile phone cases?

1. □

2. □

3. □

4. □

5. □

Thanks you

APPENDICES

Pre -Evaluation of Environment and Requirements

The materials, hardware, and software, used to achieve the objective of the study include:

I. Samsung Galaxy running Android v2.3.6. And above

II. HTC Desire, running Android v4.1.0 and above

III. Techno, running Android v4.1.0 and above

IV. Infinix, running Android v4.1.0 and above

V. Laptop, running on Windows 7, 64 bits.

VI. iPhone 4 and above

VII. USB Cable.

VIII. Analysis platform –T tool

IX. Cellebrites Physical analyzer (CPA) software

X. Oxygen Forensic Suite 2014 v6.4.0.67 (trial version).

XI. 3 SIM cards (1 Safaricom, 1 Airtel, and 1 Telekom).