ENHANCED FORENSIC FRAMEWORK FOR ROOTED MOBILE PHONES AND THE IMPACT ON USER DATA INTEGRITY – A CASE OF ANDROID SMARTPHONES

BY

CHRISANTUS ODONGO

UNITED STATES INTERNATIONAL UNIVERSITY - AFRICA

SUMMER 2018
ENHANCED FORENSIC FRAMEWORK FOR ROOTED MOBILE PHONES AND THE IMPACT ON USER DATA INTEGRITY – A CASE OF ANDROID SMARTPHONES

BY
CHRISANTUS ODONGO

A Project Report Submitted to the School of Science and Technology in Partial Fulfillment of the Requirement for the Degree of Master of Science in Information Systems and Technology

UNITED STATES INTERNATIONAL UNIVERSITY - AFRICA

SUMMER 2018
STUDENT’S DECLARATION

I, the undersigned, declare that this is my original work and has not been submitted to any other college, institution or university other than the United States International University - Africa in Nairobi for academic credit.

Signed: ______________________ Date: ______________________

Chrisantus Odongo (ID No: 645256)

This project has been presented for examination with my approval as the appointed supervisor.

Signed: ______________________ Date: ______________________

Dr. Gerald Chege

Signed: ______________________ Date: ______________________

Dean, School of Science and Technology
COPYRIGHT

All rights reserved. No part of this dissertation report may be photocopied, recorded or otherwise reproduced, stored in retrieval system or transmitted in any electronic or mechanical means without prior permission of USIU-A or the author.

Chrisantus Odongo © 2018.
ABSTRACT

The proliferation of Android smartphones has propagated negative societal issues that resulted in successful arrests of the culprits, forensic examination and prosecution. Other such cases have collapsed due to alteration of forensic evidence as a result of inadequate forensic sound frameworks. The purpose of this study was to develop and evaluate an enhanced forensic framework for Android smartphones with a key focus on data integrity. The research objectives included exploration of rooting techniques and the impact on data integrity; exploration of forensic frameworks and development of an enhanced forensic framework; and lastly, extract, examine and analyze forensic data with the aim of validating the enhanced forensic framework.

The research adopted a laboratory experiment using MOBILedit Forensic Express software to collect forensic data on three Android smartphones that were rooted using KingoRoot software. The research performed both logical and physical acquisitions in .rtf and .txt format; images in .jpeg; messages and web browsing history. Using hash values, analysis of both logical and physical copies was conducted to establish forensic data integrity issues. Through the enhanced framework, data integrity was maintained since both logical and physical copies of the report files presented the same data integrity characteristics.

Research objective one acknowledged several rooting techniques that presented shortcomings such as risks of bricking smartphones. Using KingoRoot software, the rooting technique used in this research did not affect the test devices used and the final data, but only aided in retrieving more data in physical acquisition than in a logical acquisition. The enhanced forensic sound model designed and implemented in this research addressed objective two by ensuring that if the proposed steps were carried out, both logical and physical extractions of data provided comparative data that ensured data integrity. Extraction, examination and analysis of data was well conducted and fully addressed objective three of this research. Through calculation of the hash values, data integrity was ensured since all integrity characteristics presented similar values for the same document, image, message or browsing history in both logical and physical extraction reports. The enhanced framework was therefore validated. For future work, the research recommended the development of forensic tools that could be able to decrypt specific data such as WhatsApp conversations and other highly encrypted applications.
ACKNOWLEDGEMENT

I wish to express my greatest gratitude to Almighty God for granting me life, strength and opportunity to go through my academic life.

Special acknowledgement goes to my parents Mr. Agostino Odongo and Mrs. Euniver Adi Odongo. I could not have reached this far without your support and encouragement. Thank you very much.

I am eternally grateful to my family for providing me moral and emotional support throughout my life. I am equally grateful to my friends, USIU –Africa staff and faculty as well as students who have supported me along my academic journey.

Special gratitude goes to my research supervisor, Dr. Gerald Chege, for his thorough guidance, wisdom and patience demonstrated during this research project. I am equally grateful to Dr. Benson Kioni and Dr. Stanley Githinji for their advice and in-depth knowledge towards the completion of this research project.

God bless you all.
DEDICATION

I dedicate this dissertation to my family; specifically, my parents Mr. Agostino Odongo and Mrs. Euniver Adi Odongo for their incessant support and encouragement; and more so, my wife Mrs. Winnie Akoleit and my daughter Euniver Adi Podmar.
# TABLE OF CONTENTS

STUDENT’S DECLARATION ................................................................................. ii  
COPYRIGHT ..................................................................................................... iii  
ABSTRACT ........................................................................................................ iv  
ACKNOWLEDGEMENT .................................................................................... v  
DEDICATION .................................................................................................... vi  
LIST OF TABLES ............................................................................................... x  
LIST OF FIGURES ............................................................................................ xi  

Chapter 1: Introduction ...................................................................................... 1  
1.1 Background of the Study ........................................................................... 1  
  1.1.1 Android Operating System ................................................................. 1  
  1.1.2 Rooting and Data Integrity ................................................................. 2  
  1.1.3 Digital Forensics ............................................................................... 4  
1.2 Statement of the Problem .......................................................................... 5  
1.3 General Objective ...................................................................................... 7  
1.4 Specific Objectives .................................................................................... 8  
1.5 Significance of the Study .......................................................................... 8  
1.6 Scope of the Study .................................................................................... 9  
1.7 Definition of Terms ................................................................................... 9  
1.8 Chapter Summary ..................................................................................... 11  

Chapter 2: Literature Review .......................................................................... 12  
2.1 Introduction ............................................................................................... 12  
2.2 Theoretical Foundations .......................................................................... 12  
2.3 Rooting Android Smartphones and the Impact on Data Integrity ............... 14  
  2.3.1 Understanding Android Architecture ................................................ 14  
  2.3.2 Rooting Android Smartphone ............................................................ 16  
2.4 Forensic Frameworks for Smartphones ..................................................... 18  
2.5 Data Extraction, Examination and Analysis for Framework Validation ...... 29  
  2.5.1 Data Extraction ............................................................................... 29  
  2.5.2 Examination and Analysis of Forensic Evidence ................................ 37  
2.6 Research Approach .................................................................................... 46  
2.7 Chapter Summary ..................................................................................... 47
Chapter 3: Methodology
3.1 Introduction ................................................................. 49
3.2 Research Design .......................................................... 49
3.3 Data Collection Methods ................................................. 52
3.4 Research Procedures ..................................................... 53
3.5 Data Analysis Methods .................................................. 53
3.6 Ethical Considerations .................................................... 55
3.7 Chapter Summary .......................................................... 56

Chapter 4: Model
4.1 Introduction .................................................................. 57
4.2 Analysis ........................................................................... 57
  4.2.1 Research Tools Analysis .............................................. 58
  4.2.2 Data Integrity ............................................................. 58
4.3 Modeling ........................................................................ 59
4.4 Proof of Concept ........................................................... 61
4.5 Chapter Summary .......................................................... 61

Chapter 5: Results and Findings .................................................. 63
5.1 Introduction .................................................................. 63
5.2 Rooting Techniques and Impact on Data Integrity ............... 63
5.3 Enhanced Forensic Framework for Rooted Android Smartphones .......................... 66
5.4 Data Extraction, Examination and Analysis for Framework Validation ............... 68
  5.4.1 Data Extraction ............................................................. 68
  5.4.2 Data Examination and Analysis to Validate Enhanced Framework.................. 77
5.5 Chapter Summary .......................................................... 99

Chapter 6: Discussion, Conclusions and Recommendations ........... 100
6.1 Introduction .................................................................. 100
6.2 Summary ....................................................................... 100
  6.2.1 Purpose of the Study .................................................. 100
  6.2.2 Specific Objectives ..................................................... 100
  6.2.3 Research Methodology .............................................. 101
  6.2.4 Major Findings .......................................................... 102
6.3 Discussion ..................................................................... 103
  6.3.1 Rooting Techniques and Impact on Data Integrity ............... 103
6.3.2 Enhanced Android Forensic Framework for Rooted Smartphones.............. 104
6.3.3 Data Extraction, Examination and Analysis to Validate the Framework...... 106
6.4 Conclusions........................................................................................................... 107
  6.4.1 Rooting Techniques and Impact on Data Integrity................................. 107
  6.4.2 Enhanced Android Forensic Framework for Rooted Smartphones........... 107
  6.4.3 Data Extraction, Examination and Analysis for Framework Validation...... 108
6.5 Recommendations and Future Work................................................................. 108
  6.5.1 Recommendations for the Research......................................................... 108
  6.5.2 Recommendations for Future Work......................................................... 108
References................................................................................................................. 109
LIST OF TABLES

Table 2-1: Android Standard Data Path.................................................................32
Table 2-2: A Comparison of Android Forensic Data Collection Methodologies ..........47
Table 3-1: Analysis of Smartphone Forensics Tools..............................................50
Table 3-2: Analysis of Various Research Methodologies .......................................51
LIST OF FIGURES

Figure 1-1: Global Mobile OS Market Share from 2009 to 2018 ............................................. 2
Figure 2-1: Android Architecture .................................................................................................. 16
Figure 2-2: Android Evidence Collection and Analysis Methodology ........................................ 22
Figure 2-3: Forensic Collection Process Model ............................................................................. 24
Figure 2-4: Smartphone Forensic Investigation Process Model ................................................. 27
Figure 2-5: FTK Imager Forensic Hashing ....................................................................................... 45
Figure 4-1: Basic Phases of the Forensic Process ........................................................................ 57
Figure 4-2: Research Procedural Functions ..................................................................................... 60
Figure 5-1: Rooting using KingoRoot .......................................................................................... 65
Figure 5-2: Enhanced Android Forensic Process Model ............................................................... 67
Figure 5-3: Logical Data Extraction with Itel it1508 ................................................................. 69
Figure 5-4: Forensic Data Extraction before Rooting for Itel it1508 ............................................. 70
Figure 5-5: Forensic Data Extraction before Rooting for Tecno F7 ............................................. 70
Figure 5-6: Forensic Data Extraction before Rooting for Blu Studio C5 + 5LTE ....................... 71
Figure 5-7: Tecno F7 in Recovery ................................................................................................. 72
Figure 5-8: Itel it1508 in Recovery ............................................................................................... 72
Figure 5-9: Blu Studio C5 + 5LTE in Recovery ............................................................................ 72
Figure 5-10: Physical Data Extraction with Tecno F7 ................................................................. 73
Figure 5-11: Forensic Data Extraction after Rooting for Tecno F7 ............................................. 74
Figure 5-12: Physical Data extraction with Blu Studio C5 + 5LTE .............................................. 74
Figure 5-13: Forensic Data Extraction after Rooting Blu Studio C5 + 5LTE ............................ 75
Figure 5-14: Physical Data extraction with Itel it1508 ................................................................. 76
Figure 5-15: Forensic Data Extraction After Rooting for Itel it1508 ........................................... 76
Figure 5-16: Report from the Extraction of a Logical Copy for Itel it1508 ............................... 78
Figure 5-17: Report from the Extraction of a Physical Copy for Itel it1508 .............................. 78
Figure 5-18: Report from the Extraction of a Logical Copy for Tecno F7 ................................. 79
Figure 5-19: Report from the Extraction of a Physical Copy for Tecno F7 ............................... 80
Figure 5-20: Extraction Report of a Logical Copy for Blu Studio C5 + 5LTE ............................ 80
Figure 5-21: Extraction Report of a Physical Copy for Blu Studio C5 + 5LTE ........................... 81
Figure 5-22: Extracted .rtf Documents from Logical Copy Report for Itel it1508 .................. 82
Figure 5-23: Extracted .rtf Document from Physical Copy for Itel it1508 ............................... 82
Figure 5-24: Extracted .txt Document from Logical Copy for Tecno F7 ..................... 83
Figure 5-25: Extracted .txt Document from Physical Copy for Tecno F7 .................. 83
Figure 5-26: Extracted .txt Document from Logical Copy for Blu Studio C5 + 5LTE ... 84
Figure 5-27: Extracted .txt Document from Physical Copy for Blu Studio C5 + 5LTE ... 84
Figure 5-28: Extracted Image from Logical Copy for Itel it1508 .......................... 85
Figure 5-29: Extracted Image from Physical Copy for Itel it1508 .......................... 86
Figure 5-30: Extracted Image from Logical Copy for Tecno F7 ............................. 86
Figure 5-31: Extracted Image from Physical Copy for Tecno F7 ............................. 87
Figure 5-32: Extracted Image from Logical Copy for Blu Studio C5 + 5LTE .......... 87
Figure 5-33: Extracted Image from Physical Copy for Blu Studio C5 + 5LTE .......... 88
Figure 5-34: General Representation of the Extracted Messages .......................... 89
Figure 5-35: Extracted Messages from Logical Copy for Itel it1508 ....................... 90
Figure 5-36: Deleted Messages Extracted from Physical Copy for Itel it1508 ........... 91
Figure 5-37: Extracted Messages from Logical Copy for Tecno F7 ....................... 92
Figure 5-38: Extracted Messages from Physical Copy for Tecno F7 ....................... 93
Figure 5-39: Messages from Logical and Physical Copy for Blu Studio C5 + 5LTE .... 94
Figure 5-40: Web Browsing History Logical Image for Itel it1508 ........................ 95
Figure 5-41: Web Browsing History Physical image for Itel It1508 ....................... 95
Figure 5-42: Web Browsing History Logical Image for Tecno F7 ........................ 96
Figure 5-43: Web Browsing History Physical Image for Tecno F7 ........................ 97
Figure 5-44: Web Browsing History Logical Image for Blu Studio C5 + 5LTE ....... 98
Figure 5-45: Web Browsing History Physical Image for Blu Studio C5 + 5LTE ....... 98
Chapter 1: Introduction

1.1 Background of the Study

This chapter considered the purpose of undertaking the research project with the idea of developing an enhanced Android forensic framework. This chapter introduced the area of study, background of the research area as well as general knowledge on Android operating system. It based itself on the areas the research was aimed to address by proposing solutions to the problem statement. The study also touched on other gray areas of the research topic by exploring more information about the subject matter.

Android mobile phones have rapidly grown in popularity and usage globally over the recent years. A report by Communications Authority of Kenya (2017) indicated that there were over thirty-eight million mobile subscriptions in Kenya, most which were smartphones. The ubiquitous nature, lower costing and the convenience of Android smartphones have resulted in their wide use. Android operating system is freely offered to phone manufacturers thereby ensuring production of cheaper phones. Also, they offer a rich source of personal information since their usage has been extended to high security activities such as mobile banking transactions and social interaction/communication.

1.1.1 Android Operating System

Android is an open source operating system which is based on Linux kernel (open source operating system with built-in C/C++ libraries) (Shahbaz, Bilal and Ahmad, 2016). Android applications are Java based applications that usually run inside a sandbox with reserved area for applications. The operating system was previously developed by Android Inc. and later purchased by Google Inc. Android's user interface is mainly based on direct manipulation using touch inputs that loosely correspond to real-world actions to manipulate on-screen objects, along with a virtual keyboard.

The initial development and use was meant for touchscreen mobile devices such as smartphones and tablets where its user interface is mainly based on direct operation. This is through using touch gestures that loosely correspond to real-world actions, such as swiping and tapping to manipulate on-screen objects, along with a virtual keyboard for text input (Shahbaz et al., 2016).
According to Son et al., (2013), the number of Android device users in the third quarter of 2012 was reported to be over 181 million. The author went ahead to note that the vast evolution and market presence of Android smartphones’ usage presently cannot be ignored. The ease it creates for people brings with it challenges like crime and information security breaches. These criminal activities bring about the need for mobile forensics and digital investigations for law enforcers.

Current statistics according to Statista (2018) showed that the global mobile Operating System market share, in terms of sales to end users, from 2009 to 2018 rose from as low as 1.6% to over 85% respectively. In the first quarter of 2018, 85.9 percent of all smartphones sold to end users were phones with the Android operating system. Figure 1-1 depicts these statistics.

![Figure 1-1: Global Mobile OS Market Share from 2009 to 2018 (Source: Statista (2018))](image)

1.1.2 Rooting and Data Integrity

Rooting can be compared to jail-breaking in the case of Apple iOS. It is the process of granting Android users privileged control (known as root access) to devices running the Android mobile operating system. These could be smartphones or tablets. The procedure
is performed with an intent of overcoming limitations that carriers and hardware manufacturers put on the smart devices (Lessard & Kessler, 2010).

Lessard and Kessler (2010) noted that the process of rooting and imaging the phone memory to collect digital evidence was vital in mobile forensics. This was because the memory being investigated contained additional information, metadata, history and passwords, which could easily be accessed if the said smartphone was rooted. Data integrity refers to maintenance and the assurance of the accuracy and uniformity of data over its entire life-cycle hence an imperative aspect to the design, implementation and usage of any system which stores, processes or convalesces data.

In their research, the authors annotated that altering the functionality of a device and altering data in such a manner was not forensically sound for data integrity. They relayed fears that the procedure would not be advisable to be done in an investigation (Lessard & Kessler, 2010). Depending on the information involved, data integrity could manifest itself as a single pixel in an image appearing a different color than that which was originally recorded or documented. Such events could be brought about by altering normal device functionality through the rooting process (Lessard & Kessler, 2010). The scholars continued to state that even the procedure of performing rooting to gain ‘super user’ access necessitated that the forensic investigator/examiner installs a third-party software to the phone, this could make the evidence not admissible in a court of law if data was altered in the process.

According to a study by McMillan, Glisson and Bromby (2013), the chain of custody helps to decrease the possibility that data integrity was compromised during the examination process through maintenance and documentation. Rapid usage of smartphones coupled with the expansion of capabilities used in extraction of data have complicated issues regarding admissibility of evidence. The authors noted that data that is extractable from a device largely depended on an investigators’ capabilities as well as the extraction process implemented. The principal focus of admissibility was to ensure that data stored on the device was left unchanged after the rooting process. The authors affirmed that this was problematic since activities such as switching mobile phones off and back on would lead to making changes to dates stored on the test device.
Our study focused on authenticating the evidence collected with the aim of verifying data integrity. The study obtained a copy of an original collection or previously known files with preconceived features like name, size date and time stamps, for a logical acquisition. This were thereafter matched with evidence collected from a rooted phone through a physical collection.

The study employed a cryptographic technique called hash function with the aim of checking data integrity issues to ensure forensic data admissibility in a court of law. For evidentiary purposes, the hash value was that of the newly created image. The hash value was important since without it, there would have been no proof that the acquired image was a match or copy of the original device memory (Kumar, 2011).

1.1.3 Digital Forensics

The term Forensics was invented after the Latin word 'forensis', suggesting "in open court" or rather "open". The word was utilized in this context in connection to finding computerized bits of proof information to settle a wrongdoing in case there were disputes. Solms and Louwrens, (2006) defined digital forensics as "logical and investigative methods used for the protection, identification, extraction, documentation, analysis and interpretation of computer media, which are digitally stored or encoded for evidentiary and or root cause analysis". The process required defined procedures that comply with industry practice, organizational practice and appropriate laws based on a criminal investigation or as part of a more general security incident response.

Recently, East African Data Handlers Managing Director George Njoroge raised a concern on the Standard media channel through a publication in The Standard Digital (2014). In this case, his data recovery firm was hired to investigate a case where a fired bank employee had sent alarming messages to clients, telling them to withdraw their deposits because the institution was allegedly going under. “In this situation, we had to trace who sent the message, from what machine and on what date. We successfully nailed the culprit,” he said. The main challenge his firm faced in its early days was the lack of a legal and/or forensic framework governing cyber evidence, which made admissibility of evidence in court difficult. Also, during the initial phases of the case, he reported that there were issues raised regarding the methods used to gather the forensic evidence presented in court, hence the issue of data integrity.
To resolve such issues with ease, through the Kenya National Police Service, a Forensic Laboratory has been built near the CID Headquarters on Kiambu Road and with incorporation of a state of the art digital forensics laboratory. According to Directorate of Criminal Investigations (2015) the main activities performed here include forensic examination of computer and mobile phones; maintenance of lab processes of acquisition, archival and analysis; maintenance of inventories of digital evidence as per standards/ISO; analysis of deleted and active files; location and analysis of data in ambient data sources; recovery of deleted or encrypted data/emails, SMS, MMS, videos, internet sites; uncovering passwords; forensic SIM card analysis; extraction of data from mobile phones and lastly, presentation of expert forensic evidence in court.

With such facility in place, court cases are backed by well documented evidence, enhancing chances of successful prosecutions for cybercrime culprits. With such development in cybercrime activities in Kenya, the use of available and mostly used mobile forensic software tools like Cellebrite UFED, Forensic Toolkit (FTK) - Access Data, FTK Imager, Oxygen, XRY, EnCase and MOBILedit, which rely on a rooted device to extract more data are used to carry out investigations.

According to a study by Lessard and Kessler (2010), major challenges came from the plethora of Android phones available on the market today as well as scarcity in hardware, software, and interface standardization within the forensic industry to carry out forensic examinations. Also, the high cost of commercial forensic tools resulted in forensic examiners using freeware tools with limited features. These difficulties were also experienced as a result of the wide range of media on which data is stored, disparate operating system, file systems and the effectiveness of forensic toolkits.

1.2 Statement of the Problem

Throughout the study, of great concern were issues raised on data integrity during the forensic investigation process, hence the need to understand data integrity issues caused by rooting of an Android device. According to research by Votipka, Vidas and Christin (2013), in their research to collect forensic data on Android devices; they claimed that their process had an intention of obtaining close to an ‘exact copy’ of data sets.

They acknowledged that during their interaction with the device, they altered its state in a way. During normal device operation of a phone device, data is continuously written to and
deleted from the memory. The atomic collection of a comprehensive copy on an active device therefore meant that the resultant image would be composed of data collected through various states of memory. An example would be that in the midst of a sequential copy operation, data would be orthogonally moved from the end of memory to the beginning. This would mean that the resulting data may not appear in the resultant image. Such an image would complicate analysis and or fail to represent a set of data that is valid for the device.

This research aimed to explore software flaws as a result of the rooting process since the process leveraged on the software versioning and rooted devices. The flaws were as a result of improper rooting technique which resulted in unreadable data formats. Votipka et al. (2013) also noted that it was hard for the investigator to reveal the software version running on the device when it was locked. Depending on the type of the rooting process used, this argument seemed to be remote, given the current advancement in forensic technology as well as the plethora of rooting applications available on the market.

In their study, Votipka et al. (2013) also noted that through the rooting process, some partitions of the device storing user data may be altered in a way. Indeed, this might have been true simply because if the procedure was wrongly done, it may have led to some data being changed or altered, leading to forensic data integrity issues. Also, Android security model may have been compromised due to the easy escalation brought about by the process of rooting an Android phone. This was a contentious issue because it depended on the procedure followed and the tools used to carry out the exercise. This research aimed to shed light on such gray areas by making relevant solutions towards investigating the impact of rooting an Android device on the integrity of data.

The scholars also suggested a methodology of physical data extraction using a custom recovery mode without essentially the necessity for root access methodology (Votipka et al., 2013). This methodology also seemed to be remote since newer phones, especially those released after their research have their boot-loaders locked. This therefore meant that there needed to be a mechanism that has the ability of wiping the device to unlock the boot-loader, and rooting was able to achieve this. Also, some of the current forensic tools have techniques that were able to physically and logically extract data in a forensic sound manner, sometimes without granting root access.
Lack of sound process models was seen as another major challenge in the mobile investigation as most of the earlier studies concentrated on computer based process models (Votipka et al., 2013). Others included inadequate interface standardization within the industry to carry out forensic examinations, a variety of media on which the data was stored, disparate operating systems and the effectiveness of forensic toolkits that guarantee data integrity.

Forensic problems are varied in nature, but in developing worlds like Kenya, most are due to lack of sound forensic frameworks governing cyber evidence. Through the Kenyan National Assembly, the government of Kenya introduced The Computer and Cybercrimes Act (2017) which focused on computer use and misuse and made several inputs on matters forensics. Part 2 on Offences has Section 14 which focuses on digital systems misuse; and Part 3 section 27 on Investigation Procedures which focuses on conducting forensics as well as data integrity issues. The act generalized some of the issues found within the forensics world, and the enhanced framework seeks to strengthen some of the vague issues raised in the act by solely focusing on smartphones forensics.

Another piece of study by Do et al. (2015), ascertained that strictness and standard were key in the investigation of Android mobile related crimes. The authors felt that the rapid technological development coupled with the prevalence of Android mobile devices posed challenges for investigators and law enforcement agencies. They proposed a model, although they acknowledged that the process of injecting a piece of code and alteration of application execution introduced errors hence jeopardized data integrity.

To curb against such issues, the research critically reviewed literature related to rooting, data integrity as well as Android forensics process models. The research went ahead to identify the gaps and where possible combined phases of earlier proposed models. The research built an enhanced model that guaranteed collection of forensic sound data from Android smartphones and ensured data integrity was maintained. This facilitated submission of forensic sound pieces of evidence in a court of law.

1.3 General Objective

The general objective of this study was the development and evaluation of an enhanced forensic framework for Android smartphones with a key focus on ensuring data integrity of forensic evidence was retained.
1.4 Specific Objectives

i. Explore rooting techniques and the impact on data integrity on Android smartphones.

ii. Explore forensic frameworks and develop an enhanced forensic framework for rooted Android smartphones.

iii. Extract, examine and analyze data to validate the enhanced forensic framework.

1.5 Significance of the Study

According to Kenya National Crime Research Centre (2018), endemic crimes like forged fraud in electronic commerce, illegal electronic surveillance, obtaining money fraudulently, hate speech or messages and incitement were being perpetuated using mobile phones. The act further stated that “A person commits an offence if they send a message or other matter that is totally offensive, indecent, obscene or of ominous character; or one that they know to be false for causing irritation, inconvenience or needless anxiety to another.”

The Communications Authority of Kenya (2017) instituted regulatory policies like requiring all mobile subscribers to register their SIM cards. However, this charge still faces security loopholes to be addressed. For example, enforcing the policies is a challenge both to the service provider and the government due to inadequacy of relevant laws and regulations. The major problem was that it was hard to acquire data from a culprit’s phone and even if this succeeded, the data became inadmissible in the court of law due to lack of data integrity. This was because of questionable methods used to acquire data from the phone, and inadequacy of proper digital forensics frameworks to guide the forensics process.

Based on this background, the research set out to explore issues of rooting Android devices to obtain more digital evidence that meets integrity through technology factors, forensic processes and frameworks that guided the process. An endeavor was made to investigate the impact of rooting an Android device on data integrity as well as development and evaluation of an enhanced framework that provided guidance in digital forensics processes, particularly in developing countries like Kenya where Android phones are prevalent.

The research could be used as a blueprint for further research on investigating the impact of the rooting process on the integrity of data acquired by use of forensic tools. The research
could also help to determine whether the current digital forensics technologies and frameworks adequately address the issues of user data integrity.

1.6 Scope of the Study

A proper digital forensic process offers greater opportunities including timeliness and accuracy thus aid in overcoming inadmissibility of digital evidence presented before a court of law. Therefore, the scope coverage of this study revolved around experiments with an aim of investigating the impact of rooting Android devices on user data integrity.

The forensic examination included an assessment on data integrity, issues raised by the procedure of rooting an Android phone, digital evidence procedures and frameworks in place for data extraction and analysis. Generally, the scope of this study was confined to mobile phones that use the Android operating system. This process was limited to an experimental implementation of the proposed framework with an aim to be evaluated and practically used in the market. Forensic tools being costly, we scoped the implementation to MOBIedit Forensic Express tool that allowed the examiner to extract, examine and analyze forensic data for consideration of evidence, hence validating the proposed process model. KingoRoot was used for rooting the three test devices which had been in use for over four years. The implementation focused on examination and analysis of documents, images, messages and web browsing history found within the file system.

1.7 Definition of Terms

**Acquisition:** Acquisition is the process of imaging or otherwise obtaining information from a mobile device and its associated media (Ayers, Brothers, & Jansen, 2014).

**ADB:** ADB is command line tool provided by Android SDK to interface an emulator or communicate an android device with client server basis (Shahbaz et al., 2016).

**Android:** An open source operating system based on Linux kernel and launched by Google (Liu & Yu, 2011).

**Bootloader:** The first thing that runs on booting an Android device. It packages the instructions to boot operating system kernel and most of them are specifically designed to run their own debugging or modification environment (Votipka et al., 2013).
CID: Criminal Investigations Department which is a body under Kenyan National Police Service that deals with criminal investigations (Directorate of Criminal Investigations of Kenya, 2015).

Communications Authority of Kenya - Regulatory authority for communications (Communications Authority of Kenya, 2017).

Data Integrity: Assurance and maintenance of the consistency and accuracy of information over its entire life-cycle (Do, Martini, & Choo, 2015).

Digital evidence: Probative information stored or transmitted in digital form that a party to a court case may use at trial (Son et al., 2013a).

Examination/Analysis: The examination process that uncovers digital evidence, including that which may be hidden or obscured (Ayers et al., 2014).

Forensics: Scientific knowledge and methods applied to the identification, collection, conservation, examination, and analysis of information stored or transmitted in binary form in a manner acceptable for application in legal matters (Casey, 2011).

Hashing: The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data (Ayers et al., 2014).

iOS: Mobile operating system created and developed by Apple Inc. exclusively for its hardware (Votipka et al., 2013).

Jailbreak: Privilege escalation for the purpose of removing software restrictions imposed by Apple Operating System (Apple iOS) (Votipka et al., 2013).


Playstore Protection: A built-in malware protection for Android that ensures safety of the device through blocking application deemed to be harmful (Lohrum, 2014).

Rooting: Enabling users of Android mobile operating system to attain privileged control (root access) over various Android subsystems (Votipka et al., 2013). Attained through USB debugging to allow sending commands from the computer to the phone.
1.8 Chapter Summary

Chapter one presented a general background of the research that had a basic emphasis on development of an enhanced Android forensic framework. The consideration of Android smartphones was due to its exponential growth from 1.6% to 85%, from 2009 to 2018. This showed that Android devices could be misused leading to criminal and other legal concerns. Forensic investigations have addressed some of the concerns but of concern was data integrity issues as a result techniques used to acquire the forensic evidence. An example is the rooting process with the aim to gather more evidence. The research aimed to develop and evaluate an enhanced forensic framework for Android smartphones. This was made possible by first exploring existing rooting techniques and their effects on data integrity, exploring existing forensic frameworks and develop an enhanced forensic sound framework for rooted Android smartphones, finally by extracting, examining and analyzing forensic data form the Android smartphone to validate the propose framework.

The research revealed itself as important in solving problems at personal, community and corporate levels. According to Kenya National Crime Research Centre (2018), endemic crimes like forged fraud in electronic commerce, illegal electronic surveillance, obtaining money fraudulently, hate speech or messages and incitement were perpetuated using mobile phones. Theses offenses could willfully be solved by employing a forensic sound model in the investigation process. The research included a thorough examination of extracted data from Android phones which should undergo a rooting process to allow access to more data in the phone operating system. To make evidence admissible in a court of law, the obtained data was assessed to determine data integrity status that could be influenced by the procedure of rooting Android smartphones.
Chapter 2: Literature Review

2.1 Introduction

Jaidka, Khoo and Na (2013) defined literature review as “specific sets of research papers which are commonly related in nature”. It selects information from the papers and arranges them into a logical justification for the author’s research. They are basically written by researchers or scholars who peruse through previous studies with an aim of identifying research gaps or research problems and to place their work with an intention of filling the gaps of the said previous studies.

Chapter two discussed various studies done by scholars on best techniques of rooting an Android mobile phone, performing data extraction from a rooted Android phone and forensic analysis techniques as well as analysis of the extracted data and verification of its integrity, or the lack of it. The research explored Android mobile forensic frameworks that were intended to guarantee forensic sound data from Android mobile phones. It briefly discussed on Android architecture, its security and data acquisition in Android devices. The chapter also analyzed several forensic frameworks with certain features.

2.2 Theoretical Foundations

Mobile communication has become one of the most sought-after service as characterized by proliferation of digital devices and systems around the globe. Because of the basic, helpful, advantageous and universal nature of Android cell phones, it is gradually getting to be plainly less demanding to convey and to a degree make a ‘virtual town'. Due to the simple, handy, convenient and ubiquitous nature of Android mobile devices, it is increasingly becoming easier to communicate and to an extent create a ‘virtual village (Ayers et al., 2014). This has helped to drive the economy due to reduced operational costs, efficiency and convenience of carrying out tasks that were never driven by technology.

Nevertheless, the advancement and popularity of these technologies raised a myriad of societal issues regarding the usage of mobile devices to commit digital crimes like terrorism, drug trafficking and money laundering. According to Kenya National Crime Research Centre (2018), there have been reports on the use of phones to commit other
criminal activities like fraud, hate speech/messages, incitement, cyber stalking, forgery, harassment, illegal spreading of pornographic materials and theft among many others.

According to the report, the increase of such criminal activities has placed a strain on governments’ law enforcement and private agencies to curb the menace through identification and prosecution of culprits. As the use of mobile devices for criminal activities continues, so must the mobile forensics frameworks help the law enforcement agencies. This may be through providing forensic data or digital evidence acquired to prosecute criminals. This is usually after carrying out forensic examination of evidence on the culprits’ phone. Through digital forensics, there are endeavors to identify the unwanted events carried out by the mobile device and acquire the necessary evidence in a forensic sound manner that can support a lawsuit.

Recent trends in increased digital crime indicate that developing countries have not derived the expected benefits from digital forensics. The Computer and Cybercrimes Act (2017) has put in place a measures to resolve some of the myriad challenges that come with the use of technology. Also, there may be doubts about how digital forensics will be a business enabler in developing countries like Kenya as we embrace digital economy thus the need to understand digital forensics processes and its practices to resolve the problems of digital crimes as a result of proliferation of digital technology systems.

The activities involved in collating evidential data from mobile devices must take cognizance to the laid down standards, frameworks and procedures as required by law. Forensic soundness is in some way not clear as argued by Casey (2011). The author stated as follows: “Setting an absolute standard that dictates 'preserve everything but change nothing' is not only inconsistent with other forensic disciplines but also is dangerous in a legal context. Conforming to such a standard may be impossible in some circumstances and, therefore, postulating this standard as the 'best practice' only opens digital evidence to criticisms that have no bearing on the issues under investigation”.

Android mobile devices can potentially contain vast amounts of information such as files, software, text messages, images, video and audio recordings which are related to the user’s activities and their communication patterns. Such devices could be used for heinous acts which may open cases of prosecution, hence acquiring data from such devices in a sound forensic manner that meets data integrity is a very important issue.
According to Barmpatsalou, Damopoulos, Kambourakis and Katos (2013), data on a mobile phone can be found in many locations like the Subscriber Identity Module (SIM card), the phone’s embedded memory and the phone’s removable memory, also known as Secure Digital card (SD card). The SIM card may contain information such as the International Mobile Subscriber Identity (IMSI), which is the SIM card’s globally unique identifier; language preferences and network (service provider) information; currency information, such as call charge counters; information about the current (or most recent) location of the mobile phone; phone book entries; sent and received SMS messages; and recently dialed numbers.

Data stored in phone memory may include phone settings; calendar information; Multimedia Messaging Service (MMS) and Short Message Service (SMS) messages; call log entries; time and date; ring tones, audio, video recordings and images; generic data stored in the phone’s memory and application executable. Data stored by the service provider includes subscriber information, location information, call and billing information (Barmpatsalou et al., 2013). Whenever a call is made, or a text message is sent, a ‘call data record’ is created and stored, containing, amongst other information, the sending and receiving phone numbers, the length of the call and the initial and final location of the two parties. This information is available and stored by the service provider hence it was not discussed as it was outside the scope of this project.

2.3 Rooting Android Smartphones and the Impact on Data Integrity

Patil, Sharma, Sharma, Chhaparwal and Chowdhari (2017) described rooting as a process of attaining privileged control of your device by granting super user permission to Android sub system. The vendor specific limitations set by hardware manufacturers can be overcome by rooting. The procedure supersedes Android security features that usually disallow collection of data within a phone’s storage memory dumps.

2.3.1 Understanding Android Architecture

Android is an open source mobile operating system that has grown to be one of the most usable operating system for mobile phones. The operating system boasts of a Linux kernel which many have deemed to be well secured. It was important to note that with the current upgrades and enhancements, it still faces security threats. The stock version of the operating
system provided by the device manufacturer limits the root access to the users and it is a well thought security threat prevention scheme.

According to Pal, Das and Anand (2014), the Android architecture has the Linux kernel that consists of the following key features: Wi-Fi driver, Audio drivers, the display driver, the camera driver, flash memory driver, Inter Process Communication driver, Keypad driver, and Power Management. The device may become unusable if any of the aforementioned drivers get affected.

Android applications consist of an anti-virus application which is usually used to protect it. This may not be the case if the Android device is rooted. This is because the procedure opens flawless access of the root-files and the kernel to the user. In such a case, any application installed by the user will get the access to the root files. In such a scenario, the rooted device becomes seriously vulnerable to security threats and the user must be very careful about the applications they decide to install (Pal et al., 2014).

If the investigator does not root the device correctly, it may lead to bricking the device and even render it unusable. Bricking would mean that a device is not recoverable through normal means and or that it is damaged (e.g. damaged baseband memory). This may require the investigator/user to re-root the phone and install a new bootloader. Thereafter, they can install the operating system, a procedure that may cost them to lose all data. Pal et al. (2014) illustrated the Android architecture as shown in Figure 2-1.
2.3.2 Rooting Android Smartphone

Pal et al. (2014) suggested many ways to root an Android mobile device by incorporating various software tools and procedures. The aim of rooting was to provide complete access of the root files/folders to the users, hence making the user, or an investigator in this case, a Super User. Rooting process allows complete control over the look and feel of the device being investigated. It is mainly done to gain full application control hence ability to backup, restore, batch edit applications and also remove bloatware that comes pre-installed on Android phones; to gain full control of the kernel, allowing overclocking and under-clocking the CPU and GPU; to custom automate system-level processes by using third-party applications and also, install a custom firmware (custom ROM) and software that allows additional levels of control on a rooted device.

According to their research, if a user or investigator rooted a phone that was under warranty period and runs into an error as a result of the rooting process, the user would lose the warranty. In some instances, the user/investigator may use these tools to un-root their devices and the manufacturer would never know that the device had gone through a rooting procedure.
The author also considered a more complicated methodology to perform rooting. He suggested a procedure to manually flash the mobile devices using flashing tools. Thereafter, he proposed to install zip files from the recovery mode of the devices and then get root access (Pal et al., 2014). The procedure required one to remember that to perform these operations, the boot loader of the device being investigated be unlocked. This steps to be encountered in the process of rooting varied from one device to another. The author noted that although the process varied, exploitation of security bugs in the stock Android OS remained the same in all the processes.

The authors stated that after exploitation of the security bugs in Android, a custom recovery image is flashed which bypasses the digital signature check of the stock firmware updates. Thereafter, a modified firmware update can be installed from the recovery menu which classically includes the utilities essential to run applications as root. The firmware updates can be a customized Android operating system. The updates are normally compressed into a single file with a .zip extension. This zipped file (.zip) is stored on an external drive or a secure digital memory card (SD card) (Pal et al., 2014).

The author noted that when the user enters the recovery menu, they must clear cache partition and Dalvik Cache. This is usually done from inside Advance menu. They then select “install .zip from card” and this will show the .zip file to the user. When selected, this prompts the installation process, and during this time, the user must keep the mobile device charged to not less than 80% battery level (Pal et al., 2014).

At the time of the installation, all the processes including the power management feature from the kernel is replaced with the kernel of the customized operating system. At this time, the mobile device in use does not charge its battery even though it has been connected to a source of power. Upon successful rooting of the device, several customized operating systems can be installed any number of times. The authors insist that during this period, no rooting process must be performed unless the device has been un-rooted.

Before starting the rooting process, it is advisable that the user installs the drivers of the device in the computer. Failure to install the drivers will lead to the computer not recognizing the device and as a result the flashing tool will fail to flash the file (Pal et al., 2014).
Pal et al. (2014) reported that for rooting a Samsung device, a tool called Samsung Kies was paramount. The special tool allowed connection of a Samsung phone to a computer as well as synchronized data between devices. It also included the required drivers for the Samsung device. The user needed to install a tool called Odin which is the flash tool for Samsung Devices. Odin gives users the opportunity to flash the recovery menu along with the Super-User app which is used to root the device. There is extra option named “Advanced” in the recovery menu after exploiting the stated features. The advanced mode allows the user to clear the Dalvik Cache partition and install the customized operating system (.zip extension) from the SD card. The user must copy the customized OS on the SD card before starting the rooting operation. The entire process is likely to take ten to twenty minutes (Pal et al., 2014).

Gupta, Bhardwaj and Garg (2015) presented a specific technique of rooting as using Odin tool. According to the author, using Odin may render applications not to work correctly in case the device was improperly rooted, or if the phone is not supported. The tool may damage the kernel and result in a lot of bugs in the device, for example the phone may keep rebooting and/or freeze at the start up screen.

Another noticeable piece of work was a study by Patil et al. (2017) where they described the steps of the rooting process that included downloading and installing KingoRoot; enable USB debugging; tap settings, developer options and tick the box for “USB debugging”; Tap OK to approve the setting change; Run Android Root on PC; connect phone via its USB sync cable. The device screen may show an "Allow USB debugging?" pop-up. Here, tick "Always allow from this computer," and tap OK. Thereafter, Click Root and let the utility do its work. The process can be reversed, run Android Root again, connect phone, and then click Remove Root.

2.4 Forensic Frameworks for Smartphones

The prime focus on forensic soundness lies in the process of ensuring that all actions are carried out in a strict manner (Do et al., 2015). Through their study, the authors presented two levels of forensic soundness as follows: Strict and Standard. Strictness to forensic soundness ensured that no errors were introduced. This could be in form of modification of data presented as evidence. Standards included actions that were to be documented as part of standard forensic reporting procedures.
The researchers reported that a forensic examiner or investigator with a sole objective for a strict level of forensic soundness must put in place controlled opposing capabilities. The researchers noted that a strict adherence to forensic soundness ought to have been carried out within the initial stages in any forensic investigation. The objective of this was to reduce any form of modification of evidence sources which would have led to lack of data integrity.

The authors Do et al. (2015) proposed a forensic framework with focus on forensic soundness. The framework was based on best measures and steps, coupled with methodologies to be followed for a forensically sound physical extraction of data on Android devices. Their research adopted the forensically sound investigator model for mobile devices. The framework lightened on key features to be observed during the rooting process as well as a physical data extraction.

The framework according to Do et al. (2015) envisioned forensic soundness by satisfying the following key criteria:

**Meaning**: The evidence or data that was collected ought to have maintained its originality and interpretation. There should be no change at all on user data since this would have resulted to data corruption, or rather led to the data losing its original meaning thereby impacting on data integrity.

**Errors**: In the event that an error occurred, and it was identified, there was need to have the ability for an explanation, or rather a justification that the errors had not affected the validity of the data. This comprised the installation of third party tools, for instance Android rooting tools on the target device. A clear explanation was to be made and explicitly documented to show that the application software tools did not in any way change or alter the user data.

**Transparency and trustworthy**: This aspect emphasized the need for a court of law to validate data integrity by undertaking an oversight that was independent of the forensic process used. The explanation was that this ensured that if a second opinion is sought by a court of law, the device on which the physical extraction was carried on produced the exact results.

**Experience**: The investigator or examiner carrying out a forensic investigation must have had the necessary qualifications and experience to guarantee that the findings presented could be relied upon.
The authors introduced a model specific for mobile forensic data collection and analysis. Their model was reported to have the aptitude to physically access a mobile device as well as capabilities to exploit device security vulnerabilities. The model was to obtain data considered to be confidential from a target device. This was to be done within the constraints of forensic soundness as proposed by (Do et al., 2015).

The capabilities of the framework were as follows:

Corrupt the target device by allowing the forensic examiner or investigator to take control of the target device and be able to discover the internal state or architecture of the test device. The authors noted that such functionality should be constrained to purposes that do not present errors to the device. The typical example of the errors was modification of evidential data sources leading to loss of data integrity.

Delete target device data where the investigator was constrained to activities that did not result in the introduction of errors. Such would be deletion of operations on evidential data sources.

Encrypt or decrypt target device data whereby the forensic investigator was permitted to encrypt or decrypt messages from the target device with a special key. The authors noted such a strict application of forensic soundness criteria did not affect the capability and functionality of the device. Their argument was based on the knowledge that the procedure operated on data that had been collected (forensic copy), rather than evidence source data.

Exploit the target device through incorporation of a script or a software application. The forensic soundness was maintained as the capability was restricted to functions that in some way did not lead to the introduction of errors.

Forensic copy whereby a physical image of the target device was produced with the capability to reserve the forensic soundness by avoiding errors. Thereafter, forensic examination and analysis of the data collected, and the true meaning of the data was maintained. This was followed by a process called inject. In the procedure, a piece of code was infiltrated on the target device. The framework noted that forensic soundness was maintained by avoiding introduction of errors to the target device.

Listen capability whereby the forensic investigator passively monitored a communication channel on the target device. This capability was applied with consideration for the
requirement to obtain data with a known meaning. The procedure also guaranteed that errors in collection were identified and circumvented. The process for interception was thereafter subjected to a transparent review.

Modify which included alteration of an application execution on the target device was performed. The example by the authors was modification of an existing message or data. The investigator later on replaced the device configuration. The capability was constrained to functions that did not introduce errors or result in a loss of transparency and trustworthiness or meaning.

Transmit which includes the investigator transmitting a message from the target device, an SMS message. The capability was applied with consideration for the requirement to transmit data with a foreknown effect (meaning). It had same outcome as the listen capability with guarantee that errors in transmission were identified and avoided. The process for transmission was also subjected to a transparent review.

The framework briefly outlined the forensic process flow on Android evidence collection and analysis. After the identification and preservation of the target mobile device, data collection was commenced. The forensic process began with the configuration of the Android bootloader. In Android, a bootloader runs on booting up an Android device and packages the instructions to boot an operating system kernel. The bootloader was set up to enable booting in the download mode of the device. The booting of the recovery image of the device was used to collect the physical image of the partitions of the device (Do et al., 2015). The collected physical image was thereafter processed for the purposes of analysis of the relevant data or information under investigation. The investigator prepared a forensic report that included the procedures that were used, and thereafter presentations were done (Do et al., 2015). The framework’s forensic process flow is shown in Figure 2-2.
Through his forensic framework, the author recommended two key measures to be observed during physical acquisition of forensic data from Android mobile phones:

*Adherence to standards and guidelines:* With the sole aim of preserving the integrity of the data and the whole forensic process, it was significant for the agreed standards and guidelines provided for digital forensics to be followed and observed. The researchers touched on ISO standards like the ISO/IEC 27041:2015. These standards provided good practice methods and processes for evidence acquisition and the investigation of the captured digital evidence (ISO, 2015).
Trained examiner: As fashioned by the Association of Chief Police Officers (ACPO) principles of digital evidence, principle number two directed on competent personnel handling original evidence (Goel, Tyagi, & Agarwal, 2012). The authors reported that computer forensics experts must adhere to the (ACPO) good practice guide for computer based electronic evidence. Based on rule number two, the forensic process should only involve qualified personnel capable of carrying out such activities. The personnel should understand the forensic process and document all the processes and actions they have undertaken in the acquisition of the evidential data.

Other standards have been developed to guide forensic examination profession. According to Association of Certified Fraud Examiners (2018), basic principles of ethical behavior to guide members in the fulfilling of forensic duties and obligations can be suggested as follows:

Standards of Professional Conduct: Integrity and Objectivity; whereby examiners ought to conduct themselves with integrity, knowing that public trust is founded on integrity. They acknowledge that examiners should declare any potential conflicts of interest in the case and exemplify the best interests of the reputation of the profession and not falsify any evidence. Professional Competence; whereby examiners should not accept assignments where competence is lacking and strive for professional education required by the Association of Certified Fraud Examiners; Due Professional Care where examiners shall exercise due professional care in the performance of their fraud examination services diligently with critical analysis; Understanding with client or employer by reaching an understanding with those retaining them (client or employer) about the scope and limitations of the fraud examination and the responsibilities of all parties involved; Communication with Client or Employer through communicating to those who retained them (client or employer) by giving significant findings made of the fraud examination; and Confidentiality by not disclosing privileged information obtained during the course of a fraud examination without the express permission of a proper authority or the lawful order of a court.

Standards of Examination: Certified Fraud Examiners should conduct their work in a legal, professional and thorough manner and establish predication and scope priorities at the outset of a fraud examination, and continuously reevaluate them as the examination proceeds; and Evidence where CFEs shall endeavor to establish effective control and
management procedures for documents, data and other evidence obtained during the course of a fraud examination.

Standards of Reporting: Generally, fraud examination reports may be oral or written, including fact witness and/or expert witness testimony, and may take many different forms. There is no single structure or format that is prescribed for a CFE’s report; however, the report should not be misleading; and Report Content shall be based on evidence that is sufficient, reliable and relevant to support the facts, conclusions and recommendations related to the fraud examination. The report shall be confined to the specific subject matter, principles and methodologies within the member’s area of knowledge, skill, experience, training or education.

Research by Votipka et al. (2013) established a general methodology for collection and analysis of physical memory dumps from smart devices running the Android operating system. They aver that their study was performed in a forensically sound manner with the aim of maintaining data integrity. The model is as shown in Figure 2-3.

![Figure 2-3: Forensic Collection Process Model (Source: Votipka et al. (2013))](image)

The investigator created a collection software for the device. The phone device was rebooted into a special flash mode and used a manufacturer-specific tool to transfer the collection software to the device. Thereafter, the device was rebooted into recovery mode that went ahead to execute the collection software. The device was connected to a computer using a USB cable and the Android Debug Bridge (ADB) software. Data was duplicated to the computer using a collection software.

The authors claimed that any data omitted or corrupted during collection may lead to lack of the integrity aspect. This could lead to an investigation being jeopardized after analysis has been done. For the initial purpose of meeting forensic soundness and data integrity, the authors affirmed that the methodology being used must adhere to a certain criterion. Their applicable methodology to any forensic collection was reported as follows:
Data preservation which involved total and complete data on the device being collected. This included metadata and memory areas that were thought to be deleted or empty. The next factor to be considered was atomic collection. Data is continuously written to and deleted from the device memory. This is usually done at the point of normal device operation. In the event of obtaining a comprehensive copy on an active device, the resultant image is usually composed of data collected through various states of the device memory.

Correctness was another criterion that was used. The chosen procedure must account for accurate collection of data from the device memory in use as well as accurate transfer to the target destination. Another factor was determinism. The process used in data collection ought to be repeatable in nature and produce some level of expected output/results.

Another criterion to be considered was evidence preservation. The procedure used in data collection should not physically alter or damage the functioning of the device. Preservation of physical evidence is very key to ensure that collection can be repeated if need arises. This ensures the correctness and determinism of the process undertaken.

Usability was another key factor. The procedure used must be easy to use because it is intended to be used largely by different practitioners. Vetting ability was another criterion whereby it is a requirement that the specific software applications or tools and techniques used for collection should meet a certain verification threshold. At the least, they should have been sourced from a trustworthy source or market.

The last factor was to be considered was reproducibility. In case of a device on which no data extraction or collection process has never been performed on previously, collection on the device should be possible with minimal effort.

Lessard and Kessler (2010) proposed a specific procedure for acquiring evidence from Android NAND flash. Theirs was purely a physical data acquisition which was done through a bit for bit copy of the NAND flash. The physical extraction was able to allow for the obliterated items to be recovered. The process required the device to be rooted to enable the operation of a ‘dd’ image of the partitions and there after being stored on an attached Secure Digital card of the device. The dumps were then analyzed to look out for any important evidence. The challenge it posed was that it required the device to have an SD card slot, which meant that mobile phones without slots would not have been investigated using the methodology. The process followed was that of acquiring physical evidence from
a rooted HTC Hero phone and it did not have a specific framework, but rather certain procedure to be followed. These were acquiring a physical image of the Android device; connecting the device via a data cable; imaging the memory card; rooting the device in order to obtain a dd image; creating a dd image of the memory; examination of memory; analysis with the Cellebrite and finally the author presented the results.

A study by Goel et al. (2012), proposed a fourteen-stage smartphone forensic process model by exploring the various procedures undertaken in a forensic investigation of a Smartphone. The model was proposed as one of effective ways of investigating a smartphone to find potential evidence. Their model was developed to serve as a benchmark and reference point towards investigating smartphones criminal cases. The model provided a generalized solution to the rapidly changing and highly vulnerable digital technological scenario.

Their paper presented an overview of previous forensic strategies as well as the difficulties being faced within the smartphones forensics domain. The proposed model explored the diverse processes involved in the forensic investigation of a Smartphone in fourteen stages. The Smartphone Forensic Investigation Process Model (SPFIPM) was aimed at showcasing effective techniques to investigate a Smartphone. The model is illustrated in Figure 2-4.
**Preparation:** Understanding of the nature of the crime and activities; including getting tools required for the investigations, accumulating materials for packing evidence sources, building an appropriate team assigning roles to each personnel.

**Securing the scene:** Prevent contamination and corruption of evidences and security of the crime scene from unauthorized access with the aim of protecting the integrity of potential pieces of evidence.

*Figure 2-4: Smartphone Forensic Investigation Process Model (Goel et al, 2012)*
Documenting the scene: To maintain a proper chain of custody and circumstances surrounding the incident (log of those who were present on the scene, those who reported afterwards, and those who left).

PDA Mode: The state of device in which it is working in should not be changed. An example given was that when the phone is in Active Mode there was need to shield it from external network and further communication without changing its mode so that the potential vulnerable volatile evidences remain intact. The device was moved to Communication Shielding phase before working further. “When the device is switched off, it is in Inactive or Off mode. Since we want to keep the evidences intact, it is not advised to turn the device on because this may lead to overriding of old data with new data. Thus we can continue with phase six and can skip communication shielding” (Goel et al., 2012).

Communication Shielding: Blocked the further communication options on the test devices hence ensured overwriting of the existing information on the devices was not done.

Volatile Evidence Collection: Volatile evidences were prone to destruction as the device state and memory contents may change hence needed to be collected.

Non-volatile Evidence Collection: Evidences were extracted from external storage.

Off-Set: Advancement in cloud computing and offset storage technologies led to consideration of the phase since there was a possibility of hiding criminal evidence online which was not easy to track from device easily.

Cell Site Analysis: Pinpointed the specific position of the mobile phone at the time of the crime via location of the geographical area.

Preservation: Ensured the safety of evidences through proper packaging, transportation and storage.

Examination: the model aimed to resolve and sort out the case by critically examination of the evidences collected. This involved data filtering, validation, pattern matching and searching for particular keywords with regard to the nature of the crime or suspicious incident.

Analysis: Identifying relationships between fragments of data, analyzing hidden data, determining the significance of the information obtained from the examination phase, reconstructing the event data, based on the extracted data and arriving at proper conclusions
etc. are some of the activities to be performed at this stage. This stage constitutes the technical review of the investigators on the basis of the results of the previous examination stage of the evidence.

*Presentation:* Presented results to the wide variety of audience including law enforcement officials, technical experts, legal experts and corporate management.

*Review:* Reviewed investigation steps and identified areas of improvement. Results and interpretations were used for further refining the gathering, examination and analysis of evidence in future investigations.

The model included key processes to be carried out when conducting smartphone forensics. It also tackled issues regarding the advancement in technology by looking for more efficient evidence sources in smartphones. “The model facilitates mode selection/shielding, off-set/online storage and cell site analysis which were otherwise not supported in the rest of the models making it more effective and versatile for evidence management” (Goel et al., 2012).

### 2.5 Data Extraction, Examination and Analysis for Framework Validation

#### 2.5.1 Data Extraction

There are two methods for retrieving data: Logical extraction and Physical extraction. Logical extraction has shown to be easier and less time-consuming, although it has been reported to return less information. Physical extraction is more difficult and takes much longer, but has a greater return of hidden or deleted information, (Son et al., 2013b).

In logical extraction, the extraction tool communicates with the device using its own programming language, which is available from device vendors and comes pre-loaded into the forensic tool. Logical extractions will not recover deleted files, and the process cannot be performed on locked or password-protected devices (Son et al., 2013b). Physical extraction may be thought of as the post-mortem acquisition process of computer forensics. A physical extraction will create a bit-for-bit replica of all of the data contained within the mobile device, including hidden and deleted files. Physical extraction of cell phone data leaves no signs an investigation occurred after the extraction is complete.
However, Casey (2011) added that in case a full copy of physical memory is not possible, for many devices the complete logical file system could still be acquired. The author noted that this generally does not include deleted items, it can still provide access to substantial digital evidence including MMS messages, IM fragments, and Web browsing history that are not displayed automatically by forensic tools. In case of such scenarios, the forensic examiners must locate the desired information within the file system and interpret it themselves. It is generally important for investigators to have an understanding of the underlying technology and not be overly reliant on automated tools.

A study by Patil et al. (2017) stated that data extraction can be achieved by Android debug bridge (ADB) as follows: when adb is started, it checks if there is an adb server process already running. If there is none, it starts server process. When server starts it binds to local TCP port 5037 and listens for commands sent from adb client, all adb clients use adb clients use port 5037 to communicate to adb server. The steps followed when extracting data using ADB, adb devices (gives the device model and ID), adb root (runs the adb daemon in root), adb pull <source file path in Android sub>, <destination path in development machine>.

Lessard and Kessler (2010) in their study proposed a methodology for acquiring from Android NAND flash all the data. In their methodology, the data acquisition was through a bit for bit copy of the NAND flash which allowed for the obliterated items to be recovered. To perform this process, it needed the device to be rooted to enable the operation of a ‘dd’ image of the partitions and there after being stored on an attached SD card of the device. The dumps were then analyzed to look out for any important evidence. The challenge it posed is that it required the device to have an SD card slot, therefore, mobile phones without slots may not have been investigated using this method.

Lohrum (2014) came up with methodologies of obtaining a physical image of the device memory. In his step by step procedure, he used the dd command on an Ubuntu Linux operating system as exemplified below:

Installed busybox application on the device from Playstore. On the terminal, checked that the device was connected to the computer with the command; adb devices. Got into the device’s shell with command; adb -d shell. Typed su command to gain root access. Opened another terminal session and navigated to the location where the image would be saved, in the terminal, the command adb forward tcp: 8888. On the other terminal with the shell to
the phone, the command dd if=/dev/block/mmcblk0 | busybox nc -l p 8888. This command enables the contents of /dev/block/mmcblk0 (the head block of my device) to be read and subsequently being written via port 8888 across adb using netcat. The last step, on the shell to the computer, the command: nc 127.0.0.1 8888 > device_image.dd was typed. This command enables saving the output of the contents across port 8888 to the file device_image.dd.

Chen, Yang, and Liu (2011) suggested that physically acquired data from an android device presented a procedure that doesn’t modify the device, in that the recovery mode of the Android device used in this process uploaded their own “update.zip” package on an external SD card. The package was then executed and run like a root process, and during the execution process, a physical data acquisition on the Android device was carried out and the dump stored on the external SD card. One of the challenges associated with this methodology was its reliance on the Android device’s recovery partition being flashed with a third-party recovery mode. The unlikelihood of this was that the flashing of the software was to be done manually by a user to enable them to unlock the boot-loaders.

Son et al. (2013) proposed a notable piece of fact in data acquisition whereby in their piece of work, the authors’ approach was by use of custom recovery mode that would be flashed on the boot partition. In doing this, the device will not be able to boot in the original Android operating system. In their suggestion it was quoted that the boot image be flashed with the original boot image of the device pauses a challenge because it may prove futile to get the original and may not also be forensically sound regarding the source from which it may have been obtained.

The application designed by the scholars had the capabilities of acquiring data, but it was limited to collecting user and application data. Through their study called “A study of user data integrity during acquisition of Android devices”, the scholars went ahead to propose the use of JTAG (Joint Test Action Group). Though the authors admit that, to their knowledge no studies have been conducted to determine if the JTAG method guarantees data integrity or not. They stated that during the physical acquisition of electronic data, the JTAG and the chip-off method is commonly used (Son et al., 2013b).

JTAG method was realized by identification of a JTAG debug port on the device after which the battery as well as any other cables that were connected to the device together
with the case were removed. The JTAG port and the cable were connected for communication through soldering. The process resulted in a full acquisition of the device data, however, acquiring the selected data took a long time. Their study tried to ascertain if data integrity was guaranteed during acquisition of data using JTAG and comparing with data acquired through recovery mode, (Son et al., 2013a). The JTAG acquisition method is said to be problematic because not all smartphones have the JTAG capabilities. It takes long to acquire data and may therefore not be suitable for data acquisition. Chip-off method also could be having a problem because if the memory chip is separated from the device board, repairing it may be difficult thereby rendering the device useless (Son et al., 2013a).

Shahbaz et al. (2016) noted that data integrity depended on the amount of data collected, and verification on how digital forensics was applied to collect data, with maximum data acquisition being a possibility throughout the process. A general workflow for digital forensic procedures for data acquisition was required to enable maximum collection of data from modules and paths within a device from sources as shown in Table 2-1.

Table 2-1: Android Standard Data Path (Source: Shahbaz et al. (2016))

<table>
<thead>
<tr>
<th>Modules</th>
<th>Paths</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS/MMS</td>
<td>‘/data/data/com.android.providers.telephony/databases/mmsms.db’</td>
</tr>
<tr>
<td>Default Browser</td>
<td>‘/data/data/com.android.browser/databases/browser2.db’</td>
</tr>
<tr>
<td>WhatsApp Contacts</td>
<td>‘/data/data/com.whatsapp/databases/wa.db’</td>
</tr>
<tr>
<td>WhatsApp calls</td>
<td>‘/data/data/com.whatsapp/databases/msgstore.db’</td>
</tr>
<tr>
<td>Gmail</td>
<td>‘/data/data/com.google.android.providers.gmail/databases/mailstore.e.account_name.in.com.db’</td>
</tr>
<tr>
<td>Facebook Chats</td>
<td>‘/data/data/com.facebook.katana/databases/threads_db2’</td>
</tr>
<tr>
<td>Facebook Messenger</td>
<td>‘data/data/com.facebook.orca/databases/threads_db2’</td>
</tr>
<tr>
<td>WIFI passwords</td>
<td>‘/data/misc/wifi/wpa_supplicant.conf’ from rooted extraction, or ‘flattened-data’ from backup extraction</td>
</tr>
<tr>
<td>Skype Calls</td>
<td>‘/data/data/com.skype.raider/files/&lt;account_name&gt;/main.db’</td>
</tr>
<tr>
<td>Synchronized Accounts</td>
<td>‘/data/system/users/0/accounts.db’</td>
</tr>
</tbody>
</table>
The extracted data was stored in destination directory and opened on terminal via sqlite3 module. The database extracted could be viewed using SQLite prompt since Android devices maintain databases in sqlite3 format. For there to be a forensic examination of Android device an imaging had to be done whereby three things were needed for one to image a phone:

A connection between development machine (Linux environment here) and phone via USB. Thereafter, an exploit to phone since Android is Linux based and the operating system had security features that did not allow taking of memory dumps of the phone's storage. Using the appropriate device specific exploit, phone needed to be rooted. A command to image, whereby the command needed to be run as root which copied image one bit at a time across the USB cable where we store it in a file.

**Steps to image Android phone**

“adb -d shell” (this starts a shell session with the phone allowing us to interact with our phone); “su” (assuming no errors, the shell starts with # i.e. root); “ls /data” (check if you can access the /data directory, if yes then you have gained root permissions; We use dd command (which allows to read/write block devices) to obtain bit by bit image, the command we use is device specific; To find out the block to be imaged in device, open the adb shell to device and type “mount”; “Mount” command shows all mounted partitions on the device, check for r/w block with a familiar file system like ext4; dd if=/dev/block/xxxxxx| busybox nc -l -p 8888; This command writes the contents of blockdev/block/xxxxxx via netcat to port 8888.

The authors noted that a forensic tool could be used to examine an image file (for example FTK imager by Access Data). “To open an image in FTK go to: File → Add evidence item → image. The image will be opened with all partitions visible. All packages will be visible in data partition” (Shahbaz et al., 2016).

According to a study by Do et al., (2015), their extraction of forensic data exploited several investigator abilities. They argued that if the data was used without due deliberation, it may have led to a breach of forensic soundness principles. The authors introduced the Inject capability and Modify code, which were obligatory in the process of extracting forensic data which is usually protected by Android’s OS security module.
The deliberate addition of code as well as modification of the underlying Operating System frameworks results in circumvention of the security checking code which is used to validate that the application requesting access to stored credentials is the same application that originally stored them. The tests consequentially lead to the possibility of introducing errors and violating the associated forensic soundness requirements, since there exists data modification (Do et al., 2015).

These sets of circumstances can be avoided though. The authors advised that practitioners must guarantee that the code being introduced in the test should be subjected to transparency and trustworthiness constraints. Do et al. (2015) noted that the code should be independently verified to guarantee that it does not result in any unknown modification to evidential data; as well as logging the operation of the code to ensure that the output is free of errors.

Through a study on general collection methodology for Android devices by Votipka et al. (2013), the authors reported that for minimal potential for data corruption as well as comprehensive extraction of evidence, re-purposing a special Android boot mode was required.

The technique fashioned by Votipka et al. (2013) proposed a general acquisition approach to be employed as a part of extraction of digital evidence from Android phones. The methodology comprised of a procedure whereby a bootable picture was flashed on original recovery image of the Android device. Images may take an alternate form as this depends on the mobile device model; and it was a significant prerequisite that the images should be flashed on the original recovery image of the specific test device (Android device).

The scholars suggested that data extraction from the NAND, including SD cards that could be attached, could be accomplished by using a custom recovery mode without essentially the necessity for root access methodology (Votipka et al., 2013). However, the major challenge with the mentioned methodology related to the fact that newer phones, especially those released after the date of this research had their boot-loaders locked and therefore required a mechanism that had the ability of wiping the device to unlock the boot-loader.

Votipka et al. (2013) also presented another method for data collection from Android devices that utilized the capabilities of custom image recovery that are built and eventually ported to many Android devices. The scholars noted that custom images had within them
forensic tools which had the aptitude of extracting Android’s data in a manner that is forensically sound. In this process, the person carrying out the investigation should be able to get vendor’s key that is used for signing legitimate bootloader images to bypass a locked bootloader.

The scholars presented another methodology for collecting evidence from Android devices in a forensically sound manner. They noted that forensic data omitted or corrupted during collection may result to loss of integrity of an investigation. Their technique repurposed a special Android boot mode recognized as recovery mode. The authors noted that Android phones have partitions containing different types of data. ‘System partition contains parts of the operating system, manufacturer and vendor added features, and applications that the user is not meant to modify. User data partition contains application specific data’ (Votipka et al., 2013).

The authors noted that recovery partition contained used software normally used to perform maintenance tasks. He noted that the common recovery mode tasks included returning the device to a standard configuration or applying a software updates that could not be applied while the system was executing in its standard operating mode.

To accomplish the research, the recovery software was executed by avoiding the normal boot procedure. This was by entering the device in recovery mode by pressing special keys during the early stages of the boot process. For the research, they devised a special recovery software to replace the incumbent software in the recovery partition. The tools used for data duplication were Linux command tools, cp or dd (Votipka et al., 2013).

The authors noted that cp would necessarily perform a logical collection omitting unallocated spaces, and in the case of modern mobile devices dd would also result in an incomplete collected image. They argued that data copied using dd omitted memory areas known as spare or out of-band. These memory sets were used to store metadata about associated memory segments. The researchers therefore employed a tool explicitly designed to interpret flash memory. They noted that an image could be collected that contained more information than could be collected via standard Linux tools (Votipka et al., 2013).

Android debugging tool with Android Debug Bridge component was used to transmit collected data. The device-specific components were added to their special recovery
software. Utilizing ADB in recovery mode, the investigators were able to interact with the recovery software using a computer, and perform data collection/extraction using TCP over USB. Data transfer required device-specific software tools that overwrote the existing recovery partition with the new software. They acknowledged that while the process unavoidably overwrote data only in the recovery partition, the partition was unlikely to contain potential evidence. The collector then rebooted the device and directed it into recovery mode (Votipka et al., 2013).

The process necessarily overwrote data only in the recovery partition, although it is cognizant to note that this partition was not likely to contain any potential evidence. Android operating system stores each partition in its own, distinct memory address range which ensures that writes to the recovery partition would not overwrite blocks on other partitions. The base address of a partition is usually located in the image header along with the partition size. If the base address/size pair given to the flashing device overlaps another partition it is possible that blocks from another partition could be overwritten (Votipka et al., 2013).

When booted into recovery mode, partitions other than the recovery partition were not modified as would typically occur during normal operation. By using recovery mode for forensic collection, data in other partitions was duplicated without the risk of data in those partitions being altered during collection. By utilizing the method, more data was collected, than would be with standard data duplication tools, particularly capturing flash out-of-band areas (Votipka et al., 2013).

It is imperative to understand the level of privilege an investigator needs to write to the forensic device. Some phones may have an unlock-able or signed bootloader that restricts write access to the forensic device. There have been cases of unlock-able bootloader, where the manufacturer allows the user to overwrite the device images. This is possible after the investigator/user obtains a key from the manufacturer (Votipka et al., 2013). From the authors’ analysis, there was need to bypass the bootloader restrictions for the sake of building a recovery image with a varied number. The assumption was that in a real forensic investigation, the authority prosecuting the case would obtain the manufacturer key through the legal process.
In such scenarios where the bootloader is locked, the mobile phone vendors may be reluctant to provide the key. The reason is because they are not supposed to provide such services legally (Votipka et al., 2013). The challenge is that this may result to the required key not being obtained by the investigator. A case example is the iPhone of a San Bernardino terrorism suspect Syed Farook and Apple arguing that complying with the Federal Bureau of Investigations order would have set a bad precedent for users’ privacy rights. The government agency (FBI) eventually employed the services of a third party organization to access encrypted data on the phone. The investigators were able to find iOS-related code in the cache. These were similar to scripts created to jailbreak iPhones and included modified versions of Apple firmware that were used to break security on older iPhones.

2.5.2 Examination and Analysis of Forensic Evidence

2.5.2.1 Examination of Forensic Evidence

Several techniques used in rooting, data acquisition, examination and analysis have been fashioned for Android devices. The joined utilization of these procedures, methodologies and strategies with the usage of a model had been contemplated in the improvement of the information gathering approaches (Do et al., 2015).

The physical images collected from the mobile device were examined in order to extract any potential evidential data. The first step of examination began with determining the installed apps and those apps that were of particular interest to the study. One of the methods was to list the subdirectories in the “data” directory of the “userdata” partition.

Once the available data had been examined and analyzed, from both private and external app storage, a further analysis was done on the mobile device to collect any other potential evidential data. This was conducted as a separate iteration of the forensic framework (Do et al., 2015).

A study done by Lessard and Kessler (2010) incorporated Access Data's Forensic Tool Kit (FTK) in their examination of memory image files. The tool was used due to its in-depth data carving and searching capabilities. The researchers acknowledged that existing forensic software tools did not mount the YAFFS2 file system, despite the fact that the ability for string searches is a major factor in such forensic activities.
Their test device was reported to be approximately two months old and it had been used extensively used for data applications. Their research of reassembling digital fragments was able to achieve several files. These included two hundred and seven Hypertext Markup Language (HTML) and Portable Data Format (PDF) documents (Lessard & Kessler, 2010).

Others file formats that were carved included twelve thousand seven hundred and nine Bitmaps (BMPs), several Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG), and Portable Network Graphics (PNG) images (Lessard & Kessler, 2010).

Research by Votipka et al. (2013) established a general methodology for collecting and examining physical memory dumps from Android devices. Their examination established the following key characteristics that were considered to produce forensic data that met integrity threshold: user data preservation, atomic collection, correctness, determinism, evidence preservation, usability and reproducibility as well as vetting ability.

The authors annotated that the Android Operating system stored each partition in its own, distinct memory address range, and this ensured that writes to the recovery partition did not overwrite blocks on other partitions. As a result of a distinct memory range, their test cases showed that no allocated or unallocated blocks of user data were overwritten. The authors observed fifteen devices and their examination revealed that the integrity of user data, in both allocated and unallocated blocks, was never violated. The authors compared data collected from the recovery method to the results acquired through the use of the JTAG hardware debugging port. Key focus was placed on data preservation of the recovery method and their examination confirmed that the set of data complied with their measures of data integrity.

2.5.2.2 Analysis of Forensic Evidence

Do et al. (2015) employed the use of cryptographic hash functions (MD5 and SHA1) for the purposes of validating the integrity of the physical partitions that were taken from the block devices. The forensic evidence was compared to that of the original forensic images which showed a match, hence proof of data integrity. Their analysis included the following measures:

*Application Files in Private Storage:* Their research utilized the Forensic Examination capability to examine and analyze the files stored within the applications private directories.
Their research located and analyzed several artefacts, including personally identifiable information (PII), authentication tokens, encryption keys and cached data. In PII, the researchers located and analyzed usernames, email addresses and geolocation information. Combining the encryption keys that were located with app data collected from the external storage, the authors were able to use the decrypt capability to access and analyze files which had been protected by applications.

*Application Files on External Storage:* Their Forensic Examination capability located files stored by the examined apps. The majority of these files were cached versions of files stored on the respective online services by the users and were stored unprotected. However, a subset of these files was stored using encryption, with the encryption key generally being stored within private storage.

*Application Databases:* The Forensic Examination of app databases resulted in the location of numerous artefacts of PII and file related metadata. PII data included user identifiers such as usernames and email addresses, access times, and geolocation data. The majority of data stored by the apps related to the files accessed and cached by them. File metadata included typical entries such as filename, paths, access, modification, deletion, synchronization and creation timestamps, and file types.

*Examine and Analyze Accounts Data:* Examination and analysis of accounts data utilized a number of adversary capabilities like inject/modify. The authors noted that if the adversary capabilities were to be used without due consideration, a breach of forensic soundness principles may occur. The authors gave an example of extracting accounts information using the inject capability. The accounts information was protected by Android’s OS security hence required the inject capability as well as modify that added code to the existing underlying OS framework. This resulted in bypassing security checking code (used to validate that the app which is requesting access to stored credentials is the same app that originally stored them) (Do et al., 2015).

These techniques were done in a manner not to potentially introduce errors and violate the associated forensic soundness requirements dealing with data modification. The authors independently verified the code to ensure that it did not result in unknown modification to evidential data as well as and logged the operation of the code which ensured that the output
was free of errors. Examination of accounts data returned a range of data including refresh tokens, access tokens, usernames, passwords, emails and timestamps (Do et al., 2015).

**Analyze App:** After all available evidential data had been extracted from private and external storage, databases and OS accounts storage; the authors suggested further analysis on the applications themselves. The authors reported that analysis was required to meet the meaning forensic soundness principle. They went ahead to suggest that timestamps may be recorded for “access” to an app or file, however it may not always be clear how “access” is defined by the app developers. The authors suggested that a more detailed analysis of the application would answer this question. This specific analysis was achieved using both the de-compilation of the app source code (static analysis) and analysis of the memory and operation of the app while it was running on a physical or emulated device (dynamic analysis). “Using these techniques, we were able to locate various items of interest such as URLs for authentication, app secrets and protected information, which would otherwise be obfuscated during normal app operation” (Do et al., 2015).

According to the author, Lessard and Kessler (2010), an interesting aspect of the evidence analysis involved a PDF document. The file was said to have contained useful information as discovered and although it had been extremely fragmented. The Adobe Acrobat Reader program indicated that the file had been corrupted whence not viewable indications suggested that the FTK tool could view its contents. The contents in view included information such as phone book information, browser history of sites visited previously, text messages as well as Facebook status updates. Others identified include Google search history, YouTube videos as well as music content that had been previously played from an SD card.

The first significant images discovered were the ones displayed during the initial process of phone boot-up. There was an mtd3.dd file that contained images for different applications, and so did an mtd4.dd file that contained contents of the Android cache. Some of the images that were recovered were found to be corrupted although some had not been corrupted and were intact. It is against such cases of evidence that are likely to be key to an investigation since they determine the integrity of data collected (Lessard & Kessler, 2010). It was noted that thirty images from the user’s Gmail account were found and which were very fragmented. The fragmentation condition of the images gave an impression that
the amount of space permissible for caching of images viewed from Gmail was not large enough.

Lessard and Kessler (2010) suggested that the FTK tool used was not able to locate or identify all the images. They found an mtd5.dd file containing the user data and stated that this was where most of the recovered images were found; and as such the types of images one would have expected to find are images taken with the Hero's camera device and sent to another individual via the Multimedia Messaging Service (MMS) or e-mail to those from applications such as Facebook. Others included image previews of videos from SprintTV and YouTube as well as icons from applications and downloads from browser Web pages.

Lessard and Kessler (2010) noted that browsing through images and documents generated very helpful pieces of information. The FTK tool was not capable to locate text messages or e-mail messages, contacts as well as the call history. The authors noted that the powerfulness of the search tool and go ahead by indicating that to use it, an examiner needed to have a thorough knowledge of what to search for in the locations. They reported that in the event of trying to find a thread of e-mails, a rational preliminary point would be to carve out the suspected individuals e-mail address.

The process of finding the address j.lessard802@gmail.com yielded 1628 contents as well as over 92 files. They noted that the files began with identification of the e-mail address and thereafter a preview of the message body. The tool also previewed the rest of the e-mail and recipient information (Lessard & Kessler, 2010). They suggested that if a suspect had been using mobile email client, the results would have yielded more messages than a system where only web mail was used.

The authors reported that next to a username and Uniform Resource Locator (URL), the Android browser stored passwords in plaintext format. In their exploration, several of the searches found the exhibited username as well as passwords for several Web sites. In one instance, a file generated a piece of a database that held all the password information (Lessard & Kessler, 2010). They acknowledged that the outcome was helpful in the forensic examination procedure.

In their forensic examinations, one of the most vital aspect was the degree to which the tools used could accomplish a physical examination process with the capability to carve out more data. Such examination required that deleted information that might have
otherwise gone unobserved be recovered and analyzed. According to the authors, their study found out that most of the data recovered was viewable in FTK, but fragmented and difficult to read (Lessard & Kessler, 2010).

According to Lessard and Kessler (2010), the examination revealed one hundred and fifty-four subdirectories. In their study, the naming convention of the path named contacts.db was found in the Hero test device. It was hooked up to the examination machine and the directory /data/data was inspected for carving out more details. This included perusing the folders one after another, listing the subdirectories and watching out for databases. In the examination, there were numerous valuable files revealed which aided in the examination. The Linux dd command was used in the process of copying the discovered files and folders to an external secure digital card (SD card) as shown below:

```
dd if =/data/data/subdir/databases/file.db
of =/sdcard/file.db
```

The logical examination on the Android device revealed some database files that according to the researchers was a little captivating and important to look at. There was a file called `data/data/com.htc.htctwitter/databases/htctwitter.db` that had initially been examined. It was reported to be associated with HTC twitter which is a Twitter application called Peep. The application generated account information that had an unencrypted password (Lessard & Kessler, 2010). The authors also reported other vital pieces of data which included one thousand four hundred and sixty Twitter updates, with detailed information about the sender.

For purposes of comparison, the Cellebrite forensic tool was incorporated by the researchers to obtain more information from the test phone. Cellebrite Universal Forensic Extraction Device (UFED) is a forensic tool that allows sharing of analysis reports with other authorized personnel carrying out forensic investigations. In their illustration, the forensic tool proved very important since it was able to get more data including pictures, videos, music, ringtones and text messages. Other vital information included contact lists and address books, call history, and device identifying information.

According to the authors, the UFED tool was interconnected with a cell phone though a data cable, infrared (IR), or Bluetooth (BT) and these were used to acquire Subscriber
Information Module (SIM) data and other sets of required pieces of information, (Lessard & Kessler, 2010). The UFED tool was used to acquire data logically or physically, although physical acquisition was not supported for the HTC Hero at the time of the research. The UFED forensic toolkit acted as a write blocker when the research was being carried out hence integrity was maintained. The authors noted that the write blocking ensured that no information was written to the test phone device when the procedure of directing the forensic examination was taking place. In the process of connecting HTC Hero device to the UFED forensic tool, USB storage and USB debugging needed to be turned on, (Lessard & Kessler, 2010).

The research by Lessard and Kessler (2010) revealed that the UFED tool could take the examiner through the steps needed to logically acquire forensic data or evidence. The authors noted that in their examination, the output results were an HTML file directed to a USB thumb drive for storage purposes. The examination process using the Cellebrite toolkit identified information from a basic test device type by considering areas such as the software level running the phone, phone type, mobile equipment identifier (MEID) as well as data and time of the data acquisition. The authors noted that there was a hundred percent success based on the ability to uncover files and data relating to communication. These included 49 missed calls, 69 pictures, 56 contacts, 107 incoming calls, 192 outgoing calls, 1070 SMS messages and one video on the test phone (Lessard & Kessler, 2010).

The report revealed sixty-nine images and evidence showed that they came from shots taken by the original phone’s camera. Others to be found included screenshots of bookmarked websites as well as those received and downloaded as MMS messages. The authors conducted forensic analysis on two images with EXIF information. As revealed by the authors, the test phone may have been used to capture one image, whereas the other one that was found had not been taken by the test phone in question (Lessard & Kessler, 2010).

The authors upon analysis noted that the evidence results indicated that there was a different picture file naming format. They reveal that such evidence is enough to show that the files were created by different cameras (Lessard & Kessler, 2010). The researchers in their process of acquiring information from the test device using multiple method revealed the following:
**dd analysis with FTK**

It was advantageous that the toolkit uncovered deleted text messages as well as contact information that would have likely not been carved out if a different methodology had been utilized. They reported that the toolkit could find passwords with relative ease, which is a positive aspect to forensic examiners. The disadvantage of this technique is that the procedure required root access and some of the results were extremely fragmented because of the overwriting. This resulted to more time being needed to locate and piece together evidence to make more meaning. They suggested that an alternative forensic toolkit could have obtained better handling of the test device file system. Also, they argued out that FTK toolkit could easily handle such shortcomings in the future, or with an update (Lessard & Kessler, 2010).

**Analysis of specific databases**

The advantage of this technique was that the forensic exercise recovered almost everything that could be helpful to a mobile forensic investigator when collecting forensic data. The authors reported that the acquired evidence included web search history, pictures, SMS messages, call history records, e-mail messages. Others included GPS data, voice mail and passwords. The disadvantage was that root access was required to perform the process successfully it was not able to recover all the deleted SMS messages, phone records as well as contact information (Lessard & Kessler, 2010).

**Data extraction and analysis with the Cellebrite UFED**

The advantage of this technique is that it recovered several call logs, photos, video MMS/SMS messages and contact information and it showed to be a simple and stand-alone method. The disadvantage is that the procedure performed logical extraction only since the author noted that physical acquisition was not yet supported at the time of their study. The toolkit was also reported not able to recover e-mails, browsing or search history. The authors went ahead to note that a dissimilar forensic toolkit with exact YAFFS2 support would have made the physical analysis a success. They also went ahead to suggest that FTK was valuable when performing the search for very specific strings of text (Lessard & Kessler, 2010). With the forensic image file in place, they used FTK Imager to verify its hash value prior to any subsequent analysis as shown in Figure 2-5.
On the other hand, research conducted by Votipka et al. (2013), stated that the Android Operating System stored each partition in its own, distinct memory address range. This ensured that any writes performed to the recovery partition were not overwriting blocks on other partitions. This may be one of the many concerns that raise integrity questions on collected sets of data. Votipka et al. (2013) in their research studied more than fifteen devices in which the test devices were analyzed in a forensic perspective. The integrity of the user data in both area blocks that were allocated and unallocated, was reported to having not been violated. The test was done with the aim of safeguarding integrity of the collected data. The authors noted that they performed a hashing function of the phone image. This was done before and after transmission from the targeted devices and they incorporated a trusted bit-by-bit replication tools for flash memory. The results observed correct collection hence data integrity was reported to have been achieved.

They performed three collections for every target device and observed a similar result upon each collection. Their methodology is reported not to have made changes to the physical device since it prevented any physical damage to the evidence. They reported an altered partition of the recovery image only, but at the software level only. Although the recovery image was the only partition altered, they noted that were no cases of data corruption or “bricking” the device even when a bad recovery image was used. Since there were no cases of a physical damage to the device, and the device continued to perform normally, the collection process was repeatedly done, and the evidence preserved. The integrity of the data collected was maintained (Votipka et al., 2013).
2.6 Research Approach

The proposed framework for this research was based on the best measures and steps combined with methodologies to be followed for a forensically sound logical and physical extraction of Android smartphones. The research adapted the forensically sound adversary model for mobile devices proposed by Do et al. (2015). The model illuminated some key features that were observed during the rooting process which ensured data integrity. As exhibited by these authors, the framework intended to be forensically sound by satisfying the following key criteria: meaning, errors, experience, transparency and trustworthy.

Various frameworks developed were meant to work well with a particular type of investigation or device. Most of them did not emphasize on the specific information flow associated with the forensic investigation. The enhanced Android forensic process model was developed in this research in an attempt to overcome some limitations as well as improvements to existing mobile forensic frameworks. These included:

Lack of sound process model as exhibited by Lessard and Kessler (2010) and Votipka et al. (2013) with inclusion of data integrity as a key focus. The model emphasized on systematic and methodical approach to Android forensic investigation keeping in mind that the standard practices and techniques in digital investigation as documented by Ayers et al. (2014). The research also improved on research done by (Do et al., 2015) who proposed a model that utilized another method of conducting Android forensic research; the “recovery mode” as compared to “boot live OS in memory”.

The research focused on Android forensics and not generalized smartphone forensic model which may not be adopted to current phones due to advancement in technology as well as operating system security features (Goel et al., 2012). The enhanced framework carried out both logical and physical acquisition, examined and analyzed the data for integrity issues. Previous research by Son et al. (2013a) showed that it was difficult to recover deleted data through logical acquisition, but the forensic tool used was advanced that it recovered several obliterated pieces of evidence.

The proposed enhanced framework can be used as a yardstick to future research on Android phone due to the rampant increase of Android use. The framework is scalable to future developments in Android forensic research. The enhanced framework also targeted forensic experts, law enforcement agencies as well as general users due to usability of the
MOBILedit Forensic Express solution. The tool was easy to use and not very costly, hence adopted to conduct the research for financially constrained researchers. Table 2-2 shows a comparison of existing frameworks as well as our enhanced proposed framework that seeks to fill some of the gaps identified in the literature review.

**Table 2-2: A Comparison of Android Forensic Data Collection Methodologies (Source: Author)**

<table>
<thead>
<tr>
<th>Requirements</th>
<th>(Do et al., 2015)</th>
<th>(Votipka et al., 2013)</th>
<th>(Goel et al., 2012)</th>
<th>(Son et al., 2013a)</th>
<th>Our Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require device to be rooted?</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Recovery Mode?</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Collects physical copy?</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Focuses on data integrity?</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Analyzes collected data?</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Systematic Approach?</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

2.7 Chapter Summary

Chapter two expounded on existing literature on the nature of evidence found in Android mobile phones, Android platforms, the rooting procedures, forensic frameworks, data integrity issues as well as challenges encountered in the rooting of Android devices. This chapter discussed works done by scholars on best techniques of rooting an Android mobile phone and some effects of this process on the data integrity that would serve as evidential material in the court of law. Rooting was reported to render applications not to work correctly due to improper rooting or if the phone was not supported. The tool may damage the kernel and result in a lot of bugs in the device, for example the phone may keep rebooting and/or freeze at the start up screen.
The research explored existing Android mobile forensic frameworks that were intended to guarantee forensic sound data from Android mobile phones. Based on the literature, gaps were identified which this study sought to address through the formulation and testing of a forensic framework for rooted and non-rooted Android smartphones. Finally, a procedural set of activities including performing data extraction from a non-rooted and rooted Android phone, examination of the extracted data and forensic analysis of the extracted data and verification of its integrity, or lack of it. Smartphones could be used for heinous acts which may open cases of prosecution, hence acquiring data from such devices in a sound forensic manner that meets data integrity was a very important issue to be considered.
Chapter 3: Methodology

3.1 Introduction

Research methodology outlined processes that were used to confirm that the general and specific objectives were met. The chapter focused on the research method undertaken to address the research objectives theorized in chapter one. The research methodology chapter encompassed the theoretical analysis, explanation and description of the methods and procedures that were used in conducting the research. The research went ahead to expound on research design, data collection methods, research procedures, data analysis methods and finally the chapter summary.

3.2 Research Design

Research design methods are the measures undertaken in research, and these may involve simulation methods, experimental methods as well as theoretical research methods. The methodology used in this research aimed to acquire comprehensive results. This research followed both theoretical and experimental methodology. The quasi-experimental non-randomized research method was used where treatment was administered to randomly assigned processes.

A sound and very well managed and controlled forensic environment is essential and proves crucial in any type of forensic investigation being carried out. A forensically sterile environment which has a solid prevention of any potential cross contamination, blocks out unwanted data and is essentially free from malware and viruses, which is generally desirable for a forensically sound investigation. The study had a basic theory that was proven through research, observations as well as facts, hence making the theoretical method to be used. There was need to prove the efficiency of the new models hence the choice of the laboratory experiment to manipulate the processes (rooting and recovery mode) under a controlled environment. The environment involved in this research was set up using the tools illustrated and explained in the Table 3-1.
Table 3-1: Analysis of Smartphone Forensics Tools (Source: Author)

<table>
<thead>
<tr>
<th>Tool</th>
<th>Phone OS Support</th>
<th>License</th>
<th>Function</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows 10 Enterprise Operating System</td>
<td>Windows 10</td>
<td>Commercial</td>
<td>Platform to conduct the experimental tests. Installed with MOBILedit Forensic Express and Android Drivers.</td>
<td>Windows 10 platform with to conduct both physical and logical extraction.</td>
</tr>
<tr>
<td>KingoRoot</td>
<td>Android</td>
<td>Open source</td>
<td>Rooting software.</td>
<td>Also used for unbricking Android devices</td>
</tr>
<tr>
<td>MOBIL edit Forensic Express</td>
<td>Microsoft Windows, Blackberry, Symbian, iPhone, Android</td>
<td>Commercial</td>
<td>Both Physical and Logical Acquisition. Examination and Reporting</td>
<td>Use a student version from the software owner.</td>
</tr>
<tr>
<td>Hardware</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP Elite Desk 800 G1 TWR Computer</td>
<td>Intel Corei5, 3.2 GHz, 8 GB RAM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Itel it1508, TECNO F7 and Blu Studio C5 + 5LTE</td>
<td>Android 4.2.1 and above</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>USB Cable</td>
<td>USB 3.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIM Card</td>
<td>SIM Card</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hard Drive</td>
<td>250 GB</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This research study employed a quantitative research with several systematic experimental investigations of observable phenomena that were used in meeting the objectives of the research. It was necessary to note that certain chosen methodologies had their own unique features as outlined in Table 3-2.
Table 3-2: Analysis of Various Research Methodologies (Source: Freitas (2009))

<table>
<thead>
<tr>
<th>METHODOLOGY</th>
<th>DESCRIPTION</th>
<th>APPLICABILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theoretical</td>
<td>Development of a basic theory which is thereafter proved through facts, research and observations and. Theories resulting from a theoretical study are used to support a body of research, such as experiments, reports or conclusions.</td>
<td>Aids in discovery of newer models/theories. It depends on other methods to prove the efficiency of the newer models /theories.</td>
</tr>
<tr>
<td>Methodology</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Experimental</td>
<td>It involves systematic manipulation of one or more variables, with the aim of observing the effect on other variables (dependent and independent). Advantage: Control of variables helps in drawing effect conclusions. Disadvantage: Laboratory based methods are not natural, meaning results may not be generalized. It may prove difficult to control all variables.</td>
<td>In situations where the live systems or network is not available or cannot be used.</td>
</tr>
<tr>
<td>Methodology</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Types</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Simulation</td>
<td><strong>Simulation Experiment:</strong> It gives a repeatable and controlled environment, whereby the researcher determines the nature and timing of the experimental events.</td>
<td>In cases where an experiment is expensive to do in a laboratory or field setting and research that requires longer durations of time to accomplish hence making it impractical and uneconomical for the research purpose.</td>
</tr>
<tr>
<td>Experiment</td>
<td><strong>Laboratory Experiment:</strong> Independent variables are manipulated, controlling the intervening variables, and measuring the effect of the independent variables on the dependent variables.</td>
<td>In conditions where an experiment cannot be simulated or performed in a field setting.</td>
</tr>
<tr>
<td></td>
<td><strong>Field Experiment:</strong> Occurs in a “natural setting”, where a researcher manipulates the independent variables while trying to control the most important intervening variables. The researcher then measures the effects of the independent variables on the dependent variables by systematic observation of human subjects.</td>
<td>To experiments that are not ideal for a lab or simulation setting. To acquire results that are as closer to reality as possible.</td>
</tr>
</tbody>
</table>

Based on the nature of the research study, both the theoretical method and the laboratory experimental methodologies were used. Theoretical study informed us of a basic theory
that could be established through research, observations and facts. The method gave knowledge on the existing Android forensic models as well as the technological trends of Android smartphones.

The laboratory experimental methodology is somehow similar to simulation method in that the researcher designs a closed setting to mirror the “real world” experience. This is done by measuring the response of human subjects as they interact within the system. The difference is that the laboratory experiment tries to achieve the real non-repeatable scenario which is hard to repeat. Conversely, simulation methodology involves the use of simulation software programmed in a way that can be repetitive in nature.

It was essential to prove newer models efficiency, hence the use of a laboratory experiment to manipulate the various processes under a controlled environment. The experimental study used the proposed enhanced forensic model using several tools like MOBILedit Forensic Express software to conduct tests on a non-rooted and rooted Android smartphones; and thereafter used the results to ascertain its applicability to real world scenarios. The research identified two key processes to acquisition of forensic sound evidence as rooting and the recovery mode process. Based on test findings, the techniques in use were analyzed to determine integrity of the forensic data collected during the research.

3.3 Data Collection Methods

To address the primary objective of rooting an Android smartphone and investigating the impact of the rooting process on the integrity of data acquired, a quasi-experimental non-randomized research method was used. The empirical interventional study was used due to its capability to estimate the causal impact of an intervention on the target object; without random assignment.

The research performed both logical and physical acquisition or extraction of forensic data. Key focus was placed on documents in .rtf and .txt, images in .jpeg, as well as SMS and browsing history. The data collected was done in a laboratory environment which included different software and hardware tools needed to carry out the research. Windows environment performed both physical and logical data acquisition using MOBILedit Forensic Express software. KingoRoot software was used for rooting purposes.
The acquisition was conducted as follows: Collection and preservation of data, rooting the device and thereafter booting it in recovery mode (Operating System independent) hence bypass some of Android security features. On Windows platform, the study obtained two sets of data: one logical acquisition before rooting and one physical acquisition after rooting. The procedures were repeated on the three test phones.

3.4 Research Procedures

A computer running on Microsoft Windows 10 Operating System was installed with essential functional capabilities like the memory, disk capacity and other necessary functionalities. The following software tools were installed: Itel it1508; TECNO F7 and Blu Studio C5 + 5LTE smartphone drivers and MOBILedit Forensic Express software as well as KingoRoot application. To be able to access the mobile phone data on the computer the ADB (Android Debug Bridge) was enabled. This was through opening the phone settings; tapping build number seven times to enable developer options; and thereafter the allowed USB Debugging features. ADB is a program that enabled the access of the device from a Personal Computer. The USB PC connection protocol enabled on the phone for communication was be the Media Transfer Protocol (MTP). The forensic tool was able to extract and transfer logical and physical files to a separate storage (hard drive), and this was the forensic data that was used to carry out the research.

3.5 Data Analysis Methods

The research adopted a quantitative research with several systematic experimental investigations of observable phenomena that were used in meeting the objectives of the research. Information analyzed from the mobile device included documents in .rtf and .txt and images in .jpeg, as well as SMS and browsing history. These pieces of evidence were used for data integrity checks. The mode of the analysis was adopted from research by Skotnes (2015), where the examiner would randomly pick an instance of a logical acquisition and compare it to that of a physical acquisition. The research adopted the above categories of data sets from a logical extraction report and compared the results with the report obtained through a physical extraction. The analysis of evidence was done within the Windows environment using the forensic software as well as observation of reports generated by the forensic tool. The tests were conducted on rooted and non-rooted phones.

"It is of interest to point that while rooting an Android device, the rooting tools install third
party tools on the device’’ (Ayers et al., 2014). These procedures were performed to ascertain if the rooting process as well as booting in the recovery mode had any effect on the forensic evidence or final user data retrieved. Also, the volume of data extracted in both extractions was used to draw up discussions as well as conclusions for the research. According to research by Kumar (2011), the research adopted the following three stages to perform forensic analysis:

*Forensic Data Acquisition*: Acquire the evidence by obtaining a replica of the data without compromising its integrity. Of interest were previously known files.

*Evidence Authentication*: We searched and authenticated the evidence collected with the aim to verify data integrity. The set of file evidence included extraction file from a logical acquisition as well as those of a physical acquisition. The authentication procedure assisted in proving throughout the research that the data extracted was an exact replica as the original one created. The research looked at that time and date stamps of the acquired data and thereafter matched it to that of the original collection. The forensic tool employed a cryptographic technique called a hash function (electronic fingerprint for digital data) to check on data integrity issues. The technique used was calculation of the hash value using SHA-256 Cryptographic Hash Algorithm which comes with the forensic tool. “For evidentiary purposes, it is vital that the hash value exists. Without it, there may be no proof that the acquired image is an exact match or copy of the original device memory’’ (Kumar, 2011).

*Forensic Evidence Analysis*: The research employed the capability of the forensic software (MOBILedit Forensic Express) to allow the creation of a hash value for any digitally signed file that was extracted. Since the hash value was determined by the file’s contents, any change to the file or timestamp would have resulted in a mismatch with any future SHA-256 hash value. Any form of mismatched hash values would have implied that the file had been modified either intentionally or unintentionally. “It is also important to note that a hash value cannot be generated on a partial file; therefore, if a deleted file has been partially overwritten, the hash value for that incomplete file will not be available” (Kumar, 2011). The hash value generated by the forensic tool was therefore used to determine data integrity for the pieces of evidence that were collected when conducting the research.
3.6 Ethical Considerations

This research addressed values and principles that focused on questions of what was good or bad in conducting the research. The research adopted the ISO/IEC 27041:2015 standard which offered guidance on assuring the suitability and adequacy of the forensic methods used to investigate digital evidence (ISO, 2015). This was though describing methods through the stages of the investigation process. Some of the issues tackled included adherence to standards and guidelines hence preserve data integrity. The research adopted the standard to provide good practice methods and processes for evidence acquisition and investigation of digital evidence. As fashioned by Goel et al. (2012), the research was conducted by a competent examiner who followed the good practice guide for computer based electronic evidence documenting the processes and actions undertaken in the acquisition of the evidential data.

According to Association of Certified Fraud Examiners (2018), basic principles of ethical behavior guided the research by following principles such as Standards of Professional Conduct whereby the examiner declared only the significant findings, and did not disclose privileged information obtained. Another aspect to consider was Standards of Examination whereby the research conducted its work in a legal, professional and thorough manner as described in (The Computer and Cybercrimes Act, 2017). The research adopted key issues on computer use and misuse and made several inputs on matters forensics. The research made key finding based on Part 2 (Offences) Section 14 which focused on digital systems misuse; and Part 3 Section 27 and 28 on Investigation Procedures which focused on conducting forensics as well as data integrity issues. The research was able to carry out forensic functions like rooting, but in a forensic sound manner since the process did not impact on data integrity. This was supported by The Computer and Cybercrimes Act (2017) Section 28 which dictates that an authorized person can collect evidence through the application of technical means where necessary, as long as there was no modification or alteration of digital evidence.

Finally, the research was cognizant of third-party use of data and did not allow individual access to forensic data collected the test phones. The risk of privacy violations was minimized by keeping data collected on a separate storage only accessible by the examiner. The data collected was only used for conducting this research.
3.7 Chapter Summary

Research methodology outlined processes that were used to confirm that the general and specific objectives were met. The chapter focused on the research method undertaken to address the research objectives theorized in chapter one. To carry out the research, an enhanced forensic sound model was proposed. The model was implemented through a laboratory experiment that included multiple steps such as device logical data extraction, device rooting, device booting in recovery mode and physical data extraction before the overall examination and analysis. Based on the research objectives, to implement the enhanced framework, MOBILedit Forensic Express software was used for data extraction, examination and analysis, and KingoRoot software was used to perform device rooting. To collect data MOBILedit Forensic Express extracted data and generated reports of both logical and physical copy the data.

The methodology analyzed documents in .rtf and .txt, images in .jpeg, messages of type SMS, as well as web browsing history. This data was later used to verify data integrity, hence to serve as credible evidential material to settle legal cases. The implementation of the proposed solution was conducted on a computer running Microsoft Windows 10 OS. Specific tools and drivers were also installed for the three phone modes: Itel it1508, Tecno F7 and Blu Studio C5 + 5LTE. Finally, to analyze the collected data, the research used statistical quantitative analysis through which a comparison was established between the logically and physically extracted data to establish integrity analysis.
Chapter 4: Model

4.1 Introduction

Chapter four focused on describing and implementing the conceptual model through a laboratory experiment. Chapter four was broken down into various subchapters that concentrated on specific areas in relation to the conceptual forensic model as follows: analysis; modeling and design; testing and a brief chapter summary. The proposed phases and the functions of the enhanced model were discussed followed by tests carried out to ascertain the applicability of the enhanced proposed model.

4.2 Analysis

A conceptual model can be described as a high-level representation of how a system is organized and operates. It comprises of the system inputs, processes alongside their interrelationships as well as the results/outputs. According to Kent, Chevalier, Grance, and Dang (2006), basic forensic process phases consists of collection, examination, analysis, and reporting as shown in Figure 4-1.

![Figure 4-1: Basic Phases of the Forensic Process (Source: Kent et al. (2006))](image)

The NIST guideline by Kent et al. (2006) followed a general guide towards digital forensics investigations. There was need to incorporate more ideas from other researchers whose study was geared towards mobile forensics investigations, specifically Android platform.
4.2.1 Research Tools Analysis

The research used the MOBILedit Forensic Express software due to its usability and varied capabilities of data extraction, analysis and reporting. The tool was not costly as compared to other commercial software like UFED Cellebrite and although in demo-mode, it was able to present quality reports that would aid in investigation. The Windows operating system was used to install the forensic tool which provided results used in the comparison of data acquired logically and physically. KingoRoot is an open source tool that was easy to use for the purposes of rooting and un-rooting.

4.2.2 Data Integrity

Maintenance of data integrity of the original data was paramount during acquisition of forensic evidence. Digital forensics experts use write blockers and hash functions in acquisition of data, although it is difficult in mobile forensics. The reason for this is that mobile data is ever changing from the clock to internal updates of the applications. Back to back forensic acquisition of the same device may have different hash values. The research examined hash values of selected set of forensic evidence (documents in .rtf and .txt, images in .jpeg, as well as SMS and browsing history) matched it with the original data to check any inconsistencies that may have arose on upon acquisition. The research analysis identified two key processes to acquisition of forensic sound evidence as the recovery mode process and rooting process.

The rooting process was adapted from Patil et al. (2017) and the procedure was carried out with a desktop version of the rooting tool, hence data integrity was maintained. This due to the fact that the phone was inactive hence no introduction of new evidence on the device. The research also assessed the impact of installing a third-party tool used for rooting the Android smartphones before data acquisition. This was done with the aim of addressing if the installed applications had in any way impacted the forensic data. The analysis of this investigation affirmed the rooting applications only aided in retrieving forensic data. Custom recovery mode was specific to a phone model and also the Android operating systems; although, in a general methodology of using the recovery mode for data collection, the procedures seemed to be almost the same. The study evaluated the steps taken for each specific phone model since modern phones have specific custom recoveries. The research was done in a manner that avoided unwanted metadata modification of the file system.
4.3 Modeling

According to Koch et al. (2008) various digital forensics investigations benefited from the inclusion of a formal modeling approach (e.g. relational algebra, Z-specification and UML modeling). The authors proposed UML modeling as a way of formal modeling of Digital Forensic Process Models (DFPMs). They augmented that it was the acceptable formal specification for modeling of processes that provided structured and behavioral approach for a forensic investigation.

For this research, a flowchart diagram was used to provide a visual representation of the sequence of steps and decisions that were needed to perform a certain process found within the proposed framework. The processes began with a start state and a stop state with arrows denoting a sequence of activities to be done. A computer running on Windows operating system was used to run the forensic software used in the research. ADB program was enabled to facilitate communication with the computer. This was followed by a logical acquisition of evidential data, and thereafter rooting the device to acquire physical acquisition of evidential data. The two data sets were analyzed for integrity issues. The process was done iteratively; meaning that the investigator considered going back to previous processes to collect more evidential data or repeat a certain process. Figure 4-2 shows the flowchart diagram of the proposed enhanced forensic framework.
Figure 4-2: Research Procedural Functions (Source: Author)
4.4 Proof of Concept

The implementation of the proposed solution was performed on a HP ProDesk 600 G1 TWR desktop with a Core i7 processor, 8GB RAM and 500GB HDD. To test the project solution several procedures and technical requirements were followed. MOBILedit Forensic Express suggested the activation of the tool through which a license key was provided by the software owner. The tool provided a user interface that presented the underlying phone models that we could virtually access and acquire data from using logical and physical methodologies.

The process included the use of mobile phones of models Itel it1508, Tecno F7 and Blu Studio C5 + 5LTE. The chosen Itel phone had Android 5.1 Operating System installed, while Tecno F7 used version 4.2.1 and Blu Studio C5 + 5LTE version 5.0 Android operating systems. Once connected, every phone provided a different data acquisition procedure based on models and Android OS version. As depicted in Figures 5-3 and 5-4, MOBILedit provided an environment where we could connect the phone and allow the investigator to extract forensic data that was automatically recorded in a results folder on the local machine. The implementation included a set of successive actions based on the proposed framework to practically produce the intended results. The model required carrying out forensic examination of documents in .rtf and .txt, images in .jpeg, as well as SMS and browsing history successively.

4.5 Chapter Summary

Chapter four introduced the implementation process that led to the examination and analysis of the extracted data using MOBILedit Forensic Express tool. The research used MOBILedit Forensic Express tool due to its usability and varied capabilities in data extraction, analysis and reporting. To ensure data integrity, a back to back forensic acquisition of the same device was done to verify integrity between the logical and physical copies. This process was dependent on procedural actions such as device rooting and navigation in custom recovery mode, which led to extraction of more data in physical than logical extraction. A flowchart diagram was adopted given that it provided a fitting procedural and visual representation for of a real life forensic experience. The implementation process was represented in the proposed enhanced forensic sound framework.
To carry out the research the model included steps such as collection and preservation of data, rooting the device and thereafter booting it in recovery mode (Operating System independent) hence bypass some of Android security features and access the phone system as super user, physical data extraction, examination and analysis of the extracted data, and lastly presentation of the general report. Finally, Itel it1508, Tecno F7 and Blu Studio C5 + 5LTE phones were tested on Windows 10 operating system based machine. For all three phones, different tools and drivers were installed in order to connect them with the forensic tool and extract data.
Chapter 5: Results and Findings

5.1 Introduction

Chapter five focused on introducing the technologies used to conduct the study by introducing the research topic, discussion of the objectives and lastly a brief synopsis of the chapter. This chapter presented the results of the laboratory experiment and tests solutions provided by KingoRoot software as well as MOBILedit Forensic Express software in a laboratory environment setup. The study was driven by the research objectives. Several data collection processes were conducted differently to ensure thorough collection and accuracy of the obtained results that were generated in the result folder by the MOBILedit Forensic Express software. This was based on the test phone communicating with the software to facilitate data extraction and analysis reports; functions that were provided within the forensic tool. MOBILedit Forensic Express software was used due to its usability and full features required for a commercial software. Also, KingoRoot was easy to use for the purposes of rooting and un-rooting.

5.2 Rooting Techniques and Impact on Data Integrity

Objective one of the research introduced different rooting techniques and their possible impact on data integrity. Based on this objective the research explored rooting processes and underlying impact on data integrity as presented by researchers in previous studies. Rooting allowed the research to overcome specific limitations set by hardware manufacturers by superseding Android security features that usually did not allow collection of data within a phone’s storage memory dumps. Several rooting techniques were found in literature which were originally relied upon to conduct rooting on Android architecture. The Android platform was found to be one of the most usable smartphone operating systems and it was made of a Linux kernel. This research found that Android operating systems contained an anti-virus that was used to protect the entire system against various security threats or breaches.

Three rooting techniques were evaluated throughout this research as a result of studies conducted by previous researchers as depicted in chapter two, and the best technique chosen for this study. Pal et al. (2014) suggested a technique that consisted of incorporating various software tools and procedures to provide complete access of the root files/folders
to the users, which would make the user or the investigator a direct Super User. This technique provided the ability to backup, restore and batch edit applications and also remove bloatware that comes pre-installed on Android phones. The research found that for these authors, Samsung devices for instance, were rooted using a tool called Odin before flashing a custom recovery on the device. The output of the forensic report would then be stored on an external drive or a secure digital memory card using Samsung Kies installed on a computer. However, as suggested by Gupta et al. (2015) rooting using Odin tool may have rendered applications not to work correctly if the phone was not supported. The tool may have damaged the kernel and resulted in a lot of bugs in the device, for example the phone rebooting or freezing at the start up screen. This therefore meant that the right tool for rooting should be applied to a specific test device to avoid such errors and issues of bricking the phone. In case of such occurrences, these would have led to tampering with the device rendering the evidence contained inadmissible in a court of law.

On the other hand, Patil et al. (2017) proposed another technique where they described the steps of the rooting process. This technique required the use of rooting tool, “KingoRoot” to be installed on the computer and specific steps such as enabling USB debugging in the developer option in phone settings, run Android on PC, connect phone via its USB and proceed with the rooting process through KingoRoot. We also found that it was practically possible to reverse the rooting process by removing the access grant through the same tool. The research adopted rooting technique proposed by (Patil et al., 2017).

The research established that the ability to physically image memory as the most significant in mobile device forensics. This is due to the fact that the device's memory contained extremely valuable data that could be hidden or deleted as well as other fragments of data. The research emphasized that access to memory dumps could be accomplished by rooting the test phones. Rooting would therefore mean modification of devices beyond the intentions of the device designers or vendors to run home-brewed applications and install custom firmware on the phone. Changing data in such a way was argued by previous research to be not forensically sound since this required installation of a third party program on the device. Addition of more data to the existing one could have raised integrity questions on the data collected. This reason seemed to be remote since there are different ways to gain root permissions on devices without adding anything to the phone, and also with the phone disabled for active communication. An alternative way to obtain root access
without addition of data on the test device was therefore required, and this research used the desired technique hence integrity preservation. Rooting was therefore done by a desktop version of KingoRoot software with the device in airplane mode hence no introduction of more evidential data. The tool used was solely for granting root access without modifying data. There was also the need to have forensic tools with data integrity check functions like file hash calculation after acquisition, and this was achieved by the MOBILedit forensic tool. Data integrity depended on Quality (no alteration of unique features of data) and Quantity (amount of data retrieved to aid in the investigation).

To test the enhanced forensic model, the study considered two main phases including logical and physical forensic data extraction. To realize this, data was primarily extracted from each phone before rooting to acquire logical copy of the data inside the phone that would later be compared to the physical copy after rooting. The sole aim was to establish the differences and data integrity aspects between the two sets of extracted data. To extract the physical copy of the forensic data, multiple operations were undertaken including preservation of the primary data in logical extraction, then the rooting of the device to provide an exclusive access to data within the device, and lastly boot the device in custom recovery mode to unlock the bootloader and wipe the device in the aim to acquiring even the deleted data. As shown in Figure 5-1 with a Tecno F7 smartphone, the rooting process for all the three phones was performed using KingoRoot software.

Figure 5-1: Rooting using KingoRoot
5.3 Enhanced Forensic Framework for Rooted Android Smartphones

Android digital forensic models have been fashioned in a way that they work well with one particular type of investigation. The proposed model is intended to work well with a rooted phone through the incorporation of the recovery mode. The previous models did not incorporate the issues of rooting as well as data integrity, whereas those that incorporated the ‘‘boot live OS in memory’’ option encountered application limitations provide by Android security model.

The proposed model also introduced functions that would allow checking for data integrity issues as well as allowing more data extraction. The model provided better understanding of Android forensic investigation processes to both members and non-members of the digital forensics community. Iterations were incorporated in major phases of forensic examination hence yielded more solid evidence. Some of the previous models lacked this yet it was advisable that investigations take a sequential nature given that more information may crop in, prompting the investigator to revisit previous phases.

The enhanced model had the first step as identification and preservation of the Android device. Though this, the logical copy was created and preserved for future reference after exploits had been performed on the test phones. The study used three Android smartphones to identify and preserve forensic evidence. The original data was extracted (logically and physically) and maintained; and this served as the original evidence which was used for comparison with results after rooting and recovery procedures. The subsequent steps included rooting the devices, booting in recovery mode and obtaining copies of relevant data used in the analysis stage. Preconceived files with pixels, color, size as well as time stamps; and hash values were kept. Without the original set of forensic data, there could have been no proof that the acquired evidence was a replica of the original data set.

Figure 5-2 shows the enhanced proposed model.
The research proposed an enhanced forensic framework for Android smartphones. Compared to other forensic frameworks, the enhanced framework had the aptitude to exploit device security vulnerabilities as well as perform both logical and physical data extraction. The model obtained data considered to be obliterated, analyzed it and presented reports that aided in carrying out the research. This was done within the constraints of forensic soundness driven by factors in Table 2-2. The enhanced model satisfied key criteria like; meaning whereby the collected data maintained its originality and interpretation; and error identification since the software tools used did not alter user data. The capabilities of the framework included exploit where the target device was exploited using KingoRoot for the purposes of rooting the device; Inject where the test devices were
flashed with a custom recovery in recovery with minimal introduction of errors; forensic copy by making both logical and physical copies of the test phones using MOBILedit Forensic Express software; and forensic examination and analysis through scrutiny of the data collected to provide the true meaning of the data.

The model depicted identification and preservation of the Android device as the first step; and this was done using three Android smartphones to identify and preserve forensic evidence. The original set of forensic data was the logical extraction. Without this set of data, there could have been no proof that the physical extraction was a replica of the original data set. The next step was configuration of the bootloader which required the test devices to be rooted hence grant super user access to the device. The test phones were enabled to boot up in recovery mode for each specific phone, and the forensic software used to collect logical and physical data sets. To begin with, the logical data extraction was done using MOBILedit Forensic Express software. This was so because the forensic software could not perform physical extraction on non-rooted phones. The physical extraction was done using MOBILedit Forensic Express software; but only after rooting of the test phones. The collected copies of evidence were processed for the purposes of analysis of the relevant data or information under investigation. Based on the results, the research was able to provide key findings on the proposed enhanced model.

5.4 Data Extraction, Examination and Analysis for Framework Validation

5.4.1 Data Extraction

5.4.1.1 Data Extraction Before Rooting

The potential evidence needed to be availed within a laboratory environment using the three test smartphones. Using the MOBILedit Forensic Express, the first step was to extract the logical copy of the forensic data which would later serve to establish comparison with the physical copy to verify data integrity. Figure 5-3 shows the MOBILedit Forensic Express user interface for a logical data extraction using an Itel it1508 phone.
As presented in Figures 5-4, 5-5 and 5-6 the research was based on three different smartphone models and found that through the MOBILedit Forensic Express tool, it was possible to extract data of different formats and directories. Three different Android phone models were considered: Tecno F7, Itel it1508 and Blu Studio C5 + 5LTE. The available data was created into different formats and later examined and analyzed in consideration of the proposed documents and images formats as well as directories in the research methodology.

Figure 5-4 depicts the extraction of data before the rooting process to identify and preserve the existing data on ITEL IT1508 phone that would later be used in comparison with the physical.
Figure 5-4: Forensic Data Extraction before Rooting for Itel it1508

Figure 5-5 illustrates forensic data extraction from Tecno F7 phone in a logical extraction mode.

Figure 5-5: Forensic Data Extraction before Rooting for Tecno F7

Figure 5-6 illustrates forensic data extraction from Blu Studio C5 + 5LTE phone in a logical extraction mode.
Using an operating system that has been injected into the phone memory, with the aim of accessing the phone in its recovery mode, the research was able to utilize the Forensic Copy capability to collect a physical image of the device’s flash storage. The recovery mode process required a direct operation on the device as depicted in Figures 5-7, 5-8 and 5-9. By enabling customization of certain features like wiping the cache and data partitions, the process played a unique role in the overall realization of the research objectives in compliance with the proposed sound forensic framework.
Figure 5-7: Tecno F7 in Recovery

Figure 5-8: Itel it1508 in Recovery

Figure 5-9: Blu Studio C5 + 5LTE in Recovery
To extract the physical copy as demonstrated in this research, multiple technical operations and forensic processes were applied. The phone in use had to undergo the process of rooting to allow the user to access the phone memory as Super User allowing him to view, retrieve and analyze the hidden and deleted copies of the data in the phone memory. As for the logical extraction, we found that multiple copies and data formats were created from documents, images, html files, directories and others. Figure 5-10 is the user interface for a physical extraction for the Tecno F7 phone.

![Figure 5-10: Physical Data Extraction with Tecno F7](image)

Figure 5-11 illustrates the creation of the physical copy of the existing data on the Tecno F7 phone where due to the rooting process, the user or investigator already had access to the phone memory as a super user, granting him authority to view, modify and analyze all copies of data, even the hidden and deleted ones.
Figure 5-11: Forensic Data Extraction after Rooting for Tecno F7

Figure 5-12 shows the MOBILedit user interface for a physical data extraction with Blu Studio C5 + 5LTE phone. The user interface is similar across all the extractions where users have a range of extractions they can perform being displayed.

Figure 5-12: Physical Data extraction with Blu Studio C5 + 5LTE
Figure 5-13 illustrates the creation of the physical copy of the existing data on the Blu Studio C5 + 5LTE phone where due to the rooting process after preservation, investigator had access to the phone memory as a super user, granting him authority to view, modify and analyze all copies of data, even the hidden and deleted ones.

Figure 5-13: Forensic Data Extraction after Rooting Blu Studio C5 + 5LTE

Figure 5-14 illustrates the creation of the physical copy of the existing data on the Itel it1508 phone where due to the rooting process, the investigator already had access to the phone memory as a super user, granting him authority to view, modify and analyze all copies of data, even the hidden and deleted ones.
Figure 5-14: Physical Data extraction with Itel it1508

Figure 5-15 depicts extraction of physical copies for the Itel it 1508 phone.

Figure 5-15: Forensic Data Extraction After Rooting for Itel it1508
5.4.2 Data Examination and Analysis to Validate Enhanced Framework

Using MOBILedit Forensic Express extractor, this study tested whether user data integrity was maintained during the acquisition process. Three different phone models were used in the test: Tecno F7, Itel it1508 and Blu Studio C5 + 5LTE. Therefore, some specific aspects such as hash (SHA 256) values were utilized to verify the forensic soundness of the copy operation and to ensure that errors were not introduced during extraction. Stages that utilized the forensic examination capability used the output of the Forensic Copy capability. In fact, forensic copies were generated in specific folders that encompassed different types of documents, images, messages and web browsing histories that led the groundwork in the comparison process to determine data integrity of the physically extracted copies. The reports represented mobile phone features and the nature of data that had been extracted both in logically and physically. They presented the case evidence number (CEN), general information about the device, the investigator information and data extraction information.

Figure 5-16 illustrates the presentation header of the extracted report that has been examined and analyzed using Itel it1508 phone. This report represents the logical copy of the mobile phone data that was extracted before proceeding with the physical extraction that later led to a specific comparison to determine data integrity. This practically means that the phone was not yet rooted. The extracted data in MOBILedit Forensic Express presented a report that did not provide access to the phone system as super user, hence limited in accessing hidden as well as deleted data. Therefore, as seen in Figure 5-16, the deleted data revealed only one web page in web history and 12 bookmarks in applications and browsers.
Figure 5-16: Report from the Extraction of a Logical Copy for Itel it1508

Figure 5-17 presents the header of the extracted report that has been examined and analyzed using Itel it1508 phone. This report represented the physical copy of the mobile phone data that was extracted after the phone was rooted. This report was later used to establish comparison to determine integrity of the extracted data.

Figure 5-17: Report from the Extraction of a Physical Copy for Itel it1508
After rooting the Itel it1508 phone and booting the phone in recovery mode, MOBILedit Forensic Express extracted and generated the physical image of the phone memory by providing a report on data that existed before rooting as well as the data presented in the logical copy report. Beyond that, this process extracted both hidden and deleted data as seen in Figure 5-17. So, as opposed to the logical report in Figure 5-16, this extraction mode presented more data in the deleted data report section hence demonstrated its capability to recover even the deleted data to support a forensic investigation.

Figure 5-18 illustrates the presentation header of the extracted report of the logical copy of the phone data using Tecno F7 phone. This report represented the logical copy of the Tecno F7 mobile phone data that was extracted before rooting.

Figure 5-18: Report from the Extraction of a Logical Copy for Tecno F7

Figure 5-19 illustrates the presentation header of the extracted and generated physical image of Tecno F7. This report was later on used to compare the results with those of logical extraction hence establish a comparison to determine integrity of the extracted data.
Figure 5-19: Report from the Extraction of a Physical Copy for Tecno F7

Figure 5-20 illustrates the presentation header of the extracted report of the logical copy for Blu Studio C5 + 5LTE phone. This is the logical copy of the Blu Studio C5 + 5LTE mobile phone data that was extracted and generated before rooting the device.

Figure 5-20: Extraction Report of a Logical Copy for Blu Studio C5 + 5LTE
Figure 5-21 depicts the presentation of report header of the extracted and generated physical image examined and analyzed using Blu Studio C5 + 5LTE mobile phone. The report generated served the research in establishing comparison analysis with the previously generated logical copy.

Figure 5-21: Extraction Report of a Physical Copy for Blu Studio C5 + 5LTE

5.4.2.1 Examination and Analysis of Documents

Multiple documents were generated in different formats. The presentation of the files in the documents folders in both logical and physical extraction provided characteristics of the forensic data that included the file name, the path, size and the hash value of the document. The generated documents in both logical and physical extraction report presented the identical characteristics which led to the conclusion that the same images would keep the same characteristics in both extractions while the number of files in physical extraction was always more than that in logical extraction. However, this aspect was noticed for all the Android phones that were used in this research. To examine documents as suggested in the research methodology, the research considered document in Reach Text Format (.rtf).
Examination and Analysis of Documents in .rtf for Itel it1508

Figure 5-22 illustrates a document in .rtf format that was extracted before Itel it1508 phone was rooted. This document contained specific forensic characteristics such as file name, the path, size and the hash value that could later be used in comparison with the similar document in physical extraction to establish the data integrity status. The document was the 4th in the list of logically extracted documents.

Figure 5-22: Extracted .rtf Documents from Logical Copy Report for Itel it1508

Figure 5-23 illustrates a document in .rtf format that was extracted after the Itel it1508 was rooted. This document contained forensic characteristics such as file name, the path, size and the hash value; and these served as the forensic features that were later used in comparison with the similar a document in logical extraction to establish the data integrity status. The document was the 15th in the list of physically extracted documents.

Figure 5-23: Extracted .rtf Document from Physical Copy for Itel it1508
Examination and Analysis of Documents in .txt for Tecno F7

Figure 5-24 illustrates a document in .txt format that was extracted before the Tecno F7 phone was rooted. This document contained forensic features that were used in the analysis. The document was the 1st in the list of logically extracted documents, although the extraction provided two documents as compared to five from physical.

![Figure 5-24: Extracted .txt Document from Logical Copy for Tecno F7](image)

Examination and Analysis of Documents in .txt for Blu Studio C5 + 5LTE

Figure 5-26 illustrates the document in .txt format that was extracted before the Blu Studio C5 + 5LTE was rooted. The document was the 2th in the list of logically extracted documents.
5.4.2 Examination and Analysis of Images

The forensic tool generated images of multiple formats. However, for all the phone models, the research focused on .jpg images to examine and analyze the integrity status of the physically extracted copy reports after rooting the devices. As for the analysis of documents, the identical images were chosen to forensically analyze the integrity status of the images after physical extraction. This process was applied to all three phones as...
suggested in research methodology in Section 3.5. So, both logical and physical extraction images were presented in Figures 5-28 up to 5-33.

Figure 5-28 illustrates the image in .jpeg format that was extracted before Itel it1508 phone was rooted. The image contained forensic characteristics such as file name, the file path, size and the hash value. These forensic features were later used in comparison with the similar images in physical extraction to establish the data integrity status. The image was the 1st on the list of images from the logical extraction.

![Image Files](image)

**Figure 5-28: Extracted Image from Logical Copy for Itel it1508**

Figure 5-29 illustrates the image in .jpeg format that was extracted after Itel it1508 phone was rooted. The image was the 2nd on the list of images from the physical extraction. It is good to note that whereas logical extraction gave 176 images, the physical extraction gave 2930 images.
Figure 5-29: Extracted Image from Physical Copy for Itel it1508

Figure 5-30 illustrates the image in .jpeg format that was extracted before Tecno F7 phone was rooted. The image was the 85th on the list of images from the logical extraction.

Figure 5-30: Extracted Image from Logical Copy for Tecno F7

Figure 5-31 illustrates the image in .jpeg format that was extracted after Tecno F7 phone was rooted. The image was the 41st on the list of images from the physical extraction, with more images as compared to a logical extraction.
Figure 5-31: Extracted Image from Physical Copy for Tecno F7

Figure 5-32 illustrates the image in .jpeg format that was extracted before Blu Studio C5 + 5LTE phone was rooted. The image was the 75th on the list of images from the logical extraction.

Figure 5-32: Extracted Image from Logical Copy for Blu Studio C5 + 5LTE

Figure 5-33 illustrates the image in .jpeg format that was extracted after Blu Studio C5 + 5LTE phone was rooted. The image was the 359th on the list of images from the physical extraction.
Messages were extracted and recorded in both logical and physical copies reports. The messages were sorted by time in descending order to allow faster search of forensic evidence and rapid comparison between messages from both extractions. In this study, using MOBILedit Forensic Express, none of the deleted messages were viewable, although the process of extraction indicated the total number of all deleted messages. In the court of law, the examination and analysis of messages as provided by MOBILedit Forensic Express, could only be done based on the ability for the tool to recover both deleted messages, which would precise the overall integrity of the messaging package and serve as evidence to forensic investigation.

On the other hand, physical extraction as shown in Figure 5-36 was able to recover the deleted data based on the authority and access level granted to the user who has already become a Super User due to the rooting process. The forensic examination and analysis of the messages was based on the ability for the tool to recover hidden and deleted messages. None of the deleted messages were recovered.

Generally, as shown in Figure 5-34, the analysis on messages in the image “Legend” was based on sent, received, draft, failed, unknown and deleted messages with the list of participants in the conversation. These were presented in both physical and logical extractions.
Figure 5-34: General Representation of the Extracted Messages

Figure 5-35 illustrated the general representation of message data that was extracted from the phone memory before rooting Itel it1508.
Figure 5-36 illustrates the message exchange that was extracted after Itel it1508 phone was rooted. The forensic examination and analysis of the messages was based on the ability for the tool to recover hidden and deleted messages. 184 deleted messages were recovered.
Figure 5-36: Deleted Messages Extracted from Physical Copy for Itel it1508

Figure 5-37 illustrates the message exchange that was extracted before Tecno F7 phone was rooted. The forensic examination and analysis of the messages was based on the ability for the tool to recover hidden and deleted messages. In the figure, none of the deleted messages were recovered, but only 11 messages.
Figure 5-37: Extracted Messages from Logical Copy for Tecno F7

Figure 5-38 illustrates the message exchange that was extracted after Tecno F7 phone was rooted. The forensic examination and analysis of the messages was based on the ability for the tool to recover hidden and deleted messages. In the figure, 7 deleted messages were recovered.
Figure 5-38: Extracted Messages from Physical Copy for Tecno F7

Figure 5-39 illustrates the message exchange that was extracted before and after Blu Studio C5 + 5LTE phone was rooted. Deleted messages recovered in both logical and physical extraction were the same. In the figure, 34 deleted messages were recovered.
**Figure 5-39**: Messages from Logical and Physical Copy for Blu Studio C5 + 5LTE

### 5.4.2.4 Examination and Analysis of Web Browsing History

Figure 5-40 illustrates the web browsing history for Itel it1508 before the phone was rooted. One deleted page was recovered in logical extraction. One deleted message was also recovered.
Figure 5-40: Web Browsing History Logical Image for Itel it1508

Figure 5-41 illustrates the web browsing history for Itel it1508 after the phone was rooted. The physical extraction produced 38 web pages with 1 deleted page that was recovered.

Figure 5-41: Web Browsing History Physical image for Itel It1508
Figure 5-42 illustrates the web browsing history for Tecno F7 before the phone was rooted. The logical extraction produced 9 web pages with 1 deleted page that was recovered.

![Web Browsing History Logical Image for Tecno F7](image)

Figure 5-42: Web Browsing History Logical Image for Tecno F7

Figure 5-43 illustrates the web browsing history for Tecno F7 after the phone was rooted. The physical extraction produced 10 web pages with 1 deleted page that was recovered.
Figure 5-43: Web Browsing History Physical Image for Tecno F7

Figure 5-44 illustrates the web browsing history for Blu Studio C5 + 5LTE before the phone was rooted. The logical extraction produced 63 web pages with none of the deleted pages recovered.
Figure 5-44: Web Browsing History Logical Image for Blu Studio C5 + 5LTE

Figure 5-45 illustrates the web browsing history for Blu Studio C5 + 5LTE after the phone was rooted. The physical extraction produced 63 web pages, same as the logical extraction, meaning there was no deletion of pages.

Figure 5-45: Web Browsing History Physical Image for Blu Studio C5 + 5LTE
5.5 Chapter Summary

Chapter five presented the overall results of the laboratory experiment and test solutions performed using MOBILedit Forensic Express software and KingoRoot software. The results were obtained from the generated data reports that were both logically and physically extracted form Itel it1508, Tecno F7 and Blu Studio C5 + 5LTE smartphones. The output of the forensic report would then be stored on an external drive. This chapter presented results based on the three research specific objectives.

To respond to the first objective, the research found multiple rooting techniques and their shortcomings, and proposed a safer rooting technique that used KingoRoot software to safely root the Android phone and extract its data for examination and analysis. To respond to the second specific objective, the research found that forensic analysis can be performed using different existing models. However, these models presented both strengths and weaknesses that the research exploited and to which this research added more appropriate measures to develop an enhanced forensic sound framework. Finally, this chapter presented the extracted results for both logical and physical extraction, performed a thorough examination of the extracted data and provided a final analysis of the data in the aim of comparing both physical and logical copies and determining data integrity status.
Chapter 6: Discussion, Conclusions and Recommendations

6.1 Introduction

Chapter six focused on discussing forensic data collected during the research. Additionally, conclusions and future recommendations from the research were drawn. This chapter was broken down into different sub-chapters with each focusing on a specific area in relation to the discussion, conclusions and recommendations. These were: Summary which highlighted the purpose of the study, specific objectives, research methodology used in the study and major findings of the research; Discussions which focused on the major findings of the study, interpretations of the findings and comparison to previous studies; Conclusion which came up with deductions from the study findings; and finally, Recommendations whereby based on the major findings and inferences generated from the study, gave recommendations and future work suggestions.

6.2 Summary

6.2.1 Purpose of the Study

The purpose of this study was the development and evaluation of an enhanced forensic framework for Android smartphones with key focus on ensuring data integrity of forensic evidence was retained.

6.2.2 Specific Objectives

Following a hierarchical order, the research focused on meeting its specific objectives with commitment to achieve the overall expectations. The specific objectives were documented as follows:

i. The first objective was to explore existing rooting techniques and their impact on data integrity on Android smartphones.

ii. The second objective was to explore existing forensic frameworks and develop an enhanced forensic framework for rooted Android smartphones.

iii. The third objective was to extract, examine and analyze logical and physical data hence validate the enhanced forensic framework.
6.2.3 Research Methodology

Chapter 3 introduced the research processes that were used in the implementation of the proposed enhanced framework through provision of steps and approaches taken towards the fulfilment of research objectives. The type of experimental design this research study adopted was a quasi-experimental design with capability to manipulate the rooting and recovery mode processes under a controlled environment. On the machine running Windows operating system, the following software tools were installed: Universal ADB drivers to enable access the mobile phone data on the computer; KingoRoot for rooting the test devices; and MOBILedit Forensic Express software to extract data. The test phones used were Itel it1508, Tecno Phantom F7 and Blu Studio C5 + 5LTE. All the phones had been in use for over four years. The USB-PC connection protocol enabled on the test phone for communication was the Media Transfer Protocol (MTP).

“It is of interest to point that while rooting an Android device, the rooting tools install third party tools on the device” (Votipka et al., 2013). Through installation of a desktop version of the rooting tool, the procedure was performed in a manner to avoid alterations on final user data retrieved. The experimental study used MOBILedit Forensic Express software to extract data and presented results from a logical acquisition and physical acquisition. Using SHA-256 Cryptographic Hash Algorithm, MOBILedit Forensic Express generated a unique digital signature for digitally signed files.

“For evidentiary purposes, it is vital that the hash value exists. Without it, there may be no proof that the acquired image is an exact match or copy of the original device memory” (Kumar, 2011). The research examined hash values of forensic evidence generated by the forensic tool; and these included documents in .rtf and .txt, and images in .jpeg. Another examination included SMS and conversations from browsing history and also the ability to recover and analyze obliterated information. The mode of the analysis was to randomly pick an instance of the above categories from a logical extraction report and compare that particular instance with the report from a physical extraction. The results were subjected to analysis whereby any form of mismatched hash values for the same extraction would have implied that the file had been modified; and this aided in ascertaining the integrity of the data extractions.
6.2.4 Major Findings

The implementation of this project provided an insight on the integrity of data extracted from an android smartphone that has undergone rooting process. This was carried out based on the research specific objectives. the research found that multiple rooting techniques originally existed and on which Android architecture relied. In fact, the Android platform was found to be one of the most usable smartphone operating systems and it was made of a Linux kernel. Based on the research by Pal et al. (2014), the Linux kernel consists of a Wi-Fi driver Audio drivers, the display driver, the camera driver, flash memory driver, Inter Process Communication driver, Keypad driver, and Power Management where if any of the aforementioned drivers is affected, the device may become unusable. However, in this research, we found that Android applications consist of an anti-virus used to protect them.

On the other hand, the research proposed an enhanced forensic framework for Android smartphones. Compared to other forensic frameworks, the enhanced framework has the aptitude to exploit device security vulnerabilities as well as perform both logical and physical data extraction of data. The model obtained forensic data that was considered to be obliterated, analyzed and presented in terms of reports that aided in carrying out the research. This was done within the constraints of forensic soundness driven by factors in Table 2-2. The enhanced model satisfied key criteria like; meaning whereby the collected data maintained its originality and interpretation; and error identification since the software tools used did not alter user data. The implementation of the proposed model was carried out using KingoRoot software for device rooting and MOBILedit Forensic Express software for data extraction, examination and analysis.

Finally, after implementing the proposed model, the experiment produced results from the extraction of data. Therefore, using MOBILedit Forensic Express software, as depicted in Figures 5-3, 5-4 and 5-5; data was extracted from the three phones through both logical and physical extractions. In fact, as data extraction was performed twice on each phone, the research presented both logical and physical data extraction processes that concluded with a generated report as seen in Figures 5-11, 5-13 and 5-15. The extraction in physical mode then produced a physical image of the phone data. Finally, the created reports from both logical and physical extraction of data contained multiple types of data. However, based on the data collection method proposed in this research, only documents in .rtf and .txt formats, images in .jpeg format, SMS messages and web browsing history pages were considered.
Therefore, as shown in Figures 5-16 and 5-17, the generated report in physical extraction presented more data than the one in logical extraction. This is due to the fact that after rooting a device, the user is granted the super user permission, hence is able to extract and analyze even hidden and deleted data. The overall data in documents, images, messages and web browsing history maintained the integrity features after both logical and physical data extraction. Based on this aspect, we could conclude that data integrity was maintained.

6.3 Discussion

This section focused on the major findings of the research study. Interpretation of the findings was done to compare them with the findings of the previous studies as depicted in the literature review chapter. To aid in the interpretation of results, the sections were organized into the specific objectives of the study as discussed below:

6.3.1 Rooting Techniques and Impact on Data Integrity

The technique used in the process of rooting a phone was found to be specific to certain models of the test device, and in case a device is not properly identified, the wrong rooting tool could be used hence brick the phone and render it unusable. The threat this would imply is that all the evidence expected would be lost hence complicate a case due lack of evidence. Most of the rooting application can be downloaded from Playstore and exploits performed to the test device with the aim of granting super user experience. This research used the KingoRoot application to perform the rooting process. Although ACPO principle 1 states that actions taken by the examiner during an investigation on the device should not alter or add any data, the previous processes of installing rooting tools through Playstore required that one connects to the internet and download the application then install it (Goel et al., 2012). This could pose a threat to data integrity due to connecting the phone to the internet to enable the download before installation. This could have introduced more data to the existing one hence bring about data integrity issues. Being cognizant of this breach, the rooting technique in this research installed a desktop version of KingoRoot with the phone on airplane mode as per the NIST guidelines for acquisition, hence no addition of data. The custom recovery images were carefully selected since using the wrong image could have bricked the test phones hence hamper data extraction.

In our research, some of the suggested rooting techniques of previous studies could not have applied. Gupta et al. (2015) suggested that rooting using Odin tool may render
applications not to work correctly if the phone was not supported or if the procedure was not done correctly. The tool may damage the Linux kernel and result in bugs, for example the phone rebooting or freezing at the start up screen. This meant that the right tool for rooting should be applied to avoid tampering with the device which would render the evidence inadmissible in a court of law. Another example was that during the installation of a rooting tool; Playstore Protection has recently put up a warning that advises one that the application being installed could cause a potential threat to your device. The Playstore Protection then allows you to acknowledge that the application is safe for installation and that you accept the risk of rooting your device and the potential harm it could cause. The operating system also provides a feature called “Unknown Sources” that allows one to install applications from unknown sources. Without enabling such exploits, it may not be possible to install rooting tools.

Forensic data integrity was maintained since the third-party tool used (KingoRoot) did not affect the final data as evidenced in the analysis of data collected. It was important to note that the rooting tool application did not affect the test devices used as well as the final data, but only aided in providing more privileged access in retrieving more data in a physical acquisition than in a logical acquisition.

6.3.2 Enhanced Android Forensic Framework for Rooted Smartphones

The research study found that few studies have been conducted to address the ever evolving technologies within smartphones forensics domain. Various frameworks that were previously developed were not specific to Android platforms, hence not meant to work well with a particular device model. Most of the forensics studies conducted focused on general digital forensic which included computer forensics. Other studies have focused on a more generalized investigation process for different operating systems, yet every OS has its own unique features which a generalized framework may not be able to address Therefore, the research focused on Android forensics and not generalized smartphones as proposed by Goel et al. (2012). This research focused on the forensic process model specific for Android smartphones running a higher version (4.2.1 and above). Previous studies conducted before this research exhibited investigations that had lower versions of operating systems whose security features were not as highly advanced as current Android operating systems. This
therefore means that some of the suggestions given could not have applied to modern phones whose operating systems are highly protected.

Lack of sound process model as exhibited by Lessard and Kessler, (2010) and Votipka et al. (2013) was another aspect that the research improved on by proposing a systematic and methodical approach to Android forensic investigation while keeping in mind the standard practices and techniques in digital investigation as documented by Ayers et al. (2014). Some of the studies did not emphasize on a certain specific flow of information associated with a sound forensic investigation. The enhanced Android forensic process model was developed in this research in an attempt to overcome some limitations as well as improvements to existing mobile forensic frameworks. This was by providing a systematic flow of activities as exhibited by the Figure 4-2 flow chart.

Previous models such as those presented by Son et al. (2013a) as well as that of Votipka et al. (2013) did not factor in thorough analysis of collected data. Without further analysis, one may never be able to tell that the extracted evidence met certain integrity threshold. Previous research showed that logical acquisition could not recover much of the deleted data hence the need of a physical copy. Casey (2011) added that in case a full copy of physical memory is not possible, for many devices the complete logical file system could still be acquired and used in an investigation. The author noted that although logical copies do not include deleted items, they can still provide access to substantial digital evidence including MMS messages, IM fragments, and web browsing history that are not displayed automatically by forensic tools. In case of such scenarios, the forensic examiners must locate the desired information within the file system and interpret it themselves. It is imperative for investigators to have an understanding of the underlying technology used and not be overly reliant on automated tools.

The proposed framework in this research emphasized upon data integrity and this was based on the best measures, as provided by forensic standards, to be undertaken, hence ensure forensic sound logical and physical extraction of data. The research adapted the forensically sound adversary model for mobile devices proposed by Do et al. (2015). The proposed model illuminated major features that were observed during the rooting process which ensured data integrity. As exhibited by these authors, the framework intended to be forensically sound by satisfying key criteria such as meaning whereby the data maintained
its originality and interpretation since there was no alteration of user data; errors whereby
the research did not encounter errors that could threaten validity of the data; experience
whereby the investigator had acquired technical skills on how to acquire evidence; and
lastly, transparency and trustworthy by validating data integrity through examination and
analysis of collected data. The enhanced framework carried out both logical and physical
acquisition, examined and analyzed the data collected hence check for integrity issues. The
enhanced framework targeted forensic experts, law enforcement agencies as well as general
users due to usability of the MOBILedit Forensic Express solution. The tool was easy to
use and not very costly, hence adopted to conduct the research for financially constrained
researchers. Formal modeling through Unified Modelling Language was introduced to
provide understanding to members and non-members of the digital forensics environment.
The significance of the enhanced forensic framework was to augment the trustworthiness
and acceptability of forensic evidence in a court of law. The model focused on ensuring
that the evidence collected was admissible in a court of law by meeting integrity standards.

6.3.3 Data Extraction, Examination and Analysis to Validate the Framework

Key points from the whole analysis indicated that no data change occurred when rooting
was done on the phone and subsequent physical extractions done. It was noted that while
rooting Android smartphones installed third party tool on the test device, those tools
however had no impact on the final user data retrieved.

From both the logical and physical extraction reports generated by the forensic tool, it was
noted that the documents, messages, browsing history and images retained their shape,
identity, name and the physical paths. MOBILedit Forensic Express software used SHA-
256 Cryptographic Hash Algorithm to compute the hash values for documents and images,
which depicted that logical extraction was exactly the same as the physical one.

Discussion points from the SMS messages revealed that the physical extraction recovered
most of the deleted messages, as compared to the logical extraction which did not recover
any deleted message. Another mode of analysis was comparing the time, date, sender and
the contents of the SMS messages that were found in the logical extraction and compare
them to similar ones found in a physical extraction. The research revealed that the reported
features were not changed hence data integrity was maintained.
6.4 Conclusions

Technology advancement in the smartphone industry is growing at a very spontaneous rate and so are cybercriminal activities. There have been challenges in building and maintaining forensic sound process models that drive mobile device investigations. Countermeasures need to be put in place to address gaps in technology by introducing newer mobile forensics techniques aimed at helping law enforcement agencies to prosecute criminals. The enhanced framework can be used in tandem with The Computer and Cybercrimes Act (2017) in handling cybercriminal cases. The act laid down standard procedures on forensic data collection with focus on data integrity in mind as emphasized by the research.

6.4.1 Rooting Techniques and Impact on Data Integrity

Rooting smartphones to enable physical data acquisition required the test devices to be altered, however as documented in this research, the process was carried out in a manner that avoided unnecessary changes to the user data. Rooting was performed using a desktop version of KingoRoot software with the device in airplane mode hence no introduction of more evidential data was experienced. The research explored rooting and data integrity concerns as a result of rooting that avoided alteration of user data. Key points from the whole analysis indicated that no data change occurred when rooting was done on the phone. It was noted that while rooting Android smartphones installed third party tool on the test device, the tool however had no impact on the final user data retrieved.

6.4.2 Enhanced Android Forensic Framework for Rooted Smartphones

The research evaluated existing Forensic Models that were proposed by different researchers. However, these models had differences and unsatisfactory characteristics that led this research to develop an enhanced Forensic Framework in the aim of addressing some of the existing gaps. The research proposed a framework that can be followed during a logical and physical acquisition of forensic evidence from Android smartphones with key focus on preservation of data integrity. The enhanced framework targeted forensic experts, law enforcement agencies as well as general users due to usability and the rising cases of Android misuse by cybercriminals. The enhance framework can be used as a yardstick to future research on Android phone due to the increasing use and misuse of the Android platform.
6.4.3 Data Extraction, Examination and Analysis for Framework Validation

The research used MOBILedit Forensic Express software for logical and physical data extraction. The tool computed SHA-256 Cryptographic Hash Algorithm for both images and documents, analyzed and retrieve both hidden and deleted information such as message and web browsing history. Based on the report findings, it was noted that the documents, messages, browsing history and images retained their shape, identity, name and the physical paths. The research concluded that a logical extraction had the same forensic characteristics as the particular file of a physical extraction hence data integrity was maintained.

6.5 Recommendations and Future Work

6.5.1 Recommendations for the Research

This research study focused more on smartphones running the Android platform. More research should be done using other Android phone models and compare results. Also, a study needs to be conducted on other types of devices running on Windows platform since studies have put more focus smartphones running on Android as well as Symbian, Blackberry OS and iOS operating systems. Also, it was recommended that a research be conducted with the sole aim of analyzing the impact of rooting process on running processes and the applications data. The enhanced framework is open to researchers and digital forensics experts for amendments. Finally, for a forensic sound investigation, both logical and physical data acquisition should be carried out.

6.5.2 Recommendations for Future Work

Altogether, it was noted in the research that software tools used in mobile device forensics are still limited in terms of feature support as well as operating system support. This directly impacted on mobile forensics models that used forensic tools with inability to extract all of the potential evidence an investigator may consider necessary and present it in a readable manner. An example is that of the forensic tool not being able to extract and interpret WhatsApp conversations due to its high encryption of its communication. The research recommended development of forensic tools that are able to decrypt specific data such as WhatsApp conversations and other highly encrypted applications. However, inasmuch as good forensics models are developed, there is equally a necessity to have good mobile forensics software tools that allow investigators acquire data they deem ought to have been collected.
References

https://doi.org/http://dx.doi.org/10.6028/NIST.SP.800-101r1

https://doi.org/10.1016/j.diin.2013.10.003


https://doi.org/10.1109/ICGEC.2011.46


Gupta, M., Bhardwaj, A., & Garg, L. (2015). Custom ROM ’s in Android, 6(2), 1874–


