A CRITICAL APPRAISAL OF MOBILE PHONE FORENSIC EVIDENCE IN KENYA

BY

SIMON KAIGONGI AROME

REG NO: G62/67779/2013

PROJECT WORK SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF THE DEGREE OF A MASTER IN LAWS IN THE UNIVERSITY OF NAIROBI

SUBMITTED TO SCHOOL OF LAW

UNIVERSITY OF NAIROBI

SUPERVISOR

MS EVELYN ASAALA

DECLARATION

I Simon Kaigongi Arome, do hereby declare that this project is my original work and that it has not been presented elsewhere and is not due for submission for an award of a degree in any other University.

Signed…… Date …….

Simon Kaigongi Arome

G62/67779/2013

This project has been submitted with my approval as the University of Nairobi School of Law supervisor.

Signed ……. Date …….

Ms Evelyn Asaala

Lecturer – Faculty of Law

University of Nairobi.

ACKNOWLEDGMENT

First, I thank God for enabling me write this project. I feel blessed.

Special thanks go to my family, my dear wife, Emma Mukami Ngari you have been my pillar. Your love and support throughout the programme made it easy and enjoyable. To my wonderful Kid son Kyle Mugiira Kaigongi your love kept me strong every day to achieve this goal.

My extended family and friends who encouraged me and ensured life was still enjoyable - I salute you and God bless you abundantly.

My supervisor Ms Evelyn Asaala - thank you for your constant guidance and insightful comments that challenged me in a positive way and I appreciate it.

To all School lecturers and other staff who taught me I thank you for making my dream come true.

With deep respect and appreciation I specially thank my classmates in the academic year 2013 / 2014. I appreciate the conducive learning environment and moral support you gave me. I feel greatly indebted to all of you.

To all who walked with me, I say thank you and may God bless you.

DEDICATION

This thesis is dedicated to my parents, William Ntoarome and Jane Kamami without whom I would never have started and achieved this goal. You are not only the best but also the greatest gift God ever gave to me.

Table of Contents

ABBREVIATIONS

CCTV	-	Closed Circuit Television
CD	-	Compact Disc
CID	-	Directorate of Criminal Investigations
DVD	-	Digital Versatile Disc
FBI	-	Federal Bureau of Investigation
HCCA	-	High Court Civil Appeal
HCCC	-	High Court Civil Case
HCCRA	-	High Court Criminal Appeal
HCCRC	-	High Court Criminal Case
IEBC	-	Independent Electoral and Boundaries Commission
IMSI	-	International Mobile Subscriber Identity
ODPP	-	Office of the Director of Public Prosecution
ONW	-	Online Neighborhood Watch
PC	-	Police Constable
PW	-	Prosecution Witness
PIRL	-	Prosecutor's Initial Reference List
SMS	-	Short Message Services
UFED	-	Universal Forensic Extraction Device
UK	-	United Kingdom
USA	-	United States of America

TABLE OF STATUTES

The Constitution of Kenya 2010

The Evidence Act Cap 80 Laws of Kenya

TABLE OF CASES

KENYAN CASES

William Odhiambo Oduol v Independent Electoral & Boundaries Commission & 2 Other Election Petition No. 2 of 2013 [2013] eKLR

Nonny Gathoni Njenga & Another v Catherine Masitsa & Another HCCC No 490 of 2013 [2014] eKLR

Republic v Barisa Wayu Mataguda HCCRC NO 6 OF 2008[2011] eKLR

Republic v Edward Kirui HCCRC NO.9 of 2008[2010] eKLR

Republic v Stojananovic Milan alias Allan & Another HCCRC 153 of 2004 [2008] eKLR

Republic v Ibrahim Bille Jelle HCCRC NO. 3 of 2013 [2016] eKLR

Mohamed Koriow Nur v Attorney General HCC Petition No. 181 of 2010[2011] eKLR

Karuma son of Kaniu v Republic [1955]1 ALL E.R 236

OTHER JURISDICTIONS

The State and Oscar Leonard Carl Pistorius CC 13 of 2013, In the High Court of South Africa Gauteng Division, Pretoria 12th September 2014

Republic v Stevenson [1971] ALL ER 678 at page 680 letter E-G.

Republic v Whitney [1971] ALL ER 678 at page 680 letter E-G.

United States v Gagliardi, No. 06-4541 (2d Cir. 2007)

CHAPTER ONE

1.0 BACKGROUND OF THE STUDY

Modern communication technology has made the world a global village[1]. Mobile phone is one of the devices that has revolutionized the mode of communication in the world today. Other devices include; computers, tablets, iPads, iPhone and fax. This study will focus on mobile phone forensic evidence. Today there are 7.22 billion mobile phones in the world[2]. Kenya has 32.8 million mobile phones[3]. In the normal course of life or business most people are likely to use their mobile phones: taking pictures, sending or receiving text messages, accessing the internet to send or receive e-mail, record a video, play music, and or send or receive instant message service[4]. These phones keep records which can be extracted through mobile forensic investigation.[5] Section 106B (4) (d) of the Evidence Act requires a certificate to be issued by a person occupying a responsible position in relation to the device.[6] This poses a dilemma on admissibility of mobile phone forensic evidence because section 106B (4) (d) of the Evidence Act does not define who is a person occupying a responsible position. The Courts on the other part have given contradicting interpretations. The study will analyse criminal and civil cases to recommend a standard definition. In the case of *William Odhiambo Oduol v Independent*

[1] Martin A, 'Mobile phones Forensics' (2009) http:/www.martinandrew@martinsecurity.net http://www.martinsecuritiy.net> accessed on 22nd October 2014.

[2] GSMA's real-time tracker puts the number of mobile phones at 7.22 billion whilst the US Census Bureau says the number of people is still somewhere between 7.19 and 7.2 billion.

[3] Communications Authority of Kenya, quarterly sector statistics report first quarter of the financial year 2014/15 (Jul-Sep 2014) http://techmoran.com/mobile-subscriptions-kenya-increase-32-8-million-penetration-raises-80-5/#sthash.ZeQ5fD7o.dpuf. < Accessed > 17th June 2015.

[4] Amanda Lenhart and others, 'Teens and Mobile Phones' [2010] PewResearchCentre <http://www.pewinternet.org/files/old-media/Files/Reports/2010/PIP-Teens-and-Mobile-2010-with-topline.pdf> accessed 16th November 2016.

[5] Det Cindy Murphy, 'Cellular Phone Evidence; Data Extraction and Documentation, Developing Process For The Examination Of Cellular Phone Evidence'< http://ccf.cs.uml.edu/forensicspapers/Cellular%20Phone%20Evidence%20Data%20Extraction%20and%20Documentation.pdf> accessed 17th November 2016.

[6] Evidence Act 2012 Cap 80 Laws of Kenya.

Electoral & Boundaries Commission & 2 Others the Court held the petitioner did not adduce any evidence to show who owned, operated and managed the computer, and the particulars of the computer used to produce the CD. Therefore the video clip developed into a Compact Disc (CD) was not admissible.[7] In the case of *Republic V Edward Kirui* PW6 Peter Opondo a Special Project Editor with KTN testified, played and produced a slow motion caption of a video footage of Edward Kirui shooting and killing George William Onyango and Ismail Chacha[8]. The video was captured by KTN Camera man Mr. Baraka Karama.[9] In the case of *Republic v Barisa Wayu Mataguda* the Court held the CCTV footage amounted to primary evidence and could very easily and simply have been produced as evidence by PW4 the owner of Karama restaurant in its raw form.[10] The different interpretations of section 106B (4) (d) of the Evidence Act creates confusion. The question is who better understands the scene and the gadget? This study contribute to knowledge by defining a person occupying a responsible position in relation to the gadget as,

> The owner of the device and the person operating it to capture some data.

This definition is justified on the basis that the owner of the device is the custodian of the device and therefore well placed to satisfy its working condition and give its particulars. The person operating the device is justified on the ground that he or she personally controls the device to capture the actual data evidence in its raw form. He or she can be called if need be to give further and better particulars of how he captured the data and the scene. This definition is important to broaden admissibility of mobile phone evidence and achieve uniformity in decision making.

[7] HC Election petition 2 of 2013[2013]eKLR.
[8] HCCR NO.9 OF 2008[2010]eKLR.
[9] HCCRC NO.9 of 2008[2010]eKLR.
[10] HCCRC NO.6 of 2008[2011].

1.1 PROBLEM STATEMENT OF THE STUDY

This study has identified a dilemma presenting mobile phone forensic evidence in court because section 106B (4) (d) of the Evidence Act requires a certificate to be issued by a person occupying a responsible position in relation to the operation of the device but does not define that person. This has excluded competent eye witnesses from giving evidence in court. For example in the case of *William Odhiambo Oduol v Independent Electoral & Boundaries Commission & 2 Others* the court considered the owner of the computer, its details and working condition instead of the petitioner the owner of the phone and the person who operated it to capture the video clip.[11] To alleviate the problem this study seeks to define a person occupying a responsible position a under section 106B (4) (d) of the Evidence Act.

1.2 OBJECTIVE OF THE STUDY

The main objectives of the study is to examine the efficacy of mobile phone evidence under section 106B (4) (d) of the Evidence Act.

The specific objectives are

i. Examine Courts interpretation of section 106B (4) (d) of the Evidence Act?
ii. Evaluate the admissibility of mobile phone evidence in Court.
iii. Define a person occupying a responsible position in relation to the gadget.

1.3 RESEARCH QUESTIONS

The study seeks to answer the following questions

i. What is the judicial interpretation of a person occupying a responsible position under section 106B (4) (d) of the Evidence Act.

[11] HC Election petition 2 of 2013[2013]eKLR.

ii. What is the correct definition of a person occupying a responsible position under section 106B (4) (d) of the Evidence Act.

1.4 HYPOTHESES

This study proceeds on the presumption that;

i. There is no clear jurisprudence on the interpretation of section 106B (4) (d) of the Evidence Act as to who is a person occupying a responsible position.

1.5 JUSTIFICATION OF THE STUDY

This study is justified on the basis that section 106B (4) (d) of the Evidence Act does not define who is a person occupying a responsible position. The courts on the other hand have given contradicting decisions. This is the problem this paper seeks to address.

Lack of a uniform definition of a responsible person has excluded competent witnesses from giving evidence leading to unsuccessful prosecution of cases. This therefore calls for elaboration or construction of the concept of a person occupying a responsible position under section 106B (4) (d) of the Evidence Act.

1.6 LITERATURE REVIEW

Lucy L. Thomson in her paper discusses the circumstances surrounding the killing of former Libyan dictator Moammar Gaddafi on the streets of Sirte, Libya. She found traditional eyewitness testimony can be greatly enhanced and corroborated by live recordings by observers at the scene by documenting events in detail using digital evidence such as videos, photographs, audio recordings, and real-time commentary on critical event[12]. Further she found live recordings

[12] Lucy L Thomson Esq, 'Human Rights Electronic Evidence Study; Admissibility of Electronic Documentation as evidence in US Courts'(2011) Centre for Research Libraries<

by observers supplement the more carefully documented evidence that is often available in human rights proceedings, including interviews, government records, reports, and databases[13].

This study also proposes use of photographs, video and audio recordings taken by eyewitness at the scene using their mobile phones as evidence in Court. This study is different and unique in that it will determine the person to present photographs, video and audio recordings in court as evidence.

Omeleze and Venter's paper discusses a model for acquiring digital evidence using mobile phone. They found out that many criminal activities have gone unsolved due to lack of sufficient evidence to convict the perpetrator. However, they argue with the evolution of mobile technology, with advanced features such as photo, video and voice recording options have the ability to transform such devices into real-time potential digital forensic evidence-capturing devices[14]. The paper proposes a model that enables the use of mobile and portable devices to capture potential digital evidence and preserve the integrity of such evidence taking into consideration the privacy policies, laws and ethics that may apply to the digital evidence presentation in criminal or civil proceeding[15]. The paper further stresses the need to identify the appropriate tool and use appropriate methods to maintain the forensic integrity of the acquired

---

http://www.crl.edu/sites/default/files/d6/attachments/pages/Thomson-E-evidence-report.pdf> accessed 25th April 2015.

[13] Lucy L Thomson Esq, 'Human Rights Electronic Evidence Study; Admissibility of Electronic Documentation as evidence in US Courts'(2011) Centre for Research Libraries< http://www.crl.edu/sites/default/files/d6/attachments/pages/Thomson-E-evidence-report.pdf> accessed 25th April 2015.

[14] S Omeleze and H S Venter 'Towards a Model for Acquiring Digital Evidence using Mobile phones' <https://www.cscan.org/openaccess/?id=230>accessed 25th April, 2015

[15] S Omeleze and H S Venter 'Towards a Model for Acquiring Digital Evidence using Mobile phones' <https://www.cscan.org/openaccess/?id=230>accessed 25th April, 2015.

data[16]. The paper is important to this study in that it has analyzed tools and methods used to extract mobile phone evidence. This study will now focus on the person presenting the evidence recovered in court and analyze the law applicable.

Timothy M. O'Shea and James Darnell discuss the admissibility of Forensic Mobile phone Evidence. Basically the article covers mobile phone forensics, technical and evidentiary issues[17]. This article will reliably provide a guide to this study to enable understand how mobile phone evidence is collected and who should present that evidence in court under section 106B (4) (d) of the Evidence Act.

Paul McCarthy thesis on forensic analysis of mobile phones assess the forensic soundness of the underlying methods used to acquire the data and the legal admissibility of information acquired by such methods as evidence in a Court of law[18]. His paper is significant to this research. It will enable this study analyse methods used to acquire data from mobile phone in Kenya and address the legal admissibility of evidence acquired under section 106B (4) (d) of the Evidence Act.

Sean Sobieraj discusses an overview of the forensic significance and legal implications of mobile phones[19]. His paper has helped understand the importance of mobile phone forensic evidence and the need to recommend enactment of law to govern its admissibility.

---

[16] S Omeleze and H S Venter 'Towards a Model for Acquiring Digital Evidence using Mobile phones' <https://www.cscan.org/openaccess/?id=230>accessed 25th April, 2015.

[17] Timothy M. O'Shea and James Darnell, "Obtaining and admitting electronic evidence; Admissibility of Forensic Mobile phone Evidence" (2011) United States Attorneys' Bulletin42 <www.justice.gov/sites/default/files/usao/legacy/2011/11/...30/usab5906.pdf >accessed 25th April 2015.

[18] Paul McCarthy, 'Forensic Analysis of Mobile Phones' Bachelor of Computer and Information Science (Honours) Degree, The University of South Australia October 2005 <http://www.8051projectsectionnet/files/public/1236046309_9698_FT19075_forensic_analysis_of_mobile_phonesectionpdf> Accessed 28th March 2015.

[19] Sean C. Sobieraj, 'Mobile phone Forensics Case File Integrity Verification' Degree of Master of Science, Purdue University May 2008 < framework.zend.com/issues/secure/attachment/11259/Thesis-broken.pdf>Accessed 24th march 2015.

Andrew Martins research paper documents in detail the methodology used to examine mobile electronic devices for data[20]. His methodology encompassed the tools, techniques and procedures needed to gather data from a variety of common device[21]. His paper does not address the law applicable in admitting the data recovered as evidence in a court of law. This paper has addressed the need to have unambiguous law on presentation and admissibility of electronic evidence.

Rick Ayers, Sam Brothers and Wayne Jansen discusses procedures for the data acquisition, examination and analysis, preservation, and presentation of digital evidence[22]. They address the issue of ever increasing backlogs for most digital forensics labs and guidance on handling on site triage casework. The objective of the guide is twofold; to help organizations evolve appropriate policies and procedures for dealing with mobile phones and to prepare forensic specialists to conduct forensically sound examinations involving mobile phones[23]. These guidelines will significantly inform this study in examining and proposing how evidence captured by an eyewitness at the crime scene should be admissible in a court of law.

All the literature reviewed above does not address who should present to court mobile phone data evidence captured by an eyewitness at the scene of crime. An eyewitness understands the scene, the items captured and is more reliable to answer any question compared to a person who

[20] Andrew Martin A, 'Mobile phones Forensics' (2009) < http:/www.martinandrew@martinsecurity.net http://www.martinsecurity.net > accessed on 22nd October 2014.
[21] Andrew Martin A, 'Mobile phones Forensics' (2009) < http:/www.martinandrew@martinsecurity.net http://www.martinsecurity.net > accessed on 22nd October 2014.
[22] Rick Ayers, Sam Brothers and Wayne Jansen 'Guidelines on Mobile phone Forensics' Recommendations of the National Institute of Standards and Technology' (2013) NIST Special Publication 800-101 Revision 1< http://nvlpubsectionnist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf> accessed 22nd October 2014.

extracts the data using another machine and issues the certificate as provided under section 106B (4) (d) of the Evidence Act. This study has defined a person occupying a responsible position in relation to the relevant device under section 106B (4) (d) of the Evidence Act to avoid confusion and excluding primary evidence. The definition of a responsible person will firmly introduce and affirm mobile phone forensic evidence as one strong source of electronic evidence.

1.7 THEORITICAL FRAMEWORK

This study is based on criminal investigation theory[24]. The criminal investigation is, in essence, the process of answering questions as to how, where, when, why, and by whom a crime was committed[25]. Whitney D. Gunter, defines investigation as a systematic fact finding and reporting process[26]. Criminal investigation has the end product of bringing someone to justice; that is, arresting, prosecuting, and convicting perpetrators of crimes it must not assume the role of prosecutor, judge, and jury in doing this[27]. That enormous responsibility is why ethics must be the first and foremost characteristic of criminal investigation[28]. Never should the wrong means be used to attain an end, no matter how good the end is.

Charles E. O'Hara and Gregory L. O'Hara states that Criminal investigation is an applied science that involves the study of facts, used to identify, locate and prove the guilt or innocence of a

[24] Monckton J S, Adams T, Adam H, Webb J, Introducing Forensic and Criminal Investigation<https://booksectiongoogle.co.ke/books?isbn=0857027522> accessed 3rd November, 2015.
[25]Peter W. Greenwood, Jan M. Chaiken and Joan Petersilia*, The criminal investigation process* (1977).
[26] Whitney D. Gunter and others, 'An Introduction To Theory, Practice And Career Development For Public And Private Investigators' [2005] < http://www.ifpo.org/wp-content/uploads/2013/08/intro.pdf> accessed 3rd November 2015.
[27] Weston and Lusbaugh 2003,in Brian Kingshotts,'investigation of human trafficking' https://books.google.co.ke/books?id=BhYeBQAAQBAJ&pg=PA92&lpg=PA92&dq=That+enormous+responsibility+is+why+ethics+must+be+the+first+and+foremost+characteristic+of+criminal+investigation&source=bl&ots=7ORdj7-YMG&sig=e5H44jkR418V_N8ilg-icGZdOsc&hl=en&sa=X&redir_esc=y#v=onepage&q&f=false >accessed 3rd November 2015.
[28] Brian Kingshotts, 'investigation of human trafficking' in Michael J. Palmiotto, 'Combating Human Trafficking: A Multidisciplinary Approach'<https://booksectiongoogle.co.ke/books?isbn=1482240394> accessed 3rd November 2013.

criminal[29]. According to Charles E. O'Hara complete criminal investigation can include searching, interviews, interrogations, evidence collection, preservation and various methods of investigation[30]. He further states that modern-day criminal investigations commonly employ many modern scientific techniques known collectively as forensic science. Mobile phone forensics is one of the forensic science that attempts to obtain evidence contained in a mobile phone. The roots of criminal investigation can be traced back to England in the eighteenth century, a period marked by significant social, political, and economic changes[31].

Criminal investigators have a responsibility to ensure that crimes are investigated effectively, documenting all processes and do follow-up investigations[32]. In the case of *Republic v David Ruo Nyambura & 4 others* the Court held that,

> Legal onus in criminal cases is always on the prosecution to prove the guilt of an accused person, and the standard of proof is proof beyond reasonable doubt. An accused person does not assume any burden to prove his innocence in a criminal case. He is obliged only, if he so wishes, to give an explanation or to raise a defence to the charge, which is probably or possibly true. If he does this, then he discharges his burden of proof and his explanation or defence must be accepted[33].

In the case of *Republic v Ibrahim Bille Jelle* the accused was charged with three counts of murder. PW10 PC Antony Ngugi Kuria forensically examined the Nokia mobile phone recovered from the accused and found several short messages in Kisomali language which he did

[29] Charles E. O'Hara, Gregory L. O'Hara, *Fundamentals of Criminal Investigation* (6th edn 1994).
[30] Charles E. O'Hara, Gregory L. O'Hara, *Fundamentals of Criminal Investigation* (6th edn 1994).
[31] Charles R. Swanson and others, *The Evolution of Criminal Investigation and Forensic Science* (11th edn, 2012) <highered.mheducation.com/sites/dl/free/0078111528/928629/ChapterOne.pdf> accessed 3rd November 2013.
[32] Brian Kingshotts, 'investigation of human trafficking' in Michael J. Palmiotto, 'Combating Human Trafficking: A Multidisciplinary Approach'<https://booksectiongoogle.co.ke/books?isbn=1482240394> accessed 3rd November 2013.
[33] HCCRC NO.116 OF 1999[2001]eKLR.

not understand. He did not follow up to know what those messages actually meant. The Court held,

> The hypothesis of the prosecution to connect the accused with the offence was the communication on the Nokia mobile phone. Indeed the Nokia mobile phone which was examined closely by the police was in the possession of the accused. He did not deny ownership, or possession. However a few things stood out with the information therein. Firstly, the written messages therein were said to be in Somali language. No one tried to translate what was contained therein in order to connect the accused to the incident of the killing of the three military officers[34].

The accused was acquitted. This case can be contrasted with the recent legal battle between the Federal Bureau of Investigation (FBI) and Apple over the iPhone belonging to one of the San Bernardino, California, terrorists Rizwan. The Justice Department Federal Bureau of Investigation (FBI) was able to unlock the encrypted iPhone without help from Apple and forensically examination of Rizwan Syed Farook's phone. This case demonstrates United States of America comprehensive mobile forensic investigation. This is a lessons for the Kenyan investigators to learn. They must possess essential qualities such as good communications skills, strong ethics, initiative, resourcefulness and compassion to collect electronic evidence sufficient to prove existence of a certain fact[35]. The contributions of electronic evidence to an investigation are weakened primarily by the inability, unwillingness, or failure to locate, properly collect and document the procedure used, mark, preserve and issue certificates to disclose the source of evidence collected, verify and authenticate it as required by law[36].

[34]HCCRC NO.3 of 2013[2016] eKLR.
[35] Evidence Act Cap 80 Laws of Kenya, S 107 – 110.
[36] Evidence Act Cap 80 Laws of Kenya, S 107 – 110.

1.8 RESEARCH METHODOLOGY

This is basically a desk based research conducted at Parklands School of Law Library. Library research method will be used in the collection and analysis of data from both primary and secondary sources. Primary sources shall include the Evidence Act[37], Constitution of Kenya[38], and Acts of Parliament, Rules and Regulations, government documents and the Court cases. These primary sources shall provide first-hand, original information on laws applicable in this study.

Secondary sources include books, magazines, journals and newspapers which contain writings related to mobile forensic investigation. Library and electronic methods will be used in the collection of secondary information from sources such as archives, information resource centres, public registries, websites and other institutional and individual sources of information. Secondary sources shall provide dates, names and other background information, such as the names and citations of statutes and Court cases. It shall also help scrutinise related subjects or issues and digest or synthesize the information found in primary source.

Further the study shall analyse mobile forensic examinations in Kenya and other jurisdictions like the United States of America and South Africa. The information gathered will be analysed and recommendations on good lessons or best practises Kenya can learn shall be made. Contribution to the study will be available as an LLM thesis which is published on the university website.

[37] Evidence Act Cap 80 Laws of Kenya, s 106 (4) (d)
[38] The constitution of Kenya 2010

1.9 LIMITATION

This study is limited by time and finance. The area of mobile communication technology is growing very fast each day making it difficult to have up to date information on some aspects.

1.10 CHAPTER BREAKDOWN

1.11 CHAPTER ONE

This is the introductory chapter, it will state; the problem, the objectives of the research, the research question, the hypotheses, literature review, the theoretical frame work, methodology and the limitation.

1.12 CHAPTER TWO

This chapter briefly discusses the nature of evidence found in a mobile phone, tools and methods of obtaining data (the forensic process) and challenges encountered. The chapter also briefly makes a comparative analysis of mobile forensic examinations in other jurisdictions like the United States of America and South Africa with a view to consider what good lessons or best practises Kenya can learn. The United States of America was chosen for comparative studies because of its experience of tracking down mobile phone evidence. For example, the forensic examination of Rizwan Syed Farook's phone was crucial for the FBI to obtain data to link him with the shooting at California[39]. South Africa was chosen because of its past apartheid history and the creation of an online neighbourhood watch (ONW) model to acquire potential digital evidence using mobile and portable devices in South African neighbourhoods[40]. The ONW model generates and stores potential digital evidence of criminal acts, which is then available to

[39] Kevin Johnson, Jon Swartz and Marco della Cava, USA TODAY 1:51 pm EDT March 29 2016 <http://www.usatoday.com/story/news/nation/2016/03/28/apple-justice-department-farook/82354040/> Accessed 20th July 2016.

[40] S Omeleze and H S Venter 'Towards a Model for Acquiring Digital Evidence using Mobile phones' <https://www.cscan.org/openaccess/?id=230>accessed 25th April, 2015.

law enforcement agents and digital forensic investigators. The ONW model can be applied in scenarios such as road traffic_offences, domestic violence, robberies and other incidents that require concrete evidence as prove in a Court of law in criminal and civil proceeding.

1.13 CHAPTER THREE

This chapter discusses; judicial interpretation of section 106B (4) (d) of the Evidence Act and defines who is a person occupying a responsible position under section 106B (4) (d) of the Evidence Act, examines authentication, verification and admissibility of mobile phone data evidence in Kenyan Courts. The chapter also examines factors affecting admissibility.

1.14 CHAPTER FOUR

This chapter analyses challenges implementing section 106B (4) (d) of the Evidence Act, lessons that Kenya can learn, summary of findings, conclusion and recommendations of the study.

CHAPTER TWO

2.0 FORENSIC RETRIEVAL OF DATA FROM MOBILE PHONES

2.1 INTRODUCTION

This chapter introduces the idea and practice of retrieving or obtaining digital evidence from a mobile phone. The chapter will mainly be devoted to basic principles; the nature of evidence found in a mobile phone, tools and procedures of obtaining such evidence, authentication and verification of such evidence.

The practice of mobile forensic evidence investigations in Kenya is delegated to the Directorate of Criminal Investigations[41]. The directorate is divided into two major personnel groups; the examiners and investigators[42]. The investigators carry out investigations, seize the mobile phone, prepare police file and testify in Court. The examiners receive the exhibits, forensically examine the exhibits, prepare reports and testify in Courts

There is no legal or documented procedure in Kenya and the world at large on how to conduct mobile forensic examination[43]. Generally mobile forensic investigations encompasses seizure, acquisition and analysis of data recovered from a mobile phone[44]. The examiner must at all times develop a report documenting any pertinent information while preserving integrity of the acquired data[45].

[41] National Police Service Act Cap 84 laws of Kenya, s 35.
[42] National Police Service Act Cap 84 laws of Kenya, s 35.
[43] Rick Ayers, Sam Brothers and Wayne Jansen 'Guidelines on Mobile phone Forensics' Recommendations of the National Institute of Standards and Technology' (2013) NIST Special Publication 800-101 Revision 1< http://nvlpubsectionnist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf> accessed 22nd October 2014.
[44] "Cell Phone and GPS Forensic Tool Classification System" by Sam Brothers in a presentation to Digital Forensics, <http://www.mobileforensicsworld.org/2009/presentations/MFW2009_BROTHERS_CellPhonean dGPSForensicToolClassificationSystem.pdf > May 2009.
[45] Andrew Martin A, 'Mobile phones Forensics' (2009) < http:/www.martinandrew@martinsecurity.net http://www.martinsecurity.net > accessed on 22nd October 2014.

This chapter sets out to examine the tools of obtaining data from mobile phone, methods of data acquisition, challenges posed by the tools and methods in the forensic process and process of authenticating and verifying the obtained data.

2.2 NATURE OF EVIDENCE FOUND IN A MOBILE PHONE

Some of the kinds of data that may be contained and saved in a mobile phone include; call times, dialed and received calls, text messages, contacts, address book entries, residential addresses and email addresses, calendar items, photos, graphics and videos. Such information stored on and associated with mobile phones can be forensically obtained and can help address the crucial questions in an investigation, revealing whom an individual has been in contact with, what they have been communicating about, where they have been and what they have been doing[46]. For example, in the case of *William Odhiambo Oduol V Independent Electoral & Boundaries Commission & 2 Others*[47] the petitioner's chief campaign manager used his cellphone to take a video of ballot papers which one of the Independent Electoral & Boundaries Commission (IEBC) clerks at Ujwanga polling station in Rarieda Constituency had allegedly attempted to stuff in the ballot boxes at the station[48]. He later developed the video clip into a compact disc.

In the case of *Republic V Stojananovic Milan* alias *Allan & Another* one Baktash Akasha (PW 25)[49] recorded a conversation between him and the accused No.1 (Stojananovic Milan). He later

[46]Gary Palmer, 'A Road Map for Digital Forensic Research Technical Report DTR-T0010-01 DFRWS' November 2001. Report from the First Digital Forensic Research Workshop (DFRWS); Brian Carrier,'Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers' Winter 2003, Volume 1, Issue 4 International Journal of Digital evidence <digital4nzicsectioncom/.../Defining%20Digital%20Forensic%20Examination>accessed 13th January, 2016.

[47] HC Election Petition No. 2 of 2013 [2013] eKLR.

[48] HC Election Petition No. 2 of 2013 [2013] eKLR.

[49] HCCA No. 153 of 2004 [2008] eKLR.

reproduced a second tape from the original tape because the original was not clear[50]. The second tape was opposed as evidence because the original tape was not clear.

Comparatively, in the United States of America the Tampa Bay Time's Newspaper reported how Ronald Williams somehow activated his mobile phone which then called his wife's mobile phone while he was killing her. The voice mail recorded the killing with Williams threatening to kill his wife, and Mariama Williams screaming in terror during the attack in their St. Petersburg home. During the trial the assistant state attorney Walter Manning produced a four minute fatal stabbing recording. This was key piece of evidence in Ronald Williams's first-degree murder trial. He was convicted of first-degree murder and sentenced to death'[51].

Similarly the United Kingdom (UK) media the Investigation into the death of 15-month-old Charlie Hunt showed how Darren Newton filmed himself on his mobile phone repeatedly assaulting and doing other acts of cruelty to the 15-month-old Charlie Hunt. Newton recorded footage of Charlie as he sat shivering in a bath after the water had been let out and later that same day filmed himself hitting Charlie on the head repeatedly, giving the clip the title 'Happy Slap. The video clips were found on the mobile phone after Charlie died in hospital from serious head injuries and used as evidence against him. Relying on this mobile phone information, the Court convicted Newton and sentenced him to 24 years behind bars[52]'.

[50] HCCA No. 153 of 2004 [2008] eKLR.
[51] Curtis Krueger 'A mobile phone records a fatal stabbing, becomes key evidence at a murder trial' *Tampa bay times* (Florida, Tuesday February, 8 2011 1:54pm) < http://www.tampabay.com/news/Courts/criminal/a-cell-phone-records-a-fatal-stabbing-becomes-key-evidence-at-a-murder/1150310> accessed 9th February 2016.
[52] Jaya Narain 'Face of the 'happy slap' killer: Sadist who murdered girlfriend's toddler jailed for 26 years' MailOnline (London, 3 December 2010)http://www.dailymail.co.uk/news/article-1335042/Darren-Newton-guilty-Charlie-Hunt-murder-happy-slap-attack-filmed > accessed 17th February, 2016.

In the matter between *The State and Oscar Leonard Carl Pistorius* trial in South Africa the accused *Oscar Leonard Carl Pistorius* shot and killed Steenkamp early morning hours of 14th February, 2013. His phone was examined and showed that the he was on phone at 03:19:03 calling Stander[53]. A minute later he called 911. Thereafter, one and a half minutes later, he called security[54]. The three examples discussed above demonstrates evidence found in mobile phones may in form of a call, video, photograph or sound recordings.

2.3 THE FORENSIC PROCESS

Forensic process is the use of scientifically derived and proven tools and methods towards the collection, preservation, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations[55].

There are three principles in the forensics process commonly known as laws[56]. The first law is to document all and everything. It is only with a good documentation one can follow the process evidentially[57]. The second law is to avoid changes and contamination. If the data is corrupted it becomes useless. The third law states that only competent people with the required degree of training and expertise can explain their actions should have access to the original device.

[53] CC 13 OF 2013 in the High Court of South Africa Gauteng Division, Pretoria 12th September 2014.
[54] CC 13 OF 2013 in the High Court of South Africa Gauteng Division, Pretoria 12th September 2014.
[55] Rick Ayers, Sam Brothers and Wayne Jansen 'Guidelines on Mobile phone Forensics' Recommendations of the National Institute of Standards and Technology' (2013) NIST Special Publication 800-101 Revision 1< http://nvlpubsectionnist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf> accessed 22nd October 2014.
[56] Christian Backer, 'Covert Channels and Embedded Forensics, "Digital Forensics on Small Scale Digital Device" [2009]<https://www.emsec.rub.de/media/crypto/attachments/.../baecker_digital_forensicsectionpdf>accessed 24th October 2014.
[57] Christian Backer, 'Covert Channels and Embedded Forensics, "Digital Forensics on Small Scale Digital Device" [2009]<https://www.emsec.rub.de/media/crypto/attachments/.../baecker_digital_forensicsectionpdf>accessed 24th October 2014.

Generally these laws governs the forensic process which is broken down into three main categories namely; seizure, acquisition, and examination[58].

2.3.1 SEIZURE

'Seizure is the forcible taking of property by a government law enforcement official from a person who is suspected of violating or is known to have violated the law[59]'. Generally a Search Warrant granted by a Court of law must be presented to a person before his or her phone is seized and investigated, unless the circumstances of the seizure justify a warrantless seizure[60]. In the case of *Republic v Chief Magistrate Milimani & another Ex-parte Tusker mattresses Ltd & 3 others* the complainants obtained an order/Warrant to investigate Account No. 0800797212 in the name of the 1st Applicant held with the Diamond Trust Bank Ltd, Mombasa Road Branch[61].

After investigating the Director of Criminal Investigations filed another Miscellaneous Criminal Application No.431 of 2012 and was issued with warrants to search the premises of the 1st Applicant, and the offices occupied by the suspects who are the 2nd, 3rd and 4th Applicants in this matter under section 14(1) and 19 of the Police Act and section 118 of the Criminal Procedure Code.

The investigating officer together with Cyber Crime Analysts and Economic Crime Unit proceeded to the Head Office of the 1st applicant on Mombasa road on the 17th April, 2012 upon serving the search warrants on the 1st applicant, he declined to acknowledge receipt of the search

[58] Christian Backer, 'Covert Channels and Embedded Forensics, "Digital Forensics on Small Scale Digital Device" [2009]<https://www.emsec.rub.de/media/crypto/attachments/.../baecker_digital_forensicsectionpdf>accessed 24th October 2014.
[59] Black's law dictionary.
[60] National Institute of Standards and Technology. Computer Forensic Tool Testing (CFTT). Available at: http://www.cftt.nist.gov. NIST CFTT. Disk Imaging Tool Specification, 3.16 edition, Oct 2001.
[61] Miscellaneous Civil Application No. 179 of 2012 [2013] eKLR.

warrants by way of signing, but allowed the investigators to conduct the search in premises. They searched the premises seized computes, laptops and mobile phones from the heads of departments. The investigators also retrieve electronic records from the seized laptops and computers. According to investigating officer the examiners and the Cyber Crime Analysts were imaging the information in the computers, laptops and mobile phone seized and prepared a forensic report which they would compare with the information in the files, and other correspondence[62].

The police in this case over seized the suspect properties. The order on the other part did not specify what was to be seized. Comparatively in the United States of America, one influential decision was made in the case of *United States v Comprehensive Drug Testing*[63] where the Court recognized that "over-seizure is inherent in cases involving electronically stored evidence and everything seized could be construed to be in 'plain view' as all files were examined[64]. The Court ruled that;

(a) Reliance on the plain rule exception must be waived;
(b) Search protocols should be used that are designed to uncover only the information for which law enforcement has probable cause;
(c) Segregation of nonresponsive materials must be done by parties other than the case agents; and
(d) The government must return or destroy nonresponsive search and seizure issues.

[62] Miscellaneous criminal investigation N. 431 of 2012.
[63] No. 05-55354 D.C. No. CV-04-02887-FMC Inc., 2009.
[64] The plain view doctrine is an exception to the warrant requirement which allows officers to seize items which they observe and immediately recognize as evidence or contraband while they are lawfully present in an area protected by the 4th amendment.

Guided by this decision this study proposes that search and seizure must be specific, otherwise there will arbitrary search seizure.

2.3.2 ACQUISATION.

This is the retrieval of data from the mobile phone seized[65].

2.4 METHODS FOR ACQUIRING DATA FROM MOBILE PHONES

Methods for acquiring data from mobile phones mainly depend on the condition, model, time and nature of the case[66]. The current methods used in Kenya and the rest of the world are; manual acquisition, logical, file system and physical acquisition[67].

2.4.1 MANUAL ACQUISITION

The forensic examiner manually scrolls down through the phone folders using the keypad and display of mobile phone when the phone is on[68]. This is the first method commonly applied by examiners in Kenya. The examiners documents each and every item. For example the examiner may scroll up and down the contacts folders, messages, browser, settings, backup, calendar, clock, google, photos, videos, notebook, music, games, sim tool kit, facebook, whatsapp, play store, camera, to do list, calculator, FM radio and many other folders that a phone may contain

---

[65] National Institute of Standards and Technology. Computer Forensic Tool Testing (CFTT). Available at: http://www.cftt.nist.gov. NIST CFTT. Disk Imaging Tool Specification, 3.16 edition, Oct 2001.
[65] Miscellaneous Civil Application No. 179 of 2012 [2013] eKLR.
[66] Curran K, Robinson A, Peacocke S, Cassidy S (2010) Mobile Phone Forensic Analysis, International Journal of Digital Crime and Forensics, Vol 2, No 2, pp, April-May 2010, ISSN: 1941-6210 IGI Pub <eprintsectionulster.ac.uk/20680/2/IJCDF10.pdf> accessed 23 October 2014.
[67] Keonwoo Kim and others, 'Data Acquisition from Mobile phone using Logical Approach' [2007] 1(8) World Academy of Science, Engineering and Technology International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering<waset.org/.../data-acquisition-from-cell-phone-using-logical-approach>accessed 27th April 2016.
[68] Sam Brothers "Mobile phone and GPS Forensic Tool Classification System" http://www.mobileforensicsworld.org/2009/presentations/MFW2009_BROTHERS_CellPhonean dGPSForensicToolClassificationSystem.pdf <accessed> 17th June 2015.

depending on the model, design and make of the phone[69]. This suggests only data accessible through the operating system is retrievable. Hidden and deleted data cannot be retrieved using manual acquisition. However, it is fast, works on almost every phone, requires no cables and is easy to use[70].

2.4.2 LOGICAL ACQUISITION

Logical acquisition is "what you see is what you get[71]". It is the second method commonly used in Kenya. It involves a bit-for-bit copy of a mobile phone entire storage[72]. For example one can copy the contacts, messages, browser information, calendar information, gallery, video, notebook, music, and downloads file. Copy of image is done to guarantee the integrity of data during analysis process[73]. The benefits are it acquires information from the mobile phone using original applications in the phone' produces the specific file requested, and extracts data that is accessible through the operating system[74]. Finally it does not produce any deleted information because it is not visible[75].

---

[69] Sam Brothers "Mobile phone and GPS Forensic Tool Classification System" http://www.mobileforensicsworld.org/2009/presentations/MFW2009_BROTHERS_CellPhonean dGPSForensicToolClassificationSystem.pdf <accessed> 17th June 2015.

[70] Brian Carrier, 'Defining Digital Forensic Examination and Analysis Tools 'In Digital Research Workshop II 2002 http://www.dfrwsectionorg<accessed> 17th June 2015.

[71] Harald Baier 'Data Acquisition and Foundations of File System Analysis' [2011/2012] < https://www.fbi.h-da.de/fileadmin/.../vorlesung_forensik_ws11-12_kap> accessed 17th February, 2016.

[72] Keonwoo Kim and others, 'Data Acquisition from Mobile phone using Logical Approach' [2007] 1(8) World Academy of Science, Engineering and Technology International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering<waset.org/.../data-acquisition-from-cell-phone-using-logical-approach>accessed 27th April 2016.

[73] "Cell Phone and GPS Forensic Tool Classification System" by Sam Brothers in a presentation to Digital Forensics, <http://www.mobileforensicsworld.org/2009/presentations/MFW2009_BROTHERS_CellPhonean dGPSForensicToolClassificationSystem.pdf > May 2009.

[74] Keonwoo Kim, Dowon Hong, Kyoil Chung, and Jae-Cheol Ryou 'Data Acquisition from Mobile phone using Logical Approach' [2007] Vol:1, No:8, World Academy of Science, Engineering and Technology International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering < waset.org/.../data-acquisition-from-cell-phone-using-logical-approach> accessed 17th February, 2016.

[75] Harald Baier 'Data Acquisition and Foundations of File System Analysis' [2011/2012] < https://www.fbi.h-da.de/fileadmin/.../vorlesung_forensik_ws11-12_kap> accessed 17th February, 2016.

2.4.3 FILE SYSTEM ACQUISITION

It is tracking data that may have been entered in certain files in the mobile phone[76]. It is useful for; understanding the file structure, provides access to deleted data from mobile's internal memory and extracts data hidden from handset[77]. It provides data that is not recoverable by the manual and logical methods. It is the third method commonly applied in Kenya.

2.4.4 PHYSICAL ACQUISITION

Physical extraction recovers deleted data (including system and network provider information like previous International Mobile Subscriber Identity (IMSI), translate coded data, can retrieve data from devices where no SIM is present, bypass (and retrieve) handset security codes and acquire information from password-protected mobile applications such as Facebook, Skype, Whatsapp and browser-saved passwords[78]. It can also create a "complete" memory image and is also useful for memory card analysis[79]. It provides scientifically reputable repeatable reliable evidence through the analysis of physical evidence acquired[80].

2.4.5 EXAMINATION AND ANALYSIS

When data is acquired from a mobile phone it is scrutinized to confirm any connection to the issue under interrogation[81]. The examination and analysis depends on the type of evidence required to prove the existence of the fact in question. In the case of *Republic v Ibrahim Bille*

---

[76] Harald Baier 'Data Acquisition and Foundations of File System Analysis' [2011/2012] < https://www.fbi.h-da.de/fileadmin/.../vorlesung_forensik_ws11-12_kap> accessed 17th February, 2016.

[77] Satish Bommisetty, Rohit Tamma and Heather Mahalik, 'Practical Mobile Forensics' July 2014 https://www.amazon.com/Practical-Mobile-Forensics-Satish-Bommi< accessed> 25th July 2016.

[78] Richard Ayers 'Mobile phone Forensics'< www.cftt.nist.gov/AAFS-MobileDeviceForensicsectionpd > accessed 17th February, 2016.

[79] Data Acquisition <media.uri.edu/cs/csc485/Data_Acquisition/DataAcquisition_TOC.pdf> accessed 17th February, 2016.

[80] Satish Bommisetty, Rohit Tamma and Heather Mahalik, 'Practical Mobile Forensics' July 2014 https://www.amazon.com/Practical-Mobile-Forensics-Satish-Bommi< accessed> 25th July 2016.

[81] HCCRC NO 3 of 2013 [2016] eKLR.

Jelle PW10 PC Antony Ngugi Kuria examined the accused phone and found several short message in Kisomali language which he did not understand. He did not follow up to know what those short message actually said. Therefore there was no evidence to connect the accused to the incident of the killing of the three military officers. According to this case the comprehensive examination and analysis of data acquired is very crucial[82].

2.4.6 TOOLS USED OBTAINING DATA FROM A MOBILE PHONE

The choice of tools used to extract data from a mobile phone mainly depends on the design and type of mobile phone in examination[83]. 'Universal Forensic Extraction Device' (UFED) is the mostly commonly used mobile phone forensic hardware tool in Kenya[84]. It is a hand-held device with optional desktop software, data cables, adapters and other peripheral. It does not require any computer software in order to perform its tasks, it is packaged with report management and analysis software[85]. It can be used for in-field data extraction and analysis under adverse conditions[86]. Also it has the ability to extract both physical and logical data from mobile phones such as cellular phones and other hand-held mobile phones, including the ability to recover deleted data and translate coded and password protected information[87].This implies that whatever activities, sites visited, messages sent or received, call, video, photographs and downloaded

[82] HCCRC NO.3 of 2013[2016] eKLR.
[83] Det Cindy Murphy, 'Cellular Phone Evidence; Data Extraction and Documentation, Developing Process For The Examination Of Cellular Phone Evidence'< http://ccf.cs.uml.edu/forensicspapers/Cellular%20Phone%20Evidence%20Data%20Extraction%20and%20Documentation.pdf> accessed 17th November 2016.
[84] Whitfield, Lee. "Forensic 4cast Awards 2012 – Results". Accessed 10th February, 2016.
[85] Hoog, Andrew. "Chapter 3. Cellebrite UFED". Via Forensics Accessed 10th February, 2016.
[86] Osborne, Charlie. "For investigators, a better way to extract data from mobile phones". SmartPlanet.com. Retrieved July 19, 2012. < http://www.zdnet.com/article/for-investigators-a-better-way-to-extract-data-from-mobile-devices> accessed 10th February 2016.
[87] "UFED 1.2.0.0 Release Notes" (PDF). Cellebrite. Accessed 10th February, 2016.

applications saved or deleted either in known languages or not direct words can be retrieved whether there be a password or not[88].

2.5 CHALLENGES POSED BY TOOLS AND METHODS OF OBTAINING DATA FROM A MOBILE PHONE

Mobile phone is unique and the most commonly used communication gadget in the world today[89]. Portio Research Limited predicts that mobile subscribers will reach 8.5 billion by the end of 2016[90]. Kenya has over 32.8 million mobile phones in use today[91]. These phones are of different models and designs and store information differently[92]. Some of the challenges experienced extracting data include.

2.5.1 IGNORANCE

This is lack of knowledge or illiteracy. In the case of *Republic v Ibrahim Bille Jell* the examiner never tried to translate messages from Kisomali in order to connect the accused to the incident of the killing of the three military officer and the accused was acquitted[93]

---

[88] Det Cindy Murphy, 'Cellular Phone Evidence; Data Extraction and Documentation, Developing Process For The Examination Of Cellular Phone Evidence'< http://ccf.cs.uml.edu/forensicspapers/Cellular%20Phone%20Evidence%20Data%20Extraction%20and%20Documentation.pdf> accessed 17th November 2016.

[89] Det Cindy Murphy, 'Cellular Phone Evidence; Data Extraction and Documentation, Developing Process For The Examination Of Cellular Phone Evidence'< http://ccf.cs.uml.edu/forensicspapers/Cellular%20Phone%20Evidence%20Data%20Extraction%20and%20Documentation.pdf> accessed 17th November 2016.

[90] Dr.Rajesh Kumar Pathank and others, 'New Era of Android Platform – An Operational Method' International Journal of Innovations in Engineering and Technology (IJIET) < ijiet.com/wp-content/uploads/2015/12/34.pdf > accessed 28th August 2016.

[91] Communications Authority of Kenya, quarterly sector statistics report first quarter of the financial year 2014/15 (Jul-Sep 2014) http://techmoran.com/mobile-subscriptions-kenya-increase-32-8-million-penetration-raises-80-5/#sthash.ZeQ5fD7o.dpuf. < Accessed > 17th June 2015.

[92] Det Cindy Murphy, 'Cellular Phone Evidence; Data Extraction and Documentation, Developing Process For The Examination Of Cellular Phone Evidence'< http://ccf.cs.uml.edu/forensicspapers/Cellular%20Phone%20Evidence%20Data%20Extraction%20and%20Documentation.pdf> accessed 17th November 2016.

[93] HCCRC NO.3 of 2013[2016] eKLR.

2.5.2 VOLATILE DATA

The mobile phone evidence is easily accessed, stored, and synchronized across multiple devices[94]. Due to its volatility it is quickly transformed or deleted remotely[95].

2.5.3 RAPID CHANGE IN TECHNOLOGY

The speed of change of technology renders forensic tools useless very fast. This is a challenge to manufactures and investigators to keep pace with the ever evolving technology. In the United States of America the Department of Justice federal bureau of investigation was able to access Syed Farook's iPhone and extract information despite Apple refusing to create a code to access it[96].

2.5.4 JURISDICTION

Some of the mobile crimes are global in nature. For example, Fazul Abdullah Mohammed also known as Fadil Harun[97] was a member of al-Qaeda and the leader of its presence in East Africa[98]. Mohammed was born in Moroni Comoros Island and had Kenyan as well as Comorian citizenship. He spoke French, Kiswahili, Arabic, English and Comorian[99]. He was suspected in Kenya of involvement in three attacks namely; United States of America Embassy bombing in

---

[94] Satish Bommisetty, Rohit Tamma and Heather Mahalik, 'Practical Mobile Forensics' July 2014 https://www.amazon.com/Practical-Mobile-Forensics-Satish-Bommi< accessed> 25th July 2016.

[95] K Curran and others, 'Mobile Phone Forensic Analysis' (2010) 2(2) International Journal of Digital Crime and Forensics, < eprintsectionulster.ac.uk/20680/2/IJCDF10.pdf>accessed 23 October 2014.

[96] Katie Benner And Eric Lichtblau 'U.SECTION Says It Has Unlocked iPhone Without Apple' *The New York Times* (U.S NEW YORK, March 28, 2016) http://www.nytimesectioncom/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html?_r=0 accessed 20th July 2016 Kevin Johnson, Jon Swartz and Marco della Cava, USA TODAY 1:51 pm EDT March 29 2016 http://www.usatoday.com/story/news/nation/2016/03/28/apple-justice-department-farook/82354040/
Accessed 20th July 2016.

[97] Nelly Lahoud, 'Beware of Imitators: Al-Qa'ida Through the Lens of its Confidential'< https://www.ctc.usma.edu/.../beware-of-imitators-al-qaida >Accessed 20th July 2016.

[98] The Long War Journal "Al Qaeda names Fazul Mohammed East African commander "http://www.longwarjournal.org > Accessed 20th July 2016.

[99] Fazul Abdullah Mohammed, Federal Bureau of Investigation, US Department of Justice <http://www.revolvy.com/main/index.php?s=Fazul%20Abdullah%20Mohammed> accessed 20th July 2016.

1998, Paradise Hotel bombing at Mombasa and the launch of two shoulder-fired missiles at an Israeli airliner[100]. His dual citizen enabled him to move in and out of the country and delayed investigations[101].

2.6 CONCLUSION

The constant change of technology has produced different models and design of mobile phone in the market with different brand-name and operating systems[102]. These mobile phone keep daily record of the calls made, text messages sent or received, internet sites visited, videos and photographs. This data is accessed through mobile forensic investigation. Generally mobile forensic investigations encompasses seizure, acquisition and data analysis[103].The choice of tools used to extract data from a mobile phone mainly depends on the design, model and type of mobile phone in examination[104]. The tools and methods of extracting this data differs from the manufacture, model, design and the nature of data sought to be extracted. The methods commonly applied in Kenya are; manual acquisition, logical, file system and physical acquisition[105]. The choice of tool presents some challenges such as volatile data, change of

[100] Aronson, Samuel. "Crime and Development in Kenya". http://www.inquiriesjournal.com/articles/278/crime-and-development-in-kenya-emerging-trends-and-the-transnational-implications-of-political-economic-and-social-instability<accessed> 21st July 2016.

[101] Fazul Abdullah Mohammed, Federal Bureau of Investigation, US Department of Justice <http://www.revolvy.com/main/index.php?s=Fazul%20Abdullah%20Mohammed> accessed 20th July 2016.

[102] Det Cindy Murphy, 'Cellular Phone Evidence; Data Extraction and Documentation, Developing Process For The Examination Of Cellular Phone Evidence'< http://ccf.cs.uml.edu/forensicspapers/Cellular%20Phone%20Evidence%20Data%20Extraction%20and%20Documentation.pdf> accessed 17th November 2016.

[103] "Cell Phone and GPS Forensic Tool Classification System" by Sam Brothers in a presentation to Digital Forensics, <http://www.mobileforensicsworld.org/2009/presentations/MFW2009_BROTHERS_CellPhonean dGPSForensicToolClassificationSystem.pdf > May 2009.

[104] Det Cindy Murphy, 'Cellular Phone Evidence; Data Extraction and Documentation, Developing Process For The Examination Of Cellular Phone Evidence'< http://ccf.cs.uml.edu/forensicspapers/Cellular%20Phone%20Evidence%20Data%20Extraction%20and%20Documentation.pdf> accessed 17th November 2016.

[105] Keonwoo Kim and others, 'Data Acquisition from Mobile phone using Logical Approach' [2007] 1(8) World Academy of Science, Engineering and Technology International Journal of Electrical, Computer, Energetic,

technology, jurisdiction and sometimes ignorance by the investigators and examiners. To retrieve admissible evidence the correct tool, procedure and methods must be applied.

Electronic and Communication Engineering<waset.org/.../data-acquisition-from-cell-phone-using-logical-approach>accessed 27th April 2016.

CHAPTER THREE

3.0 INTERPRETATION AND ADMISSIBILITY OF MOBILE PHONE EVIDENCE IN COURT

3.1 INTRODUCTION

Sometimes in our Courts we face a situation where a witness in the course of giving evidence produces evidence captured by him or her in the ordinary course of life showing a scene of crime that he or she witnessed. When it comes to producing such data as evidence the defense objects because section 106B (4) (d) of the Evidence Act provides that for such evidence to be admissible a certificate must be issued and signed by a person occupying a responsible position under section 106B (4) (d) of the Evidence Act

This chapter examines authentication, verification and admissibility of mobile phone data evidence in Kenyan Courts. It discusses how Kenyan Courts have interpreted section 106B (4) (d) of the Evidence Act and how they have defined a person occupying a responsible position under section 106B (4) (d) of the Evidence Act. Section 106B of the Evidence Act generally provides for the Admissibility of electronic records both in criminal and civil cases. Section 2 of the Evidence Act provides the Evidence Act shall apply to all judicial proceedings in or before any Court other than a Khadhi's Court, but not to proceedings before an arbitrator. This study discusses criminal and civil cases.

3.2 JUDICIAL INTERPRETATION OF SECTION 106B (4) (D) OF THE EVIDENCE ACT.

There is no clear jurisprudence on the interpretation of section 106B (4) (d) of the Evidence Act. Different Courts have given different interpretations on the part of who is a person occupying a responsible position in relation to the device to issue the required certificate. For example, in the

case of *William Odhiambo Oduol V Independent Electoral & Boundaries Commission & 2 Others*[106], the court considered who owned, operated and managed the computer and the particulars of the computer used to produce the CD[107]. The petitioner who operated his phone to capture the video clip was not considered. The Court never gave the petitioner an opportunity to prepare and file the required certificate. The petitioner's evidence was just dismissed. This case can be contrasted with High Court Civil Case of *Nonny Gathoni Njenga & another v Catherine Masitsa & another* where the Standard Media Group through KTN broadcasted on 9th November, 2013 in the Samantha's Bridal Show, Literary work 'Weddings With Noni Gathoni' and dubbed 'The Baileys Wedding Show With Noni Gathoni' the contents and substance which were substantially copied and reproduced from the works which infringed on the copyrights of the 1st Plaintiff Nonny Gathoni Njenga against which injunctive orders had been issued. The Plaintiffs had annexed three (3) DVDs that demonstrated the contemptuous conduct of the respondent. The Court held that;

> However, in the interest of justice, it is my view that the Plaintiffs are at liberty to produce such certificate for the admissibility of the said evidence. When that is done, the Court will be able to examine the evidence and evaluate the probative value of the said DVDs as well as the authenticity. The Respondent has alleged that the DVDs were obtained illegally, however that cannot be ascertained at this stage until the Certificate is filed and the Court is able to determine the source of the DVDs[108].

The two decision above can be distinguished by the reasoning in the criminal case of *Republic v Barisa Wayu Mataguda* where PW11 Sergeant Michael Oduor of CID Mombasa viewed the

[106] HC Election Petition 2 [2013] eKLR.
[107] HC Election Petition 2 [2013] eKLR.
[108] HCCC No 490 of 2013 [2014] eKLR.

CCTV footage at Karama hotel together with PW4 Lydia Kaguna Japheth the owner and made a CD. He submitted that CD as evidence and the Court in the course of making its ruling stated,

> If this CCTV footage was available then it amounted to primary evidence and could very easily and simply have been produced as evidence by PW4. Court wonders why police had to complicate matters by making a CD tape out of the CCTV footage. It would have been far more logical to produce the CCTV footage in its raw form[109].

The Court found the owner of the restaurant to be the responsible person to issue the certificate and not the officer who extracted the CCTV footage from the CCTV camera. Whereas in the *Nonny Gathoni Njenga & another v Catherine Masitsa & another case*[110], the Court considered the plaintiff and gave her opportunity to file the relevant certificate this was contrary in *William Odhiambo Oduol v Independent Electoral & Boundaries Commission & 2 Others*[111] case where the Court considered the producer, the machine and owner of the details of machine producing the certificate. This study concludes that if there was a standard definition of the person occupying a responsible position in relation to the device, magistrate's Court and other persons relying on precedent 'stare decisis' would have uniform decisions.

In the criminal case of *Republic v Edward Kirui,* the accused police constable Edward Kirui was among police officers quelling the riotous mobs gathered at Kondele market on 16th January, 2008 after Mwai Kiabaki was announced winner of the 2008 presidential elections and Orange democratic movement party protested. He was filmed by KTN camera man Mr. Baraka firing at George William Onyango and Ismael Chacha killing them on the spot[112].

[109] HCCRC No 6 of 2008 [2011] eKLR.
[110] HCCC No 490 of 2013 [2014] eKLR.
[111] HC Election Petition 2 [2013] eKLR.
[112] HCCRC NO. 9 of 2008 [2010] eKLR.

At the hearing, a slow motion video clip was played and produced in Court by Peter Opondo a Special Project Editor with KTN showing police constable Edward Kirui firing at the deceased and later lifting up the cover of his helmet to expose his face. The video placed him at the scene firing at the deceased. Mr. Mitei, the learned advocate for the accused, submitted that the prosecution ought to have had the cameraman who had captured the incident, asked to identify the persons shown on the video. It was his further submission that the cameraman should also have been called upon to try and identify the police officer who was captured on the video. The Court rejected an application by the prosecution to have the cameraman produce the video. The video was later admitted after it was produced by one Peter Opondo an editor with KTN who issued an expert certificate as provided for under section 106B (4) (d) of the Evidence Act. Though the video in this case was not captured by a mobile phone it confirms the conditions for the admissibility of electronic evidence in a Court of law. Though peter produced the video he never knew how the video was taken, how the scene looked like or who was capture at the scene. This study is of view that the camera man Mr. Baraka who captured the video photograph at the scene was the right person to produce the video and issue the certificate. The Evidence Act need to be amended to have a standard definition of the person occupying a responsible position contemplated under section 106B (4) (d). Otherwise the right witnesses will be excluded rendering relevant evidence inadmissible.

3.3 WHO IS A PERSON OCCUPYING A RESPONSIBLE POSITION UNDER SECTION 106B (4) (D) OF THE EVIDENCE ACT?

Considering the case law cited above and the Evidence Act, this study is of the view that the definition under section 106B(4)(d) of the Evidence Act does not require any qualification, special expertise, designation in law or specialty for one to be a responsible person capable of

producing electronic evidence. The bar of the person who can produce electronic evidence is so low and it's only for the judicial officer to ascertain the credibility and probative value of the evidence given. Guided by the case of *Republic v Barisa Wayu Mataguda*[113] to contribute new knowledge by defining a person occupying a responsible position in relation to the gadget as,

> The owner of the device and the person operating it to capture some data.

This definition is justified on the basis that the owner of the device is the custodian of the device and therefore well placed to satisfy its working condition and give its particulars. The person operating the device is justified on the ground that he or she personally controls the device to capture the actual data evidence in its raw form. This definition is important to broaden admissibility of evidence and achieve uniformity in decision making.

The case of *William Odhiambo Oduol v Independent Electoral & Boundaries Commission & 2 Others* where the petitioner operated his phone and captured the IEBC clerks at Ujwanga polling station in Rarienda Constituency stuffing ballot boxes at the station justifies why the owner and the person operating the device should be considered as responsible person.

3.4 AUTHENTICATION AND VERIFICATION OF MOBILE PHONE DATA EVIDENCE

Authentication is the basic process of proving evidence is in fact genuine while verification is the process of proving that nothing has been altered since the data evidence was acquired[114]. To demonstrate authenticity and verification for process-generated records, the proponent is required to introduce evidence that describes a process or a system used to produce a result and

[113] HCCRC NO. 6 of 2008 [2011] eKLR.

[114] Eoghan Casey and Benjamin Turnbull, 'Digital Evidence on Mobile Devices' http://booksite.elsevier.com/9780123742681/Chapter_20_Final.pdf>accessed 20th July 2016.

to show that the process or system produces an accurate result[115]. In the case of *William Odhiambo Oduol v Independent Electoral & Boundaries Commission & 2 others* the court did not call the petitioner to produce as part of evidence a video which he personally captured[116]. In the United States Federal Rules of Evidence Section 901(a) states;

> The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.

Federal Rule of Evidence 901(b) offers a non-exhaustive list of authentication methods. For example, Rule 901(b) (1) provides that evidence may be authenticated by a person with knowledge that a matter is what it is claimed to be. In our case the petitioner was at the scene, used his phone to take the photograph and therefore the most qualified with knowledge to prove the evidence was what he claimed it to be. In the case of *United States v. Gagliardi*[117] witness and undercover agent sufficiently authenticated emails and chat log exhibits by testifying that the exhibits were accurate records of communications they had had with the defendant. On whether the proponent need to prove beyond doubt that the evidence is authentic, the Court in the case of *United States* above held, that the proponent need not prove beyond all doubt that the evidence is authentic and has not been altered. Instead, authentication requirements are threshold preliminary standards to test the reliability of the evidence, subject to later review by an opponent's cross-examination. Kenya is yet to entrench authentication and verification prerequisite in the Evidence Act.

[115] Evidence Act 2012, S 107-110.
[116] HC Election Petition No. 2 of 2013 [2013] eKLR.
[117] No. 06-4541 (2d Cir. 2007).

3.5 ADMISSIBILITY OF MOBILE PHONE DATA EVIDENCE IN KENYAN COURTS

Admissible evidence is any evidence that is allowed to be introduced during trial[118].

Section 106B (1) of the Evidence Act[119] provides;

> Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on paper, stored, recorded or copied on optical or electro-magnetic media produced by a computer (herein referred to as "computer output") shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein where direct evidence would be admissible.

Evidence is so sensitive that any slight interference will render it unacceptable. Any act that may render it unacceptable must be avoided. Lack of certificate required under section 106B (4) (d) of the Evidence Act affects admissibility of mobile phone evidence. Some of the other factors are relevance and integrity.

3.5.1 RELEVANCE

Relevance is what is applicable to the issue in question or affording something to the purpose[120]. In the case of *Kuruma Son of Kaniu –V- Republic* [121] the court set out general rule that any material which is relevant and of a probative value is admissible. Nonetheless it set out exceptions as follows;

[118] Law dictionary <thelawdictionary.org/admissible-evidence> accessed 21st March 2016.
[119] Evidence Act 2012 Cap 80 Laws of Kenya.
[120] The Law Dictionary Featuring Black's Law Dictionary Free Online Legal Dictionary 2nd Ed.
[121] [1955] 1 ALL E.R. 236.

i. The accused person is not to give evidence on his own behalf. That is; oral or written statements that incriminate the accused and one made by him must be voluntary and are inadmissible if obtained by intimidation or inducement.

ii. Second, is founded on natural justice that is: a judge has a discretion to exclude a matter the prejudicial effect of which exceeds its prohibitive value.

Section 5 of the Evidence Act on the other part provides that;-

> Subject to the provisions of this act and any other written law, No evidence shall be given in any suit or proceeding except evidence of the existence or non-existence of a fact in issue, and of any other fact declared by any provision of this fact to be relevant[122].

In the case of *William Odhiambo Oduol v Independent Electoral & Boundaries Commission & 2 Others*[123] the video clip was relevant to the issue for determination before the court but was inadmissible because a certificate was not issued as required. In the case of *Republic v Ibrahim Bille Jelle* the messages in Kisomali were not translated in a language understandable by the court in order to connect the accused to the incident of the killing of the three military officers. Therefore the evidence extracted from the mobile phone was irrelevant[124].

3.5.2 INTEGRITY

Integrity of the digital evidence affects admissibility of electronic evidence. In the case of *Mohamed Koriow Nurv Attorney General* Mr. Buchianga an investigator with Anti-Corruption commission organised a meeting with the Petitioner. In the course of the meeting, through a concealed recording, Mr. Buchianga engaged the Petitioner in a mock bribe-bargaining that led

[122] Evidence Act 2012, Cap 80 Laws of Kenya Chapter II part 1.
[123] HC Election Petition 2 [2013] eKLR.
[124] HCCRC NO. 3 of 2013 [2016] eKLR.

them to settle on a bribe of 1 million shillings payable in two instalments of Kshs 500,000 each. It was further agreed that the first instalment would be paid the following day. On 15/3/2007 Mr Buchianga proceeded to the agreed venue with five other officers with a view to arrest the Petitioner if he bribed him as he had promised the previous day. The Petitioner arrived at the scene and allegedly gave a brown envelope which contained Kshs 500,000. He was promptly arrested and charged with three offences relating to the contravention of the Anti-Corruption and Economic Crimes Act, No 3 of 2003. The Court held as follows;

> Taking into consideration the above factors, this Court concludes that the actions and conduct of Mr. Buchianga went beyond those of undercover agent because he instigated the offence and that there is nothing to suggest that without his intervention and participation, the offence would have nevertheless been committed[125].

This case prohibits set-up and seeks to maintain integrity of electronic data evidence. The integrity test ensures an accurate presentation of the facts.

3.6 CONCLUSION

Section 106B (4) (d) of the Evidence Act requires that a certificate must be presented by a person occupying a responsible position under section 106B (4) (d) of the Evidence Act. However the act does not define who this responsible person in relation to the device is. The Courts on the other hand have given different decisions. This study is of the view that the definition under section 106B(4)(d) of the Evidence Act does not require any qualification, special expertise, designation in law or specialty for one to be a responsible person capable of producing electronic evidence. The bar of the person who can produce electronic evidence is so low and it's only for

[125] HC Petition 181 of 2010 - [2011] eKLR.

the judicial officer to ascertain the credibility and probative value of the evidence given. Guided by the case of *Republic v Barisa Wayu Mataguda*[126] to contribute new knowledge by defining a person occupying a responsible position in relation to the gadget as,

> The owner of the device and the person operating it to capture some data.

This definition is justified on the basis that the owner of the device is the custodian of the device and therefore well placed to satisfy its working condition and give its particulars. The person operating the device is justified on the ground that he or she personally controls the device to capture the actual data evidence in its raw form. This definition is important to broaden admissibility of evidence and achieve uniformity in decision making.

Once the responsible person is properly defined, the evidence recovered requires to be authenticated and verified before it admitted. Evidence is so sensitive that any slight interference will render it unacceptable. Lack of certificate required under section 106B (4) (d) of the Evidence Act affects admissibility of mobile phone evidence. Some of the other factors are relevance and integrity.

[126] HCCRC NO. 6 of 2008 [2011] eKLR

CHAPTER FOUR

4.0 CHALLENGES IMPLEMENTING THE DEFINITION OF THE RESPONSIBLE PERSON UNDER SECTION 106B (4) (D) OF THE EVIDENCE ACT

Long period preparing the bill. The attorney general will prepare policy instructions. These instructions will in turn form the basis of instructions to the Office of Parliamentary Counsel to draft the Bill. Instructions to counsel will set out the background and relevant current law and explain the changes in the law to be brought about by the Bill. They will analyze the instructions and may have questions that need to be answered before drafting can begin. Once the drafters feel they have a clear idea of the policy, they will send drafts to the relevant departmental lawyer. The lawyer will discuss the drafts with the relevant policy officials and send comments back. This

Lack of political will. When passing the law there may be some political cost as the law may upset some people and please others. "Political will" refers to that collective amount of political benefits and costs that would result from the passage of any given law[127].

Lack of finances. Amending section 106B (d) (4) of the evidence act to define a person occupying responsible position involves formulating the bill through political channel and subjecting it to the interested groups, government bureaucracies and parliament[128]. This requires finances.

Political priorities of the Government. The government or a member of parliament will be required to present the bill to the parliament. Both must be convinced of the need for the Bill.

[127]< https://assets.publishing.service.gov.uk/media/57a08cbfed915d622c001551/R8236Appendix3.pdf>.

[128] Mulyanyuma, 'the challenges in policy formulation policy analysis and implementation in developing countries'< http://www.slideshare.net> accessed 19th November 2016.

They may want to consider whether a similar outcome can be achieved without legislation. The political priorities of the government may take precedence over the amendment.

4.1 WHAT LESSONS KENYA CAN LEARN FROM THIS STUDY?

Kenya can learn best practice in mobile phone forensic examination.

The general rules of evidence should be applied to all digital evidence[129];

1. Upon seizing digital evidence, actions taken should not change that evidence.
2. When it is necessary for a person to access original digital evidence that person should be suitably trained for the purpose.
3. All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.
4. An individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession.

Criminalizing unlawful access to data. Section 86 of the South Africa Electronic Communications and Transactions Act creates statutory criminal offences aimed at addressing cybercrimes.[130] Section 86(1) creates a criminal offence of unlawful access to data. 'A person who intentionally accesses data without permission or authority is guilty of such an offence'. As a result, certain data can only be accessed by certain people hence it ensures that evidence is not tampered with during obtaining of digital evidence.

[129]Kessler, G C (2015) 'Are Mobile Device Examinations Practiced Like 'Forensics? *Digital Evidence and Electronic Signature Law Review, (2015) 12*(). http://dx.doi.org/10.14296/deeslr.v12i0.2237.

[130] Jason Jordaan, 'Ensuring the Legality of the Digital Forensics Process in South Africa' (2013) 68(23) International Journal of Computer Applications (0975 – 8887) < http://www.lex-informatica.org/Ensuring%20the%20Legality%20of%20the%20Digital%20Forensics%20Process%20in%20South%20Africa.pdf> accessed 14th October 2014.

Kenya should similarly create statutory offences that protect the obtaining of digital evidence in order to ensure that digital evidence is obtained and presented in court without tampering thus making it reliable.

Public investigative institutions engaged in obtaining digital evidence should work together with private actors who have more specialized knowledge. For example the Federal Bureau of Investigation (FBI) and the Justice Department were able to unlock Rizwan Syed Farook's phone encrypted iPhone with help from a third party and forensically examined it.

When tendering evidence the best evidence rule applies. Section 15 of the Electronic Communications and Transactions Act 25 of 2002 provides that the rules of evidence must not be applied to deny the admissibility of a data message purely because it is constituted by a data message, or on the grounds that it is not in its original form, if it is the best evidence that the person adducing it can obtain.[131]. However, there is a set threshold of admissibility of digital evidence. Such threshold principles for admissibility of digital evidence include[132]:

1. The reliability of the manner in which the data message was generated, stored or communicated;
2. The reliability of the manner in which the integrity of the data message was maintained;
3. The manner in which its originator was identified; and
4. Any other relevant factor.

[131] Johann Herschensohn, 'IT Forensics: The Collection and Presentation of Digital Evidence' http://icsa.cs.up.ac.za/issa/2005/Proceedings/Full/076_Article.pdf > accessed 20th October, 2014.
[132] Johann Herschensohn, 'IT Forensics: The Collection and Presentation of Digital Evidence' http://icsa.cs.up.ac.za/issa/2005/Proceedings/Full/076_Article.pdf.

In South Africa, the position is that when a data message is used merely to establish the fact that information in it was sent, received or stored the law of evidence does not exclude it on the basis of hearsay. Where a data message is however used to show the truth of its contents, the common law requires that the person responsible for the message should be available to be cross-examined about its contents. If this cannot be done, the data message is hearsay and will be inadmissible as doubt exists regarding the reliability of its content and not about the reliability of the technology used.[133] This standard may be borrowed to apply to admissibility of digital evidence in Kenya.

Admissibility of electronic evidence in court in the United State of America, The Federal Rules of Civil Procedure and the Federal Rules of Evidence govern admissibility of digital evidence in federal court whereas State court rules of procedure and evidence, which may differ by State, govern admissibility in state courts.[134] In order for electronic evidence to be admissible in federal courts, there are five foundations which need to be proved. These are: relevance, authenticity, rule on hearsay, the best evidence rule and probative value must outweigh any prejudicial effect.[135]

From this, Kenya can learn that with technology which is ever advancing, there might arise certain cases with special circumstances than others. Therefore, the courts should not limit themselves to the basic criterion set for admissibility of digital evidence. The courts should

[133] Prof. Murdoch Watney, 'Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position' (2009) 1 Electronic Law Journals Journal of Information Law & Technology<http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2009_1/watney/watney> accessed 20th November 2016.

[134] Lucy L Thomson, Admissibility of Electronic Documentation As Evidence in U.S Courts, December 1 2011 Center for Research Libraries. Available at www.crl.edu/sites/default/files/d6/attachments/pages/Thomson-E-evidence-report.pdf.

[135] Lucy L Thomson, Admissibility of Electronic Documentation As Evidence in U.S Courts, December 1 2011 Center for Research Libraries. Available at www.crl.edu/sites/default/files/d6/attachments/pages/Thomson-E-evidence-report.pdf.

instead make use of their judicial discretion when it comes to such cases in order to determine what degree of admissibility, above the basic criterion, should be established and the reasons therefore should be given.

One key thing that Kenya needs to bear in mind is that technology is continuously changing with new evolutions coming up every day. As a result, as more sophisticated technology arises so do new ways of committing crimes. Therefore, new procedures need to be developed in obtaining evidence from such digital devices and the standards of admissibility should be continuously reviewed to keep up with the ever changing field of technology[136]. This should be done with the assistance of experts with those fields because law is created to regulate society. It must therefore understand the society that it seeks to regulate.

4.2 SUMMARY OF FINDINGS

The admissibility of electronic evidence or mobile phone evidence in Kenya is unsatisfactory. The Evidence Act does not define who is a person occupying a responsible position. The Courts on the other part have given contradicting decisions. This study concludes that the definition under section 106B (4) (d) does not require any qualification, special expertise, designation in law or specialty for one to be a responsible person capable of producing electronic evidence. The bar of the person who can produce electronic evidence is so low and it's only for the judicial officer to ascertain the credibility and probative value of the evidence given. This study contributes to knowledge by defining a person occupying a responsible position in relation to the gadget as,

[136] Lucy L Thomson Esq, 'Human Rights Electronic Evidence Study; Admissibility of Electronic Documentation as evidence in US Courts'(2011) Centre for Research Libraries< http://www.crl.edu/sites/default/files/d6/attachments/pages/Thomson-E-evidence-report.pdf> accessed 25th April 2015.

The owner of the device and the person operating it to capture some data.

This definition is justified on the basis that the owner of the device is the custodian of the device and therefore well placed to satisfy its working condition and give its particulars. The person operating the device is justified on the ground that he or she personally controls the device to capture the actual data evidence in its raw form. This definition is important to broaden admissibility of evidence and achieve uniformity in decision making.

There is no standard procedure for analysing each and every mobile phones internal memory[137]. The choice of tools and methods used to extract data from a mobile phone mainly depends on the design, model and type of phone in examination[138].

Mobile phone forensic evidence supplements the oral evidence in courts[139]. It is stronger than human memory which is mortal[140]. Its usefulness depends on how that evidence is obtained, preserved, authenticated and presented in Court[141].

The Evidence Act does not have a specific provision for the authentication and verification of electronic evidence. Section 107 – 110 of the Evidence Act sets mandatory onus on the party seeking to rely on certain evidence to specifically proof the soundness of the evidence he or she

[137] Timothy M. O'Shea, James Darnell, "Obtaining and admitting electronic evidence; Admissibility of Forensic Mobile phone Evidence" (2011)42 <www.justice.gov/sites/default/files/usao/legacy/2011/11/.../usab5906.pdf <accessed> 25th April 2015.

[138] Det Cindy Murphy, 'Cellular Phone Evidence; Data Extraction and Documentation, Developing Process For The Examination Of Cellular Phone Evidence'< http://ccf.cs.uml.edu/forensicspapers/Cellular%20Phone%20Evidence%20Data%20Extraction%20and%20Documentation.pdf> accessed 17th November 2016.

[139] Lucy L Thomson Esq, 'Human Rights Electronic Evidence Study; Admissibility of Electronic Documentation as evidence in US Courts'(2011) Centre for Research Libraries< http://www.crl.edu/sites/default/files/d6/attachments/pages/Thomson-E-evidence-report.pdf> accessed 25th April 2015.

[140] CC 13 of 2013, in the High Court of South Africa Gauteng Division, Pretoria 12th September 2014.

[141] HC Election Petition 2 of 2013[2013] eKLR.

seeks to rely on. The party also must be able to demonstrate similar evidence would be obtained if the same acquisition, tools, processes, procedures and methods were to be used[142].

4.3 CONCLUSION

Section 106B (4) (d) of the Evidence Act requires that a certificate must be presented by a person occupying a responsible position under section 106B (4) (d) of the Evidence Act. However the act does not define who this responsible person in relation to the device is. The Courts on the other hand have given different conflicting decisions. This study concludes that the definition under section 106B(4)(d) of the Evidence Act does not require any qualification, special expertise, designation in law or specialty for one to be a responsible person capable of producing electronic evidence. The bar of the person who can produce electronic evidence is so low and it's only for the judicial officer to ascertain the credibility and probative value of the evidence given. Guided by the case of *Republic v Barisa Wayu Mataguda*[143] this study contributes to knowledge by defining a person occupying a responsible position in relation to the gadget as,

> The owner of the device and the person operating it to capture some data.

This definition is justified on the basis that the owner of the device is the custodian of the device and therefore well placed to satisfy its working condition and give its particulars. The person operating the device is justified on the ground that he or she personally controls the device to capture the actual data evidence in its raw form. He or she can be called if need be to give further and better particulars of how he captured the data and the scene. This definition is important to broaden admissibility of evidence and achieve uniformity in decision making.

[142] Evidence Act 2012, s 107 – 110.
[143] HCCRC NO. 6 of 2008 [2011] eKLR.

4.4 RECOMMENDATIONS

1. This study urges the parliament to amend the Evidence Act to adopt the definition of the person occupying a responsible position in relation to the gadget as set out under section 106B (4) (d) of the Evidence Act as,

   'The owner of the device and the person operating it to capture some data'

   This definition is justified on the basis that the owner of the device is the custodian of the device and therefore well placed to satisfy its working condition and give its particulars. The person operating the device is justified on the ground that he or she personally controls the device to capture the actual data evidence in its raw form. He or she can be called if need be to give further and better particulars of how he captured the data and the scene. This definition is important to broaden admissibility of evidence and achieve uniformity in decision making.

2. The parliament to enact a law to govern search, seizure, extraction and analysis of data acquired from mobile phone and other electronic devices. Seizure is the forcible taking of property by a government law enforcement official from a person who is suspected of violating or is known to have violated the law[144]. Generally a Search Warrant granted by a Court of law must be presented to a person before his or her phone is seized and investigated, unless the circumstances of the seizure justify a warrantless seizure the affected person must be explained the law allowing the search[145]. Guided by the case cited above, this study urges the parliament to draft a law to confine police investigators and examiners to search, seizure and analyse what is contained in the search warrant only. If there is need to gather more

[144] Black's law dictionary.
[145] National Institute of Standards and Technology. Computer Forensic Tool Testing (CFTT). Available at: http://www.cftt.nist.gov. NIST CFTT. Disk Imaging Tool Specification, 3.16 edition, Oct 2001.

evidence not covered by the search warrant, officers should guard the scene and obtain a further search warrant to avoid arbitrary search. This will protect against unreasonable search and seizure by police and other government investigators.

3. The parliament to enact a law to govern the process of recording voice or sound conversation and or taking data evidence using a mobile phone and other electronic gadget. The recording and use of voice or sound recordings as evidence is one of the most misunderstood areas of legal practice in Kenya[146]. For example the recording of Alfred Keter threatening Gilgil weighbridge staff for refusing corruption. The ordinary Kenyan citizen cannot understand why Keter was not charged in a court of law[147]. Same was the case in 2006 when Mr. Githongo former governance permanent secretary of Kenya secretly recorded Mr. Kiraitu Murungi former Minister of Justice and Constitutional Affairs in Kenya where he advised him to 'go slow' on his investigations[148]. The question to ask is whether secretly recorded mobile phone or any other electronic recording is admissible in a court of law in Kenya. For example Ababu Namwamba secretly recorded the cord leader Raila Amollo Odinga using mobile phone to gather evidence over graft claims in Public Accounts Committee[149].
4. The parliament to enact rules of evidence to verify and authenticate the various types of data obtained from mobile phones and other electronic gadgets. Electronic Evidence has involved into a fundamental pillar of evidence. Section 106B of the Evidence Act general provides admissibility of electronic evidence. It is not specific on how to validate that evidence.

[146] Chelanga, 'Admissibility of Video/Electronic Evidence in Kenya - What you see is not what you get' (2012) http://chelanga-advocates.blogspot.co.ke/2012/06/admissibility-of-videoelectronic.html
[147] ANGIRA ZADOCK and JACQUELINE KUBANIA, Alfred Keter claims officers at Gilgil weighbridge were soliciting bribes' Daily nation (Nairobi, Sunday 25th January 2015).
[148] John Githongo, 'cover letter accompanying report on my findings of graft in the government of Kenya' 22nd November 2005.
[149] John Ngirachu 'Secret Ababu Namwamba tape that's causing ruckus' D*aily Nation (*Nairobi, Sunday, March 8, 2015<http://www.nation.co.ke> accessed 11 April 2016.

Mobile phone digital evidence is one form of electronic evidence increasingly being used in Civil and Criminal Litigations[150]. During trials, Judges and magistrates are often asked to rule on the admissibility of electronic evidence and it substantially impacts the outcome of civil suit or conviction / acquittal of the criminal case. The Courts continue to grapple with this new electronic frontier as the unique nature of digital evidence, as well as the ease with which it can be fabricated or falsified, creates hurdle to admissibility not faced with the other evidences[151]. Neeraj Aarora states various categories of electronic evidence such as website data, social network communication, e-mail, and computer generated documents poses unique problem and challenges for proper authentication[152].

5. The parliament to enact law to create statutory offences that protect the obtaining of digital evidence in order to ensure that digital evidence is obtained and presented in court without tampering thus making it reliable. This will ensure integrity of the data.

[150] Neeraj Aarora, 'Admissibility of Electronic Evidence : Challenges for Legal Fraternity' (2015) http://www.neerajaarora.com/admissibility-of-electronic-evidence-challenges-for-legal-fraternity/ accessed 20th November 2016.

[151] Neeraj Aarora, 'Admissibility of Electronic Evidence : Challenges for Legal Fraternity' (2015) http://www.neerajaarora.com/admissibility-of-electronic-evidence-challenges-for-legal-fraternity/ accessed 20th November 2016.

[152] Neeraj Aarora, 'Admissibility of Electronic Evidence : Challenges for Legal Fraternity' (2015) http://www.neerajaarora.com/admissibility-of-electronic-evidence-challenges-for-legal-fraternity/ accessed 20th November 2016. The Indian Evidence Act has been amended by virtue of Section 92 of Information Technology Act, 2000 (Before amendment). Section 3 of the Act was amended and the phrase "All documents produced for the inspection of the Court" were substituted by "All documents including electronic records produced for the inspection of the Court". Regarding the documentary evidence, in Section 59, for the words "Content of documents" the words "Content of documents or electronic records" have been substituted and Section 65A & 65B were inserted to incorporate the admissibility of electronic evidence.

BIBLIOGRAPHY

1. "Cell Phone and GPS Forensic Tool Classification System" by Sam Brothers in a presentation to Digital Forensics, <http://www.mobileforensicsworld.org/2009/presentations/MFW2009_BROTHERS_CellPhonean dGPSForensicToolClassificationSystem.pdf > May 2009.
2. Al-Zarouni M, `Mobile Handset Forensic Evidence: A Challenge for Law Enforcement' (2006), originally published in the proceedings of the Australian Digital Forensics Conference Edith Cowan University Perth West Australia<http://ro.ecu.edu.au/adf/24>accessed on 24th September 2014.
3. Brian Carrier, Defining Digital Forensic Examination and Analysis Tool In Digital Research Workshop II, 2002. Available at: http://www.dfrwsectionorg.
4. Chet Hosmer. Proving the Integrity of Digital Evidence with Time. International Journal of Digital Evidence, 1(1). Spring 2002.
5. Curran K, Robinson A, Peacocke S, Cassidy S (2010) Mobile Phone Forensic Analysis, International Journal of Digital Crime and Forensics, Vol 2, No 2, pp, April-May 2010, ISSN: 1941-6210 IGI Pub < eprintsectionulster.ac.uk/20680/**2**/IJCDF10.pdf> accessed 23 October 2014.
6. Curzon LB, *Jurisprudence*: *Lecture Notes* (2nd edition, cavendish publishing limited 1995) 83.
7. Engman M, 'Forensic investigations of apples iPhone' (2013) Maj Kandidatuppsats www.diva-portal.org/smash/get/diva2:651693 /FULLTEXT01.pdf accessed 14 October 2014.

8. Eoghan Casey and Benjamin Turnbull, 'Digital Evidence on Mobile Devices' http://booksite.elsevier.com/9780123742681/Chapter_20_Final.pdf>accessed 20th July 2016.
9. Eoghan Casey. Error, Uncertainty, and Loss in Digital Evidence. International Journal of Digital Evidence, 1(2), Summer 2002.
10. Finnis J, *Natural and Natural Rights* (1980).
11. Freeman MDA, *Lloyd's Introduction to Jurisprudence* (8th edn, Thomson Reuters 2008) 849-857.
12. Greenwood Peter W, Chaiken Jan M and Petersilia Joan, *The criminal investigation process* (1977).
13. Gunter D and others, 'An Introduction To Theory, Practice And Career Development For Public And Private Investigators' [2005] < http://www.ifpo.org/wp-content/uploads/2013/08/intro.pdf> accessed 3rd November 2015.
14. Harris JW, *Legal Philosophies* (2nd edition, Lexis Nexis Butterworths 2003) 19 – 20.
15. HLA Hart, *The Concept of Law* (2nd edn, Oxford University Press Inc 1994) 193 – 200.
16. Hoog A and Strezmpka K, `Iphone and IOS Forensics Investigation Analysis and Mobile Security for Apple iPhone iPad and IOS Devices' (2011), Elseiver Science,<http://uae.souq.com/ae-en/iphone –and-iOS-forensics by Andrew Hoog-and-Katie-Strezmpka-4709107/i/>accessed on 23rd September 2014.
17. Kingshotts Brian, 'investigation of human trafficking' in Michael J. Palmiotto, 'Combating Human Trafficking: A Multidisciplinary Approach'<https://booksectiongoogle.co.ke/books?isbn=1482240394> accessed 3rd November 2013.

18. Lewis DL, 'Examining Cellular Phones and Handheld Device' (2009) <www.forensicmag.com/ar...p?pid=288> accessed 16th October 2014.

19. Martin A, 'Mobile phones Forensics' (2009) http:/www.martinandrew@martinsecurity.net http://www.martinsecurity.net> accessed on 22nd October 2014.

20. Microsoft Organization. FAT: General Overview of On-Disk Format, 1.03 edition, December 2002.

21. Monckton J S, Adams T, Adam H, Webb J, Introducing Forensic and Criminal Investigation<https://booksectiongoogle.co.ke/books?isbn=0857027522> accessed 3rd November, 2015.

22. Murphy Det Cindy, 'Cellular Phone Evidence; Data Extraction and Documentation, Developing Process For The Examination Of Cellular Phone Evidence'< http://ccf.cs.uml.edu/forensicspapers/Cellular%20Phone%20Evidence%20Data%20Extraction%20and%20Documentation.pdf> accessed 17th November 2016.

23. NIST. Computer Forensic Tool Testing (CFTT). Available at: http://www.cftt.nist.gov. NIST CFTT. Disk Imaging Tool Specification, 3.16 edition, Oct 2001.

24. O'Shea MT and Darnel J, 'Obtaining and Admitting Electronic Evidence: Admissibility of Forensic Mobile phone Evidence' (2011) 59(6) 42 United States Attorneys' Bulletin < www.justice.gov/.../usab5906> accessed on 22nd October 2014.

25. O'Hara Charles E, O'Hara Gregory L, Fundamentals of Criminal Investigation (6th edn 1994) ISBN 0-398-05889-X.

26. Peter Gutmann. Secure Deletion of Data from Magnetic and Solid-State Memory. In Proceedings of the 6 the USENIX Security Symposium, 1996.

27. Punja S, 'Mobile phone Analysis in Small Scale Digital Device' (2008)1 Forensics Journal <http://www.ssddfj.org/papers/SSDDFJ_V2_1_Punja_Mislan.pdf> accessed 22nd October 2014.

28. Raymond Wacks, *Understanding Jurisprudence: An Introduction to Legal Theory* (Oxford University Press 2005) 21.

29. Swanson Charles R. and others, The Evolution of Criminal Investigation and Forensic Science (11th edn, 2012). <https://www.amazon.com/Criminal-Investigation-Charles-Swanson/... >accessed 3rd November 2013.

30. Thomson Lucy L Esq, 'Human Rights Electronic Evidence Study; Admissibility of Electronic Documentation as evidence in US Courts'(2011) Centre for Research Libraries< http://www.crl.edu/sites/default/files/d6/attachments/pages/Thomson-E-evidence-report.pdf> accessed 25th April 2015. Whitney.