ENHANCED MOBILE FORENSIC PROCESS MODEL FOR HAND-HELD DEVICES – A CASE OF SMARTPHONES

BY
JANE M. MUTIA

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF DEGREE OF MASTER OF SCIENCE IN DATA COMMUNICATION IN THE SCHOOL OF COMPUTING AND INFORMATION MANAGEMENT AT KCA UNIVERSITY

NOVEMBER, 2013

DECLARATION

I declare that this Research project is my original work and has not been previously published or submitted elsewhere for award of a degree. I also declare that this Research project contains no material written or published by other people except where due reference is made and author duly acknowledged.

Student Name: …………………………………………Reg. NO….…………………..

Sign: _______________________________________Date: ___________________

I do hereby confirm that I have examined the master's Research project of

AND have certified that all revisions that the Research project panel and examiners recommended have been adequately addressed.

Sign: ____Date: __________________

ENHANCED MOBILE FORENSIC PROCESS MODEL FOR HAND-HELD DEVICES – A CASE OF SMARTPHONES

ABSTRACT

This research is aimed at developing an operating system independent mobile forensics Process Model for Hand-held devices. The earlier works in digital forensics process model have mainly concentrated on process models for computers while those that have dealt with mobile devices are mainly Operating system specific hence they can only be applied to a specific Operating System mobile device. In order to yield the enhanced process model, the researcher examines the various existing process models tailored for the specific operating Systems picking the outstanding phases and combining these various phases to give a neutral yet an enriched process model which is Operating system independent. The proposed Hand-held Process Model is tested using two types of Phones that run different Operating Systems namely iPhone (iOS) and Samsung Galaxy S III (Android OS). Three mobile Forensics tools mainly Cellebrite UFED Physical Analyzer, Oxygen Forensic Suite 2013 and MOBILedit forensics Lite are used to facilitate the experimental tests.

Key words: Mobile Forensics, Process Model, Smartphones, Hand-held Device (s)

TABLE OF CONTENTS

DEDICATION

I dedicate this dissertation to all my family members. When things were very tough and i felt like giving up, they were always there to give me a shoulder to lean on and moreso encourage me. Their endless love and moral support gave me the spirit to keep on!

LIST OF FIGURES

LIST OF TABLES

ACRONYMS AND ABBREVIATIONS

ARM - Advanced RISC Machines

ASCII - American Standard Code for Information Interchange

2D - Two Dimensional

BSD - Berkeley Software Distribution

3D - Three Dimensional

EMFPM – Enhanced Mobile Forensics Process Model

EXT – Extended file system

EXT3 - Third Extended File system

FAT – File Allocation Table

FB- Facebook

GIS - Geographic information system

GPS - Global Positioning System

IDC - International Data Corporation

iOS - iPhone Operating System

Java ME – Java Micro Edition

LAN- Local Area Network

MAN- Metropolitan Area Network

MB – Megabyte

MDS - Mobile Data Service

MIPS - Million Instructions Per Second

MMS - Multimedia Messaging Service

MP3 -Moving Picture Experts Group Layer-3 Audio

MPEG-4 - Motion Picture Experts Group Layer-4 Video

MS-Word – Microsoft Word

NIJ - National Institute of Justice

NIST - National Institute of Standards and Technology

NTFS – New Technology File System

OS – Operating System

PC – Personal Computer

PDA – Personal Digital Assistant

PNG - Portable Network Graphics

RAM – Random Access Memory

RIM API - Research in Motion Application programming interface

RIM JVM – Research in Motion Java Virtual Machine

ROM – Read Only Memory

SIM - Subscriber Identity Module

SMS - Short Message Service

SNAs- Social Networking Applications

UI- User Interface

WiFi- Wireless Fidelity

WiMAX - Worldwide Interoperability for Microwave Access

VM – Virtual Machine

VMWare – Virtual Machine Software

YAFFS2 - Yet Another Flash Filing System

TERMS AND DEFINITIONS

Mobile Forensics is “a branch of digital forensics that deals with the recovery of digital evidence from mobile devices” (nvdigitalforensics.com, 2013).

A Process Model (Digital forensic process) is “a recognized scientific and forensic process used in digital forensics investigations”, (computerforensicsworld.com, 2013).

A Handheld Device is a pocket-sized computing gadget which has a display screen and input/output interface like an external or touch screen keyboard. Such devices and gadgets include mobile phones, PDAs and Tablets, (Author, 2013).

A Smartphone is a mobile phone with very advanced features. A typical smartphone has a WiFi connectivity, a high-resolution touch screen display, Web browsing capabilities and ability to support a wide range of applications, (techopedia.com, 2013).

CHAPTER ONE: INTRODUCTION

Introduction

The rise in sophisticated handheld devices such as smartphones is driving digital forensics into a new dimension. Digital forensics can be defined as the “application of science in identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data”, (Kent et al., 2006).

According to (Yadav, 2011), digital forensics can be classified into four types of areas as shown in figure 1.1;

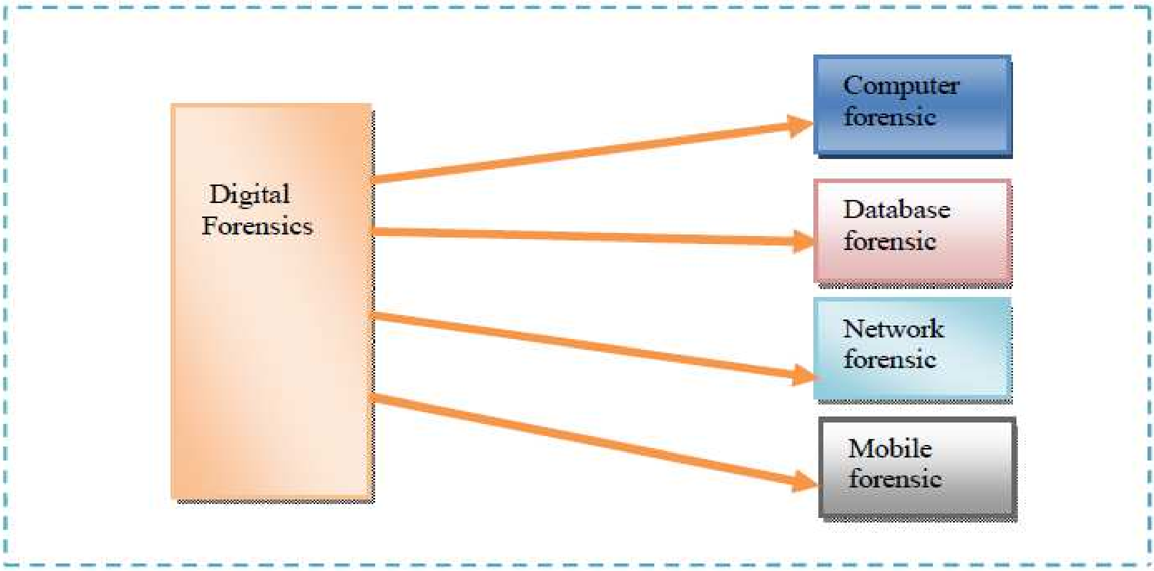


Figure 3.1 Classification of Digital Forensics, (Yadav, 2011).

i.) Computer forensics focuses on digital evidence from computers. It covers a range of information ranging from data stored on the computers such as system logs and browser history.

ii.) Database forensic is centered on the contents of the database contents and its associated data (metadata). It uses of database contents and log files to generate the needed information.

iii.) Network forensic deals with analysis and monitoring of computer network traffic with a view of obtaining information for legal evidence. Network forensics enables an investigator to gather information based on the observed network traffic patterns.

iv.) Mobile forensics deals with recovery of data from mobile devices. The investigation focuses on artifacts such as call details, SMS and Emails. Mobile forensic can also give information about the device location.

This research is centered on the fourth type of Digital Forensics which is the **Mobile Forensics**.

1.1Background

Digital devices such as PCs, laptops, PDAs and Smartphones store precise evidence/records of incriminating activity much more than is typically realized. Digital evidence can be extracted from these digital devices and be used in a court of law to secure a conviction. To extract this evidence requires the right examination methods and tools.

For conventional platforms such as PCs, the standard procedure for extracting digital evidence is making a bit by bit copy of a seized media (such as an hard drive), examining it by employing any of the various available tools that bypasses the OS altogether. This process works well since the file structure for hard drives is standardized to only a limited few types namely; EXT, FAT and NTFS. The Open filing system formats encourage wider adoption; consequently, fewer storage types emerge. Consequently, forensic investigators can easily recover deleted files in standard formats such as MS-WORD and ASCII which are hidden to the OS (Moore, 2006).

In contrast with PCs, information in hand-held devices (for instance in smartphones) is stored in the internal memory of the phone with no particular standardized format. The associated data such as SMS logs and call histories are usually stored in proprietary formats in areas (locations) that changes with the model of the phone, (Moore, 2006). Moreover, the data cable for accessing the memory of an handset varies with the make/model of the phone, thus direct data extraction from the memory of a phone is much costlier for mobile phones devices compared to PCs since no standard storages as well as document formats like for the PCs. As well, unlike in traditional computers, even after switch off, mobile phone devices remains active and their content is updated throughout. The clock of these devices is always changing hence constantly altering its memory content. This means that the forensic hash value obtained from these mobile devices yields a different figure value each moment the function runs on the device's memory, (Rick et al., 2007). This explains why it is hard to yield a bit by bit copy of the smartphone's memory entire data.

Another distinguishing feature of hand-held devices from other conventional platforms such as PCs is the issue of data storage medium. Hand held devices such as the smartphones and mobile phones store data in volatile memory as compared to computers that employ non-volatile storage media like hard-disks. When handheld devices are unplugged from power and their internal battery gets depleted, the user data is likely to be lost as opposed to non-volatile hard-disk where the user data is saved incase the power is unplugged, (Marwan, 2006). This means that evidence on a handheld device (such a phone) could be lost if power is not retained on it.

Due to above factors and many more others, handheld device needs appropriate forensic process model which may not be the same as the convectional devices like PCs hence the reason of this research study.

1.2 Sources / Causes of the problems in the area of Hand-held digital forensics

There are a number of challenges facing the use of Digital Forensics in Hand-held devices which are discussed below;

i.) Lack of Sound Process Models

A study by (Archit et al., 2012), views lack of a sound process model as a major challenge in smartphone investigation who highlights the need for a sound process model.

This challenge is also acknowledged by (Ramabhadran, 2011) study, who ascertains that the approach and methodology are extremely critical in the digital forensic investigation. Besides, a research carried out by (Noora et al., 2012), ascertained that a major challenge in digital forensics for smartphones was attributed to lack of the right tools and examination methods. Their study concluded that potential evidence held on Smartphone devices could be retrieved with the right examination methods and tools.

In their study, (Khawla et al., 2011), (Zareen et al., 2010) and (Raghav et al., 2009), several challenges are mentioned as well as the difficulties faced in this area (field):

ii.) There is increased change in the Smartphone device Technology – The rising huge numbers of various models of Smartphone in the market leads to increase in problems in development of scientifically sound methods for data capturing from these devices.

iii.) Wide range of OS for Smartphone devices – Various OS for smartphones exist namely open source and proprietary. Different OS store data differently. Forensic investigators therefore need to understand the location of the data storage and how such data can be retrieved in all these operating Systems.

iv.) Data Volatility – Once a device is seized, its signals should be blocked to avoid any alteration of the data held in the smartphone device.

This research seeks to solve problem **i.) Lack of Sound Process Models**

1.3 Definition of key terms – (As used in the Title)

Mobile Forensics is “a branch of digital forensics that deals with the recovery of digital evidence from a mobile device under forensically sound conditions.” (nvdigitalforensics.com, 2013).

A Process Model (Digital forensic process) is “a recognised scientific and forensic process used in digital forensics investigations. It can be viewed as a process consisting of a number of steps from the original incident alert through to reporting of findings. The process is predominantly used in computer and mobile forensic investigations and s made up of mainly three steps: acquisition, analysis and reporting”, (computerforensicsworld.com, 2013).

A Handheld Device is a pocket-sized computing gadget which has a display screen and input/output interface like an external or touch screen keyboard. Such devices and gadgets include mobile phones, PDAs and Tablets, (Author, 2013).

A Smartphone is a mobile phone with very advanced features. A typical smartphone has a WiFi connectivity, a high-resolution touch screen display, Web browsing capabilities and ability to support a wide range of applications. The majority of these smartphone devices run on any of these popular mobile operating systems: BlackBerry, Symbian, Android and iOS, (techopedia.com, 2013).

In summary the title ‘Enhanced Mobile Forensics Process Model for Handheld Devices’, is a research topic aimed at developing an improved digital investigation guideline process for the emerging pocket size computing devices such as the smartphones.

1.4 Problem Statement

Forecasts by (IDC, 2013), predict that rmore than 1 billion phones will be sold worldwide in 2014. Increasingly more smartphones are envisaged to be shipped globally compared to the ordinary phones in 2013, the first history of occurrence in the mobile phones market on yearly basis. This revolution in mobile phones is envisaged to give rise to more and new types of crimes such as kidnappings, stalking, impersonation, defamation, forgery among other crimes (Khawla et al., 2011) and (Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders, 2009).

Lack of sound process models is seen as a major challenge in the mobile investigation as most of the earlier studies have concentrated on computer based process models;

- A study by (Anup, 2011), ascertains that the methodology and approach are key in the forensic investigation of digital mobile related crimes and proposes a windows mobile process model. Anup feels that the rapid technological development coupled with the rising popularity of Windows mobile devices poses great challenges for investigators and law enforcement globally hence a need for a sound process model for handheld devices.
- (Xian et al., 2009), acknowledges the challenge associated with different versions of Symbian smartphones and proposes a model for forensic analysis of Symbian smartphones.
- (Archit et al., 2012), agrees that lack of sound Process Model is a major challenge in Smartphone investigation. He proposes a smartphone Process Model.

The great challenge in achieving a sound process model for handheld devices is attributed to a number of problems as seen in section 1.2 above. To solve this problem, the researcher critically reviews all the literature related to digital forensics process models, identifying the gaps and where possible combining phases of the various earlier proposed models so as to build a neutral yet an enriched model that will serve as a benchmark for a sound handheld forensic investigation. The proposed Hand-held Process Model is operating system independent and is tested using two types of smarphones that run different Operating Systems namely; iPhone (iOS) and Samsung Galaxy Tab (Android OS). Three mobile forensics tools mainly UFED Physical Analyser 3, Oxygen Forensic Suite 2013 and MOBILedit are employed to facilitate the tests.

1.4.1 Purpose of the Research

The main aim of this research is to come up with an improved Digital Forensics Process model for Hand-held devices which is operating system independent.

1.4.2 Specific Objectives

The specific objectives of this research are:

a) Review critically literature related to Digital Forensics Process Models for Hand-held devices

b) Design (Model) an improved Process Model for Hand-held devices

c) Implement the improved Process Model for Hand-held devices

d) Test the improved Hand-held Process model

1.4.4 Justification of the research

There are minimal research studies tailored towards Process Models for hand-held devices as most of the existing models have been tailored for computers. This is ascertained by (Anup, 2011), (Xian et al., 2009) and (Archit et al., 2012) who propose various hand-held forensics process models.

While there are some earlier proposed Hand-held forensics models by some researchers, such models are mostly operating system dependent hence there is a great need for process models which are operating system independent. This research therefore aids in boosting Forensics field investigation process by proposing an operating system independent hand-held process models hence making an important step towards achieving better electronic evidence in the fast growing mobile phone technologies which are prone to misuse.

By exploring the loopholes in digital forensics process model for Hand-held devices and suggesting possible (model) solution, the research aids in enabling success in mobile forensics investigations hence enabling the much needed confidence in adaptation of mobile phones evidence that can stand in a court of law.

Moreover, Hand-held devices are becoming a repository of potential evidence hence research in this area is of critical importance. Increasingly evidence from hand-held devices is being used to determine cases in courts; a good example is the case of Dr. Conrad Murray trial in ruling of Michael Jackson’s death, (Helen et al., 2012).

CHAPTER TWO: LITERATURE REVIEW

This chapter focuses on the literature review relating to the research of Hand-held device Forensic Process Models. The state of the art of literature related to Digital Forensics is discussed by themes. The state of practice and technological advancement is also discussed and lastly a critique of the related earlier works is highlighted. The literature serves as a foundation for the proposed Hand-held device process Model and more so as rich information on Digital Forensics specifically on Process Models.

2.1 State of the art

There have been a lot of studies related to Digital Forensics. Some of the initial works in this field are centered on the acquisition techniques and the general forensics analysis of both computers and mobile device. Extensive research has also been undertaken in computer process models but only limited studies have been carried out for process models in emerging handheld devices such as smartphones.

2.1.1 Digital Forensics

Digital forensics is the application of science in identifying, collecting, examining, and analysing of data while preserving the integrity of the information and maintaining a strict chain of custody for the data, (Kent et al., 2006). The goal of digital forensics investigation is to present some form of evidence in a court of law using the correct legal procedures that have scientific backing, (Kohn et al., 2008).

Forensic investigators conduct digital forensics mainly to find digital evidence of a crime. A range of various kinds of crime may be discovered in a computing environments as highlighted by (Khawla et al., 2011) and (Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders, 2009), in Table 2.1;

Table 2.1: Types of Crimes in computing

Type of Crime	Description	Potential evidence Source
Murder	Intentional killing of someone	-Internet logs. -Images. -Address books. -Medical records. -Financial/asset records.
Child abuse	Ill-treatment and usage of the children that may impact their psychology and development	-Chat logs -Internet logs -Movies files. -Internet searches. -Images.
Harassment	Behaviour leading to bothering of a person	-calendars/notes. -Internet logs. -Address books. -Images. -Internet searches about victims.
Identity theft	Stealing of someone else personal information such as credit card numbers	-Credit card information. -Electronic money transfer. -Forged document. -Financial records.
Counterfeiting	Illegal actions aimed at producing imitations that look like an original	-Financial records. -Reproductions of signature. -Credit card information
Terrorism	Dangerous actions against civilians in order to achieve political or even Organizational goals.	-Credit card information -Electronic money transfers. -Financial records. -Fictitious identification

Table 2.1: Crimes in the computing environment**:** (Khawla et al., 2011) and (Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders, 2009).

2.1.2 Mobile Forensics versus Computer Forensics

Mobile phone forensics can be defined as the art of retrieving digital evidence from a mobile phone using acceptable methods under forensically sound conditions, (Panagiotis et al., 2012).

Computer forensics is concerned with the digital evidence from a computer. It focuses mainly on the current states of a digital artifact, such as storage medium or electronic document of the computer, covering broad range of digital information from system logs such as browser history with the help of actual files stored on the drive, (Yadav, 2011).

There is a rising shift for using mobile phone data as evidence in civil or criminal cases, (Ahmed et al., 2009). A wide range of data can be acquired from an hand-held device using commercial forensic tools. Such data include: call logs, Email, phone books, SMS, chat logs, MMS, Internet web logs, Videos, images and Audio content, (Hoog, 2011).

The functionality of smartphone devices is similar to that of computers but there exists a number of differences between the computer digital forensics and that of smartphone devices as found out by (Khawla et al., 2011). These differences are illustrated in table 2.2;

Table 2.2: Computer forensics versus Smartphone (mobile) forensics

Aspect	Computer Forensics	Smartphone Forensics
Evidence Source	RAM, Hard disk and external memory cards.	SIM, Internal memory and external memory cards.
Whether possible to remove the internal media storage	Yes it is quite possible to remove the hard disk media	Its not possible to remove the internal media storage of a smartphone
Operating system	Limited number of Operating systems.	Consists of a number of Operating systems.
Whether possible to bypass the authentication password	Its possible	Impossible to bypass the password during logical acquisition.
Power and data cables	Standard data cables and power	Variety of data cables and power.
File system	Standard file system (e.g FAT).	Variety of file systems

Table 2.2: Computer forensics versus Smartphone (mobile) forensics, (Khawla et al., 2011)

2.1.3 Mobile Operating Systems

Various Mobile operating systems exist in the market which can be categorized into proprietary and open source operating systems. The section below examines the top most popular mobile device operating systems in the market as outlined by (Yates, 2011);

i). Android OS

Android is an OS build by the Open Handset Alliance. Its layout is made up of four main levels: Linux Kernel, Libraries and Android Runtime, Application framework and Applications, (Lessard et al., 2010).

The Linux Kernel facilitates access to core-services including; driver model, network stack, security and memory management. Besides, the Linux Kernel also facilitates support for threading to the Dalvik virtual machine.

Libraries are the immediate layer up and are split into two, namely; the application libraries and the Android Runtime library. The Android Runtime Libraries is made up of the **Dalvik Virtual Machine (VM) and the core libraries** providing the functionality available for the applications. The Android OS has other components which utilise C/C++ libraries and these include:

- **LibWebCore –** This is a modern web-browser engine which is tasked with powering the Android browser as well as the embeddable web view
- **SQLite –** This is relational database engine which is available to all applications. Usually this database is lightweight and powerful.
- **Media Libraries** - These supports recording of many video and audio formats and also static image files, such as MP3, MPEG4, JPG, and PNG

The core-set of services supporting the open development are as outlined below;

- A rich set of Views to generate applications, consisting of textboxes, grids, lists and buttons.
- A Notification Manager enabling applications to display customized alerts in their status bar
- Content Providers enabling applications to access data from other applications
- An Activity Manager to manage the lifecycle of applications

- A Resource Manager enabling access to non-code resources such as graphics and localized strings

The top most layer is the Applications and it consists of JAVA applications such as SMS program, email client, maps, calendar, contacts and browser. This is illustrated in figure 2.1;

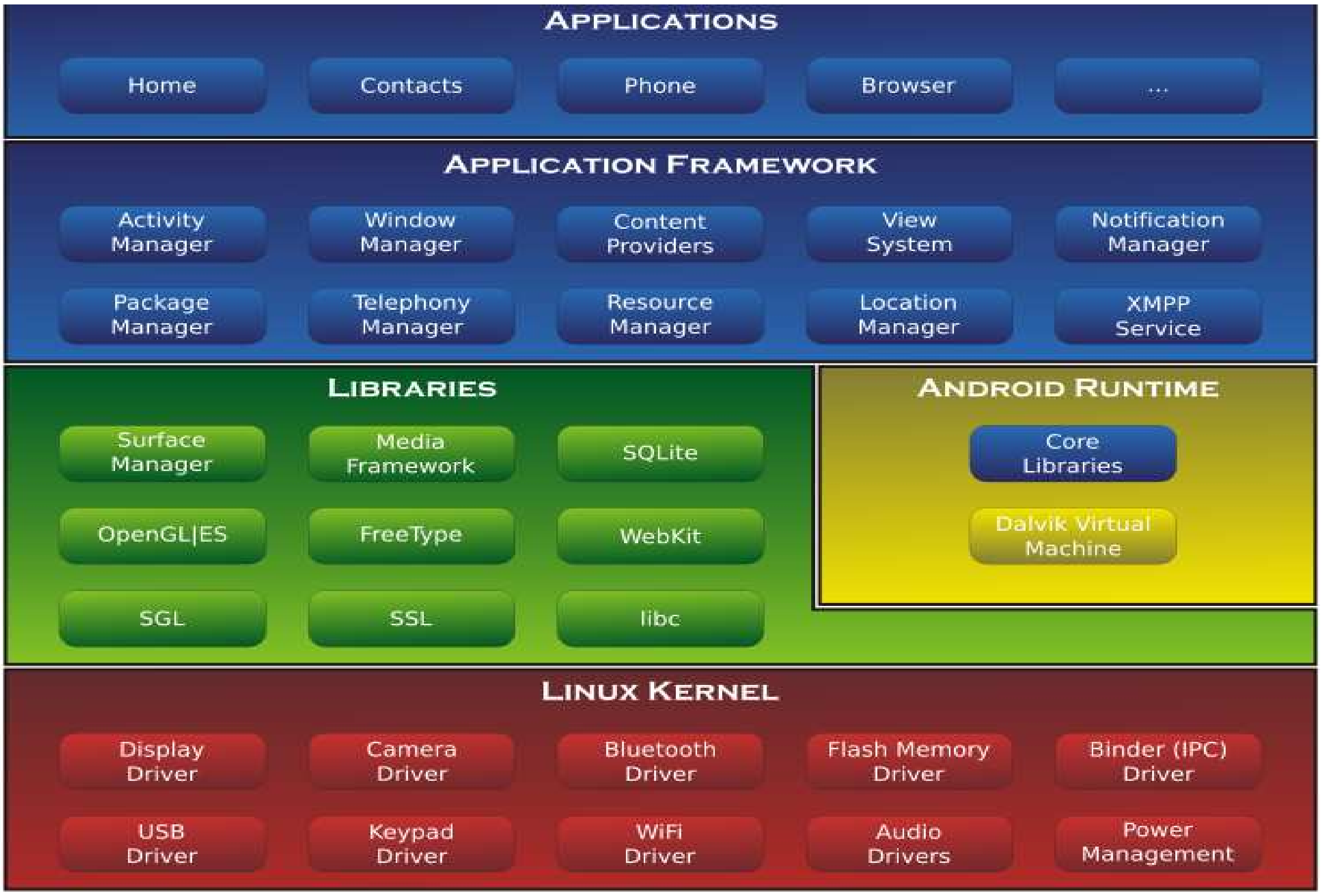


Figure 4.1: The Android OS architecture, (Yates, 2011)

A research carried out by (Panagiotis, 2012), ascertains that the most popular file systems which investigators can come across during the Android OS analyzing are; FAT, YAFFS2, EXT3 or 4 or other proprietary systems like Samsung's Robust FAT file system (RFS).

ii). Blackberry OS

The Blackberry phone was originally created by RIM (a Canadian company) for business use aimed at keeping professionals in network while in transit. The OS powering Blackberry phones is proprietary with scanty information about it known publicly. Similarly to Android, the

Blackberry also runs through the virtual machine specifically the JAVA", (Yates, 2011) and (Schiffman, 2010). Figure 2.2 shows the Blackberry OS Architecture;

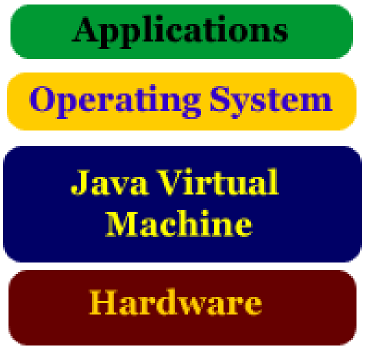


Figure 2.2: The Blackberry OS architecture, (Yates, 2011) and (Schiffman, 2010)

The Blackberry OS architecture consists of 2 runtime environments namely: the Mobile Data Service (MDS) and Proprietary. The MDS deals mainly with services for web and enterprise while the proprietary environment houses the main RIM APIs such as the calendars, memo and Bluetooth, (Yates, 2011).

iii). iPhone iOS

The iPhone OS is regarded to be a UNIX based OS as it shares the Darwin Foundation from OS X. The iPhone Operating System is made up of four layers which are: Cocoa Touch, media, the core services and the core OS. The top most layer is the Cocoa Touch and this offers the necessary infrastructure used by the iPhone OS. The Media is the immediate layer containing the various technologies to support 2D and 3D drawings as well as video and audio. At the bottom most are two layers namely, the Core Services and the Core OS and these host the various iPhone OS interfaces, including those for accessing files and low-level data types as illustrated in figure 2.3, (Yates, 2011);

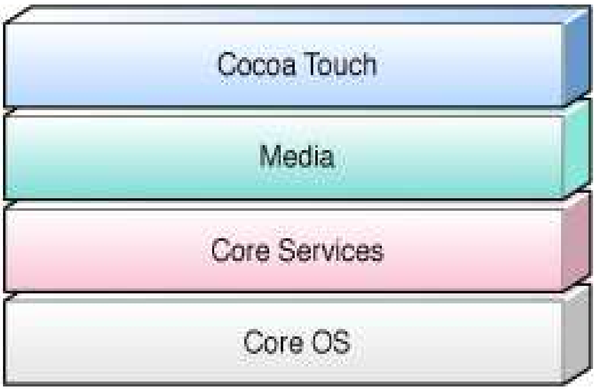


Figure 2.3: The iPhone architecture, (Yates, 2011)

iv). Windows Mobile OS

Windows Mobile OS is for the Windows mobile devices, (Casey et al., 2010). The Windows Mobile OS is structured similarly with Windows OS in regards to for instance user info and activities such as registry entries info, files, and web activities. Moreover, there are notable differences between the Windows Mobile and the Windows OS. Windows OS consists of two main types of filing systems namely, FAT and NTFS. On the other hand, the Windows Mobile OS utilizes a variance of the FAT filing system known as Transaction-Safe FAT, which offers some recovery capability in a case of an unexpected system shutdown.

The Windows Mobile OS consists of four kinds of processors namely, ARM, MIPS, x86 and SH4. Also, there are two various types of flash memory namely; NOR and NAND. NAND can be regarded as a solid state equivalent of a hard disk.

NOR consists of a RAM like interface with an address bus, a data bus and control lines. NOR memory flash is directly mapped into the memory of the processor map hence the processor code can be directly executed unlike with NAND flash which is never mapped into the processor's memory space requiring its code to be first loaded into RAM prior to execution, almost like a hard disk, (Klaver, 2010).

v). Symbian OS

(Yates, 2011), discusses the Symbian system architecture which is seen to have three layers, with each layer containing packages. These packages in turn consist of collections of components as illustrated in figure 2.4;

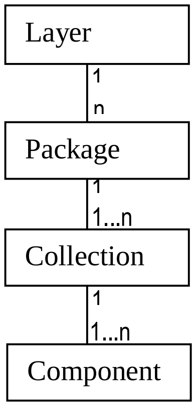


Figure 2.4: Decomposition Hierarchy for the Symbian OS, (Yates, 2011)

2.1.4 Mobile Device Forensics

A study by (Punja et al., 2008) provided some of the foundational concepts of forensics analysis of the new generations of handheld devices like BlackBerry, Android and iPhones. The study covered the technologies practised, the handling procedures, and the common evidence storage location for the various devices. They found out that data could be extracted from the various internal memories of these devices and such data would include, SMS, call logs, photos, MMS, emails, videos, and calendar notes.

Much of other recent research studies by (Archit et al., 2012), (Xian et al., 2009) and (Anup, 2011), have centered on specific makes of handheld devices, investigating the methods that could be employed for acquisition and analyses of a device's internal memory as well as the information that could be extracted from the various devices. In iPhone, the data could be acquired by use of a physical or a logical method. "The physical method requires jailbreaking the system, that causes a slight alteration into the system's data," (Kubasiak et al., 2009).

One of the techniques regarded to be latest by Zdziarski acquires a physical logical image of an iPhone without jailbreaking the phone. This is regarded as the best forensics method for acquiring iPhone and has been evaluated by the National Institute of Standard and Technology, (Zdziarski, 2010). Like iPhones, Android-based handheld devices can be acquired by employing either physical or logical methods. According to (Lessard et al., 2010), the physical method entails obtaining of a dd image of the phone's memory. This consequently requires the device's root access.

2.1.5 Process Models

A Process Model (Digital forensic process) Can be defined as “the process of analytical and investigative techniques used for the preservation, identification, extraction, documentation, analysis and interpretation of computer media (digital data) which is stored or encoded for evidentiary and or/or root cause analysis”, (Solms et al., 2006). Several forensic processes have been proposed in the field of Digital Forensics. Most of these proposed forensic models are centered on “the investigative process and the various different steps, addressing the complexity of an investigation, the features and functionality of devices, and the concrete principles of an investigation”, (April et al., 2010). As well, most of these process models have been mainly dominated by general digital forensic process models and lately a few mobile forensic process models. The growth of handheld device technology including mobile phone and smartphones is triggering the need for specific process models which best address the forensic analysis in the new generation mobile technology.

2.1.6 Computer Digital Forensic Process Models

There exist extensive research studies on Computer Digital Forensics Models. Some of these include “The U.S. Department of Justice process model” , (NIJ, 2001), "The Integrated Digital Investigation Model (IDIP)" , (Carrier et al., 2003), the “Enhancement IDIP model” , (Baryamereeba et al., 2004), the “Computer Forensics Field Triage Process Model (CFFTPM) , (Rogers et al., 2006), the “ Generic Computer Forensic Investigation Model (GCFIM) by (Yunus et al., 2011) and the “Systematic Digital Forensic Investigation Model (SRDFIM) proposed by (Ankit et al., 2011).

The computer forensic models have evolved over time to cope with the changing technological trends and advancement in crime. The following Computer process models have been discussed;

i). The U.S. Department of Justice process model, (NIJ, 2001)

ii). The Integrated Digital Investigation Model, (Carrier et al., 2003) and the

iii). Generic Computer Forensic Investigation Model (GCFIM), (Yunus et al., 2011)

i). The U.S. Department of Justice process model, (NIJ, 2001)

The NIJ model is one of the earliest computer process models and it is made up of four phases, namely; *Collection phase* entailing the search for evidence, evidence recognition, evidence collection and evidence documentation; The *Examination phase* serves to facilitate the visibility of evidence, while explaining its origin and significance. The phase also involves discovering hidden and obscured information as well as the relevant documentation; The *Analysis phase*, focuses on the product of the examination for its significance and probative value to the case; while the *Reporting phase, (*which is the final phase) entails reporting of the results of the analysis, (NIJ, 2001).

ii). The Integrated Digital Investigation Model (Carrier et al., 2003)

Another computer forensic process model is by (Carrier et al., 2003) by the name "Integrated Digital Investigation Model (IDIP)". Their work involved combining the various available investigative processes into one integrated model. The resultant model organized the process into five groups as shown in figure 2.5 below;

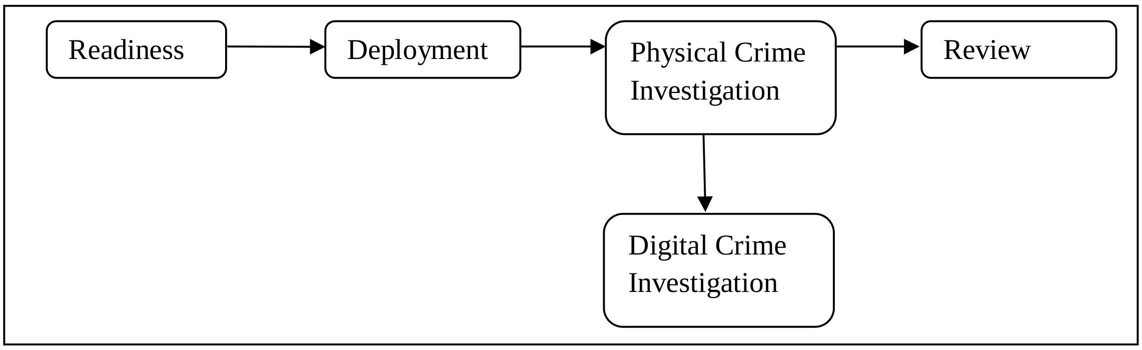


Figure 2.5: The Integrated Digital Investigation Model, (Carrier et al., 2003)

- **The Readiness phase** ensures that the operations and infrastructure can fully support an investigation and it includes two phases, namely Operations Readiness phase and Infrastructure readiness phase.
- **The Deployment phase** facilitates a means for an incident to be logged and confirmed. It is made up of two phases, namely Detection and Notification phase, where once the incident is detected then the appropriate people are notified; The Confirmation and Authorization phase; confirms the incident and enables the investigator to seek authorization for legal approval to carry out a search warrant.
- **The Physical Crime Scene Investigation phase** aims at data collecting and analyses of the physical evidence and reconstruction of the various actions that took place during the

crime. It is made up of six stages namely; Preservation, Survey, Documentation, Search and collection phase, Reconstruction phase, and the Presentation phase.

- **The Digital Crime Scene Investigation phase** main aim is to collect and analyze the digital evidence obtained from the physical investigation phase and through any other relevant future means. Its phases are similar to those of the Physical Investigation phases, but the primary focus is on the digital evidence.

iii). Generic Computer Forensic Investigation Model , (Yunus et al., 2011)

Among the most recent Computer Forensic Models is the (Yunus et al., 2011), "Generic Computer Forensic Investigation Model (GCFIM)" which was achieved by analysing the previously proposed digital forensic models and identifying the common and shared processes among all the previous process models. The sole purpose of this model was to serve as a good starting point for the building/development of new computer forensics investigation models. The model is shown in figure 2.6 below;

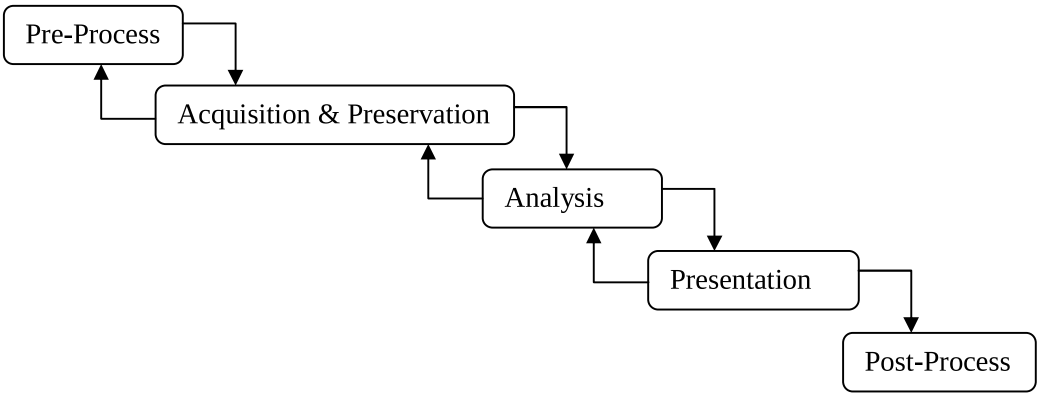


Figure 2.6: Generic Computer Forensic Investigation Model (GCFIM) by (Yunus et al., 2011)

2.1.7 Handheld (Mobile) Digital Forensic Process Models

There are few research studies on mobile device digital forensic process models with those few being mainly operating system dependent. Examples of such mobile forensics device models are the “Process model for forensic analysis of Symbian Smartphones” by (Xian et al., 2009), the “Forensic investigation process model for Windows mobile devices” by (Anup, 2011), and the (Archit et al., 2012) “Smartphone Forensic Investigation Process Model (SPFIPM): The three mobile forensics process models are discussed next;

i). Symbian Smartphone Process model, (Xian et al., 2009)

The forensic analysis of Symbian Smartphones by (Xian et al., 2009) is an adaptive process model based on the different versions of Symbian Smartphones. The model contains the different stages of forensics. The author argues out that Symbian Smartphones forensics is relatively a new field of interest among scientific and law enforcement and as such the various mobile phones process models may not be able to solve the problems of the Symbian Smartphones adoption. In their paper, they describe an investigation process model for forensic analysis of Symbian Smartphones and assert that their new model could overcome some problems of the traditional model of digital investigation on Symbian Smartphones. Figure 2.7 shows the Symbian Smartphone Forensic Process Model;

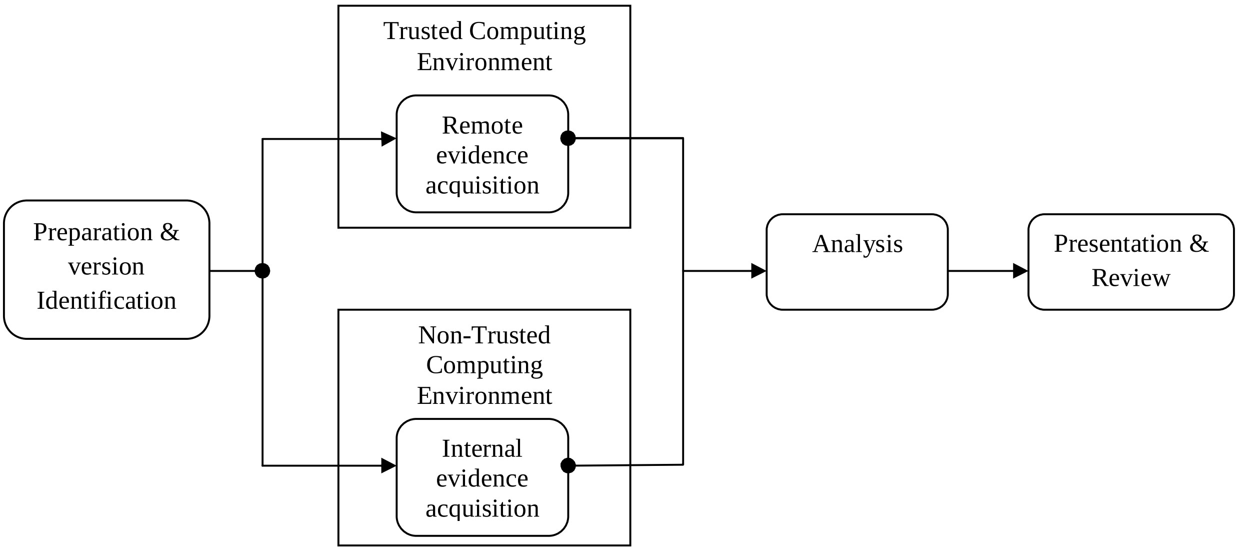

Trusted Computing Environment
Remote evidence acquisition
Preparation & version Identification
Analysis
Presentation & Review
Non-Trusted Computing Environment
Internal evidence acquisition

Figure 2.7: The Symbian Smartphone Forensic Process Model, (Xian et al., 2009)

ii). Windows mobile devices Forensic investigation process model

(Anup, 2011), came up with a Windows mobile forensic investigation process model consisting of a twelve-stage process. The investigation process model focuses on specific information flow associated with the forensic investigation of windows mobile devices as shown in figure 2.8. The model also emphasizes on a systematic and methodical approach for digital forensic investigation.

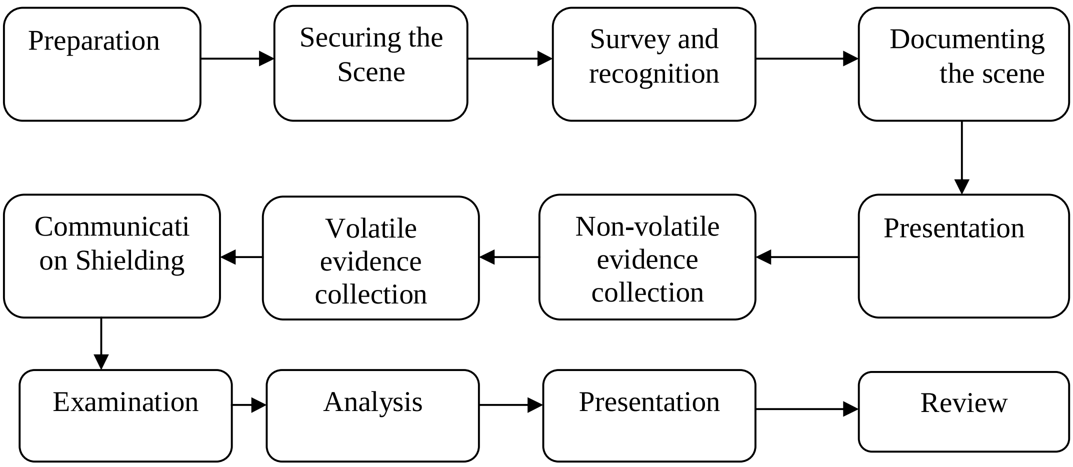


Figure 2.8: Phases of the Windows Mobile Device Forensic Model, (Anup, 2011)

iii). The Smartphone forensic investigation process model (SPFIPM)

(Archit et al., 2012), proposed a smartphone forensic investigation model by exploring the various processes found in the forensic investigation of a Smartphone in the form of a fourteen-stage model. The model was built (developed) with a sole aim of guiding an effective way to investigate a smartphone with more area of finding the potential evidence. The proposed model is illustrated in the figure 2.9;

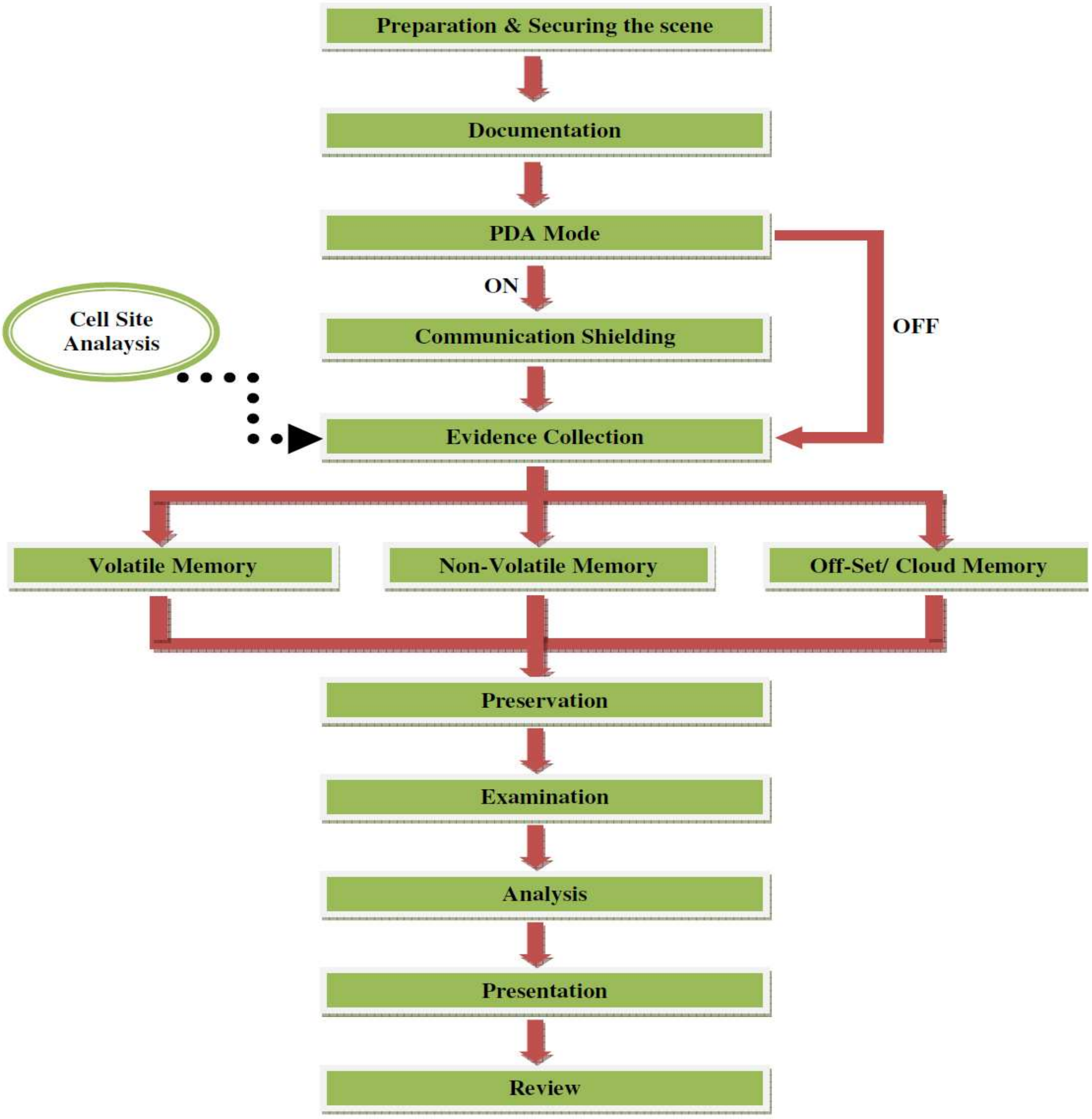


Figure 2.9: Smartphone Forensic Investigation Process Model, (Archit et al, 2012)

2.2 State of Practice – Case studies

There have been many cases which have involved Forensic Analysis of handheld devices for electronic evidence.

i.) One example showing the use of handheld devices for evidence is the case of Dr. Conrad Murray trial, in which his iPhone contained enough evidence regarding the Michael Jackson's death for prosecutors to make the case, (Helen et al., 2012).

ii.) In yet another case, Ronald Williams killed his wife Mariama, apparently in a fit of rage after learning that she had an affair. Unbeknownst to Williams, his cell phone pocket dialed his wife's cell phone during the crime and the call went to voicemail. The recording on his wife's voicemail captured him stating that he was going to kill her, followed by her screams and their 2-year-old daughter pleading with Williams to stop, (Krueger, 2011).

2.3 Technological Advances in the area Mobile Forensics

Digital forensics has been in existence from as early 1984 with the United States FBI laboratory and other law enforcement agencies. This field has continued to grow and to change with the changing trends in technology. The field started with computer forensics of the convectional personal computers (PCs) and it has advanced with time to incorporate new technologies (handheld devices) like mobile phones, smartphones, cloud forensics among others.

The change in technologies like social networking applications and other newer technologies have as well led to the change in approach in process models to cater for the new types of approach in forensic analysis of such technologies. Many Computer Forensic tools have been developed to perform a range of functions. Tools have moved from being just function specific to being able to serve a number of functions. Such software tools include Forensics Tool Kit (FTK) and Oxygen Forensic Suite. Digital Process Models especially computer –based models, have been developed to provide a sound Forensics investigation process. Hand-held Forensic process Models are also now beginning to emerge and the focus is now on developing models that are Operating System independent.

2.4 Critique of the Related Work

The critique of the related work is summarized under two sub-sections namely; Computer Digital Forensics Models and Hand-held Forensics models;

2.4.1 The Computer digital forensic models

As seen in earlier sections, most of the existing process models are ideally convectional computer digital forensic process models and lately a few mobile forensic process models. Due to the nature of mobile device technology as discussed in section 1.2, the convectional digital forensic process models of PCs cannot exactly apply in mobile handheld devices situation. The advanced capabilities of handheld devices and the rapid growth in mobile technology like PDAs and Smartphone's cushioned by the growing handheld mobile device related crimes has triggered the need for Hand-held process models which best address the mobile forensic analysis in the new generation mobile technology.

2.4.2 The handheld device digital forensic models

Only very few hand-held forensic process models exist with majority of them being Operating System dependent. A major issue in Smartphone handheld devices forensics is non-existence of any widely accepted standard investigation process model, (Archit et al., 2012). However, there are a number of research works in an effort to address the issue. As seen in section 2.1.7, such works include the "Windows Mobile Device Forensic Model" by (Anup, 2011), "Symbian Smartphone Forensic Process Model" by (Xian et al., 2009) and the "Smartphone Forensic Investigation Process Model (SFIPM)" by (Archit et al., 2012). The Windows Mobile Device Forensic Model and the Symbian Smartphone Forensic Process Model have some common similarities between them though they differ in certain areas. Both of these models are operating system dependent. The Symbian model was build for Symbian phones while the Windows model is build for Windows phones.

The (Archit et al., 2012) generic Smartphone Forensics model takes into account volatile and non-volatile data which are a key to Smartphone forensics. All the phases are however sequential with no iterations yet it is less likely to yield more concrete evidence without a revisit to some phases.

Moreover, the earlier existing models do not emphasize on Live Forensics yet the trend to digital forensics has now shifted from the traditional Forensics (Dead Forensics) to incorporate Live Forensics. There is hence a need for a sound hand-held Forensic Process Model that not only puts into account of Live Forensics but which is operating system independent.

CHAPTER THREE: METHODOLOGY

The success of any research study depends on the methodologies employed to carry out the given study. There are different types of methodologies which exist but the selection of the appropriate methodology depends on the type of research under study.

3.1 Existing methodologies

Research methods are the various procedures and algorithms employed in a research. Such methodologies include experimental methods, Simulation methods and theoretical methods.

The choice of the best methodology is paramount for any given research study. Each of the methodologies has unique benefits and drawbacks as outlines in Table 3.1 below;

Methodology	Description	Applicability
Theoretical methodology	This methodology can be described as the practice of developing a basic theory that is then proved through research, observations, and facts. It is the framework that is used to achieve an effective hypothesis. The theories resulting from a theoretical study do not have to be brand new but they are used to support a body of research, such as experiments, reports, or conclusions. Some of the ideas are the existence of conceptual and formal models (data models and algorithms).	Used in finding new mathematical models or theories, but it still needs other methods to prove the efficiency of the new models or theories.
Experimental methodology	In this method, a systematic manipulation of one or more variables is conducted so as to observe/study the effect on other variables. *Advantage*: Control of variables helps one draw effect conclusions. *Disadvantage*: Laboratory based method is not natural hence results may not be generalizable; It may also be difficult to control all variables. **<u>Types</u>:** **Simulation Experiment:** It is a form of experimental method	Applicable in situation where the live system or network is not available or cannot be used. Simulation tools such as NS-2, NS 3, OPNET, OMNeT++, Matlab etc are used. The experiments done in simulatio method are usually either very expensive to do in a Laboratory or field setting or they require a long

	which provides a repeatable and controlled environment for network experimentation. In this method, the researcher determines the nature and timing of the experimental events. It is easy to configure and easy to use hence allowing for exploration of large parameter spaces	duration of time to accomplish hence making it impractical and uneconomical for a research purpose.
	Laboratory Experiment: In this methodology, the independent variables are manipulated, controlling the intervening variables, and measuring the effect of the independent variables on the dependent variables.	Applicable in a situation where the experiment cannot be simulated as well as cannot be done in a field setting.
	Field Experiment: This occurs in a "natural setting." Where a researcher manipulates the independent variables while trying to control the most important intervening variables. The researcher then measures the effects of the independent variables on the dependent variables by systematic observation of human subjects.	Are applicable to experiments that are not ideal for a lab or simulation setting. Some type of experiments also require this type of experiment so as to acquire results that are as much close to reality as possible.
Field Study Methodology	Behavior that is observed in the environment in which it naturally occurs. The quality of the field study depends on the quality of the data gathered. Advantage: Provision of firsthand behavioural information. Disadvantage: The presence of the observer could change the behavior of the participant. It is unclear the extent to which generalizations could be made to other participants and settings The recording behavior of the observer may be biased;	Applicable to experiments which require field data collection through informal interviews, direct observation, participation in the life of the groups, collective discussions, analyses of personal documents produced within the group, self-analysis, results from activities undertaken off- or on-line, and life-histories.
Case Study Methodology	This type of study relies on observations made during or following a real-world project. Advantage: Results into a great amount of detailed descriptive information. Very useful for hypotheses forming.	Appropriate for discovering potential behaviors of systems or people as well as in identifying the candidate independent and

	Disadvantage: The case(s) studied may not be representative of the whole population. May be costly and time consuming. There is also a potential likelihood of observer bias	dependent variables.

Table 3.1: Comparison of different Research Methodologies

3.2 Evaluation of the methodologies;

From the comparison of the different research methodologies in table 3.1 above, based on the nature of this research study, both the **Theoretical method** and **the Laboratory Experimental approaches are employed.**

This research study has a basic theory that could be proved through research, observations, and facts hence making Theoretical method an ideal candidate method of choice. Besides, there is a need to prove the efficiency of the new models hence the choice of the Laboratory Experiment which is employed here to manipulate the various independent variables (hand-held devices running different operation systems) under a controlled environment.

3.3 Proposed Methodology

This research study employed both **theoretical review and laboratory experimental methods.**

The theoretical method aided in understanding the existing digital forensic models and the technological trends of the handheld devices which served as a basis for proposing the improved hand-held forensics process model. The experimental method was employed in the testing of the proposed hand-held forensics process model. The laboratory experimental methodology has similarity to simulation method; in both methodologies, the researcher designs a closed setting to mirror the “real world” measuring the response of human subjects as they interact within the system. The difference between the two is that the Laboratory experiment tries to achieve the real non-repeatable scenario which is hard to repeat while a Simulation method involves the use of simulation software programmed in a manner that can be repetitive in nature.

3.3.1 The experimental study

The experimental study here entails testing of the handheld devices to ascertain their applicability in the proposed hand-held forensics process model. Three kinds of Smartphones are employed namely; Blackberry, iPhone and Android. The experiment is conducted using forensically sound approaches under the proposed forensic model as per the mobile forensic testing guidelines.

a) The experimental Tools

Forensic software tools for mobile devices/ handheld devices are fewer compared to those for PCs, and of those available, their application is generally limited to the popular OS as ascertained by (Hemendra et al., 2012) study. Also the data present on handheld devices are mostly stored in a proprietary format, hence forensic tools specific to those type of handheld devices should be used because hardly there exists tools which can cut across all the different types of proprietary and open source operating systems, (Eoghan et al., 2011). Each tool has strengths and weaknesses towards each type of operating system.

The table 3.2 summarizes the different available Smartphone Forensic tools;

Tool	Phone OS support	License	Function	Feature support	Comment
Encase Smartphone Examiner (guidancesoftware.com,2013)	Apple's iOS, Android OS, Rim's Blackberry, Nokia Symbian, Microsoft's Windows Mobile OS	Commercial	Acquisition, Examination, Reporting	Process and analyzes all common features in mobile phones	Enables investigators to process and analyze smartphone device data alongside other types of digital evidence within any Guidance Software EnCase product
FTK MPE (Mobile Phone Examiner) (accessdata.com,	Chinese MediaTek (MTK), Android,	Commercial	Acquisition, Examination, Reporting	Process and analyzes all common features in mobile phones	Integrates seamlessly with FTK computer forensics software, making it easy to

2013)	Windows, Blackberry, LG, Nokia Series 30/40, Samsung, iPhone, Motorola, ZTE, Sony Ericsson etc				correlate evidence from multiple mobile devices with evidence from multiple computers within a single interface
Cellebrite UFED physical analyzer (cellebrite.com, 2013)	Palm OS, Microsoft windows, Blackberry, Symbian, iPhone, and Google Android	Commercial	Acquisition, Examination, Reporting	Standard mobile forensic plus forensic on Social Networks and messengers (FB messenger, skype, yahoo etc) in addition to other common features in all mobile phones.	Full featured 30 day free trial version available
Paraben's Device Seizure (paraben.com, 2013)	PDA's, Symbian, iPhone, Android, Blackberry, GPS devices and over 4,000 mobile phones	Commercial	Acquisition, Examination, Reporting	Supports recovery of internal and external SIM. Supports only cable interface	Free trial available
Oxygen Forensic Suite 2013 Analyst **(**oxygen-forensic.com, 2013)	Android and iPhone	Commercial	Acquisition, Examination, Reporting	Standard mobile forensic plus forensic on Social Networks and messengers (FB messenger, skype, yahoo etc) in addition to other common features in all mobile phones.	Full featured trial version for 30 days or 23 executions available
MOBILedit (mobiledit.com,	Microsoft windows, Blackberry, Symbian,	Commercial	Acquisition, Examination, Reporting	Internal and external SIM support. Supports cable and	Has a free trial version

2013)	iPhone, and Android			IR interfaces	
BitPIM (bitpim.org,2013)	CDMA phones only : LG, Samsung, Sanyo etc	open source	Acquisition, Examination, Reporting	Phone Book, SMS ,Calendar, Ringtones, wallpapers, Filesystem, Media, Memo, Call history, T9 editor	Support CDMA phones only
TULP2G (tulp2g.sourceforge.net,2013)	Cell Phones	open source	Acquisition, Reporting	Recovers basic data	Was designed as a basic tool to proof an idea.

Table 3.2: Summary of the mobile forensic tools

The Laboratory experiment for this study employs **Cellebrite UFED Physical Analyzer 3** (cellebrite.com, 2013), **MOBILedit forensics** (mobiledit.com, 2013) and **Oxygen Forensic Suite 2013 Analyst** (oxygen-forensic.com, 2013) mobile forensic software tools.

These tools contain free trial versions which are sufficient to achieve the main objectives of the study. **The Cellebrite UFED Physical Analyzer 3** has enhanced capability of decoding handheld applications such as Twitter, Google+, Facebook Contacts, Facebook Messenger, PingChat, Skype, Viber and WhatsApp (cellebrite.com, 2013).

The **MOBILedit forensics** supports a number of mobile phones including; Microsoft windows, Blackberry, Symbian, iPhone, and Android and contains a free trial version sufficient to achieve the experimental tests.

b) The experimental Test Data

The experimental data was created by performing standard operations on the handheld devices such as internet browsing, photo capture, and performing common activities on the Social Networking applications on each of the handheld devices, such as facebook chatting, status updates and messaging.

3.4 Characteristics of the proposed model

The few existing mobile device digital forensic models have been developed in a way that they work well with one particular type of investigation. The proposed model should be able to work well with any type of investigation.

- The proposed forensic model will be applicable to all handheld mobile devices regardless of the type of Operating System. The previous handheld digital forensic models mainly concentrated on the specific Operating System (OS) of the devices.

- The proposed model introduces some form of formal modeling through the use of UML. The significance of this modeling is to provide better understanding of the forensic investigation processes to both members and non-members of the digital forensics community.
- The new model integrates physical crime scene data investigation. The main purpose of the physical crime scene investigation phases is to perform data collection and analyses of the physical evidence that would help in reconstructing the chain of events that took place during the crime / incident.
- Iterations are incorporated in all the major phases inorder to help yield more solid evidence. The previous models lack this yet it is less likely for investigations to take a sequential nature given that more information may crop in prompting the investigator to revisit previous phases.
- Besides, a great emphasis of both Live and Dead forensics is put into account, meaning that the mobile device investigation would follow a slightly different process subject to the state of the phone at the time of seizure. The idea of Live and Dead forensics is borrowed from (Archit et al., 2012) model, “Smartphone Forensic Investigation Process Model (SPFIPM)”.

3.5 Summary of the Research Methodology Used

Table 3.3 summarizes the methodology used in achieving the objectives of this research as outlined in Chapter One.

Task		**Methodology / Tool**
Methods of study		Theoretical (Literature Review) and Empirical methods (Experimental)
Data Collection		Literature review and experimental results
Experimental study	Forensic Tools	Cellebrite UFED Physical Analyzer 3 Oxygen Forensic Suite 2013 MOBILedit forensics Lite
	Other Tools	Workstation running windows Operating System
	Smartphones	Samsung Galaxy S III (Android OS) and iPhone 4 (iPhone iOS)
Test Data		- Making phone calls, sending SMSes, adding phone book contacts etc

Table 3.3: Summary of the methodology

CHAPTER FOUR: CONCEPTUAL MODEL

4.1 Introduction

A conceptual model can be described as a high-level representation of how a system is organized and operates. It comprises of the system inputs, processes alongside their inter-relationships and the outputs.

The basic phases of the forensic process as recommended by (NIST, 2006) consists of: collection, examination, analysis, and reporting. Figure 4.1 illustrates this;

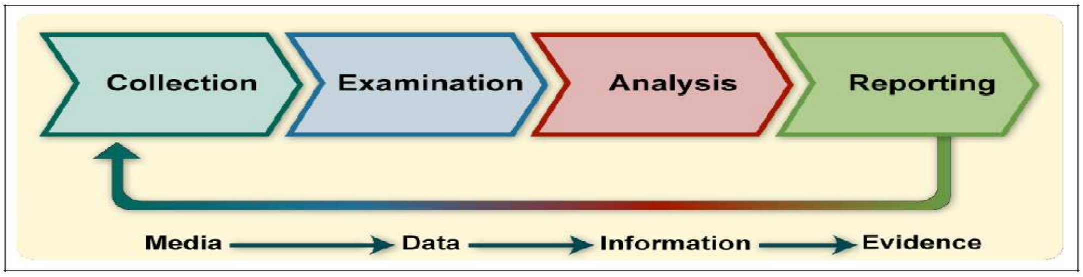


Figure 4.1: Basic phases of the forensic process, (NIST, 2006).

4.2 The Proposed High-level Conceptual Model

The conceptual model of the proposed Hand-held forensics process model follows the NIST's guideline, (NIST, 2006) and it comprises of three major high level phases mainly:

- Preparation phase
- Data Collection & Analysis Phase
- Post-Analysis and Reporting

It should however be noted that the NIST guideline, (NIST, 2006) is a generic guide for digital forensics investigations hence there is a need to incorporate more ideas from other researchers whose work is geared towards mobile forensics investigations.
The high-level conceptual model is illustrated in Figure 4.2;

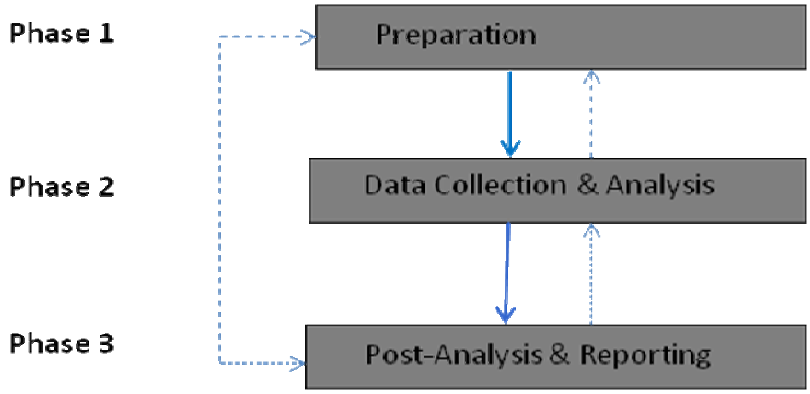


Figure 4.2: High-Level design of the proposed model

Preparation Phase 1

The phase 1 activities are carried out before the actual digital (laboratory) data collection. The phase is made up of several sub-phases namely;

- **Authorization to conduct search**
- **Planning**
- **Securing the scene**
- **Survey and Recognition**
- **Physical Crime scene data collection**
- **Device mode determination and**
- **Signal Isolation**

Phase 2 covers the digital (laboratory) data collection of the evidence and the subsequent analysis of the same. The processes involved include the, **preservation, laboratory data collection, examination and analysis.** The iteration between Phase 1 and Phase 2 allows the investigator to loop within the phases for more evidence.

Phase 3 is the Post-Analysis and Reporting which is made up of the **presentation, reporting and review of the results** of the forensic examination.

Figures 4.3 show an expanded logical design of the proposed hand-held forensics model and the corresponding inputs, processes and outputs;

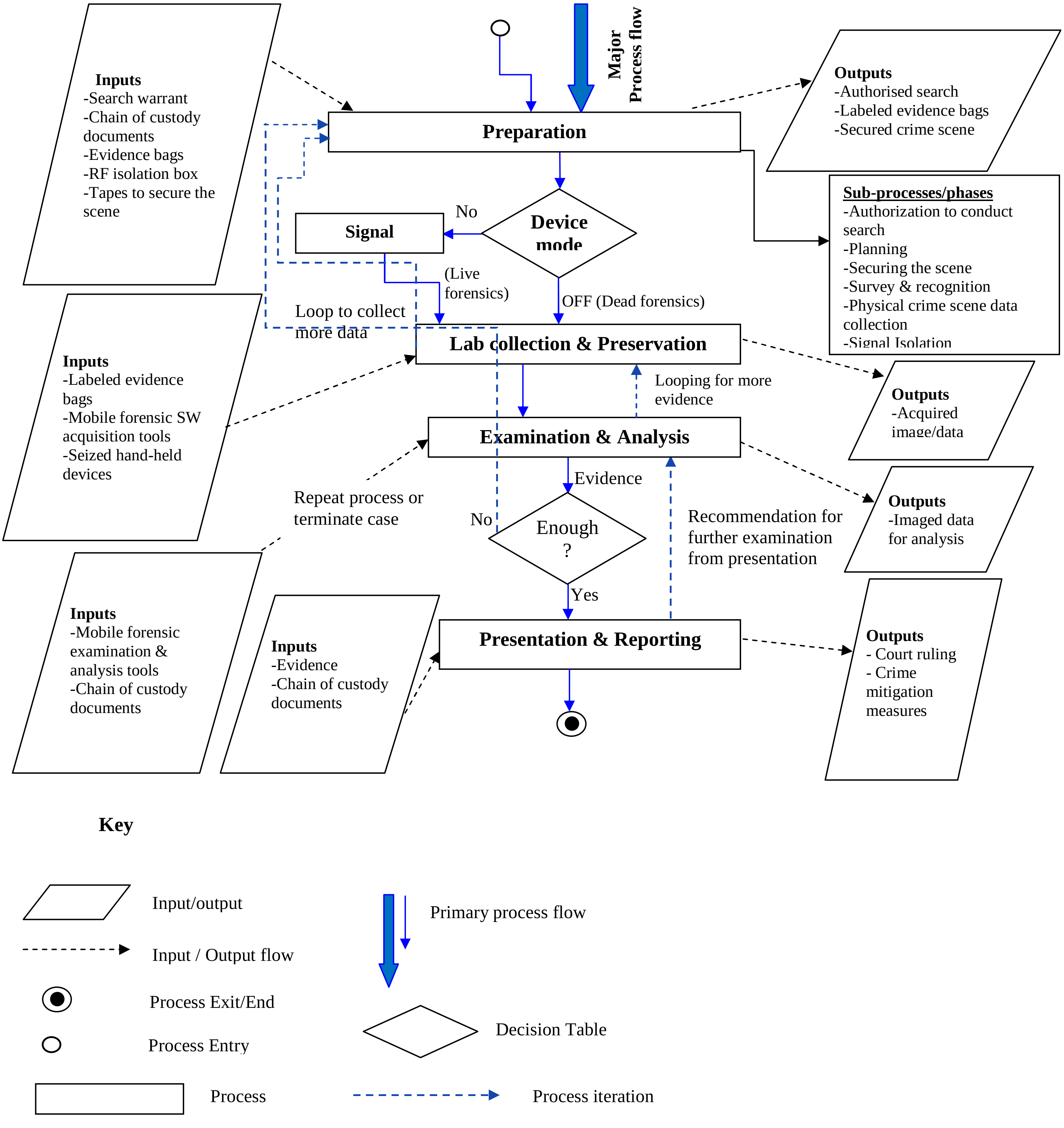


Figure 4.3: Detailed Logical design of the proposed EMFPM

In the expanded logical design of the proposed process model (Figure 4.3), there is a decision diamond sign in Phase 1 (Preparation Phase); this signifies a decision of whether the mobile device is in ON state or OFF state. In the case that it is in ON state, the device undergoes signal isolation to prevent evidence interference since mobile devices especially Smartphones change data dynamically to the extent of even being remotely controlled without physical contact with the phone.

The iteration within Phase 2 between “Laboratory Collection & Preservation” and “Examination and Analysis” sub phases indicate that during the examination stage, the forensic examiner can reference back to the collected & preserved data for more evidence if needed. As well there are iterations between sub-phase 2 “Examination and Analysis” and sub phase 3”presentation and reporting” aimed at allowing the investigator to loop between the two phases for further evidence refining.

During Phase 3, presentation and Reporting, depending on the outcome of the forensic report or recommendations of the presentation, the forensic examiner can either close the case or be referred back to collect more evidences to backup the earlier presented report, hence the reason for the decision and an iteration to Phase 1.

4.3 Formal Modeling Using Unified Modeling Language

4.3.1 Introduction to UML

“Majority of the forensic models focus mainly on the investigative process and its different phases and are characterized by a rather informal and intuitive approach”, (Sabah et al., 2012).

Digital forensics investigation can benefit from the inclusion of a formal modeling approach, (Kohn et al., 2008). Examples of such formal modeling approaches are: relational algebra, Z-specification and UML modeling. (Kohn et al., 2008), proposes the use of UML modeling as the vehicle for the formal modeling of the Digital Forensic Process Models (DFPM) as it is an acceptable formal specification for modeling of processes that also provides a structured and behavioral approach for a forensic investigation.

The **Unified Modeling Language (UML)** is a visual, object-oriented, and multi-purpose modeling language. While primarily designed for modeling software systems, it can also be used for other types of process modeling, (Gregory et al., 2005).

The basic building block of a process description in UML is the activity. An activity is a behavior consisting of a coordinated sequencing of actions. It is represented by an activity diagram. The Activity diagrams visualize sequences of actions to be performed including control flow and data flow, (Gregory et al., 2005).

Section (4.3.2) and (4.3.3) discusses the process flow in the activity diagram and the Use Case design of the proposed mobile forensics process model respectively;

4.3.2 Activity diagram

In the proposed model, **Collect, Preserve, Examine & Analyse and report** are processes. These processes begin with a start state and close/terminate with a finish state. The arrows denote a sequence of activities and the dotted lines indicate iteration meaning that, the investigator can consider going back to a previous process to collect more data or repeat a process. The entire process is triggered by a criminal incidence/ action which calls for the starting point. Figure 4.4 shows the activity diagram of the proposed model.

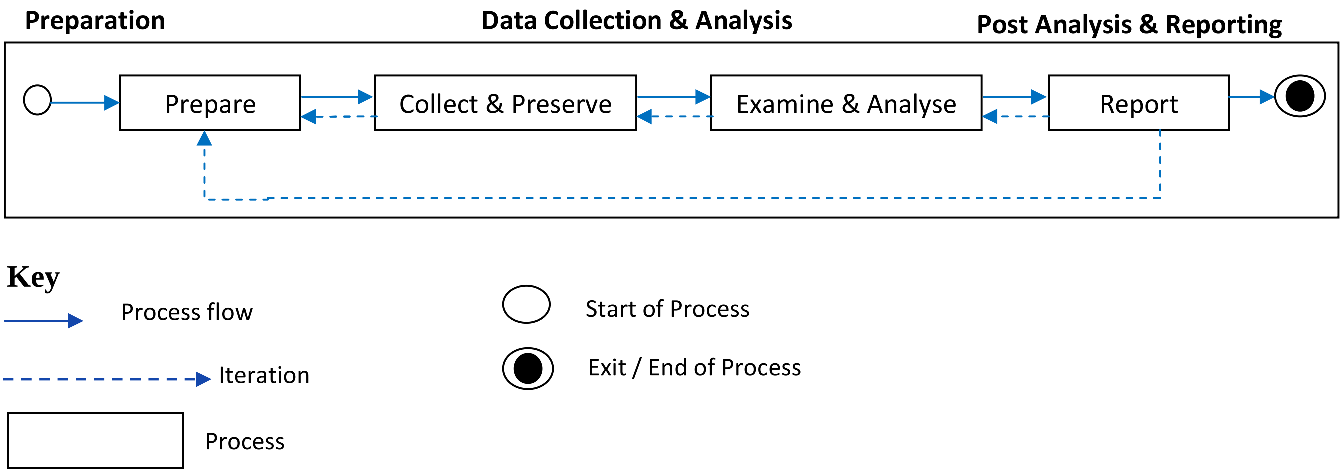


Figure 4.4: Activity diagram of the proposed model

The activity diagram of the proposed EMFPM starts with a prepare activity which is regarded as phase 1 and involves the initial readiness for the forensic investigation.

Collect and preserve are the next processes and entail evidence conservation, transportation and acquisition while maintaining a strict chain of custody. Examine and analyse phase aims to discover any hidden or vague data. The outcome of these processes yields evidence that can be used in court.

The report phase results in a report presented in court about the process followed during the investigation.

4.3.3 Use Case Diagram

In the use case diagram, there are four main actors that interact with the system, namely; the investigator, the prosecutor, the defense and the Court. An Investigator can be either a police officer or a forensic investigator. The Investigator can be specialized to a First Responder, which can be Emergency Response Team or even a System Administrator. The Prosecutor and the Defense are role players in a criminal matter only. They are interested in the steps taken in each of the use cases. The Investigator interacts with all the use cases.

The Court is used to evaluate the presented evidence report. It evaluates the final documents of the prosecution and defense and does not interact with the system during any other level before the reports are presented to it. Its interest is only in the findings presented in the evidence report, and it will reach a finding based on the presented evidence. The Court also determines the admissibility and weight of each of the pieces of evidence included in the evidence report.

Figure 4.5: illustrates the Use case diagram of the proposed model;

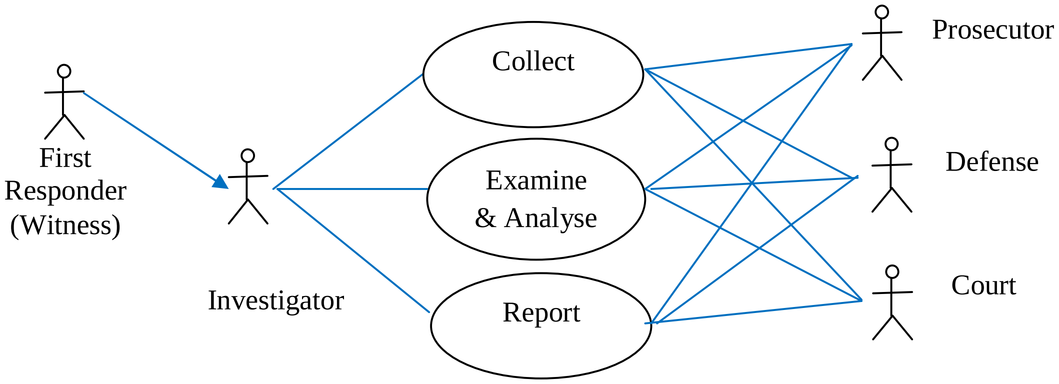


Figure 4.5: Use case diagram design of the proposed model

CHAPTER FIVE: IMPLEMENTATION MODEL

5.1 Introduction

This chapter introduces the proposed hand-held forensic process model, the Enhanced Mobile Forensic Process Model for Hand-Held Devices (EMFPM). The phases and the functions of the new model are discussed followed by the test results carried to ascertain the applicability of the proposed model.

5.2 The Proposed EMFPM Model

This research proposes an Enhanced Mobile Forensic Process Model for Hand-Held Devices (EMFPM) which is aimed at improving and providing a standardized hand-held device digital forensic investigation process, especially on Smartphones. The model was developed using ideas borrowed from previous digital forensics models namely;

- " Symbian Smartphones Process model", (Xian et al., 2009)
- "Windows mobile devices Forensic investigation process model", (Anup, 2011)
- "Smartphone Forensic Investigation Process Model (SPFIPM)", (Archit et al., 2012)
- "The Integrated Digital Investigation Model" , (Carrier et al., 2003)

However, some new processes and attributes to specifically suit mobile hand-Held digital forensic have been introduced. Table 5.1 summarizes the mapping of the previous digital forensics models to the proposed model;

Standard Digital Forensics Processes – (NIST, 2006)	**Mapping of the previous forensics models to the Proposed Model;**					
	NIJ Law Enforcement Model – (NIJ, 2001)	**IDIP Model – (Carrier et al, 2003)**	**Symbian Smartphone Phone forensics Model – (Xian et al., 2009)**	**Windows Mobile device forensic Model – (Anup, 2011)**	**Smartphone Forensic Investigation process Model (SPFIPM) – (Archit et al., 2012)**	**Enhanced Mobile Forensic Process Mobile (EMFPM) – Proposed**
Collection	✓	✓	x	✓	✓	✓
Examination	✓	x	x	✓	✓	✓
Analysis	✓	✓	✓	✓	✓	✓
Reporting	✓	x	✓	✓	✓	✓

Table 5.1: Mapping of the previous mobile forensics models to the Proposed Model

Key:

✓ - Model's process directly conforms to NIST standard digital forensic processes

x - Model's process do not directly conform to NIST standard digital forensic processes

At first glance, one would think that the proposed mobile devices model contributes little more than what is in existence. However, it should be noted that the proposed EMFPM brings with it enormous contributions into the mobile digital forensics field. Highlighted below are the unique features of the proposed model;

- The conceptual design of the proposed model introduces process modeling through the use of UML. Most forensic models dwell on the investigative process and its different phases and are characterized by a rather informal and intuitive approach, (Sabah et al., 2012). The significance of this modeling is to enable both members and non-members of the digital forensics community to utilize and understand the nuances of the proposed model.
- The preparation phase of the new model integrates physical crime scene data collection and analysis. This idea is borrowed from (Carrier et al., 2003) model, "Integrated Digital Investigation Model". The goal of the physical crime scene investigation phases is to conduct data collection and analyze the physical evidence that would help in reconstructing the actions that took place during the incident.
- Iterations are incorporated in all the major phases inorder to help yield more concrete evidence. The previous models lack this yet it is less likely for investigations to take a sequential nature given that more information may crop in prompting the investigator to revisit previous phases.
- Besides, a great emphasis of both Live and Dead forensics is put into account, meaning that the mobile device investigation would follow a slightly different process subject to the state of the phone at the time of seizure. The idea of Live and Dead forensics is borrowed from (Archit et al., 2012) model, "Smartphone Forensic Investigation Process Model (SPFIPM)".

5.3 The proposed EMFPM phases

The proposed handheld forensics implementation model is as shown in figure 5.2;

As seen in chapter 4 above, the proposed mobile forensics model consists of three major phases. These three major phases are in turn constituted of sub-phases as discussed below;

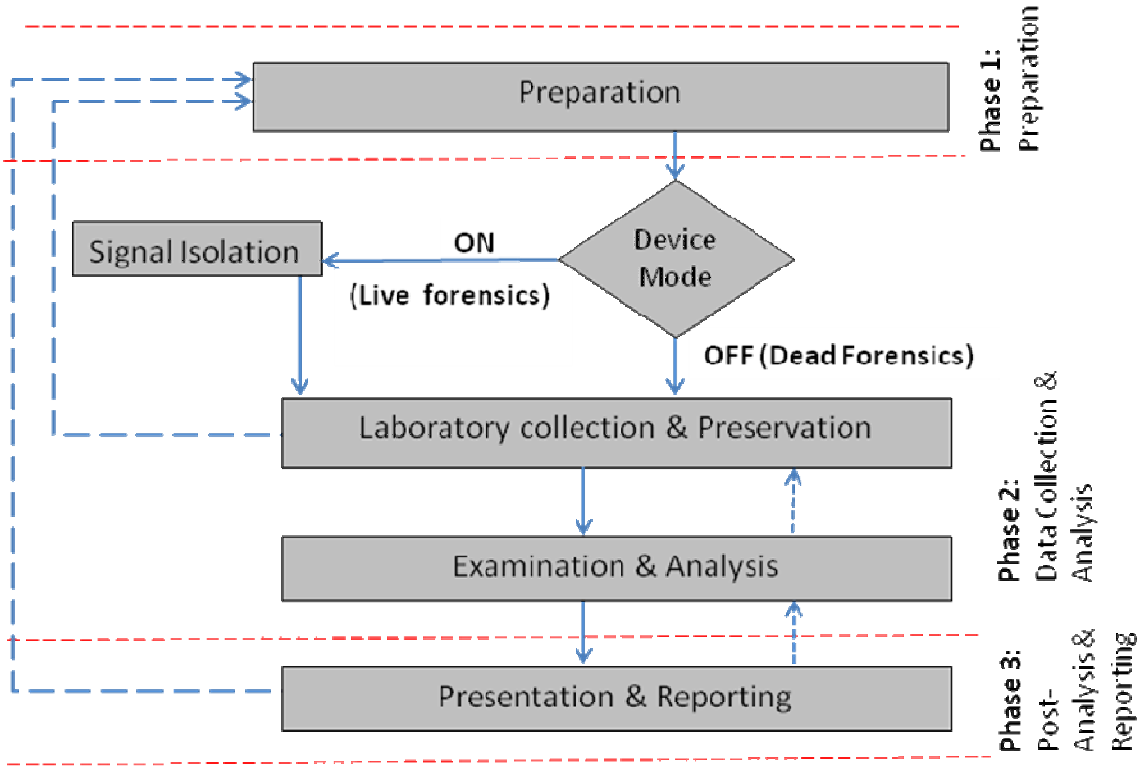


Figure 5.2: The proposed handheld forensics implementation model

5.3.1 Phase One: Preparation

This is the first major phase of the proposed forensic mobile forensics process model and it consists of seven processes (sub-phases) namely; **Authorization to conduct search, Planning, Securing the scene, Survey and Recognition, Physical Crime scene data collection**, **Device mode determination and Signal Isolation.**

- **Authorization to conduct search**, widely known as “search warrant” in legal terms is the first step for any forensic investigation before moving to any scene, depending on the nature of the crime. The operation must be legally authorized to avoid future legal setbacks such as invasion of personal privacy, (Anup, 2011).

- **Planning sub-phase**

  The Planning sub-phase entails getting an initial understanding of the form/nature of the incidence (crime) and activities like preparing the tools required for standard portable electronic device investigations, building an appropriate team, assigning roles to each personnel, accumulating materials for packing evidence sources etc. In most hand-held devices, especially Smartphones, the power may drain before evidence collection is over, so it is essential to prepare a toolkit consisting of standard power supplies, cables and cradles.

- **Securing the Scene**

  This is the second sub-phase of the Preparation phase and entails securing of scene of crime from unauthorized access and preserving the evidence from contamination. The investigators need to make sure that interference of the crime scene is avoided. Minimizing the corruption of evidence should be the top priority. This sub-phase phase is very crucial and determines the success of the investigation through the quality of the evidence.

- **Survey and Recognition sub-phase**

  This is the third sub-phase of the Preparation phase. It involves a prior site survey carried out by the investigator to evaluate the scene, identify potential sources of evidence and formulate an appropriate search plan.

- **Crime scene data collection**

  This is the fourth sub-phase of the Preparation phase. The phase is borrowed from (Carrier et al, 2003) model, “Integrated Digital Investigation Model”. The main aim of this phase is to collect and analyze the physical evidence that would help in reconstructing the actions that took place during the crime/incident.

  The phase covers photographing of the crime scene along with documentation, sketching and crime-scene mapping. All the electronic devices found at the scene must be photographed. If a mobile device is switched on (‘ON’ mode), whatever is visible on the screen is should be documented as well. A record of all visible data must be created, that aids in reconstructing the scene and reviewing it as need be. Circumstances surrounding the crime / incident, including those who reported the incident, at what date and time, should be included. Logs of those who left and those present at the scene should also be documented alongside with their roles, (Archit et al., 2012),

- **Device mode determination**

  Always is advised never to alter the mode in which a device is working in, (Archit et al., 2012). This phase therefore decides on the first course of action subject to the device status in hand at the time of seizure.

  - ✓ **'ON' Mode:** A hand-held device is ON' mode if it is running/switched on. In such a case the hand-held device is shielded from outside network interference while maintaining the device status (mode) such that the potential vulnerable volatile evidence is kept intact. For this reason, the hand-held device is moved first to Signal Isolation sub-phase prior to further working.
  - ✓ '**OFF' Mode:** A hand-held device is in OFF' mode if it is switched off. To keep the evidence unchanged, it is advised never to turn the device on since this may lead to overwriting of old data with new data", (Archit et al., 2012). Thus we can continue with Laboratory data collection and Preservation skip signal isolation.

5.3.2 Phase Two: Data Collection & Analysis Phase

This is the second major phase of the proposed hand-held forensics digital process mode. The stage involves the actual digital investigation process after the initial preparation stage is completed and consists of the following processes: **Laboratory evidence collection, Preservation, Examination and Analysis.**

- ✓ **Preservation -** Having determined the device mode and performed signal isolation for the 'ON' mode devices where available, the next phase is to preserve and avail the devices into a forensic laboratory so as to commence on the data imaging. The preservation sub-process entails packaging of the evidence, transportation and storage. Procedures should be followed and documented throughout the whole process so that the electronic evidence collected from the scene is not altered nor destroyed. Potential sources of evidence should be identified and labeled appropriately prior to packaging. The labeled potential evidence and accessories must be placed in an evidence bag and kept in a radio frequency isolation container to avoid further communications with any other device, (Anup, 2011). Chain of custody is also very crucial for the digital to meet the admissibility test and must be maintained all the time, (Archit et al, 2012).

- ✓ **Laboratory Data Collection –** Once the potential evidence sources are availed at the laboratory, Dead or Live Forensics data acquisition is chosen depending on the state of the phone at the time of seizure. If the device is in 'OFF' mode, Dead forensics is performed and incase the device is in 'ON' mode then Live forensics acquisition is followed.

- **Examination -** This entails examining the contents of the evidence collected by forensic specialists and extracting information, relevant for proving the case. Evidence back-ups must be created prior to proceeding with the examination. This process aims at making the evidence transparent enough while also explaining its originality and significance.

- **Analysis*:*** This step can be regarded to be more of a technical review which is performed by the forensic investigative team on the basis of the results obtained from the examination sub-phase. The evidence results of the examination sub-phase is analyzed to identify relationships between data fragments, hidden data, determining the significance of the information obtained from the examination sub-phase, reconstructing the event data, based on the data extracted and drawing proper conclusions. In many instances, iteration of examination and analysis sub-phases is be needed in order to get the full picture of an incident or crime, (Ankit et al., 2011).

5.3.3 Phase Three: Post-Analysis and Reporting

This is the last phase after the digital forensic evidence has been examined and analyzed. The stage involves the presentation of the analyzed evidence before a number of audiences that include; law enforcement, corporate management, legal experts etc. "Depending on the nature of the crime, the results of the findings are presented in a court of law, if it is a police investigation or before appropriate corporate management, if it is an internal company investigation," (Ankit et al., 2011). In the Reporting sub-phase, a detailed report summary of the various events that took place during the incident/crime together with the complete description of the various steps involved in the process of investigation and the conclusions drawn should be documented and provided. The laboratory report is regarded as one of the most important documents for the investigator and all the parties involved in a case, (Vlachopoulos et al., 2012).

After reporting, a review of all the steps involved during the investigation process is carried out to identify the areas of improvement. The results and their interpretations may be used in future for further refining the gathering, examination and analysis of evidence in future investigations.

5.4 Testing of the proposed mobile forensics process model

5.4.1 Scope of the tests

The test covers the last process of the first phase which is the **Device mode determination** and second phase of the proposed process model which is **Data collection and Analysis**. These phases are chosen as the test points because;

- It is in these phases where a significance contribution is found
- The Device mode determination sub-phase and the Data collection and Analysis phases are easily testable unlike other phases

Several tools are used to facilitate the tests namely;

- Cellebrite UFED Physical Analyzer 3 (Cellebrite.com, 2013)
- Oxygen Forensic Suite 2013 Standard Edition (Oxygen Forensics.com,2013)
- MOBILedit forensics Lite (mobiedit.com, 2013)

Two types of Phones running different Operating Systems namely; iPhone (iOS) and Samsung Galaxy S III (Android OS) were employed for the experimental tests.

5.4.2 Specific test objectives of the proposed forensics process model and the results

i.) To test whether it is possible to extract and analyse data from a phone which is in 'OFF' state (Dead Forensics) ii.) To test whether it is possible to extract and analyse data from a phone which is in ‘ON’ state (Live Forensics)

iii.) Testing extend at which data can be extracted from a range of different phones that have been initially fed with similar data (Using either Dead or Live Forensics).

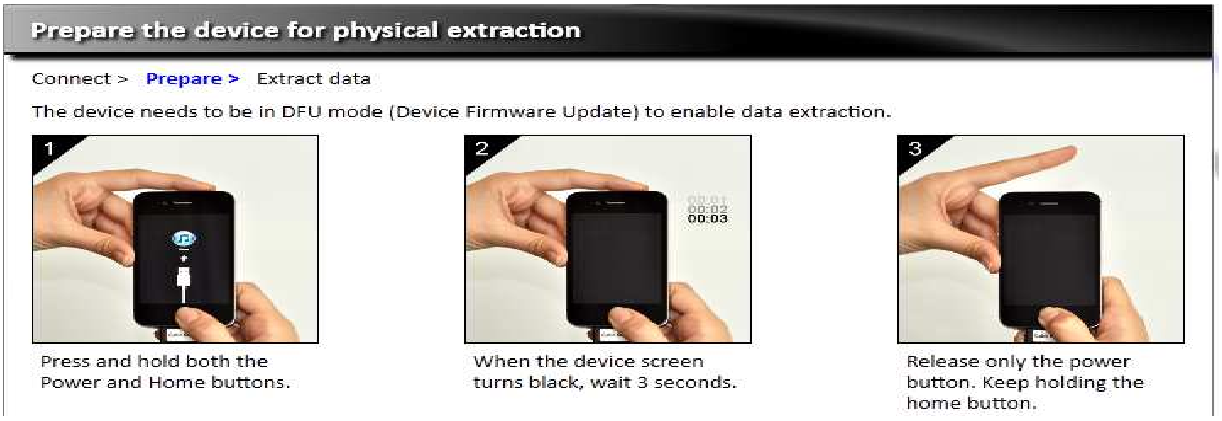
A discussion and illustration of the tests follows;

Test objective 1; to test whether it is possible to extract and analyse data from a phone which is in ‘OFF’ state (Dead Forensics);

This test is accomplished through the use of iPhone and Cellebrite UFED Physical Analyser mobile forensics tool. The iPhone already had sample data accumulated over time and this is what was used for the tests. The investigation here proceeded with the phone being on ‘OFF’ state.

Steps;

- ✓ We avail the iPhone and its USB data cable. Secondly, we ensure that we have a laptop that has Cellebrite UFED Physical Analyser 3 installed to it.
- ✓ Next, we launch the UFED Physical Analyser 3 and click on the iOS Physical device menu option. The below screen pops up guiding the investigator on how to prepare the iPhone device for data extraction;



Prepare the device for physical extraction

The device needs to be in DFU mode (Device Firmware Update) to enable data extraction.

1 Press and hold both the Power and Home buttons.

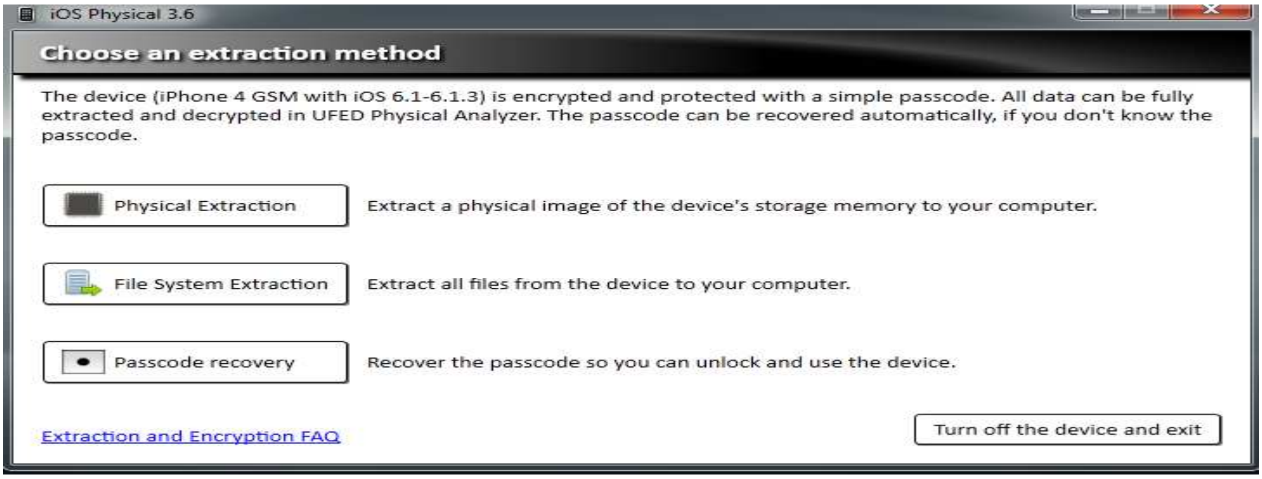
2 When the device screen turns black, wait 3 seconds.

3 Release only the power button. Keep holding the home button.

Screenshot 5.1 Preparing iPhone phone for physical data extraction

- ✓ After successfully following the above steps, the iPhone is successfully connected to the UFED Physical Analyzer

- ✓ Next, we are prompted with a screen asking to choose the extraction method; In this case, the File System Extraction method was selected; The iPhone contained a passcode and this was automatically detected by the UFED physical Analyser;



Choose an extraction method

The device (iPhone 4 GSM with iOS 6.1-6.1.3) is encrypted and protected with a simple passcode. All data can be fully extracted and decrypted in UFED Physical Analyzer. The passcode can be recovered automatically, if you don't know the passcode.

Extract a physical image of the device's storage memory to your computer.

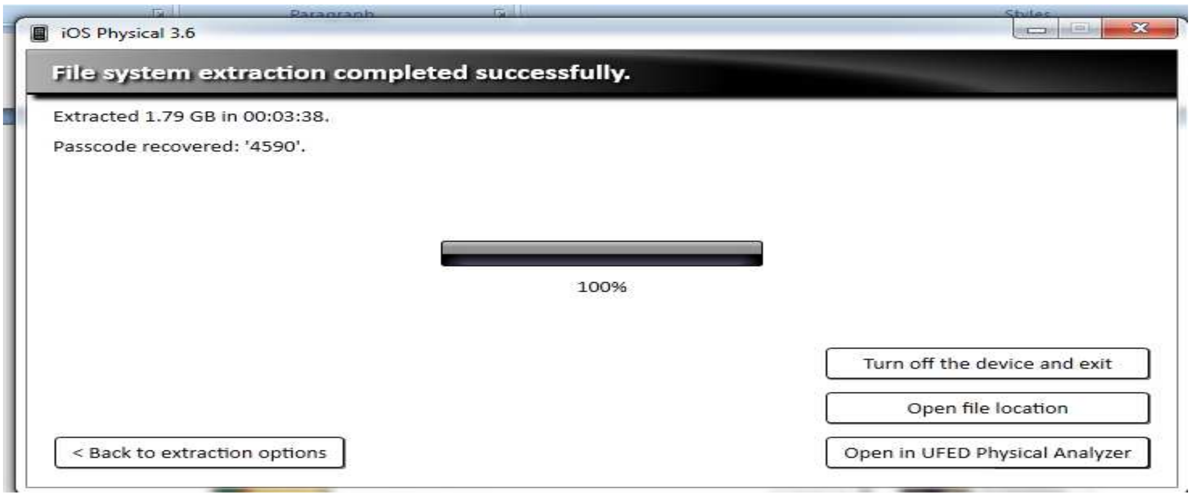
Extract all files from the device to your computer.

Recover the passcode so you can unlock and use the device.

Screenshot 5.2 Choosing an extraction method

- ✓ Assumption was made that the passcode for the phone was unknown and we let the UFED physical analyser recover the passcode. The passcode was automatically recovered and file extraction completed successfully as show in screenshot 5.4;

  Just to note, the forensic software tools requires a root access to the phone's prior to data extraction.



File system extraction completed successfully.

Extracted 1.79 GB in 00:03:38.

Passcode recovered: '4590'.

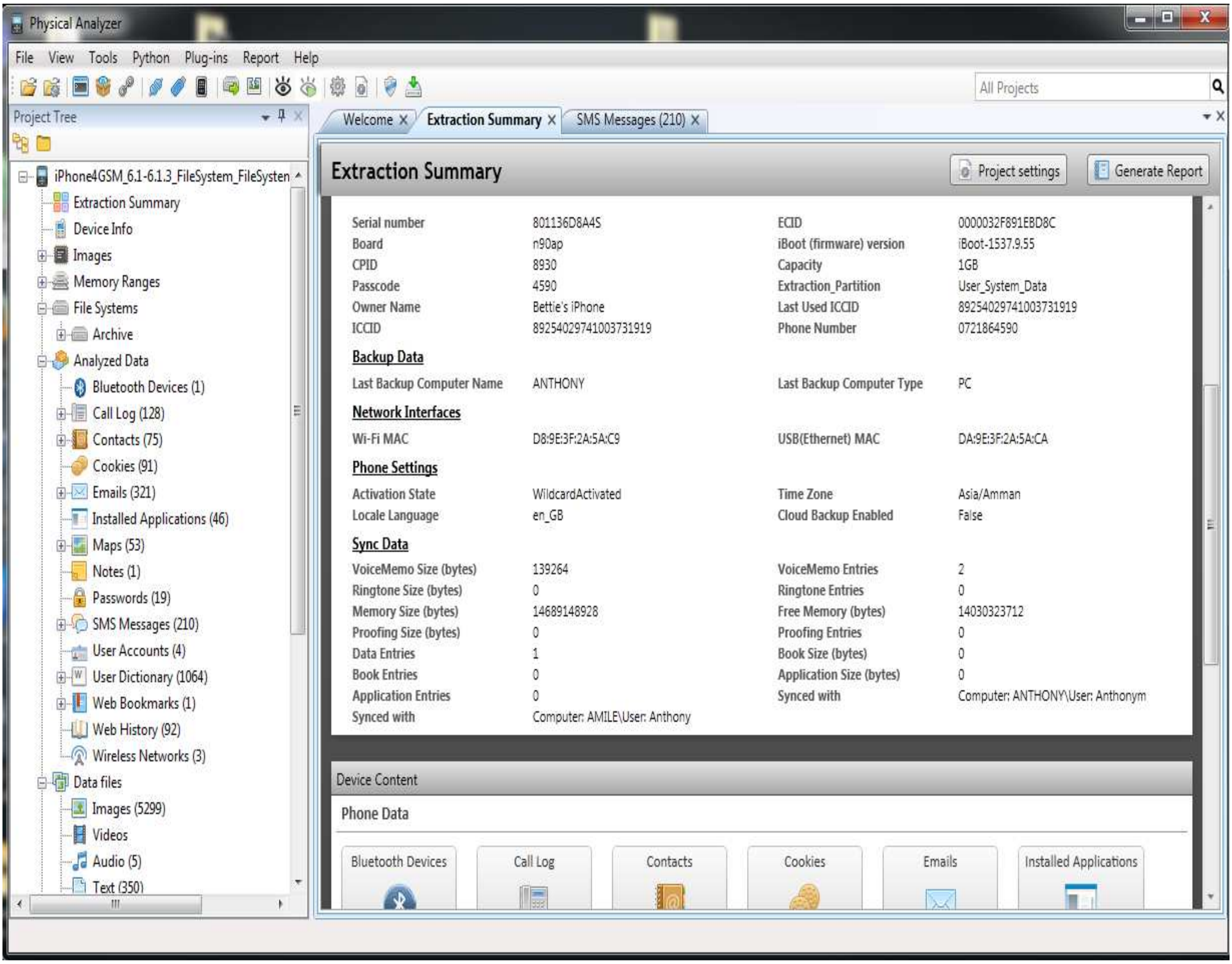
100%

Turn off the device and exit
Open file location
< Back to extraction options
Open in UFED Physical Analyzer

Screenshot 5.3: Passcode recovery and file system extraction completion

- ✓ Having extracted data it's the time for Examination and analysis. The acquired data is as illustrated in Screenshot 5.4a and 5.4b:

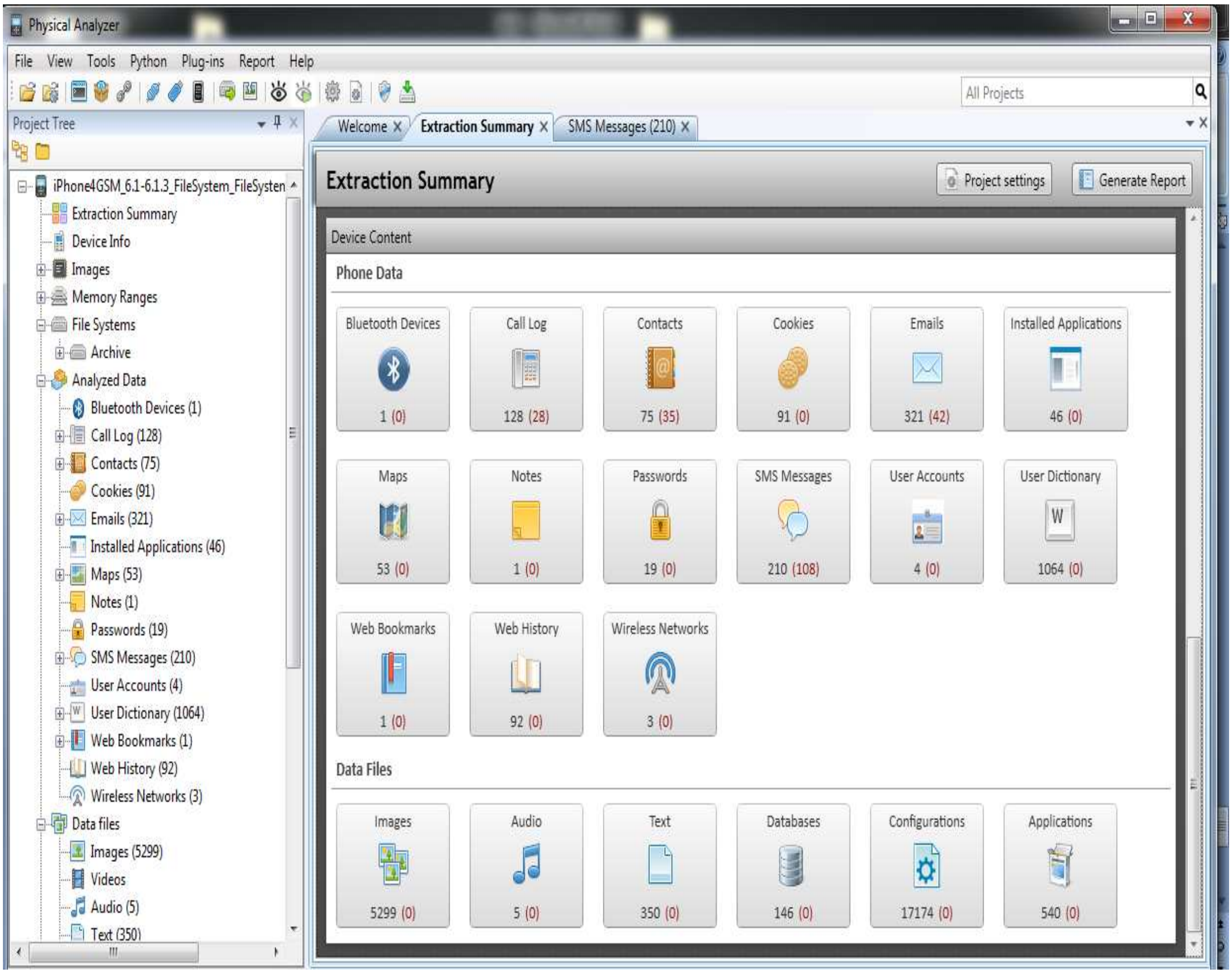
Screenshot 5.4a Summary of the Extracted data from the iPhone though Dead acquisition



Extraction Summary

Serial number	801136D8A4S	ECID	0000032F891EBD8C
Board	n90ap	iBoot (firmware) version	iBoot-1537.9.55
CPID	8930	Capacity	1GB
Passcode	4590	Extraction_Partition	User_System_Data
Owner Name	Bettie's iPhone	Last Used ICCID	89254029741003731919
ICCID	89254029741003731919	Phone Number	0721864590
Backup Data			
Last Backup Computer Name	ANTHONY	Last Backup Computer Type	PC
Network Interfaces			
Wi-Fi MAC	D8:9E:3F:2A:5A:C9	USB(Ethernet) MAC	DA:9E:3F:2A:5A:CA
Phone Settings			
Activation State	WildcardActivated	Time Zone	Asia/Amman
Locale Language	en_GB	Cloud Backup Enabled	False
Sync Data			
VoiceMemo Size (bytes)	139264	VoiceMemo Entries	2
Ringtone Size (bytes)	0	Ringtone Entries	0
Memory Size (bytes)	14689148928	Free Memory (bytes)	14030323712
Proofing Size (bytes)	0	Proofing Entries	0
Data Entries	1	Book Size (bytes)	0
Book Entries	0	Application Size (bytes)	0
Application Entries	0	Synced with	Computer: ANTHONY\User: Anthonym
Synced with	Computer: AMILE\User: Anthony		

Screenshot 5.4b Summary of the Extracted data from the iPhone though Dead acquisition



Test objective 1 Results:

i).Testing whether it is possible to extract and analyze data from a phone which is in 'OFF' state (Dead Forensics);

The test objective of Dead forensics was achieved. The results of the tests are as illustrated in the figures above. Under this test we assumed that the seized phone was on 'OFF' mode thus conducting the Dead forensics data acquisition. As shown from the above extraction summaries, a lot of data was recovered from the phone. The evidence data included 128 call logs, 75 contacts, 321 emails, 46 installed applications, 19 passwords, 210 SMS messages among other data. It is important to stress that the data acquisition was conducted on an iPhone that was switched 'OFF'

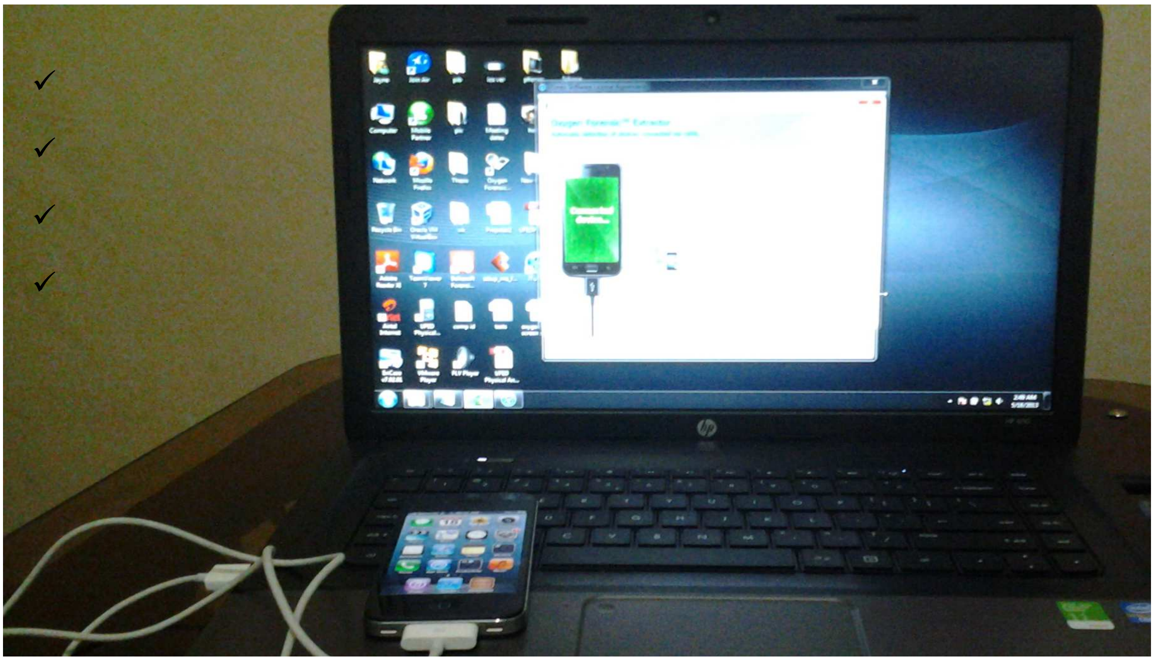
Test objective 2:

i.) **Testing whether it is possible to extract and analyse data from a phone which is in 'ON' state (Live Forensics);**

This test is accomplished through the use of iPhone and Oxygen Forensics Suite 2013 Smartphone forensics software tool. The iPhone already had sample data fed over time and this is what was used for the tests. The investigation here proceeded with the phone being on 'ON' state.

Steps;

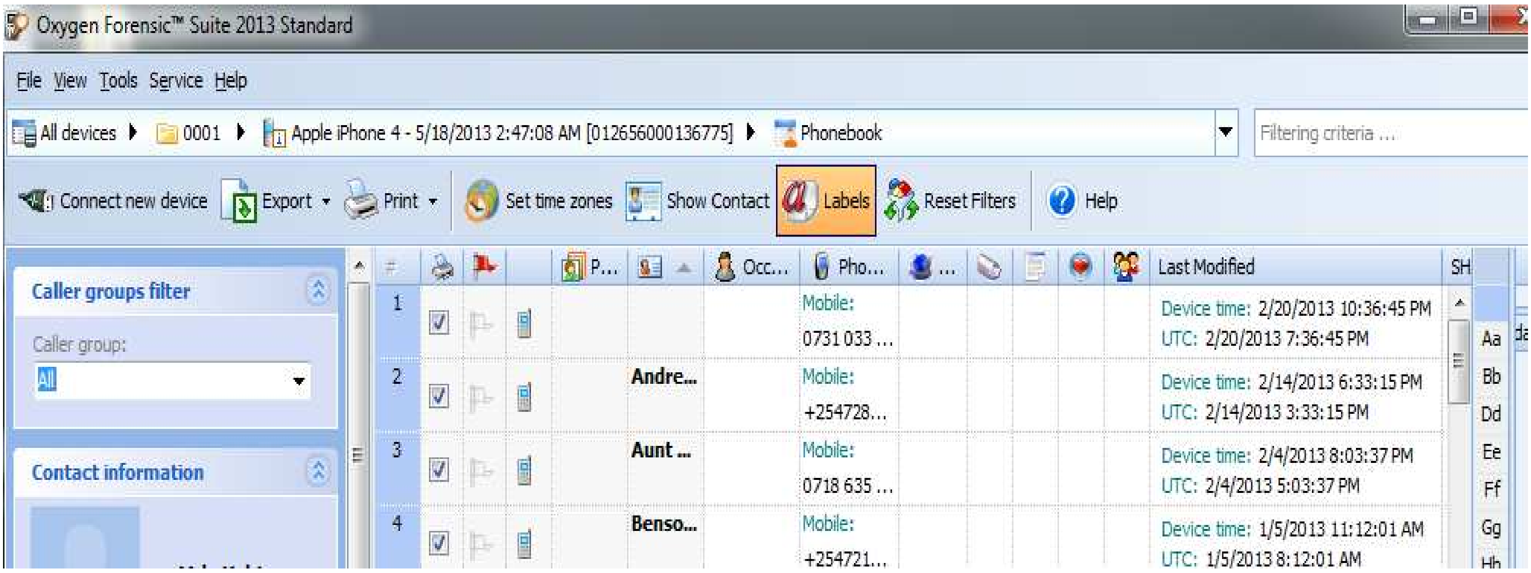
- ✓ We avail the iPhone and its USB data cable. Secondly, we ensure that we have a laptop running Oxygen Forensics Suite 2013.
- ✓ Next, launch the Oxygen Forensics Suite 2013 and connect the iPhone device while it is still on 'ON' state. From the file menu, click on to Connect new device.
- ✓ If successful, the device will be connected as illustrated in screenshot 5.5;



Screenshot 5.5: iPhone successfully connected to Oxygen forensic suite 2013

- ✓ Next we initiate the data extraction process.
- ✓ The data extracts contains primarily of personal data such as phone contacts, names and for this reason the data is deliberately not fully displayed;

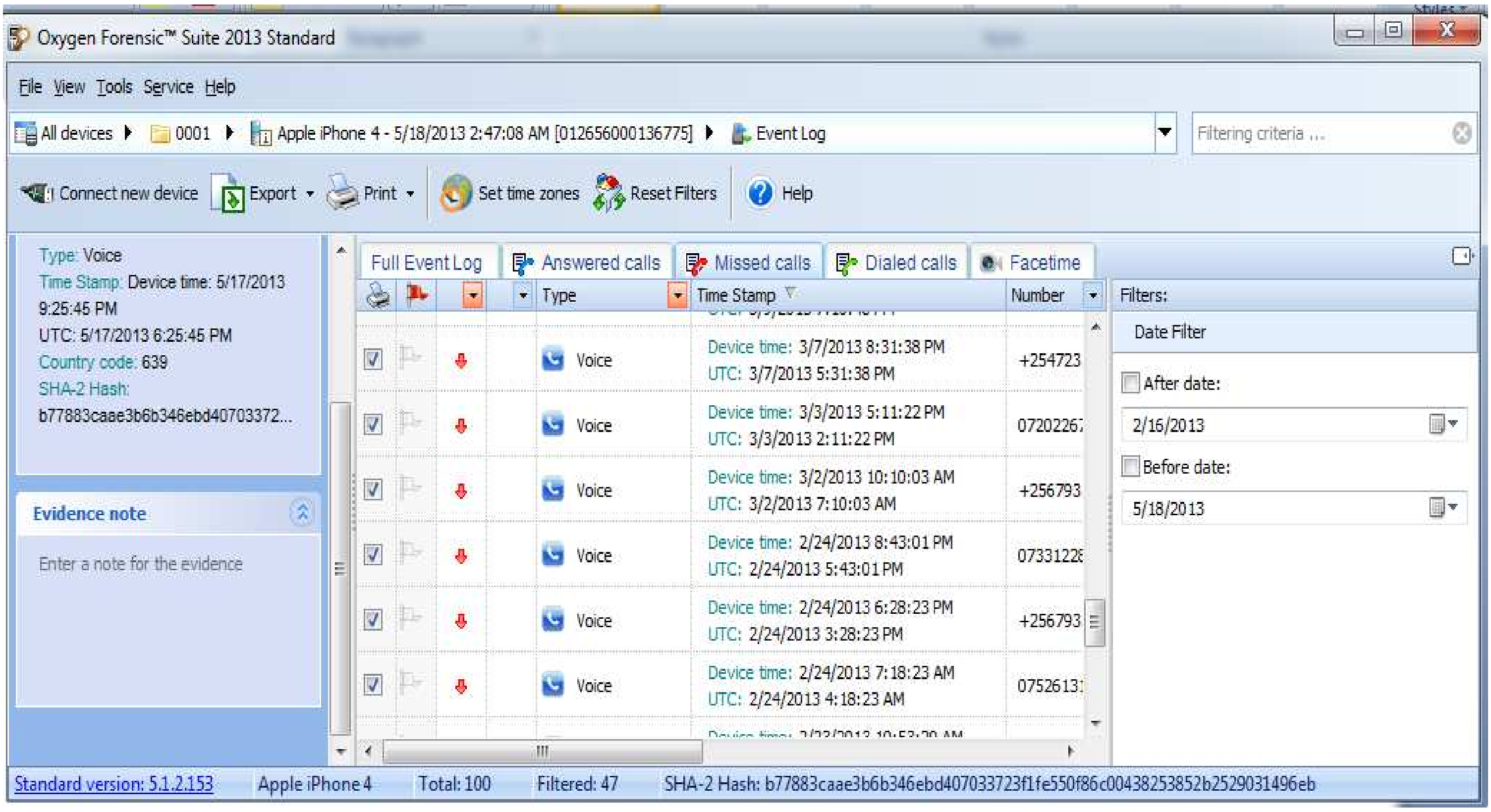
This screen capture 5.6 displays the acquired phone contacts:



#	P...	Occ...	Pho...	Last Modified
1			Mobile: 0731 033 ...	Device time: 2/20/2013 10:36:45 PM UTC: 2/20/2013 7:36:45 PM
2	Andre...		Mobile: +254728...	Device time: 2/14/2013 6:33:15 PM UTC: 2/14/2013 3:33:15 PM
3	Aunt ...		Mobile: 0718 635 ...	Device time: 2/4/2013 8:03:37 PM UTC: 2/4/2013 5:03:37 PM
4	Benso...		Mobile: +254721...	Device time: 1/5/2013 11:12:01 AM UTC: 1/5/2013 8:12:01 AM

Screen capture 5.6: Displays acquired phone contacts:

The screen shot 5.7 displays the full event log (answered calls, missed calls, dialed calls, etc):



Type: Voice
Time Stamp: Device time: 5/17/2013 9:25:45 PM
UTC: 5/17/2013 6:25:45 PM
Country code: 639
SHA-2 Hash:
b77883caae3b6b346ebd40703372...

Type	Time Stamp	Number
Voice	Device time: 3/7/2013 8:31:38 PM UTC: 3/7/2013 5:31:38 PM	+254723
Voice	Device time: 3/3/2013 5:11:22 PM UTC: 3/3/2013 2:11:22 PM	07202267
Voice	Device time: 3/2/2013 10:10:03 AM UTC: 3/2/2013 7:10:03 AM	+256793
Voice	Device time: 2/24/2013 8:43:01 PM UTC: 2/24/2013 5:43:01 PM	07331228
Voice	Device time: 2/24/2013 6:28:23 PM UTC: 2/24/2013 3:28:23 PM	+256793
Voice	Device time: 2/24/2013 7:18:23 AM UTC: 2/24/2013 4:18:23 AM	0752613

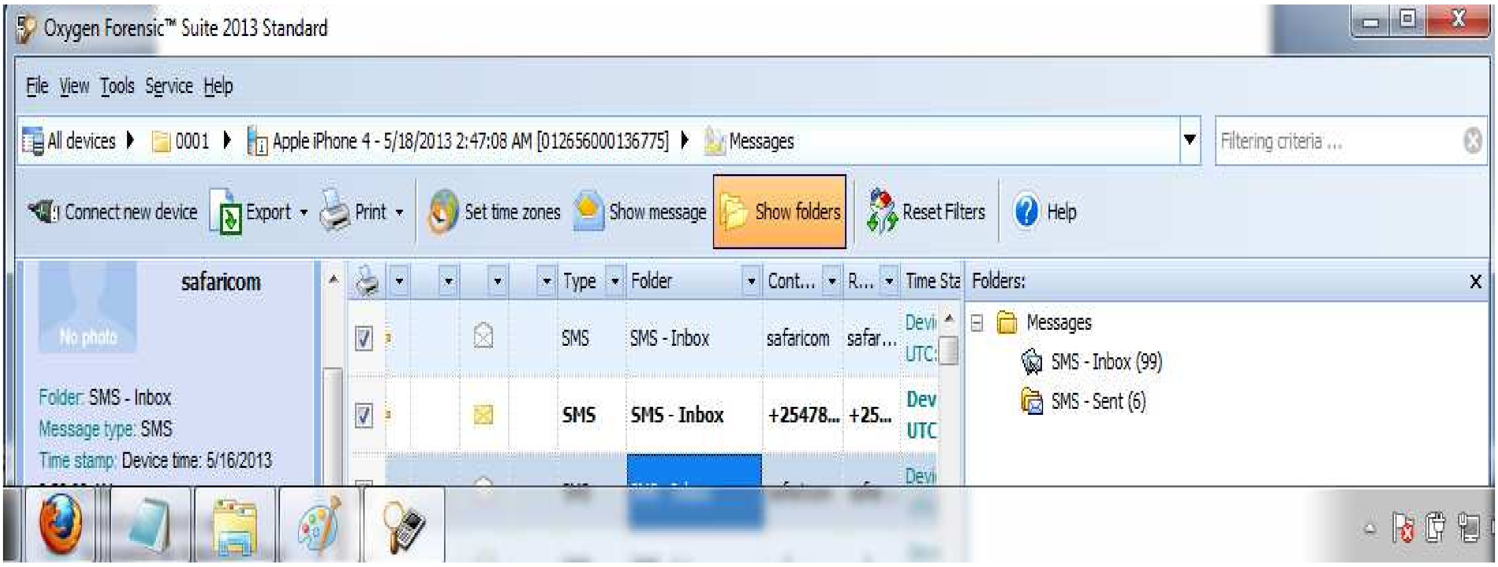
☐ After date:
2/16/2013
☐ Before date:
5/18/2013

Standard version: 5.1.2.153 Apple iPhone 4 Total: 100 Filtered: 47 SHA-2 Hash: b77883caae3b6b346ebd407033723f1fe550f86c00438253852b2529031496eb

Screenshot: 5.7 Full event log (answered calls, missed calls, dialed calls, timelines etc)

This screenshot 5.8 displays SMS logs including the sender name, number etc:

The acquired data is partially displayed due to the sensitivity of the personal data involved.



safaricom

Folder: SMS - Inbox

Message type: SMS

Time stamp: Device time: 5/16/2013

Type	Folder	Cont...	R...	Time Sta
SMS	SMS - Inbox	safaricom	safar...	Devi UTC:
SMS	SMS - Inbox	+25478...	+25...	Dev UTC

Screenshot 5.8 capture: displays SMS logs including the sender name, number etc:

Test objective 2: Summary of results:

ii.) Extracting and analyzing data from a phone which is in ‘ON’ state (Live Forensics);

- The test objective of Live forensics was achieved. The results of the tests are as illustrated in the figures above. Under this test, the acquisition proceeded with the phone in ‘ON’ state. The extracted process acquired a substantial amount of data from the iPhone. The extracted data consisted of information such as SMS, phonebook, phone event logs such as received calls, missed calls and dialed calls.
- It is important to note that the Office forensics suite 2013 trial version does not display social network data for it is limited.

Test objective 3:

iii). Testing extend at which data can be extracted from a range of different phones that have been initially fed with similar data (Using Live Forensics).

This test is accomplished through the use of iPhone (iPhone iOS) and Samsung Galaxy S III (Android OS) and MOBILedit forensic Lite software tool. Common data was fed to the two phones. The data included dialed calls, missed calls, received calls, SMS messages and a new phone book entry (for Jane tab (0716560xxx)

The below phone numbers were used to generate the test data and have been partially displayed due to personal privacy sensitivity;

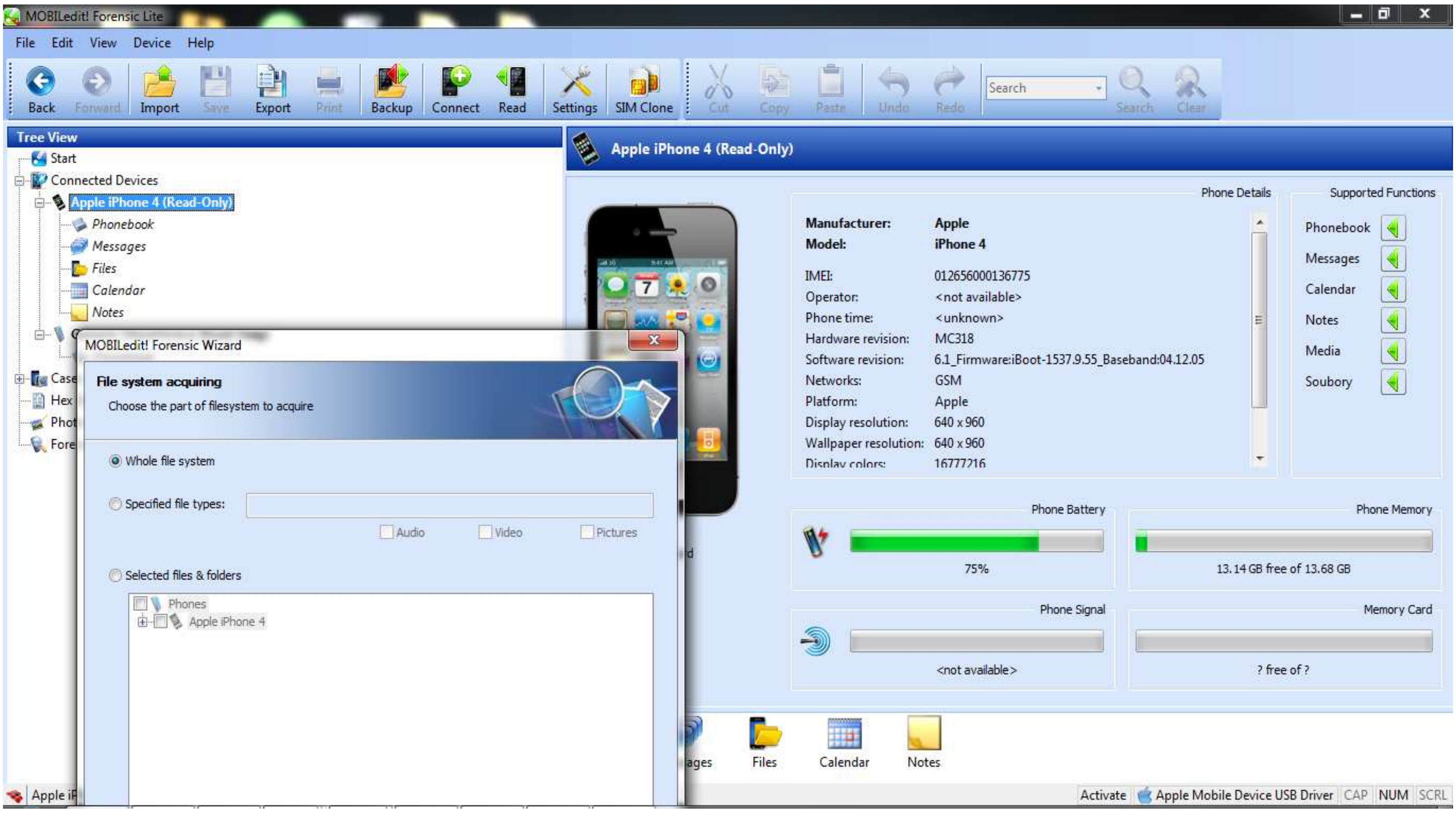
- Betty (0731271xxx)
- Jane tab (0716560xxx)
- Jane (073024xxx)

Web-based and social network data was deliberately not included since the MOBILedit forensic Lite tool does not support this. The both phones were acquired while in 'ON' state (live data acquisition).

Attached are the capture screens of both the iPhone and Samsung Galaxy S III tests respectively;

iPhone acquisition screen capture screens;

The Screenshot 5.9 illustrates the iPhone details as displayed from MOBILedit forensic Lite during data acquisition;


MOBILedit! Forensic Lite
File Edit View Device Help
Back Forward Import Save Export Print Backup Connect Read Settings SIM Clone Cut Copy Paste Undo Redo Search Search Clear
Tree View
Start
Connected Devices
Apple iPhone 4 (Read-Only)
Phonebook
Messages
Files
Calendar
Notes
Case
Hex
Phot
Fore
Apple iP
Apple iPhone 4 (Read-Only)
ages Files Calendar Notes
Activate
Apple Mobile Device USB Driver
CAP NUM SCRL

MOBILedit! Forensic Wizard

File system acquiring

Choose the part of filesystem to acquire

● Whole file system

○ Specified file types:

□ Audio □ Video □ Pictures

○ Selected files & folders

□ Phones
□ Apple iPhone 4

Phone Details

Manufacturer: **Apple**
Model: **iPhone 4**
IMEI: 012656000136775
Operator: <not available>
Phone time: <unknown>
Hardware revision: MC318
Software revision: 6.1_Firmware:iBoot-1537.9.55_Baseband:04.12.05
Networks: GSM
Platform: Apple
Display resolution: 640 x 960
Wallpaper resolution: 640 x 960
Display colors: 16777216

Supported Functions

Phonebook
Messages
Calendar
Notes
Media
Soubory

Phone Battery: 75%

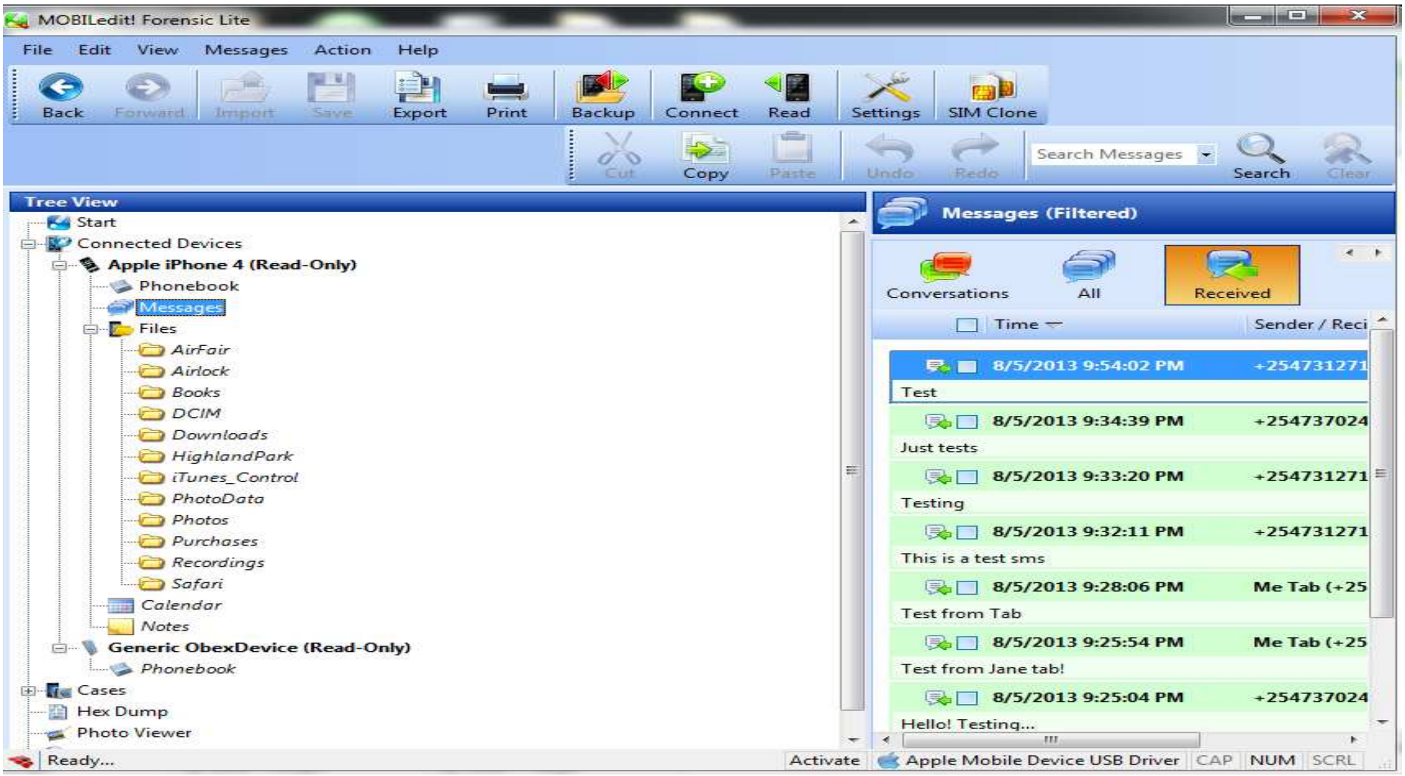
Phone Memory: 13.14 GB free of 13.68 GB

Phone Signal: <not available>

Memory Card: ? free of ?

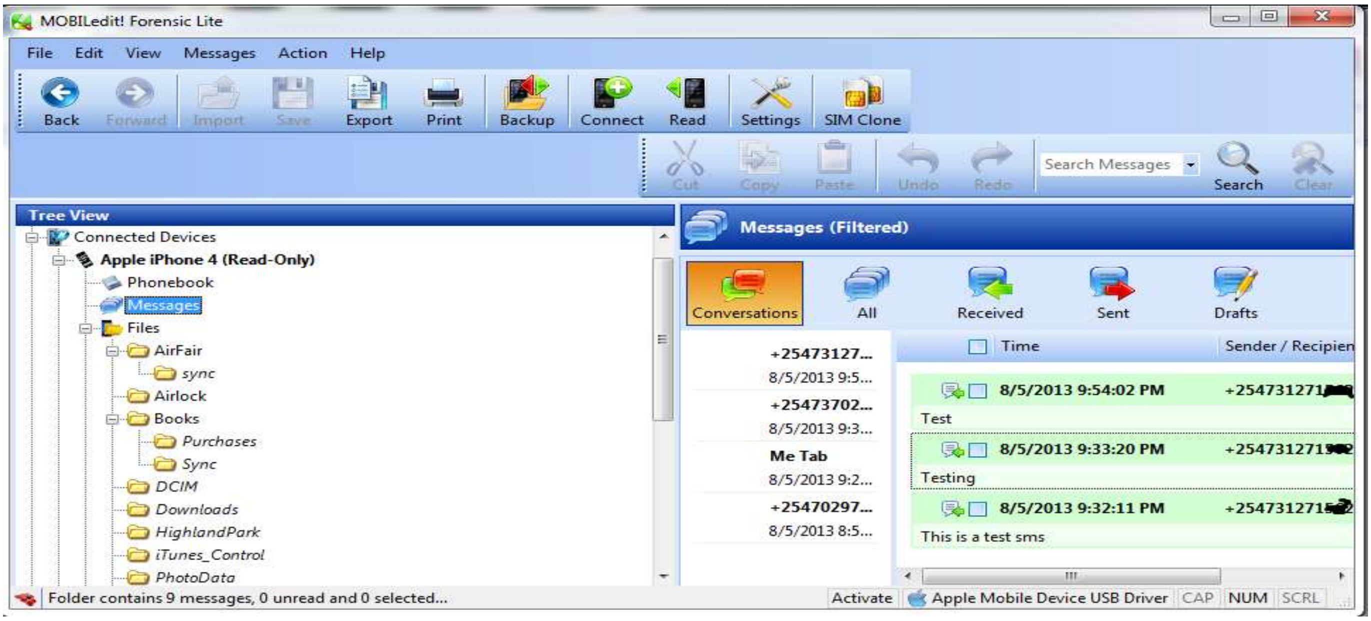
Screenshot 5.9: iPhone details as displayed from MOBILedit forensic Lite

The Screen capture 5.10 displays the received SMS logs as acquired from the iPhone using the MOBILedit forensic Lite;


MOBILedit! Forensic Lite
File Edit View Messages Action Help
Back Forward Import Save Export Print Backup Connect Read Settings SIM Clone
Cut Copy Paste Undo Redo Search Messages Search Clear
Tree View
Start
Connected Devices
Apple iPhone 4 (Read-Only)
Phonebook
Messages
Files
AirFair
Airlock
Books
DCIM
Downloads
HighlandPark
iTunes_Control
PhotoData
Photos
Purchases
Recordings
Safari
Calendar
Notes
Generic ObexDevice (Read-Only)
Phonebook
Cases
Hex Dump
Photo Viewer
Messages (Filtered)
Conversations All Received
Time Sender / Reci
Ready...
Activate Apple Mobile Device USB Driver CAP NUM SCRL

Time	Sender / Reci
8/5/2013 9:54:02 PM	+254731271
Test	
8/5/2013 9:34:39 PM	+254737024
Just tests	
8/5/2013 9:33:20 PM	+254731271
Testing	
8/5/2013 9:32:11 PM	+254731271
This is a test sms	
8/5/2013 9:28:06 PM	Me Tab (+25
Test from Tab	
8/5/2013 9:25:54 PM	Me Tab (+25
Test from Jane tab!	
8/5/2013 9:25:04 PM	+254737024
Hello! Testing...	

Screenshot 5.11 displays Conversation extracts as acquired from the iPhone using the MOBILedit forensic Lite;

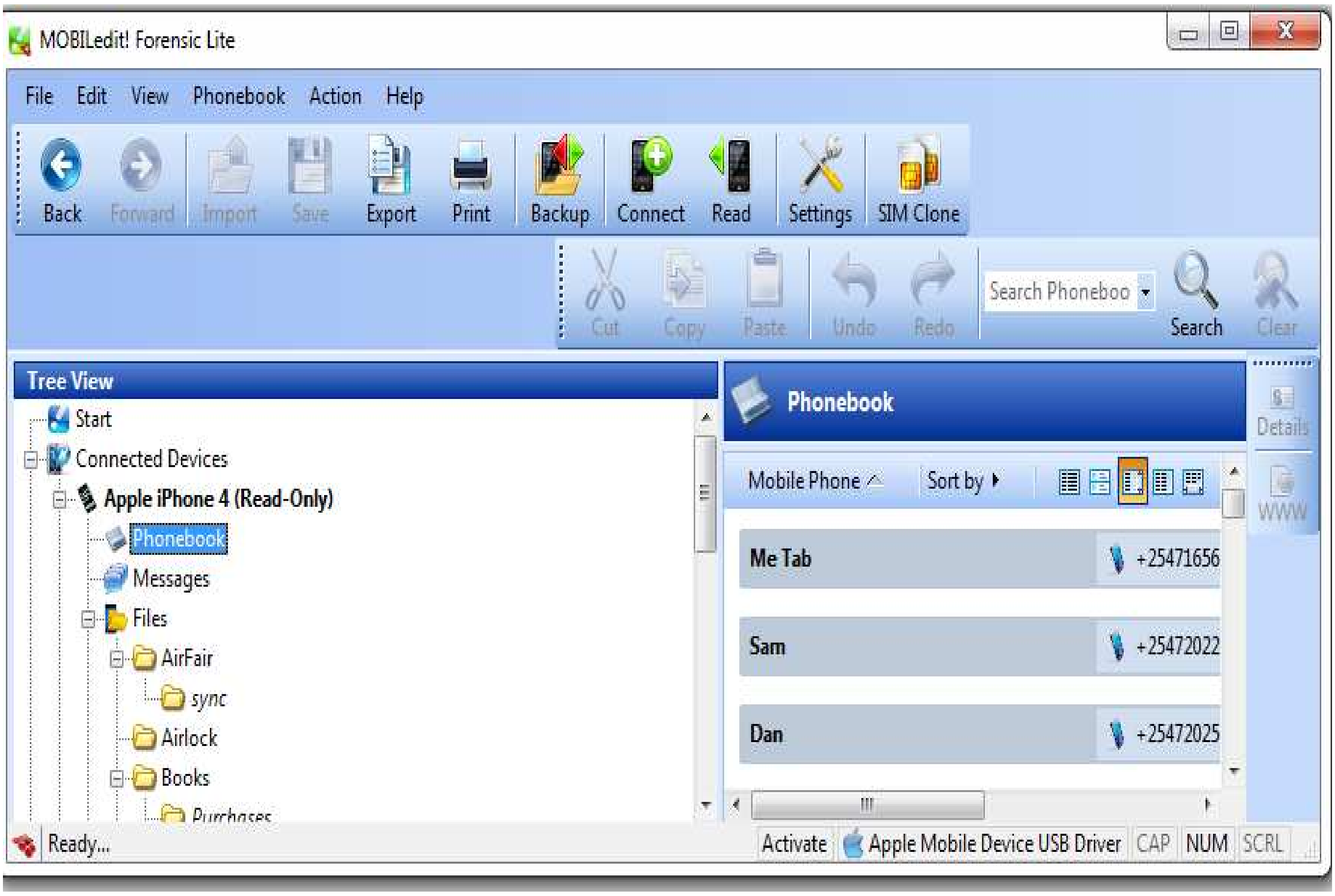

MOBILedit! Forensic Lite
File Edit View Messages Action Help
Back Forward Import Save Export Print Backup Connect Read Settings SIM Clone
Cut Copy Paste Undo Redo Search Messages Search Clear
Tree View
Connected Devices
Apple iPhone 4 (Read-Only)
Phonebook
Messages
Files
AirFair
sync
Airlock
Books
Purchases
Sync
DCIM
Downloads
HighlandPark
iTunes_Control
PhotoData
Messages (Filtered)
Conversations All Received Sent Drafts
Time Sender / Recipien
Activate Apple Mobile Device USB Driver CAP NUM SCRL

+25473127...
8/5/2013 9:5...
+25473702...
8/5/2013 9:3...
Me Tab
8/5/2013 9:2...
+25470297...
8/5/2013 8:5...

Time	Sender / Recipien
8/5/2013 9:54:02 PM	+254731271[redacted]
Test	
8/5/2013 9:33:20 PM	+254731271[redacted]
Testing	
8/5/2013 9:32:11 PM	+254731271[redacted]
This is a test sms	

Folder contains 9 messages, 0 unread and 0 selected...

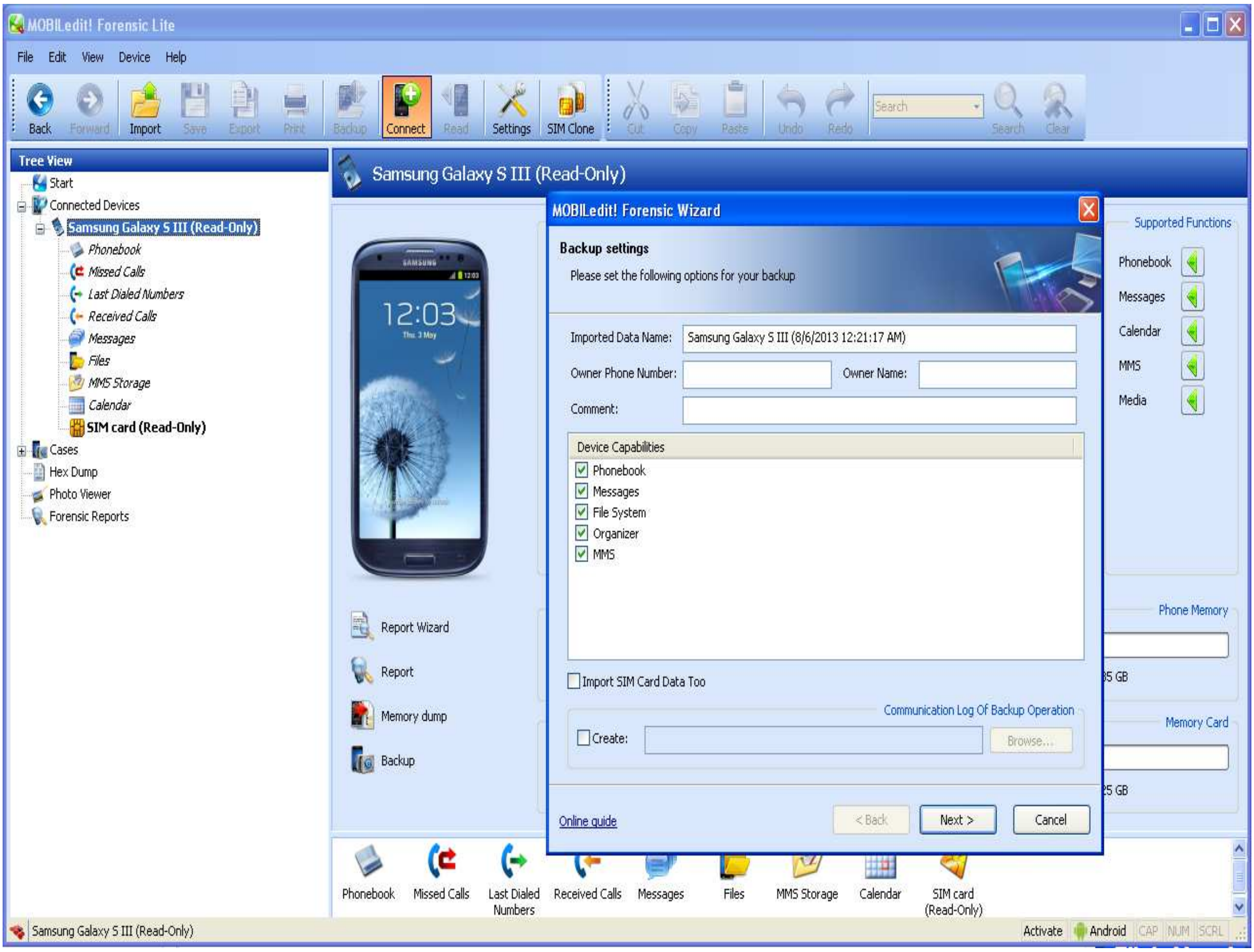
Screenshot 5.11: Sample phone contacts acquired from the iPhone using the MOBILedit forensic Lite



Me Tab	+25471656
Sam	+25472022
Dan	+25472025

Samsung Galaxy SIII Screen shots;

Screenshot 5.12 displays the Samsung Galaxy SIII acquisition process as it runs from MOBILedit forensic Lite;



MOBILedit! Forensic Wizard

Backup settings

Please set the following options for your backup

Imported Data Name: Samsung Galaxy S III (8/6/2013 12:21:17 AM)

Owner Phone Number:

Owner Name:

Comment:

Device Capabilities

☑ Phonebook
☑ Messages
☑ File System
☑ Organizer
☑ MMS

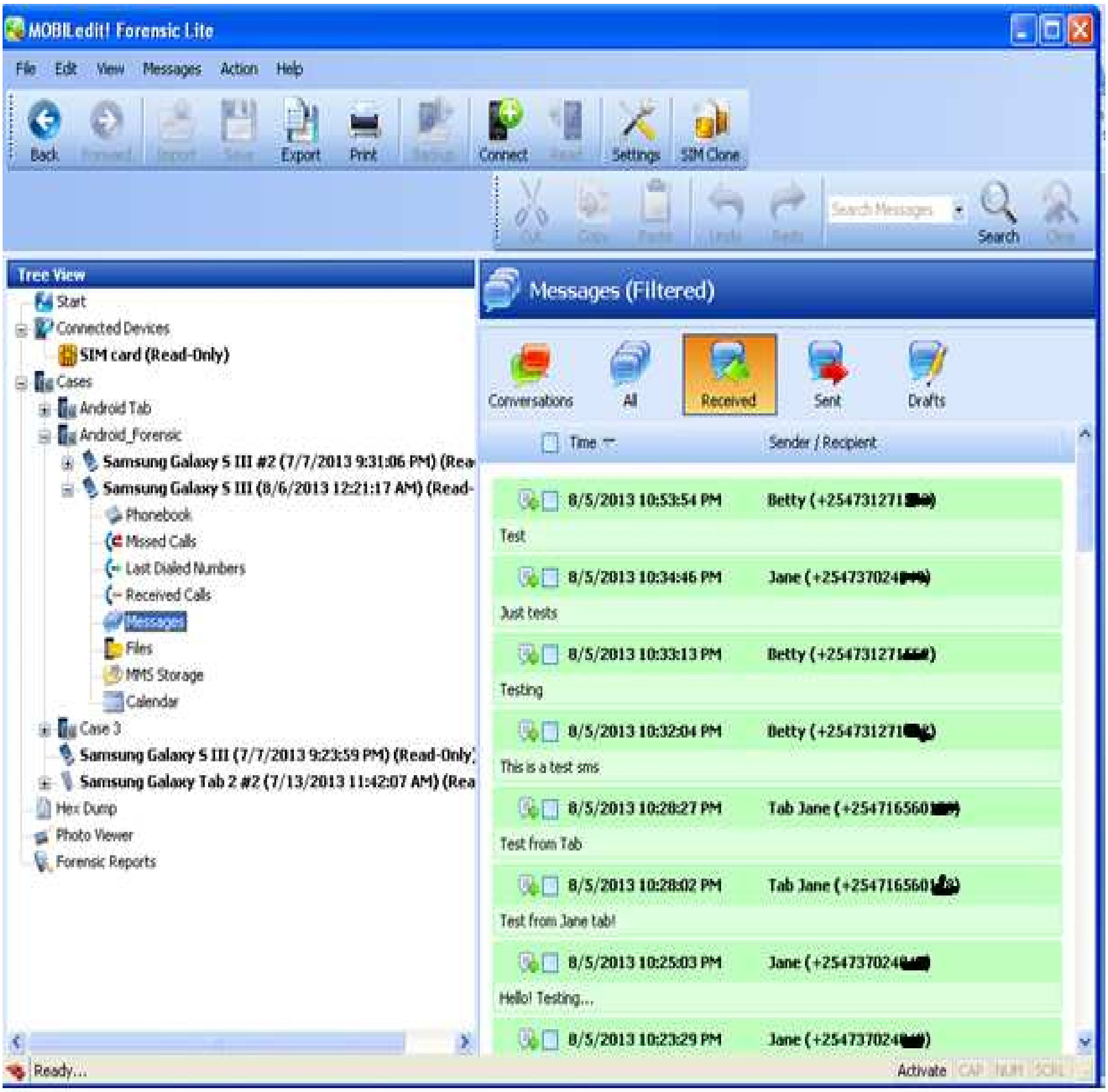
□ Import SIM Card Data Too

Communication Log Of Backup Operation

□ Create:

Screenshot 5.12 displays the Samsung Galaxy SIII data acquisition from MOBILedi forensics Lite

Screenshot 5.13 displays the received SMS logs acquired from the Samsung Galaxy SIII using the MOBILedit forensic Lite



8/5/2013 10:53:54 PM Betty (+254731271[redacted])
Test

8/5/2013 10:34:46 PM Jane (+254737024[redacted])
Just tests

8/5/2013 10:33:13 PM Betty (+25473127[redacted])
Testing

8/5/2013 10:32:04 PM Betty (+254731271[redacted])
This is a test sms

8/5/2013 10:28:27 PM Tab Jane (+254716560[redacted])
Test from Tab

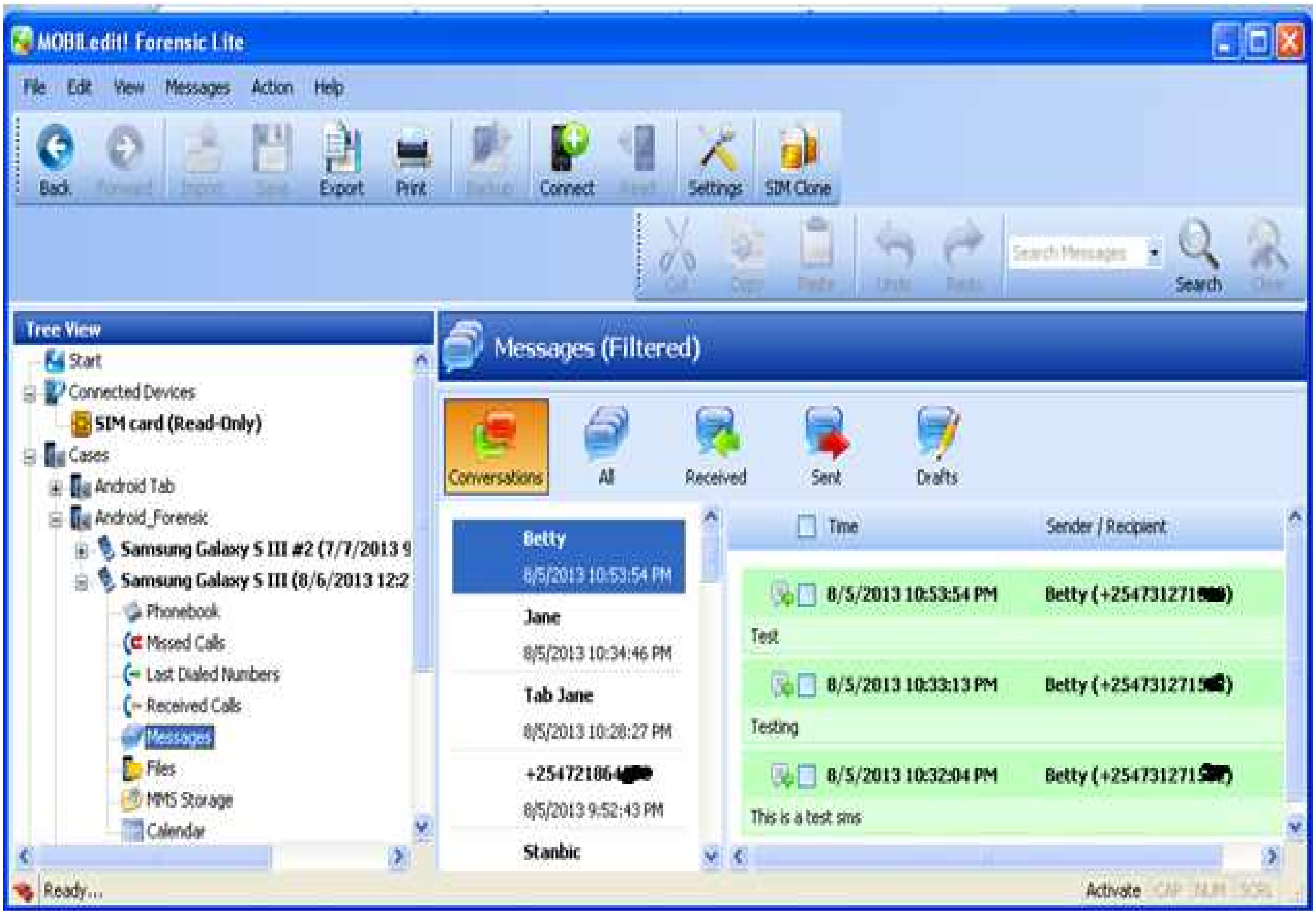
8/5/2013 10:28:02 PM Tab Jane (+254716560[redacted])
Test from Jane tab!

8/5/2013 10:25:03 PM Jane (+254737024[redacted])
Hello! Testing...

8/5/2013 10:23:29 PM Jane (+254737024[redacted])

Screenshot 5.13 displays received SMS logs from the Samsung SIII

The screenshot 5.14 displays the Conversation logs as acquired from the Samsung Galaxy SIII using the MOBILedit forensic Lite;


MOBILedit! Forensic Lite
File Edit View Messages Action Help
Back Forward Import Save Export Print Backup Connect Send Settings SIM Clone
Cut Copy Paste Undo Redo Search Messages Search Clear
Tree View
Start
Connected Devices
SIM card (Read-Only)
Cases
Android Tab
Android_Forensic
Samsung Galaxy S III #2 (7/7/2013 9
Samsung Galaxy S III (8/6/2013 12:2
Phonebook
Missed Calls
Last Dialed Numbers
Received Calls
Messages
Files
MMS Storage
Calendar
Messages (Filtered)
Conversations All Received Sent Drafts
Ready...
Activate CAP NUM SCRL

Betty
8/5/2013 10:53:54 PM

Jane
8/5/2013 10:34:46 PM

Tab Jane
8/5/2013 10:28:27 PM

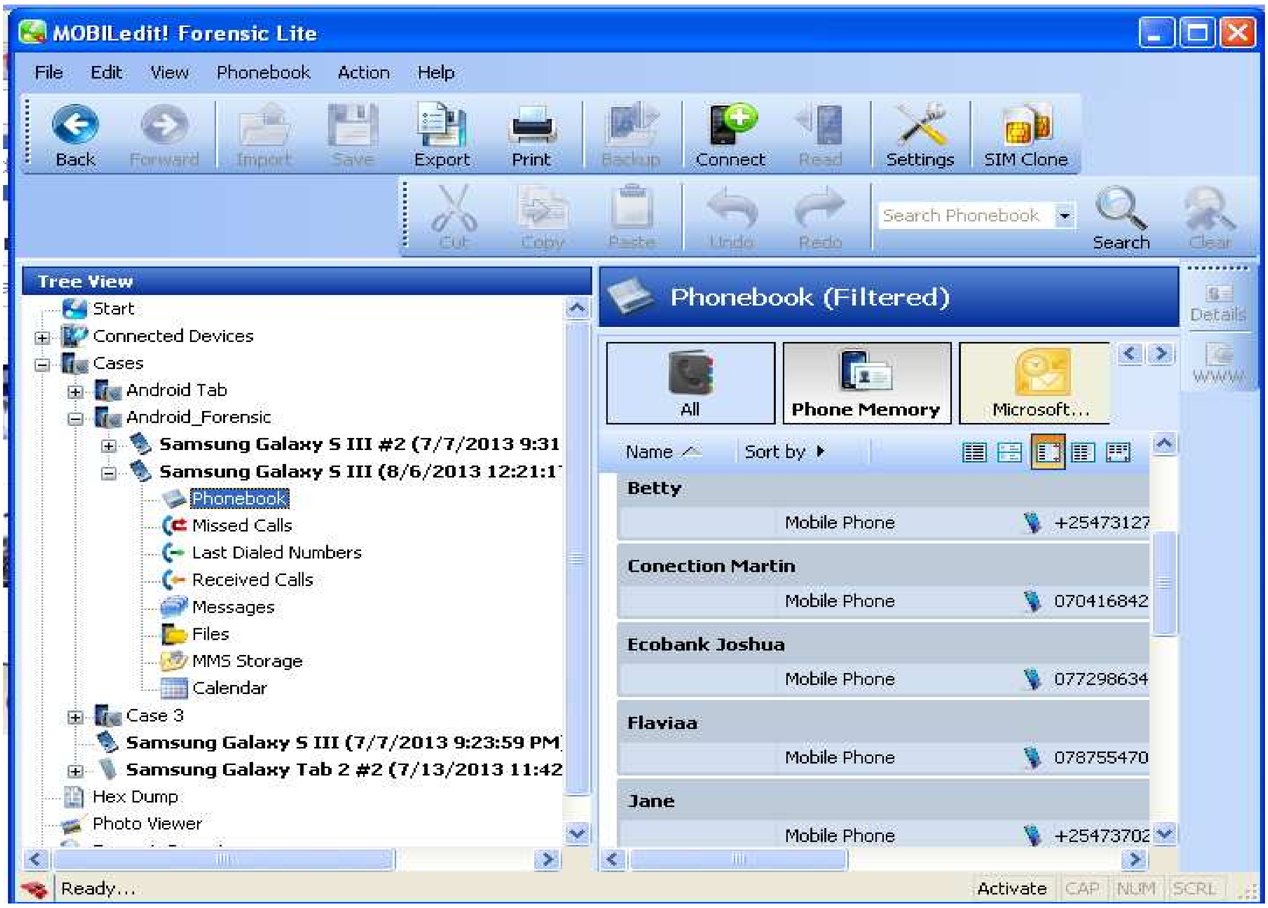
+25472186[redacted]
8/5/2013 9:52:43 PM

Stanbic

□ Time	Sender / Recipient
□ 8/5/2013 10:53:54 PM	Betty (+25473127[redacted])
Test	
□ 8/5/2013 10:33:13 PM	Betty (+254731271[redacted])
Testing	
□ 8/5/2013 10:32:04 PM	Betty (+254731271[redacted])
This is a test sms	

Screenshot 5.14: Displays Conversation logs from Samsung Galaxy S III

Lastly, Screenshot 5.15 displays the sample phone contacts acquired from the Samsung Galaxy SIII using the MOBILedit forensic Lite;



Start
Connected Devices
Cases
Android Tab
Android_Forensic
Samsung Galaxy S III #2 (7/7/2013 9:31
Samsung Galaxy S III (8/6/2013 12:21:1
Phonebook
Missed Calls
Last Dialed Numbers
Received Calls
Messages
Files
MMS Storage
Calendar
Case 3
Samsung Galaxy S III (7/7/2013 9:23:59 PM
Samsung Galaxy Tab 2 #2 (7/13/2013 11:42
Hex Dump
Photo Viewer

Betty
Mobile Phone +25473127

Conection Martin
Mobile Phone 070416842

Ecobank Joshua
Mobile Phone 077298634

Flaviaa
Mobile Phone 078755470

Jane
Mobile Phone +25473702

Screenshot 5.15: Displays Sample phone extracted from Samsung Galaxy S III using MOBILedit forensics lite

Test objective 3: Summary of results:

iii). Testing the extend at which data can be extracted from a range of different phones that have been initially fed with similar data (Using Live Forensics);

The test objective of this objective was achieved. Both the iPhone and the Samsung Galaxy S III were able to acquire the sample test data generated for the tests. The imaged data consisted of all the earlier sample data namely; SMS messages and phone call logs (received calls, missed calls and dialed calls).

CHAPTER SIX: RESULTS, CONCLUSIONS AND RECOMMENDATIONS

6.1 Discussion of Results

This study found out that only few studies have addressed the mobile digital forensic investigation process. These few studies have also been limited to the different OS of the mobile devices, in that they have focused on specific mobile operating systems.

This research focused on the forensic process model of the mobile devices regardless of the OS. The objective of the study was achieved, that is coming up with 'an enhanced hand-held forensics process model which is operating system independent'. The proposed model introduced both Live and Dead forensics while incorporating more interactions between the different processes within the model. Formal modeling through the use of UML was introduced to help provide better understanding to both members and non-members of the digital forensics environment. The proposed mobile forensics process model also integrates physical crime scene investigation aimed at mapping the physical evidence to the digital evidence. This idea is borrowed from (Carrier et al., 2003) model, "Integrated Digital Investigation Model". The goal of the physical crime scene investigation sub-phase is to collect and analyze the physical evidence that would aid in reconstructing the events that took place during the incidence.

In the experimental study conducted, tests were conducted on the new model and the logical image of each of the devices acquired using mobile forensic software tools. On analysis of the devices using the proposed model, data was found which could be linked to the different devices used in the test.

The significance of using this enhanced hand-held forensics device model is to enhance the trustworthiness and acceptability of the evidence in a court of law. The model focuses on ensuring all the evidence collected is admissible and easy to the prosecutor to support the corresponding case.

6.2 Conclusions

The rapid development in technology for Smartphone devices is making the digital forensic of these devices a very complicated task. This development in technology is leading into increasingly more challenges in building and maintaining scientifically sound process models for mobile device investigations. In this research study, a guideline has been laid through the proposed EMFPM to be followed in the digital forensics process for the investigations of the hand-held devices. Moreover, it was found out that the software tools for the mobile device forensics are still limited in terms of feature support and operating system support hence directly impacting on the mobile forensics models; as much as we have good forensics models there is hence need to equally have good mobile forensics software tools.

6.3 Future Work / Research

The model should be improved to fully extend to the virtual environment. As of now the basic mobile cloud data can be captured but there is a need to extend this concept.

Future work could also include location forensics for the suspect through technologies such as the GIS, however development of the relevant forensic tools will play a key role in helping achieve this.

6.4 Recommendations

The mobile forensics tools needs to be improved to enable support for a wide range of OS and features. Some tools are very basic providing very limited functionality which could provide a major setback for a sound mobile forensics process models as these two go hand in hand towards the analysis and ruling of a case.

Lastly, the EMFPM is open to the researchers and digital forensics experts for review and criticisms.

REFERENCES

Ahmed, R. and Dharaskar, R. (2009), “Mobile forensics: An introduction from indian law enforcement perspective,” in Proc. Third International Conference on Information Systems, Technology and Management (ICISTM 2009), 2009, pp. 173–184.

Ankit, A, Megha, G, Saurabh, G & Subhash, G (2011), Systematic Digital Forensic Investigation Model, International Journal of Computer Science and Security, (IJCSS), Volume (5), Issue (1), (2011).

Anup, R (2011), Forensic Investigation Process Model for Windows Mobile Devices. Available: from: < http://www.forensicfocus.com/downloads/windows-mobile-forensic-process model.pdf> - Last accessed on 23 July 2013

April, T & Dampier, D (2010), An Approach for Managing Knowledge in Digital Forensics Examinations, International Journal of Computer Science and Security, (IJCSS), Volume (4): Issue (5), (2010).

Archit, G, Anurag, T, & Ankit, A (2012), Smartphone Forensic Investigation Process Model, International Journal of Computer Science and Security, (IJCSS), Volume (6): Issue (5), (2012).

Baryamureeba, V & Tushabe, F (2004), ‘The Enhanced Digital Investigation Process Model’, in Proceeding of Digital Forensic Research Workshop, Baltimore, MD.

BitPIM forensics software tool, (2013) <www.bitpim.org>

Carrier, B, Spafford, E (2003), Getting Physical with the Investigative Process, International Journal of Digital Evidence, Fall 2003, Volume 2, Issue 2.

Casey, E., Bann, M., & Doyle, J. (2010): Introduction to Windows Mobile Forensics. Digital Investigation Volume 6, Issues 3-4, Pages 136-146

Cellebrite UFED physical analyzer, (2013), <http://www.cellebrite.com>

Electronic Crime Scene Investigation, (2009): An On-the-Scene Reference for First Responder, The National Institute of Justice.

Encase Smartphone Examiner software tool (2013), <http://www.guidancesoftware.com>

FTK MPE (Mobile Phone Examiner) software tool (2013) : <https://www.accessdata.com>

Gregory, E, Forster, A, Heckel, R & Thone, S 2005, ‘Process modeling using UML’ in Process Aware Information Systems, pp 85-117.

Helen A &, Dr Robert A, (2012): iPhone Forensics Digital Fingerprint Analysis, Liverpool John Moore’s University 2012.

Hemendra S, Manoj P, Siddharth S, & Koushel A, (2012), Study on Different Digital Forensics Tools for Mobile Embedded System. National Conference on Security Issue s in Network Technologies (NCSI -2012)

H¨obarth S, and Mayrhofer R, (2011) “A framework for on-device privilege escalation exploit execution on android,” in Proc. IWSSI/SPMU 2011: 3rd International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use, Jun. 2011.

Hoog A, (2011) Android Forensics. Waltham, MA: Syngress-Elsevier, 2011.

lDC, (2013): Press release; Smartphones Expected to Outship Feature Phones for First Time in 2013 : http://www.idc.com/getdoc.jsp?containerId=prUS23982813 - Last accessed 10th June 2013

Kent K, Chevalier S, Grance T and Dang H, (2006) “Guide to Integrating Forensics into Incident Response”, Special Publication 800-86, Computer Security Division Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD, (2006), http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf.

Khawla A, Andrew J & Thomas A, (2011) Guideline for the digital forensic processing of smartphones

Klaver, C. (2010). Windows Mobile Advanced Forensics. Digital Investigation, Volume 6, Issues 3-4, Pages 147-167, May 2010,

Kohn M, Eloff J & Olivier MS, (2008): UML Modelling of Digital Forensic Process Models (DFPMs)

Krueger, C. (2011). Man found guilty of lesser charge in murder recorded on cell phone.

Kubasiak, R, Morrissey, S & Varsalone, J 2009, ‘Macintosh OS X, iPod, and iPhone forensic analysis DVD toolkit’, Burlington, MA: Syngress; 2009.

Lessard, J. & Kessler G, (2010), Android Forensics: Simplifying Cell Phone Examinations

Marwan, A (2006), ‘Mobile Handset Forensic Evidence: a challenge for Law Enforcement’, 4th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia,

MOBILedit Forensics Lite, (2013), available from: http://www.mobiledit.com/

Mobile Forensics definition - http://www.nvdigitalforensics.com – Last accessed 10th April 2013.

Moore, T (2006), ‘The Economics of Digital Forensics’, Fifth Annual Workshop on the Economics and Information Security.

National Institute of Justice, (July 2001), Electronic Crime Scene Investigation. A Guide for First Responders, Available from: http://www.ncjrs.org/pdffiles1/nij/187736.pdf

NIST, (2006): Guide to integrating forensic Techniques into Incident Response. Available at<http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf>

Noora A, Ibrahim B & Andrew M, (2012), Forensic analysis of Social Networking applications on mobile devices. SciVerse ScienceDirect Digital Investigation volume 9 (2012) S24–S33

Oxygen Forensic Suite 2013 Analyst, (2013), <http://www.oxygen-forensic.com>

Panagiotis A, George O & Theo T, (2012), Forensic Analysis of Wireless Networking Evidence of Android Smartphones

Paraben’s Device Seizure, (2013), <http://www.paraben.com>

Process Model definition- http://www.computerforensicsworld.com – Last accessed 10th April 2013

Raghav, S., & Saxena, A. K. (2009), Mobile Forensics: Guidelines and Challenges in Data Preservation and Acquisition. IEEE student Conference on Research and Development (SCOReD 2009), (pp. 5-8), Malaysia

Ramabhadran A (2011), Forensic Investigation Process Model for Windows Mobile Devices. Available:http://www.forensicfocus.com/downloads/windows-mobile-forensic-process model.pdf

Rick A, Wayne J, Nicolas C & Ronan D. (2007), “Cell Phone Forensic tools: An Overview and Analysis”. Internet: http://csrc.nist.gov/publications/nistir/nistir-7250.pdf.

Rogers, K, Goldman, J, Mislan R, Wedge, T & Debrota, S (2006), ‘Computer Forensic Field Triage Process Model’, presented at the Conference on Digital Forensics, Security and Law, pp. 27-40

Sabah A and Bashayer A, (2012): Modeling the Forensics Process, International Journal of Security and Its Applications Vol. 6, No. 4, October, 2012

Schiffman, J. (2010), Blackberry OS Report 2. Retrieved June 24, 2013, from http://www.cse.psu.edu/~enck/cse597as09/ slides/appmodel_blackberry.pdf

Smartphone definition – http://www.techopedia.com/definition/2977/smartphone - Last accessed 10th April 2013.

Solms, V, Lourens, C & Grobler, T 2006, ‘A control framework for digital forensics’ *IFIP 11.9*, 2006

TULP2G mobile forensic software tool, (2013)<http://tulp2g.sourceforge.net/>

Vlachopoulos, K., Magkos, E., & Chrissikopoulos, V. (2012). A Model for Hybrid Evidence Investigation, International Journal of Digital Crime and Forensics (IJDCF), 4(4), 47-62 doi:10.4018/jdcf.2012100104

Xian Y, Lie-Hui J,Hui S, Qing Y, Tie-Ming L (2009), A Process Model for Forensic Analysis of Symbian Smart Phones

Yadav S. (2011), Analysis of Digital Forensic and Investigation VSRD-IJCSIT, Vol. 1 (3), 2011, 171-178

Yates M, (2011): Practical Investigations of Digital Forensics Tools for Mobile Devices

Yunus, Y, Roslan I & Zainuddin, H (2011), Common Phases of Computer Forensics Investigation Models, International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 3, June 2011

Zareen, A., & Baig, S. (2010), Mobile Phone Forensics Challenges, Analysis and Tools Classification. Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE.2010), (pp. 47 –55)

Zdziarski, J 2010, iPhone forensics: recovering evidence, personal data, and corporate assets. Sebastopol, CA: O’Reilly; 2010.