Digital forensic process model for mobile business devices: Smart technologies

PAULA RAYMOND LUTUI

BCS, PGDipComp., MComp. (Hons).

A thesis submitted to
Auckland University of Technology
in fulfilment of the requirements for the degree of
Doctor of Philosophy (PhD)

2015

School of Computer and Mathematical Sciences

Declaration

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person (except where explicitly defined in the acknowledgements), nor material which to a substantial extent has been submitted for the award of any other degree or diploma of a university or other institution of higher learning.

....

Paula Raymond Lutui

Acknowledgements

Nothing makes me happier than the successful completion of this thesis. Therefore, it is with the utmost joy and gratitude that I thank the following people. They dedicated their time, advice and endless support towards the compilation of this thesis. To begin with, I must give thanks to the Heavenly Father for His continuous blessings upon me during this strenuous yet extremely rewarding journey towards effectively completing this study.

I am extremely thankful to my primary supervisor Dr. Brian Cusack whose support has known no bounds throughout this study. He dedicated the same amount of time, effort, patience and hard work into this study as I have and that will never cease to amaze me. Krasie Petrova, your assistance in supporting this work has not gone unnoticed. Thank you. During this study I had the privilege of working together with a colleague but a good friend of mine, Sotharith Tauch, the countless rounds and discussions have been much appreciated.

Reverend Dr. Liufau Vailea Saulala, the president of Christ’s University in Pacific and the Tokaikolo Christian Church, your prayers, support and words of encouragement have been truly appreciated. Last but not least, to my wife and family, I can praise the name of the Lord for having you by my side during the years of my study. I am thankful for the numerous prayers, support and encouragement I have received throughout the years which have motivated me to finish this thesis despite the challenges that I have met along the way.

Abstract

Worldwide usage of mobile SMART devices has been dramatically increased over the past decade. The popularity of these devices has also grown as a result of the increase in terms of their processing power, large storage capacity and large memory. Mobile SMART devices such as SMART phones, tablet, phaplets and Personal Digital Assistants (PDAs) are now very common and very much part of most businesses' network. As a result, these devices hold enormous amounts of both personal and private business data. Consequently, they have become the target for criminals. They have been found to be involved in criminal activities particularly cybercrimes. These devices are often seized as part of a criminal investigation, and this has led to the need to acquire the data contained in these devices. The SMART device data has become potential evidence in criminal cases.

The vital information held by these mobile SMART devices trigger the need for mobile SMART device forensic capability. The primary aim of digital forensic is to identify the digital information and capture all potential evidence in the device, including call logs, phone book data, text messages, and so on. This process is very important therefore, potential evidence must not be altered in the process so it can be admissible in a court of law. This requires following standardised investigation procedures. However, there is currently no standardised digital forensic investigation process model for SMART devices.

Yet, there are a number of digital investigation process models available. However, they were either developed for a specific sub-field such as computer forensics, mobile forensics, and network forensics or, a generic digital forensic investigation model. This study is aimed to fill the gap identified in the literature; there is no investigation process model that can be used on an investigation that involves multi-disciplinary requirements. The question raised here is *"What can be done to improve the effectiveness and efficiency of digital forensic investigation for SMART devices?"* this question will be answered in chapter seven.

This study involves developing of a new digital forensic investigation process model and a framework. To answer the research question and make sure that the new artefact is evaluated and refined to a high standard, the Design

Science (DS) research method is employed to guide the study. DS method defines the processes from identifying and defining of the problem to communicating the findings through scholarly and professional publications. The DS method influences the design of the study and the evaluation methodology employed to evaluate the artefact which is done in the fifth phase of the DS research method.

As a result, this study found that the problem and the gap identified in the literature are real because digital forensics has a complex nature and it needs multi-disciplinary capabilities and abilities. The implication is that for a SMART device – that brings convergence of many segregated areas - investigation knowledge from each of the implicated areas will be required for effective and efficient investigations. As a result, this study found that employing the current investigation process models in an investigation in a multi-disciplinary environment, the effectiveness and efficiency of the investigation is compromised.

The completed study contributes to the body of knowledge in the field of digital forensics when a multi-disciplinary investigation process model is required that will help an investigator in an environment where more than one sub-field of digital forensics is present. The experimental test data was analysed and the results were used to improve the multi-disciplinary model and develop a multi-disciplinary investigation framework that can be continuously improved as technology and devices change. The professional significance is for improvement in the effectiveness and efficiency of digital forensic investigation processes in a multi-disciplinary environment.

Publications

Lutui, R., & Cusack, B. (2015). Improving SMART Phone Investigation Methods. *Digital Forensics: Investigating the Digital World, 1*(22), 44-48.

Lutui, R., & Cusack, B. (2014). Exploring Network Element Vulnerabilities. *Digital Forensics: Investigating the Digital World, 1*(21), 44-48.

Lutui, P. R., & Narayan, S. (2012). TCP/IP Jumbo Frames Network Performance Evaluation on A Test-bed Infrastructure. *International Journal of Wireless and Microwave Technologies (IJWMT), 2*(6), 29-36.

Lutui, R., & Cusack, B. (2014). Up-dating investigation models for smart phone procedures. *Proceedings of the 12th Australian Digital Forensics Conference*. (pp. 53-63). WA: Edith Cowan University.

Lutui, R., & Cusack, B. (2014). Evaluating the security vulnerabilities of the IP6to4 tunnelling mechanism. *Proceedings of the 12th Australian Information Security Management Conference.* WA: Edith Cowan University.

Lutui, R., & Cusack, B. (2013). Including Network Routers In Forensic Investigation. *Proceedings of the 11th Australian Digital Forensics Conference.* WA: Edith Cowan University.

Lutui, P. R., & Narayan, S. (2013). Network Performance Evaluation of Jumbo Frames on a Network. *Proceedings of the 2013 6th International Conference on the Emerging Trends in Engineering and Technology (ICETET)* (pp. 69-72). Nagpur: IEEE.

Lutui, P. R., Narayan, S., Sodhi, S. S., & Vijayakumar, K. J. (2010). Network performance evaluation of routers in IPv4/IPv6 environment. *Proceedings of the 2010 IEEE International Conference on the Wireless Communications, Networking and Information Security (WCNIS)* (pp. 707-710). Beijing: IEEE.

Lutui, P. R., Narayan, S., Vijayakumar, K., & Sodhi, S. (2010). Performance analysis of networks with IPv4 and IPv6. *Proceedings of the 2010 IEEE International Conference on the Computational Intelligence and Computing Research (ICCIC)* (pp. 1-4). Coimbatore: IEEE.

Lutui, P. R., & Narayan, S. (2010). Impact on network performance of jumbo-frames on IPv4/IPv6 network infrastructure: An empirical test-bed analysis. *Proceedings of the 2010 IEEE 4th International Conference on the Internet Multimedia Services Architecture and Application (IMSAA)* (pp. 1-4). Bangalore: IEEE.

Table of Contents

Chapter One - Introduction

Chapter Two - Defining Device And Network Contexts: Literature Review

Chapter Three - Digital Forensic Techniques & Investigation Models: Literature Review

Chapter Four - Methodology

Chapter Five - Findings

Chapter Six - Framework & Best Practice Guidelines For Practitioners

Chapter Seven - Discussions of Findings

Chapter Eight - Conclusion

List of Tables

List of Figures

List of Abbreviations

1G	First Generation
2G	Second Generations
3G	Third Generations
ACL	Asynchronous Connection-Less
ACM	Association for Computing Machinery
ACPO	Association of Chief Police Officers
AP	Access Point
API	Application Programming Interface
APP	Application
ATM	Asynchronous Transfer Mode
AuC	Authentication Centre
AUT	Auckland University of Technology
BP	Beacon Period
BSMAP	Base Station Management Application Part
BSS	Broadcast Satellite Services
CFFTPM	Computer Forensic Field Triage Process Model
C/I	Carrier-to-Interference
CPU	Central Processing Unit
CSA	Cloud Security Alliance
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CUFED	Cellebrite's Universal Forensic Extraction Device
DCF	Distributed Coordination Function
DCSA	Digital crime scene analysis
DFIF	Digital Forensic Investigation Framework
DFRW	Digital Forensics Research Workshop
DNA	Deoxyribonucleic Acid
DoJ	Department of Justice
DS	Design Science
DTAP	Direct Transfer Application Part
ECU	Edith Cowan University
EDA	Exploratory Data Analysis
EIR	Equipment Identity Register

Ext4	Fourth Extended file system
FAT	File Allocation Table
FBI	Federal Bureau of Investigation
FPS	Frames Per Seconds
FSS	Fixed Satellite Services
FTK	Forensic Tool Kit
GB	GigaByte
GCFIM	Generic Computer Forensic Investigation Model
GHz	Giga Hertz
GID	Group Identification
GLONASS	Global Navigation Satellite System
GPS	Global Positioning System
GPU	Graphics Processing Unit
GSM	Global System for Mobile
HBR	Harvard Business Review
HFS	Hierarchical File System
HLR	Home Location Register
HR	High Rate
IaaS	Infrastructure-as-a-Service
ICT	Information and Communication Technologies
IDC	International Data Corporation
IDIP	Integrated digital investigation process model
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IJCSDF	International Journal of Cyber-Security and Digital Forensics
IJRREST	International Journal of Research Review in Engineering Science and Technology
IJS	International Journal of Security
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IOCE	International Organization on Computer Evidence
IoE	Internet of Everything
iOS	iPhone Operating System

IoT	Internet of Things
IP	Internet Protocol
ISO	International Standard Organisation
IT	Information Technology
JSF	Journaling File System
LAN	Local Area Network
LEA	Law Enforcement Agency
LED	Light-Emitting Diode
LLC	Logical Link Control
LOS	Line of Sight
LR	Low Rate
LTE	Long-Term Evolution
MAC	Media Access Control
MAN	Metropolitan Area Network
MCC	Mobile Country Code
MDFIPM	Multi-disciplinary Digital Forensic Investigation Process Model
ME	Mobile Equipment
MEID	Mobile Equipment Identifier
MMS	Multimedia Messaging Service
MNC	Mobile Network Code
MP	MegaPixels
MSC	Mobile Switching Centre
MSS	Mobile Satellite Services
NIJ	National Institute of Justice
NIST	National Institute of Standards and Technology
NLOS	Non-Line of Sight
NTFS	New Technology File System
OHA	Open Handset Alliance
OS	Operating System
OSI	Open Systems Interconnection
PaaS	Platform as a Service
PAN	Personal Area Network
PC	Personal Computer

PDA	Personal Digital Assistants
PhD	Doctor of Philosophy
PIM	Personal Information Management
PIN	Personal Identification Number
PList	Property List
POS	Personal Operating Space
PPI	Pixels Per Inch
PSTN	Public Switched Telephone Networks
QoS	Quality of Service
RAM	Random Access Memory
RAND	Research and Development
RIM	Research in Motion
RTA	Radio Tactics’ Aceso
SaaS	Software as a Service
SAP	Systems, Applications and Products
SAS	Serial Attached SCSI
SCO	Synchronous Connection Oriented
SCSI	Small Computer System Interface
SD	Secure Digital
SIM	Subscriber Identity Module
SMS	Short Message Service
SPN	Service Provider Name
SSL	Secure Socket Layer
SU	Super User
TCP/IP	Transmission Control Protocol/Internet Protocol
TDD	Time Division Duplexing
TDMA	Time Division Multiple Access
TFAT	Transaction-safe FAT
TWGCSI	Technical Working Group on Crime Scene Investigation
UID	Unique Identification
USB	Universal Serial BUS
USIM	Universal Subscriber Identity Module
VLR	Visitor Location Register

VPN	Virtual Private Network
WAN	Wide Area Network
WBAN	Wireless Body Area Network
WCDMA	Wideband Code Division Multiple Access
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WinCE	Windows Embedded Compact
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network

Chapter One

Introduction

1.0 INTRODUCTION

Mobile SMART devices such as SMART phones and Tablets have become an essential part of businesses day to day business processes. The rapid growth within the communication technologies have enabled these mobile SMART devices to have direct connectivity with the organisation's private network and are used to conduct business from anywhere at any time (Alghafli, et al., 2011, p.1).

As a result, organisations are embracing the new development and the use of the mobile SMART technologies as a key component to improve the quality of life, knowledge and international competitiveness (Ogunsola, 2005, p.1). This significant development of the mobile SMART technologies is projected to keep on growing. The enhancement in these devices' features, functionalities and its storage capacity and processing power has justified the global popularity (Azadegan, et al., 2012, p.5254). According to a report developed by Yased working group, the Information and Communication Technologies (ICT) sector contributes to the rise of many innovations that increases the welfare of individuals by affecting the way they conduct business and live their daily lives both directly and indirectly (Özyiğit, et al., 2012, p.12).

Therefore, great amounts of private information are stored in these devices, from contact list in the phone book to photos and videos (Akers, et al., 2011, p.1). Information is stored in these devices include text messages and e-mails, web-browsing history and chat logs, calendar and notes, social networking account and bank account access details, connection details such as cellular network, Wireless Fidelity (Wi-Fi) and Bluetooth, Global Positioning System (GPS) and location details (Alghafli, et al., 2011, p.1). These data in these devices including private information can be exploited. At the same time, it is very inviting for criminals, the power and the abilities and capabilities of these mobile SMART devices to facilitate criminal activities (Casey & Turnbull, 2011, p.1). The information on these devices can be vital in an investigation. Such information can reveal whom criminals have been in contact with, what was the communication about and where they have been. Criminals such as sexual predators may use the phone to make contacts with their victims, exchange photos and videos which will leave a cybertrail of vital information to a forensic investigator (Casey, 2011, p.6).

According to Casey and Turnbull (2011), these devices have been helpful in solving homicide cases; they have been used by terrorists to explore and coordinate their activities. Mobile SMART devices have always been found to be used by members of major gangs to coordinate outside activities and share information even from inside prison (p.1). However, digital forensics is still in its early years and still developing when compared to the traditional forensics methods. As a result, it is critical to make sure that any potential digital evidences recovered from a mobile device can retain. The National Institute of Standards and Technology (NIST) have test digital forensics tools and reviewing digital investigation methods on a regular basis. NIST has published a guide on cell phone forensics with an overview and analysis on cell phone forensics tools to help digital forensics practitioners.

Due to the large number of people using smart phones, there is a growing potential electronic crime. Therefore, the digital forensics technique for SMART phones has become an essential requirement for forensic analyst and security specialists. Investigators found that smart phones are now a significant potential source of digital evidence in criminal investigations (Said, et al., 2011, p.120). Forensics Investigators working for LEA(s) are faced with technical and legal challenges during the course of investigation and collection of digital evidence leading to analysis and presentation at courts of Law (Achi, et al., 2009a, p.283).

Digital forensics is defined as “analytical and investigative techniques used for the preservation, identification, extraction, documentation, analysis and interpretation of digital data which is stored or encoded for evidentiary and/or root cause analysis (von Solms, et al., 2006, p.346). Over the past decade, digital forensics has developed significant importance due to the number of security incidents over this period. According to Valjarevic and Venter (2012), in order for the potential evidences to be admissible in the court of law, digital forensics investigation needs to follow a standardised and formalised method and techniques. However, there is currently no international standardised method for digital forensics investigation processes (Valjarevic & Venter, 2012, p.1).

1.1 MOTIVATION

The primary aim of this study is to review the existing literature in the body of knowledge in relation to digital forensic investigation process models. Also, to review the approaches that is employed to identify the research gap for this study. However, the ultimate goal of this study is to fill a gap and to answer the research question: *"What can be done to improve the effectiveness and efficiency of digital forensic investigation?"*

According to Valjarevic & Venter (2012), there are significant differences within the existing forensic investigation process model. The differences are because of the various number of phases included in each model. The scope of each investigation model is different and the range of similarities of the naming of the phases variable (p.1). Some of the models were designed based on physical crime investigation processes. Similarly, the current digital forensics procedures and principles were primarily developed for desktop computers, not for mobile devices. In the mobile device forensic domain, every investigation is different, in conditions and environment which means that it will be hard to take one procedural approach for every case.

The research question is derived from the literature reviewed in chapters 2 and 3. The existing digital forensic investigation process models were identified and reviewed. The purpose was to identify the scope of each model, determine the digital forensics sub-field that each model is applied to and the outcome will be an input to help answer the research question. Following are the four hypotheses that will be used to test the new digital forensic investigation process model. These hypotheses are assertions derived from the literature and are labelled H1, H2, H3 and H4 as follows. H1: *network forensic investigation process model will be suitable for mobile forensic investigation.* H2: *computer forensic investigation process model will be suitable for cloud forensic investigation.* H3: *a multi-disciplinary digital forensic investigation process model will improve the effectiveness and efficiency of digital forensic investigation.* H4: *a comprehensive framework to guide the investigator on best practices will improve the effectiveness and efficiency of digital forensic investigation.* Further description the four hypotheses are in chapter 4 and section 4.6 together with the research question. The research question will be answered in chapter 7 section 7.1 and also the testing of the four hypotheses.

1.2 THE PROBLEM

Digital forensic investigators are faced with many different investigation process models and frameworks advocating best practices for extracting and preserving potential evidences. SMART technologies have created a problem where an investigator must apply many previously used investigation process models to collect and preserve evidence. The proliferation of investigation process models has arisen from the rapid and continuous innovation of SMART devices, systems and application software for business use. Different proprietary designs, software, and access controls have influenced the adoption of digital forensic investigation models and the continuing revision of best practices.

As mentioned earlier in section 1.0, individuals and businesses are very much dependent on computers, corporate networks, digital mobile devices and the Internet to conduct their daily businesses and tasks. At present, digital mobile devices are now known as SMART devices, this is due to their processing power, memory and storage spaces are very similar to that of a desktop computer. These SMART devices are capable of storing, transmitting and processing large amounts of private and confidential data (Owen & Thomas, 2011, p.25). These SMART devices have become a target for criminals. As a result, it is very important that digital forensic investigators can complete their investigation effectively and efficiently within the constantly changing technological environment. In order for the investigators to achieve best practice goals, the forensic investigation process models require constant updating and adapting to new technologies and challenges.

Digital forensics comprises of various areas that relate to different technologies. There are four main areas and these are Computer forensics, Network forensics, Mobile forensics and Cloud forensics (Lin et al., 2011, p.387). Computer forensics is defined as the use of specialised techniques for recovery, authentication and analysis of electronic data when a case involves issues relating to reconstruction or computer usage, examination of residual data, authentication of data by technical analysis or explanation analysis of technical features of data and computer usage (Hankins et al., 2009, p.233). Network forensics on the other hand is defined as the use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyse and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorised activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities (Palmer & Corporation, 2001, p.27). Mobile phone forensics is defined by the National Institutes of Standards and Technology as, the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods (Jansen & Ayers, 2007, p.6). Final type of digital forensic is known as Cloud forensics. Cloud forensic is defined as a mixture of traditional computer forensics, small-scale digital device forensics and network forensics. Therefore, Cloud forensics is the application of digital forensic science in the cloud computing environments (Ruan et al., 2013, p.38).

As mentioned in the first paragraph, over the past decade, business mobile SMART devices have become a target for criminals. As a result, they have been found to be involved in various digital crimes. Therefore, it is vital for investigators to employ appropriate tools and techniques to help them conduct their investigation effectively and efficiently. At present, the digital forensic investigation process has been motivated by the tools available to the investigator and the technology being investigated (Carrier, 2006, p.1). The process that the investigator employs in conducting the digital forensic investigation is critical to the outcome. An overlooking of one step or interchanging any of the steps may compromise the final results of the investigation (Baryamureeba & Tushabe, 2004, p.1).

This study is going to focus on developing a digital forensic investigation process model that is informed by current investigation process models but updated to represent the current state of the art (Tamilarasi, 2013, p.60). The study is aimed at resolving the most relevant current model (of models) and then developing an investigation process model to help investigators in a case that involves all of the digital forensic sub-fields described earlier in this section. The innovation will be a cross area model that better fits the current SMART technology environment and an investigation framework. The framework is to conceptualise the principles of the phases of the investigation process model developed (Pilli et al., 2010, p.25). Once resolved, the model will be applied in the lab on case scenarios on SMART mobile devices for performance reports and phase stages analysis. The thesis outcome will then be an investigation process model, a framework and best practice guideline. The literature review in chapters 2 and 3 identifies in more detail the problem area, the gap in knowledge base, and the opportunity to innovate and add value.

1.3 THE APPROACH

The approach taken by this study is to start off by synthesising in the work done in chapters two and three. Here the design methodologies of the twelve investigation models are reviewed. In section 4.2, a discussion of the similar research methods in the qualitative method domain is made to identify the best research method for the study. As a result, the Design Science (DS) research method is taken as the most suitable approach for this study. The study is to develop an artefact which is a new digital forensic investigation process model that forensic personnel can use in an investigation that involves more than one digital forensic sub-field.

DS clearly defines the phase entry points. It starts with identifying the problem and defining the problem. Entry point number two focusses on the objectives of the solution. Entry point three focusses on the artefact, the design and the development of the artefact. Entry point four is the client context and this focusses on the demonstration of the solution. DS also provides two extra phases which are designed to guide the evaluation of the artefact and how to communicate the solution. DS also provides an iterative feature which allows the researcher to critically evaluate the solution/artefact developed in the study.

1.4 THE FINDINGS

A detailed discussion of the findings of this study is provided in chapter five. The research findings chapter is designed to report the results of work being performed based on the methodology discussed in chapter four. The initial analysis allows a best guess “STRAW MAN” model to be designed for later testing and improvement. The research findings are divided into four main sections. Section 5.1 shows all the experimental data collected when the STRAW MAN model is applied when investigating the two fictitious case studies explained in chapter four sections 4.4.1 and 4.4.2.

In section 5.2, an explanation of the improvements to the STRAW MAN model is given. Table 4.2 shows the process used to test the performance of the STRAW MAN model. This illustration shows that five reputable organisations in the field of digital forensics have developed standards and principles and these standards and principles will be used to test the STRAW MAN model. This is followed by figure 5.32 showing the new and improved digital forensic investigation model.

The findings confirm that the field of digital forensics has a very complex nature. The literature review identified the gap and shows that the existing investigation process models in the field were either developed for specific sub-field of digital forensics or developed as a generic investigation process model. However, the findings show that the STRAW MAN model does improve the effectiveness and the efficiency of digital investigation processes. Chapter seven provides a detailed discussion of the findings given in chapter five.

1.5 THESIS STRUCTURE

This thesis is divided into eight chapters: The first chapter of the thesis provides an introduction overview. Chapter two is a theoretical review of the literature. This concentrates on the mechanisms of various types of network that a mobile SMART device can access. For instance, the cellular network, private businesses that provide wireless access for these devices and also the services provided in the Cloud. Chapter three provides a review of selected digital forensic investigation process models from the existing models in the literature. These models are selected from the sub-fields that they belong to. For instance, Cloud forensics, Network forensics, Computer forensics, Mobile forensics and a few generic digital forensic models. Chapter four looks at the design of this study by identifying studies and choosing the research methodology that is suitable for the study. This chapter also discusses the problem area identified in the literature. The research question is derived from the literature and a series of hypotheses are given which will be tested in the discussion chapter.

Chapter five gives the findings of the study which leads to Chapter six which has a recommendation of best practice guidelines for digital forensic practitioners developed as part of the deliverable. Chapter seven is a detailed discussion of the findings starting off with the discussion of the criteria used in testing of the hypotheses. This is followed with the discussion of each of the hypotheses tested and the result of the tests. In sub-section 7.1.1 gives the answer of the research question followed by sub-section 7.1.2 discussing the limitations of the study. The chapter finishes off with section 7.2 which provides a conclusion to the discussion. The last chapter of this thesis is the conclusion which is Chapter eight. This chapter provides an overall conclusion for this study and also gives the possibility of future work based on the limitations in this research.

Chapter Two

Defining Device And Network Contexts: Literature Review

2.0 INTRODUCTION

The advancement of digital technologies and the adoption into personal and business uses has provided a context in which investigations for legal purposes may occur. Advancement in the wireless communication domain in particular has greatly enlarged the scope of investigation to include mobile devices, cloud repositories and different types of sensor networks (Kotsopoulos & Stamatiou, 2012, p.927). In this chapter 2 a review of different technical contexts in which a digital investigation may occur is made. To start an explanation is made of the way the literature was selected to justify the inclusions and the possibility that some important references may have been missed or excluded. The following sections respectively review wireless contexts, mobile SMART devices, business network contexts, and cloud environments. The chapter 2 concludes with a link to chapter 3 where specific digital investigation methodologies are reviewed and analysed.

2.1 THE LITERATURE SELECTION

The literature contains a selection of noteworthy academic literature related to mobile business SMART devices and forensic investigation measures. Relevant issues, challenges, techniques and approaches that are present in the literature have been highlighted. As a result, this section is designed to define the approach used to select the literature.

2.1.1 Delphi Method Definition

The study employed the Delphi technique for the literature selection. This technique was a product of the Delphi project by the RAND Corporation in the 1940s. The main objective of this technique is to methodically acquire the most reliable unanimity of opinion of a group of experts (Dalkey & Helmer, 1963). Yet, this technique has proven its popularity in the Information Systems (IS) as a research tool and a methodology to justify literature selection (Okoli & Pawlowski, 2004a, p.15). Delphi method is also known to be a qualitative research technique with quantitative elements.

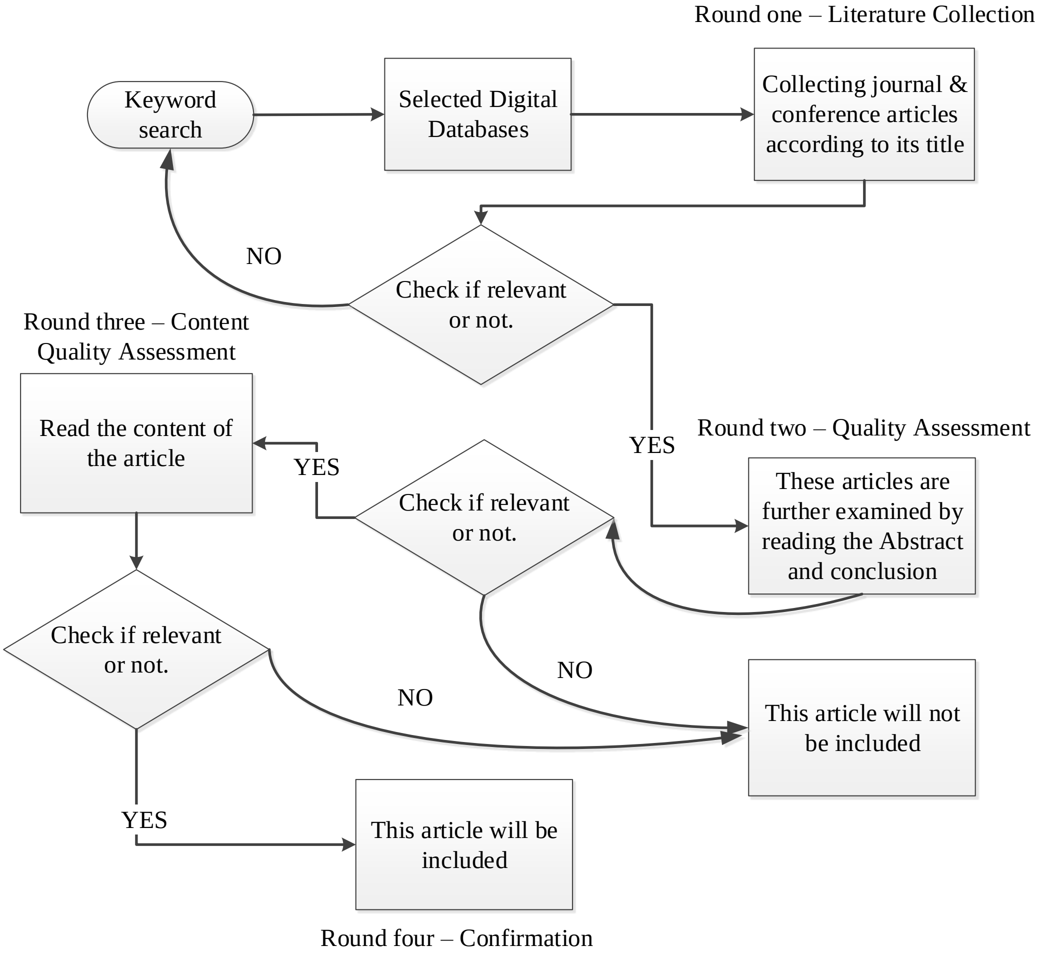

Round one – Literature Collection
Keyword search
Selected Digital Databases
Collecting journal & conference articles according to its title
Check if relevant or not.
NO
YES
Round three – Content Quality Assessment
Read the content of the article
YES
Check if relevant or not.
Round two – Quality Assessment
These articles are further examined by reading the Abstract and conclusion
Check if relevant or not.
NO
NO
This article will not be included
YES
This article will be included
Round four – Confirmation

Figure 2.1: The Delphi technique.

The Delphi technique can also be used as a research methodology. It is used to provoke, filter, and determine the opinions of experts from a given field by engaging a number iterative round (Nworie, 2011, p.24). These are iterative rounds of questions combined to extract the quality and the applicability of the feedback to the topic (Donohoe, et al., 2012, p.39).

The technique can also be used to identify the pros and cons in the field of research in order to measure capability and also to evaluate their possible contributions (Martino, 1976, p.441). However, the process is designed to avoid conflict or unnecessary inducement. As a result, in order to extract the best results, for the selection process, a selection criteria will be developed (Delphi Technique, 2003). Figure 2.1 shows the process steps that this study employs. Figure 2.1

above illustrates in detail the iterative rounds involved in the technique and section 2.1.2, explains in more detail the processes involved in each round and how the criteria are applied to the literature selection.

2.1.2 Define Method Applications

Delphi method is adopted in this chapter to drive the literature selection process. This will ensure the quality of the literature chosen for this study and assist the management of such a large body of knowledge. Electronic libraries hold millions of academic papers and hence selection methods are required to fairly select the ones for closer scrutiny. The design concept of the Delphi method was to elude unnecessary inducement.

A good selection of published literature will provide this research with a solid academic basis. It will also highlight the ideas and findings and also vital in identifying potential issues with plan of the work to do. Therefore, a good search strategy will break the research question into keywords. This is very important because it is often a good idea to think around the topic as much as possible in order to identify useful terms. Your search strategy will break your research question into keywords or phrases. These are very important to a successful search, so it is often a good idea to 'think around' a topic as much as possible to identify useful terms. Some technical terms are spelt different in the United States and the United Kingdom so, it is a good idea to include both spelling in the search (Havard, 2007, p.33). However, selecting keywords is best to use words or phrases that simply and distinctively describe the topic of the research. This can be a very straight forward process and need to think carefully about the keywords that often used to express the ideas for the study (De Montford University, 1999, p.4).

The following steps outline the processes involved and the selection criteria.

Keywords were created according to the topic of this study. The topic is *"Digital forensic process model for mobile business devices: Smart technologies"*. Therefore, the keywords were formulated to cover the following areas: digital forensic, digital forensic investigation process model, smart devices, and within the areas of digital forensic investigation it certainly involves the sub-fields of digital forensics. The queries were performed on these six electronic databases available from the university's e-library website. The following keywords were used: ***Digital forensic, Digital evidence, Digital investigation, Mobile forensic, Cell phone forensic, SMART device, Cloud computing, Cloud forensics, Network forensic.***

There were six main databases selected for the initial search. They were; ***IEEE Xplore, ACM Digital Library, Elsevier, ScienceDirect and SpringerLink.*** These databases were chosen due to their quality of being relevant to the field of Computing, Computer Science, and Computer Engineering. This decision was also validated by an expert. As a result, the expert also point out the (ECU) Edith Cowan University database as they have specialised database on computer security and also on the digital forensic research.

A timeline feature was also defined to limit the publication year range of the query. For this study, the search limit was set to go back as far as the year 2005. In addition to the aforementioned databases, the keywords were also queried on ***Google Scholar.*** Google's ***Specialised Search*** feature was also engaged to configure an ***Alert*** (sent to my gmail account) using the chosen keywords as well. The chosen keywords were also used on the AUT University Library website to get more literature.

The defined selection criterion mentioned above was then applied to the initial search section of the Delphi method illustrated in figure 2.1 in order to initiate the selection process. The first round of the process is designed to process the returned results of the query and round one selection decision will be based solely on the relevancy of the literature title. The defined keywords were also set as an *Alert* on the *specialised search* feature of Google. Google Scholar was also utilised and a lot of significant literature were returned in the queries. The results included Master's and PhD theses from various Universities. The queries also yielded academic literature from journal databases such as the ***International Journal of Cyber-Security and Digital Forensics (IJCSDF)***, the ***Journal of Theoretical and Applied Information Technology***, the ***IJRREST: International Journal of Research Review in Engineering Science and Technology,*** the ***International Journal of Security (IJS),*** the ***International Journal of Computer Theory and Engineering***. All the literature that passed round one will be put through round two.

Round two was designed to process the selected literature based on the quality of the literature abstract and conclusion being directly related the study topic and questions. All the chosen literature that passed round two will put through to the final round for the final process. In the final round, round three, was designed to depict the quality of the literature by processing the whole content of the paper. Round three will finalise the literature selection. Round three will also identify the literature that the whole content is not directly correlated to this study and exclude them from the final result.

2.1.3 Limitations of the Method

The Delphi method is like any other research tool that has advantages and limitations. The advantage of the method is that it allows the researcher to remain focused on the problem. The method also allows the researcher to systematically collect expert opinions that enables the researcher to arrive at an informed decision (Donohoe, et al., 2012, p.39).

However, Franklin & Hart (2007, p.239) argues that the technique was not designed to produce consensus or to be utilised as a mechanism for decision making. According to them, the technique was intended to identify options and suggest alternatives. This will allow the researcher to identify pros and cons within the subject matter. On the other hand, the main limitation of the Delphi technique is directly related to the importance of the questions asked (Franklin & Hart, 2007, p.239). However, Goodman (1987, p.245) rightly explained that, *"a key component of the Delphi method is the development of a valid first round questionnaire."* For the same reason, this study developed the selection criteria at the beginning to eliminate the problem identified by Franklin and Hart (2007).

2.2 WIRELESS BUSINESS INFORMATION SYSTEMS

Various types of technologies are engaged in a wireless communication system. However, looking at the cellular network in particular, the development and the advancement in its technologies over the past 20 years has enabled wireless communication from a range as close as within a meter to as far as millions of kilometres away (Tudzarov & Janevski, 2011, p.112). There are also various types of wireless networks such Personal Area Network (PAN), Local Area Network (LAN), Metropolitan Area Network (MAN) and Wide Area Network (WAN). These various types of networks employ different wireless technologies to make communication possible (Nicopolitidis, et al., 2003, p.299). Another well-known wireless global network that makes international communication possible is the cellular network. The technologies employed by this particular type of network allow communication between mobile devices possible from anywhere at any time (Zheng & Ni, 2006, p.1). The technological innovation in the cellular network over the past 20 years has allowed mobile device developers to develop what is known today as a mobile SMART device (Yates, 2010, p.156).

The first mobile phones' system deployed in the 1980s was known as the first generation; commonly known as 1G. This technology was developed for making phone calls only using the analogue signals. The second generation (2G) technology was deployed in the late 1990s; this allowed the use of digital signals. The users of a 2G enabled mobile device can make not only phone calls but also can send text messages (SMS), multimedia messages (MMS) and also e-mails. Third generation (3G) technologies were deployed around the year 2000 and it allows its users to experience high performance and higher data rates than the 2G (Mshvidobadze, 2012, p.1).

Wireless communication technologies have grown rapidly over the past decade and the Internet technologies have also grown equally. Internet applications can be utilised by a wide range of technologies such as network and computer based technologies. The advancement has brought convenience and efficiency and changed the world into an information oriented society especially in the wireless and mobile communication sphere (Donghyuk, et al., 2008, p.197). The growth enables the introduction of more access devices which entail new security vulnerabilities, incidents and threats to both businesses and private users (Achi, et al., 2009b, p.283). These new vulnerabilities in Wireless networks and access devices have become the main targets for malicious attacks. There has been research and studies conducted in this area in an attempt to prevent or at least deter intruders from hacking the communication system. There are many prevention and detection methods and techniques but criminals and others find a way to break these security mechanisms (Achi, et al., 2009a, p.46).

Various types of Wireless networks and their architectures are discussed in chapter 2, section 2.3.3 and also the mobile devices that utilises those communication networks. It shows how these different types of wireless mobile devices utilise diverse wireless networks, including the cellular network. This enables the anytime, anywhere connectivity while being mobile. In the NIST

Special Publication 800-124, the National Institute of Standards and Technology (NIST) points out that, mobile devices including notebooks and laptops have now become essential tools for commuters and individual users. Thus, there are security implications associated with these devices due to their pervasiveness nature and it is a growing concern among business and individual users (Jansen & Scarfone, 2008, p.1).

Mobile devices are now known as mobile SMART devices due to their advance functionalities. SMART devices have the ability to combine several functions onto one device such as, camera, video, Internet access, calendar, address book and so on. They are running on an operating system like a PC which allows users to install third party applications. Security and privacy protection became a major concern when businesses and private users' realised the amount of private information and data that these SMART devices hold (Lin, et al., 2006, p.386).

SMART devices also have the ability to establish Wi-Fi or Bluetooth connectivity and most of them also have the ability to utilise the cellular network. These devices also support multimedia applications and messaging service also has GPS, gyroscopes, and accelerometer sensors built in. SMART devices advancement and growth in usages and popularity raises a lot of security concerns (Wang, et al., 2012, p.52; Leavitt, 2011, p.11). However, the pervasiveness and ubiquitous nature of these SMART devices increase the complexity of the situation for security experts (Bednar, et al., 2008, p.3).

While business and private users embrace the mobility and advancements of these technologies, criminals and others also find other ways to utilise these devices to conduct illegal activities (Lin, et al., 2011, p.386; Dezfouli, et al., 2012, p.186). As a result, to deal with this emerging and growing new phenomenon, a new field of study and practice known as digital forensics has emerged in both professional and in academics areas (Hankins, et al., 2009, p.230).

2.3 MOBILE SMART DEVICES' OPERATING SYSTEMS

The powers, features and capabilities of the new generation mobile devices play a significant role in digital crimes (Dezfouli, et al., 2012, p.186). In special publication 800-101 released by NIST, they point out that mobile phones in particular, the design keeps changing and is still going through changes as technology improves or new technologies are introduced (Jansen & Ayers, 2007, p.6). Three of the top five operating systems for mobile SMART devices that are currently on the world market with top market share (IDC, 2015, p.1) have been chosen for this section. This section is designed to discuss the security measures of these technologies and also to look at the digital forensic methods and approaches currently employed by investigators.

2.3.1 iOS from Apple.

iOS is the operating system developed by Apple, this operating system runs on their mobile devices such as the iPhones, iPod touch and the iPads. The function of the operating system is to manage the device's hardware and at the same time provides various system applications such as Phone, Mail and Safari for Internet browsing (Apple Developer, 2012, p.7). Apple has an application approval system in place. Every application submitted to Apple's App store will be analysed for security purposes before making it available on the App store for consumer downloads (Banuri, et al., 2012, p.631).

With regards to data security, most organisations allowed their employees to connect their own mobile device to the organisation's network. These devices are used to access e-mails as a result, possibly a considerable amount of data are stored on these devices. Therefore, both business and individual users expect their data to be stored in a secure environment. Apple SMART devices are said to be known for having the ability to secure users' data. These devices have hardware encryption for data stored on the device and data transmissions over the network are also encrypted. However, the hardware encryption on the iPad in particular is enabled by default and users' cannot disable it (Hoog & Strzempka, 2011, p.80). Yet, all the efforts put in by Apple to secure their mobile devices, hackers invented a technique known as jailbreak to access the root of the iOS. This invention bypassed all the security measures of the device and allowed unsigned applications to run on the device and such a security breach is vital information to an investigator (Morrissey, 2010, p.32).

Apple business mobile devices such as iPhone, iPad and iPod touch is different from other mobile devices because, they do not have external storage such as SD Card or USB port. Apple mobile devices have only two partitions, one being the operating system partition and the other is for data. The data partition is where information is located which will assist investigators. Information on the data partition is stored in databases. Apple employed SQLite for these databases and there are applications available such as SQLite database browser to view the data in these databases as illustrated in figure 2.2.

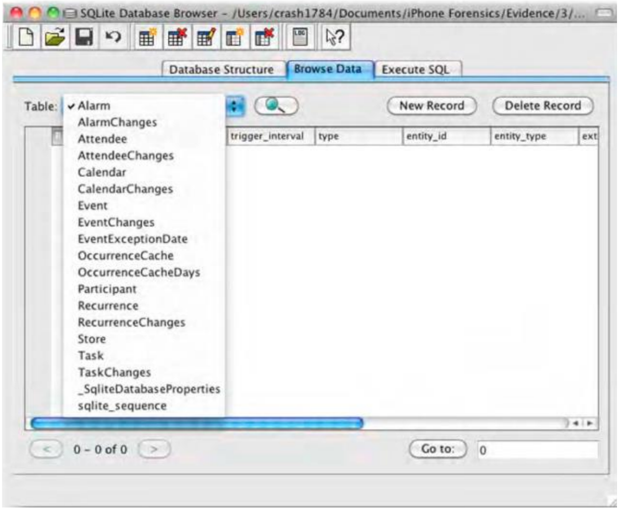


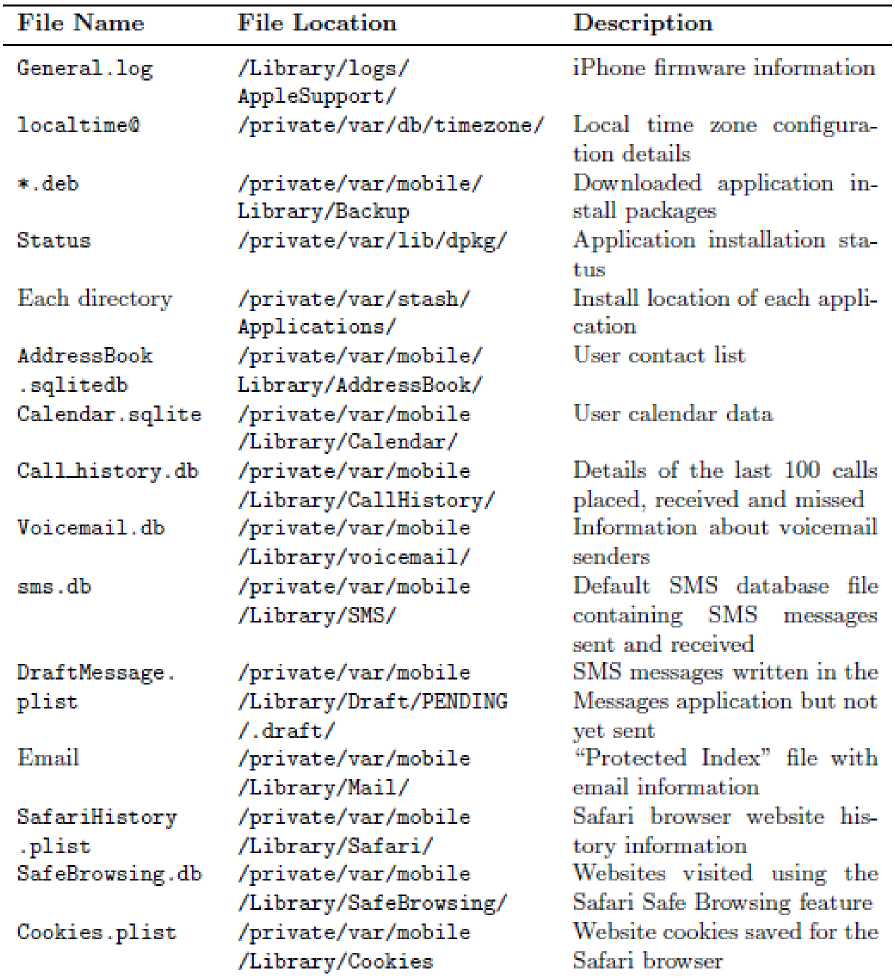
Figure 2.2: SQLite database browser (Morrissey, 2010, p.55).

Following in table 2.1 are the names files and the locations of files that can be found on an Apple mobile device.

These files in table 2.1 showed some of the data that are located in the data partition of an Apple mobile device and their corresponding locations. However, in a case of an investigation, the data has to be extracted from the device for analysis and the extraction conducted in a way that it will not affect the integrity of the data. The procedure is critical to the investigator's findings being admissible in a court of law. For the Apple devices' databases, a study conducted by Said, et al. (2011) shows that three different file formats were obtained from the iPhone (p.121). As a result, three different applications are needed to read these files. These applications are the ***plist Editor***, the ***SQLite Database Browsers*** and the ***Hex Editor Neo***.

Carrying out an investigation on mobile SMART devices differ significantly from conducting an investigation on desktop computers. Therefore, it is recommended for the investigators to document data extraction steps and methods employed. This information can be used to cross validate their results obtained from various tools used. This will improve their understanding of various data types which will also contribute to the accuracy of their investigation (Punja & Mislan, 2008, p.12).

Table 2.1: Potential evidence on iOS filesystem (Cheema, et al., 2014, p.230).



File Name	File Location	Description
General.log	/Library/logs/ AppleSupport/	iPhone firmware information
localtime@	/private/var/db/timezone/	Local time zone configuration details
*.deb	/private/var/mobile/ Library/Backup	Downloaded application install packages
Status	/private/var/lib/dpkg/	Application installation status
Each directory	/private/var/stash/ Applications/	Install location of each application
AddressBook .sqlitedb	/private/var/mobile/ Library/AddressBook/	User contact list
Calendar.sqlite	/private/var/mobile /Library/Calendar/	User calendar data
Call_history.db	/private/var/mobile /Library/CallHistory/	Details of the last 100 calls placed, received and missed
Voicemail.db	/private/var/mobile /Library/voicemail/	Information about voicemail senders
sms.db	/private/var/mobile /Library/SMS/	Default SMS database file containing SMS messages sent and received
DraftMessage. plist	/private/var/mobile /Library/Draft/PENDING /.draft/	SMS messages written in the Messages application but not yet sent
Email	/private/var/mobile /Library/Mail/	"Protected Index" file with email information
SafariHistory .plist	/private/var/mobile /Library/Safari/	Safari browser website history information
SafeBrowsing.db	/private/var/mobile /Library/SafeBrowsing/	Websites visited using the Safari Safe Browsing feature
Cookies.plist	/private/var/mobile /Library/Cookies	Website cookies saved for the Safari browser

2.3.2 ANDROID from Google

The Android operating system was released as open source software. This means that anyone can download the source code and use it to construct a device that runs on Android. However, the open source idea was followed until the version three. The Android versions 3.0 and later are closed source and they are designed to work with specific hardware (Gunasekera, 2012, p.2).

The Android operating system has four components namely the Kernel, the Libraries and Dalvik virtual machine, the Application framework and the Applications as showed in figure 2.3.

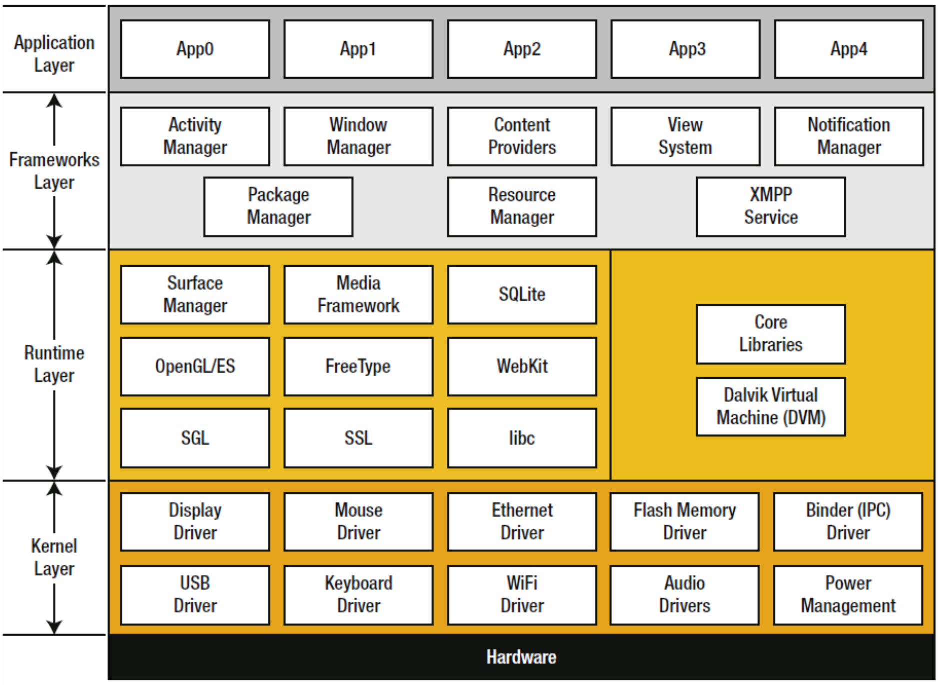


Figure 2.3: Android components (Gunasekera, 2012, p.2).

The Android operating system is running on top of Linux kernel, which is the first layer software that communicates with the hardware. The libraries component is the translator that sits between the kernel and the application framework. The Android operating system employed the Dalvik Virtual Machine as a guest operating system. This was designed specifically to allow devices running on Android to execute applications in a manner that will require less power and memory. The framework layer is designed to provide application developers with the application programming interface (API). This will give the developer access to user interfaces such as text boxes, buttons and other content providers. Lastly is the application component which contains applications that users' use such as contacts, phone, messaging and other applications on the device. The applications in this component will use the API libraries and the Dalvik virtual machine when executing an application (Gunasekera, 2012, p.4).

With regards to security on Android operating system, every application that runs on Android has its own User ID (UID) and Group ID (GID). The Android operating system has a permission system which makes it impossible one application to read and write from another application (Gunasekera, 2012, p.33; Banuri, et al., 2012, p.633). This is very effective especially when each application is executed from different virtual machine. However, the threat is from when applications start using messaging to communicate with each other.

An attacker can exploit this and modify an application by reverse engineering or write their own application and use tools such as *APKTool* for compiling *apk* files. Tools like smali can be used to assemble Dalvik binary files, *dex* files. Android applications have multiple sources unlike applications for Apple devices which are only available from the App store. Android applications can be downloaded from sources such as the Android Market, user developed applications or download from an unauthorised websites (Pocatilu, 2011, p.164). However, Android does not have an application approval system in place like Apple (Banuri, et al., 2012, p.631).

Some security concerns have been observed on Android when installing an application. When installing an application on an Android device, the user has no choice to accept or deny a permission request from the app. The user will have to accept all in order for the installation to be successful. Another concern is due to the fact that Android does not examine the run time behaviour of the applications in order to ensure the integrity of the system (Banuri, et al., 2012, p.633). The file system is Ext4, this is the most and widely utilised Linux based file system. Android adopted Ext4 mainly for its ability to handle large files. Android also employed Journaling File System (JFS) together with ext4 to provide better fault tolerance for its system (Kim, et al., 2012b, p.437). The Android's popularity is still growing as is the use of devices running on Android. However, despite the security concerns and privacy protection issues, users are still using their devices to exchange information, to access the Internet, and online banking as normal. Criminals are continuing to exploit vulnerabilities on these devices (Mahajan, et al., 2013, p.38).

A study conducted by Mahajan, et al., (2013, p.39) showed that a file system extraction from an Android device will acquire all the files and folders on the device's internal memory. However, obtaining file system requires administrative right and the superuser permission on Android is disabled by default. There are procedures that can be followed to enable this account (Albano, et al., 2011a, p.688). It is noted that designers have variable approach to security implementation such as, their moving on from using PIN and pattern drawing to face recognition technology to unlock the device. A digital signature is now used as a proof of identity for application developers (Arabo & El-Mousa, 2012, p.84).

However, similarly to the Apple devices and the method of jailbreaking the iOS, a technique known as rooting is used to bypass Android restrictions. This technique will allow the user to install and execute programs that are not signed for the device. The process involves modifying the system files in order to gain full access therefore such information will be stored on the device (Gomez-Miralles & Arnedo-Moreno, 2011, p.202). Most users do not know that these devices store geographical location data from every application that uses the geolocation feature (Van Hal, 2013, p.1). This information is vital to investigators. Mobile SMART devices are now becoming a significant source of evidence for digital forensic investigators. Mobile SMART devices can contain not only personal data but also information about their employers (Hoog, 2011, p.161).

Android devices nowadays are capable of carring data of at least 16 Gigabytes internally. Android devices are different from the Apple mobile devices because Android devices can also have an external storage space added such as a Secure Digital Card (SD Card). This can add another 16 Gigabytes or more of storage space to the device (Hoog, 2011, p.169). There are five methods of storing data on an Android device's internal NAND memory or external SD Card. The Android five methods of data storage are shared preferences, internal storage, external storage, SQLite and Network. Android devices are known to conduct forensic analysis on them without having an impact on the device as oppose to an analysis conducted on a desktop computer. There are parts of the storage space on an Android device that cannot be easily obtained data from, if the device's power is on, a shutdown and power on again will change the state of the device (Hoog, 2011, p.107).

A study conducted by Grispos, et al. (2013) showed that data deleted by the user or as a result of clearing the applications' cache can be found. On an Android device, Android stored these deleted data on the device itself or transferred to the SD Card. They also found that powering off and on of the Android device has no effect on data recovered from the device (p.4915).

2.3.3 WINDOWS for Mobile from Microsoft

Windows mobile is a platform for mobile devices from Microsoft designed based of the Windows CE versions 5.0. Windows CE also known as WinCE is said to be an integrated OS that was designed to be a foundation for embedded devices. The

Windows mobile OS was optimised especially for devices with minimal processing power, memory and storage spaces (Savoldi, et al., 2009, p.547). With regards to Windows mobile development language, this is different to that of Android and iOS. Windows mobile is based on the .NET using either C# or VisualBasic. Windows mobile OS is a closed platform like the iOS and Android version 3.4 and later. Not only that but, these three mobile platforms also differ in their APIs in terms of user interface and application life cycle. Similarly to the Android OS, Windows mobile also execute its applications on a virtual environment (Puder & Antebi, 2013, p.).

Windows mobile design incorporate sophisticated security system aiming to protect the communication between the device and corporate networks. The system will also provide safeguard for the device itself from running malicious code which also help in securing communications. In terms of securing communications, Windows mobile employed digital certificates for validating user's identity and Secure Socket Layer (SSL) to establish the connection with corporate network. With regards to data encryption, Windows mobile provides cryptographic services to encrypt data for internal and external storage. It also employs hashing to ensure the integrity of the data. Windows mobile also provides support for VPN connections and Wi-Fi encryption as well (Microsoft, 2007, p.4).

Similarly to Apple's app store for its mobile devices, Microsoft has the Widows phone market place as the single online distribution centre for Windows mobile applications. Windows phone market place is designed to provide a centralised approval mechanism to verify the application developer's identity and to avoid software piracy. This is done by issuing every application that is submitted to Windows phone market place with a license. Every application submitted to the Windows Phone market place, will be tested for malware, the application is free of security-critical code. Application execution on a Windows mobile device has the same concept as application execution on an Android device. Every application is launch from its own isolated environment known as sandbox. This is done to avoid the applications from talking to each other and only communicate with services offered by the OS using a well-defined standard mechanism (Lee & Chuvyrov, 2012, p.479).

Microsoft used a variation of its File Allocation Table (FAT) file system known as Transaction-safe FAT (TFAT) on their OS for mobile devices. TFAT is designed to provide recovery features in the case of unexpected device shutdown. Figure 2.4 shows the hierarchy of the TFAT file system which looks very similar the Windows desktop OS (Casey, et al., 2010, p.137).

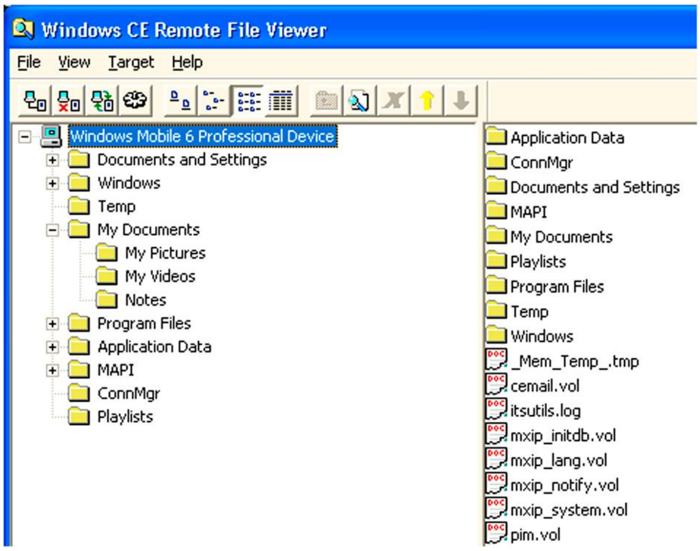
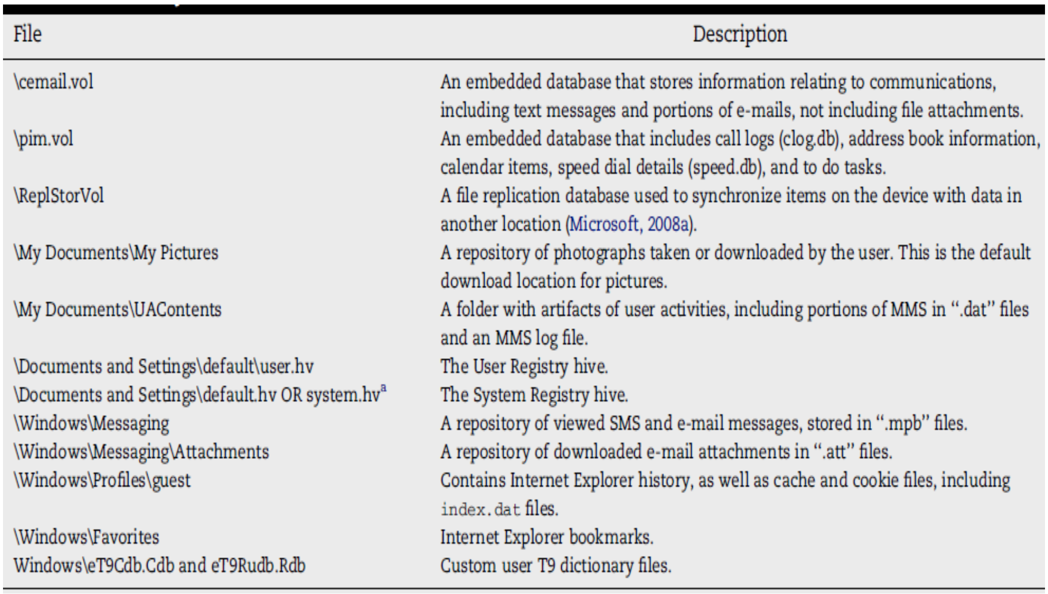


Figure 2.4: TFAT file system (Casey, et al., 2010, p.137).

Similarly to the Microsoft Windows desktop computer's OS, user's files, photos and videos are stored in the "My Documents" folder. Table 2.2 provides some more useful sources of evidence on a Windows mobile device. However, some files that hold user activities are locked by the OS which makes it hard for investigators to extract from the device (Casey, et al., 2010, p.138).

Microsoft shifted the same hive-based registry concept from their Windows desktop OS over to the Windows mobile OS. On a Windows mobile, both the device's and user's configurations are stored in the registry. This can be found in three different files for instance, the "HKEY_LOCAL_MACHINE (HKLM), HKEY_CLASSES_ROOT and HKEY_USERS" holds all the keys that are needed for initialisation of all drivers that control the media during the boot process. All these keys can be found in a file called \boot.hv (Rehault, 2010, p.41).

Table 2.2: Useful sources of evidence on TFAT system (Casey, et al., 2010, p.137).



File	Description
\cemail.vol	An embedded database that stores information relating to communications, including text messages and portions of e-mails, not including file attachments.
\pim.vol	An embedded database that includes call logs (clog.db), address book information, calendar items, speed dial details (speed.db), and to do tasks.
\ReplStorVol	A file replication database used to synchronize items on the device with data in another location (Microsoft, 2008a).
\My Documents\My Pictures	A repository of photographs taken or downloaded by the user. This is the default download location for pictures.
\My Documents\UAContents	A folder with artifacts of user activities, including portions of MMS in ".dat" files and an MMS log file.
\Documents and Settings\default\user.hv	The User Registry hive.
\Documents and Settings\default.hv OR system.hv[a]	The System Registry hive.
\Windows\Messaging	A repository of viewed SMS and e-mail messages, stored in ".mpb" files.
\Windows\Messaging\Attachments	A repository of downloaded e-mail attachments in ".att" files.
\Windows\Profiles\guest	Contains Internet Explorer history, as well as cache and cookie files, including index.dat files.
\Windows\Favorites	Internet Explorer bookmarks.
Windows\eT9Cdb.Cdb and eT9Rudb.Rdb	Custom user T9 dictionary files.

2.4 MOBILE SMART DEVICES

The cellular network deployment of the third generation system enabled the mobile device developers to start developing what is known today as mobile SMART devices. These devices provide its users with more and enhanced processing power and more storage spaces (Cinque, et al., 2007, p.586). Section 2.4.1 will provide more a detailed definition of mobile SMART devices. The purpose of section 2.4 is to define the device and the technical context.

2.4.1 Definitions

A mobile device with a subscriber identity module (SIM) card alongside being controlled by the network provider is defined as a mobile phone. These phones come with basic functionalities and such as, send text messages. These phones are known as *feature phones* and are running on proprietary operating system which is embedded to the device. Not only that, but their functionalities cannot be extended by third party applications (Becher, et al., 2011, p.97).

On the other hand, the term SMART phones is commonly used among the research community and adopted by the industry to describe the modernistic mobile device. These SMART devices also require SIM or USIM (universal subscriber identity module) card as well as, they also run on proprietary operating system. Yet, their functionality can be extended by third party applications which differentiate a SMART device from its predecessor (Theoharidou, et al., 2012, p.7). The SMART phone's operating system allows the installation of third party applications and this makes it more complex than an embedded operating system in feature phones (Mohtasebi & Dehghantanha, 2013, p.352). Mobile SMART devices also have increasing storage capacity and processing power (Azadegan, et al., 2012, p.5424).

It is now becoming harder and harder to distinguish between mobile SMART devices and desktop computers. Modern SMART devices' processing power, storage capacity, memory and functionalities are more like personal computers (Derr, 2007, p.1). SMART devices also support various applications such as web browsers, e-mail clients, global positioning system (GPS) and navigation systems. Large organisations developed their own specialised business applications these days especially for mobile SMART devices such as universities, banks, social networking sites (Albano, et al., 2011, p.685). All the facts presented in this section with regards to mobile SMART devices are responsible for the rapid growth in the demands for these devices; especially the fact that these devices can be used anywhere at any time. These devices are also referred to as the first true ubiquitous computer (Ballagas, et al., 2006, p.70).

2.4.2 Business Usages of SMART Devices

Gartner, Inc. conducted a study that showed in 2013 a worldwide figure of 2.4 billion units which is an increase of 9% from the year 2012 of device shipment. Figure 2.5 represents combined total shipment for devices such as Smartphones, tablets and PCs however, for tablets alone a total of 197 million units in 2013 which is a 69.8% increase from 2012 shipments. The report also shows a 7.6% decline in the Desktop computers and notebooks market. These SMART devices are getting more affordable than ever but, users are now addicted to the applications available on these devices. The devices' ability to backup and update to and from the cloud, and the variety of devices' physical styles available to choose from seems to be the main factor behind the increase in demands (Gartner, 2013). With regards to Internet usage, according to Smart Insights analysts, their forecast shows that by the year 2014, mobile devices will be the preferred device for Internet users rather than desktop computers (Bosomworth, 2013).

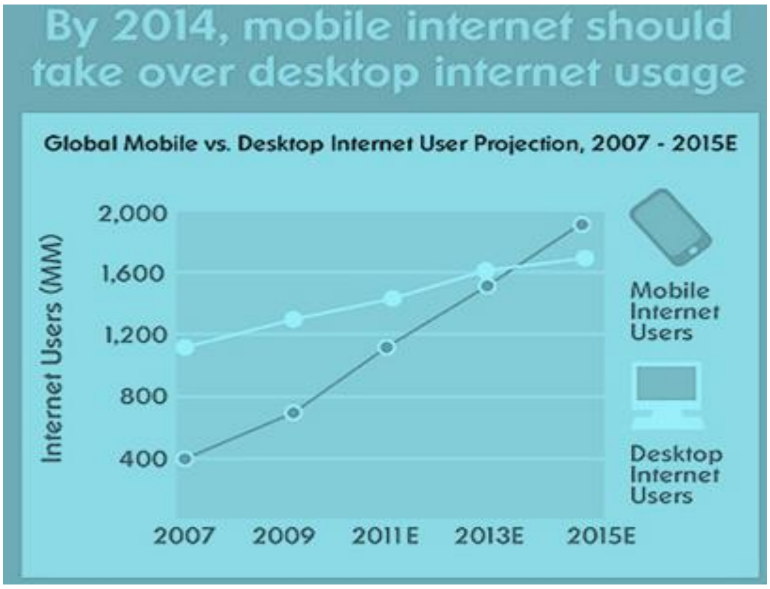


Figure 2.5: Mobile vs. Desktop Internet user projection (Bosomworth, 2013, p. 22).

There are seven reasons defined by the Harvard Business Review report that motivates Smartphone users to conduct daily businesses from their SMART devices. In a business environment, planning and scheduling is very important. *Discovery* and last minute research for answers, productivity in terms of *retrieving* customer information in real time. These devices allow business commuters to access a company database and retrieve the required information about a customer or products as needed. They can *manage finances*, check and *update appointments.* Business people on the road are very busy people, and with the help of these SMART devices they can do their *shopping online.* Not only that, they also have time to *check comments and post updates* on social media marketing sites. They also *spend a little time for themselves* and update their own social networking sites (HBR, 2013).

It is evident that SMART devices are more and more integrated in to businesses' networks. Large organisations are allowing their employees to obtain mobile devices these days because they have the ability to improve productivity (Derr, 2007, p.1). The Systems, Applications and Products in Data Processing (SAP), a multinational business software company has developed a mobile application known as *Business One Software.* This will allow SMART device users to remotely access accounting, controlling, cost accounting, banking functions (Foltin, 2012, p.31). Universities have developed a database management system in order to manage access from students' SMART devices. Students can use their SMART devices such as iPod, iPad and Smartphones to interact with their lecturers. They can access lecture materials, respond to a question posted by the lecturer, even answer a multiple choice test (Lu, et al., 2012, p.1).

As discussed earlier in this section, the technological advancement of the mobile SMART devices evolves very rapidly. As a result, its influence on consumers' behaviour is also evident in the education, marketing and other business activities (Aldhaban, 2012, p.4). On the other hand, great concern is increasing as well. This is because these devices have been found to be involved in criminal activities (Said, et al., 2011, p.120). Criminals have found the advancement of these mobile SMART devices very useful as well.

2.4.3 The Business Systems

This section is intended to explore how today's mobile SMART devices interact with businesses networks. "Consumerisation of IT" is a phrase used to refer to the trend of developing mobile phones now for consumers not for businesses. Even though consumers are buying the device and still used for business purposes. As a result, Smartphones are used far more than just texting, phone calls and sending emails. For instance, the extensive used of the device's camera for taking pictures and videos for business purposes. The amount of audio recording and note taking done on the device is implausible (Thakur, et al., 2011, p.1514).

With the advancement of the mobile technologies, new business opportunities emerged in the mobile communication market. For instance, businesses are now pushing their advertisement on to mobile devices as their new avenue of gaining new businesses (Peng-Ting, et al., 2009, p.625). Mobile devices with the ability to access the Internet are now the common Internet access device. In the mobile device arena, a shift is noticeable from voice to data transmission (Eul, 2010, p.1).

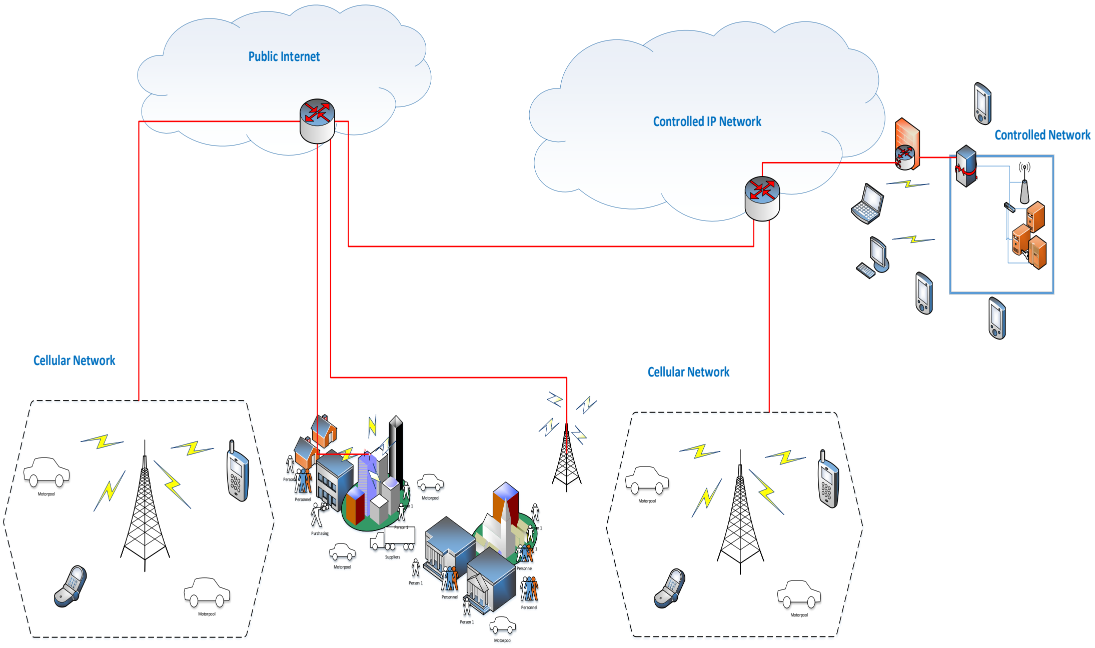


Figure 2.6: Illustrations of Wireless Business Systems.

One of the business mobile SMART device's advantages is the fact that it can connect to the network from anywhere. These devices can connect via the cellular network or wireless fidelity (Wi-Fi). The cellular network enables pervasive connectivity while Wi-Fi can be found in places like restaurants, airport, hotels and motels to name a few. Some businesses such as cafes, restaurants provide free Wi-Fi connections for their customers as part of their service (Wright, 2009, p.1177).

2.4.4 The Device's Hardware

With regards to mobile phones, over the past twenty years these devices have demonstrated a major development in terms of technologies. Mobile phone evolved from being a simple device for voice communication only into Smartphones. A device that can provide innovative services such as Internet access from anywhere at any time, GPS and maps, multimedia streaming at high data rate connectivity just to name a few (Perrucci, et al., 2011, p.1).

Following in figure 2.7 illustrates the hardware of a digital mobile SMART phone which in this case is an iPhone 5. Figure 2.7 also labels all visible external parts of the device and also the default software that come with the device.

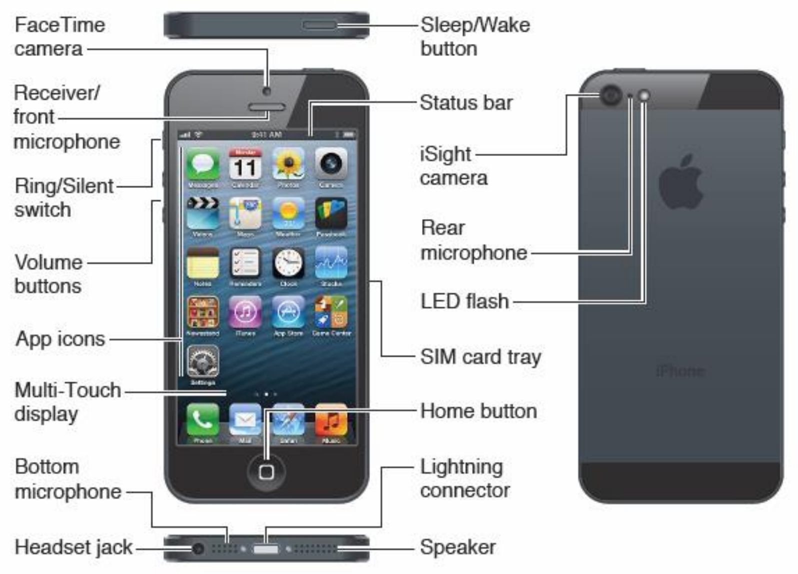


Figure 2.7: iPhone 5 overview (Apple.Inc., 2013, p.7).

According to Apple Inc., the camera can be used to take still pictures at 8 megapixels (MP) and also video footage at 1.2 megapixels (MP) 1080p HD video recording at 30 frames per seconds (fps). The same camera can also be used for video calling, the flash light comes in the LED (light-emitting diode) technology (Apple.Inc., 2013, p.74).

The display on the iPhone 5 in particular adopted the Retina display technology. It has 1136-by-640-pixel resolution at 326 ppi (pixels per inch) with 800:1 contrast ratio (typical). In terms of networking, this Smartphone supports both GSM and WCDMA systems on 3G and LTE network. On a wireless network, it supports 802.11a/b/g/n Wi-Fi however; on an 802.11n connection it can support both 2.4GHz and 5GHz frequency. In terms of the Bluetooth wireless technology, this Smartphone come with the version 4 which has low energy and high speed technology and the range can be up to 100 meters (Apple.Inc., 2013).

This Smartphone also comes with GPS (Global positioning system) and GLONASS (Global navigation satellite system) (Apple Inc., 2013). Three Smartphones, the Motorola Droid X, iPhone 4 and the Galaxy S were employed in a study where their GPS systems were compared. This study concluded that 95% accuracy on all of the three devices when they are within 10 meters of the tracking target (Menard, et al., 2011, p.989). Figure 2.7 also showed a connector known as the Lightning connector, this is the new connector used for charging the device which is different from the usual 30-pin to USB connector (Apple.Inc., 2013, p.13).

Taking a look inside the device, these SMART devices are battery powered. The battery on these devices employed lithium-ion technology (Perrucci, et al., 2011, p.1). Figure 2.8 following show the iPhone 5 battery. According to Brett Hartt, the iPhone 5 battery has a larger capacity than the iPhone 4s. Larger battery capacity means longer talk and standby time. In this study, the author found that iPhone 5 battery has 3.8V - 5.45Wh - 1440mAh. This device has up to 8 hours of talk time on 3G and a standby time of up to 225 hours (Hartt, 2012, p.10).

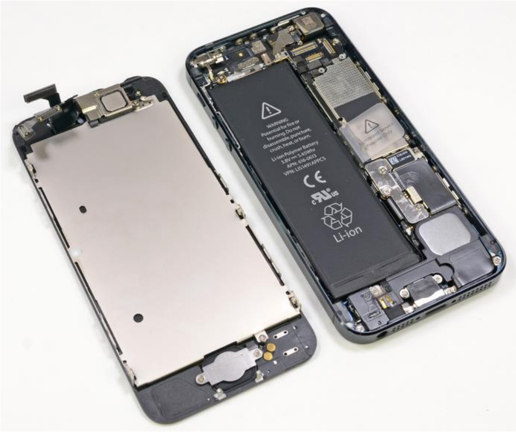


Figure 2.8: iPhone lithium-ion battery (Hartt, 2012, p.10).

However, the Samsung Galaxy S III battery has the same voltage as the iPhone 5 but with more power. It shows 3.8V - 7.98Wh - 2100mAh which has up to 11 hours 40 minutes talk time on 3G and up to 790 hours on standby (Hartt, 2012, p.10). Every SMART device has a processor which is the engine of the device. The iPhone 5 was released with a new processor chip from Apple, the A6 processor. The A6 chip is considered to be 22 percent smaller the A5 chip in the iPhone 4s. The A6 chip has two CPU which double the graphics performance and still used less energy (Gizmodo, 2012).

Following in figure 2.9 illustrates the new A6 chip processor in the iPhone 5. The fact that A6 chip is a dual core processor but it is 22 percent smaller than the A5 is a power saving from the iPhone 5. These authors conducted an analysis study of the power characteristics of the Smartphones. The findings showed that the CPU is one of the hardware components that consume most power (Jung, et al., 2012, p.356).

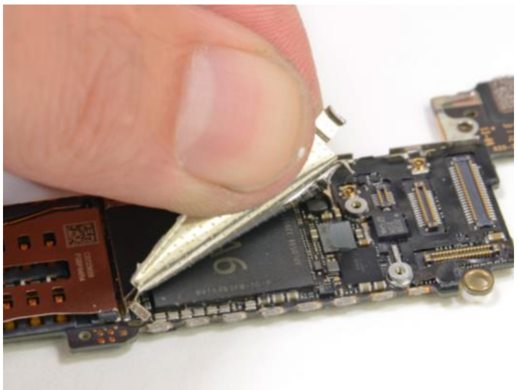


Figure 2.9: iPhone 5 A6 processor (Hartt, 2012, p.10).

Every SMART device requires a CPU even though they will be different in shape, size, speed and processing power. For instance, iPhone 5 A6 processor was a Dual-core 1.3 GHz processor while the Samsung S3 came out with a Quad-core 1.4 GHz processor (Engadget Mobile, 2012, p.1). On the high end embedded systems such as the mobile SMART devices, the design is likely to adopt a single chip design. This means that the CPU and the graphics processing unit (GPU) will be on a single chip (Keckler, et al., 2011, p.8). This is to meet the users' requirements for more memory performance and capacity when they use graphics and multimedia applications (Kim, et al., 2012a, p.888).

The memory is another important aspect of the internal parts of a SMART device. There are two types of memory in these devices. One is volatile and the other is non-volatile. The main difference by these two types of memory is that, the volatile memory will lose everything on it when the power is off. The non-volatile memory stores the data even when the power is off. The volatile memory is only used by the programmes and applications in the devices when they are running. The non-volatile memory is used by the device for storage. Flash memory technology has established its reputation in this type of storage media. This technology has a number of factors and features that suit the needs particularly for mobile devices. These features include low cost, small in size, very light in weight, non-volatile, and its resistance to shock and low energy requirements (Junseok, et al., 2009, p.228).

The advancement in the technologies utilised by these SMART devices are getting more sophisticated and more complex. The applications running on these devices are refining as well. As a result, all the major Smartphone developers such as, iPhone 5, Samsung S3, the Motorola Droid Razr and the HTC One X were released with 1GB of memory. This is to gather for the demands from its powerful processor and its resource hungry applications (Targeted News Service, 2012).

In order for the users with devices that utilises the cellular network to connect to a network, they need a card known as the subscriber identity module or commonly known as SIM card.

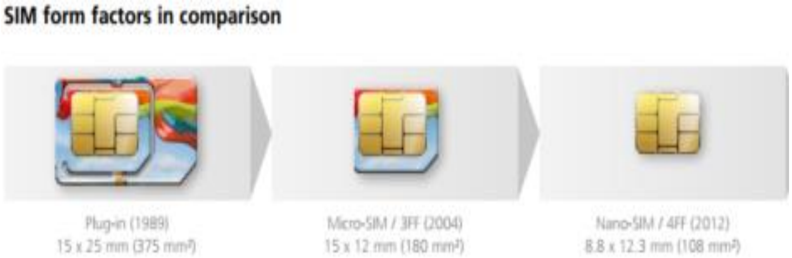


Figure 2.10: SIM form factor in comparison (Chadha, 2012).

Figure 2.10 above shows a comparison of various types of SIM cards that are currently utilised by different mobile SMART devices that operate on the cellular network. SIM card evolved from standard SIM size into the microSIM and now Smartphones such as iPhone 5 employed the nanoSIM. In order for a mobile SMART device to operate on a cellular network, both the user and the device need to be identified by the network. The SIM may be different is size but they are all used for the same purpose. They all store the same user information and they are all a removable module (Calvet & Noll, 2010, p.2).

The user information that is stored on a SIM card is encrypted for security purposes. This information is used to authenticate the user of the device to the cellular network (Welte, 2010, p.10). The user information is also used to also identify the services that the user subscribed for. However, this is not enough to start the communication over the network. The device itself needs to be authenticated also to the network. The Mobile Equipment (ME) is on the remaining partition on the handset. This number is also known as the International Mobile Equipment Identity (IMEI) (Jansen & Scarfone, 2008, p.11).

2.4.5 The Device's Operating System

Mobile SMART device operating system is the system software that is designed to run on the device's hardware. The operating system is then managed both the hardware and the applications running on the device. Well known mobile device operating systems are currently developed by desktop computer companies such as Apple, and Microsoft. The major mobile device developers have developed their own operating systems. For instance: the Symbian operating system from Nokia and the Blackberry OS by Research in Motion (RIM). Also the well-known open source Linux based mobile operating system from Google, the Android (Tilson, et al., 2011, p.28).

According to IDC tracker, in the year 2012 the top five Smartphone operating systems that dominate the consumer market are Android from Google, iOS from Apple, Blackberry, Symbian and Windows (mobile editions) from Microsoft. Following in table 2.3 below shows their standings in the world market share in the year 2012. The figures are in millions.

Table 2.3: Top Five Smartphone OS Market Share (IDC, 2015).

Period	Android	iOS	Windows Phone	BlackBerry OS	Others
2015Q2	82.8%	13.9%	2.6%	0.3%	0.4%
2014Q2	84.8%	11.6%	2.5%	0.5%	0.7%
2013Q2	79.8%	12.9%	3.4%	2.8%	1.2%
2012Q2	69.3%	16.6%	3.1%	4.9%	6.1%

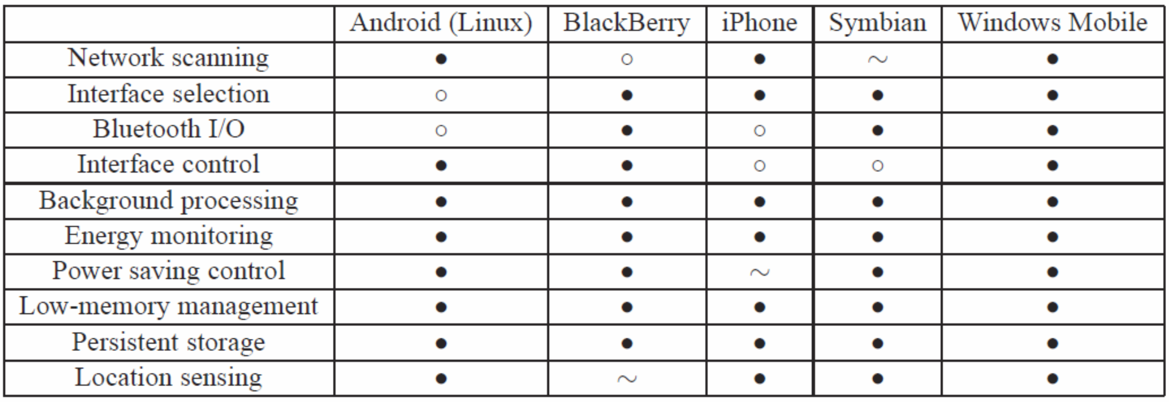
Android is a Linux based operating system from Google as a result of their Open Handset Alliance (OHA) project. The Android operating system is built with ability to support multitasking from its applications. This allows more complex business application on a SMART device that requires more than one activity to run (Allen, et al., 2010, p.35). As a result, applications that are built for the Android operating system are designed with components. These components are divided into four types namely activities, services, broadcast receivers and content providers. Hence, the components can be used to evaluate the behaviour of the application (Juanru, et al., 2012, p.553).

The iOS operating system from Apple, the iOS 4 was the first operating system released with a multitasking feature. This multitasking feature enables the user to process something in the background while using a different application to work on a different task (Moren, 2010, p.46). The file system adopted by the iOS operating system is Hierarchical File System (HFS). The HSF filing system utilised cataloguing file system to organise data (Morrissey, 2010, p.33).

The Windows SMART device from Microsoft is designed following a hierarchical organisation with nested folders and menus concepts similar to its desktop operating system. This is to provide its users with a familiar experience. (Allen, et al., 2010, p.65). The main advantage of the Windows mobile operating system is that the fact that it is taking advantage of a rich environment. This is referring to the Microsoft .Net framework environment. For mobile SMART devices it is known as the .Net compact framework. This is considered to be a rich environment which assists applications and databases that run on the mobile device (Gronli, et al., 2010, p.7)

Ten characteristics considered to be the most desirable on Smartphones were involved in a study. The world market share top five mobile SMART device operating system were engaged in this study. Table 2.4 shows the characteristics and also the findings from this study (Oliver, 2009, p.56).

Table 2.4: Mobile platforms requirements summary (Oliver, 2009, p.58).



	Android (Linux)	BlackBerry	iPhone	Symbian	Windows Mobile
Network scanning	●	○	●	∼	●
Interface selection	○	●	●	●	●
Bluetooth I/O	○	●	○	●	●
Interface control	●	●	○	○	●
Background processing	●	●	●	●	●
Energy monitoring	●	●	●	●	●
Power saving control	●	●	∼	●	●
Low-memory management	●	●	●	●	●
Persistent storage	●	●	●	●	●
Location sensing	●	∼	●	●	●

The top five platforms for mobile phones are the Symbian and Blackberry operating system. Symbian is said to have sophisticated design which supports multiple languages. Blackberry design concepts adopted the open source idea as its development platforms while all of its applications are written in Java (Oliver, 2009, p.60). Symbian is like Android adopting the open source design feature innovation. The Symbian design architecture includes the multi-threading, multi-tasking technologies. At the same time its design also includes a memory protection feature which helps to reduce resource consumption and memory usages more effectively (Hou, et al., 2012, p.3497).

2.4.6 The Device's Applications

The technological advancements in the business SMART device area, drives users' expectations higher. Smartphone users are imagining more interactive applications. There are expectations for high responsive user interfaces and 3D graphics. Users are expecting their SMART devices to deliver a desktop computer like performance such as high-definition audio and video, web-browsers with dynamic web content (Gutierrez, et al., 2011, p.82). On a press release by Apple, they announce that the App store contains more than 775,000 applications for iPhone, iPad and the iPod touch. These applications range from newspapers and magazines to games and health and travel. In this press release Apple announced that there have been 40 billion downloads excluding updates and re-downloads (Miller & Monaghan, 2013).

However, when the developers released these devices into the market, the device comes with basic applications. For instance, the iPhone was released and it came with Stock market application, simple messaging, Calendar, Maps with GPS navigation system, Weather, You Tube, Calculator, iTunes, Safari, Mail, Photos, Siri, Contacts, Passbook, Phone, Voice Memo and Notes (Morrissey, 2010, p.33).

Figure 2.11: iPhone built-in-apps and from the app store (Apple Inc., 2013, p.1).

Figure 2.11 above illustrated the basic built-in applications that come with the device when it is released and the third party applications that can be downloaded from the app store. A look into the future of SMART devices, Smartphones will become a constant companion for humans. This means that these mobile SMART devices will be an impeccable assistant for users regardless their age (Siewiorek, 2012, p.56).

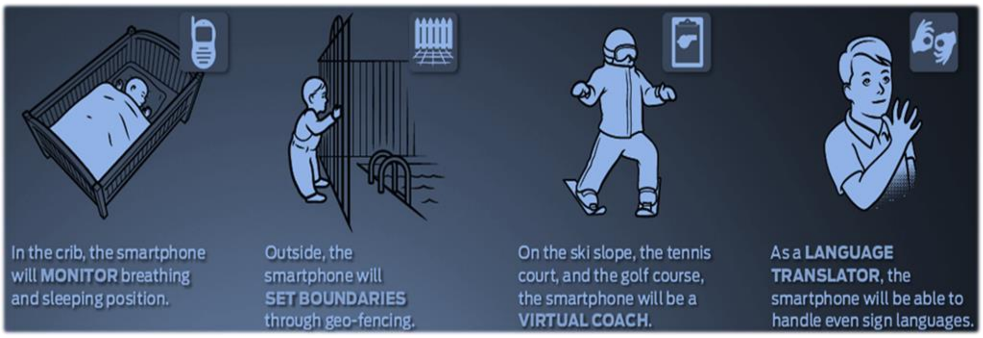

In the crib, the smartphone will MONITOR breathing and sleeping position.
Outside, the smartphone will SET BOUNDARIES through geo-fencing.
On the ski slope, the tennis court, and the golf course, the smartphone will be a VIRTUAL COACH.
As a LANGUAGE TRANSLATOR, the smartphone will be able to handle even sign languages.

Figure 2.12: Future applications for Smartphones (Siewiorek, 2012, p.57).

As figure 2.12 shows, mobile SMART devices of the future will be able to use applications that have the ability to monitor babies breathing and sleeping position. Applications for language translation, a virtual sports coach, an indoor mapping application for universities and malls are already readily available. A virtual watchdog application can provide the users with warning of a potentially dangerous situation in advance. Most of these applications are already in research laboratories (Siewiorek, 2012, p.57).

2.5 BUSINESS NETWORK ENVIRONMENTS

Mobile business devices are capable of connecting to businesses' networks as a result of its heterogeneous and ubiquitous connectivity nature (Lagerspetz & Tarkoma, 2010, p.826). These devices can connect to data centres and Internet servers and acquire data such as weather reports, social media or Internet TV (Lagerspetz & Tarkoma, 2011, p.117). Despite the fact that Wireless Wide Area Network (WWAN) is said to be based on the cellular radio signals, there are various types of wireless networks that are primarily different from the cellular networks (Nair, 2008, p.2). This section is designed to explore various types of wireless networks that provide connectivity for these SMART devices. Network architectures and the protocols that enable communication between these devices are defined for investigation purposes.

2.5.1 Wireless Networks

There are various types of wireless networks that exist today. They are categorised by their size, the smallest is known as Wireless Personal Area Network (WPAN), Wireless Local Area Network (WLAN), Wireless Metropolitan Area Network (WMAN) and the largest is known as Wireless Wide

Area Network (WWAN) (Jha, 2002, p.275). The range for the Wireless PAN is only 5 to 10 meters, and for the Wireless LAN can cover up to 100 meters. Wireless MAN coverage is more than 100 meters or WMAN is referred as a network within one city. The largest is known as Wireless Wide Area Network (WWAN), this type of wireless network provides wireless connectivity between cities and beyond. The diagram in figure 2.13 graphical illustrations of the differences between these networks (Lammle, 2010, p.3).

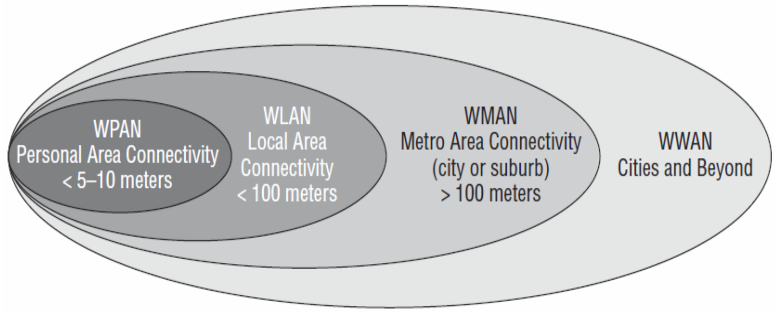


Figure 2.13: Various types of wireless networks (Lammle, 2010, p.3).

With regards to Personal Area Network, the frequency engaged by this type of network is unlicensed, meaning that the users do not have to pay. The devices in this type of networks are low powered and only cover a distance of up to 10 meters (Lammle, 2010, p.4). However, there is another type of wireless network known as Wireless Body Area Network (WBAN). The WBAN comprises of two types of networking known as an in-body area network and an on-body area network (Ullah, et al., 2012, p.1067). Figure 2.14 illustrates the location of the WBAN in the wireless network domain.

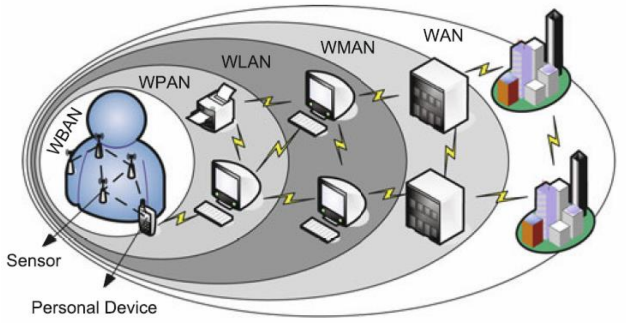


Figure 2.14: WBAN position in wireless network (Latré, et al., 2011, p.6).

The in-body area network is said to be an invasive type of networking because the devices are implanted inside the human body. The on-body area network on the other hand is non-invasive because the devices are wearable. These devices communicate with the monitoring base station that allows medical personnel to monitor a patient’s health (Ullah, et al., 2012, p.1067). The main difference between WPAN and WBAN is that WPAN provides short range wireless connectivity around a human. The WBAN provides even shorter range connectivity in or on human body (Molisch, 2010, p.14).

As illustrated in figure 2.14, WLAN has a larger coverage area than WBAN and WPAN. Wireless LANs provide its users with larger coverage area and higher bandwidth connectivity. Wireless LANs use unlicensed frequency which means that, WLAN users do not need to pay to use that frequency band before using it (Lammle, 2010, p.4). Development in the WLAN technologies has enabled businesses to enhance their services high speed data access in homes, offices and hot-spots (Rajan, 2011, p.9). WLAN is capable of delivering a higher data rate to its users. It is considered to be more suitable for networking within an office, building, campus or at home to provide its users’ with the benefit of being mobile while continuously connecting to the network (Sabat, 2002, p.510). However, its services are still limited to small geographical areas when compared to other types of wireless networks such as Wireless Metropolitan Area Networks (WMAN) (Rizvi, et al., 2010, p.92).

Wireless MAN is fundamentally described as a network that is designed to provide wireless connectivity for its users within one city. WMAN networks common these days due to the development and advancements in its technologies. Wireless MAN are said to be a more economical alternative companies than point to point leased line. The only downside of Wireless MAN is that to establish a wireless connection in a metropolitan area every node needs line of sight geometry (Lammle, 2010, p.4).

The two diagrams shown in figures 2.13 and 2.14 give the fact that Wireless WAN covers a larger geographical area than Wireless MAN and Wireless LAN (Sabat, 2002, p.510). Sturniolo (2001) defined Wireless WAN as a computer data network that covers a large geographical area. As a result, data transmission in Wireless WAN employs radio signals when communicating with mobile device systems (Sturniolo, 2001, p.12). Yet, the advancement in high bandwidth technologies enables Wireless WAN network to replicate the fixed wired networks’ performance (Kevan, 2004, p.22). The coverage and nomadic use of this type of network is made possible by the network providers in the area of coverage for a fee (Jha, 2002, p.275).

2.5.2 Cellular Networks

Due to the advancement in cellular technologies and the rapid growth in its accepted practices, the cellular network is recognised as the fastest growing access network (Tipper, et al., 2010, p.1). In the past two decades, there have been substantial changes in the telecommunication industry. However, the cellular network engages different design methodologies (Garg, 2010, p.1). The cellular network's design is hierarchical which is different from Wi-Fi system design which is flat (Bosch, et al., 2007, p.3865). Nonetheless, the cellular network design is based on four criteria; coverage, capacity, C/I and cost. Coverage referred to how much area it is going to cover while capacity concerns with how much traffic the network can gather for. C/I stand for "carrier-to-interference" ratio. The final criterion is cost which concerns the network resource expenditure (Arpee, 2001, p.26).

2.5.3 The Network Architectures

Figure 2.14 indicated that the smallest type of wireless network is known as the Wireless Body Area Network. As portrayed by its name, also explained earlier, this type of wireless network is either on or in the human body as illustrated in figure 2.15 below. This type of network employs various types of biosensors. In the health industry, they engage this type of network to measure patients' heartbeat, body temperature for instance. The body area network allows health personnel to monitor the patient regardless of the patient's location (Latré, et al., 2011, p.3).

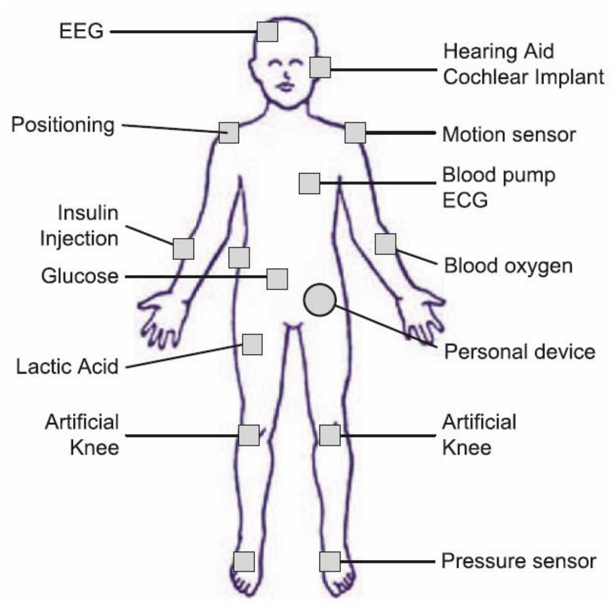


Figure 2.15: WBAN as in patient monitoring system (Latré, et al., 2011, p.3).

On the other hand, health is not the only industry that Wireless BAN can be applied. Motion sensors are now worn on hands and elbows for accurate extraction of movement data by sport professionals and on military training. On Interactive gaming such as boxing and shooting, the players are required to wear body sensors for movement accuracy. On daily life applications such as shopping, information exchange, private or business information can be stored on these body sensors for information sharing purposes (Chen, et al., 2011, p.172).

Wireless BAN network communication architecture has three-tiers. Tier one is referred to as Intra-BAN communication, tier two is Inter-BAN communication and tier three is Beyond BAN communication. Intra-BAN communication in tier one refers to the communication between the body sensors and the user’s mobile SMART device, a phone, PDA or tablet.

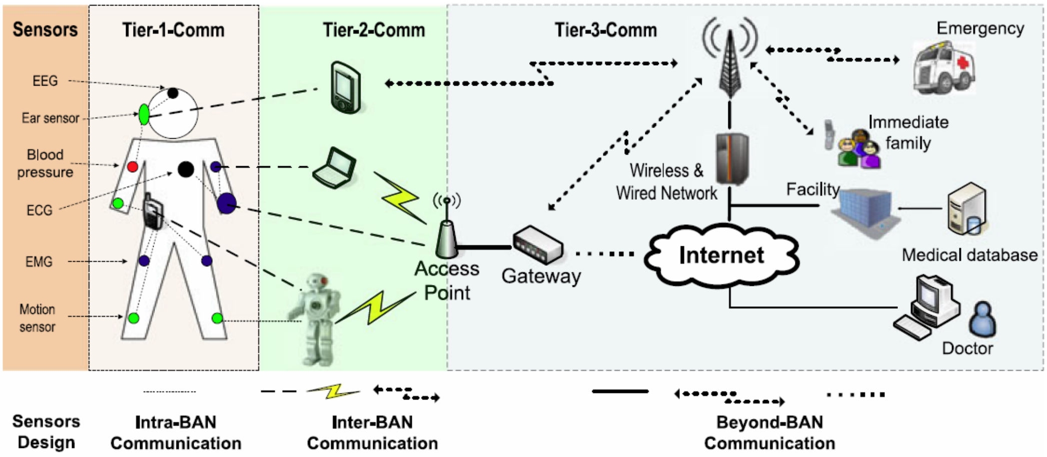


Figure 2.16: WBAN three-tier communication system (Chen, et al., 2011, p.173).

The Inter-BAN communication refers to the communication between the user's mobile SMART device and the local access point (AP), whether infrastructure or ad hoc based. Tier two communication architecture enables communication between WBAN and other types of networks such as the Internet or the cellular network as illustrated in figure 2.17 (Chen, et al., 2011, p.174). The final tier, beyond-BAN is designed to enable the communication between the Inter-WBAN network and the beyond-BAN network. This is to allow the system to alert doctors or emergency health personnel via email or text messages when any abnormalities are found (Chen, et al., 2011, p.174).

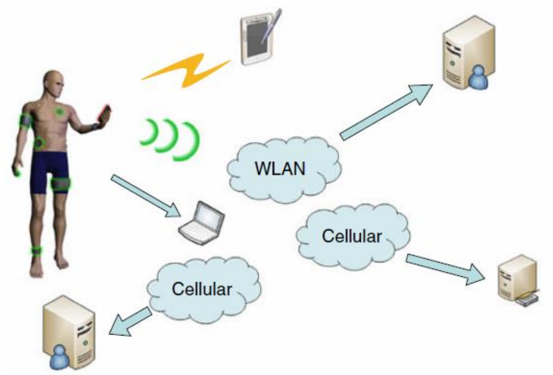


Figure 2.17: WBAN tier-two communication architecture (Chen, et al., 2011, p.174).

With regards to Wireless PAN, the goal is to eliminate the wires that connect devices that are close to each other (Siep, et al., 2000, p.38). The communication coverage for Wireless PAN is up to 10 metres in all directions. Wireless PAN is an ad hoc, also known as Pico network, wireless data communication system that enables autonomous devices to communicate within mutual range of each other

(Braley, et al., 2000, p.29). Due to the advancement in technologies and electronic devices surrounding Personal Operating Space (POS) today, the need for mobility and the demand to network these devices have grown as well (Ali & Mouftah, 2011, p.675). Figure 2.18 shows the two main architectures of Wireless PAN.

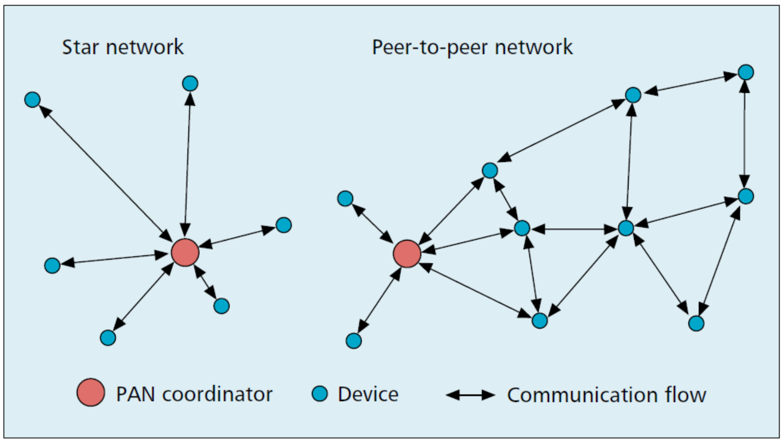


Figure 2.18: Two WPAN architecture (Callaway, et al., 2002, p.71).

Even though that Wireless PAN was designed only for short range connectivity and for POS networking, it has many advantages as well because of its ad hoc nature. For instance, being ad hoc makes it very flexible and there is no need for an infrastructure therefore cost is very low. The Institute of Electrical and Electronics Engineers (IEEE) standard for Wireless PAN was designed to support a number of topologies including star and peer-to-peer as illustrated in figure 2.18. However, while the accentuation was on the ad hoc nature of Wireless PAN, its interconnection with larger networks such as the cellular network infrastructure was also prominent as is shown in figure 2.19 below (Johansson, et al., 2001, p.29)

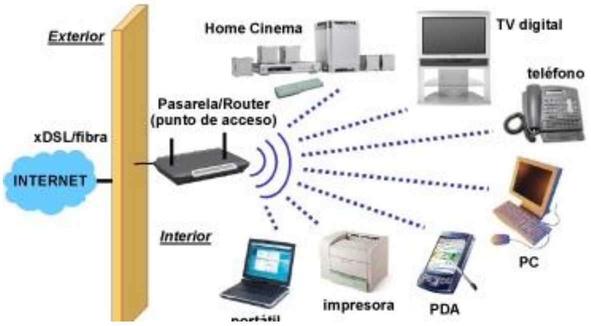


Figure 2.19: WPAN Star topology (Jain, 2006, p.4-1).

Since the Wireless PAN can interconnect with larger network infrastructures, its usage has become more common. As a result, a new specification was developed for Gigabit data communication and for data transmission requirements (Miyahara, 2011, p.345). The Wireless LAN environment requires an access points to act as a coordinator between users' device and the local network. On the other hand, user's device requires wireless interface card to enable communication with the access point as illustrated in figure 2.20.

Wireless LAN's standard has allowed its users to be mobile around offices, homes, hotels, restaurants and universities just to name a few while having constant high speed data access. As illustrated in figure 2.20, regardless of the type of users' device whether it is a desktop computer, laptop, tablet or a Smartphone, as long it has wireless interface, then it can utilise the network (Rajan, 2011, p.9). In a basic Wireless LAN environment, only two main devices are required in order to establish a connection, the wireless interface card and an access point as shown in figure 2.20. An access point in a wireless network environment is acting like an access switch in a wired network environment. Its function is to connect all the hosts together so they can talk to each other (Lammle, 2010, p.5).

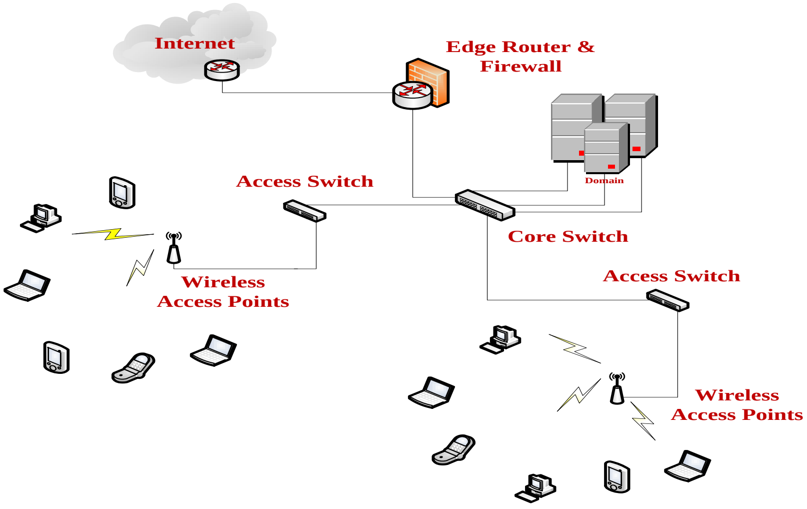


Figure 2.20: Wireless LAN environment.

Figure 2.21, shows the architecture of a Wireless MAN which is a larger type of wireless network than Wireless LAN. Wireless MAN can be referred to as a bridging network. This provides an alternative which is a more economical solution as opposed to a dedicated leased line, Asynchronous Transfer Mode (ATM) or Frame relay connection (Lammle, 2010, p.5).

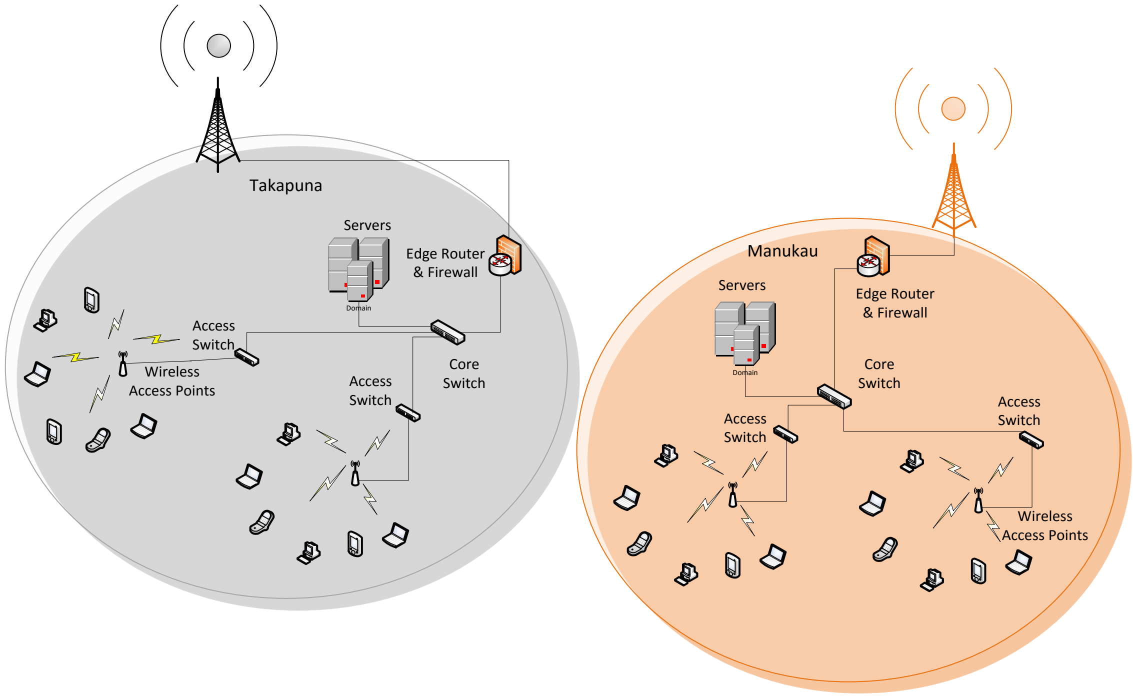


Figure 2.21: Wireless MAN environment.

In a WMAN environment, Microwave technologies are usually employed to connect two or more remote WLAN networks sites of up to 30 kilometres or more (Lee, et al., 2006, p.57). Wireless MAN technologies are considered to be transparent and compatible with the Ethernet standard. As a result, it supports all Ethernet applications and functionalities (Kotsch, 1996, p.125). The main difference between the Wireless MAN and Wireless WAN is their geographical sizes. Wireless MAN is the interconnection between two or more local area networks within one city or metropolitan area. Wireless WAN is the interconnection of one or more networks from different cities or countries - as illustrated in figure 2.22 – and is the largest type of wireless network (Lammle, 2010, p.5).

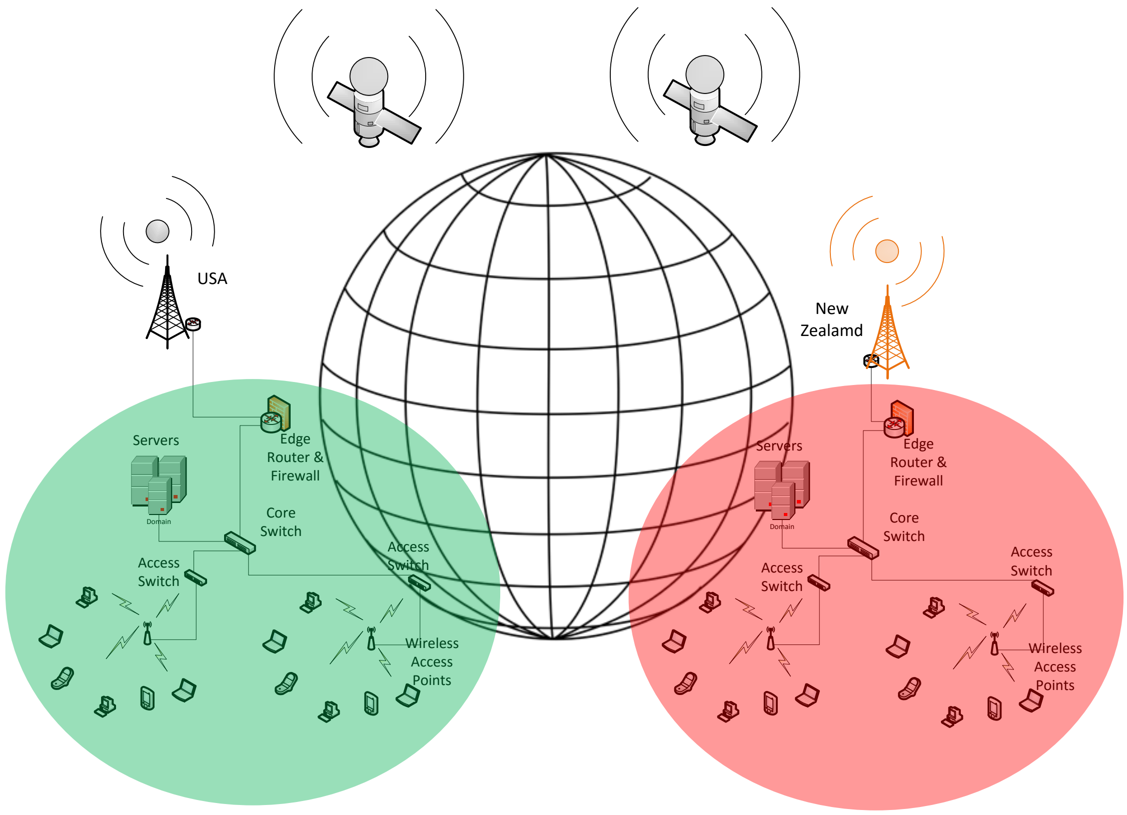


Figure 2.22: Wireless WAN environment (Globe adapted from Hansen, 2012, p.1).

Wireless WAN is a network that enables data transmission via satellite. Similar to Wireless MAN, Wireless WAN is more flexible, economical and easier to implement than traditional networking wired technologies (Enticknap, 2003, p.44). The merging of communication and computing technologies has changed the requirement of digital mobile wireless communication devices. The Wireless WAN is based on the cellular network infrastructure. The advancement of the WWAN technologies has provided businesses with more opportunities as it is growing in a direction that specifically meets business requirements in wireless long distance communications (Nair, 2008, p.8).

In addition, the advancement and the growth in the IP technologies domain have become the main influence in the development of future communication satellites (Pelton, 2012, p.104). Communication satellites service scope is known as the “Big Three”. The “Big Three” is divided in to three main categories namely, Fixed Satellite Services (FSS), Broadcast Satellite Services (BSS), and Mobile Satellite Services (MSS) (Pelton, 2012, p.15). Figure 2.23 shows the Big Three services and their area of applications.

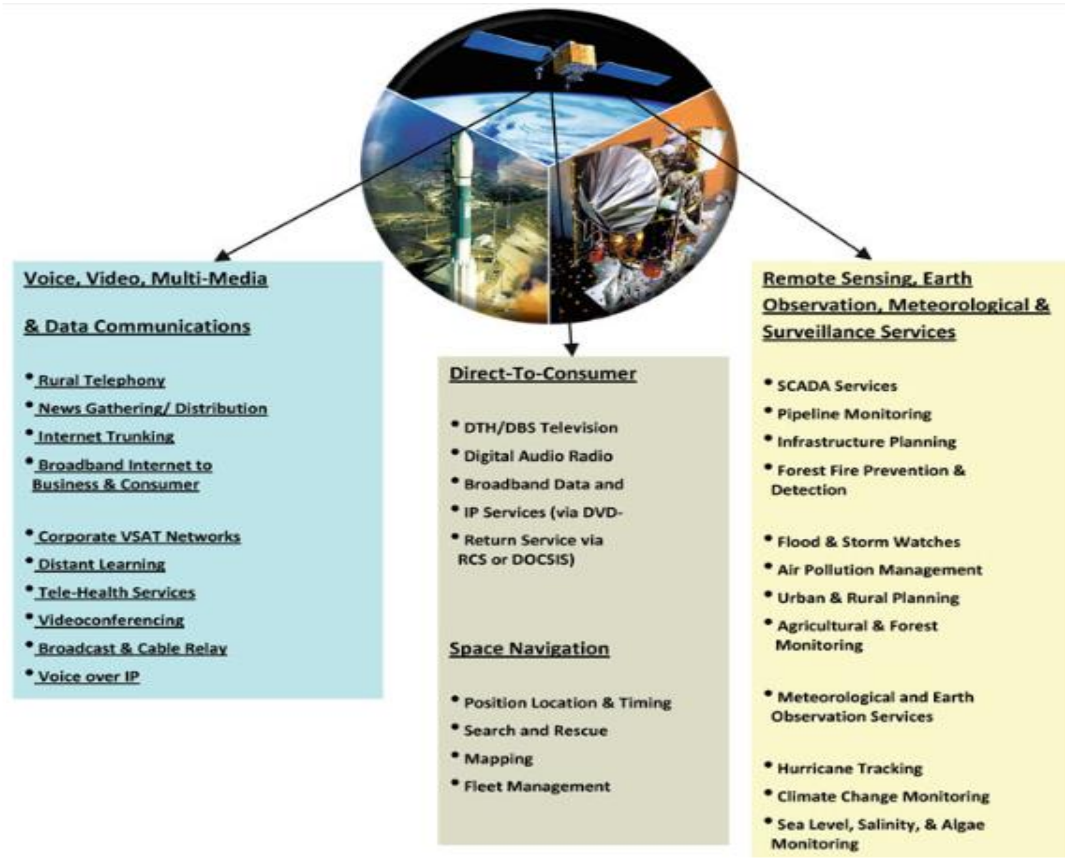


Figure 2.23: The Big Three (Pelton, 2012, p.15).

The integration of the computing technologies and the communication technologies contributed to the rapid changes of the wireless devices' requirements (Nair, 2008, p.2). However, Sang-Rock, et al. (2008, p.1) argues that, Wireless WAN system is built on the IEEE standard which utilises the five frequency band that employed by the cellular network. With regards to the cellular network itself, the design philosophy is very complex (Potter, 1999, p.63). The first cellular network structure was consist of one base station only that has the ability to provide the required coverage for the whole mobile communication system. Due to the spontaneous growth in the demand for the cellular services, more base stations have to be deployed. Users' expect services from the network mainly for their mobile devices. The challenge was from services such as navigation data, video and interactive network applications which require high bandwidth and faster response time (Lin, et al., 2006, p.347). As a result, the network needs to be restructured because of the frequency spectrum limitations (Mazzini, et al., 2003, 659); and, estimating the coverage area was a key problem (Sayrac, et al., 2012, p.43).

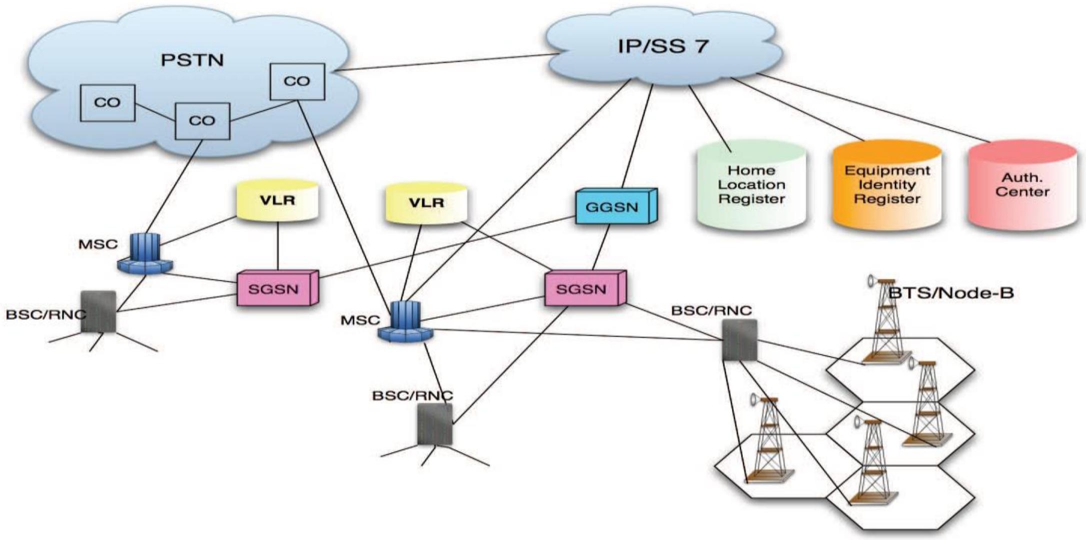


Figure 2.24: Cellular network architecture (Tipper, et al., 2010, p.1).

A standard cellular network architecture illustrated in figure 2.24 is based on the mobile third generation technology. Figure 2.24 shows five main databases in the cellular network. It also shows the interconnection between the cellular network and Public Switched Telephone Networks (PSTN) and the Wi-Fi IP network. To provide quality of service (QoS) for various wireless technologies is a real challenge thus, the integration can enhance the performance of the network (Bhargava & Wang, 2004, p.393). The cellular network five databases are the Mobile Switching Centre (MSC), Equipment Identity Register (EIR), Home Location Register (HLR), Visitor Location Register (VLR) and the Authentication Centre (AuC).

The HLR database holds the mobile subscribers' information and the services subscribed (Sauter, 2010, p.14). When a mobile device is turned on, the International Mobile Subscriber Identity (IMSI) is retrieved from the SIM card and sent to the MSC for analysis. The purpose of this analysis is to identify the devices Mobile Country Code (MCC) and its Mobile Network Code (MNC). The MSC will then request the subscriber's information from HLR. However, when the device leaves the coverage area of the MSC, the subscriber's information will be copied and sent to the next MSC's VLR then the information is then deleted from the previous MSC's VLR database (Sauter, 2010, p.15). The AuC database holds the subscriber's individual key which is the copy of the key hidden in the subscriber's SIM card (Sauter, 2010, p.18). The EIR database holds information regarding the identity of the mobile device. This information can be used in conjunction with the AuC database for authentication purposes. This combination is very useful when preventing calls from the device if it gets stolen (Kabir, 2009, p.5). Section 2.5.4 is designed to provide an outline of the protocols that are employed by these wireless networks. These protocols enable dissimilar devices that utilises the services to be able to communicate on various layers of the heterogeneous wireless communication networks.

2.5.4 Network Applications (Protocols)

Figure 2.13 showed in section 2.5.1 various types of wireless networks. WBAN is recognised to be the smallest type of wireless network today and the protocol standard is incorporated into the IEEE 802.15 family. Due to the fact that WBAN is dealing with network regarding On/In human body, the standard approved for WBAN is IEEE 802.15.4 also known as Low-Rate WPAN (LR-WPAN) (Kok Seng, et al., 2011, p.851).

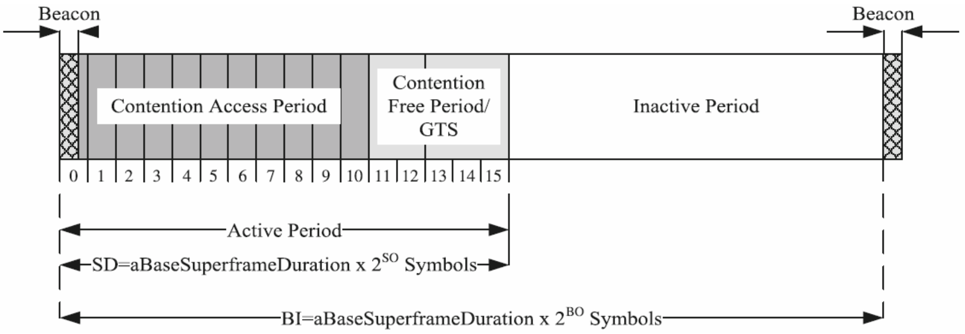

Beacon
Beacon
Contention Access Period
Contention Free Period/ GTS
Inactive Period
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
Active Period
SD=aBaseSuperframeDuration x 2^SO Symbols
BI=aBaseSuperframeDuration x 2^BO Symbols

Figure 2.25: LR-WPAN frame structure (Ullah, et al., 2012, p.1077).

The LR-WPAN frame structure in figure 2.25 illustrates how the protocol is arranged. The beacon bit is used to flag the beginning and the end of the frame however, data transmission only happens in the active period not the inactive period (Ullah, et al., 2012, p.1077). The IEEE 802.15.4 protocol is designed to work on the Data Link Layer (DLL) of the Open Systems Interconnection (OSI) model. The OSI is a network architecture layered model was adopted by the International Organisation for Standardisation (ISO).

On layer two of the OSI model, DLL layer, is further divided into two sub layers known as the MAC and Logical Link Control (LLC) sub layers. In the MAC sub layer, IEEE 802.15.4 engaged the Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) as an access method in order to control the communication channel access (Howitt & Gutierrez, 2003, p.1482). The development of the IEEE 802.15.4 is concerned with the MAC sub layer and also with physical layer. The physical layer is concerned with the frequency band for the device while the MAC sub layer provides flow control to the physical channel and the acknowledgement of packet delivery. The physical layer also defines the technique engaged for data transmission (Callaway, et al., 2002, p.71).

In terms of Wireless PAN, is defined as a network around Personal Operating Space (POS) or around a person (Latré, et al., 2011, p.6). The Wireless PAN employed two different standard protocols, Bluetooth and High Rate-WPAN (HR-WPAN). The development of these two protocols is a result of the growth in the demand from high bandwidth multimedia application. This demand comes especially from digital mobile end user electronic devices that require wireless connectivity, high data transfer rates with low power consumption QoS (Yin & Leung, 2006, p.681). The Bluetooth was standardised into the IEEE 802.15 family as IEEE 802.15.1 while HR-WPAN was standardised as the IEEE 802.15.3.

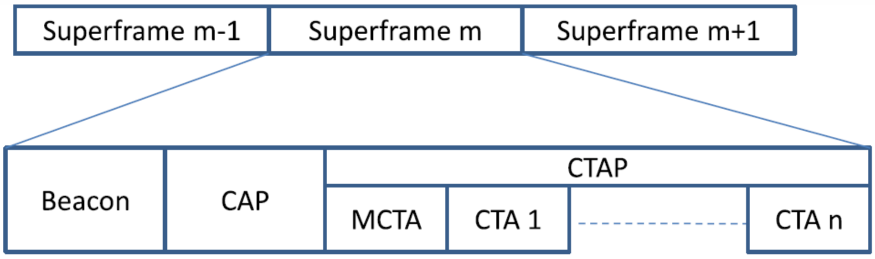


Figure 2.26: HR-WPAN frame structure (Ali & Mouftah, 2011, p.678).

The structure for the HR-WPAN protocol's frame shown in figure 2.22 illustrated the layout of the frame. The HR-WPAN frame consists of the Beacon Period (BP) similar to LR-WPAN frame structure. The BP is used for management purposes such as, in this period the network coordinator flags the transmission time allocation (Ali & Mouftah, 2011, p.678). Similarly to LR-WPAN, these two protocols utilise the unlicensed frequency channel and work on both the MAC sub layer and the physical layer of the OSI model. These two protocols define the devices features such as, low power consumptions, low cost and its coverage range. LR-WPAN and HR-WPAN both employ an access technique known a Time Division Multiple Access (TDMA). This technique is used to allocate channel time slots to each node in the network for data transmission (Ali & Mouftah, 2011, p.678).

Bluetooth protocol on the other hand, the protocol was developed by Ericsson in 1994 defining a standard for low cost, low power and short range wireless communication. Bluetooth is now standardised by IEEE into their 802.15 family as IEEE 802.15.1. There are three logical groups within the Bluetooth protocol stack namely, Transport Protocol group, Middleware Protocol group and the Application Protocol group as illustrated in figure 2.27. Similarly the IEEE 802.15.3 and 802.15.4 protocols, 802.15.1 operates in the DLL and physical layers of the OSI Model. (McDermott-Wells, 2004, p.33).

The Transport Protocol group is responsible for supporting the communication between Bluetooth enabled devices. The Middleware Protocol group is responsible for existing and new application operations over a Bluetooth link while the Application Protocol group consists of the actual applications the utilise Bluetooth links (van der Linde & Hancke, 2008, p.452).

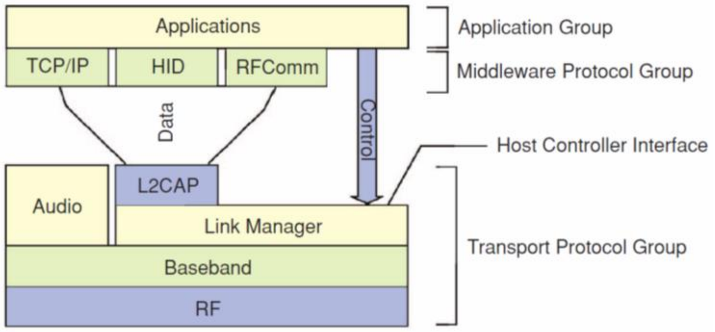


Figure 2.27: Three groups in the Bluetooth protocol (McDermott-Wells, 2004, p.33).

The Bluetooth protocol stack defines Baseband as part of the Transport Protocol group as shown in figure 2.27. Baseband specification defines two types of links namely Synchronous Connection Oriented (SCO) and Asynchronous Connection-Less (ACL). The SCO link type is known to be symmetric point-to-point with synchronous timing while ACL link type can provide a point-to-multipoint connection with asynchronous timing The Bluetooth protocol employed two access techniques known as Time Division Duplexing (TDD) and TDMA (McDermott-Wells, 2004, p.34).

IEEE 802.11 family of protocols on the other hand defines the specifications for Wireless LANs. The protocol was standardised and approved as an international standard for Wireless LAN in 1997 by the Institute of Electrical and Electronics Engineers (IEEE) (Baranov & Lyakhov, 2005, p.1101). In a Wireless LAN environment, the coordinator is a device known as Access Point

(AP). The coordinator (AP) plays a vital part in this environment. The AP is accountable for connecting the Wireless LAN with the Wired LAN. In order to avoid collisions with regards to bandwidth consumptions, an access method protocol known as Medium Access Control (MAC) is employed for Quality of Service (QoS) purposes.

Within the MAC protocol is the Distributed Coordination Function (DCF) protocol that defines the basic access method. In order to avoid collisions during data transmission, DCF employs CSMA/CA protocol to sense the channel before it starts transmitting. This method will also minimise delay, jitter and the packet drop rates (Chen, et al., 2005, p.741). Figure 2.28 illustrates the two layers of the OSI model that the IEEE 802.11 protocol operates in and the two sub layers of the DLL layer as well.

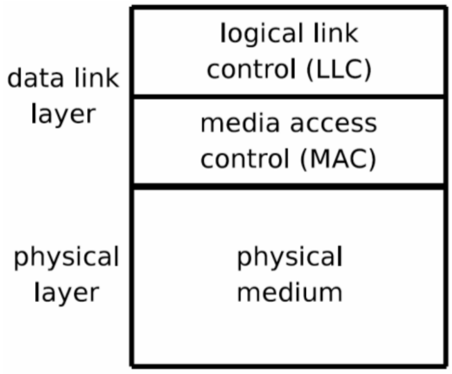
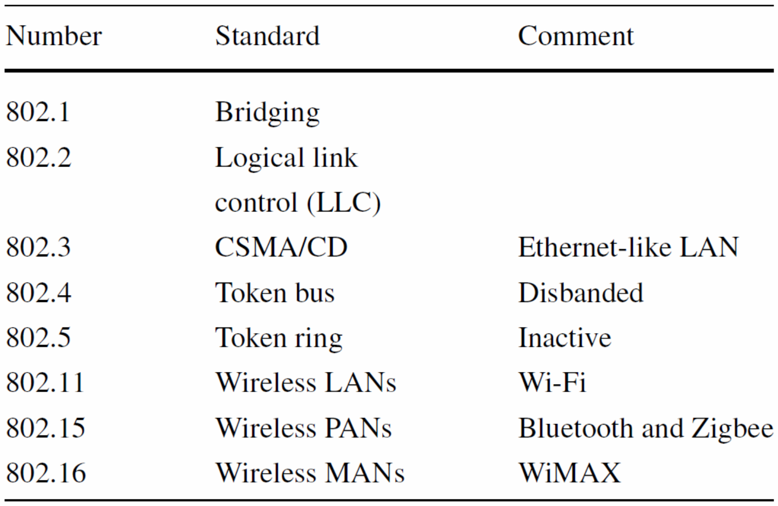


Figure 2.28: MAC layer is a sub layer of DLL layer (Holt & Huang, 2010, p.2).

One of the DLL sub layers is LLC, its main responsibility is to facilitate the communication between the MAC layer and the upper layers of the OSI model such as the Network layer (Holt & Huang, 2010, p.2). Following in table 2.5 shows some of the IEEE 802 standards. IEEE 802.16 protocol defines the standard for Wireless MAN. As showed in table 2.5, Worldwide Interoperability for Microwave Access (WiMAX) is one of the wireless technologies that was developed based on the IEEE 802.16 standard and can be employed by Wireless MAN. WiMAX is a technology that needs line of sight (LOS) for point to point connectivity and this usually utilised on a backbone connection aggregating two or more Wireless LAN (Pareek, 2006, p.151).

Table 2.5: The IEEE 802 standard (Holt & Huang, 2010, p.3).



Number	Standard	Comment
802.1	Bridging	
802.2	Logical link control (LLC)	
802.3	CSMA/CD	Ethernet-like LAN
802.4	Token bus	Disbanded
802.5	Token ring	Inactive
802.11	Wireless LANs	Wi-Fi
802.15	Wireless PANs	Bluetooth and Zigbee
802.16	Wireless MANs	WiMAX

Wireless networks tend to present more challenges then Ethernet networks due to its nature and environment. As a result, it affects the efficiency of the Internet Protocol (IP) especially the WWAN backbone connections such as satellite. It introduces more propagation delay, packet loss and low bandwidth (Astuti, et al., 2008, p.121).

To address this problem, the IEEE 802.16 protocol defines two different access systems and also specifies the frequency ranges for each system. The line of sight (LOS) system works on the 10 to 66 GHz range while the non-line of sight system will work on the 2 to 11 GHz range (Pareek, 2006, p.164). The standardisation of the NLOS system was finalised in January 2003 as the IEEE 802.16a. The phenomenal development of the wireless technologies has enabled the integration of various both wired and wireless networks today. At the same time, it has made satellite technologies and the cellular network as the main WMAN and WWAN provider (Pelton, 2012, p.103).

The cellular technologies have notably grown over the past twenty years. This growth is responsible for enabling the anywhere at any time connectivity possible and also the integration between various types of networks (Rizvi, et al., 2010, p.92). The cellular network architecture shown in figure 2.24 has many protocols that are responsible for making communication possible in such a complicated design. For instance, the communication between the MSC and the BS, a protocol known as Base Station Management Application Part (BSMAP) is used. Another protocol is employed to deal with call processing and mobility management such as Direct Transfer Application Part (DTAP) which must be mapped to the MSC signalling protocol (Botta, et al., 2009, p.440; Sauter, 2010, p.9). MSC is a different protocol that works on the layer 3 of the OSI model and it is responsible for routing voice or data packets around the network (Sauter, 2010, p.7; Ergen, 2009, p.419).

However, there are two features of the cellular network that are significant in terms of its capability to successfully handle mobile users. First is how the network deals with handling mobile users from one cell site to the next. Secondly is how the system locates the device and assigns frequencies to it while it is on the move (Pareek, 2006, p.53; Rizvi, et al., 2010, p.92). This issue has triggered a substantial amount of research in the area to accomplish smooth handoff while the device is mobile (Mehbodniya, et al., 2013, p.485). Unquestionably, connecting wirelessly to corporate networks and the Internet from Smartphones and tablets are more common these days and still increasing. Cellular network providers have to deal with network and bandwidth capacity complications to meet the demands of these devices (Kolios, et al., 2011, p.25).

2.6 CLOUD COMPUTING

This section of the chapter is designed to provide definitions of Cloud computing. The technology has introduced a new character into the computing domain. Cloud computing brings about the idea of moving IT resources away to data centres in the cloud (Sugiki & Kato, 2011, p.306). This section will also cover various cloud architectures and services associated with this technology. Privacy and security challenges will also be highlighted.

2.6.1 Definitions

Cloud computing has been defined in various ways for instance, Furht (2010, p.3) defined Cloud computing as, *“a new style of computing in which dynamically scalable and often virtualized resources are provided as a services over the Internet”*. According to Mollah, et al. (2012, p1), Cloud computing is a, *“TCP/IP based high development and integrations of computer technologies such as fast microprocessor, huge memory, high-speed network and reliable system architecture.”* However, the National Institute of Standards and Technology released their Special Publication 800-145 and Mell & Grance (2011, p.2) defined Cloud computing as *“a model for enabling ubiquitous, convenient, on-demand* *network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".* The cloud is said to be a network of data centres working together to provide powerful applications, platforms and services that can be accessed by its users over the Internet (Abhishek & Mahasweta, 2011, p.3).

Cloud computing has four various deployment models. The first model is known as **"Private Cloud"**, this model refers to a cloud infrastructure that may be owned and operated by an organisation for private use only. The second model is known as **"Community Cloud"**, this model refers to a cloud infrastructure that is owned, managed and used exclusively by a community with similar concerns such as security requirements, policies or mission. The third model is called **"Public Cloud"**, this model refers to an infrastructure that is open to the general public. This infrastructure may be owned and operated by an academic institution, government organisation or a business. The final cloud model is called **"Hybrid Cloud"**, this model refers to an infrastructure which is a combination of two or more of the other three models. This particular model allows the infrastructure to remain exclusive while they are bound by standards or branded technologies (Mell & Grance, 2011, p.3). The following section will outline the various architectures of Cloud computing.

2.6.2 Cloud Computing Architectures

This particular set up is called Layered architecture. It is due to the fact that the design is composed of layers such as the Individual Cloud Provider Layer. This layer allows each provider to set up their own data centre. Another layer that is showed in figure 2.29 is the Mapping layer. This layer is employed to deal with different features applied by the provider. The Mapping layer will also be useful in dealing with these different features when migrating cloud applications to another cloud. Virtualisation technology plays a significant role in Cloud computing. Virtualisation advantages such as multiplexing of resources, flexibility and isolation suites Infrastructure-as-a-Service (IaaS) cloud system perfectly (Sugiki & Kato, 2011, p.306).

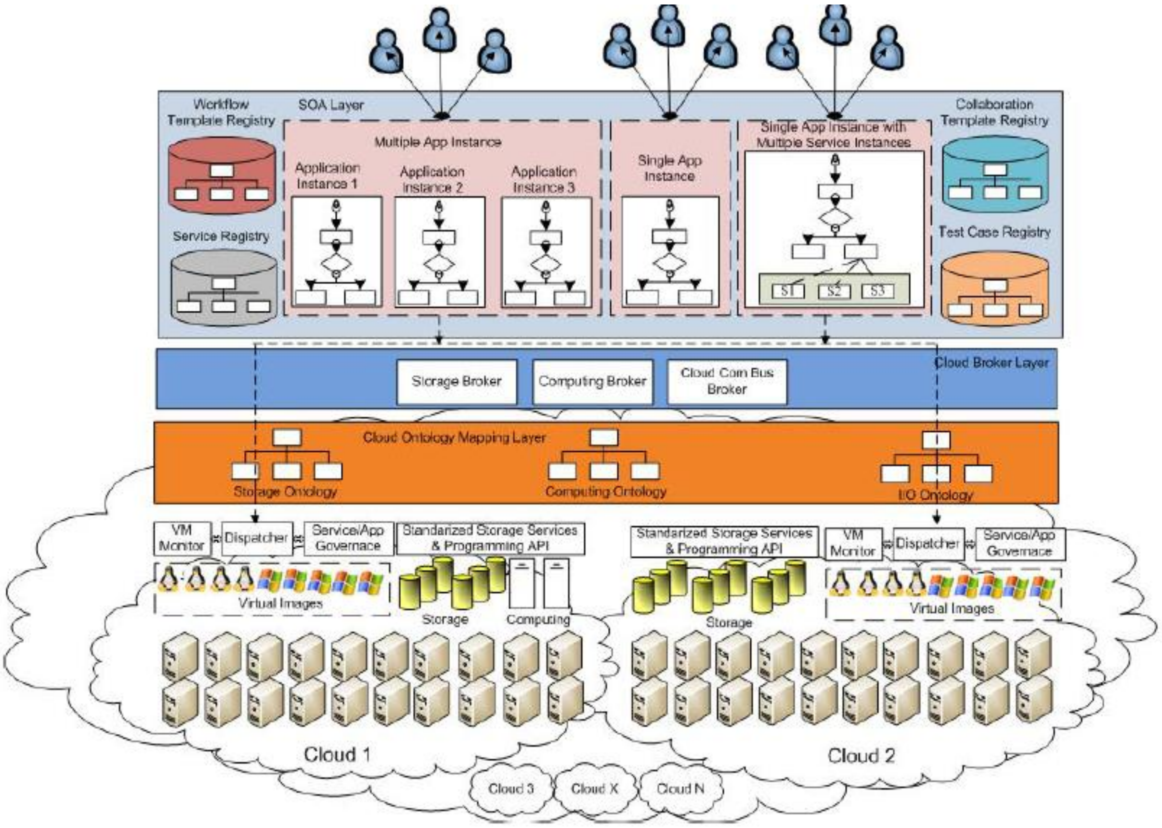
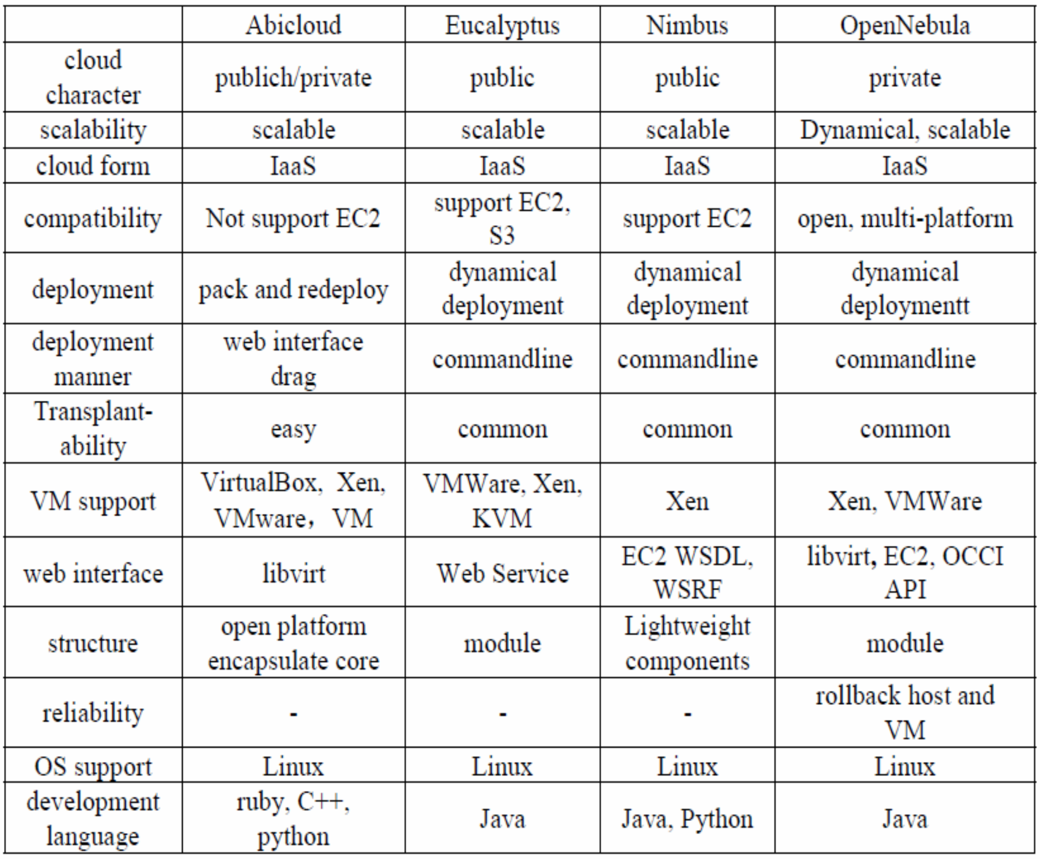


Figure 2.29: Cloud computing architecture (Wei-Tek, et al., 2010, p.686).

There are several virtualisation platforms employed by cloud computing available today such as OpenNebula and Open-Stack (Sugiki & Kato, 2011, p.306), Eucalyptus (Graubner, et al., 2011, p.243) and Nimbus (Marshall, et al., 2010, p.44).

Table 2.6 provides a comparison of several cloud computing platforms. The table outlines each platform including the cloud model, operating system supported and the type of service that each platform can provide. With regards to cloud architecture, each virtualisation platform has its own architecture design such as the Abicloud platform illustrated in figure 2.30. Abicloud is open source infrastructure software. Abicloud has three different versions aiming to provide services to three different layers of business requirements. At the community level for instance, education; at the enterprise level and the level of an Internet Service Provider which can be a more advance level.

Table 2.6: Several cloud platforms comparison (Junjie, et al., 2009, p.26).



	Abicloud	Eucalyptus	Nimbus	OpenNebula
cloud character	publich/private	public	public	private
scalability	scalable	scalable	scalable	Dynamical, scalable
cloud form	IaaS	IaaS	IaaS	IaaS
compatibility	Not support EC2	support EC2, S3	support EC2	open, multi-platform
deployment	pack and redeploy	dynamical deployment	dynamical deployment	dynamical deploymentt
deployment manner	web interface drag	commandline	commandline	commandline
Transplant-ability	easy	common	common	common
VM support	VirtualBox, Xen, VMware，VM	VMWare, Xen, KVM	Xen	Xen, VMWare
web interface	libvirt	Web Service	EC2 WSDL, WSRF	libvirt, EC2, OCCI API
structure	open platform encapsulate core	module	Lightweight components	module
reliability	-	-	-	rollback host and VM
OS support	Linux	Linux	Linux	Linux
development language	ruby, C++, python	Java	Java, Python	Java

According to table 2.6, Abicloud platform can be deployed as a Private cloud, Public cloud or Hybrid and it is suitable for the IaaS cloud infrastructure (Junjie, et al., 2009, p.24). Eucalytus as illustrates in figure 2.30 on the other hand, is a platform more suitable for the Public cloud model only for an IaaS infrastructure.

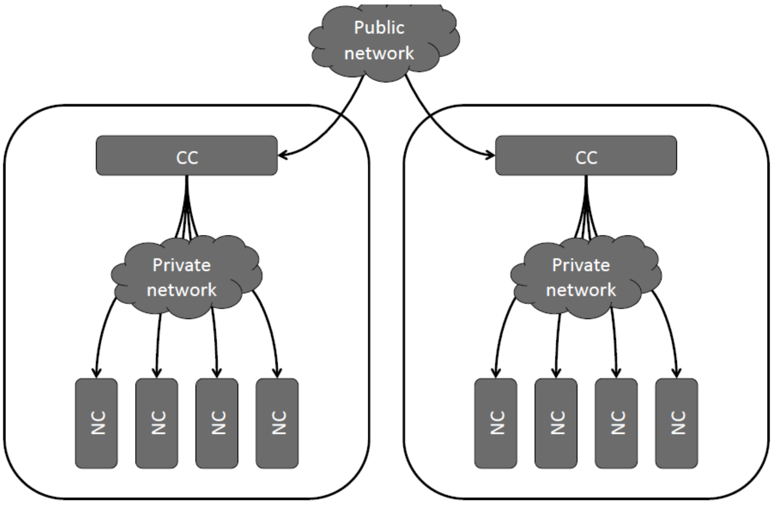


Figure 2.30: Eucalyptus cloud computing system (Nurmi, et al., 2009).

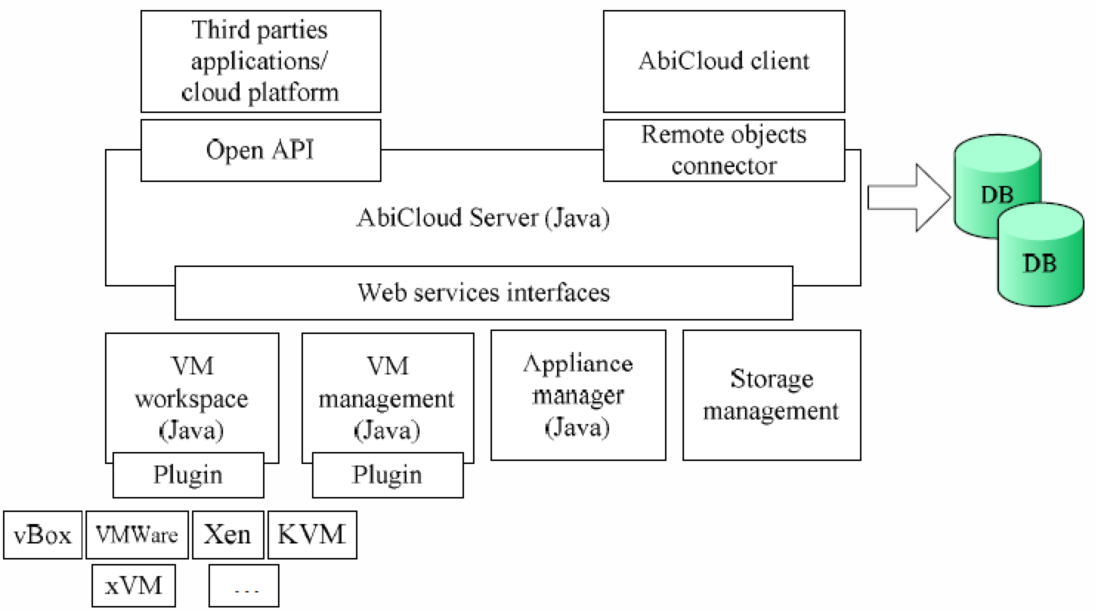


Figure 2.31: Abicloud platform architecture (Junjie, et al., 2009, p.24).

The Nimbus platform shown in figure 2.31 is running with the Xen support. Nimbus is similar to the Eucalyptus platform suitable for Public cloud model only and it can be deployed as an IaaS infrastructure.

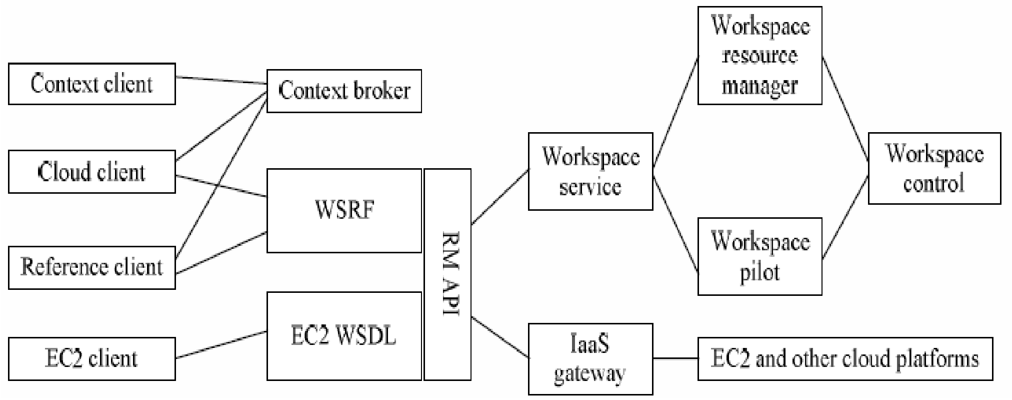


Figure 2.32: The Nimbus platform architecture (Junjie, et al., 2009, p.25).

Section 2.6.3 reviews the various services offered by the cloud computing technologies.

2.6.3 Cloud Service Implications

There are three services that are associated with Cloud computing are: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) as shown in figure 2.32 (Pokharel, et al., YoungHyun, 2009, p.1).

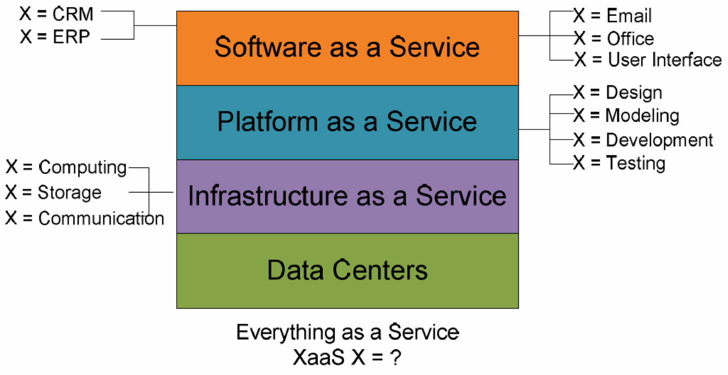


Figure 2.33: Services offered by Cloud computing (Wei-Tek, et al., 2010, p.684).

The illustration shown in figure 2.32 portrays a hierarchical view of cloud computing. At the bottom layer it shows the data centre, this layer is the basis of a cloud computing infrastructure. The data centre holds all the hardware that responsible for driving the cloud infrastructure (Wei-Tek, et al., 2010, p.684). SaaS model is deployed as a pay-as-you-go model. SaaS providers offer software applications which are accessible over the Internet by the users. The advantage of this model is that, there is no need to worry about powerful hardware to run resource hungry applications through SaaS and only pay for use (Yusoh & Maolin, 2012, p.1).

PaaS model is very similar to SaaS however; PaaS users have access to development tools to develop their own programme such as Google Apps and Microsoft Windows Azure (Wenbo, et al., 2012, p.395). IaaS is the final cloud model appears to be the most attractive cloud computing model to businesses. Apart from the fact that there is no need to purchase expensive hardware, software and license, businesses can pay per use. One of the IaaS model advantages is instant scalability. IaaS provides its client with a platform that is built on virtualisation to its clients (Bu Sung, et al., 2011, p.335). These days cloud is said to be the next big thing however, every big thing will always have challenges and issues (Hasteer, et al., 2013, p.4). Section 2.6.4 is designed to highlight the challenges and issues with regards to privacy and security in the cloud.

2.6.4 Privacy and Security

To organisations and even individuals, security and privacy is a major issue when a third party is involved with private information. The Cloud Security Alliance (CSA) released a report on a study conducted by their Cloud Vulnerability Working Group 2013, their study found that the three top vulnerabilities which are responsible for 64% of all incidents are: Insecure Interfaces and APIs, Data Loss and Leakages and Hardware Failure (Cloud Security Alliance, 2013, p.1).

When it comes to the issues of privacy and confidentiality, it is very challenging when a third party is involved. The control is dependent on the third party service provider and most of the time users do not know what happens to their data (Hayes, 2008, p.11). However, to comply with the regulations, clients are still responsible for the security and integrity of their data even when data storage is outsourced. Cloud storage has an open and multi-tenant environment which raises the concerns regarding data security and privacy protection (Deyan & Hong, 2012, p.648). The main concern emerges from the fact that cloud providers cannot warranty physical separation of users' data in the cloud storage (Mollah, et al., 2012, p.5).

2.6.5 Data Storage in the Cloud

Data storage is referred to as a *"Game Changer"*, at the end of 2011 there were about 150 million subscribers and reached around 500 million subscribers at the end of 2012. This growth is expected to reach 625 million subscribers by the end of 2013 and double by the end 2017 (Sangani, 2013, p.82). Figure 2.33 provides a simple architecture of the cloud computing data storage. Data storage in cloud computing consists of thousands of cloud storage devices that are networked as illustrated in figure 2.33. The system utilises distributed file systems working together with network protocols to control access rights to the file system (Talib, et al., 2011, p.127). Storing data in the cloud storage does not engage the same concept as storing data on local network data storage.

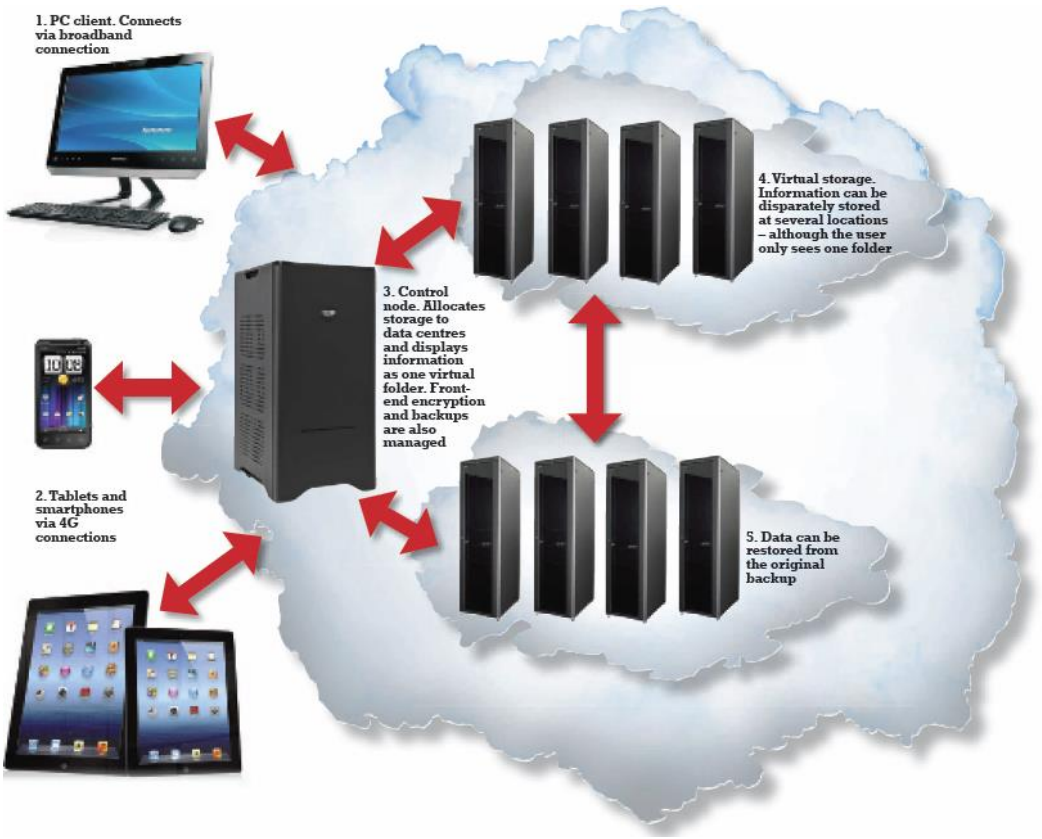

1. PC client. Connects via broadband connection
4. Virtual storage. Information can be disparately stored at several locations – although the user only sees one folder
3. Control node. Allocates storage to data centres and displays information as one virtual folder. Front-end encryption and backups are also managed
2. Tablets and smartphones via 4G connections
5. Data can be restored from the original backup

Figure 2.34: Data storage architecture in the cloud (Sangani, 2013, p.82).

In cloud computing, user data is stored on several third party servers but not on dedicated servers as in LAN environment (Kumar, et al., 2012, p.337). When a user transfers data into cloud storage, the user sees a virtual server and from the user’s point of view, the data will be on that server. However, that location does not really exist. The name given by the provider is an alias that refers to a computer-generated space in the cloud storage system. The user’s data location could be on one or more of the servers that are employed to form the cloud storage system (Itani, et al., 2009, p.713). Regardless of the location of the user’s data, the user can see and manage it as if the data is located locally.

The cloud computing storage system in figure 2.33, the architecture showed a basic cloud storage system with only one master control server that connects to the Internet. When the user accesses the cloud storage system over the Internet via a web-based interface, the user connects direct to the master control server. This server is responsible for displaying of the information to the user which will look like as if there is only one directory. The master control server is also responsible for allocating user’s data into the data centre. The master control server is also responsible for managing of data's front-end encryption and data backups as well (Sangani, 2013, p.82). There are various algorithms employed by cloud providers in the process of storing and retrieve data when user's request it. However, figure 2.34 shows one the algorithms known as PDDS proposed by Selvakumar, et al., (2013, p.7). This particular algorithm utilises a data partitioning technique for storing data in the cloud storage. Yet, it also improves data security by employing an integrity checking protocol to detect data corruption and server irregularities.

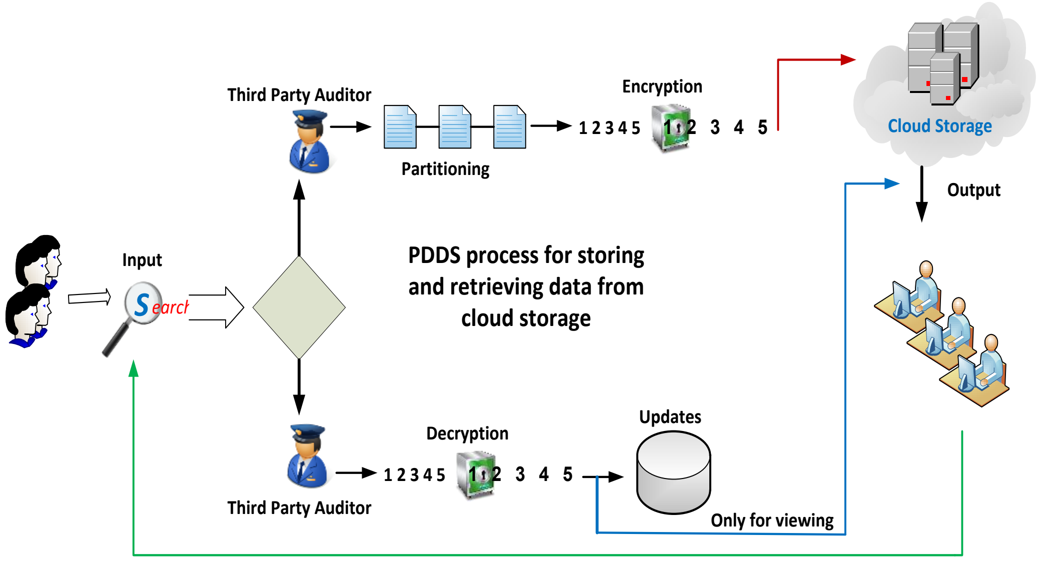


Figure 2.35: PDDS process for cloud data storage (Selvakumar, et al., 2013, p.10).

The particular algorithm allows the user to remotely check the integrity of the data. The encryption technique employed by the PDDS algorithm can generate private and public keys before the data is sent to the storage. The private key is symmetric and 2048 bit in length while public key uses asymmetric encryption and randomly generated. These keys are used for encrypting and decrypting of the data which add another layer of protection.

Another feature of PDDS is known as partitioning. Partitioning is referred to the process of dividing large data file sizes into several smaller file sizes. The algorithm checks the data file before sending it to the storage, if it is more than the allowed file size than perform partitioning method. When partitioning is done than the extensions and index value will apply. The files will then be encrypted before sending them to the data storage as illustrated in figure 2.34. In terms of retrieving those files, PDDS will just look at the index value and count, if they are match then decrypt them before reassembling the files for the user (Selvakumar, et al., 2013, p.10). PDDS algorithm partitioning feature is said to be very effective especially for storing and retrieving of user’s data from the cloud storage. Another layer of protection is added on top to ensure data integrity.

2.7 CONCLUSION

In conclusion, this chapter has provided a justification for the selection of the literature for this thesis (section 2.1). It has defined in detail wireless business systems (section 2.2) and SMART device operating systems (section 2.3). In section 2.4 the devices themselves have been defined and the capabilities specified. In section 2.5 the networks that are utilised by business people in enterprise systems are defined by type, kind and protocols. Section 2.6 reviews cloud computing environments and the architectures that are available for business use. The scope of the Information Technology (IT) that this thesis is concern with is now specified. In addition sufficient attention to detail allows the transfer of knowledge for people involved with investigating crimes to be confident a system and its dependencies and links can be systematically traced.

In chapter 3 the next group of knowledge is to be reviewed from the literature. Chapter 3 is concerned with the methodologies, models and guidelines that are used by investigators when investigating digital crime and the search for digital evidence. The focus remains on SMART technology business environments.

Chapter Three

Digital Forensic Techniques & Investigation Models: Literature Review

3.0 INTRODUCTION

This chapter broadens the literature review from technical environments for SMART business devices and digital evidence contexts reviewed in chapter 2, to look directly at guidelines and investigation models that are currently and historically applied to digital evidence. It also starts by reviewing the tools available to digital forensic investigators that have potential application in SMART device environments (as reviewed in chapter 2). The analysis of the literature suggests that much more can be done to improve the readiness and the relevance of current models and methods of investigation and to better meet the demands of the technologies defined in chapter 2. Chapter 3 concludes with the theoretical analysis of 12 digital investigation models. From the apparent gaps and redundancies identified in the analysis a “STRAW MAN” investigation model is constructed for scenario testing and improvement in chapter 4. Consequently chapter 3 has three main sections: Tool Review (3.1), Investigation Guideline Review (3.2), and the Literature Analysis (3.3). The analysis reveals the gap in literature for this thesis and from the analysis a “STRAW MAN” investigation model can be constructed for testing and improvement (3.4).

3.1 DIGITAL FORENSIC TOOL ENVIRONMENTS

Each mobile device developer has their own interpretations of what their potential customers would prefer to see on a mobile device. As a result, each device has its own characteristics in terms of hardware and software. Software with regards to the operating system that mediate between the device’s hardware and third party applications on the device such as iOS, Android and Windows mobile (See section 2.3). Not only that but also various types of network that provides these devices with the ubiquitous connectivity such as 3G on TDMA, on GSM or WCDMA, Wi-Fi and Bluetooth WLAN, WMAN or WWAN (Mohtasebi & Dehghantanha, 2013, p.351). (See section 2.5).

This section provides an overview of digital forensic tools that are currently in use at the present time in accordance with the scope of the literature reviewed. Each tools' capabilities are outlined in terms of acquiring and analysing evidence.

3.1.1 Definitions

It is now a challenge to digital forensic investigators to stay abreast of both new and emerging technologies in the field. Mobile SMART devices are used for both personal and professional purposes. Due to the omnipresence nature of these devices, they play substantial role in digital crime. Regardless of their differences, they all carry precious information that can be vital to an investigator (Mohtasebi & Dehghantanha, 2013, p.351).

To obtain data from a mobile device for forensic analysis, the investigator needs the help of a tool and often several. Due to the differences in terms of the technologies employed by these devices, investigators will have to engage different methods and tools depending on the devices involved (Albano, et al., 2011b, p.381). The most challenging part is data acquisition especially acquiring data from volatile memory (Dezfouli, et al., 2012, p.186). As described in the NIST Special Publication 800-101, mobile device forensics is the art of employing science to extract digital evidence from a mobile device under forensically compliant conditions while employing accepted techniques (Jansen & Ayers, 2007, p.6).

3.1.2 Data Acquisition

Procuring data from a compromised mobile device can be vital evidence for any digital crime. Thus, due to the fact that technology has rapidly advanced over recent years, this advancement has changed the way people do business and live their personal lives. Digital data on mobile devices has three known properties - they are easy to copy, easy to modify and difficult to acquire (Lin, et al., 2011, p.386; Yadav, et al., 2011, p.437). Therefore, prior to acquiring data from a mobile SMART device, extra pre-cautions must be taken, standard procedures and base practices must be followed carefully. This process is purposely implemented in order to preserve the integrity of the data or change the state of the device (Jansen & Ayers, 2007, p.45). Figure 3.1 shows the relationship of various fields of digital forensic.

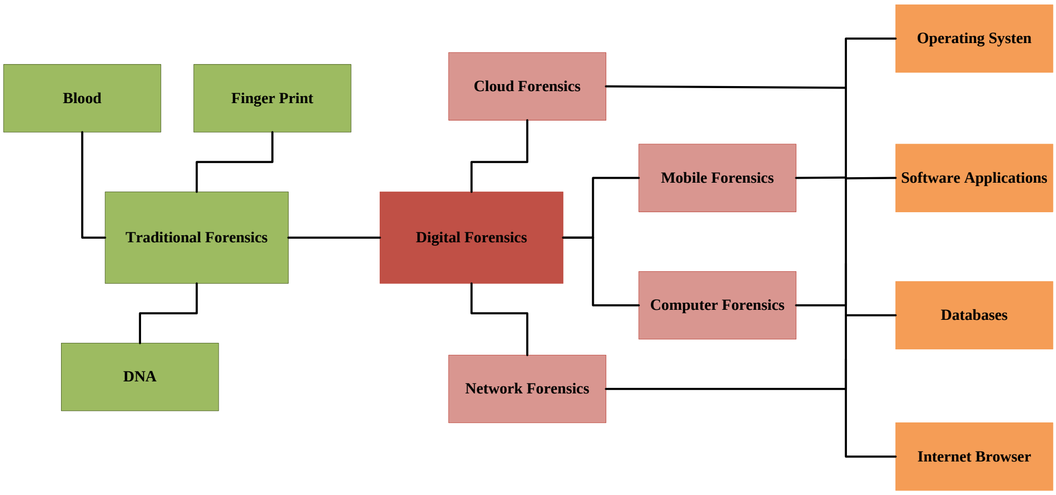


Figure 3.1: Various fields of Digital Forensic.

Digital forensic is the art of employing computer technology in order to identify, preserve, analyse and report digital evidence gathered from a compromised device (Achi, et al., 2008c, p.263). As illustrated in figure 3.1, in digital forensic, there are four main areas - Computer forensics, Network forensics, Cloud forensics and forensic investigation on Mobile SMART devices (Lin, et al., 2011, p.387). Regardless of the area of relevance, to start off an investigation, number one is to *"identify"*. To satisfy the identification phase, data will have to be extracted from the target device. However, the four areas of digital forensic also required different techniques with regards to data acquisitions. As a result, a focus is required on the business mobile SMART devices such as phones and tablets.

In terms of data acquisition, extracting data from mobile SMART devices is different from obtaining data from a computer. In the case of a computer, the hard disk can be isolated and start the investigation. For that reason, the forensic investigator will only work with a clone and not the actual data. However, trying to extract data from the SMART phone's internal memory is more challenging (Jansen & Ayers, 2007, p.6; Fang, et al., 2012, p.130). The most important component of this practice is to warrant the integrity of potential evidences. Accordingly, certain principles and standards must be met so that the findings can be admissible in the court of law (Jansen & Ayers, 2007, p.25).

Extracting data from mobile SMART devices can be accomplished in two ways, logical or the physical acquisition methods. However, Liu, et al. (2012)

argues that there are three methods which are Logical, Physical and Manual acquisition (p.149).

3.1.2.1 Logical Acquisition

The logical acquisition approach is achieved by using software tool which extracts a bit-by-bit copy of the active data in logical storage such as files and directories only (Ayers, 2007, p.1). However, the device's memory also contains information such as data that has been deleted. This is not recoverable through logical or the manual acquisition approach (Jansen & Ayers, 2007, p.46).

Forensic software tools are designed to gather for a wide variety of mobile devices. Even so, these tools often fall short and accomplish extracting data logically by employing common protocols for synchronisation (Ayers, 2007, p.1). Logical acquisition methods are quick, easy to use, reliable and 100% forensically secure. The logical acquisition technique can only the active data including phone book lists, call logs, calendar contents, appointments, Internet browsing history, text messages, photos and so on (Mislan, 2010, p.37). Therefore, the logical acquisition tool acts together with the mobile device's operating system (Dezfouli, et al., 2012, p.186). Thus, the tool obtains logical objects that are stored in the SMART device's file and directory systems, rather than the raw image of a memory chip (Jansen & Scarfone, 2008, p.2-1).

3.1.2.2 Physical Acquisition

Physical acquisition refers to the extraction of a bit-by-bit copy of the entire physical data storage of the device such as a disk drive, RAM or Flash memory. The main difference between these two approaches is, the logical acquisition tool processes the device through the device's operating system. The operating system can only provide a logical view of the device's storage space. The physical acquisition tool can see the device's memory the same way as the other hardware components which are a physical view (Ayers, 2007, p.10).

The physical acquisition technique can give forensic investigators more data than the logical method. This is because the physical acquisition tool can generate a comprehensive and an all-inclusive image of the phone's memory bit-by-bit. All-inclusive means, the digital forensic physical acquisition tool can also extract the deleted data. Yet, true physical acquisition is very intrusive and destructive. The technique employed involves physically removing of the memory from the device or gaining low level access to the device via the bootloader. These techniques are very risky in terms of the possibility of affecting the data on the device and even destroying it (Klaver, 2010, p.151).

In addition, physical acquisition technique can also bypass the handset's security code. However, in computer forensics, the computer can be easily isolated and its hard drive can be removed for analysis. In the mobile forensics domain, attempting to do the same to the device's internal memory can risk permanent damage to the device's memory or circuit board (Grispos, Storer & Glisson, 2011, p.23). Regardless, physical acquisition is vital to forensic investigators due to its ability to extract deleted data, and any data present in the unallocated space of the memory or the unused space of the filesystem (Ayers, 2007, p.10).

3.1.3 Manual Acquisition

Liu, et al. (2012) suggested that manual acquisition can employ the user interface of the device to obtain data from the device's memory. Manual acquisition has an advantage because the device's operating system can resolve the raw data format obtained from the device's memory in to a format that human can understand. However, the drawback of this technique is that, only the data that is detectable to the operating system can be obtained (p.149).

The manual acquisition approach is based on observing the device's user interface, and fully extraction of evidences when other techniques are not possible (Grispos, et al., 2011, p.31).

3.1.4 Digital Forensic Tools Performance

As mentioned earlier, obtaining evidence from any digital device requires the help of a tool and every digital forensic tool is different in its core set of features (NIST, 2013, p.4). Obtaining data from mobile SMART devices on the other hand is a challenge on its own because there is no known standard file system. So, to gain a better understanding of a file system, the differences have to be understood. The tools that can be used to acquire data from a PC can easily bypass evidence in the SMART device operating system because, SMART devices may not have a

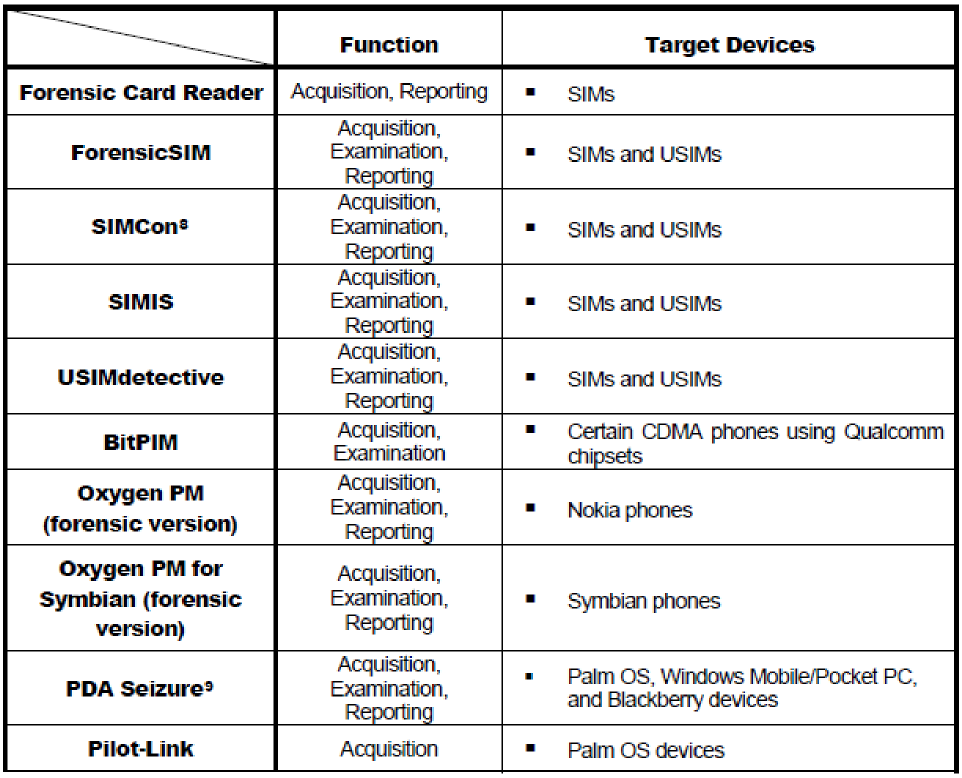
standardised format in place for the organisation of the data on a computer hard drive, for instance FAT, NTFS, ext, HFS etc., (Yadav, et al., 2011, p.437).
Mobile SMART devices on the other hand, despite the fact that almost same kinds of information can be retrieved from these devices such as call history record, phone book list, text messages and so on; the operating system's file system formats are different (Bader & Baggili, 2010, p.1). As a result, digital SMART device forensics investigator will need to engage different data acquisition tool depending on the target device. Thus, it is impossible to make a complete copy of the entire phone. Available commercial tools and also the open source tools have a common problem; the tool can only extract part of the data on the device. In addition, forensic tools for mobile phones have limited functions when compared with the available tools for computer forensics (Mohtasebi & Dehghantanha, 2013, 353).

Despite the fact that a lot of elements contribute to making one SMART mobile device, there are core sets of data that forensic tools can recover. These sets of data can be found on the device's internal memory and associated media. These data sets including the International Mobile Equipment Identifier (IMEI) on GSM device memory, Mobile Equipment Identifier (MEID) on CDMA device, Personal Information Management (PIM) data for instance, address book, calendar entries, tasks and memos.

On the SIM memory, the Service Provider Name (SPN) can be found and also the International Mobile Subscriber Identity (IMSI). On the device's memory, data created by applications on the device can also be located and Internet data as well such as bookmarks, history of visited websites. Also data such as call logs and last number dialled and text messages can found on the devices internal memory. Part of the core data sets is the location data and GPS related data (Ayers, 2007, p.119). There are a number of tools appearing in the digital forensic domain which have not been validated or verified scientifically. These tools have only been tested by their developers so; digital forensic practitioners have seen this to be a challenge. Even though there are a wide selection of forensic tools available but the forensic personnel has to consider the admissibility of evidence obtained. As a result, it is crucial for an investigator to know the reliability and accuracy of the tool engaged in an investigation before using it (Kubi, Saleem & Popov, 2011, p.2).

With regards to digital forensic tool performance, the National Institute of Standards and Technology (NIST) have conducted a test on various forensic tools. NIST test results provided in table 3.1 identify the services that each tool provides. These services are data acquisition, examination or reporting. This test was conducted on mobile phones.

Table 3.1: Digital forensic tools test results (Jansen & Ayers, 2007, p.16).



	Function	Target Devices
Forensic Card Reader	Acquisition, Reporting	▪ SIMs
ForensicSIM	Acquisition, Examination, Reporting	▪ SIMs and USIMs
SIMCon[8]	Acquisition, Examination, Reporting	▪ SIMs and USIMs
SIMIS	Acquisition, Examination, Reporting	▪ SIMs and USIMs
USIMdetective	Acquisition, Examination, Reporting	▪ SIMs and USIMs
BitPIM	Acquisition, Examination	▪ Certain CDMA phones using Qualcomm chipsets
Oxygen PM (forensic version)	Acquisition, Examination, Reporting	▪ Nokia phones
Oxygen PM for Symbian (forensic version)	Acquisition, Examination, Reporting	▪ Symbian phones
PDA Seizure[9]	Acquisition, Examination, Reporting	▪ Palm OS, Windows Mobile/Pocket PC, and Blackberry devices
Pilot-Link	Acquisition	▪ Palm OS devices

As illustrated in table 3.1, the tools involved in this test were grouped into two exclusive groups, SIM or the handset. The test results showed that the performance of forensic tools is limited to certain hardware with a particular operating system (Jansen & Ayers, 2007, p.16). Table 3.1 showed that most of the tools involved in this test were able to deliver all three services except for the Pilot-Link tool can only acquire the data from Palm OS devices. It is recommended not to utilise tools that were not specifically developed for digital forensic investigation purposes. These tools extracted data from the device for analysis however, they also allow certain data to be rewritten onto the device (Jansen & Ayers, 2006, p.107).

An experiment conducted by Grispos, et al., (2011) tested and compared eight different digital forensic tools. In this experiment, the authors also tested the abilities of these tools with a Windows mobile SMART phone. The experiment was conducted including the three main forensic data acquisition methods as shown in figure 3.2.

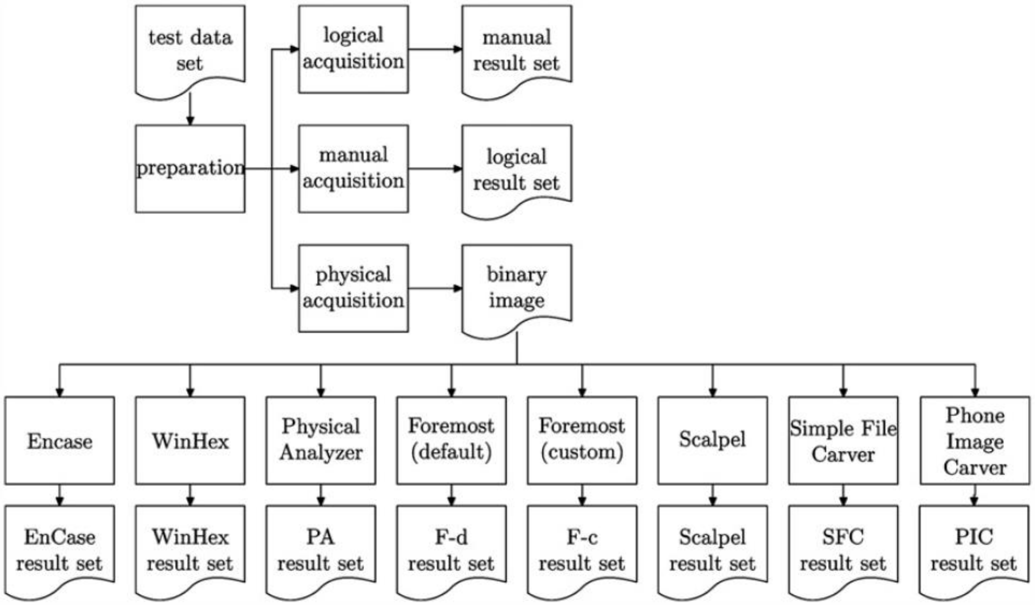
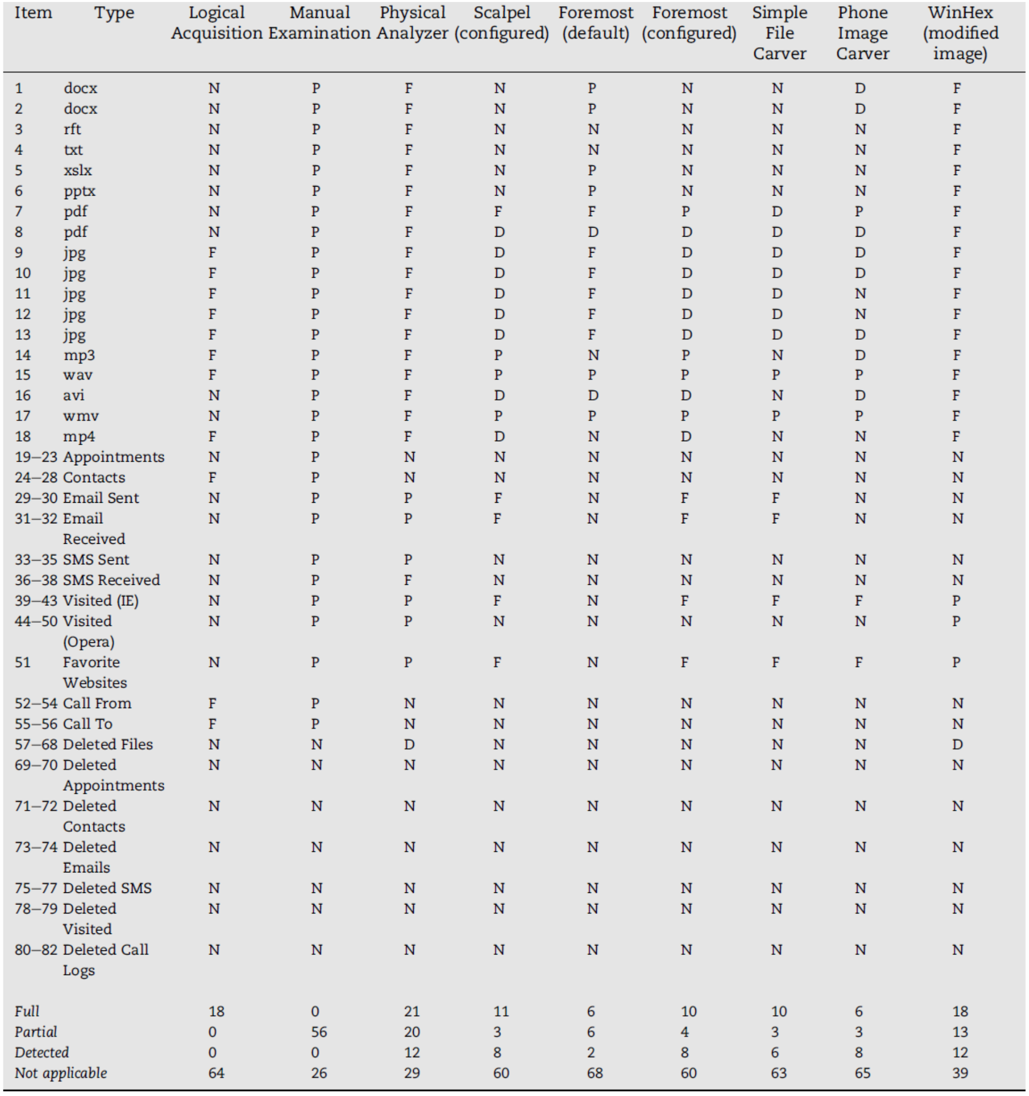


Figure 3.2: Experiment progressions (Grispos, et al., 2011, p.27).

The experiment results showed that a range of various data were recovered from the Windows based mobile SMART device. However, the data acquisition results were also varied depending on the tools and methods employed. As a result, the authors argued that their study has showed that it is possible to extract data from the device's memory by employing combinations of tools. Table 3.2 provides a complete view of the results. Table 3.2 also demonstrated each tool performance under each data acquisition technique employed. The authors also pointed out that the existing forensic tools showed weaknesses when extracting data from partially corrupted file system. For instance, the Physical Analyser tool cannot process and decode the data while the FTK and Encase tool kits were unable to process the image at all (Grispos, et al., 2011, p.35).

Another digital forensic tool test conducted at Norwich University focused on the features, ease of use, documentation, support and value for money of the tools involved. The test was aimed to compare and determine whether these tools actually produced what the developers claimed them to be. Table 3.3 and 3.4 outlines the findings from this study when the tools functionalities were compared against its advertised specifications (Dailey, 2012, p.50).

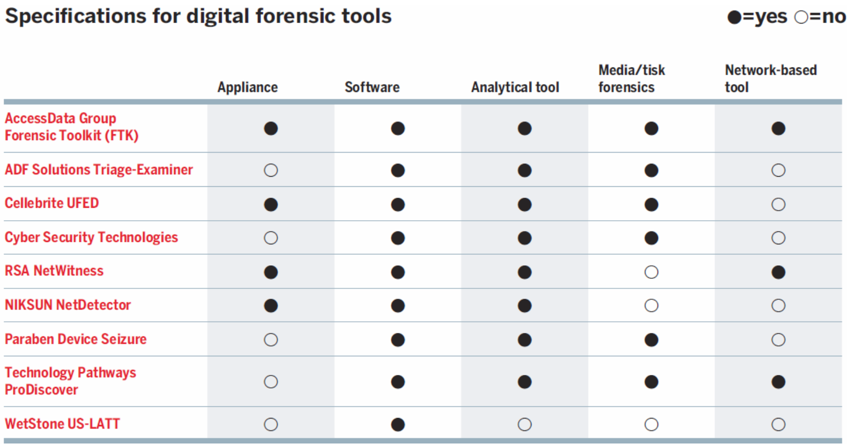
Table 3.2: Experiment results (Grispos, et al., 2011, p.30).



Item	Type	Logical Acquisition	Manual Examination	Physical Analyzer	Scalpel (configured)	Foremost (default)	Foremost (configured)	Simple File Carver	Phone Image Carver	WinHex (modified image)
1	docx	N	P	F	N	P	N	N	D	F
2	docx	N	P	F	N	P	N	N	D	F
3	rft	N	P	F	N	N	N	N	N	F
4	txt	N	P	F	N	N	N	N	N	F
5	xslx	N	P	F	N	P	N	N	N	F
6	pptx	N	P	F	N	P	N	N	N	F
7	pdf	N	P	F	F	F	P	D	P	F
8	pdf	N	P	F	D	D	D	D	D	F
9	jpg	F	P	F	D	F	D	D	D	F
10	jpg	F	P	F	D	F	D	D	D	F
11	jpg	F	P	F	D	F	D	D	N	F
12	jpg	F	P	F	D	F	D	D	N	F
13	jpg	F	P	F	D	F	D	D	D	F
14	mp3	F	P	F	P	N	P	N	D	F
15	wav	F	P	F	P	P	P	P	P	F
16	avi	N	P	F	D	D	D	N	D	F
17	wmv	N	P	F	P	P	P	P	P	F
18	mp4	F	P	F	D	N	D	N	N	F
19–23	Appointments	N	P	N	N	N	N	N	N	N
24–28	Contacts	F	P	N	N	N	N	N	N	N
29–30	Email Sent	N	P	P	F	N	F	F	N	N
31–32	Email Received	N	P	P	F	N	F	F	N	N
33–35	SMS Sent	N	P	P	N	N	N	N	N	N
36–38	SMS Received	N	P	F	N	N	N	N	N	N
39–43	Visited (IE)	N	P	P	F	N	F	F	F	P
44–50	Visited (Opera)	N	P	P	N	N	N	N	N	P
51	Favorite Websites	N	P	P	F	N	F	F	F	P
52–54	Call From	F	P	N	N	N	N	N	N	N
55–56	Call To	F	P	N	N	N	N	N	N	N
57–68	Deleted Files	N	N	D	N	N	N	N	N	D
69–70	Deleted Appointments	N	N	N	N	N	N	N	N	N
71–72	Deleted Contacts	N	N	N	N	N	N	N	N	N
73–74	Deleted Emails	N	N	N	N	N	N	N	N	N
75–77	Deleted SMS	N	N	N	N	N	N	N	N	N
78–79	Deleted Visited	N	N	N	N	N	N	N	N	N
80–82	Deleted Call Logs	N	N	N	N	N	N	N	N	N
Full		18	0	21	11	6	10	10	6	18
Partial		0	56	20	3	6	4	3	3	13
Detected		0	0	12	8	2	8	6	8	12
Not applicable		64	26	29	60	68	60	63	65	39

Keys that the authors used in Table 3.2 are F = Full, P = Partial, D = Detected and N = Not.

Table 3.3: Experiment results (Dailey, 2012, p.51).

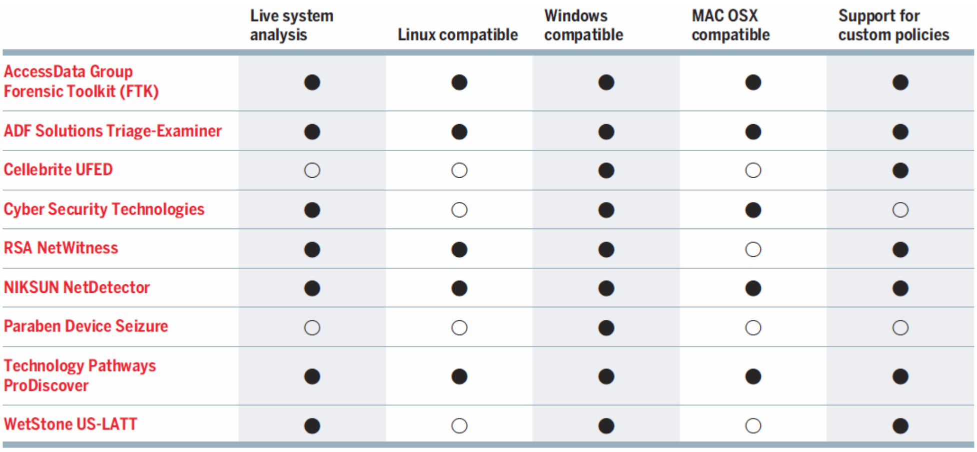


Specifications for digital forensic tools ●=yes ○=no

	Appliance	Software	Analytical tool	Media/tisk forensics	Network-based tool
AccessData Group Forensic Toolkit (FTK)	●	●	●	●	●
ADF Solutions Triage-Examiner	○	●	●	●	○
Cellebrite UFED	●	●	●	●	○
Cyber Security Technologies	○	●	●	●	○
RSA NetWitness	●	●	●	○	●
NIKSUN NetDetector	●	●	●	○	○
Paraben Device Seizure	○	●	●	●	○
Technology Pathways ProDiscover	○	●	●	●	●
WetStone US-LATT	○	●	○	○	○

Table 3.3 showed the nine tools selected for this study. The results also highlighted the ability in terms of features and functionalities.

Table 3.4: Experiment results (Dailey, 2012, p.51).



	Live system analysis	Linux compatible	Windows compatible	MAC OSX compatible	Support for custom policies
AccessData Group Forensic Toolkit (FTK)	●	●	●	●	●
ADF Solutions Triage-Examiner	●	●	●	●	●
Cellebrite UFED	○	○	●	○	●
Cyber Security Technologies	●	○	●	●	○
RSA NetWitness	●	●	●	○	●
NIKSUN NetDetector	●	●	●	●	●
Paraben Device Seizure	○	○	●	○	○
Technology Pathways ProDiscover	●	●	●	●	●
WetStone US-LATT	●	○	●	○	●

Table 3.4 shows the ability of each tool to work on different platforms such as Linux, Windows or the Apple Macintosh operating system. Another approach was taken in order to test the performance of digital forensic tools available to investigators. Glisson, et al. (2013) compared and evaluated data sets recovered using various data acquisition techniques. In this test, the authors evaluated and compared the extracted data sets for completeness and the verifiability of the results based on the data acquisition technique employed (p.45).

There were a number of mobile devices involved in this test and the SMART phones that were involved were iPhone 3G, Blackberry and several Android devices. The digital forensic tools employed were the Cellebrite's Universal Forensic Extraction Device (CUFED), the XRY Forensics' Examination Kit (XRY) and the Radio Tactics' Aceso (RTA). These tools collectively provided the investigator with six data acquisition methods. For instance, the CUFED is capable of Physical, Logical and File recovery methods while XRY can only do Logical and Physical acquisition. The RTA tool can only offer Logical data acquisition (Glisson, et al., 2013, p.45).

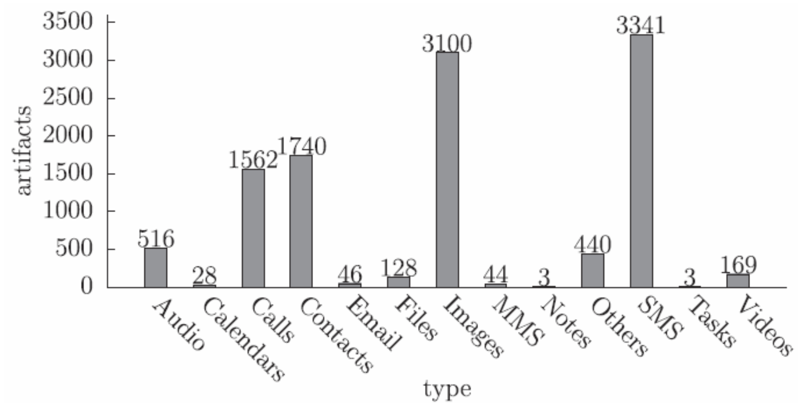


Figure 3.3: Summary of data types recovered (Glisson, et al., 2013, p.46).

Figure 3.3 provides a summary of the types of data that were obtained from the devices involved in the test. For instance, 516 audio files were found while 3341 text messages found. 3100 images were found also were the two highest but notes and tasks were the two lowest with only three artefacts each was found in the device. An illustration of the data acquisition techniques employed together with the tool used in figure 3.4 and also the success rate.

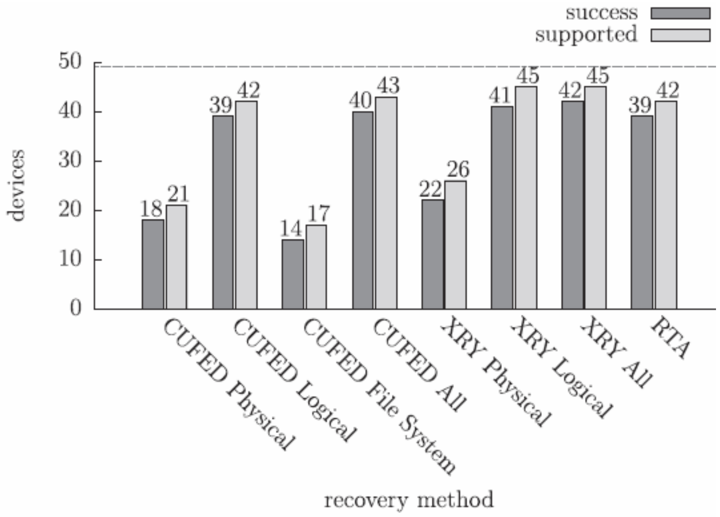
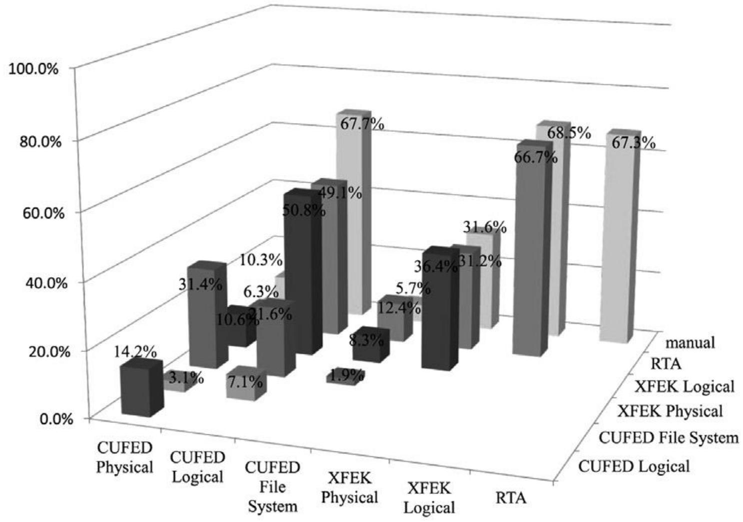


Figure 3.4: Data acquisition methods involved (Glisson, et al., 2013, p.47).

In figure 3.5, the authors showed and compared the results of data extracted by one forensic tool but different acquisition techniques. As a result, it is important for the investigator to know when to employ which tool and which acquisition method to apply. In figure 3.5, it is evident that the investigator may need more than one data acquisition method in order to obtain a more complete data out of the device involved (Glisson, et al., 2013, p.51).



(a) all artifacts

Figure 3.5: Verification rate of all techniques (Glisson, et al., 2013, p.51).

In spite of everything, all logical data can be acquired and analysed yet, tool developers seem to over claim their tool's capabilities while the tool can only obtain the contact list. As a result, forensic tools should be evaluated based on their abilities and not the costs. In this test, the author noted that the tool that had better support for the Apple SMART devices outperform the most expensive tools involved (Morrissey, 2010, p.130).

3.2 INVESTIGATION GUIDELINES

This section delineates an overview of the principles, approaches and techniques involved in the investigation of electronic crimes. Section 3.2.1 provides a brief definition of the term digital forensic and the processes involved. All these processes are aimed to help maintain the integrity and the credibility of potential evidences. Therefore, reputable organisations such as the Association of Chief Police Officers (ACPO) in the United Kingdom and the National Institute of Standards and Technologies (NIST) in the USA have also developed best practice guidelines to help digital forensic personnel with their investigations.

Section 3.2.2 and 3.2.3 discuss these two guidelines while section 3.2.4 provides a summary and a review of most of the existing investigation process models. This will be followed by an analysis in section 3.3 of the literature reviewed in section 3.2.4. The gap identified for this study is discussed in section 3.4 then followed by a summary of the issues and problems before the conclusion.

3.2.1 Definitions

Digital forensic is relatively still a new field of forensic investigation. The rapid growth in the development and usages of mobile SMART devices presents investigators with new challenges (Raghav & Saxena, 2009, p.5). Kent et al. (2006) stated that digital forensic is, "*considered the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data"* (p.9). Therefore, there is a need to maintain the integrity and credibility of digital evidences in order to be admissible in the court of law. Reputable organisations such as the ACPO in the United Kingdom and NIST in America made an effort to develop guidelines to help investigators. The following sections will explain the ACPO and NIST guidelines.

3.2.2 The NIST Guidelines

In the NIST Special Publication 800-101, Wayne Jansen and Rick Ayers explained that the purpose of their guideline is divided into two. The guideline is designed to help organisations in evolving proper policies and procedures for dealing with mobile phones. Not only that but to also prepare digital forensic experts in how to deal with new circumstances when they arise. The authors believed that employing their recommendations would facilitate efficient and effective digital forensic investigations on mobile devices (Jansen & Ayers, 2007, p.9). Table 3.5 following shows NIST guidelines.

Table 3.5: NIST guidelines for mobile device forensic (ACPO, 2007, p.9).

Organizations should ensure that their policies contain clear statements about forensic considerations involving cell phones.	At a high level, policy should allow authorized personnel to perform investigations of organizationally issued cell phones for legitimate reasons, under the appropriate circumstances. The forensic policy should clearly define the roles and responsibilities of the workforce and of any external organizations performing or assisting with the organization's forensic activities. The policy should also indicate internal teams and external organizations to be contacted under various circumstances.
Organizations should create and maintain procedures and guidelines for performing forensic tasks on cell phones.	Guidelines should focus on general methodologies for investigating incidents using forensic techniques. While developing comprehensive procedures tailored to every possible situation is not generally feasible, organizations should consider developing step-by-step procedures for performing all routine activities in the preservation, acquisition, examination and analysis, and reporting of digital evidence found on cell phones and associated media. The

	guidelines and procedures should facilitate consistent, effective, accurate, and repeatable actions carried out in a forensically sound manner, suitable for legal prosecution or disciplinary actions. The guidelines and procedures should support the admissibility of evidence into legal proceedings, including seizing and handling evidence properly, maintaining the chain of custody, storing evidence appropriately, establishing and maintaining the integrity of forensic tools and equipment, and demonstrating the integrity of any electronic logs, records, and case files. The guidelines and procedures should be reviewed periodically, and also whenever significant changes in cell phone technology appear that affect them.

The guidelines outlined in table 3.5 and table 3.6 are the recommendations from the NIST. It does not define how law enforcement and investigators handle mobile devices in an investigation. Yet, the guideline can be very helpful in setting policies and procedures (Jansen & Ayers, 2007, p.9).

Table 3.6: NIST guidelines for mobile device forensic (ACPO, 2007, p.10).

Organizations should ensure that their policies and procedures support the reasonable and appropriate use of forensic tools for cell phones.	Policies and procedures should clearly explain what actions are to be taken by a forensic unit under various circumstances commonly encountered with cell phones. They should also describe the quality measures to apply in verifying the proper functioning of any forensic tools used in examining cell phones and associated media. Procedures for handling sensitive information that might be recorded by forensic tools should also be addressed. Legal counsel should carefully review all forensic policy and high-level procedures for compliance with international, federal, state, and local laws and regulations, as appropriate.
Organizations should ensure that their forensic professionals are prepared to conduct activities in cell phone forensics.	Forensic professionals, especially first responders to incidents, should understand their roles and responsibilities for cell phone forensics and receive training and education on related forensic tools, policies, guidelines, and procedures. Forensic professionals should also consult closely with legal counsel both in general preparation for forensics activities, such as determining which actions should and should not be taken under various circumstances. In addition, management should be responsible for supporting forensic capabilities, reviewing and approving forensic policy, and examining and endorsing unusual forensic actions that may be needed in a particular situation.

3.2.3 Association of Chief Police Officers (ACPO) Guidelines

Sue Wilkinson, the Chair of the ACPO E-Crime working group explained that the guideline is essential considering the rapid growth in the advancement of today’s technologies. The guideline is designed to warrant that appropriate practices and procedures are followed. Acquiring digital evidences while trying to maintain its integrity may seem a challenge however, if it is done correctly than it will produce evidence that is irrefutable and is cost effective (ACPO, 2007, p.46).

The ACPO argued that even though the digital world has evolved but the principles of preserving evidences are still highly relevant. The ACPO guidelines consists of principles which are aligned with the G8 Lyon groups principles and provides the ACPO guidelines a basis for international comparison (ACPO, 2007, p.3). The following in table 3.7 are the four ACPO principles from the ACPO guidelines.

Table 3.7: ACPO guidelines four principles (ACPO, 2007, p.4).

Principle 1	No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.
Principle 2	In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
Principle 3	An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
Principle 4	The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

In addition to the principles outlined in table 3.7, there are other issues to consider especially when working with mobile devices. The investigator takes into consideration other forensic evidence such as DNA, fingerprints that can be obtained from the device. In that regards, the examining of the device without considering such evidence might destroy such vital evidences (ACPO, 2007, p.50).

3.2.4 Review Of Process Models

In summary, the two guidelines outlined in section 3.2.2 and section 3.2.3 both strongly recommend following strict policies and procedures. Compliance is required in order for the evidence obtained from the target device to be admissible in the court of law. The ACPO guideline sets out to ensure that proper practises and procedures are followed. The NIST guidelines are aimed at helping forensic experts in developing proper policies and procedures. Another purpose is to also prepare forensic practitioners for future technological changes (Owen & Thomas, 2011, p.135).

Pollitt (1995) from the Department of Engineering Technology at the University of Central Florida developed a model that contains four phases as illustrated in figure 3.6. In this model, the author defines clearly the relationship between the law and the digital investigation processes. As a result, in the data acquisition phase, the evidence must be acquired from the device in an acceptable manner with proper approval from an authority. For instance, the law specifies what can be seized, under what conditions, from whom, and from where it may be seized. The identification phase is divided into three steps.

Step one is looking at the evidence in its physical form, that is, its physical location on the media. Step two is concerned with the logical position of the evidence that it must be identifiable. The last step is dealing with the evidence conversion into a format that human can read and understand its meaning. The evaluation phase is concerned with evaluating of the gathered data to determine whether it is relevant to the case. Not only that but to also determine whether it can be considered as valid evidence. In the final phase, admission, the evidence identified and evaluated in the previous phases of the investigation is admitted in the court of law as evidence (Pollitt, 1995, p.489).

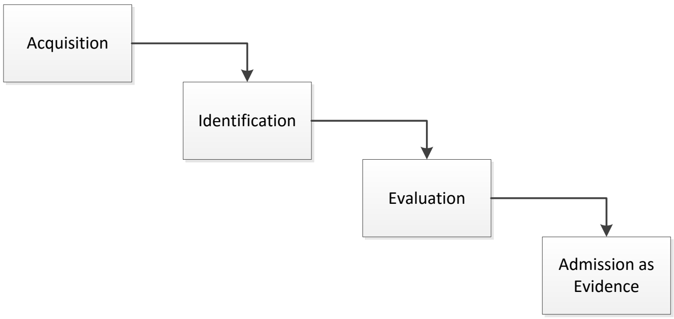


Figure 3.6: Computer Forensic Investigation Process (Based on Pollitt, 1995, p.489).

Pollitt's model was developed following a paper-based investigation process. In the first stage the task is to acquire the first document such as a search warrant or consent. In the second stage, the document will go through the identification process in order to determine its readability for instance, is it in English? In the digital world, this identification stage will concern with converting the binary data into a format that is readable by human. The evaluation stage is dealing with determining whether the information in the document is any relevant to the case.

Also determine who should be testifying regarding the information on the document. In terms of digital evidence, the investigator can make the same decisions in this stage.

Pollitt's model was developed for computer forensics however, the Digital Forensics Research Workshop (DFRW) proposed a general purpose digital forensics investigation process which comprises of six phases the first DFRW in 2001.

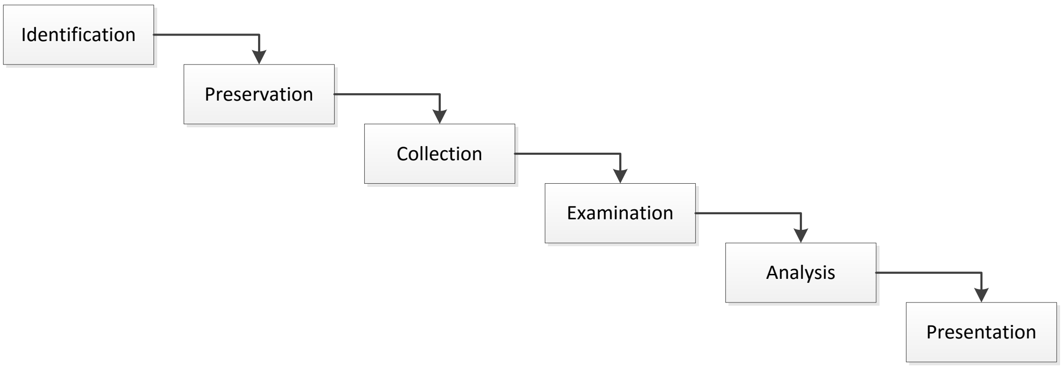


Figure 3.7: Computer Forensic Investigation Process (Based on Palmer & Corporation, 2001, p.17).

This model comprises of six phases (figure 3.7) and it was developed to provide investigators with a general investigation process for digital forensics. In the identification phase of the DFRWS model is concerned with event and crime detection. The identification phase is designed to resolve signature, identify the profile and anomalies, system monitoring and complaints and audit analysis. This is followed by the preservation phase which defines the case management processes including imaging technologies employed and the chain of custody.

The next phase, collection, is designed to ensure that evidence collection is performed by employing an approved and acceptable technique. This also includes utilising approved software and hardware tools only. In the examination and analysis phases, the phases are both dealing with tracing of the evidence however, in the examination phase, validating of the evidence collected and recovering of the hidden data is performed. The analysis phase is more focused on the mining of the data, timeline, protocols and also linking the data collected. In the final phase of the DFRWS model, presentation; this outlines the tasks such as documenting of the findings, dealing with expert testimony and also recommending counter measures.

In the year 2002, Reith, Carr & Gunsch, (2002, p.7) proposed a new digital forensic model (figure 3.8). This new model comprises of nine investigation phases and it is known as the "Abstract digital forensic model." The abstract digital forensic model has an iterative feature implemented between the examination phase and the analysis phase as it is illustrated in figure 3.8.

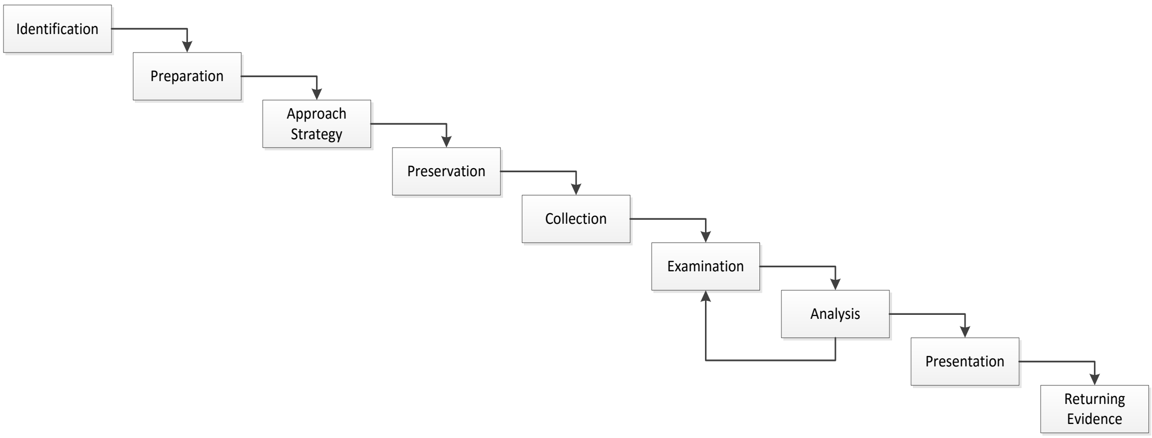


Figure 3.8: Abstract digital forensic model (Based on Reith, et al,, 2002, p.7).

In the identification phase of this model, it is designed to deal with recognising and determining the type of the incident. This is followed by the preparation phase which deals with tools, techniques, search warrant and authorisation and management. The third phase is the approach strategy phase that has a goal of maximising the collection of untainted evidence while minimising impact on the victim. In the fourth phase, it is concerned with preserving the state of the digital evidence. The fifth phase deals with the physical scene and duplicating of the digital evidence by employing standardised and accepted methods. In the sixth phase, the examination concerns the in depth examination of the evidence while the seventh phase deals with the analysis, reconstructing data and draw conclusion. The eighth phase concerns the presentation of the conclusion while the final phase deals with returning of physical and digital property to its rightful owner.

In 2003, Carrier and Spafford proposed a new forensic model known as *"An Integrated Digital Investigation Process"*. This Integrated Digital Investigation Process model consists of 17 phases organised into five groups (Carrier & Spafford, 2003, p.7) as it is illustrated in Figure 3.9.

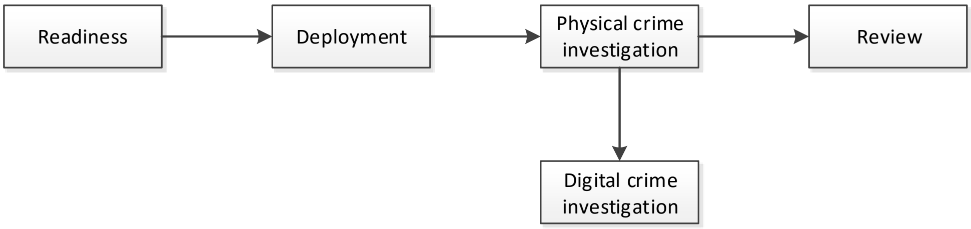


Figure 3.9: Phases of the IDIP Model
(Based on Baryamureeba & Tushabe, 2004, p.3).

The IDIP investigation process model is said to be adopting the theory that a computer itself is a crime scene. This is known as the digital crime scene and applies the digital crime scene investigation technique. The readiness phase is responsible for making sure that the operations and the infrastructure are capable of supporting fully the investigation. With digital and physical evidences, they are easy to be lost if are not gathered and maintained properly.

The readiness phase is an on-going and is not bound to a specific incident or crime. The deployment phase is devised to provide a system for an incident to be detected and confirmed. The physical crime scene investigation phase is aiming at collecting and analysing of the physical evidences and also the reconstruction of the incident. The digital crime scene investigation phase on the other hand is focusing on the digital devices obtained from a physical crime scene. The purpose of the digital crime scene investigation phase is to identify the electronic events that occurred on the system then present it to the physical crime scene investigation.

The final phase of the IDIP model is known as the review phase. The goal of the review phase is to review the whole investigation process in order to identify areas may require improvement. The results obtained from the review phase could be new procedures or new training however, if everything went as planned then no further action is required (Baryamureeba & Tushabe, 2004, p.5). In the year 2006, Rogers, et al. (2006) proposed a new digital forensic investigation model known as the "Computer forensic field triage process model" (CFFTPM). This computer forensic model was developed based on other two existing investigation process models in the field. These two process models are the *"Integrated digital investigation process model" (IDIP)* introduced by Carrier and Spafford in the year 2002 and the *"Digital crime scene analysis model" (DCSA)* introduced by Rogers in 2006.

The CFFTPM model consists of six primary phases and further six sub-phases as illustrated in figure 3.10. The planning phase of this model is devised to allow the lead investigator to quantify various possibilities of the crime scene. As the same time, identify various experts in the team. Immediately after the planning phase is the triage phase. The triage phase is known to be the fundamental of this process model. Along with proper planning, this phase is where the investigator needs to process the scene and rank pieces of evidence or potential containers of evidence in terms of importance or priority. Not only that but to also re-verify that the CFFTPM model is still valid.

The usage/user profile phase on the other hand is focusing on examining and analysing activities and user's profile on the digital media. This is conducted with a purpose of finding the link between the evidence obtained from the media to a specific identifiable suspect. It is vital information to an investigator when building a case to have the ability to construct the timeline. The Chronology/Timeline phase of the CFFTPM model provides the investigator with the chance to build the case from a chronological viewpoint by utilising the MAC time. This is defined by the temporal value of the digital evidence. Looking at the Windows MAC times for instance, modification is defined by when a file contents has been changed, access time is defined by when a file was viewed and creating time is defined by when a file was created.

The Chronology/Timeline phase is followed by the Internet phase; this is due to the fact that almost every case requires the examination of artefacts related to Internet activities such as e-mails and Internet browsing history. This phase allows the investigator to evaluate the type of Internet activities that is believed the suspect or victim were involved in and what is their relationship to the case.

The final phase of the CFFTPM model is known as Case Specific Evidence phase. This phase provides the investigator with the ability to adjust the focus of every examination to the specifics of the case and each specific set of circumstances. For instance: focusing the examination to the specifics of the case such as in, child pornography will definitely be different to that of drug activity cases. The graphical representation in figure 3.10 illustrates the phases and sub-phases of the CFFTPM process model.

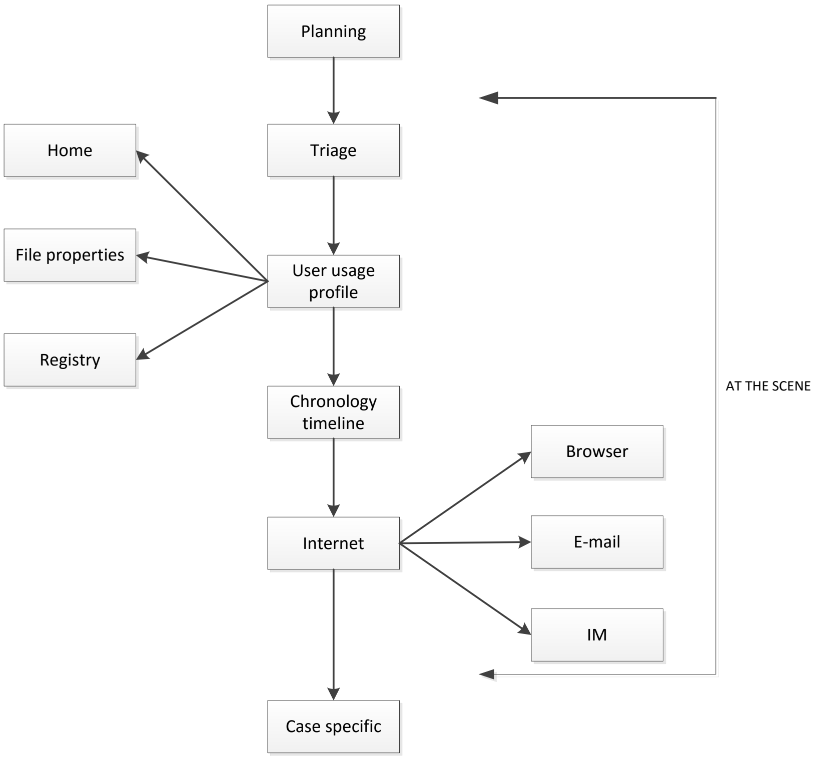


Figure 3.10: Phases of the CFFTPM model (Based on Rogers, et al., 2006, p.30)

The computer forensic field triage process model (CFFTPM) is a formalization of real world investigative approaches meaning that it was developed primarily based on child pornography cases. However, the model is general enough to be utilised in various cases such as financial fraud, identity theft, cyber stalking and even murder cases. Thus, the sub-phases of the model needs to be modified accordingly to suit the specifics of each case.

In 2007, a new investigation process model known as the common process model for incident and computer forensics was proposed by Felix Freiling from the University of Mannheim & Bastian Schwittay from Symantec Germany. This process model was developed with the purpose to conceptualise the processes of incident response and computer forensics into one framework in order to improve the overall process of investigation.

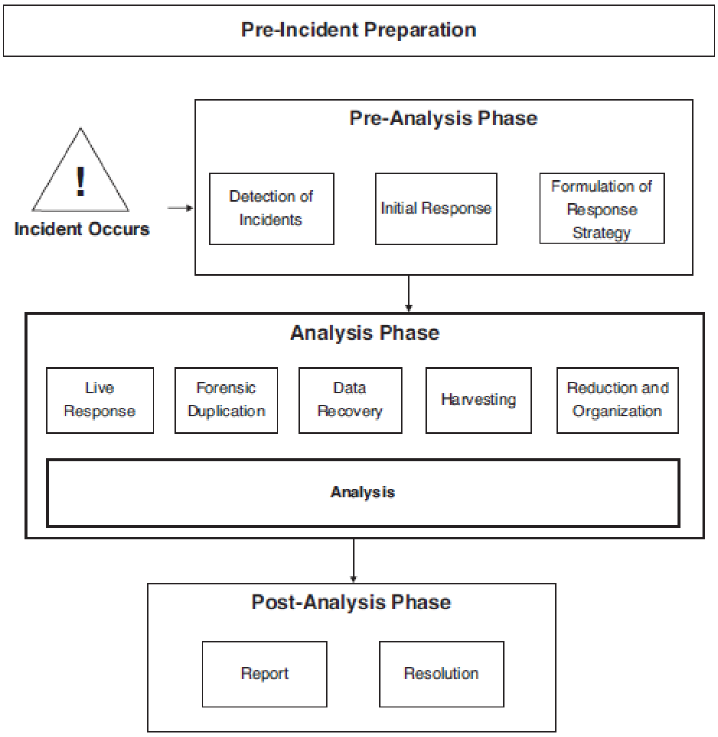


Figure 3.11: Common Process Model for Incident Response and Computer Forensics (Freiling & Schwittay, 2007, p.10).

The primary focus of this framework is on analysis and this shows in the illustration of the model in figure 3.11. This framework consists three primary phases namely Pre-Incident Preparation, Pre-Analysis, Analysis and Post-Analysis. As it is showed in figure 3.11, the pre-analysis phase contains all the necessary steps and activities which correspond to the respective steps in the incident response process model. These are performed before the actual analysis begins.

The analysis phase is where the actual analysis begins and it adopts part of the investigative process model which based on the computer forensic process model but without the live response steps. The final phase of this framework is the post-analysis phase. The post-analysis phase is concerned with the documentation of all the activities throughout the investigation. Following in table 3.8 is an outline of mapping processes of the digital forensic investigation framework proposed by Selamat, Yusof & Sahib in 2008. The mapping process model was a result of reviewing the existing investigation frameworks and models.

Table 3.8: Mapping process model of digital forensic (Selamat, et al., 2008, p.166).

Phase	Phase Name	Output
Phase 1	Preparation	Plan, Authorization, Warrant, Notification, Confirmation
Phase 2	Collection and Preservation	Crime type, Potential Evidence Sources, Media, Devices, Event
Phase 3	Examination and Analysis	Log Files, File, Events log, Data, Information
Phase 4	Presentation and Reporting	Evidence, Report
Phase 5	Disseminating the case	Evidence Explanation, New Policies, New Investigation Procedures, Evidence Disposed, Investigation Closed

As a result of this review, it was evident to the authors that each proposed framework and model build on the experience of the previous publications. The authors also noted that even though that the processes or activities are slightly different in terms of their orders of terms used but their outputs are similar. Therefore, table 3.8 shows a map of digital forensic investigation framework (DFIF) by grouping and merging the same activities or processes that provide the same output into an appropriate phase. This mapping process was purposely designed to balance the process which can produce concrete evidence for presentation in a court of law.

In 2009, Perumal (2009, p.40) proposed an investigation model known as “Digital Forensic Model Based on Malaysian Investigation Process” (figure 3.12). The motivation behind this new development in accordance to the author, the previous models do not show the information process flow focusing on issues such as chain of custody, attention to fragile evidences and data acquisition processes. As illustrated in figure 3.12, the proposed investigation model consists of seven phases with planning being the first phase.

In the planning phase, there are two sub-procedures to be completed before proceeding to the next phase. Need to get authorisation the local enforcement team and also needs to obtain a search warrant to seize any items involved. In the identification phase, consists of two sub-procedures as well. The investigator needs to identify all the digital devices involved. The other one is, the investigator also needs to identify the fragile evidence and in this process, the investigator may need to decide whether to isolate devices involved by turning it off.

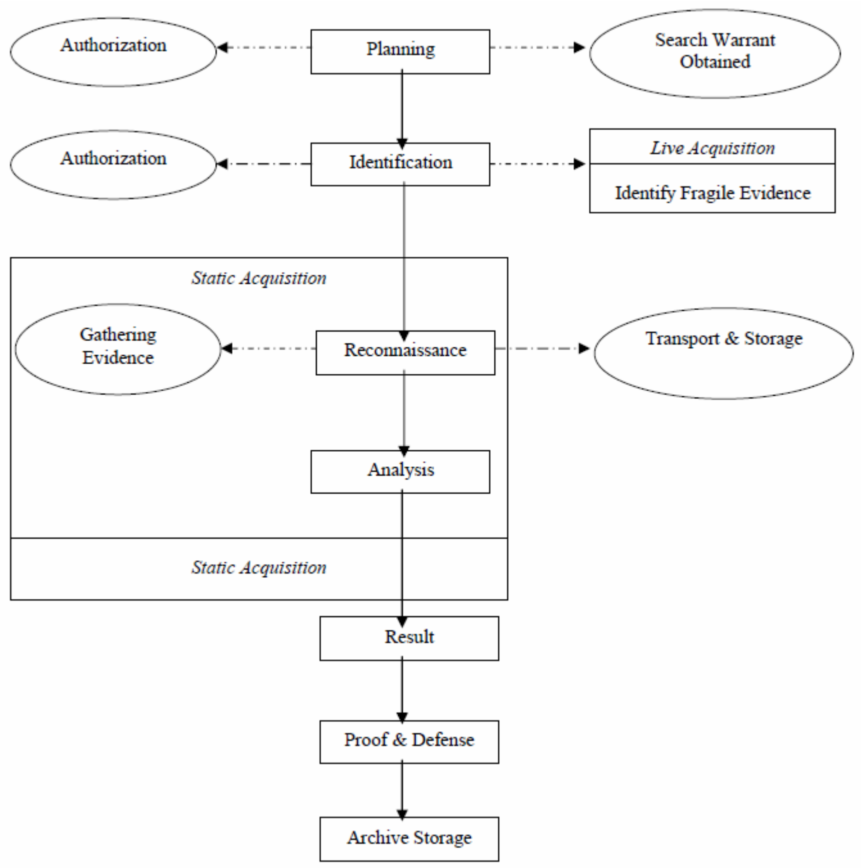


Figure 3.12: Digital Forensic Model based on Malaysian Investigation Process Model (Perumal, 2009, p.40).

The identification phase is followed by the reconnaissance phase where the investigator may need to conduct live forensics. This is purposely done to capture fragile evidence and disrupts normal day to day business operations by pulling the compromised device from the organisation’s network such as a server. Another important sub-procedure of the reconnaissance phase is concerned with the transportation and storage of the evidence. This is important as all evidence collected from the scene must be stored in a secure manner to prevent further tampering and to preserve its integrity.

The next phase of this model is the analysis phase. The analysis phase is concerned with the analysis techniques adopted in order to analyse the data collected and the connection of that data into a clear picture. After analysing the data there is the proof and defence phase dealing how the investigator presents and defence the investigation result in the court of law. The final phase of this model concerns with the handling and storage of the evidence for future reference. The evidence must be handled and stored in an approved and secure manner to preserve its integrity.

In the year 2010 Pilli, Joshi & Niyogi (2010, p.20) proposed a new model known as the "Generic process model for network forensic" as it shows in figure 3.13.

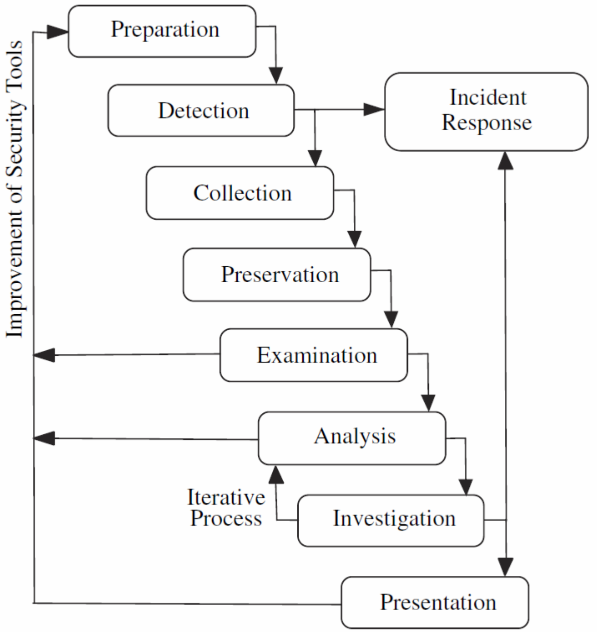


Figure 3.13: Generic process model for network forensics (Pilli, et al., 2010, p.20).

According to the authors, this generic model was developed in order to formalize a methodology specifically for network based investigation. As illustrated in figure 3.13, this model consists of eight phases with some particular processes and phases that have iterative features. The new feature that this generic process model for network forensics introduced is that it provides a connection to incidence response through the second phase which is the detection phase. This is important because, when an incident is detected in the detection phase, an approved and proper incidence response procedure must be initiated. The type of incidence response to be initiated will depend wholly on the report generated from the detection phase.

A new model known as the "Digital Forensic Model for Digital Forensic Investigation" proposed in 2011 by Ademu, Imafidon & Preston (2011, p.177) as it shown in figure 3.14.

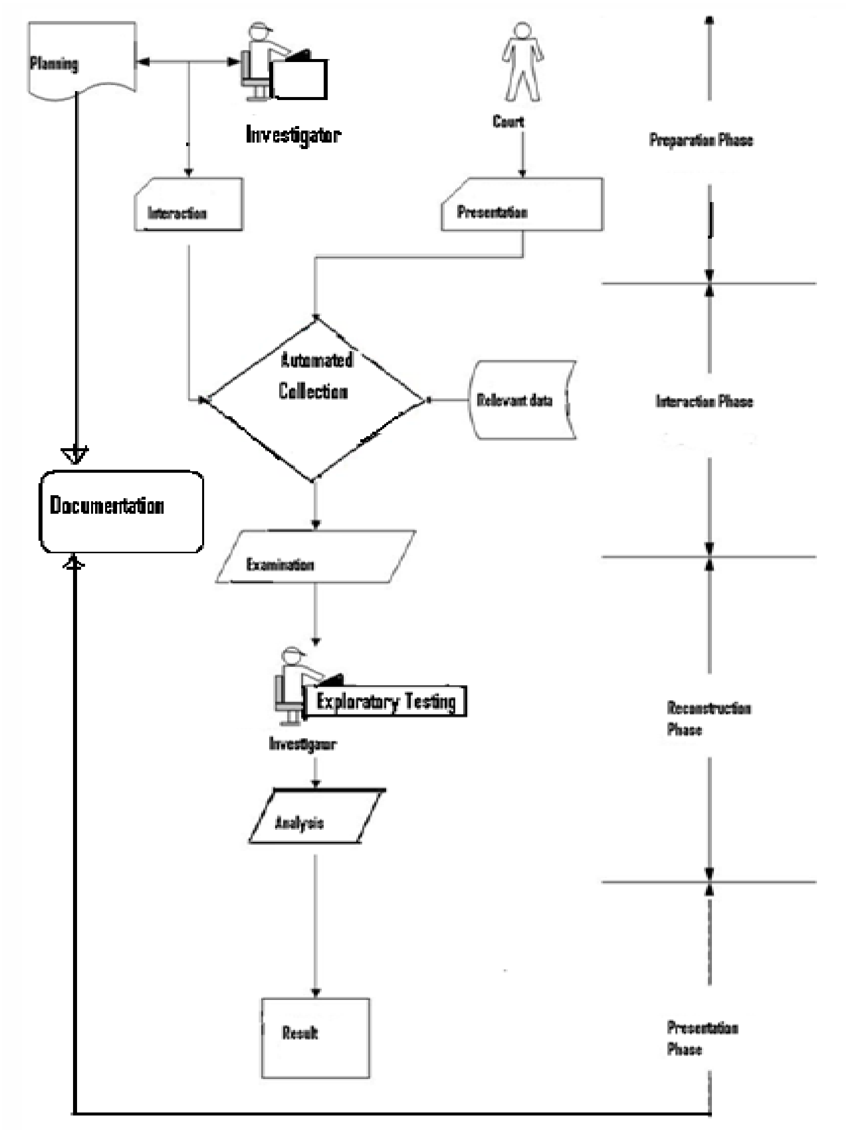


Figure 3.14: Digital forensic investigation Model (Ademu et al., 2011, p.177)

This digital forensic investigation process model is generalised into four main tiers with iterative approach. According to the authors, the entire investigation process is conceptualised as it happens iteratively in four different phases. The first tier of this investigation process model is the preparation phase and this phase occurs over the course of an investigation beginning from assessment to the final phase which is the presentation phase.

This model adopted rules, and a different rule is used in each tier. The first tier of the model contains four rules which are preparation, identification, authorisation and communication. The second tier contains three rules which are collection, preservation and documentation while the third tier contains rules such as examination, exploratory testing and analysis. The final tier is known as the presentation phase contains rules such as result, review and report.

Also in the year 2011, Yusoff, Ismail & Hassan (2011, p.29) proposed a new computer forensic investigation model known as the "Generic Computer Forensic Investigation Model (GCFIM)" as illustrated in figure 3.15. This new development is a result of a study conducted by the authors. In this study, the authors investigate previous forensic investigation process models and they found that each of the previous proposed models' recommended phases can be placed in at least one of their own proposed generic phases. As result, they proposed their own forensic investigation model known as the ***"Generic Computer Forensic Investigation Model".***

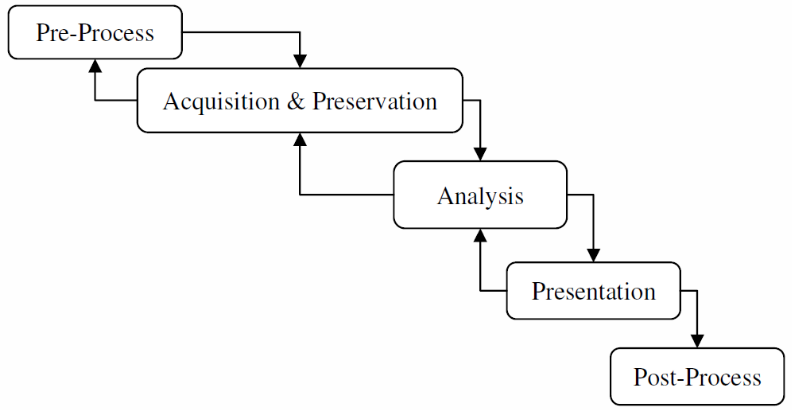


Figure 3.15: Generic Computer Forensic Investigation Model (GCFIM) (Yusoff, et al., 2011, p.29)

The GCFIM model consists of five phases with iterative features for all phases except for the last phase. Phase one is called the "Pre-process" phase which is responsible for all of the tasks that are required to be completed before the actual investigation can starts. The second phase is called "Acquisition & Preservation" phase where tasks such as identifying, acquiring, collecting, transporting, storing and preserving of data are performed.

The second phase is where all the tasks that are relevant to the actual acquisition and storing of that data for the next phase are conducted. The next phase of the GCFIM model is called the "Analysis" phase. According the result of the study conducted by the authors, this phase seems to be the main one and the central concern. In all the literature that they reviewed, data analysis is the main focus of most models. In the analysis of the GCFIM model, various types of analysis are conducted on the obtained data in order to identify the source of the crime and the person responsible.

The fourth phase of this model is known as the “Presentation” phase. According to the authors, this phase is critical because, the case be presented in a manner that is understandable to the party that is presented to but must also be supported with adequate and acceptable evidence. The final phase of the GCFIM model is the “Post-process” phase and this phase is responsible for the proper closing of the investigation. Both physical and digital evidences are required to be securely stored and returned to its rightful owner.

The growth in both popularities and usages of cloud services has presented opportunities for both criminal activities and challenges to law enforcement agencies. In the year 2012, Martini & Choo (2012, p.74) proposed a digital forensic investigation framework for cloud computing as shown in figure 3.16.

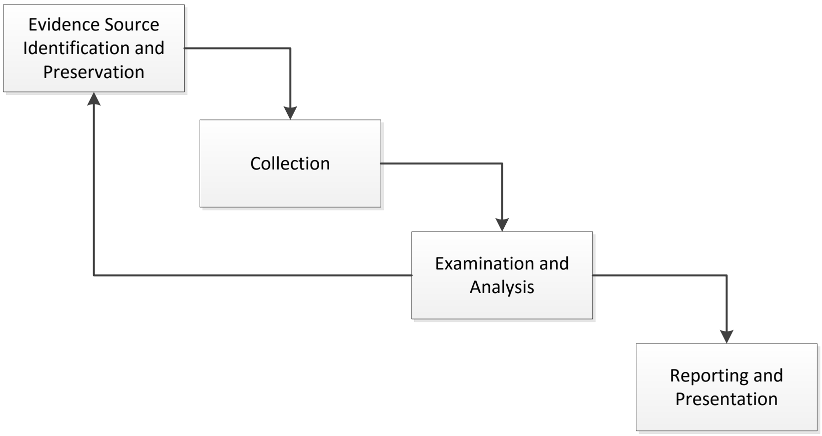

Evidence Source Identification and Preservation
Collection
Examination and Analysis
Reporting and Presentation

Figure 3.16: An integrated conceptual digital forensic framework for cloud computing (Martini & Choo, 2012, p.74)

According to Martini & Choo (2012, p.74), the Integrated conceptual digital forensic framework for cloud computing was developed based on the frameworks developed by McKemmish in 1999 and Kent et al. in 2006. Martini & Choo (2012) said that even though their framework is based on those two previous frameworks the meanings and processes of each phase are different. However, according to the authors, the key difference is that the integrated framework is the iteration feature of the phases. For instance, if any evidence of cloud computing activities is discovered in the third phase of the integrated framework which is examination and analysis, another iteration of the framework will run simultaneously.

This second iteration starts from the first phase which is evidence source and identification and preservation that run via the cloud service provider. If somehow the second iteration examination and analysis phase of the obtained data discovered further evidence sources then a third iteration will commence.

In the next section 3.3, further analysis of all the models reviewed in this section will be made in order to identify the gap in the literature where innovation may occur.

3.3 LITERATURE ANALYSIS

There is no doubt that we are living in a technological age where various digital devices are very much part of our life from individuals to businesses. When these devices are found to be involved in criminal activities then a new field known as digital forensics was developed in order to investigate and examine for digital evidences. However, the field of digital forensic investigation has only gained significant importance over the past decade due to the increasing number of security incidence that have occurred (Valjarevic & Venter, 2012, p.1).

Digital forensic originated as a synonym for computer forensics as its definition expanded to include forensic examination of all digital technologies. As computer forensics is defined as *"the collection of techniques and tools used to find evidence in a computer"* (Reith, et al., 2002, p.2). However, Kroll Ontrack a specialised computer forensic and data recovery company defines computer forensics as, *"the use of specialized techniques for recovery, authentication, and analysis of electronic data when a case involves issues relating to reconstruction of computer usage, examination of residual data, authentication of data by technical analysis or explanation of technical features of data and computer usage"* (Hankins, Uehara & Jigang, 2009, p.233).

Digital forensic is also defined as *"the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorised actions shown to be disruptive to planned operation"* (Reith, et al., 2002, p.2). However, digital forensic can be also be broken down into categories such as, computer forensics and mobile forensics. Mobile forensics is used to deal with forensic investigation on crimes that involves mobile SMART devices such as SMART phones and tablets. Types of data that can be retrieved from these

SMART devices such as call logs, text messages and contact list (Mellars, 2004, p.267; Da-Yu, et al., 2009, p.1).

Handling of digital evidences and for the findings to be admissible in the court of law, the investigator requires the use of standardised and formalised investigation process. There are published guidelines that attempt to remedy the situation both by practitioners in the industry and academic researchers over the past two decades (Valjarevic & Venter, 2012, p.1). As a result, there are a number of methods, frameworks and digital forensic investigation process models were proposed that can be found in academic and professional literature and can be dated back as far as 1995. However, international standards are still being developed to formalise digital forensic investigation processes and to provide digital forensic practitioners with a set of standardised guidelines.

In section 3.2.4, twelve digital forensic investigation process models were reviewed. The first model was the Computer Forensic Investigation Process by Mark Pollitt (1995, p.489). This model seems to focus only in the investigation process beginning with data acquisition. The model does not define how the investigator can approach a crime scene. The model also seems to put its emphasis on the evaluation stage by providing three extra investigation steps within the stage. This extra step is to determine the path that the digital evidence took starting from its physical context, logical context and legal context. This is debateable because digital evidence must be gathered by employing approved and reliable methods. Also, digital evidence must be analysed without bias or modification (Reith et al., 2002, p.3). The six phase Investigative model from the DFRWS was developed for computer and network forensics (Palmer & Corporation, 2001, p.17).

The DFRWS investigative model does address the short comings of the computer forensic investigation processes developed by Mark Pollitt in 1995. The DFRWS model was also developed to cover not only forensic investigation on computers but networks too. However, the DFRWS model is under developed in the identification phase which was designed to resolve signature and identify the profile and anomalies, system monitoring and complaints and audit analysis. Therefore, it left out the pre-incident preparation in order to organise the forensic processes prior to responding to an incident. Pre-incident processes such as outlining detail procedures to help investigator on how to deal with both digital and physical evidences (Reith et al., 2002, p.3).

The DFRWS model was also developed to cover forensic investigation on computer networks. Thus, the pre-incident phase should also outline how the investigator should approach getting authorisation to access the network. Also, the analysis phase is inappropriately defined and vague. For example, the instances arise as an interpretation of the examination phase results. Also, even though analysis and interpretation are two different processes but the process confuses the two (Baryamureeba & Tushabe, 2004, p.2).

The new digital forensic model that was proposed by Reith et al., in the year 2002 was called "Abstract digital forensic model." This new model comprises of nine investigation phases with an iterative feature implemented between the examination and the analysis phase. This model seems to offer good expression of the digital forensic processes. However, it still leaves an opening for comment. For instance, the third phase approach strategy, to an extent it is a duplication of the second phase, the preparation phase. This is because when responding to an incident, identifying the most appropriate procedure is likely to involve determining of the technique to be employed (Baryamureeba & Tushabe, 2004, p.3).

Carrier and Spafford introduced a new forensic investigation model known as *"An Integrated Digital Investigation Process"* in the year 2003. This model comprises of 17 phases but organised into five main groups only. The authors of this integrated digital investigation process outline the weaknesses of their model. The first one is that the model's classifications may be defined as too general for practical use. Secondly, there is no easy or obvious method for testing the model and thirdly, with all the sub-categories added to the model will just make it problematic to utilise. The final phase of the model in known as review phase which was purposely designed to review the whole investigation process in order to identify areas may require improvement. Therefore, this model misses defining the process of how to handle the evidence's chain of custody which is an important aspect of any investigative work (Perumal, 2009, p.40). The Computer forensic field triage process model (CFFTPM) on the other hand was introduced by Rogers, et al. (2006) to help investigators. Even though the evidence triage consists of the user profile, Internet usages and the chronological timeline activities still, depending on the type of investigation, the evidence triage will guide the investigator to possible evidence if the others have been removed. However, there are six key questions that every investigator should ask, the *what, why, how, who, where and when* type questions about the evidence and usually during the data analysis phase (Beebe & Clark, 2005, p.151).

The CFFTPM process model however proposes an onsite or field approach to help investigator in identifying, analysis and the interpretation of digital evidence in a very short time frame. The problem is that the fact the CFFTPM model has no requirement to take the compromised system or media back to the lab to obtain a complete image for further examination thus, the CFFTPM framework is not applicable for all investigative situations (Selamat et al., 2008, p.165).

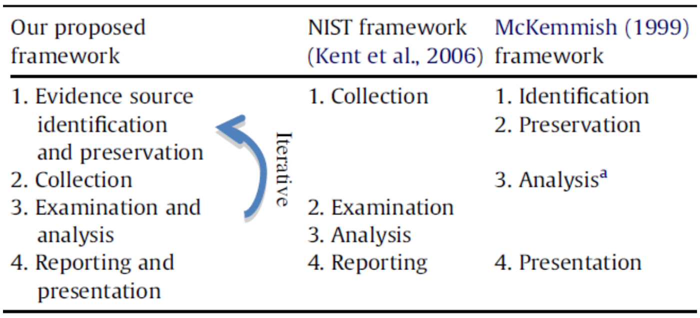
The common process model for incident and computer forensics on the other hand was proposed by Felix Freiling and Bastian Schwittay in the year 2007. As it was mentioned earlier in the literature contextual section, the common process model focused significantly on analysis. This model consists of pre-incident preparation, pre-analysis, analysis and post-analysis. The pre-analysis phase comprises of steps and activities that are performed before the actual analysis starts. The post-analysis phase is concerned with the final report of the whole investigation activities. The actual analysis takes place in the analysis phase. Therefore, it is evident that the common process model significantly focuses on the analysis processes only. The digital forensic model based on Malaysian investigation process on the other hand was proposed in the year 2009 by Sundresan Perumal from the University of Malaysia. According to Sundresan Perumal, the previous models do not show the information process flow focusing on issues such as chain of custody, attention to fragile evidences and data acquisition processes.

A generic process model for network forensics was proposed by Pilli, Joshi & Niyogi in the year 2010. The main purpose of the generic model was to formalize a methodology specifically for network based investigation. This model consists of eight phases with some particular processes and phases that have iterative features. The new feature that this generic model provides is that it has a connection to incidence response through the second phase which is the detection phase however, as it mentioned earlier, it was developed specifically for network forensics.

On the other hand, the Digital Forensic Model for Digital Forensic Investigation was proposed by Ademu, Imafidon & Preston in 2011. This particular process model is generalised into four main tiers however, these tiers has an iterative approach therefore, the entire investigation process is conceptualised as it happens iteratively in four different phases. Also in 2011, Yusoff, Ismail & Hassan (2011, p.29) proposed a new generic computer forensic investigation model (GCFIM). In this study, the authors investigate previous forensic investigation process models and they found that each of the previous proposed models' recommended phases can be placed in at least one of their own proposed generic phases.

With regards to forensic investigation in the cloud environment, this new technology has presented opportunities for both criminal activities and challenges to law enforcement agencies. Martini & Choo proposed a new digital forensic investigation framework for cloud computing in the year 2012 (Table 3.9). This cloud investigation framework consists of four phases which are the evidence source identification and preservation phase, collection phase, examination and analysis and the reporting and presentation phase.

This digital forensic framework for cloud computing was developed based on the frameworks developed by McKemmish in 1999 and Kent et al. in 2006. However, the key difference is the iteration feature implemented on the evidence source identification and preservation phase phases and the examination and analysis phase. Due to the fact that virtualization is the key element in implementing cloud computing, this provides forensic investigators with more challenges. The decentralised nature of how data is processed in the cloud also creates new disruptive challenges to investigators. As a result, traditional ways of acquiring data is no longer practical (Birk & Wegener, 2011, p.1).

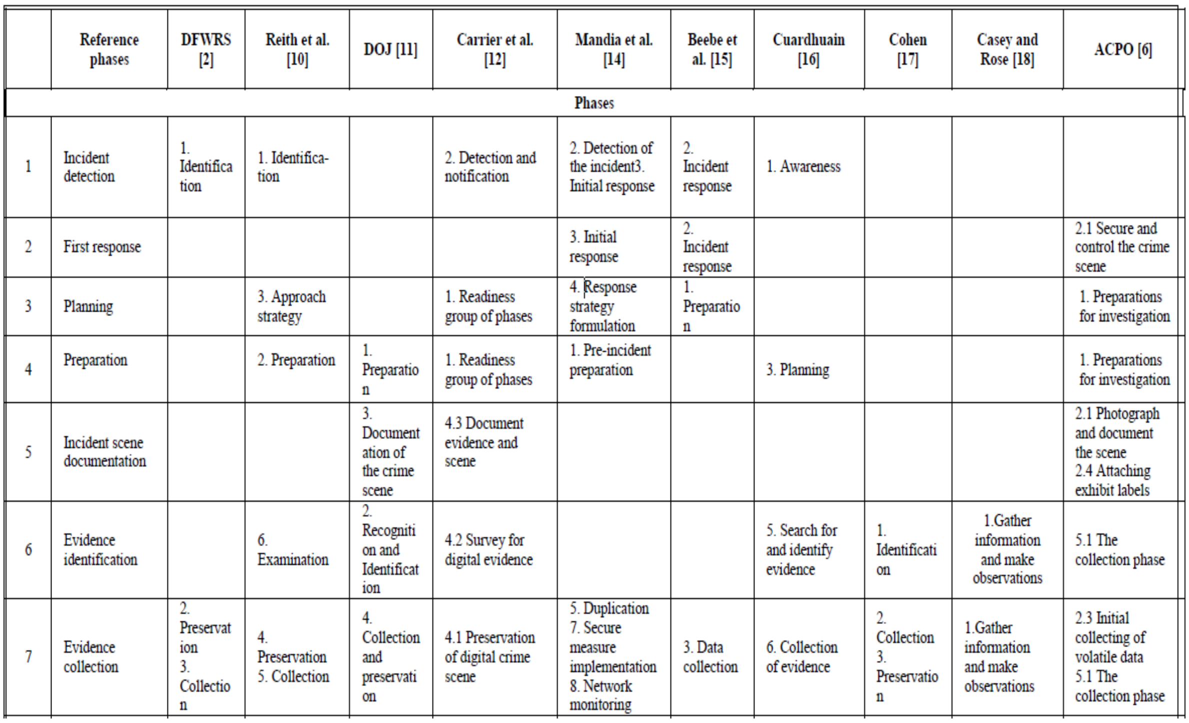


Our proposed framework		NIST framework (Kent et al., 2006)	McKemmish (1999) framework
1. Evidence source identification and preservation	Iterative	1. Collection	1. Identification 2. Preservation
2. Collection			3. Analysis[a]
3. Examination and analysis		2. Examination 3. Analysis	
4. Reporting and presentation		4. Reporting	4. Presentation

Table 3.9: Digital forensic framework comparison (Martini & Choo, 2012, p.74).

In a study conducted by Almulla, Iraqi & Jones from the University of South Australia, their findings showed that, identifying and extracting evidence from virtual machines with persistent storage, current digital forensics procedures can be applied. Identifying and extracting evidence in a cloud environment with multi-tenant architecture, current forensic procedures cannot be applied (Sharma & Sabharwal, 2012, p.618; Almulla, Iraqi & Jones, 2013, p.3).

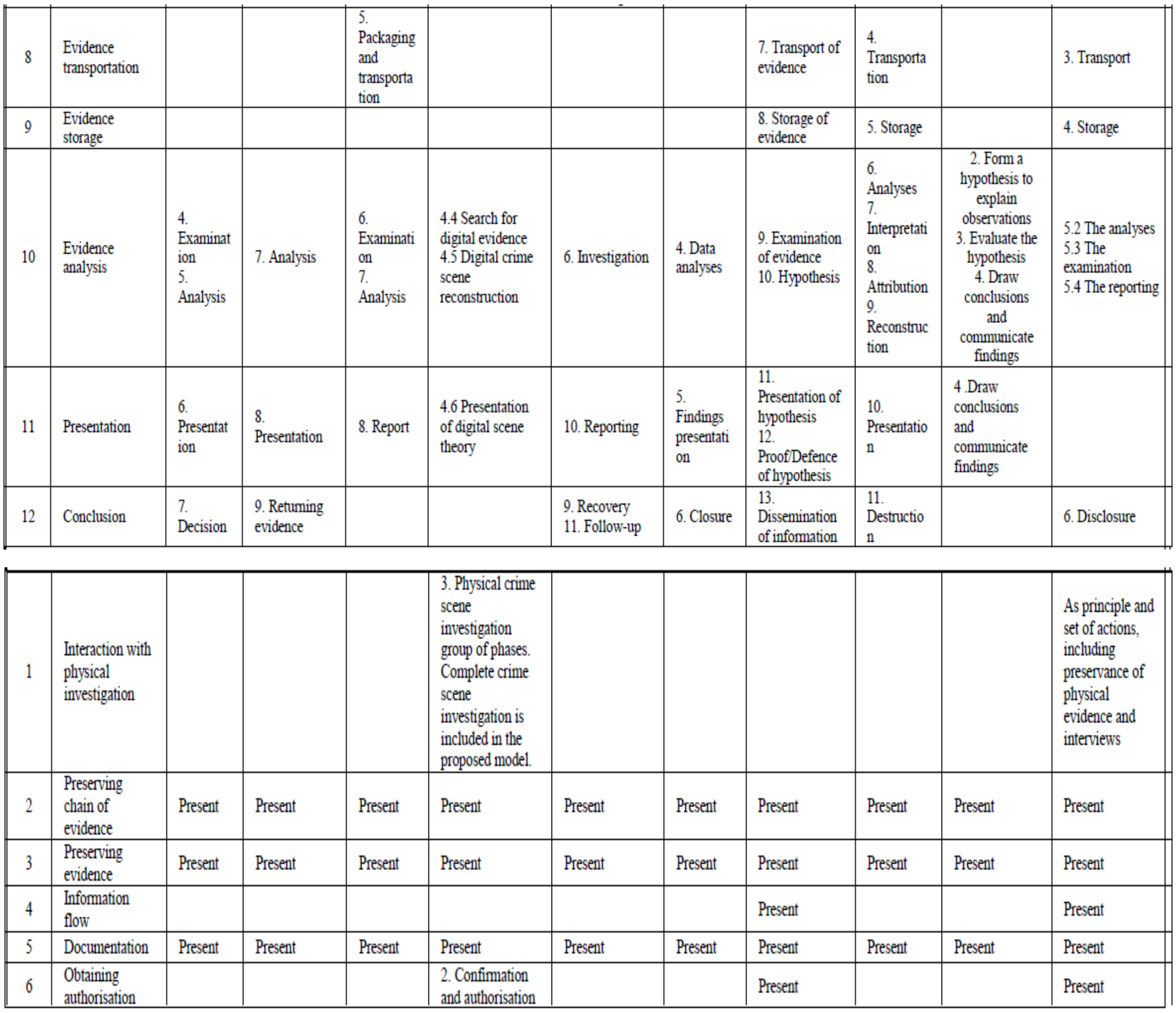
Table 3.10: Comparison of existing forensic investigation process models (Valjarevic & Venter, 2012, p.8).



	Reference phases	DFWRS [2]	Reith et al. [10]	DOJ [11]	Carrier et al. [12]	Mandia et al. [14]	Beebe et al. [15]	Cuardhuain [16]	Cohen [17]	Casey and Rose [18]	ACPO [6]
						Phases					
1	Incident detection	1. Identifica tion	1. Identifica-tion		2. Detection and notification	2. Detection of the incident3. Initial response	2. Incident response	1. Awareness			
2	First response					3. Initial response	2. Incident response				2.1 Secure and control the crime scene
3	Planning		3. Approach strategy		1. Readiness group of phases	4. Response strategy formulation	1. Preparatio n				1. Preparations for investigation
4	Preparation		2. Preparation	1. Preparatio n	1. Readiness group of phases	1. Pre-incident preparation		3. Planning			1. Preparations for investigation
5	Incident scene documentation			3. Document ation of the crime scene	4.3 Document evidence and scene						2.1 Photograph and document the scene 2.4 Attaching exhibit labels
6	Evidence identification		6. Examination	2. Recogniti on and Identificat ion	4.2 Survey for digital evidence			5. Search for and identify evidence	1. Identificati on	1.Gather information and make observations	5.1 The collection phase
7	Evidence collection	2. Preservat ion 3. Collectio n	4. Preservation 5. Collection	4. Collection and preservati on	4.1 Preservation of digital crime scene	5. Duplication 7. Secure measure implementation 8. Network monitoring	3. Data collection	6. Collection of evidence	2. Collection 3. Preservatio n	1.Gather information and make observations	2.3 Initial collecting of volatile data 5.1 The collection phase

In table 3.10 and 3.11, a detailed comparison of the investigation process models evaluated above is presented. Some of the proposed investigation models that are included in the comparisons such as the DOJ's and the ACPO's were not included in this study's literature contextual section.

Table 3.11: Actionable principles (Valjarevic & Venter, 2012, p.8).



8	Evidence transportation			5. Packaging and transportation				7. Transport of evidence	4. Transportation		3. Transport
9	Evidence storage							8. Storage of evidence	5. Storage		4. Storage
10	Evidence analysis	4. Examination 5. Analysis	7. Analysis	6. Examination 7. Analysis	4.4 Search for digital evidence 4.5 Digital crime scene reconstruction	6. Investigation	4. Data analyses	9. Examination of evidence 10. Hypothesis	6. Analyses 7. Interpretation 8. Attribution 9. Reconstruction	2. Form a hypothesis to explain observations 3. Evaluate the hypothesis 4. Draw conclusions and communicate findings	5.2 The analyses 5.3 The examination 5.4 The reporting
11	Presentation	6. Presentation	8. Presentation	8. Report	4.6 Presentation of digital scene theory	10. Reporting	5. Findings presentation	11. Presentation of hypothesis 12. Proof/Defence of hypothesis	10. Presentation	4 .Draw conclusions and communicate findings	
12	Conclusion	7. Decision	9. Returning evidence			9. Recovery 11. Follow-up	6. Closure	13. Dissemination of information	11. Destruction		6. Disclosure
1	Interaction with physical investigation				3. Physical crime scene investigation group of phases. Complete crime scene investigation is included in the proposed model.						As principle and set of actions, including preservance of physical evidence and interviews
2	Preserving chain of evidence	Present	Present	Present	Present	Present	Present	Present	Present	Present	Present
3	Preserving evidence	Present	Present	Present	Present	Present	Present	Present	Present	Present	Present
4	Information flow							Present			Present
5	Documentation	Present	Present	Present	Present	Present	Present	Present	Present	Present	Present
6	Obtaining authorisation				2. Confirmation and authorisation			Present			Present

Table 3.10 and table 3.11 are comparing the investigation models according to their phases however, it showed that some of the models either left a phase out or name it differently. For example, Table 1 shows the phase one called *"Incident detection"*. The DFWRS model and the An Examination of Digital Forensic Models by (Reith, Carr & Gunsch, 2002) named it as *"Identification phase"*. At the same time, the DOJ and the ACPO models did not have such a phase in their models.

3.4 GAP IDENTIFIED FOR THIS STUDY

According to the literature reviewed and analysed in section 3.2 and 3.3, it is evident that the current digital forensic investigation process models were developed for specific aspects of the digital forensic field only. For example, the models were designed for computer forensics, network forensics or cloud forensics only. These then leave the problem of SMART devices that draw on every area of digital forensic knowledge.

The gap that can be identified in the literature for this study is that, there is no digital forensic investigation process model that was developed to guide forensic investigators in a case that involved more than one sub-field of digital forensic investigation. This study shows the character of digital forensic investigation on a digital mobile SMART device (with scenario tests) and the problem identified in the literature exists. As a result, a Multi-disciplinary digital forensics investigation process model was developed as illustrated in figure 3.17 for testing. The proposed model was drafted from the learning of the analysis in this chapter and formulated to fill the gap and avoid repetition. The result is a tentative best investigation model for SMART devices that requires testing and validation against the other alternative models reviewed in this chapter 3. This will be termed the “STRAW MAN” and act as the starting point for improvement.

The STRAW MAN model has 22 phases comprising of 12 main phases for mobile SMART devices and five each for cloud and network based investigation. The implication is that for a mobile SMART device - which converges many segregated areas - investigation knowledge from each of the implicated areas is required for effective and efficient investigations. Models are an abstraction of a process to examine potential evidence. Irrespective of the originality of the evidence whether a result of traditional or digital forensic investigation (Peisert, et al., 2008, p.116). Forensic experts also believe that forensic investigation process models generalise an informal procedure to deliver a framework. That framework provides a detailed understanding of what each process is to do and not do. Jankun-Kelly, et al. (2007) explained that the model and framework provides an effective means to acquire information within the process. These processes are used to capture relevant aspects of the investigation (p.357). Figure 3.5 showed the evidence that with the existing digital forensic investigation models, forensic experts may need more than one models for one case.

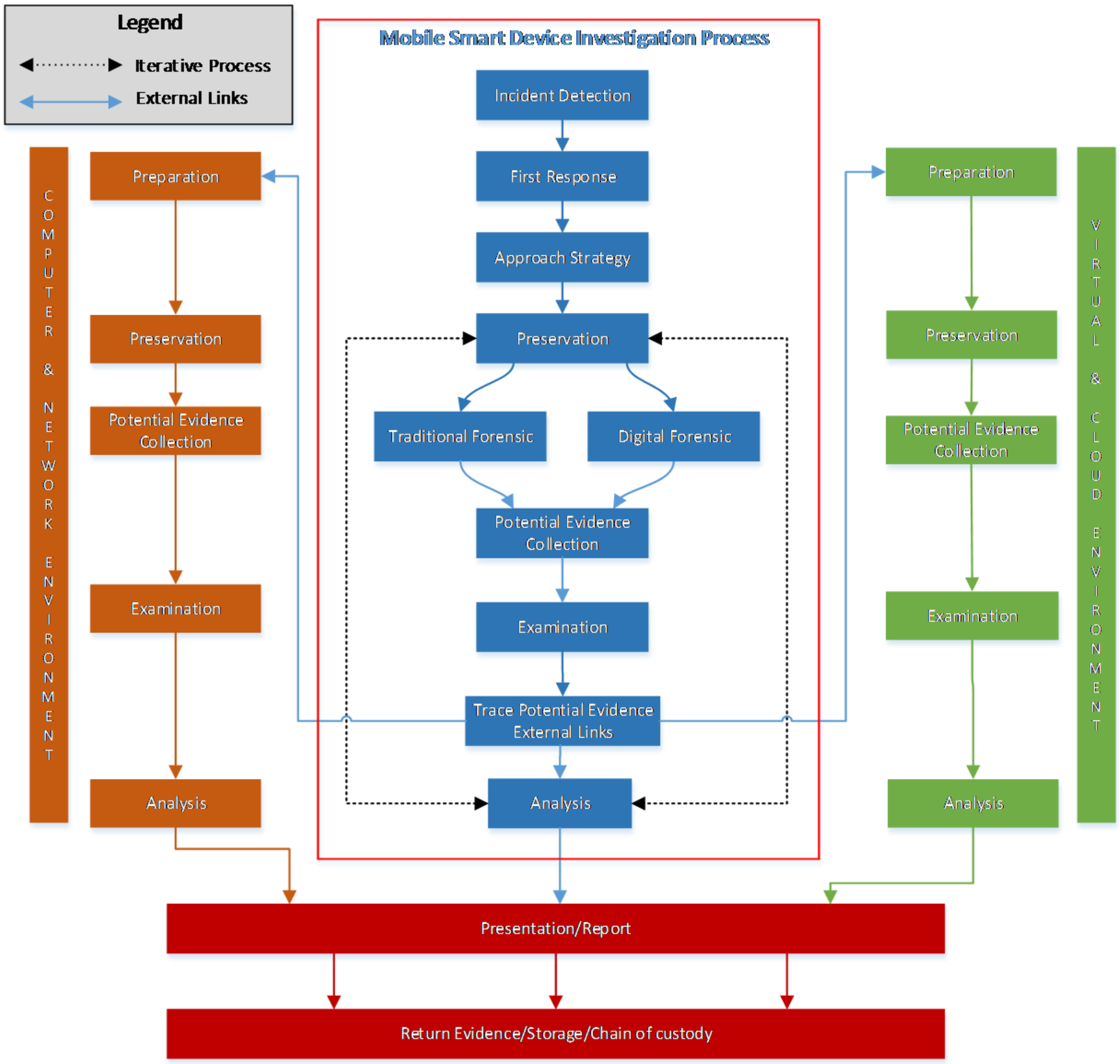

Legend
Iterative Process
External Links
Mobile Smart Device Investigation Process
Incident Detection
First Response
Approach Strategy
Preservation
Traditional Forensic
Digital Forensic
Potential Evidence Collection
Examination
Trace Potential Evidence External Links
Analysis
COMPUTER & NETWORK ENVIRONMENT
Preparation
Preservation
Potential Evidence Collection
Examination
Analysis
VIRTUAL & CLOUD ENVIRONMENT
Preparation
Preservation
Potential Evidence Collection
Examination
Analysis
Presentation/Report
Return Evidence/Storage/Chain of custody

Figure 3.17: The STRAW MAN model.

3.5 ISSUES AND PROBLEMS SUMMARY

This section is designed to highlight the issues and problems identified in the literature reviewed in this chapter. Mobile devices these days are known as mobile SMART devices because their features and functionalities are similar to that of a desktop computer. These mobile SMART devices are running on an operating system which allows its users to install third party applications which add more functionality to the device. Section 2.3 explained three operating systems for mobile SMART devices chosen based on the International Data Corporation (IDC) top five world market share report (IDC, 2015, p.1).

These three operating systems were developed by three different companies. The iOS operating system developed by the Apple Corporation, Android developed by Google and Windows mobile from Microsoft Corporation. These three chosen mobile operating systems are very similar in terms of their features and functionalities. However, their main differences are in their architectures and type of file system utilised. As a result, this is one of the main issues and challenges that are encountered by digital forensic investigators. Therefore, investigators will need to employ different tool kit for each device depending on the operating system running on it.

With regards to digital forensic tools, the literature reviewed in section 3.2 revealed some issues in terms of performance. Among those literature is the special publication published by the NIST organisation. In this special publication, NIST outlined the results of the test they conducted on forensic tools. The results showed the fact that, the performance of the tools are dependent on the method employed and what the investigator is looking for. However, in the study conducted by Morrissey (2010, p.130) found that tools with better support with regards to investigation requirements, yielded better results than the most expensive tool involved.

The issue here is that, the investigator will need to carry a number of tools in the tool kit. This is because, different set of tools required for different type of device, and no one tool exists yet for all platforms. This is a real challenge faced by today’s forensic practitioners, they really have to familiarise and update themselves with the tools available to them. They also need to know how each tool performs under various data acquisition methods and to various platforms.

In section 3.3, literature with regards to forensic investigation guidelines has been reviewed. Two reputable government organisations in the field have developed and published their guidelines and recommendations. However, with regards to the NIST guidelines, this is more like a set of recommendations for forensic organisations than investigators. ACPO on the other hand, outlined four principles however, these principles are very general and it was developed as a guide on how to handle all computer-based evidences. It was developed specifically for mobile devices only. Hence a gap for research and innovation is visible.

3.6 CONCLUSION

In conclusion, it is evident from the literature reviewed in this chapter that the mobile device forensics is still in its early days. This field is still in the development stage when compared to a more matured digital forensic field such as computer forensics. This has opened more study avenues for researchers in both academia and in the industry itself. This chapter has provided an analysis of current investigator guidelines and models and identified gaps for the mobile SMART device forensics domain.

The literature reviewed in this chapter has elaborated on different architectures of the three chosen SMART device operating systems. Their differences have led the discussions into the issues and challenges that are encountered by investigators in terms of tool requirements. It can be concluded that performing forensic investigation on these different SMART devices also requires different tools. It is also evident that the investigator has to be familiar with the tools that are available and familiarise themselves with the devices' forensic data acquisition methods in order to know which tool to utilise and under which method.

It can also be concluded from the literature analysis that the mobile device forensic domain has a lack of standardised procedures, methodology, models and frameworks. These are required to aid investigators in order to preserve the integrity of evidence obtained from these devices. Hence the model developed from the literature analysis of this chapter (figure 3.17) requires testing in practice to confirm or otherwise its relevance. In chapter 4 a research methodology will be specified to run a pilot study with the proposed innovative model.

Chapter Four

Methodology

4.0 INTRODUCTION

Chapters 2 and 3 have reviewed the technical and theoretical contexts for digital investigation in contemporary network and SMART business device environments. Chapter 2 defined the devices, networks and cloud environments concerned. In chapter 3, the theoretical frameworks for tool testing, digital investigation and professional practice were reviewed in relation to what they offered for doing a SMART device investigation in a contemporary environment. These models were analysed by consolidating previous comparison studies and undertaking comparative analysis. The analysis showed deficits, redundancies and confusions when the investigation models and methods were to be applied to a contemporary SMART business device environment. Consequently, the "STRAW MAN" model was derived from the result of the analysis (see Figure 3.17) and proposed for testing. In this chapter 4, a methodology for scenario testing of the "STRAW MAN" model is defined.

This chapter is organised into eight sections (4.1 – 4.8) which starts off with a review of the design methods of the twelve digital forensics investigation process models that was reviewed in chapter three section 3.2.4. This is followed by section 4.2 which provides a discussion on the philosophy behind research. The fundamental anticipations of research are also discussed and that leads up to a discussion on qualitative research methodology. Here the Exploratory research method is compared with the available alternatives in the qualitative research domain. This is followed by sub-section 4.2.1 which discusses the research method employed by this study.

This is followed by section 4.3 that provides a detailed review of the STRAW MAN Model including a discussion of its attributes and properties. Section 4.4 discusses the specifications of the test scenario including an explanation of the two case studies in sub-sections 4.4.1 and 4.4.2 that are used to evaluate the performance of the STRAW MAN model. Section 4.5 provides a discussion of the design of this study where the processes are explained. Table 4.2 outlines the design evaluation methodology employed then in section 4.6 the research question and the hypotheses are given. Section 4.7 discusses the data requirements and the test-bed setup. Sub-section 4.7.1 defines how the data is going to be processed and 4.7.2 discusses how the data will be analysed. Finally, section 4.8 concludes the chapter.

4.1 DESIGN METHODS OF THE 12 MODELS

In chapter 3, twelve digital investigation process models were reviewed. This section is designed to review the methodologies that the authors employed in the development of their investigation process models.

At the first digital forensic research workshop held in New York in 2001, the attendees concluded that digital forensic was a process with reasonable steps. As a result, four core processes were identified as preservation, collection, examination and analysis. There was no defined methodology employed by the attendees of this workshop in the development of this investigation process model. However, the development was entirely based on observations and systematically reviews of fifteen existing models identified in the literatures. Another model known as an "Abstract Digital Forensics Model", the development of this model was based the design methods and ideas behind the development of traditional forensics methods and in particular, the protocol for an FBI physical crime scene search. The outcome of this study was a seven phase abstract investigation process model which they claim that it can be applied to any sub-fields of the digital forensic arena at present and the future.

Baryamureeba & Tushabe (2004) proposed an investigation process model known as "An Integrated Digital Investigation Process". The approach employed in the development of this model was to adopt most of the phases from the models reviewed in their paper. However, their model is approaching the problem from a different point of view. The theory behind their approach is that the computer itself is a crime scene therefore the crime scene investigation techniques must apply. Rogers, et al. (2006) proposed an investigation process model known as the "Computer Forensic Field Triage Process Model". In the creation of the model, the approach they adopted was based on developing onsite/field tactics that provides those investigative processes that are performed within the first few hours of the investigation. The designed method focuses on the initial information gathering conducted in a relatively short time frame. As a result, the proposed model’s emphases is on finding useable evidence immediately; identifying victims at acute risk; guiding the on-going investigation; identifying potential charges; and accurately assess the offender’s danger to society. At the same time, process protects the integrity of the evidence and/or potential evidence for further examination and analysis.

Freiling & Schwittay (2007) also proposed a process model known as “Common Process Model for Incident Response and Computer Forensics” in their paper. The methodology that they adopted in the development of this model was a management focus approach. This allows the authors to develop an investigation process model that can combine the advantages of both Incident Response and Computer Forensics processes. With this approach, it allows Incident Response process to address the security incident while the Computer Forensics processes provide the potential evidences.

Selamat, et al. (2008) proposed an investigation process framework known as the “Mapping Process of Digital Forensic Investigation Framework”. The approach that the authors adopted for the development of this investigation framework is to construct the mapping framework based on the literature they reviewed in their study. The focus is to develop an investigation framework that can map the processes between the activities and the output on each of the phases of the proposed framework.

Perumal (2009) proposed a new investigation process model based on the Malaysia Cyber Law. The methodology that the author adopted for the development of this new investigation model was based on the existing models. The approach was, review the investigation process models that are available to digital forensic practitioners today. After that then apply the Malaysia Cyber Forensic law then developed and proposed a new model that can capture the full scope of the Malaysia Cyber Law. The new model is known as the “Digital Forensic Model Based on Malaysian Investigation Process”

Pilli, et al. (2010) proposed a network forensics investigation process model known as the “Generic process model for network forensics” in the paper titled “Network forensic frameworks: Survey and research challenges”. The approach they employed in their research started off with an exhaustive review of various network forensic frameworks published in the literature prior to their work. As a result, a generic investigation process model for network forensics was proposed. That was developed based on various existing models for digital forensics that they reviewed. Their methodology also allowed them to define, categorise and state clearly motivation for network forensics. The functionalities of various network forensics tools and network security monitoring tools available to forensic practitioners was also discussed. The research methodology led them to the identification of research gaps in the implementation of frameworks, process models and analysis tools. Major challenges were also highlighted.

Ademu, et al. (2011) published a paper titled "A New Approach of Digital Forensic Model for Digital Forensic Investigation". In this study, the authors employed a methodology as a guide during their study. As a result, they developed an investigation process model to improve the whole investigation process. Their approach started off with reviewing the existing digital forensics frameworks available in the literature. After that, they proceed on to compiling the literature analysis and results. The results were evaluated to be used to produce a new model which they believed will improve the whole investigation process. According to the authors, research approach introduced a structured and consistent methodology for digital forensic investigation.

Martini & Choo (2012) proposed an iterative conceptual digital forensic framework which highlights the differences between preservation and collection of digital data in the cloud environment for forensic purposes. Their proposed framework is known as "an integrated conceptual digital forensic framework for cloud computing". Their methodology started off with reviewing two of the most widely accepted documents in the field. The first is titled "What is Forensic Computing?" written by Rodney McKemmish 1999. The second is titled "Guide to Integrating Forensic Techniques into Incident Response" written by Karen Kent and her colleagues 2006. The methodology employed allowed the authors to use the results from the reviewed literature to identify the changes required to current forensic practices in order to conduct forensics investigation in a cloud environment successfully.

In all of the methodologies discussed, they have one thing in common. The development of their proposed investigation process models and frameworks were all based on the existing literature. All their design approaches and purposes were to improve and enhance the existing investigation processes. Each of these models and frameworks has their own strength; however, still there is no single investigation process model or framework that can be a general guideline for investigating all of the sub-fields of digital forensics. Therefore, further research is needed to design a general framework to overcome this problem (Selamat, et al., 2008, p.166). In the next section, the chosen research methodology for this study is outlined.

4.2 METHODOLGY/RESEARCH METHODS

The word research is seen as a way of thinking, critically examining of various aspects of your profession, understanding and formulating guiding principles that govern a particular procedure (Kumar, 1998, p.1). Since research is defined as a way of thinking, it needs a method. Method is a logical and orderly course of action for accomplishing the goal. Another view is that method is a body of methods, rules and postulates employed by a discipline, a particular procedure or set of procedures (Merriam-Webster, 2011, p.1). Although a methodology does not define precise methods however, it is regarded as a highly intellectual human activity used in the investigation of nature and matter and deals specifically with the manner in which data is collected, analysed and interpreted (Pattron, 2009, p.1). These human activities that Pattron (2009) referred to are used in an investigation and are comprised of a framework. This framework is used to distinguish one type of research from another.

Computer and network forensics also known as digital forensics has been defined by many researchers in different ways. However, the National Institute of Standards and Technology (NIST) defined digital forensics as the application of science to the 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, p.1). The Association of Chief Police Officers' (ACPO) published in the official release version of the *"Good Practice Guide for Computer-Based Electronic Evidence"* the four principles of computer-based electronic evidence. The first principle is concerned with the integrity of the evidence found on a computer or storage media. The second principle is concerned with the competency of the person that finds it necessary to access original data held on a computer or on storage media. Also, the person's competent to give evidence explaining its relevance and their action's implications. Third principle is concerned with the record of all processes applied to computer-based digital evidence should be preserved. However, an independent investigator should be able to examine those processes and still achieve the same result. The final principle is concerned with the responsibility of the person in charge of the investigation. This person is responsible for ensuring that the law and these principles are adhered to (ACPO, 2007, p.4).

As a result, an Information Technology researcher will have to decide on the type of research to be conducted. Confirmatory and exploratory research is the two most common research types. Confirmatory deals specifically with measurement models, that is, the relationship between observed measures or indicators (Brown, 2006, p.1). However, confirmatory research is said to proceed from a series of alternatives, a prior hypothesis concerning some topic of interest, followed by the development of a research design (often experimental) to test those hypotheses (Jaeger & Halliday, 1998, p.64). Exploratory research on the other hand, this type of research is employed mainly to gain a deeper understanding of something (Malhotra, 2007, p.28). For instance, every time we learn of a release of a new technology such as the iPad from Apple, it does not mean that we know how the iPad works. Exploratory research is very useful in this type of study as it allows the researcher to go deeper into an issue or a problem.

Figure 4.1 illustrates the relationship between research types, from the type of research approach taken, the techniques used for collecting and the ways of analysing the data. Relating the two types of research shown above to this work has shown that there was no predicament in choosing between confirmatory and exploratory research. Since that a research question and hypotheses is to be pre-defined for this study, it can be said that this study is an exploratory research.

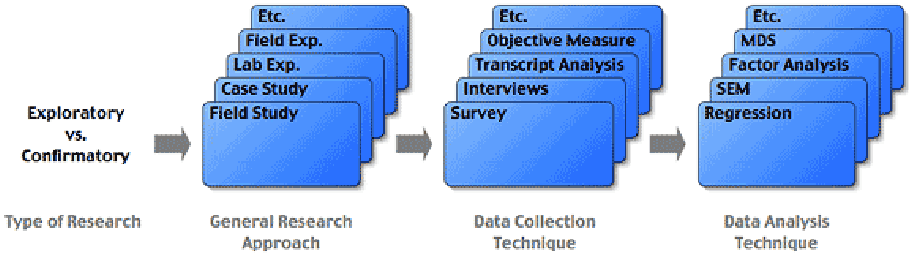


Figure 4.1: Exploratory vs. Confirmatory (Straub, Boudreau, & Gefen, 2004, p.1).

The next section is designed to discuss the research methodology to be used in this study.

4.2.1 Research Methodology Employed

It is evident in the literature that this study requires a building of IT artefacts. Digital forensic investigation has a complex nature and for that reason, it requires multi-disciplinary skills and abilities. As a result, this study employed the "Design Science (DS) Research Methodology for Information Systems Research" as the methodology to guide this study. Since this study is aimed to yield a new digital forensic investigation process model and an investigation framework, DS is a suitable research methodology for this study. The word *"design"* in English, is both a noun and a verb as a result, design is the creation of a plan for the construction of an artefact that, is both a product and a process. These phases are not independent; the design process must produce the product to be designed (Walls, et al., 2004, p.45). In other words, DS is the design and investigation of artefacts in context. The DS research methodology's phases incorporate processes for the production of the artefact.

March and Smith in the year 1995 developed a framework to reveal the relationship, activities and outputs of design and natural science research. The authors identified the four products of design science as - constructs, models, methods, and implementations (March and Smith, 1995, p.260).

In a study conducted by Shirley Gregor in the year 2006 aimed at examining the structural nature of theory in Information Systems. Shirley Gregor identified five interrelated typed of theory: theory for analysing, theory for explaining, theory for predicting, theory for explaining and predicting and theory for design and action. The theory for design and action in particular, is about the principles of form and function, methods, and justificatory theoretical knowledge that are used in the development of IS. The artefact is emphasized as the prime or only contribution of Design Science (Gregor, 2006, p.629). In addition, Hevner, et al., (2004) also outlined some criteria that is effective in which they believe it contributes to the novelty of the artefacts. That is, the models and methods designed under Design Science can be evaluated for completeness, simplicity, consistency, ease of use, and the quality of results obtained through use of the method and Gregor, 2006 also agreed that it is a valid claim.

The purpose of the DS research methodology is not only to develop an artefact but also to answer the research question. However, in order to make sure the answer is credible, employing a research method is vital. In Design Science, it is possible to use any methodology in the process to answer any questions regarding the artefacts. Depending on the characteristics and the goals of the research, any methodology will be valuable (Johannesson & Perjons, 2014, p.77). The DS research methodology consists of six main phases: problem identification and motivation, define the objectives for a solution, design and development, demonstration, evaluation and communication (Peffers, et al., 2007, p.54) as it showing in figure 4.2.

According to Hevner and Chatterjee (2010), DS is solution oriented whereas the other research methodology such Natural Science or Social Science, they are problem oriented (p. 3). The illustration shows in figure 4.2 highlighted four entry points. The first entry point is known as the problem-centred initiation. This entry point is designed to identify the problem and the motivation of the study. When the identification completed then the next task is to define the problem and extract its significance. The problem identification entry point involves analysing the existing relevant literature, identify the problem, interview experts in the field and also conduct a pre-evaluation of the study to confirm its relevance and importance.

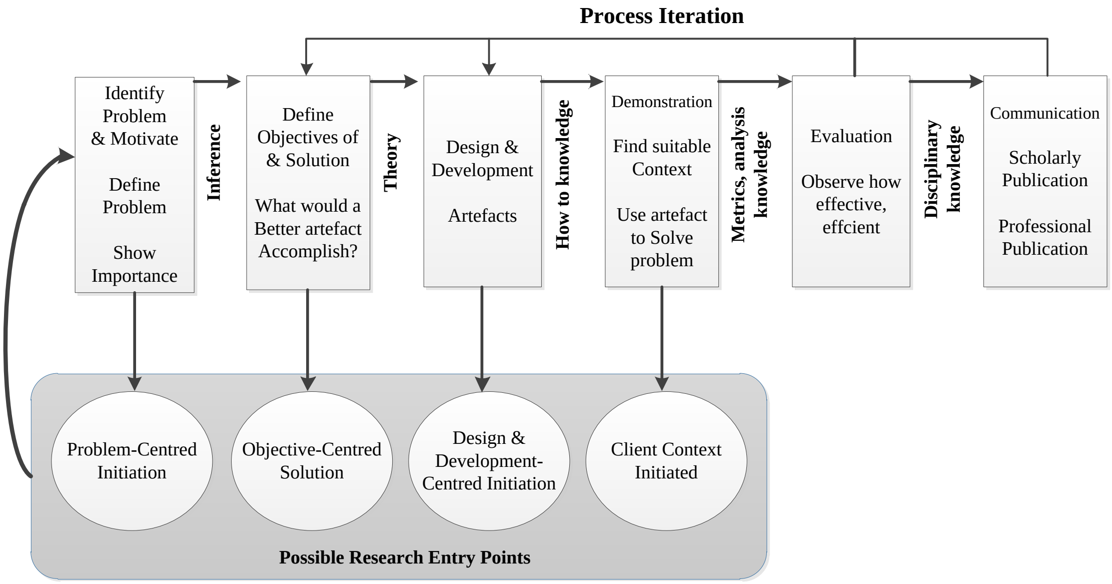

Process Iteration
Identify Problem & Motivate
Define Problem
Show Importance
Inference
Define Objectives of & Solution
What would a Better artefact Accomplish?
Theory
Design & Development
Artefacts
How to knowledge
Demonstration
Find suitable Context
Use artefact to Solve problem
Metrics, analysis knowledge
Evaluation
Observe how effective, effcient
Disciplinary knowledge
Communication
Scholarly Publication
Professional Publication
Problem-Centred Initiation
Objective-Centred Solution
Design & Development-Centred Initiation
Client Context Initiated
Possible Research Entry Points

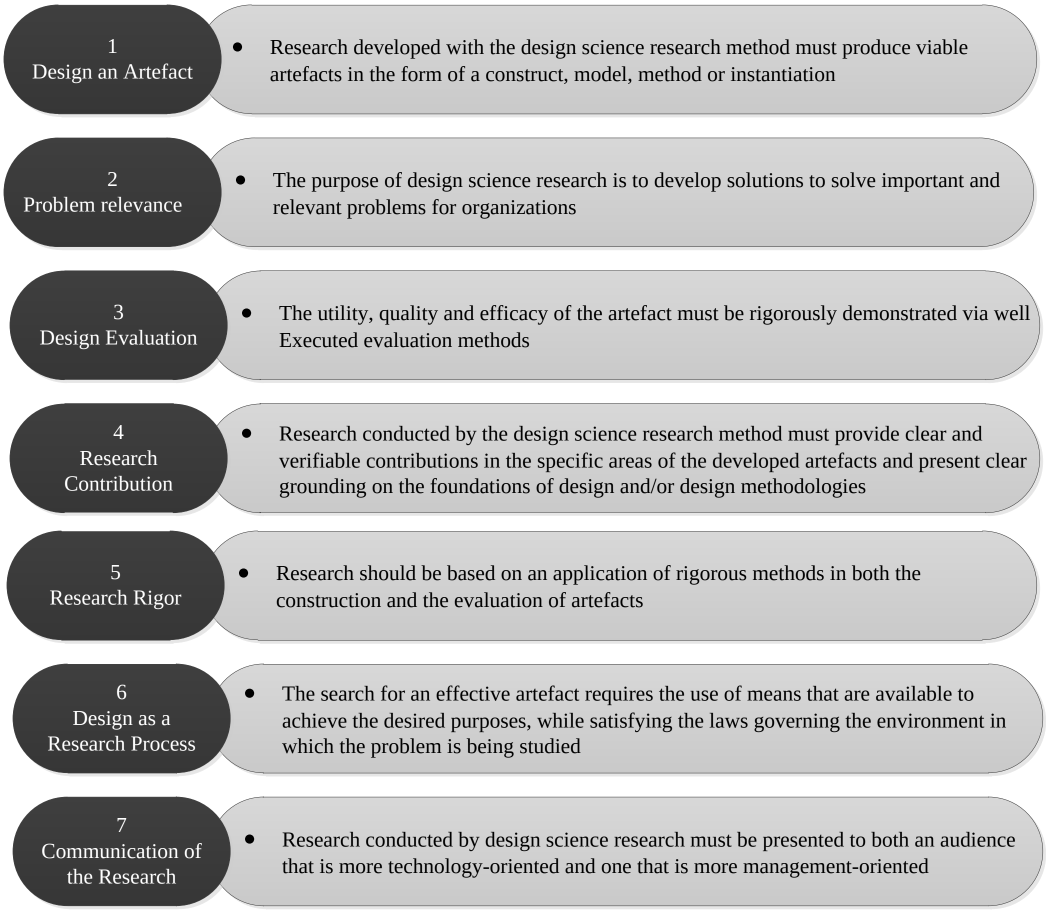
Figure 4.2: DS research methodology (Based on Peffers, et al., 2007, p.54).

This means that once the problem is identified, its relevance needs to be evaluated. For instance, pre-evaluate the relevance of the hypothesis, check with various stakeholders, experts in the field and so on. If they agree with the hypothesis of the study then look at running a pilot study in order confirm any pre-assumed theory to support the hypothesis (Offermann, et al., 2009, p.4).

The second entry point is known as the objective-centred solution. This entry point is designed to support the designing of the artefact and the supporting literature research. After evaluating its relevance and importance, then a solution has to be developed in the form of an artefact. In the solution designing phase or the second entry point, existing solutions and technologies have to be taken into account. In the course of designing the solution (artefact), the problem can be re-iterated. Events beginning from the problem identification entry point are also iterated and all these actions must be documented as this phase, research rigour has to be ensured by using all related work available. Design & development-centred initiated entry point or phase three of the DS research methodology is concerned with the creation of the artefact. These potential artefacts can be models, new methods or new properties of technical, social or informational resources. Design & development is concerned with the determining of the desired functionality of the artefact, its architecture and then the actual creation of the artefact.

The client context initiated entry point four or the fourth phase of the DS research methodology has activities in this phase involve that involve demonstration and finding of the most suitable environment. In this phase, also involves using the artefact to solve problem. With regards to demonstration, this is dealing with the use of the artefact to solve instances of the problem in various environments such as experimentation, case study or other suitable activities. Demonstration can also be very useful in terms of knowing how to use the artefact to solve a problem effectively (Peffers, et al., 2007, p.55). Evaluation is the fifth phase of the DS research methodology; this involves observing and evaluating how effective and how efficient that the artefact is in solving a problem. In this phase, the evaluation and observation results from the entry point number four will be compared with the objectives of a solution. A satisfaction survey result, client feedback and data from a system performance such as availability and response time will be included in the evaluation. At the end of this phase, the researcher will then decide whether to iterate back to entry point number 3 to improve the effectiveness of the artefact (Dresch, et al., 2015, p.68).

The final phase of DS research methodology is known as Communication. This phase is designed to allow the researcher to employ various scholarly electronic databases to communicate the outcome of the study. This communication might include the problem and its importance, the artefact, the rigor of its design and its effectiveness to other researchers and practitioners in the field (Dresch, et al., 2015, p.68). It is also suggested that researchers should conclude their studies with communicating the implications of their research results for the practical field. March and Storey (2008) state that it is vital for when conducting DS research that a contribution is made to the advancement of general knowledge and also improve practical situations in the field (p.726). To ensure that appropriate contributions be made with DS research, specific elements must be considered as illustrated in figure 4.3.



1 Design an Artefact
- Research developed with the design science research method must produce viable artefacts in the form of a construct, model, method or instantiation

2 Problem relevance
- The purpose of design science research is to develop solutions to solve important and relevant problems for organizations

3 Design Evaluation
- The utility, quality and efficacy of the artefact must be rigorously demonstrated via well Executed evaluation methods

4 Research Contribution
- Research conducted by the design science research method must provide clear and verifiable contributions in the specific areas of the developed artefacts and present clear grounding on the foundations of design and/or design methodologies

5 Research Rigor
- Research should be based on an application of rigorous methods in both the construction and the evaluation of artefacts

6 Design as a Research Process
- The search for an effective artefact requires the use of means that are available to achieve the desired purposes, while satisfying the laws governing the environment in which the problem is being studied

7 Communication of the Research
- Research conducted by design science research must be presented to both an audience that is more technology-oriented and one that is more management-oriented

Figure 4.3: Criteria for conducting DS research (Based on Dresch, et al., 2015, p.70).

Design Science is chosen for this study because it is solution oriented not problem oriented as mentioned earlier in this section. Not only that but it also focus on the creation process and refining of the artefact to get a good quality solution. The purpose of this study is to develop a solution for digital forensic investigation processes, and the result will be an artefact that is a solution. For that reason, DS provides a systematic, testable and communicable approach. This will allow the study to produce a quality artefact as a solution for the problem identified in the literature.

According to Offermann, et al., (2009), design science refers to *"an explicitly organised, rational and wholly systematic approach to design; not just the utilisation of scientific knowledge of artefacts"* (p.2). Therefore, it is believed that DS will be the most suitable research methodology to guide this study in order to develop an artefact as a solution for the problem identified in the literature. Figure 4.4 shows relevance and rigor in DS research. It clearly illustrated how DS research considers the identified problems from the environment and organisational requirements as a significant part of developing the solution. This includes peoples' roles, skills and characteristics. DS research method also sees the structure of the organisation, their culture, processes and strategies as relevant part new solution design and development. Another significant and relevant part of this process is the technology such as the existing communication infrastructure, applications and skills development. DS research requires analysing the existing knowledge base rigorously and exploring the literature in both academic and professional areas to adopt applicable knowledge.

Figure 4.4 shows the relationships between DS and the environment which consists of people, organisations and technology which are all part of the problem area. The knowledge base on the other hand provides the applicable knowledge which consists of foundations and methodologies that can be of assistance in providing data analysis techniques and validation criteria. The next section is designed to review the STRAW MAN model.

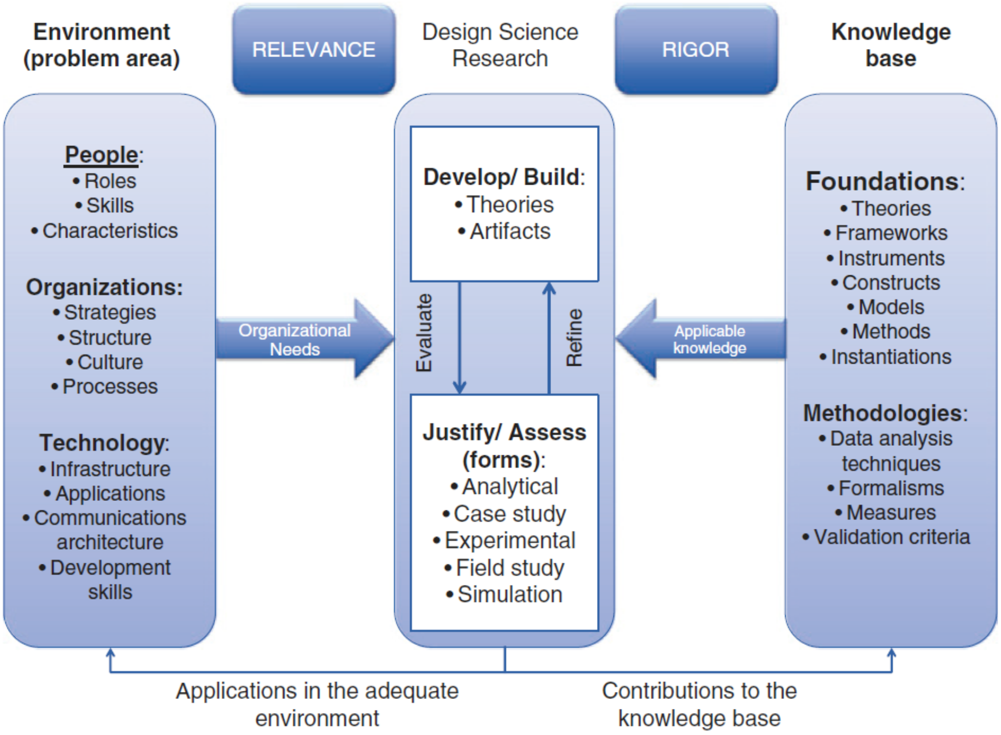


Figure 4.4: Relevance and Rigor in DS research in IS (Hevner, et al., 2004, p.80).

4.3 REVIEW OF "STRAW MAN" MODEL

In chapter 3, the analysis of the literature implied that there are chances and opportunities to improve the readiness and the abilities of the current investigation models and procedural frameworks to meet the demands of the changes in technologies. Chapter 3 concludes with a theoretical analysis of 12 existing digital investigation process models. The gap was identified in the literature as a result of the analysis; a "STRAW MAN" model was constructed. This model is the first attempt at filling the gap.

Table 4.1: Features of the STRAW MAN model (Venable, et al., 2012, p.426).

Features	STRAW MAN Investigation Process Model
Attributes	Completeness, consistency, accuracy, reliability, usability, fit with the organization
Properties	Efficiency, effectiveness, efficacy, ethicality and elegance, performance

The data showed in table 4.1 outlines the attributes and the properties expected from the artefact. This can be referred to as the design goal, the expected performance measure. DS research methodology can use them during the iteration process in re-evaluating and refining the artefact. The artefact in this study is called the straw man model. The straw man model consists of three different sub-fields of the digital forensics domain. The SMART device forensics, network forensics and cloud forensics. Each of these sub-fields forensic investigation environments is different in scopes, characteristics and nature in terms of risks, security, challenges and so on. For instance, the scope of network forensics encompasses the networks, systems and devices associated with the physical and human networks (Cusack & Lutui, 2013, p.59). Investigating network forensics differs in scope and objective from one perspective to another.

However, the scope and objective of an investigation usually depict its characteristic features. For that reason, it is evident that digital forensic investigation has a complex nature therefore; it requires multidisciplinary skills and abilities. As stated earlier, DS research methodology is chosen for the study because it has the ability to deal with the type of artefact that this study is looking at developing as a solution. DS research methodology has an iterative nature which allows the researcher to keep on re-evaluating and refining the artefact until the desired quality is reached. This is a vital solution as the process (methodology and approach) one adopts in conducting a digital forensics investigation is crucial to the outcome of such an investigation. Overlooking one step or interchanging any of the steps may lead to incomplete or inconclusive results hence wrong interpretations and conclusions. (Baryamureeba & Tushabe, 2004, p.1). DS research methodology allows the researcher to look at things systematically.

4.4 SPECIFICATION OF SCENARIO TESTS

Process artefacts are methods, procedures and so on, that guides someone or tells them what to do to accomplish some task (Venable, et al., 2012, p.427). Digital forensics is a new field and researchers from the industry and the academic domain are still studying the processes and technologies in the field for the past decades. Digital forensics deals with the collection, preservation and managing of potential evidences various types of technologies. These technologies range from standalone computers, private organisation’s networks, mobile SMART devices and the cloud/virtual environments (Palmer & Corporation, 2001, p.4).

In network forensics, potential evidences may be found in several and various types of network media. These media ranges from network routers and wireless access points to switches, client computers and network servers. In a cloud environment, cloud forensics was born from the necessity of managing digital crimes in various architectures of the cloud computing services (Ruan, et al., 2013, p.37). These days, organisations around the globe are more and more dependent upon information systems for the daily operations of their business (Elyas, et al., 2015, p.70). The most important in any process of digital forensics is the admissibility of the potential evidence in the court of law.

As a result, there is legal, contractual, regulatory, security and operational reasons why there is a need to conduct digital forensic investigations. Hence, digital forensics analysis must be conducted systematically, formalised and legal manner to ensure the admissibility of the potential evidence. So, Forensic readiness is defined as: the ability of an organisation to maximise its potential to use digital evidence whilst minimising the costs of an investigation (Rowlingson, 2004, p.5). Digital forensic readiness focuses on interpreting the current environments of computing and its capabilities with regards to, collecting and preserving of potential digital evidences from an investigation.

There are known issues in the process of digital forensic readiness, one of which being the changing nature of the investigation procedures. This can be derived from the skills and techniques employed by the criminals and the evolving nature of technological innovations. As a result, in order to overcome the challenge, it is necessary for digital forensic practitioners to adopt tested investigation procedures and techniques (De Marco, et al., 2014, p.238). Nonetheless, conducting forensic investigations, collecting digital potential evidences is a challenging task. This is due to the complexity of corporate environments, variety of computing platforms, and large amount of data to be analysed. Digital forensic investigations in such environments are likely to encounter a more complex acquisition and analysis of digital potential evidences.

According to the National Institute of Justice in the United States of America, the demand for responses to electronic evidence is expected to increase in the future. Therefore, it requires dedicated resources to be allocated for such services. The nature of electronic evidence has different challenges for its admissibility in court. In order to meet these challenges, there should be proper procedures to follow. These procedures consist of four phases: collection, examination, analysis and reporting (NIJ, 2001, p.4). Collection phase involves searching, recognising, collecting and documenting of electronic evidences. This is important because it can involve potential evidences that may be lost if the proper precautions are not taken.

According to the DS research methodology, the first entry point has been completed in this thesis as, the literature has been reviewed and analysed. The result is a problem and a gap for this study identified. Now looking at the second entry point and focussing on an objective-centred solution, two fictitious case studies were created based on the problem identified and the theory developed from the literature. The problem identified from the literatures is that all the digital investigation process models are for a specific sub-field of digital forensics. For instance, computer forensics, network forensics, mobile forensics or cloud forensics. Some were developed as a generic digital forensic investigation process model meaning, it can be used for any investigation in any of the sub-fields. This is being identified as a problem because, if an investigator faces an investigation with more than one of the sub-fields involved, there is yet to be a model or framework to guide the investigation. The case studies were developed to reflect the theory identified in the literature and are in the following two sub-sections.

4.4.1 Fictitious Digital Forensics Case One

"Alleged attack on a private company and stole company secrets"

An iPad was turned over to authorities; an investigation was set underway into the iPad. When the data was acquired from the iPad, when the investigator examines the data, two various accesses activities look suspicious to the investigator. The data showed that the user access a private company network. Further analysis of the data shows that some company private documents were taken and uploaded to a cloud account.

4.4.2 Fictitious Digital Forensics Case two

"Alleged young children kidnapping and trafficking"

A deal gone wrong and from that crime scene a mobile smart device was found and suspected of being involved in some criminal activities. When that mobile smart device went through the data acquisition phase, the data showed some e-mail messages were received from a private company e-mail address. During the data analysis phase, the investigator found that a private cloud account has been used many times to upload and download images.

4.5 DESIGN OF STUDY

Design is a search process to realise an effective solution to a problem (Hevner et al., 2004, p.88). The design of this study is based on the DS research methodology that was chosen to guide this study. The design shows the three major processes of the research which is input, process and the output. The inputs consist of two phases which are concern with exploring the existing literature in the field. The main purpose is to identify and formulate the problem and show its importance.

The research processes are organised to develop an artefact which is a digital forensic investigation process model. Part of these processes is the designing of the test-bed which will be used to demonstrate the artefact and evaluate the performance of the solution. An iterative feature is implemented within the "processes" section of the design of this study to enable the application of the two test case scenarios to evaluate the artefact. The final part of the design of the study is designed to include the development of the final outputs for this study. These are the investigation framework and the best practice guidelines for forensic practitioners.

The illustration in figure 4.5 showed the phases of this study. The design is divided into three parts. Part one is designed to match the entry point number one of DS research method. Problem-centred initiation - identifies the problem, the motivation for the study and then defines the problem. This phase is also designed to show the importance of the problem to initiate the study.

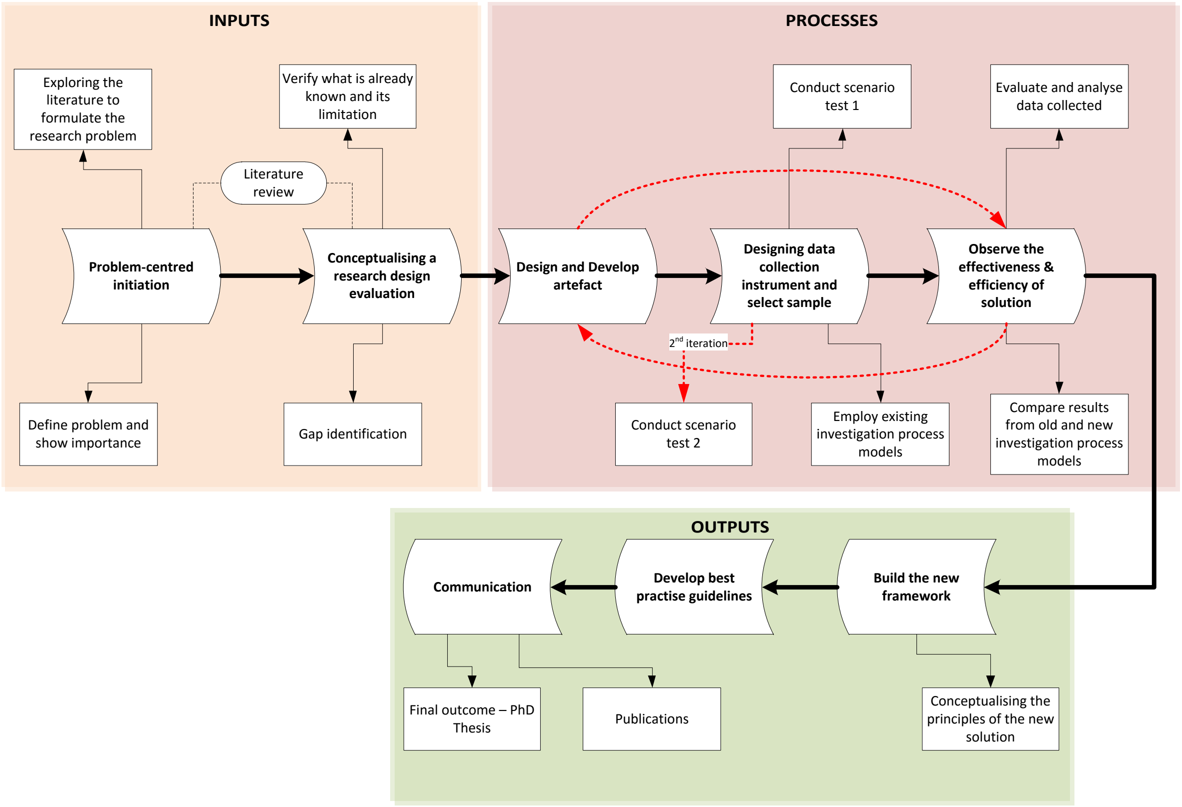

INPUTS
Exploring the literature to formulate the research problem
Verify what is already known and its limitation
Literature review
Problem-centred initiation
Conceptualising a research design evaluation
Define problem and show importance
Gap identification
PROCESSES
Conduct scenario test 1
Evaluate and analyse data collected
Design and Develop artefact
Designing data collection instrument and select sample
Observe the effectiveness & efficiency of solution
2nd iteration
Conduct scenario test 2
Employ existing investigation process models
Compare results from old and new investigation process models
OUTPUTS
Communication
Develop best practise guidelines
Build the new framework
Final outcome – PhD Thesis
Publications
Conceptualising the principles of the new solution

Figure 4.5: The design of this research.

DS entry point number two, three and four aligns with the second part of the design of this research. The second part is known the *"Process"*, entry point number two of DS is "Objective-Centred solution, focusing on defining the objectives of the solution. Entry point three is focusing on "Design and Development"; this entry point is responsible for the designing and the development of the artefact, the solution for the identified problem. Entry point four of the DS research method is "Client-Context Initiated." This focuses on the demonstration, finding of a suitable context and also uses the artefact to solve the problem. The fifth phase of DS research method focuses on evaluating the artefact. They both fall in to the *"Process"* section of the design which also involves the designing of the test-bed; this test-bed will be used to evaluate the artefact on fictitious test cases in order to observe its performance. The third part of the research design is called the "*Outputs,"* this is planned to align to the last phase of the DS research method. This last phase focuses on communicating the artefact to the outside world. This can be achieved via utilising the academic databases and other professional publications in the industry. Both of the DS research method and the design of this study have iterative features. This feature enables the evaluation of the artefact to be done repeatedly until perfection. Table 4.2 is the evaluation methodology that will be used to evaluate the design of the artefact.

Table 4.2: The evaluation methodology employed (Venable, et al., 2012, p.426).

Design Evaluation Methodology	
1. Observational	**Case study:** Study the artefact in depth in a test case environment
2. Analytical	**Static analysis:** Examine structure of artefact for static qualities (e.g. complexity)
	Architecture analysis: Study fit of artefact into technical IS architecture
	Optimization: Demonstrate inherent optimal properties of artefact or provide optimality bounds on artefact behaviour
	Dynamic analysis: Study artefact in use for dynamic qualities (e.g., performance)
3. Experimental	**Controlled Experiment:** Study artefact in controlled environment for qualities (e.g., usability)
4. Testing	**Functional Testing:** Execute artefact interfaces to discover failures and identify defects
5. Descriptive	**Informed Argument:** Use information from the knowledge base (e.g., relevant research) to build a convincing argument for the artefact's value (effectiveness & efficiency)
	Scenarios: Construct detailed scenarios around the artefact to demonstrate its value (effectiveness & efficiency)

This evaluation methodology has five steps. The method begins with the case study with an observational technique. This allows the researcher to study the artefact in depth. The second step is to analyse the artefact using various analytical techniques for different purposes. For instance, the dynamic analysis technique will be used to study the performance of the artefact. Third is to study the artefact on a test-bed in a controlled environment then, execute the artefact using the design of the research to identify any defects. The final step is known as descriptive and uses information from the knowledge base to build an argument for the artefact.

4.6 THE RESEARCH QUESTION AND HYPOTHESES

The proposed study aims to answer the question, *"What can be done to improve the effectiveness and efficiency of digital forensic investigation?"* Four hypotheses were also developed to be tested as part of this study, these hypotheses are assertions derived from the literature reviewed in chapter three. The four hypotheses are labelled H1 to H4.

H1: *network forensic investigation process model will be suitable for mobile forensic investigation.*

H2: *computer forensic investigation process model will be suitable for cloud forensic investigation.*

H3: *a multi-disciplinary digital forensic investigation process model will improve the effectiveness and efficiency of digital forensic investigation.*

H4: *a comprehensive framework to guide the investigator on best practises will improve the effectiveness and efficiency of digital forensic investigation.*

These hypotheses are to be tested by collecting two sets of data: one from each of the case studies. The first case study will be used to confirm (or otherwise) the validity of the gap identified in the literature review; and, the full scenario tests the validity (or otherwise) of the new model. Following in Figure 4.6 is a graphical illustration of a summary of how a researchable question and hypotheses were developed based on the literatures reviewed in chapters 2, 3. Figure 4.6 also illustrated the correlation between the literature and the deliverables of this study.

4.7 DATA REQUIREMENTS

Section 4.2.1 explained the method that is employed to guide this study. The design is shown in figure 4.5; however, a general research approach is taken to collect the data for data processing by way of scenario testing. The test-bed for the tests was set up in a controlled environment in a laboratory. The tests were set up on a server with the following specifications. 2 x Xeon quad-core processors; 8 Gigabytes of RAM and SAS hard drives. The hypervisor running on the host was VMware ESXi 5.1.0. In this virtual environment, a simulation of a private network consisting of a Domain Controller, Proxy server, Web server and Mail server.

A private cloud environment was also set-up employing the Synology technology. Figure 4.6 shows the test environment set-up and the diagram shows a wireless access point was also employed in order to simulate an access environment from a public place such as a cafeteria. The data collection environment also utilise an iPad 4 with both wireless and 3G capabilities. The servers showing in this test bed were all running on a 64bit Microsoft Windows Server 2008 R2. Two fictitious digital forensic cases were also developed with grounds for digital forensic investigation aiming to validate the new Forensic Investigation Process Model.

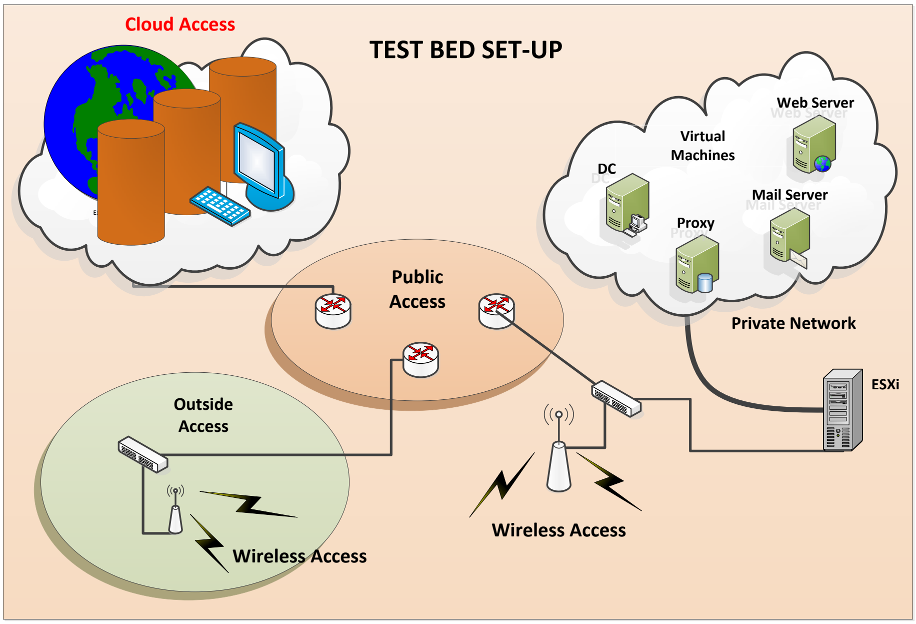


Figure 4.6: Test bed set-up in the laboratory.

4.7.1 Data Processing

Data processing as explained by Sakr, Liu & Fayoumi (2013) is the process of re-structuring or re-ordering of the raw data by human and machine in order to increase its usefulness (p.2). Following in Figure 4.7 is an illustration of the three steps that constitute the life cycle of data processing. In order to process any set of data, there must be an input for processing and an output will be produced as the result. In this case, the raw data is collected from the experiments and after processing it and the output is presented to users in several report formats, such as printed report, audio, video, or on to their monitors.

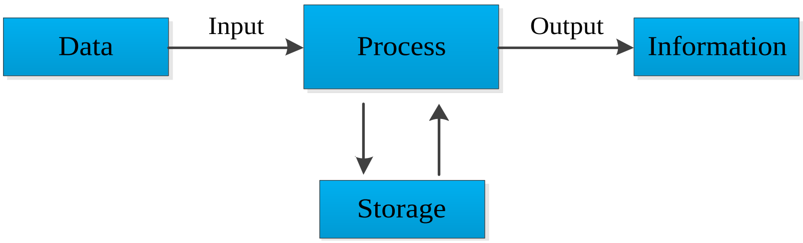


Figure 4.7: Data processing life cycle.

4.7.2 Data Analysis

DS research methodology enables researchers to use other approaches together with DS method. Johannesson and Perjons (2014) stated that, with DS research methodology, it is possible to take any approach to answer any questions regarding artefacts. However, depending on the characteristics and the goals of the research, any methodology will be valuable (p.77). As a result, the Exploratory Data Analysis (EDA) approach will be employed during the data analysis phase. Gorunescu (2011) explained that EDA involves reviewing, communicating and using data to identify systematic relations between certain attributes and variables. This approach will also allow data to reveal their underlying structure. Here are the main reasons for utilising the EDA technique; detecting of mistakes in the data, checking of assumptions, preliminary selection of appropriate models and also determining the relationships among the explanatory variables (Seltman, 2014, p.61). Following in figure 4.8 is the exploratory data analysis sequence.

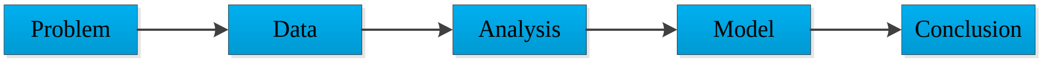


Figure 4.8: Exploratory Data Analysis life cycle (NIST, 2013b, p.20).

One of the disadvantages of the EDA is that, it usually does not provide decisive solutions therefore; it is difficult to avoid optimistic bias. One of its advantages, it has flexible ways to generate hypotheses. It also has more realistic statements of accuracy and it does not require more than the data can support. This promotes deeper understanding of processes. Criteria number five from the DS research methodology is research rigor meaning, the research should be based on an application of rigorous methods during the construction and the evaluation of the artefacts.

Following the illustration shown in figure 4.8, the problem has been identified in the literature and explained in section 3.4. Data collection method also explained in section 4.5 and data analysis method is shown in figure 4.8. Out of this will be the new forensic investigation process model and finally the conclusion is drawn. As it shown in figure 4.5, the design of the study, the phases need to work together from the design to collection and processing. An iterative feature is also implemented just in case additional data needs to be collected (Unwin, 2010, p.1).

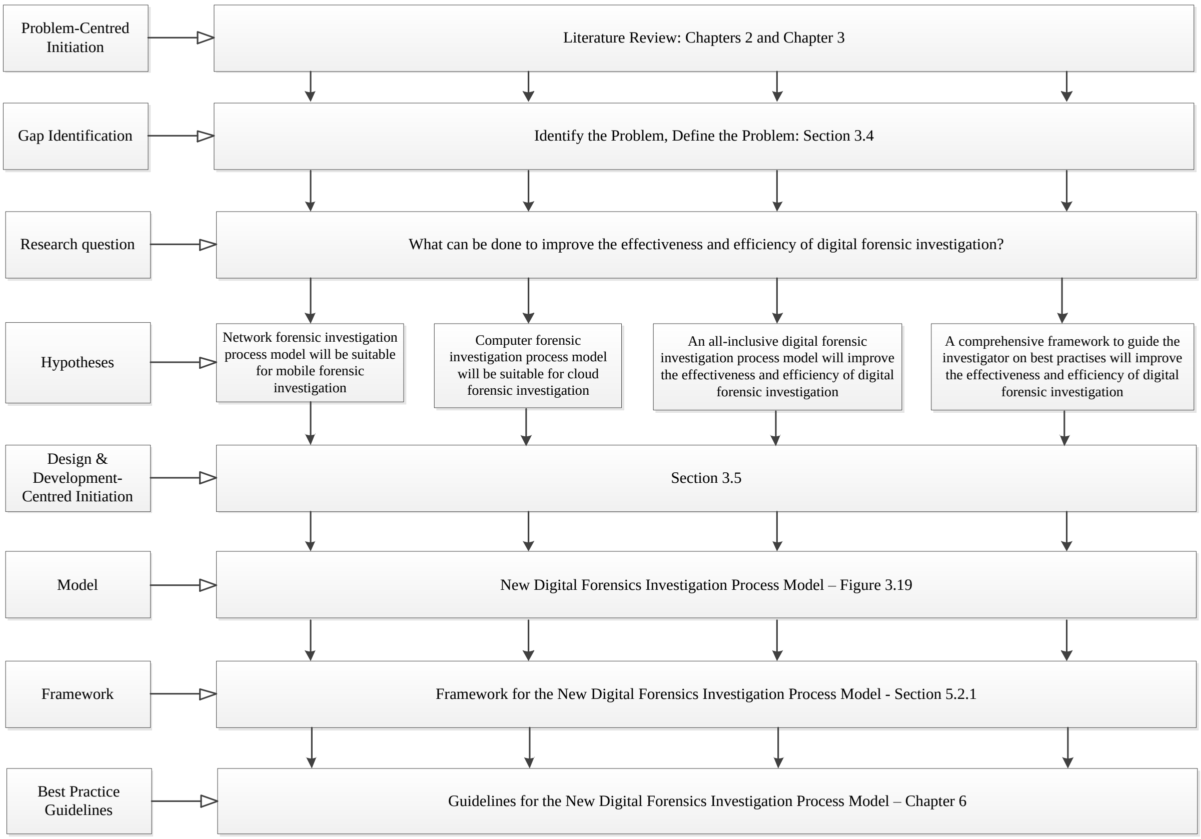

Problem-Centred Initiation
Literature Review: Chapters 2 and Chapter 3
Gap Identification
Identify the Problem, Define the Problem: Section 3.4
Research question
What can be done to improve the effectiveness and efficiency of digital forensic investigation?
Hypotheses
Network forensic investigation process model will be suitable for mobile forensic investigation
Computer forensic investigation process model will be suitable for cloud forensic investigation
An all-inclusive digital forensic investigation process model will improve the effectiveness and efficiency of digital forensic investigation
A comprehensive framework to guide the investigator on best practises will improve the effectiveness and efficiency of digital forensic investigation
Design & Development-Centred Initiation
Section 3.5
Model
New Digital Forensics Investigation Process Model – Figure 3.19
Framework
Framework for the New Digital Forensics Investigation Process Model - Section 5.2.1
Best Practice Guidelines
Guidelines for the New Digital Forensics Investigation Process Model – Chapter 6

Figure 4.9: The evolution of the artefact from the literature

Figure 4.9 showed in a graphical representation how the artefacts evolved starting from the review of the existing digital forensic investigation models available in the current literature. The flow was adopted from the DS research method processes. The result of the literature analysis was the problem identification and resolve question, the hypotheses were formulated so the DS research methodology will be used to answer the question and test the hypotheses at the same time.

4.8 CONCLUSION

Chapter 3 analysed 12 various digital forensic investigation process models. In this chapter, the design methodologies of those 12 investigation process models were analysed. The data from that analysis was used as the basis for the selection of the methodology. As a result, DS research methodology was chosen to guide the study especially in the development of the artefact. The gap for this study was identified in chapter 3 as a result of the literature analysis. In this chapter, the problem was defined and its significance and importance are shown. The design for this study was defined (figure 4.5) as a result, the data required and the test-bed for the collection of the data was designed as well (figure 4.6).

In the next chapter, the methodology elaborated will be used to test the STRAW MAN (figure 3.17) and to provide data that may be used for quality improvement.

Chapter Five

Findings

5.0 INTRODUCTION

Chapter 5 reports the findings of the testing specified in chapter 4; compares these findings with the potential outcomes from each of the reviewed historical models for digital investigation; and, proposes improvements to the "STRAW MAN" model derived in chapter 3 (see Figure 3.17). This chapter then links to chapter 6 where the learning from these findings is applied to develop the framework and best practice guide for practitioners doing digital investigations.

5.1 DATA

A pilot study was set up and executed to confirm (or otherwise) the issues, problems and gap identified in the literature for practice that related to a business SMART mobile device forensic investigation. Section 4.6.1 and 4.6.2 explained two fictitious digital forensic cases. Case one was used in the pilot study to test the hypothesis that motivated this research. In this section, the results from the pilot study are presented and explained using the test-bed shown in figure 4.6.

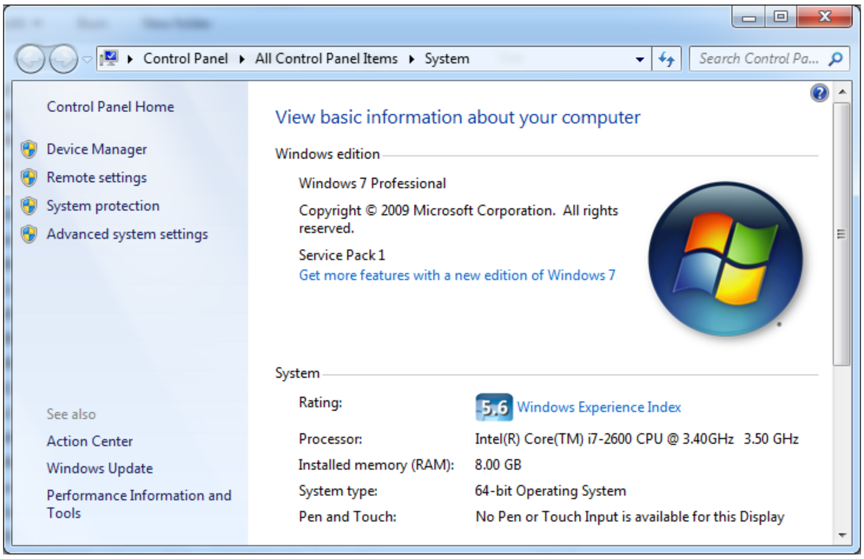
5.1.1 The pilot study

Case one - "Alleged attack on a private company and stole company secrets"

The test-bed shown in figure 4.6 was configured to reflect the case in order to collect data. These data will later be analysed and used to answer the research question and hypotheses developed for this study as defined in section 4.6.

The particular test-bed setup showed in figure 4.6 shows three different types of network. These diverse networks have the capability of providing ubiquitous wireless access to mobile SMART devices. The case involved in this section, an iPad was turned over to authorities and it triggers an investigation. When the data acquired from the iPad was examined, the investigator noticed two various accesses made from the iPad that looked suspicious. The access was made to a private company network and it showed that private documents were copied and uploaded to a private cloud account.

The machine that was used during the forensic investigation process was running on a 64bit Microsoft Windows 7 Professional with service pack one. The computer also runs on Intel core i7-2600 processor with eight gigabytes of memory.



View basic information about your computer

Windows edition

Windows 7 Professional

Copyright © 2009 Microsoft Corporation. All rights reserved.

Service Pack 1

Get more features with a new edition of Windows 7

System

Rating:	5.6 Windows Experience Index
Processor:	Intel(R) Core(TM) i7-2600 CPU @ 3.40GHz 3.50 GHz
Installed memory (RAM):	8.00 GB
System type:	64-bit Operating System
Pen and Touch:	No Pen or Touch Input is available for this Display

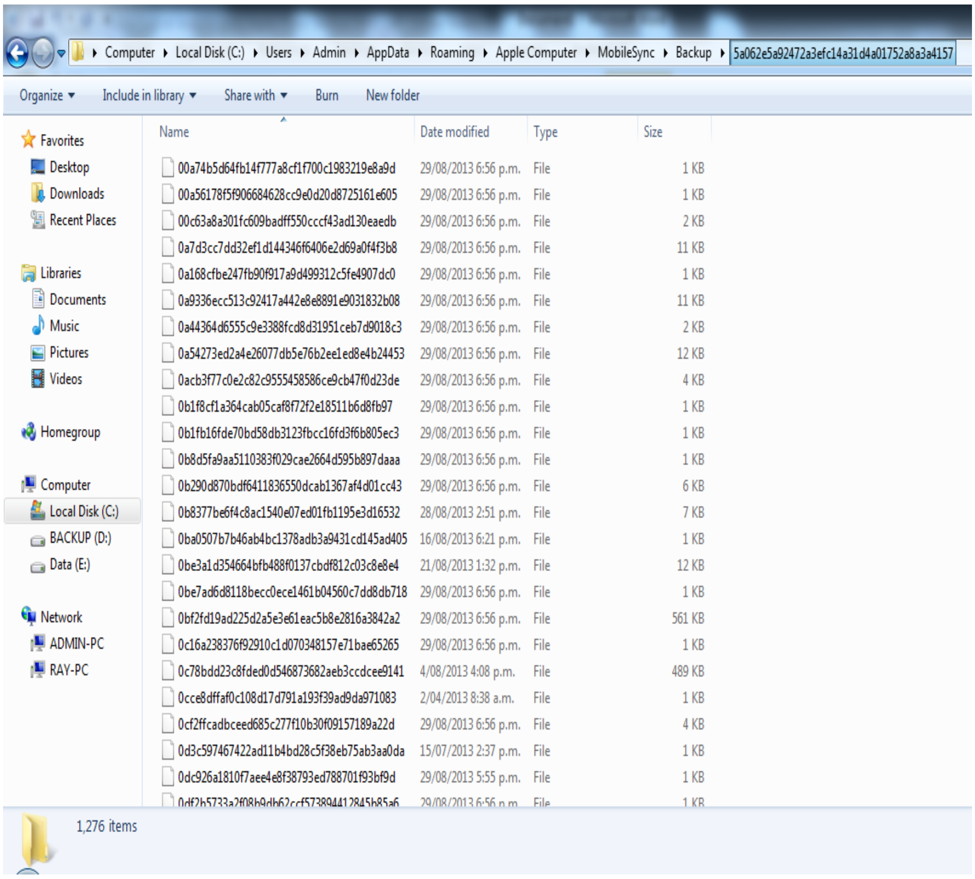
Figure 5.1: The specifications of forensic computer utilised.

Section 5.1.2 outlines the examination processes taken to find evidences of crimes committed during the pilot test.

5.1.2 The Examination Process

To examine the iPad, logical acquisition approach was the technique employed. Logical acquisition is defined as a bit-by-bit copy of objects stored logically such as directories and files stored on a logical store of the device such as the file system partition (see section 3.1.2). With regards to digital forensics tools employed for the pilot study, free and open source tools only were applied. The logical acquisition approach was taken and the SMART device involved was an iPad. As a result, the iTunes 11.0.5.5 is a free backup utility provided by Apple was used to acquire the data from the iPad, SQLite database browser was also employed to read the databases and the plistEditor Pro v2.1 was used to read the .plist files (see section 2.3.1).

Prior to acquiring the data from the iPad, the automatic synchronisation feature of iTunes was disabled. The iPad was then connected to the computer through the USB cable. The data acquisition process was then initiated manually and once completed; the iPad was disconnected to avoid further unsolicited processes. Data acquired from the iPad goes to the iTunes default backup location which is C:\Users\Admin\AppData\Roaming\Apple Computer \Mobile Sync\ Backup\. The name of the folder containing the data extracted from the iPad is very long which is a combination of forty hexadecimal characters "5a062e5a92472a3efc14a31d4a01752a8a3a4157" representing the unique identifier of the iPad. The names of the acquired files also adopted the same naming convention which signifies the unique identifier for each data obtained from the iPad (see section 2.5 and 3.4).

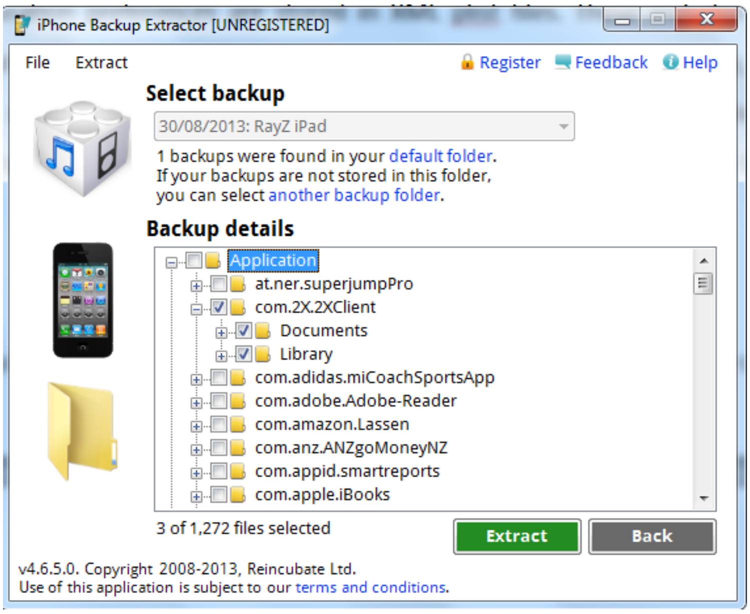


Name	Date modified	Type	Size
00a74b5d64fb14f777a8cf1f700c1983219e8a9d	29/08/2013 6:56 p.m.	File	1 KB
00a56178f5f906684628cc9e0d20d8725161e605	29/08/2013 6:56 p.m.	File	1 KB
00c63a8a301fc609badff550cccf43ad130eaedb	29/08/2013 6:56 p.m.	File	2 KB
0a7d3cc7dd32ef1d144346f6406e2d69a0f4f3b8	29/08/2013 6:56 p.m.	File	11 KB
0a168cfbe247fb90f917a9d499312c5fe4907dc0	29/08/2013 6:56 p.m.	File	1 KB
0a9336ecc513c92417a442e8e8891e9031832b08	29/08/2013 6:56 p.m.	File	11 KB
0a44364d6555c9e3388fcd8d31951ceb7d9018c3	29/08/2013 6:56 p.m.	File	2 KB
0a54273ed2a4e26077db5e76b2ee1ed8e4b24453	29/08/2013 6:56 p.m.	File	12 KB
0acb3f77c0e2c82c9555458586ce9cb47f0d23de	29/08/2013 6:56 p.m.	File	4 KB
0b1f8cf1a364cab05caf8f72f2e18511b6d8fb97	29/08/2013 6:56 p.m.	File	1 KB
0b1fb16fde70bd58db3123fbcc16fd3f6b805ec3	29/08/2013 6:56 p.m.	File	1 KB
0b8d5fa9aa5110383f029cae2664d595b897daaa	29/08/2013 6:56 p.m.	File	1 KB
0b290d870bdf6411836550dcab1367af4d01cc43	29/08/2013 6:56 p.m.	File	6 KB
0b8377be6f4c8ac1540e07ed01fb1195e3d16532	28/08/2013 2:51 p.m.	File	7 KB
0ba0507b7b46ab4bc1378adb3a9431cd145ad405	16/08/2013 6:21 p.m.	File	1 KB
0be3a1d354664bfb488f0137cbdf812c03c8e8e4	21/08/2013 1:32 p.m.	File	12 KB
0be7ad6d8118becc0ece1461b04560c7dd8db718	29/08/2013 6:56 p.m.	File	1 KB
0bf2fd19ad225d2a5e3e61eac5b8e2816a3842a2	29/08/2013 6:56 p.m.	File	561 KB
0c16a238376f92910c1d070348157e71bae65265	29/08/2013 6:56 p.m.	File	1 KB
0c78bdd23c8fded0d546873682aeb3ccdcee9141	4/08/2013 4:08 p.m.	File	489 KB
0cce8dffaf0c108d17d791a193f39ad9da971083	2/04/2013 8:38 a.m.	File	1 KB
0cf2ffcadbceed685c277f10b30f09157189a22d	29/08/2013 6:56 p.m.	File	4 KB
0d3c597467422ad11b4bd28c5f38eb75ab3aa0da	15/07/2013 2:37 p.m.	File	1 KB
0dc926a1810f7aee4e8f38793ed788701f93bf9d	29/08/2013 5:55 p.m.	File	1 KB
0df2b5733a2f08b9db62ccf573894412845b85a6	29/08/2013 6:56 p.m.	File	1 KB

Figure 5.2: Data acquired from the iPad.

The extracted data shown in figure 5.2 came in three different file formats the plist file, mddata files and the mdinfo files. The plist files are in Apple's property list file format which stores data in plaintext and can be read using the plist editor software. The mddata files stores data in raw binary format while the mdinfo file contains encoded metadata for the corresponding binary mddata files. In general, the iPad operating system (iOS) stores data in binary list and database files. Other information such as the device's status, application settings and user's configuration preferences are stored in XML plist files. These includes time zone, pairing records with devices and computer, email accounts, network identification, browser history, cookies and bookmarks. Information such as text messages, email messages, contacts list, call logs, notes, calendar are stored in SQLite database files. However, to read the binary files, a parsing tool called "iPhone Backup Extractor" is used (see section 2.3.1).

Various tools and techniques are applied and the iPhone backup extractor was the analysis tool that is employed to read the extract the binary files into a readable format as it showed in figure 5.2.



iPhone Backup Extractor [UNREGISTERED]

Select backup

30/08/2013: RayZ iPad

1 backups were found in your default folder.
If your backups are not stored in this folder,
you can select another backup folder.

Backup details

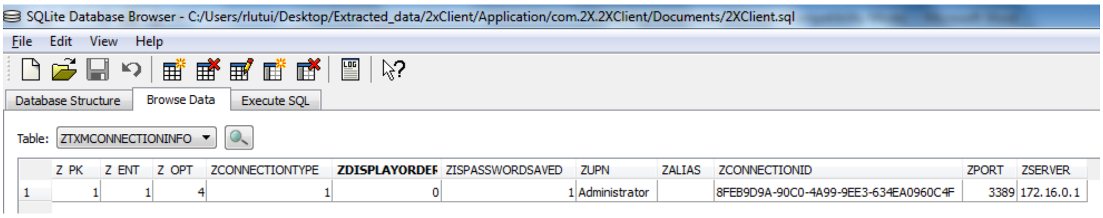
☐ Application
☐ at.ner.superjumpPro
☑ com.2X.2XClient
☑ Documents
☑ Library
☐ com.adidas.miCoachSportsApp
☐ com.adobe.Adobe-Reader
☐ com.amazon.Lassen
☐ com.anz.ANZgoMoneyNZ
☐ com.appid.smartreports
☐ com.apple.iBooks

3 of 1,272 files selected

v4.6.5.0. Copyright 2008-2013, Reincubate Ltd.
Use of this application is subject to our terms and conditions.

Figure 5.3: The iPhone Backup Extractor.

During the test, an application called 2xClient was used to access the private network from the iPad. The record was located in a folder named "com.2X.2XClient" as it showed in figure 5.4.



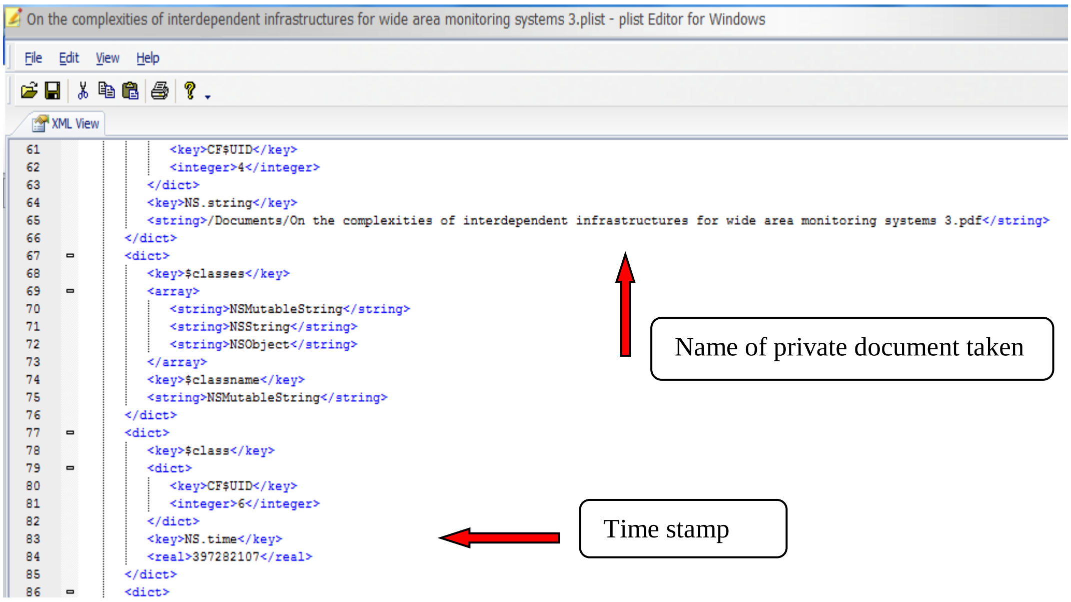
SQLite Database Browser - C:/Users/rlutui/Desktop/Extracted_data/2xClient/Application/com.2X.2XClient/Documents/2XClient.sql

Table: ZTXMCONNECTIONINFO

	Z PK	Z ENT	Z OPT	ZCONNECTIONTYPE	ZDISPLAYORDEF	ZISPASSWORDSAVED	ZUPN	ZALIAS	ZCONNECTIONID	ZPORT	ZSERVER
1	1	1	4	1	0	1	Administrator		8FEB9D9A-90C0-4A99-9EE3-634EA0960C4F	3389	172.16.0.1

Figure 5.4: 2xClient SQLite file.

As it can be seen in figure 5.4, the connection record stores the username used (Administrator), the connection ID, the access port number (3389) and IP address of the server (172.16.0.1) that the iPad accessed.

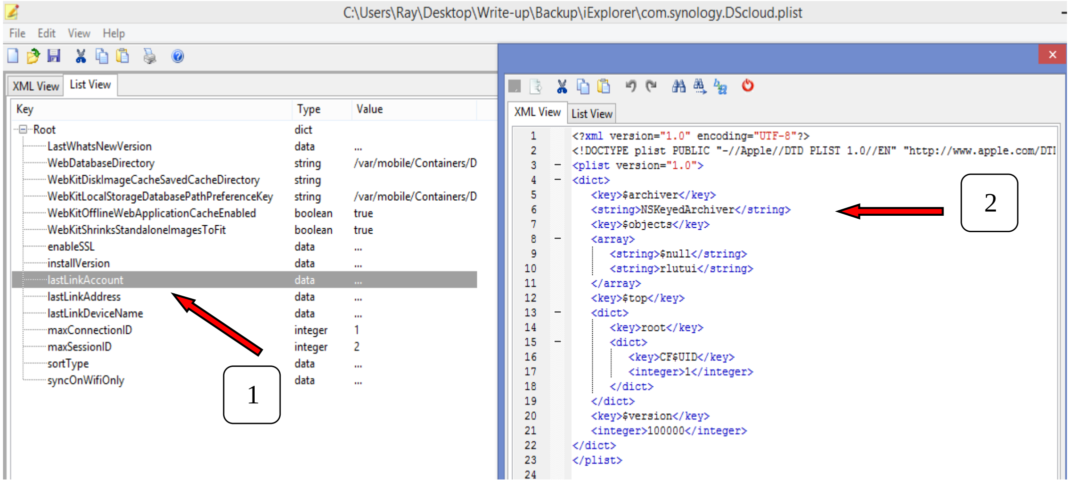


On the complexities of interdependent infrastructures for wide area monitoring systems 3.plist - plist Editor for Windows
File
Edit
View
Help
XML View
Name of private document taken
Time stamp

```
            <key>CF$UID</key>
            <integer>4</integer>
        </dict>
        <key>NS.string</key>
        <string>/Documents/On the complexities of interdependent infrastructures for wide area monitoring systems 3.pdf</string>
    </dict>
    <dict>
        <key>$classes</key>
        <array>
            <string>NSMutableString</string>
            <string>NSString</string>
            <string>NSObject</string>
        </array>
        <key>$classname</key>
        <string>NSMutableString</string>
    </dict>
    <dict>
        <key>$class</key>
        <dict>
            <key>CF$UID</key>
            <integer>6</integer>
        </dict>
        <key>NS.time</key>
        <real>397282107</real>
    </dict>
    <dict>
```

Figure 5.5: plist file record on com.comcsoft.iTransferPro.

The illustration presented in figure 5.5 showed the complexities of interdependent infrastructures. The illustration was taken from the Apple's property list file. Figure 5.5 showed two significant potential evidences. One is the name of one of the documents taken from the private company's network and the second is the time of the incident. An online Unix Time Conversion tool was used to convert "397282107" to "Wed, 04 Aug 2013 04:08:27 GMT" and following in figure 5.6, 5.7 and 5.8 are information of the private account accessed.



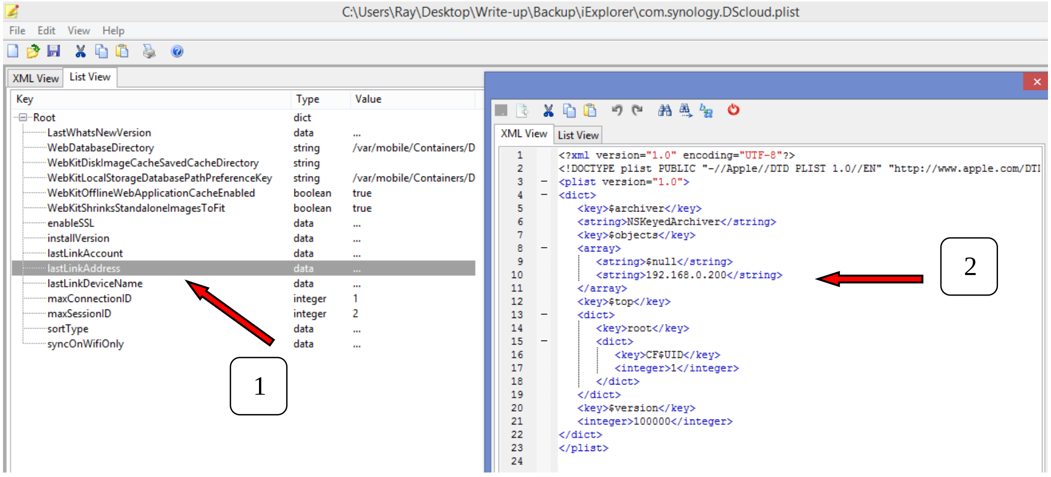
C:\Users\Ray\Desktop\Write-up\Backup\iExplorer\com.synology.DScloud.plist
File
Edit
View
Help
XML View
List View
1
2

Key	Type	Value
Root	dict	
LastWhatsNewVersion	data	...
WebDatabaseDirectory	string	/var/mobile/Containers/D
WebKitDiskImageCacheSavedCacheDirectory	string	
WebKitLocalStorageDatabasePathPreferenceKey	string	/var/mobile/Containers/D
WebKitOfflineWebApplicationCacheEnabled	boolean	true
WebKitShrinksStandaloneImagesToFit	boolean	true
enableSSL	data	...
installVersion	data	...
lastLinkAccount	data	...
lastLinkAddress	data	...
lastLinkDeviceName	data	...
maxConnectionID	integer	1
maxSessionID	integer	2
sortType	data	...
syncOnWifiOnly	data	...

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTI
<plist version="1.0">
<dict>
    <key>$archiver</key>
    <string>NSKeyedArchiver</string>
    <key>$objects</key>
    <array>
        <string>$null</string>
        <string>rlutui</string>
    </array>
    <key>$top</key>
    <dict>
        <key>root</key>
        <dict>
            <key>CF$UID</key>
            <integer>1</integer>
        </dict>
    </dict>
    <key>$version</key>
    <integer>100000</integer>
</dict>
</plist>
```

Figure 5.6: Login detail for the cloud.

Double clicking on the data labelled number one shows the data displaying on the right. Number two shows the account detail used to access the private cloud account.



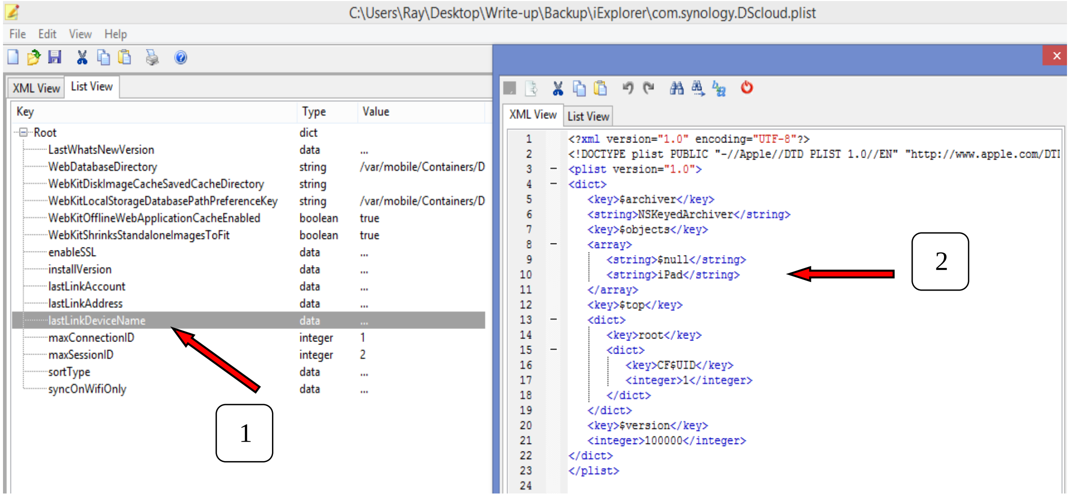
C:\Users\Ray\Desktop\Write-up\Backup\iExplorer\com.synology.DScloud.plist

Key	Type	Value
Root	dict	
LastWhatsNewVersion	data	...
WebDatabaseDirectory	string	/var/mobile/Containers/D
WebKitDiskImageCacheSavedCacheDirectory	string	
WebKitLocalStorageDatabasePathPreferenceKey	string	/var/mobile/Containers/D
WebKitOfflineWebApplicationCacheEnabled	boolean	true
WebKitShrinksStandaloneImagesToFit	boolean	true
enableSSL	data	...
installVersion	data	...
lastLinkAccount	data	...
lastLinkAddress	data	...
lastLinkDeviceName	data	...
maxConnectionID	integer	1
maxSessionID	integer	2
sortType	data	...
syncOnWifiOnly	data	...

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTI
<plist version="1.0">
<dict>
   <key>$archiver</key>
   <string>NSKeyedArchiver</string>
   <key>$objects</key>
   <array>
      <string>$null</string>
      <string>192.168.0.200</string>
   </array>
   <key>$top</key>
   <dict>
      <key>root</key>
      <dict>
         <key>CF$UID</key>
         <integer>1</integer>
      </dict>
   </dict>
   <key>$version</key>
   <integer>100000</integer>
</dict>
</plist>
```

Figure 5.7: IP address of the accessed.

Accessing the data labelled number one in figure 5.7 shows data number two. Window number two shows the IP address that was used to access the private cloud account.



C:\Users\Ray\Desktop\Write-up\Backup\iExplorer\com.synology.DScloud.plist

Key	Type	Value
Root	dict	
LastWhatsNewVersion	data	...
WebDatabaseDirectory	string	/var/mobile/Containers/D
WebKitDiskImageCacheSavedCacheDirectory	string	
WebKitLocalStorageDatabasePathPreferenceKey	string	/var/mobile/Containers/D
WebKitOfflineWebApplicationCacheEnabled	boolean	true
WebKitShrinksStandaloneImagesToFit	boolean	true
enableSSL	data	...
installVersion	data	...
lastLinkAccount	data	...
lastLinkAddress	data	...
lastLinkDeviceName	data	...
maxConnectionID	integer	1
maxSessionID	integer	2
sortType	data	...
syncOnWifiOnly	data	...

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTI
<plist version="1.0">
<dict>
   <key>$archiver</key>
   <string>NSKeyedArchiver</string>
   <key>$objects</key>
   <array>
      <string>$null</string>
      <string>iPad</string>
   </array>
   <key>$top</key>
   <dict>
      <key>root</key>
      <dict>
         <key>CF$UID</key>
         <integer>1</integer>
      </dict>
   </dict>
   <key>$version</key>
   <integer>100000</integer>
</dict>
</plist>
```

Figure 5.8: plist file record on com.synology.DSfile.

The illustration showed in figure 5.8 has two windows. Window one contains detail information regarding some of the databases can be found in root directory. Inside root, there is a database that contains information about the name of the last device that connects to this account. When this database is opened as shown in window number two, it showed the name of the device that was last used to access the cloud account. In section 5.1.3 the data collected from the fictitious test case scenario two is reported.

5.1.3 The Case Scenario Two

Case two - "Alleged young children kidnapping and trafficking"

A deal gone wrong and from that crime scene a mobile SMART device was found and suspected of being involved in some criminal activities. When that mobile SMART device went through the data acquisition phase, the data showed some e-mail messages were received from a private company e-mail address. During the data analysis phase, the investigator found that a private cloud account has been used many times to upload and download images. The test-bed that was used to process case one was also used to process this case scenario. The hardware and operating system specifications for the forensic computer were also kept the same. However, during the data acquisition and data analysis phase, a different software application was employed. The Forensic Tool Kit – FTK Imager 3.2.0.0 from AccessData Group was employed to acquire and analyse the data.

5.2.2 Data Acquisition Process

The FTK Imager was engaged during the process of extracting data from the suspected computer hard disk.

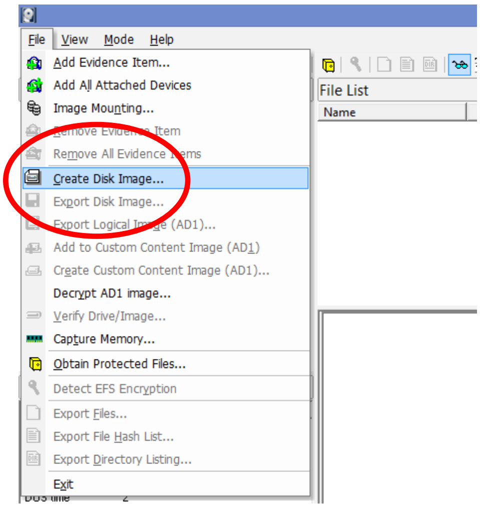
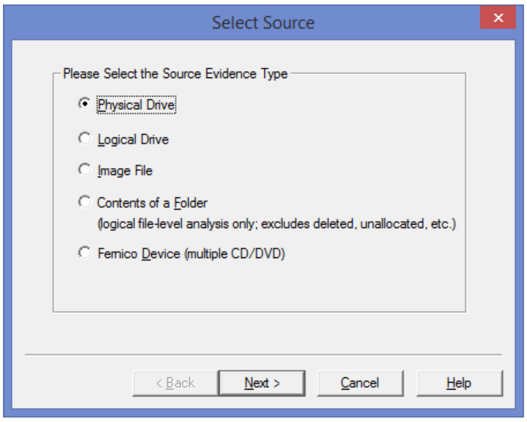


Figure 5.9: Creating an image of the hard disk.

To extract data from the suspected hard disk, the physical acquisition approach was taken as it shows in figure 5.10. After selecting the source evidence type then in figure 5.11 asks for the source drive.



Select Source

Please Select the Source Evidence Type

● Physical Drive

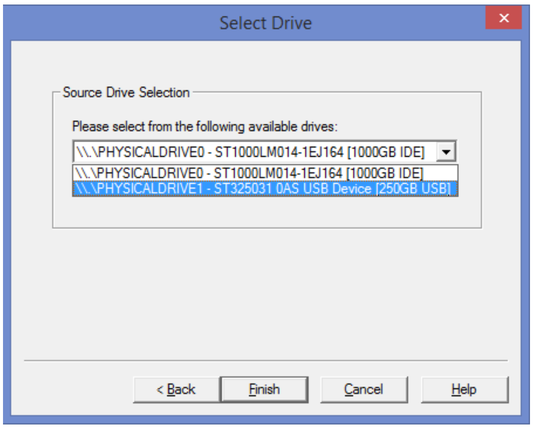
○ Logical Drive

○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

○ Femico Device (multiple CD/DVD)

Figure 5.10: The physical acquisition approach.



Select Drive

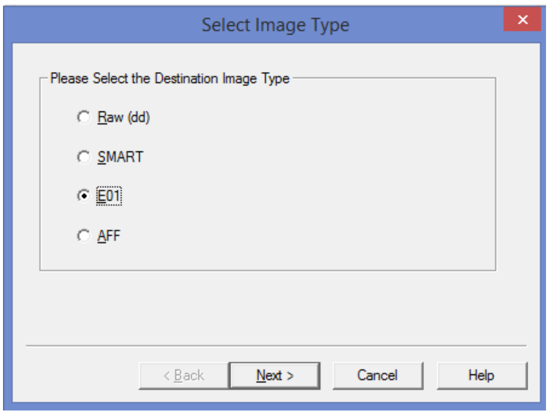
Source Drive Selection

Please select from the following available drives:

\\.\PHYSICALDRIVE0 - ST1000LM014-1EJ164 [1000GB IDE]
\\.\PHYSICALDRIVE0 - ST1000LM014-1EJ164 [1000GB IDE]
\\.\PHYSICALDRIVE1 - ST325031 0AS USB Device [250GB USB]

Figure 5.11: The source drive selection.

After selecting the source drive, the location of the hard disk that contain all the potential evidences. The next task is to determine the type of image required. In FTK Imager, there are four to select from, the raw image dd format also known as GNU dd, SMART, E01 and AFF.



Select Image Type

Please Select the Destination Image Type

○ Raw (dd)

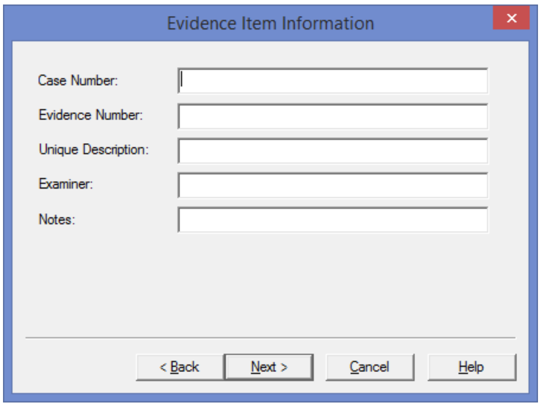
○ SMART

● E01

○ AFF

Figure 5.12: The destination type.

As it is shown in figure 5.12, in this case the Encase file format E01 was selected. The next window form asked for the detail information for the evidence as it is shown in figure 5.13. In figure 5.14 the form asked to point to the destination folder that will be used for the image.



Case Number:

Evidence Number:

Unique Description:

Examiner:

Notes:

Figure 5.13: The evidence information.

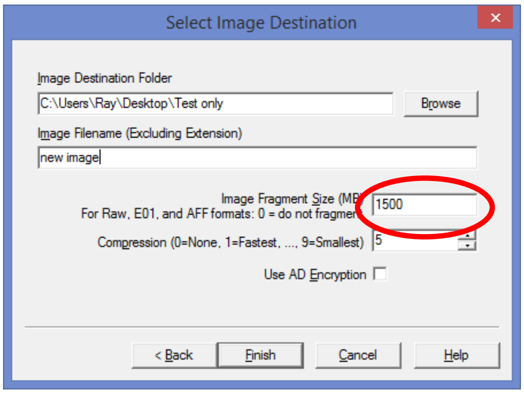


Image Destination Folder
C:\Users\Ray\Desktop\Test only

Image Filename (Excluding Extension)
new image

Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment 1500

Compression (0=None, 1=Fastest, ..., 9=Smallest) 5

Use AD Encryption □

Figure 5.14: The destination information for the image.

In the next field in figure 5.14 it asked for a name for the new image but without the file extension.

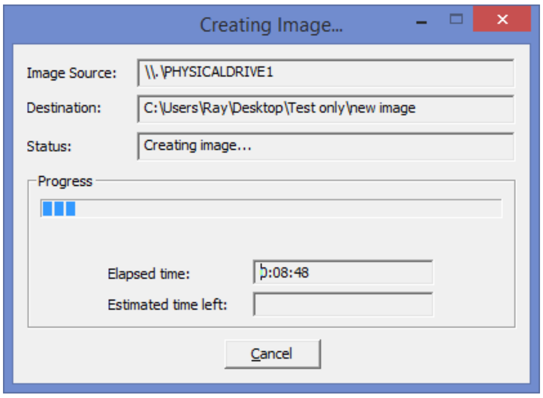


Image Source: \\.\PHYSICALDRIVE1

Destination: C:\Users\Ray\Desktop\Test only\new image

Status: Creating image...

Elapsed time: 0:08:48

Estimated time left:

Figure 5.15: The creation of the image.

Notice in the field with the red coloured circle in figure 5.14, if the image needs to be fragmented, each fragment size can be defined here in MegaBytes. For this scenario's image, a zero (0) was entered indicating that a non-fragmented image is required. In the image creation window as it showed in figure 5.15, it provides all the necessary information such as the source of the image and its destination. The progress bar provided an estimation of the duration of the whole task.

5.1.4 Data Analysis Process

After creating an image of the hard disk, to analyse the image for potential evidences, the image needs to be added into FTK Imager. Following this process of adding the acquired image to FTK Imager, figure 5.17 shows source type selection.

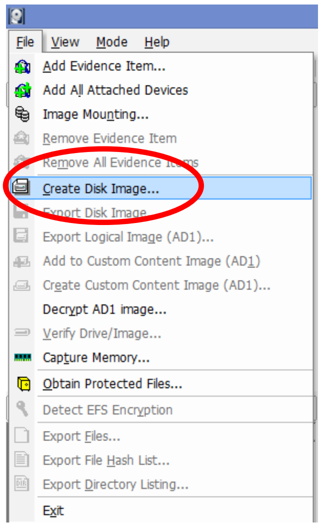
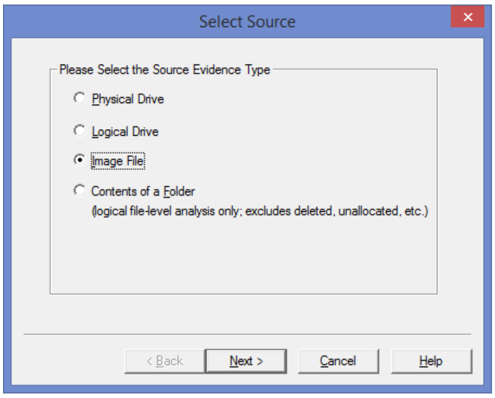


Figure 5.16: Adding image to FTK Imager.



Please Select the Source Evidence Type

○ Physical Drive

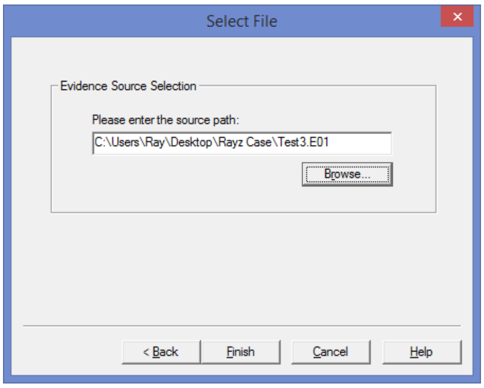
○ Logical Drive

● Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

Figure 5.17: Select type of source evidence.

The eclipse in figure 5.16 showed where to click to add the image. Next, in the pop up window, the analyst needs to select the of the source images. In this case, it will have to be an image file.



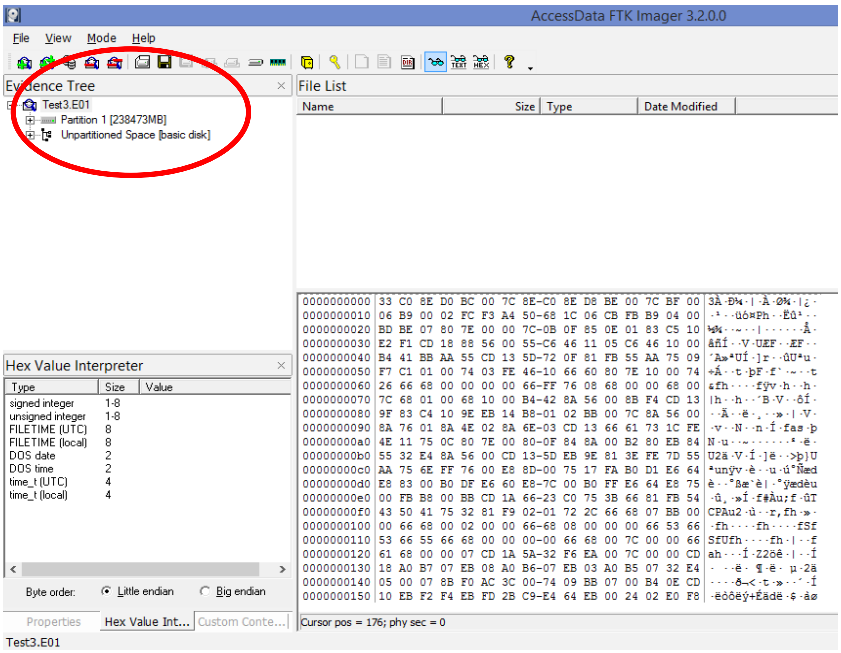
Evidence Source Selection

Please enter the source path:

C:\Users\Ray\Desktop\Rayz Case\Test3.E01

Figure 5.18: Select the path of source image.

In the next pop up window, the path to the image is defined. The eclipse in figure 5.19 showed what will appear in FTK Imager after adding the acquired image to FTK Imager. In this case, as it is illustrated in figure 5.10, the data acquisition approach was the physical acquisition method.



Type	Size	Value
signed integer	1-8	
unsigned integer	1-8	
FILETIME (UTC)	8	
FILETIME (local)	8	
DOS date	2	
DOS time	2	
time_t (UTC)	4	
time_t (local)	4	

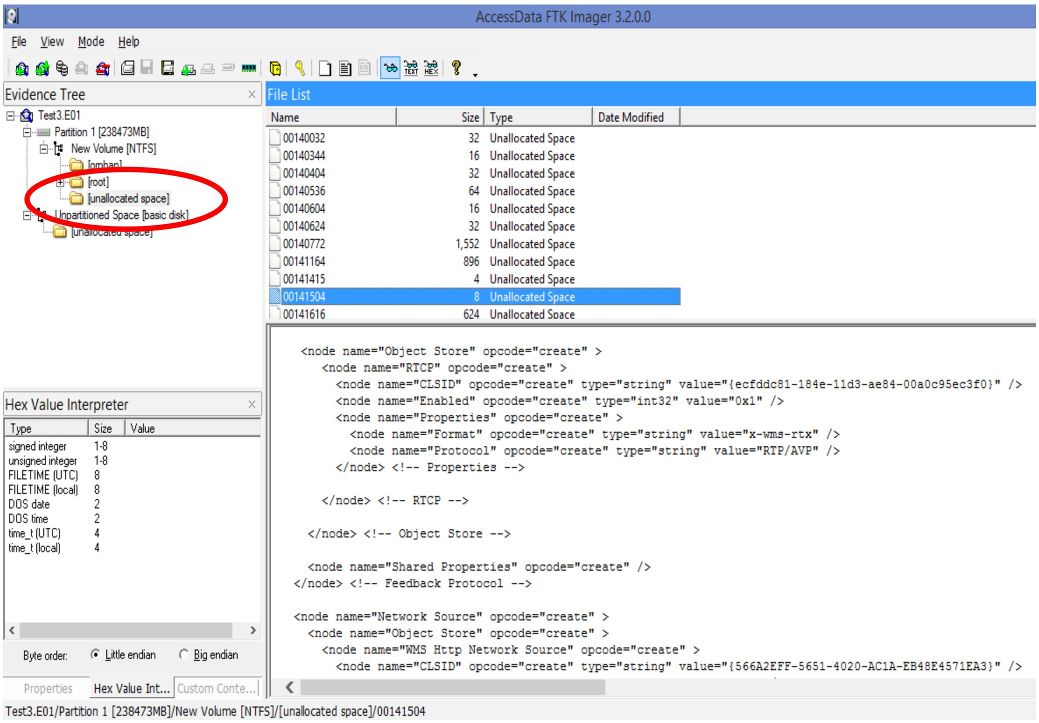
Byte order: ● Little endian ○ Big endian

```
0000000000 33 C0 8E D0 BC 00 7C 8E-C0 8E D8 BE 00 7C BF 00 3À·Ð¼·|·À·Ø¾·|¿·
0000000010 06 B9 00 02 FC F3 A4 50-68 1C 06 CB FB B9 04 00 ·¹··üó¤Ph··Ëû¹··
0000000020 BD BE 07 80 7E 00 00 7C-0B 0F 85 0E 01 83 C5 10 ½¾··~··|······Å·
0000000030 E2 F1 CD 18 88 56 00 55-C6 46 11 05 C6 46 10 00 âñÍ··V·UÆF··ÆF··
0000000040 B4 41 BB AA 55 CD 13 5D-72 0F 81 FB 55 AA 75 09 ´A»ªUÍ·]r··ûUªu·
0000000050 F7 C1 01 00 74 03 FE 46-10 66 60 80 7E 10 00 74 ÷Á··t·þF·f`·~··t
0000000060 26 66 68 00 00 00 00 66-FF 76 08 68 00 00 68 00 &fh····fÿv·h··h·
0000000070 7C 68 01 00 68 10 00 B4-42 8A 56 00 8B F4 CD 13 |h··h··´B·V··ôÍ·
0000000080 9F 83 C4 10 9E EB 14 B8-01 02 BB 00 7C 8A 56 00 ··Ä··ë·¸··»·|·V·
0000000090 8A 76 01 8A 4E 02 8A 6E-03 CD 13 66 61 73 1C FE ·v··N··n·Í·fas·þ
00000000a0 4E 11 75 0C 80 7E 00 80-0F 84 8A 00 B2 80 EB 84 N·u··~······²·ë·
00000000b0 55 32 E4 8A 56 00 CD 13-5D EB 9E 81 3E FE 7D 55 U2ä·V·Í·]ë··>þ}U
00000000c0 AA 75 6E FF 76 00 E8 8D-00 75 17 FA B0 D1 E6 64 ªunÿv·è··u·ú°Ñæd
00000000d0 E8 83 00 B0 DF E6 60 E8-7C 00 B0 FF E6 64 E8 75 è··°ßæ`è|·°ÿædèu
00000000e0 00 FB B8 00 BB CD 1A 66-23 C0 75 3B 66 81 FB 54 ·û¸·»Í·f#Àu;f·ûT
00000000f0 43 50 41 75 32 81 F9 02-01 72 2C 66 68 07 BB 00 CPAu2·ù··r,fh·»·
0000000100 00 66 68 00 02 00 00 66-68 08 00 00 00 66 53 66 ·fh····fh····fSf
0000000110 53 66 55 66 68 00 00 00-00 66 68 00 7C 00 00 66 SfUfh····fh·|··f
0000000120 61 68 00 00 07 CD 1A 5A-32 F6 EA 00 7C 00 00 CD ah···Í·Z2öê·|··Í
0000000130 18 A0 B7 07 EB 08 A0 B6-07 EB 03 A0 B5 07 32 E4 · ··ë· ¶·ë· µ·2ä
0000000140 05 00 07 8B F0 AC 3C 00-74 09 BB 07 00 B4 0E CD ····ð¬<·t·»··´·Í
0000000150 10 EB F2 F4 EB FD 2B C9-E4 64 EB 00 24 02 E0 F8 ·ëòôëý+Éädë·$·àø
```

Cursor pos = 176; phy sec = 0

Figure 5.19: Image with potential evidences in FTK Imager.

As a result, the tool also extracted the deleted data located in the unallocated partitions. Figure 5.20 showed a piece of code found in an unallocated space of the partition where the potential evidences may be located in the extracted image.



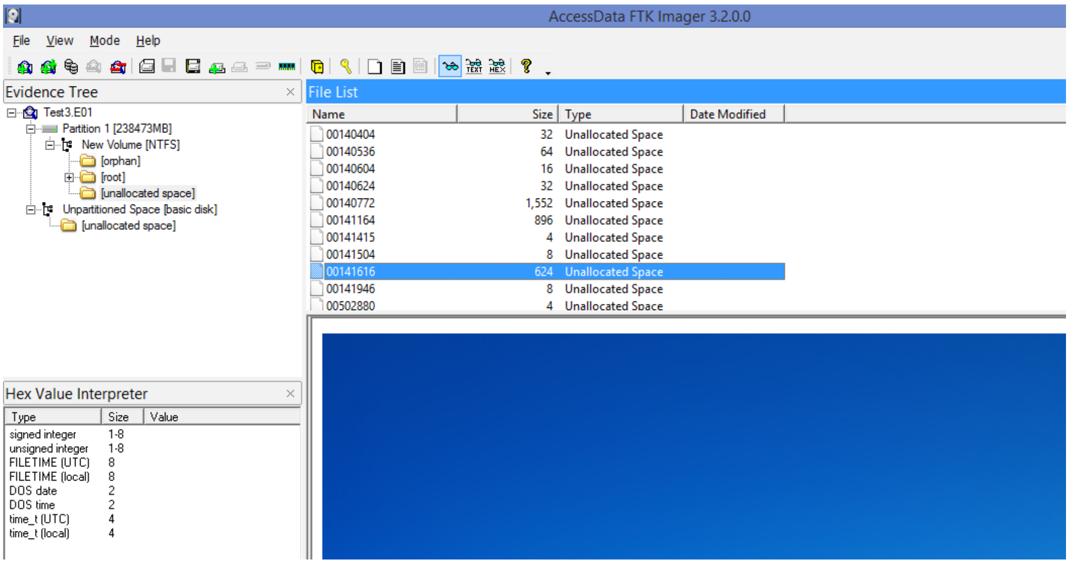
Name	Size	Type	Date Modified
00140032	32	Unallocated Space	
00140344	16	Unallocated Space	
00140404	32	Unallocated Space	
00140536	64	Unallocated Space	
00140604	16	Unallocated Space	
00140624	32	Unallocated Space	
00140772	1,552	Unallocated Space	
00141164	896	Unallocated Space	
00141415	4	Unallocated Space	
00141504	8	Unallocated Space	
00141616	624	Unallocated Space	

Type	Size	Value
signed integer	1-8	
unsigned integer	1-8	
FILETIME (UTC)	8	
FILETIME (local)	8	
DOS date	2	
DOS time	2	
time_t (UTC)	4	
time_t (local)	4	

```
   <node name="Object Store" opcode="create" >
      <node name="RTCP" opcode="create" >
        <node name="CLSID" opcode="create" type="string" value="{ecfddc81-184e-11d3-ae84-00a0c95ec3f0}" />
        <node name="Enabled" opcode="create" type="int32" value="0x1" />
        <node name="Properties" opcode="create" >
          <node name="Format" opcode="create" type="string" value="x-wms-rtx" />
          <node name="Protocol" opcode="create" type="string" value="RTP/AVP" />
        </node> <!-- Properties -->

      </node> <!-- RTCP -->

    </node> <!-- Object Store -->

    <node name="Shared Properties" opcode="create" />
  </node> <!-- Feedback Protocol -->

  <node name="Network Source" opcode="create" >
    <node name="Object Store" opcode="create" >
      <node name="WMS Http Network Source" opcode="create" >
        <node name="CLSID" opcode="create" type="string" value="{566A2EFF-5651-4020-AC1A-EB48E4571EA3}" />
```

Test3.E01/Partition 1 [238473MB]/New Volume [NTFS]/[unallocated space]/00141504

Figure 5.20: Example of information stored in the unallocated/deleted space.



Name	Size	Type	Date Modified
00140404	32	Unallocated Space	
00140536	64	Unallocated Space	
00140604	16	Unallocated Space	
00140624	32	Unallocated Space	
00140772	1,552	Unallocated Space	
00141164	896	Unallocated Space	
00141415	4	Unallocated Space	
00141504	8	Unallocated Space	
00141616	624	Unallocated Space	
00141946	8	Unallocated Space	
00502880	4	Unallocated Space	

Type	Size	Value
signed integer	1-8	
unsigned integer	1-8	
FILETIME (UTC)	8	
FILETIME (local)	8	
DOS date	2	
DOS time	2	
time_t (UTC)	4	
time_t (local)	4	

Figure 5.21: Example of information stored in the unallocated/deleted space.

Also figure 5.21 showed another sample of an image found in the unallocated space. In the case of potential evidences, in figure 5.22, a list of users was found. However, in that list there is only one legitimate user name which is *"rlutui."* Inside the document directory of the *"rlutui"* username, a text document named contacts.txt was found. In this document, three names from one company were found along with their street address, mobile number and e-mail address.

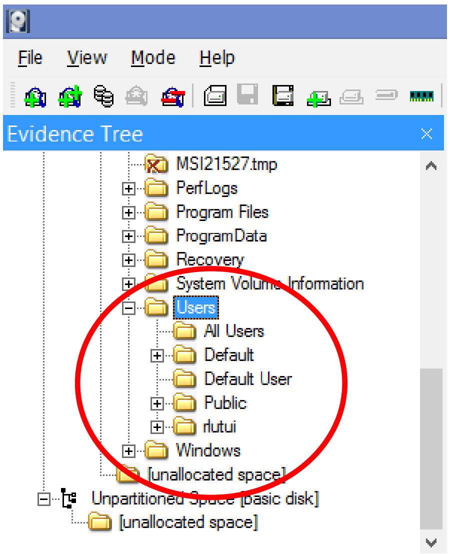
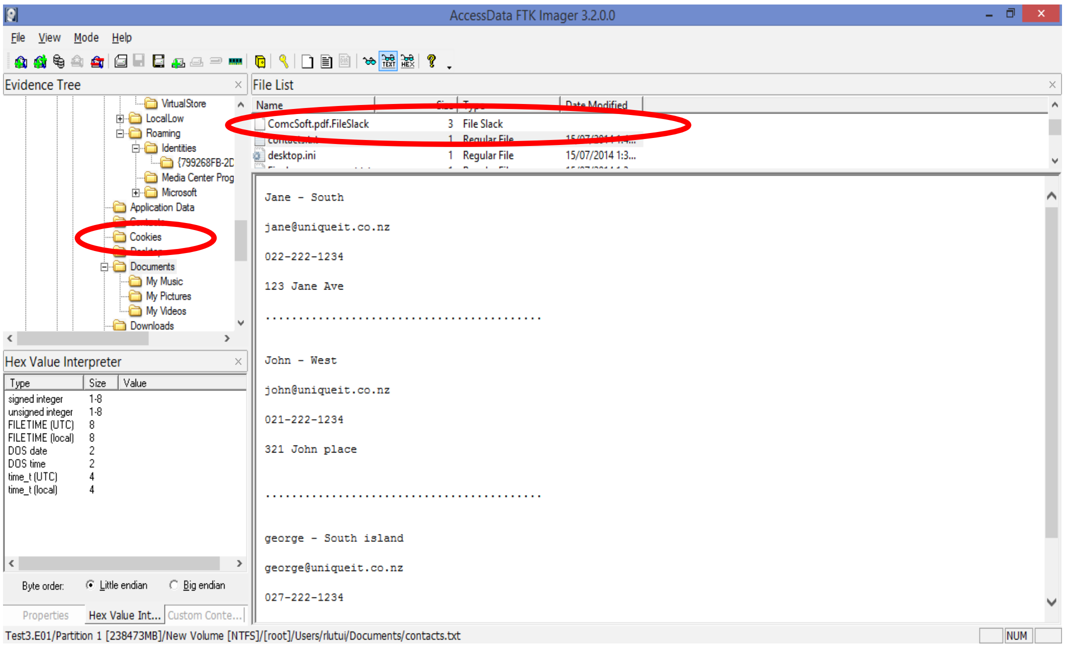


Figure 5.22: List of users' found on the acquired image.



Name	Size	Type	Date Modified
ComcSoft.pdf.FileSlack	3	File Slack	
desktop.ini	1	Regular File	15/07/2014 1:3...

```
Jane - South

jane@uniqueit.co.nz

022-222-1234

123 Jane Ave

.........................................


John - West

john@uniqueit.co.nz

021-222-1234

321 John place


.........................................


george - South island

george@uniqueit.co.nz

027-222-1234
```

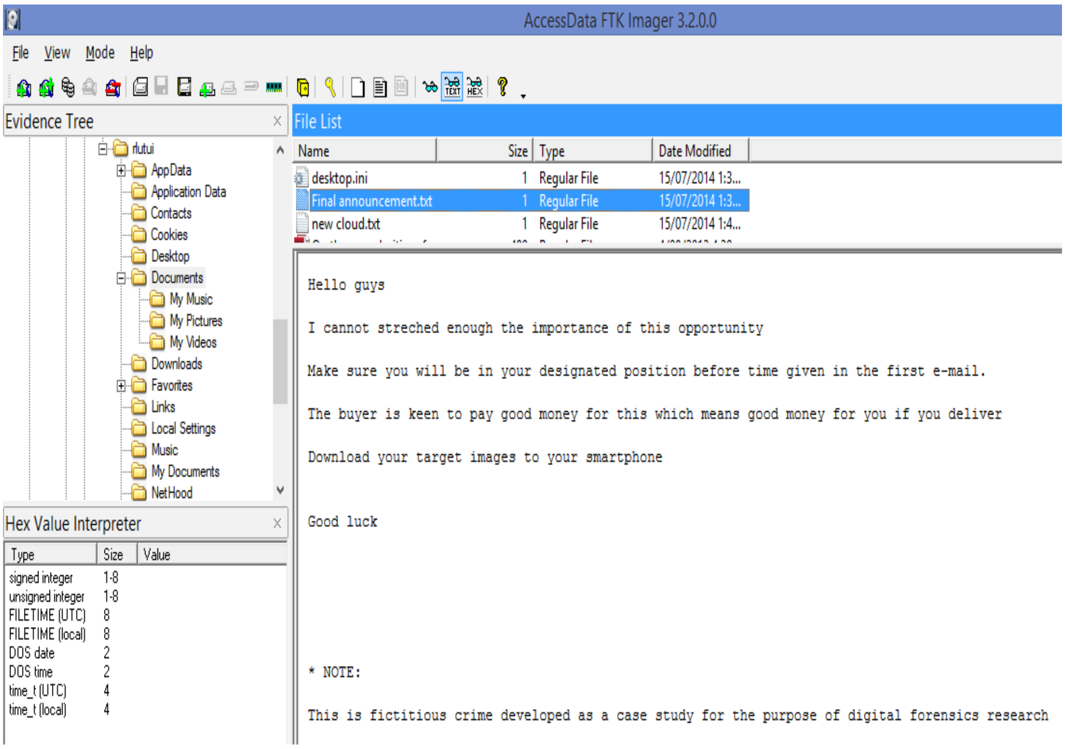
Type	Size	Value
signed integer	1-8	
unsigned integer	1-8	
FILETIME (UTC)	8	
FILETIME (local)	8	
DOS date	2	
DOS time	2	
time_t (UTC)	4	
time_t (local)	4	

Byte order: ● Little endian ○ Big endian

Test3.E01/Partition 1 [238473MB]/New Volume [NTFS]/[root]/Users/rlutui/Documents/contacts.txt

Figure 5.23: Contact information found on a text document.

The contact information will be very useful in an investigation. Another text document was also found named *"final announcement.txt."* The information in this document indicated that some kind of important deal is going to happen as it is illustrated in figure 5.24.

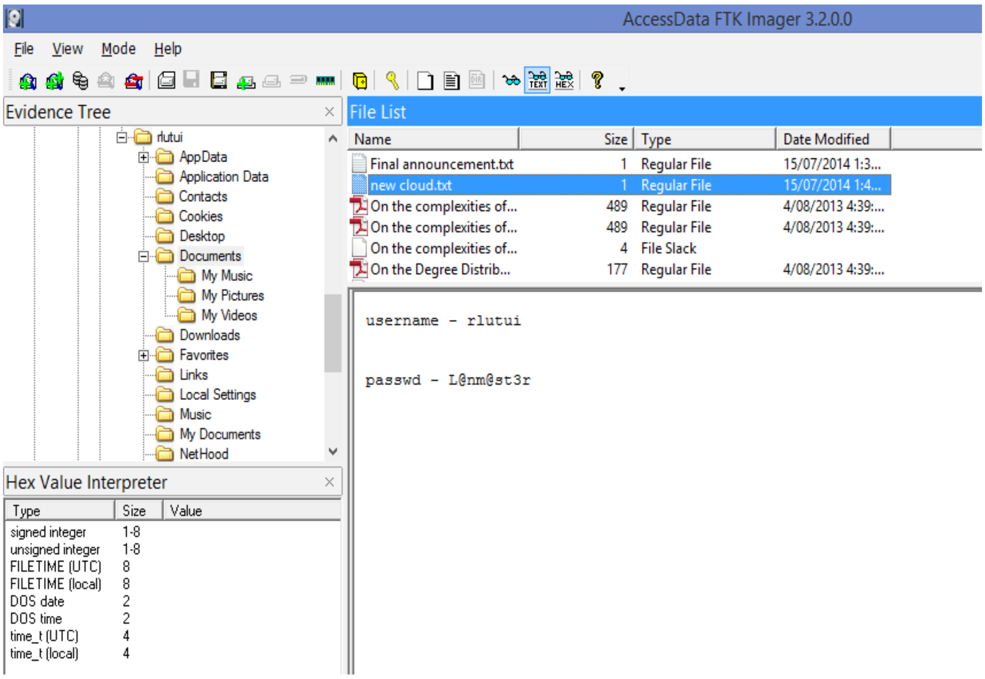


Type	Size	Value
signed integer	1-8	
unsigned integer	1-8	
FILETIME (UTC)	8	
FILETIME (local)	8	
DOS date	2	
DOS time	2	
time_t (UTC)	4	
time_t (local)	4	

Name	Size	Type	Date Modified
desktop.ini	1	Regular File	15/07/2014 1:3...
Final announcement.txt	1	Regular File	15/07/2014 1:3...
new cloud.txt	1	Regular File	15/07/2014 1:4...

```
Hello guys

I cannot streched enough the importance of this opportunity

Make sure you will be in your designated position before time given in the first e-mail.

The buyer is keen to pay good money for this which means good money for you if you deliver

Download your target images to your smartphone


Good luck





* NOTE:

This is fictitious crime developed as a case study for the purpose of digital forensics research
```

Figure 5.24: More information found on the announcement text document.



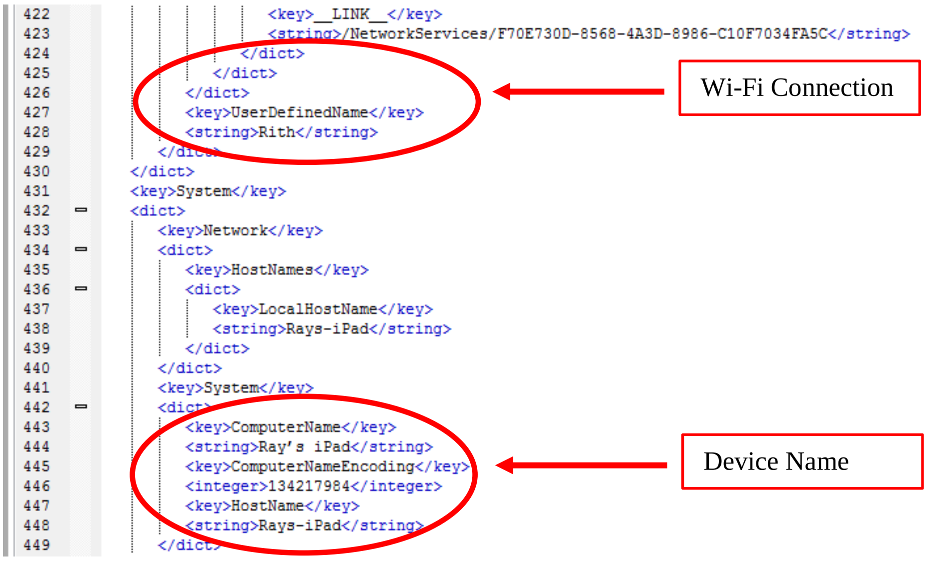
Type	Size	Value
signed integer	1-8	
unsigned integer	1-8	
FILETIME (UTC)	8	
FILETIME (local)	8	
DOS date	2	
DOS time	2	
time_t (UTC)	4	
time_t (local)	4	

Name	Size	Type	Date Modified
Final announcement.txt	1	Regular File	15/07/2014 1:3...
new cloud.txt	1	Regular File	15/07/2014 1:4...
On the complexities of...	489	Regular File	4/08/2013 4:39:...
On the complexities of...	489	Regular File	4/08/2013 4:39:...
On the complexities of...	4	File Slack	
On the Degree Distrib...	177	Regular File	4/08/2013 4:39:...

```
username - rlutui


passwd - L@nm@st3r
```

Figure 5.25: More information found on the cloud text document.

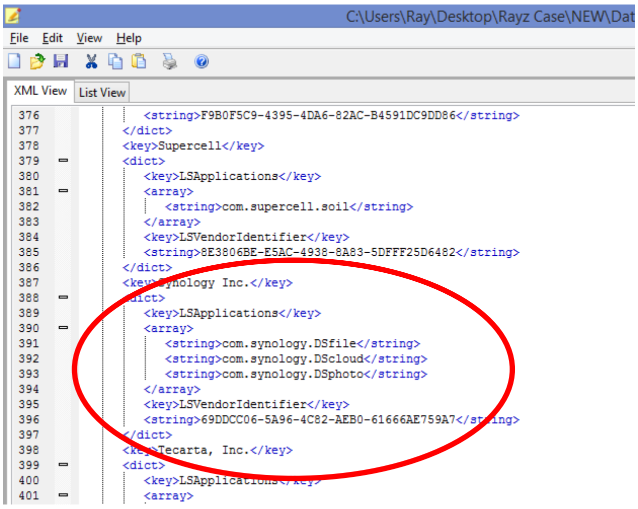
Another text document named *"new cloud.txt"* was found. In this document, it was only a username and a password was stored. As mentioned earlier in this chapter, FTK Imager was employed to extract data from suspected hard disk and also to analyse the acquired data. The same tools that was employed to acquire and analysed the data from the iPad in scenario one was also employed to acquire and examine the iPad in scenario two. After extracting the data from the iPad, the plist editor pro v2.1 tool was employed to read the Apple property list files that was acquired from the iPad.



```
          <key>__LINK__</key>
          <string>/NetworkServices/F70E730D-8568-4A3D-8986-C10F7034FA5C</string>
        </dict>
      </dict>
    </dict>
    <key>UserDefinedName</key>
    <string>Rith</string>
  </dict>
</dict>
<key>System</key>
<dict>
  <key>Network</key>
  <dict>
    <key>HostNames</key>
    <dict>
      <key>LocalHostName</key>
      <string>Rays-iPad</string>
    </dict>
  </dict>
  <key>System</key>
  <dict>
    <key>ComputerName</key>
    <string>Ray’s iPad</string>
    <key>ComputerNameEncoding</key>
    <integer>134217984</integer>
    <key>HostName</key>
    <string>Rays-iPad</string>
  </dict>
```

Figure 5.26: Device information and Wi-Fi connection details.

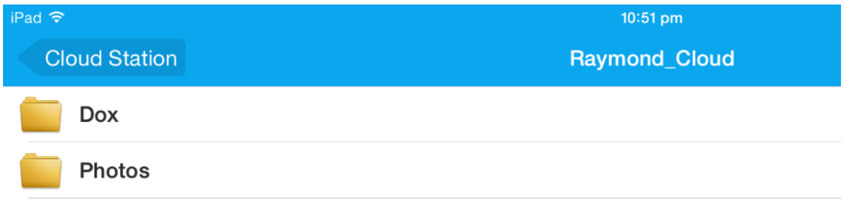
After using the iPhone Extractor tool to extract the backup image from the iPad, a directory named *“SystemConfiguration”* was created and in this directory a file named *“preferences.plist”* was found. Figure 5.26 showed the information contained in this file, the name of the device and the name of the Wi-Fi that it was connected to.



```
    <string>F9B0F5C9-4395-4DA6-82AC-B4591DC9DD86</string>
  </dict>
  <key>Supercell</key>
  <dict>
    <key>LSApplications</key>
    <array>
      <string>com.supercell.soil</string>
    </array>
    <key>LSVendorIdentifier</key>
    <string>8E3806BE-E5AC-4938-8A83-5DFFF25D6482</string>
  </dict>
  <key>Synology Inc.</key>
  <dict>
    <key>LSApplications</key>
    <array>
      <string>com.synology.DSfile</string>
      <string>com.synology.DScloud</string>
      <string>com.synology.DSphoto</string>
    </array>
    <key>LSVendorIdentifier</key>
    <string>69DDCC06-5A96-4C82-AEB0-61666AE759A7</string>
  </dict>
  <key>Tecarta, Inc.</key>
  <dict>
    <key>LSApplications</key>
    <array>
```

Figure 5.27: Cloud information found on plist.

A .plist file named *"com.apple.lsdidentifiers"* was also found in the iPad. Three applications from a company known as Synology.Inc, these applications are used to access cloud. In figure 5.25 showed a log in information to a private cloud that was found in the hard disk image. There was no information found in the hard disk to indicate which cloud provider but the information shown in figure 5.27 must be the private cloud provider that the iPad accessed. When the login details were tried on the Synology cloud application, two directories were found in this account as shown in figure 5.28 and also the name of the account owner.

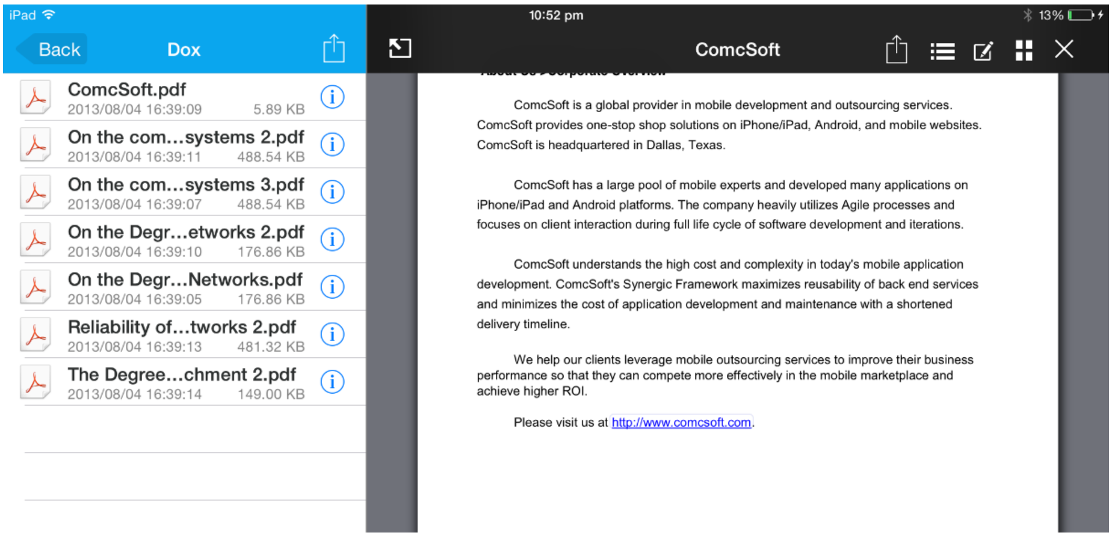


Dox

Photos

Figure 5.28: Content of the cloud account found.

In the Dox directory, figure 5.29 showed the content of this directory. Figure 5.30 showed the content of the Photos directory.



ComcSoft.pdf	2013/08/04 16:39:09	5.89 KB
On the com...systems 2.pdf	2013/08/04 16:39:11	488.54 KB
On the com...systems 3.pdf	2013/08/04 16:39:07	488.54 KB
On the Degr...etworks 2.pdf	2013/08/04 16:39:10	176.86 KB
On the Degr...Networks.pdf	2013/08/04 16:39:05	176.86 KB
Reliability of...tworks 2.pdf	2013/08/04 16:39:13	481.32 KB
The Degree...chment 2.pdf	2013/08/04 16:39:14	149.00 KB

ComcSoft is a global provider in mobile development and outsourcing services. ComcSoft provides one-stop shop solutions on iPhone/iPad, Android, and mobile websites. ComcSoft is headquartered in Dallas, Texas.

ComcSoft has a large pool of mobile experts and developed many applications on iPhone/iPad and Android platforms. The company heavily utilizes Agile processes and focuses on client interaction during full life cycle of software development and iterations.

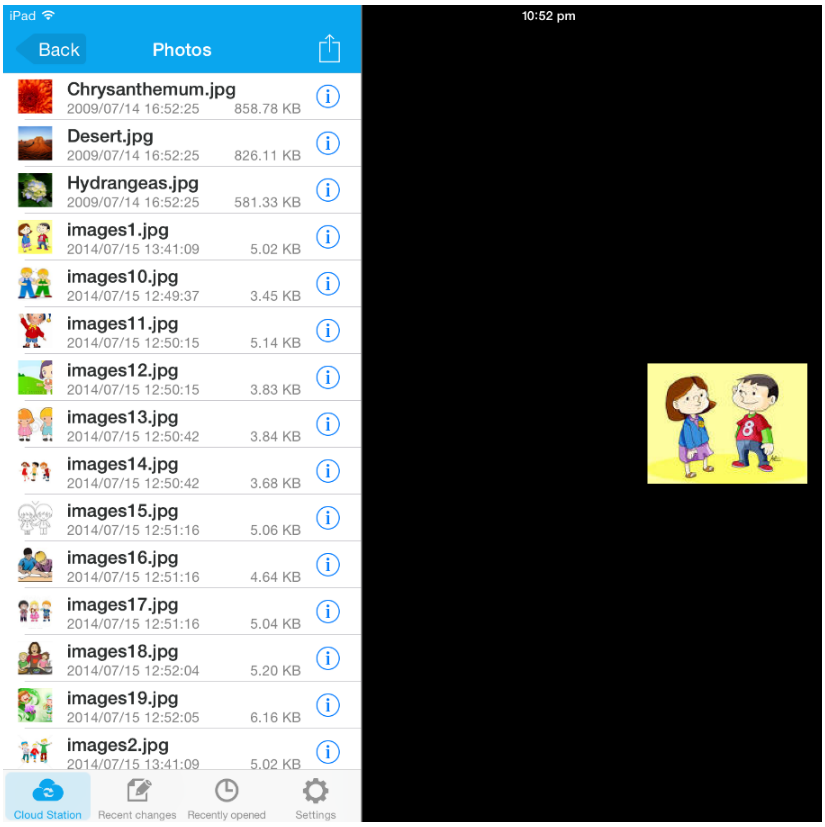
ComcSoft understands the high cost and complexity in today's mobile application development. ComcSoft's Synergic Framework maximizes reusability of back end services and minimizes the cost of application development and maintenance with a shortened delivery timeline.

We help our clients leverage mobile outsourcing services to improve their business performance so that they can compete more effectively in the mobile marketplace and achieve higher ROI.

Please visit us at http://www.comcsoft.com.

Figure 5.29: Content of the Dox directory.

Following in figure 5.30 shows the content of the photos directory.



Chrysanthemum.jpg	2009/07/14 16:52:25	858.78 KB
Desert.jpg	2009/07/14 16:52:25	826.11 KB
Hydrangeas.jpg	2009/07/14 16:52:25	581.33 KB
images1.jpg	2014/07/15 13:41:09	5.02 KB
images10.jpg	2014/07/15 12:49:37	3.45 KB
images11.jpg	2014/07/15 12:50:15	5.14 KB
images12.jpg	2014/07/15 12:50:15	3.83 KB
images13.jpg	2014/07/15 12:50:42	3.84 KB
images14.jpg	2014/07/15 12:50:42	3.68 KB
images15.jpg	2014/07/15 12:51:16	5.06 KB
images16.jpg	2014/07/15 12:51:16	4.64 KB
images17.jpg	2014/07/15 12:51:16	5.04 KB
images18.jpg	2014/07/15 12:52:04	5.20 KB
images19.jpg	2014/07/15 12:52:05	6.16 KB
images2.jpg	2014/07/15 13:41:09	5.02 KB

Figure 5.30: Content of the Photos directory.

5.2 "STRAW MAN" MODEL IMPROVEMENTS

The pilot study was designed and conducted to confirm the problem identified in the literature as explained in section 3.4. The pilot study indicated that the problem identified in the literature did exist. Correspondingly, the pilot study demonstrated the character of digital forensic investigation on a mobile SMART device. It also shows where the "STRAW MAN" model can be improved. In section 2.4.1, the term SMART device is defined and section 2.4.2 has outlined the business usages of these devices.

Section 2.4.2 also highlighted evidence found in the literature from analyst such as Gartner, Smart Insights and other researchers in the field that, these devices have the ability to interact with various private networks and backup data to the cloud. They also highlighted the fact that these devices have the ability to connect to private organisation's network from anywhere at any time. As a result, no doubt that these devices will be the preferred device for many users and recovering residual forensic potential evidence from these SMART devices are vital to digital forensic practitioners. As mentioned earlier, the results from the pilot study supported the theory that the problem exists as defined in section 3.4.

However, section 3.4 highlighted that currently there are no investigation process model with multi-disciplinary investigation process competence.

The character of forensic investigation on mobile SMART devices is changing. In the early days of digital forensics, the field was only known as computer forensics. The main reason is because; computers were the only common source of digital information. These days, digital investigation is broad and covers all types of digital crime. It can be as simple as examining a mobile phone to determine contacts to a more serious crime where all the sub-fields of digital forensics involved. Nevertheless, as mobile SMART devices' popularity increases, pervasive and ubiquitous connectivity among all types of networks were common. As a result, mobile forensics, network forensics and cloud forensics were added to the sub-fields of digital forensics. So, digital forensic practitioners will have to adapt to these devices that carry a large amount of personal and confidential information.

The relationship between these devices, the cloud and private networks is evident in the case studies for the mobile device used in this study, figure 5.6 showed the login details used to access the cloud account. Figure 5.7 showed the IP address while figure 5.8 confirmed the name or type of device that was used. The second case study also confirmed the multi-disciplinary nature of forensic investigation on mobile SMART devices. Apart from a number of potential evidence of the crimes committed, figure 5.26 details of a private Wi-Fi account that was used by the mobile device involved. Figure 5.27 showed details of proprietary software applications in the device. These applications were only used in conjunction with the private cloud involved, figure 5.28 showed the content of the cloud account.

As mentioned earlier, the character of digital forensic investigation on mobile SMART devices is changing and forensic practitioners need to adapt. As a result, a Multi-disciplinary digital forensics investigation process model was developed and shown as the “STRAW MAN” as shown in figure 3.17. The goal of the STRAW MAN investigation process model is to improve the effectiveness and the efficiency of an investigation. The model was tested on fictitious test case scenarios and it can be seen that the model's performance can be optimised and improved. Investigation process models serve as boundary objects. It represents aspects of the digital forensics investigation for various purposes, to predict and explain the operation and mechanism of the investigation.

5.2.1 Effectiveness and Efficiency Evaluation

Digital forensics investigation has a complex nature and for that, it requires multidisciplinary skills and abilities. There are various types of wireless networks that mobile SMART devices utilise. On the other hand, there are also various areas of knowledge in the digital forensic arena. In comparison to the use of the existing investigation process models, the new model should have the ability to define the relationships between various sub-fields in the digital forensic arena. In order for the model to have the ability to define the relationships between various sub-fields in the digital forensics arena, optimising its performance and the features of each process of the model must be understood.

In this sub-section, the findings of the STRAW MAN model’s evaluation for effectiveness and efficiency are reported. These two terms can be defined as; efficiency” *is doing things right.”* It can also be referred to as completing a task at minimal time. Effectiveness on the other hand *”is doing the right things,”* effectiveness can add value to processes, it enhances innovation. Effectiveness is the scope to which objectives are met and an activity fulfils its purpose. Following in table 5.1 shows a combination of the evaluation method used together with the attributes and properties of the model. They are used in the evaluation of the effectiveness and the efficiency of the STRAW MAN model.

Table 5.1: Evaluation method

Evaluation Methods	Attributes	Properties
Observational	• Completeness • Consistency • Accuracy • Reliability • Usability • Fit with the organization	• Efficiency • Effectiveness • Efficacy • Ethicality • Elegance • Performance
Analytical		
Experimental		
Testing		

Effectiveness and efficiency are part of the STRAW MAN's properties however; there are key important influences of effectiveness and efficiency that can be identified in the literature. Number one is speed/movement of the processes; two is dealing with the structure of the model that synchronises the whole process and lastly, create a space. Providing a transferable space is a critical factor in terms of task management, this important in order to avoid any bottlenecks.

In the following sub-sections, the "STRAW MAN" model is evaluated based on the results of test case scenarios created for this study. In figure 4.5 showed the design of the study which provided a process phase feedback loop that applied to "observe the effectiveness and efficiency" of the "STRAW MAN" in practice. The "STRAW MAN" design is evaluated according to the five criteria outlined in table 4.2. The features of the "STRAW MAN" are assessed according to the model's expected attributes and properties as outlined in table 4.1. The final evaluation is for relevance and rigour as outlined in figure 4.4. Following in table 5.2 and 5.3 are the results from the evaluation of effectiveness and efficiency based of the test case scenario results.

The data from the test case scenarios were also used to evaluate the effectiveness and efficiency of the STRAW MAN model. The evaluation was based on the methodology outlined in table 4.2 and the important factors of effectiveness and efficiency.

Table 5.2: Effectiveness evaluation result.

EFFECTIVENESS EVALUATION RESULTS					
Key Factors	**Observational**	**Analytical**	**Experimental**	**Testing**	**Descriptive**
Speed/Movement	Medium	Medium	High	High	High
Model Structure	Medium	Medium	High	High	High
Space	High	High	High	High	High

It can be seen in the results in table 5.2 that the observational and analytical results for processes movement are still on medium. The observational and analytical results for the structure of the STRAW MAN also yielded medium however, the rest of the evaluation results were high. Following in table 5.3 outlined the result from the STRAW MAN's efficiency evaluation.

Table 5.3: Efficiency evaluation result.

EFFICIENCY EVALUATION RESULTS					
Key Factors	**Observational**	**Analytical**	**Experimental**	**Testing**	**Descriptive**
Speed/Movement	Medium	Medium	High	High	High
Model Structure	Medium	Medium	High	High	High
Space	High	High	High	High	High

The results for the STRAW MAN's efficiency evaluation results were very similar to the effectiveness evaluation results. The observational and analytical results for processes movement among the phases of the model were rated medium. The structure of the model was rated medium also under the analytical and observational test results while the rest yielded high ratings. Following in sub-section 5.2.2, the design of the STRAW MAN model was evaluated and the findings are outlined in this section.

5.2.2 Design Evaluation

The evaluation method outlined in table 5.1 was also used to evaluate the design of the STRAW MAN model. Figure 7.1 also provided a graphical representation of how the evaluation methodology works together with the attributes and properties of the model.

Table 5.4: The model's design evaluation result.

The STRAW MAN Model's Design Evaluation Results					
Attributes/ Properties	**Observational**	**Analytical**	**Experimental**	**Testing**	**Descriptive**
Completeness	Medium	Medium	High	High	High
Consistency	Medium	Medium	Low	Low	High
Accuracy	Medium	Medium	High	High	High
Performance	Medium	Medium	Medium	Medium	High
Reliability	Medium	Medium	Medium	Medium	High
Usability	High	High	High	High	High
Efficiency	Medium	Medium	High	High	High
Effectiveness	Medium	Medium	High	High	High
Ethicality	High	High	High	High	High

The evaluation results of the design of the STRAW MAN yielded very interesting information which shows that there is still room for improvements. The majority of the attributes and properties of the STRAW MAN were rated medium under observational and analytical except for usability and ethicality yielded high ratings. Under experimental and testing, high ratings for most of the attributes and properties while performance and reliability were rated medium. However, consistency yielded a low rating on both approaches, experimental and testing. All of the attributes and properties of the STRAW MAN were rated high when evaluated under the descriptive approach.

5.2.3 Relevance and Rigour Evaluation

Design science research methodology is the approach employed to guide this study. DS puts its focuses on the artefact created as a result of a study, from the development stage to its creation, optimisation and communication. Evaluating the artefact, the STRAW MAN model in this case, relevance and rigor are part of the evaluation process of DS research approach. To support and justify the developments, creations and evaluation activities of the new artefact, the existing knowledge base needs to be employed.

The existing knowledge base consists of well-informed bases and methods that are recognised among both academic and professional communities. These methods support evaluation activities of a new artefact and the results can be used for improvements. Figure 4.3 outlined seven criteria of conducting as DS research however; criterion number five demanded that the study should be based on an application of rigours techniques in both the construction and the evaluation of the STRAW MAN. The purpose is to validate the study and expose its reliability. It is important that this is conducted with an appropriate amount of rigor to demonstrate the suitability of the STRAW MAN model for its proposed application. Following in table 5.5 are the results yielded when the artefact is evaluated under the same evaluation methodology.

Table 5.5: The model’s relevance and rigor evaluation result.

Relevance and Rigor Evaluation Results					
Attributes/ Properties	**Observational**	**Analytical**	**Experimental**	**Testing**	**Descriptive**
Completeness	Low	Low	Medium	Medium	High
Consistency	Low	Low	Medium	Medium	High
Accuracy	Medium	Medium	Medium	Medium	High
Performance	Medium	Medium	Medium	Medium	High
Reliability	Medium	Medium	Medium	Medium	High
Usability	High	High	High	High	High
Efficiency	Medium	Medium	Medium	Medium	High
Effectiveness	Medium	Medium	Medium	Medium	High
Ethicality	High	High	High	High	High

Figure 4.4 illustrated the relationships between the relevance of the problem which was identified in the literature and discussed in section 3.4 and the rigor of the applicable knowledge employed from the knowledge base. However, when the relevance and rigor of the STRAW MAN model is evaluated under the same evaluation methodology, the results indicated that improvements are required. Under observational and analytical, completeness and consistency were both rated low while accuracy, reliability and performance together with effectiveness and efficiency were all rated medium. Approaches such as experimental and testing, almost all of the artefact’s attributes and properties were rated medium except for usability and ethicality were rated high.

5.2.4 Summary of Required Improvements

Following in table 5.6 is a summary of the results of the evaluation conducted on the artefact developed in this study which is the STRAW MAN model. Based on the summary provided, table 5.6 highlighted the weaknesses of the STRAW MAN model and areas where improvements are imminent. As a result, figure 5.32 showed the improved STRAW MAN and now termed the Multi-Disciplinary Digital Investigation Process Model (MDIPM). The improvement made to the STRAW MAN model was based on the results produced by the evaluations conducted. The key indicators for improvements were the areas rated with a low such as, consistency and completeness. Consistency was rated with low ratings in the design evaluation and also the relevance and rigor evaluation.

Table 5.6: Areas where improvements are required.

EFFECTIVENESS AND EFFICIENCY REQUIRED IMPROVEMENTS					
Key Factors	**Observational**	**Analytical**	**Experimental**	**Testing**	**Descriptive**
Speed/Movement	Medium	Medium			
Model Structure	Medium	Medium			
Attributes/ Properties	**Design Evaluation Required Improvements**				
Completeness	Medium	Medium			
Consistency	Medium	Medium	Low	Low	
Accuracy	Medium	Medium			
Performance	Medium	Medium	Medium	Medium	
Reliability	Medium	Medium	Medium	Medium	
Efficiency	Medium	Medium			
Effectiveness	Medium	Medium			
Relevance and Rigor Required Improvements					
Completeness	Low	Low	Medium	Medium	
Consistency	Low	Low	Medium	Medium	
Accuracy	Medium	Medium	Medium	Medium	
Performance	Medium	Medium	Medium	Medium	
Reliability	Medium	Medium	Medium	Medium	
Efficiency	Medium	Medium	Medium	Medium	
Effectiveness	Medium	Medium	Medium	Medium	

That report flagged that the design is weak or the structure is incomplete and inconsistent. As a result, the knowledge base was consulted and brought in again. The standards and principles developed by organisations such as ISO/IEC, ACPO, NIST, NIJ were reviewed again against the STRAW MAN's areas of weaknesses. Following in table 5.7 and 5.8 outlined the recommendation for improvements made to the STRAW MAN model.

Table 5.7: Recommendation for improvements in Network forensics.

STRAW MAN's Network/Cloud	Recommendations For Network Forensics
Preparation	Identification by observing physical characteristics such as device design elements, power connector or device labels.
Preservation	Preserve the status of digital device (don't switch on/off) unless transport is required and it cannot be done while the device is operating.
Collection	Devices with one physical network connection might be connected to several logical and/or virtual networks. Thus, before disconnecting, should conduct a logical acquisition of data related to logical connections. Make a decision on whether to collect or acquire potential evidence.

There are recommendations that found in the literature with regards to network forensics. The STRAW MAN has preparation, preservation and collection however, in the literature; identification is more suitable in a network environment. Collection on the other hand, it is recommended that a logical acquisition of data should be taken before start disconnecting devices in a network environment. However, a decision should be made based on the situation and the environment whether potential evidences are to be collected or acquired.

Table 5.8: Recommendation for improvements in Cloud forensics.

STRAW MAN's Network/Cloud	Recommendations For Cloud Forensics
Preparation	It is recommended that customers identify the additional data sources unique to the cloud service model.
Preservation	Preservation is the protection of the integrity of potential digital evidence. Potential digital evidence and digital devices must be safeguarded from tampering or spoliation.
Collection	Due to the multi-tenant nature of cloud infrastructures, acquisition should usually be preferred over collection to avoid impacts to parties not involved in the matter

Table 5.8 shows recommendations for improvement regarding forensic investigation in cloud environment. In this environment, there are various service models however; there are three fundamental service models known as Software

as a service (SaaS), Platform as a service (PaaS) and Infrastructure as a service (IaaS). One of the recommendations found in the literature is to identify any data unique to the cloud service model. In addition, potential evidences and digital devices need to be secured properly to avoid further tempering or spoliation. Also, need to consider the multi-tenant nature of cloud technology. It is recommended that acquiring the data should always be considered rather than collecting the potential evidence. This is to avoid impacts to other tenants of the cloud that are not involved in the investigation. Table 5.9 highlights and summarises the required improvements for the STRAW MAN model.

Table 5.9: Summary of improvements for the STRAW MAN model.

STRAW MAN's Network/Cloud	MDFIPM Network	MDFIPM Cloud
Preparation	Identification	Identification
Preservation	Collection/ Acquisition	Data Acquisition
Collection	Preservation	Preservation
Examination	Examination	Examination
Analysis	Analysis	Analysis

After comparing the recommendations found in the knowledge base and the results of the STRAW MAN model's evaluations, the required improvements were evident. The STAW MAN model's phases for Network forensics were the same as the Cloud forensics phases. The evaluation results showed that these two are totally different and they also have different investigation environments and requirements. As a result, need to use identification instead of preparation, network needs to use collection/acquisition while cloud environment best to use acquisition than followed by preservation, examination and analysis. The new improvement STRAW MAN is now known the Multi-Disciplinary Digital Forensic Investigation Process Model (MDFIPM) as illustrated in figure 5.32.

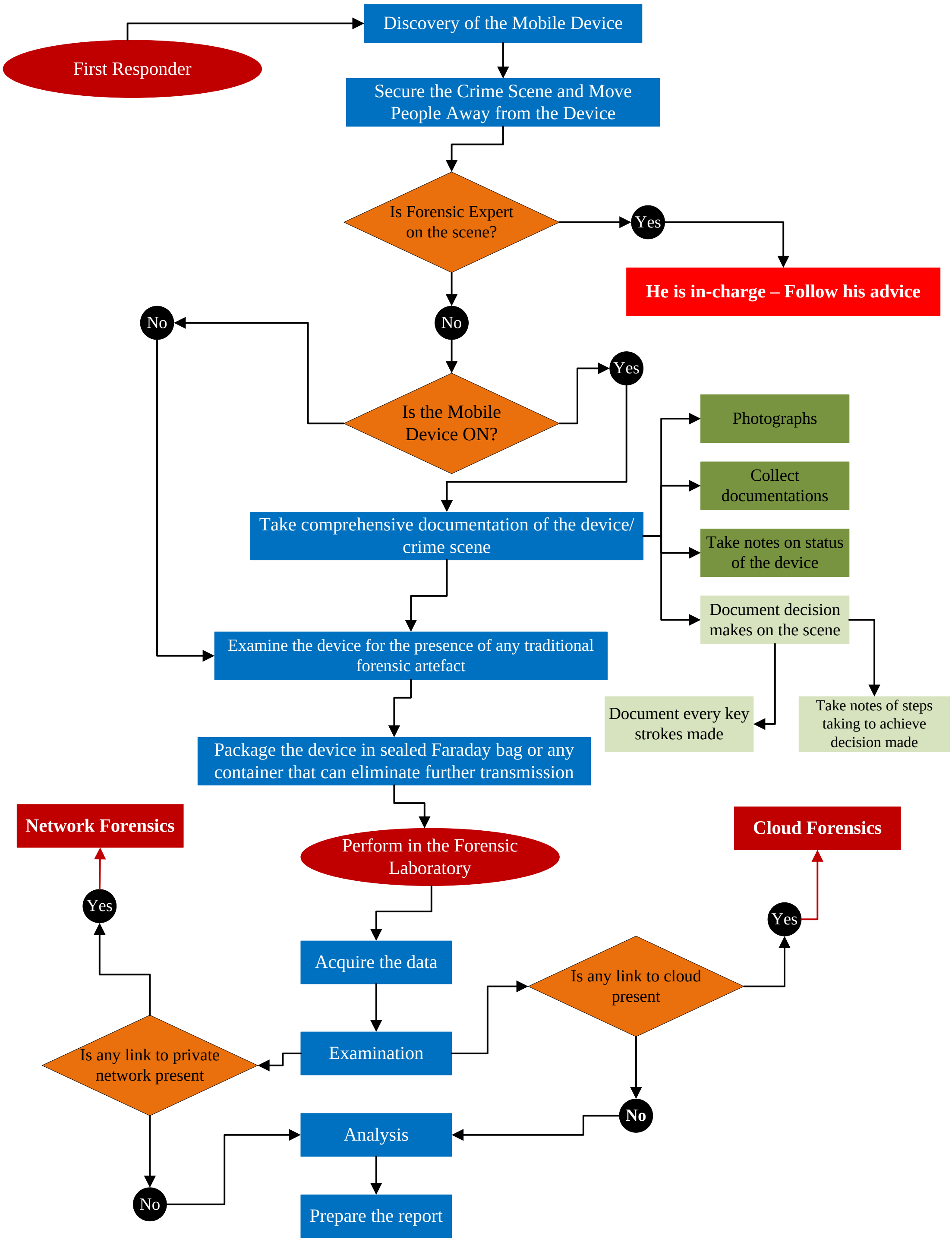
As reflected in the name, the MDFIPM is designed for an investigation in a Multi-disciplinary environment. In order to achieve that, the MDFIPM is divided into three main parts. Section 5.2.1 showed the results for the model's effectiveness and efficiency evaluation. Section 5.2.2 evaluated the design of the model and 5.2.3 showed the relevance and rigour of the model. Table 5.6 showed all the areas where the STRAW MAN needs to be improved. Tables 5.7 and 5.8 showed the required improvements for network and cloud forensics and table 5.9 summarised all the improvements made. The main investigation path of the MDFIPM is the mobile forensics investigation path. The mobile forensics path has been evaluated as well. Figure 5.31 shows what has been changed and what is recommended.

Section 3.2.3 discusses the ACPO principles of digital evidence as it showed in table 3.7. The purpose of these principles is to preserve the integrity of the evidence. Tables 3.10 and 3.11 showed a comparison of ten various investigation process models. One of these models was proposed by the U.S Department of Justice, and advices on how to handle electronic evidence in the crime scene. Table 5.10 compares instructions developed by the DoJ and ACPO on how to handle digital evidence.

Table 5.10: Handling electronic evidence at the crime scene (Ashcroft, 2001, p.6).

DoJ - Standards	**ACPO - Instructions**
Recognition and identification of the evidence	Any interaction with the handset on a mobile phone could result in loss of evidence
Documentation of the crime scene	Before handling, decide if any other evidence is required from the phone (such as DNA/fingerprints/drugs/accelerants).
Collection and preservation of the evidence	General advice is to switch the handset OFF due to the potential for loss of data if the battery fails or new network traffic overwrites call logs or recoverable deleted areas (e.g. SMS); there is also potential for sabotage.
Packaging and transportation of the evidence	However, investigating officers (OIC) may require the phone to remain on for monitoring purposes while live enquiries continue. If this is the case, ensure the unit is kept charged and not tampered with. In all events, power-down the unit prior to transport.

The mobile forensics investigation path processes of the MDFIPM have been improved based on the instructions developed by the DoJ and the ACPO organisations shown in table 5.10.



First Responder
Discovery of the Mobile Device
Secure the Crime Scene and Move People Away from the Device
Is Forensic Expert on the scene?
Yes
He is in-charge – Follow his advice
No
No
Yes
Is the Mobile Device ON?
Photographs
Collect documentations
Take notes on status of the device
Document decision makes on the scene
Take comprehensive documentation of the device/ crime scene
Examine the device for the presence of any traditional forensic artefact
Document every key strokes made
Take notes of steps taking to achieve decision made
Package the device in sealed Faraday bag or any container that can eliminate further transmission
Network Forensics
Perform in the Forensic Laboratory
Cloud Forensics
Yes
Yes
Acquire the data
Is any link to cloud present
Examination
Is any link to private network present
No
Analysis
No
Prepare the report

Figure 5.31: Recommended steps for mobile forensics (Based on ACPO, 2007).

The improvements made to the investigation processes of the mobile forensics path of the MDFIPM are shown in figure 5.31. As a result, figure 5.32 has the new improvements in the mobile forensics model for the MDFIPM presentation.

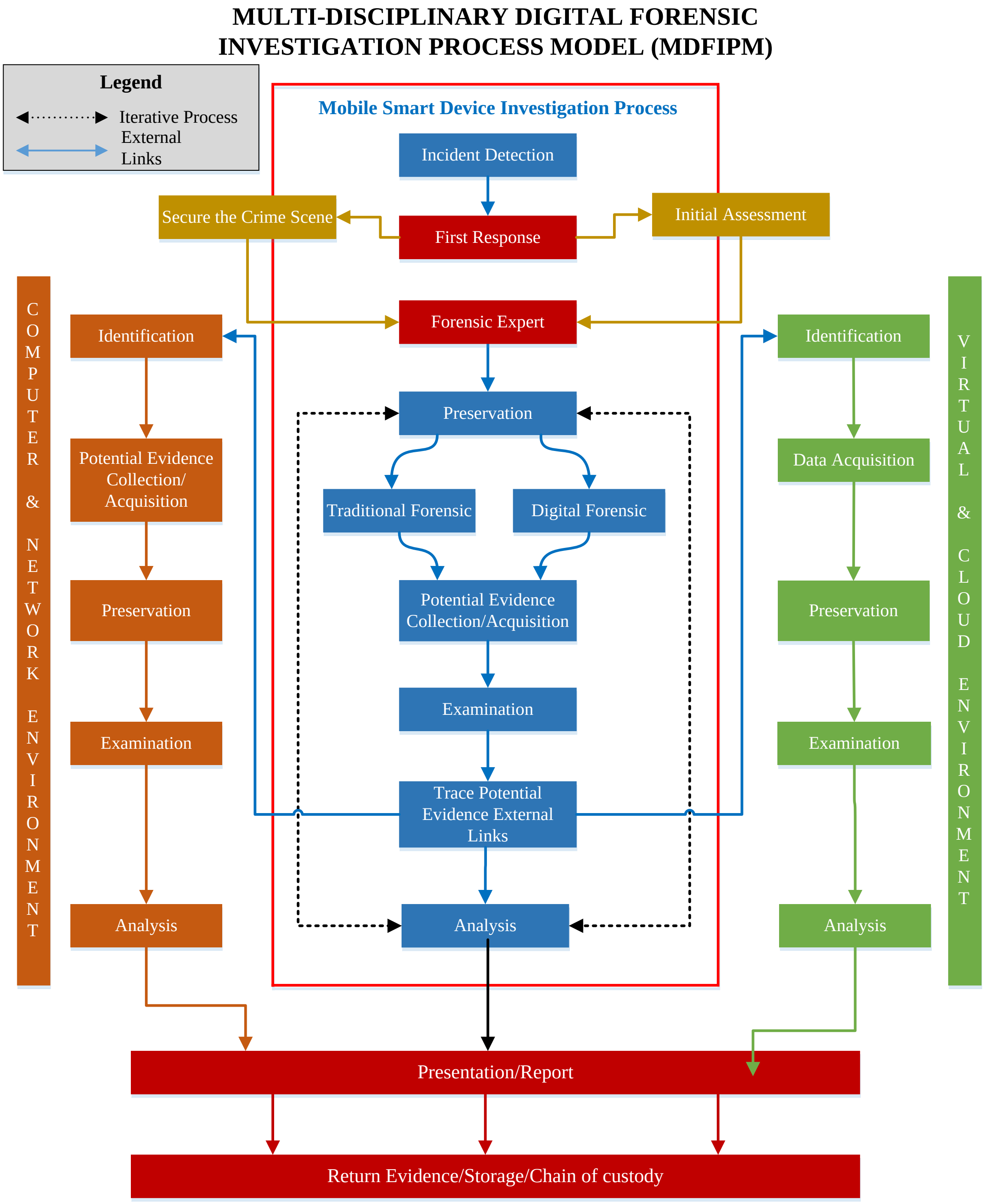

MULTI-DISCIPLINARY DIGITAL FORENSIC INVESTIGATION PROCESS MODEL (MDFIPM)
Legend
Iterative Process
External Links
Mobile Smart Device Investigation Process
Incident Detection
Secure the Crime Scene
First Response
Initial Assessment
Forensic Expert
Preservation
Traditional Forensic
Digital Forensic
Potential Evidence Collection/Acquisition
Examination
Trace Potential Evidence External Links
Analysis
COMPUTER & NETWORK ENVIRONMENT
Identification
Potential Evidence Collection/ Acquisition
Preservation
Examination
Analysis
VIRTUAL & CLOUD ENVIRONMENT
Identification
Data Acquisition
Preservation
Examination
Analysis
Presentation/Report
Return Evidence/Storage/Chain of custody

Figure 5.32: The Multi-disciplinary Digital Forensic Investigation Process Model.

To contextualise the context and the scope of the artefacts, this study endeavoured to build a set of artefacts that can be applied in any jurisdiction and interpreted by the digital forensic experts in any jurisdiction to fit their requirements. The digital forensic experts can pick up the artefacts and apply the local legal frameworks such as the evidence act in order to preserve the integrity of the evidence. The model and the framework were developed to guide a digital forensic investigator in a very complex and difficult problem. That is – how to deal with a digital investigation that is compliant both of law but also up to date and sufficiently efficient that it can treat the information technology and the problem of cost to conduct the investigation.

The artefacts were developed particularly for investigations that involve a mobile smart device. In the model (figure 5.32) for instance, it is in three parts, mobile device which is the main investigation path and two other paths, Network forensics on one side and Cloud forensics on the other. The Mobile device forensics investigation path can be used on its own or used together with one of the two or used them all together in an investigation.

5.3 CONCLUSION

This chapter focusses on the findings from the test case scenarios. These findings were then used to evaluate the STRAW MAN model. The "STRAW MAN" model has been evaluated and reviewed in order to identify its strength, weaknesses and opportunities for improvements. The STRAW MAN has been put through on a number of evaluations such as, effectiveness and efficiency evaluation, design evaluation and relevance and rigor evaluation. These evaluations were run against the DS evaluation method together with the STRAW MAN attributes and properties.

The evaluation results clearly showed the weaknesses of the STRAW MAN model and the required improvements to be made as summarised in table 5.9. Figure 5.32 showed the improved STRAW MAN model and the new name, the Multi-Disciplinary Digital Forensic Investigation Process Model as it showed in the literature that, digital forensic investigation has a complex nature so; it requires multi-disciplinary skills and abilities. The professional significance of the Multi-Disciplinary Digital Forensic Investigation Process Model is for greater efficiencies and effectiveness in digital investigations. In chapter 6 the implications for practice of the findings in chapter 5 will be applied to develop an implementation guide for best practice for a practitioner when undertaking a digital forensic investigation.

Chapter Six

Framework & Best Practice Guidelines For Practitioners

6.0 INTRODUCTION

Chapter 5 has defined an investigation model derived from the theories in chapter two and three and presented in figure 3.17. Improvements to the first attempt “STRAW MAN” investigation model were made to iterate improvement. In Chapter 6 the data and experience gathered during the pilot study and with reference to the relevant standards and practice guidelines on investigation framework for practitioners and a user’s guideline are to be developed. The chapter is structured to first develop the framework (section 6.1) and then to write the guideline (section 6.2).

6.1 THE INVESTIGATION FRAMEWORK

There are a number of investigation models, frameworks and guidelines in the digital forensic domain available to practitioners. A digital forensic investigator may be able to recognise the potential evidence in various crime scenes but the process cannot be described in a general way. Section 2.2 explained various types of wireless networks that a mobile SMART device utilises. Section 2.3 mentioned a special publication 800-101 released by NIST which pointed out that the design of mobile phones in particular often changes and it is likely to keep changing as technology improves or new technologies are introduced.

Section 2.3.4 reviewed various investigation process models found in the literature. It is evident clear that each was developed for a specific technology such as cloud, SMART phone or network. To date, digital investigation has been directed by technology under investigated or tools available to investigators. As a result, when targeted technology changes, new investigation methods have to be formulated to suit the investigation environment. As a result, the NIST guidelines were developed to help forensic experts in developing proper policies and procedures and also in preparing them for future technological changes (section 3.2.4).

Digital forensic processes are a recognised scientific forensic process with investigative nature; they are also referred to by researchers in the field as number of steps beginning from the recognition of new incident to the reporting of the findings. They were primarily used and known as computer forensics with six main steps; identification, preservation, collection, examination, analysis and presentation as a result of the first digital forensic workshop 2001 as in figure 3.7. Section 5.2.1 explained that, investigation process model is referred to as an abstraction of a process to examine evidences irrespective of its originality.

Experts also believe that investigation process models generalise an informal procedure. Investigation frameworks on the other hand, experts believe that forensic investigation frameworks provide detail understanding of what each process is to do or not do. Frameworks include objective based phases that are applicable to various layers of abstraction. This means that each phase has an objective and tasks to complete. This will guide forensic practitioners to be more efficient and reduce error rates at the same time. Section 3.4 explained that, model and framework provides an effective means to obtain information within the processes which used to capture relevant aspects of the investigation.

Best practice guideline is described as a method that showed results that is more recognised than results achieved using other techniques. Results from using best practice methods are often used as a benchmark. It is also used to describe processes of following a standard way of doing things. Digital forensic investigation best practice guideline is employed in order to maintain the quality and integrity of the investigation findings. Best practice guidelines are referred to as alternative standards such as those from reputable organisations such as ISO, NIST, NIJ and ACPO as shown and explained in sections 3.2.2, 3.2.3 and 3.2.6.

6.1.1 The Multi-Disciplinary Investigation Framework

The pilot study was designed to test the theory that was developed from the literature. The test case scenarios were conducted to measure the performance and efficiency of the STRAW MAN model. The goal is to improve the effectiveness and efficiency of digital forensic investigations. Measuring the performance of a model is necessary because a model is only an abstraction of something that contains sufficient detail to be useful. Forensic personnel think that a model is just a formula however, computer scientists think of models as simplifications of reality as explained in section 5.2.1.

The performance measurement system is used to measure the effectiveness and the efficiency of actions. After the test case scenarios, it was clearly understood how well the investigation processes performed, whether the goals are met and if the processes were in control of the whole investigation processes. To achieve effectiveness in an investigation, the result of the investigation processes should conform to the requirements indicating that we are doing the right things. In terms of efficiency, the investigation processes should produce the required result at minimum resource costs indicating that we are doing things right.

All digital based evidence is fragile and particularly the evidences residing on cellular phones. Data on a phone can be lost at any time when the device is on (section 1.2). In attempting to encompass the diversity of the digital world, several reputable organisations such as the NIST, ACPO, ISO/IEC helped by developing standards and guidelines. The illustration provided in figure 5.32, is a graphical representation of how this study evaluated the performance of the STRAW MAN model and made the necessary improvements. This was achieved by following the guidance of the DS research method as shown in figure 4.2. The knowledge gained from the literature as in section 3.3, combined with the findings from the test case scenarios. These were employed together with the standards and guidelines developed by reputable organisations to evaluate the STRAW MAN's performance. As a result, the improvements were made to the STRAW MAN model and the Multi-disciplinary Digital Forensic Investigation framework was established.

The ACPO developed four principles as a good practice guide for digital evidences as it shown in table 6.5. It is evident that there are two characteristics of digital evidence; physical mechanisms, peripherals and media. They can all hold data that can be potential evidence to a crime. Each of these components has associated issues in terms of chain of custody. Therefore, the International Organization on Computer Evidence (IOCE) developed and proposed five principles and published in the year 2000 regarding the exchange of digital evidence as it showed in table 6.1.

Table 6.1: IOCE principles for exchange of digital evidence.

Number	Principles
1	Upon seizing digital evidence, actions taken should not change that evidence.
2	When it is necessary for a person to access original digital evidence, that person must be forensically competent.
3	All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.
4	An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.
5	Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles.

The IOCE principles were developed to warrant the integrity of digital evidence. Ensure the correct way of handling of the evidence through its entire investigation so it can be admissible in the court of law. The Daubert criteria on the other hand also provided a set of five principles and published by Watkins in 1994. These principles were developed to deal with the reliability of evidence and its being used in reporting and forensic examination as in table 6.2.

The Department of Justice in the United States of America, Technical Working Group on Crime Scene Investigation (TWGCSI) in the year 2000 has developed a guide for law enforcement on crime scene investigation as in table 6.2. The International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC) have developed a guideline for the identification, collection, acquisition and preservation of digital evidence known as the ISO/IEC 27037:2012. After evaluating the model against the performance criteria mentioned in table 5.1. The evaluation information shown in tables 5.2, 5.3, 5.4, 5.5 and table 5.6 provided a summary of the areas of the STRAW MAN model that needs improvements. This information was then compared to the standards and principles mentioned earlier in this section. The following tables summarise those principles and standards.

Table 6.2: Daubert criteria for evidence reliability

Number	Principles
Testability	Has the scientific theory or technique been empirically tested?
Acceptance	Has the scientific theory or technique been subjected to peer review and publication? This ensures that flaws in the methodology would have been detected and that the technique is finding its way into use via the literature.
Error Rate	What is the known or potential error rate? Scientific measures generally have associated error rates, which can be estimated with a fair amount of precision. Known threats exist against the validity and reliability in any test (experimental and quasi-experimental) of a theory.
Credibility	What is the expert's qualifications and stature in the scientific community? Does the technique rely upon the special skills and equipment of one expert, or can it be replicated by other experts elsewhere?
Clarity	Can the technique and its results be explained with sufficient clarity and simplicity so that the court and the jury can understand its plain meaning? This criterion is implicitly assumed to be incorporated in Daubert.

These were developed aiming to increase the reliability of evidence. Not concerning with reliability only but its use in reporting and examination. For instance, the reliability of the theory and the technique employed. Also, look at the error rate and the credibility of the expert.

Table 6.3: DoJ standards for crime scene investigation

Name	Principles
Securing and Evaluating the Scene	Steps should be taken to ensure the safety of individuals and to identify and protect the integrity of potential evidence.
Documenting the Scene	Create a permanent record of the scene, accurately recording both digital-related and conventional evidence.
Evidence Collection	Collect traditional and digital evidence in a manner that preserves their evidentiary value.
Packaging, Transportation, and Storage	Take adequate precautions when packaging, transporting, and storing evidence, maintaining chain of custody.

The TWGCSI guide is aimed to law enforcement on crime scene investigation such as securing and evaluating the crime scene in order to ensure their safety. Not only that but creating a permanent electronic and paper based evidence of the crime scene as shown in table 6.3.

Table 6.4: ISO/IEC 27037 standards.

Name	Guide
Identification	• Physical incident scene search and documentation • Non-digital evidence collection • Additional, non-digital information should be collected e.g. by interviewing individuals to obtain passwords. • Decision-making process for collection or acquisition • A determination must be made to collect or acquire potential evidence.
Collection	• Collection is a process in the digital evidence handling process where devices that may contain digital evidence are removed from their original location to a laboratory or another controlled environment for later acquisition and analysis.
Acquisition	• Powered on digital devices • Scenarios exist in which acquisition may need to be conducted when the digital devices are powered on. • The Digital Evidence First Responder (DEFR) should make an accurate digital evidence copy of the digital device's storage media. • Acquisition of volatile live data is important. • Suspect systems' programs or tools should never be used. Only use verified external (statically linked) tools. • Store volatile data on prepared/sanitized storage media in file container and conduct appropriate hashing. • Use validated imaging tools for non-volatile data.
Additional Activities	• Try to detect data encryption on volatile data • Use a reliable time source. • It may be appropriate to associate the DEFR with the acquired potential digital evidence.

The ISO/IEC 27037 standards was developed aiming to guide forensic practitioners in identifying, collecting, acquiring and preserving digital evidences.

Table 6.5: ACPO principles of digital evidence.

Number	Principles
1	No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.
2	In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
3	An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
4	The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

The ACPO developed four principles as a good practice guide for digital evidences as in table 6.5. These principles and standards were compared with the STRAW MAN model's evaluation results as explained in section 5.2.4. The outcomes of the comparison were shown in tables 5.7 and 5.8 as recommendations. These recommendations were then used to make improvements to the STRAW MAN model as it summarised in table 5.9 as a result, the new improved model in now known as the Multi-Disciplinary Digital Forensic Investigation Model as in figure 5.32.

Section 4.1 explained the core processes of digital forensic investigation that was developed as a result of the first digital forensic research workshop held in New York 2001. These processes were identified as preservation, collection, examination and analysis. Section 3.4 identified the gap for this study and also explained that, experts referred to process models as an abstraction of a process to examine potential evidences regardless of their originality. As mentioned earlier, the investigation process model is an abstract representation of reality. The framework can be viewed from several viewpoints such as a structured idea, concepts and various areas that can be easily interconnected with others.

Advancements in communication technologies are still increasing but unfortunately, there is still no standardised digital forensics investigation process methodology at the time of writing. However, in use today is a set of procedures and tools created based on the law enforcement officers' guidelines, system administrator guidelines and hacker's methods. This is a problem because digital forensic evidence should be acquired and analysed using methods that are proven to be reliable and without modification for it to be admissible in the court of law. This is why the STRAW MAN model's performance was evaluated and compared to known principles and standardised processes in the field. As a result, improvements were made to maximise its effectiveness and efficiency and the result is the Multi-disciplinary Digital Forensic Investigation Process Model as shown in figure 5.32. In addition, forensic experts also believe that forensic investigation process models generalise an informal procedure to deliver a framework. That framework provides a detailed understanding of what each process is to do and not do. Following in figure 6.1 is the Multi-disciplinary Digital Forensic Investigation Framework that was developed as part of this study.

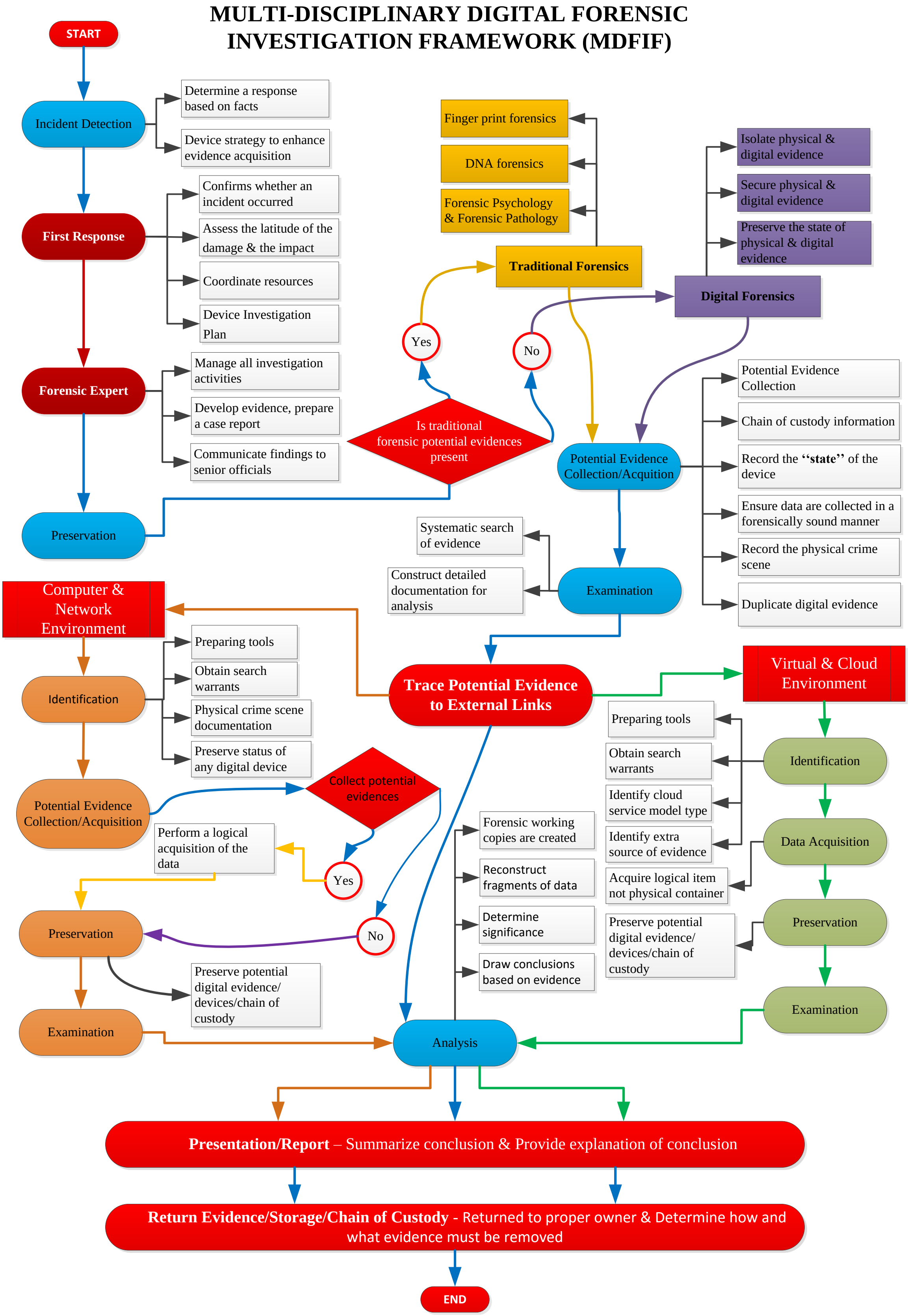

MULTI-DISCIPLINARY DIGITAL FORENSIC INVESTIGATION FRAMEWORK (MDFIF)
START
Incident Detection
Determine a response based on facts
Device strategy to enhance evidence acquisition
First Response
Confirms whether an incident occurred
Assess the latitude of the damage & the impact
Coordinate resources
Device Investigation Plan
Forensic Expert
Manage all investigation activities
Develop evidence, prepare a case report
Communicate findings to senior officials
Preservation
Finger print forensics
DNA forensics
Forensic Psychology & Forensic Pathology
Traditional Forensics
Isolate physical & digital evidence
Secure physical & digital evidence
Preserve the state of physical & digital evidence
Digital Forensics
Yes
No
Is traditional forensic potential evidences present
Potential Evidence Collection/Acquition
Potential Evidence Collection
Chain of custody information
Record the ''state'' of the device
Ensure data are collected in a forensically sound manner
Record the physical crime scene
Duplicate digital evidence
Systematic search of evidence
Construct detailed documentation for analysis
Examination
Computer & Network Environment
Trace Potential Evidence to External Links
Virtual & Cloud Environment
Identification
Preparing tools
Obtain search warrants
Physical crime scene documentation
Preserve status of any digital device
Potential Evidence Collection/Acquisition
Collect potential evidences
Perform a logical acquisition of the data
Yes
No
Preservation
Preserve potential digital evidence/ devices/chain of custody
Examination
Preparing tools
Obtain search warrants
Identify cloud service model type
Identify extra source of evidence
Acquire logical item not physical container
Preserve potential digital evidence/ devices/chain of custody
Identification
Data Acquisition
Preservation
Examination
Forensic working copies are created
Reconstruct fragments of data
Determine significance
Draw conclusions based on evidence
Analysis
Presentation/Report – Summarize conclusion & Provide explanation of conclusion
Return Evidence/Storage/Chain of Custody - Returned to proper owner & Determine how and what evidence must be removed
END

Figure 6.1: The multi-disciplinary investigation framework.

The framework shown in figure 6.1 includes objective based phases and sub-phases that are applicable to various layers of abstraction. This means, each of the phases has an objective and tasks to complete. These will guide forensic practitioners to be more efficient while reducing the error rates, also significantly improves the performance of investigation processes by contributing to achieving a comprehensive and integrative perspective of multi-disciplinary approaches into one unified whole and systematic pathway. As a result, its professional significance is for greater efficiencies and effectiveness in digital investigations.

6.2 INTRODUCTION TO GUIDELINE

This guideline recommends best practice for digital forensic professionals with regards to investigation processes. In chapter 4, the existing forensic investigation process models were reviewed and as a result, improvements to the "STRAW MAN" model were proposed in chapter 5. This best practice guideline is a result of the learning derived from those findings.

The definition found regarding computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. However, with the rapid growth of digital communication technologies, there are now sub-fields such as mobile forensics, network forensics, and cloud forensics under the umbrella of digital forensic. Digital forensic can be defined in the literature as the science of acquiring, retrieving, preserving and presenting data that has been processed electronically and stored on digital media. These technological changes have direct impact on the work that is done within the digital forensic domain. Digital forensics is in the arena of persistent changes, at the same time, practitioners need to re-evaluate their status and adapt. At the time of writing this guideline, according to the literature, there is still no standardised digital forensic investigation process model or framework. Yet, there will always be a need to acquire and analyse electronic data from digital devices that can be potential evidences in an investigation. This guideline is written for the Multi-disciplinary Digital Forensic Investigation Process Model (MDFIPM) shown in figure 5.32 and the Multi-disciplinary Digital Forensic Investigation Framework (MDFIF) shown in figure 6.1.

This document is divided into the following sections and sub-sections:

- Section 6.2 provides an introduction to this guideline.
- Section 6.2.1 discusses the purpose and the scope of the guideline.
- Section 6.2.2 explains the intended audience for the guideline.
- Section 6.2.3 provides background information of digital mobile SMART devices.
- Section 6.2.4 explains the goals and policies of the investigation framework.
- Section 6.2.5 explains the phases of the investigation framework.
- Section 6.2.5.1 explains the phases dealing with mobile SMART devices forensics
- Section 6.2.5.2 explains the phases dealing with virtual/cloud forensics
- Section 6.2.5.3 explains the phases dealing with network forensics
- Section 6.3 provides conclusion for the guideline

This best practice guideline was designed based on the structure of the National Institute of Standards and Technology (NIST) "Guidelines on Cell Phone Forensics" publication.

6.2.1 Purpose And Scope

There are sub-fields under the digital forensic umbrella. The Multi-disciplinary Digital Forensic Investigation Process Model (MDFIPM) and the Multi-disciplinary Digital Forensic Investigation Framework (MDFIF) is an attempt to bridge the gap having to use one investigation process model multiple times in one investigation that involved more than one sub-fields of digital forensics. The purpose of this work is to provide an in-depth understanding into the processes of the MDFIPM and the MDFIF and also explaining processes involved in each of the phases. It covers processes for an investigation involving a mobile SMART device such as SMART phones to an investigation involving virtual environment/cloud technologies and private local area network environments.

There are two objectives to this guideline: organisations may find this guideline helpful in developing policies and procedures on how to deal with such situation where they have to face more than one sub-fields of digital forensics. Digital forensic professionals may also find this guideline useful when such circumstances arise. However, the information provided in this guideline should not be treated as a legal advice but as a starting point for developing digital forensic proficiency in combination with available principles and standardised procedures when fronting such an investigation environment.

The information in this guideline is best for the MDFIPM and the MDFIF mentioned in this document however, every digital forensic investigation is unique. Therefore, judgement of the digital forensic experts should be respected when using the information provided in this guideline. In the application of the recommendations in this guideline should simplify effectiveness and efficiency of the processes of a digital forensic investigation that involves multi-disciplinary environments.

The information provided in this document regarding investigation processes and techniques are a result of consulting the literature from various academic databases and available principles and standards in the field.

6.2.2 Intended Audience

The intended audience for this guideline can be varied from first responders that may be handling security incident in an organisation to a digital forensic practitioner in the field investigating a criminal related case. The processes recommended in this guideline are intended to be used in combination with the MDFIPM and the MDFIF mentioned in this document.

6.2.3 Background

Mobile phones have now become part of our daily lives. They have also become the primary tool for personal and business communication. With the vast enhancement of the communication technologies, these devices are now known as SMART devices such as the SMART phones. This is due to the fact that, they are not principally for making phone calls anymore. They have new features, more powerful, more memories and more storage spaces. Information that can be stored on these devices is call logs, text messages, e-mail, user locations, contact information, photographs, videos and so on. These can all be vital information to a digital forensic investigator.

SMART phones are part of the mobile SMART devices family. A SMART device come in many types and forms such as tablet PCs, Personal Digital Assistants (PDA), music players and so on. Not only that but, they all come in various design structures and they are running on an operating systems developed by different companies such as iOS for Apple devices, Android from Google for devices such as Samsung and Windows from Microsoft. As mentioned earlier, these devices can contain personal and private information regarding their users. However, the different networks that they connect to such as home network, Cellular networks, company networks, social networks and clouds.

Digital forensic investigators have found these mobile SMART devices to be a significant part in the process of identifying illegal activities and the producing of digital evidences in criminal investigation. However, digital forensics is a new field compared to the traditional forensic approaches. In order to maintain the integrity of potential evidences acquired from these devices, digital forensic investigators need to use proper and standardised investigation methods and for which there is still no such method.

As a result, reputable organisations such as the National Institute of Standards and Technology (NIST), Association of Chief Police Officers (ACPO), International Organisation for Standardisation and the International Electrotechnical Commission (IEC) have frequently reviewing tools and methodologies; develop principles and standards for digital forensics. Researchers in the field and the academic arena have also published their work in various academic reputable databases such as IEEE, ACM, Elsevier, Springer, International Journal of Computer Science and Security and International Journal of Digital Evidence.

The main concern within the digital forensic communities, various areas of digital forensics requires different methods and procedures. At the same time, every device has its own structure, architecture and operating system design and requirements. For instance, acquiring data from mobile SMART devices is very much different from obtaining data from a computer or the cloud environment. The increase in the number of digital crimes puts more pressure on law enforcement and government intelligence agencies. The rapid shift from paper based evidence to digital and electronic evidence has necessitated a rapid reformation of principles, standards and investigation procedures. The process and procedure employed has a direct influence on an investigation results. The most important component of this practice is to warrant the integrity of potential evidences in order for the investigator’s findings to be admissible in the court of law. Employing of an unsuitable investigation processes may compromise the end results and the effectiveness and efficiency of the investigation.

6.2.4 Goals And Policy

The MDFIP Model and the MDFI Framework has particular goals that derived from the literature. The MDFIP Model and the MDFI Framework should:

a) Maximise the effectiveness of digital forensic investigation.

b) Maximise the efficiency of digital forensic investigation.

c) Maximize the integrity of potential digital evidence.

Section 6.2.5 will describe the investigation framework shown in figure 6.1 in more detail.

6.2.5 The Framework's Phase Descriptions.

The investigation framework shown in figure 6.1 starts off with SMART device forensics. There are recommended tasks to perform in each of the phases, the following sections provides detail explanations of these processes. The focus is to maintain the integrity of the digital evidence throughout the whole investigation process.

Potential evidences on mobile SMART devices can be very challenging to handle for a number of reasons. They can store digital evidences in both volatile and non-volatile form, some can be hidden or concealed, and they can cross jurisdictional boarders easily and quickly. Digital evidences are very easy to be manipulated, damaged or destroyed and they are time sensitive as well. As a result, it is highly recommended the use of well accepted investigation methods and techniques.

6.2.5.1 Mobile SMART Device Forensics

Digital Mobile device forensics is defined as the science of recovering digital evidence from a mobile device under forensically sound conditions using accepted methods. Mobile device forensics is one of the new specialised sub-fields of the digital forensics arena. This section of the guideline explains the phases involved and their relationship to forensic procedures of each phase of the multi-disciplinary investigation model and framework.

Incident Detection: this phase is performed at the crime scene. Involving determining the response based on facts and response strategy should enhance the evidence acquisition. It involves systematically documenting the crime scene, taking sketches, photographs and videos in order to have a permanent record of the crime scene. This type of documentation will also provide an accurate record and conventional evidence of the location and condition of the device involved including its power status. Taking a proper record of the crime scene is very important for preserving the chain of potential evidences and the preparation for the investigation findings presentation.

First Response: this phase is designed to provide first responders with guidance and help needed in order to conduct their tasks successfully and also to confirm that the detected incident occurred. This phase can be critical in terms of the integrity of the evidence. Identify potential evidence and secure it, keep people away from the evidence and so on. Assess the scope of the incident, co-ordinate resources. However, depending on the type and seriousness of the incident preferably, the team should not corrupt the data. It is important to include this phase in the process of the SMART device investigation in order to ensure the integrity of the evidence. It should be included to make sure that the initial response team won't destroy or corrupt potential evidence.

NOTE: *"All of the data collected by the first responders will be handed over to the forensic personnel when arrived. The forensic personnel will then responsible for managing the rest of the investigation."*

Preservation: the preservation phase is also concerned with preserving the integrity and also the current state of the evidence. Evidence preservation is the process of confiscating the suspect's property without altering any data on the device. Failure to do this properly in order to preserve potential evidences in its original state could jeopardise the whole investigation.

The framework recommends preserving both traditional forensic evidences and digital forensic evidences. For traditional forensics evidences such as blood and/or hair sample, figure prints or saliva and so on. The digital forensic domain includes isolating physical & digital evidence, securing physical & digital evidences. Preserving the current state of the physical & digital evidences, this includes checking the SMART device if the power is ‘ON or OFF’. If the device is ‘ON’ then it needs to be put in a faraday bag or a rigid container, secured with support ties and ready for transportation in order to prevent further transmission. If it is ‘OFF’ then do not turn it ‘ON’ to prevent the device’s operating system from writing anything further on to the device otherwise it might modify potential evidences.

Potential Evidence Collection: the potential evidence collection phase is critical. This also applies to recovering and collecting of non-electronic evidences such as any written password, any hand written notes, hardware or software manuals, calendars, any computer printouts or photographs, any blank note pads because there might be indented writing on it. Therefore, a thorough documentation of potential evidences, the chain of custody information and this must show continuous possession and control of evidences. This will include who is responsible every time the evidence is transported or transferred.

Acquisition: acquiring of the data from any SMART device should be done only with methods that prevent or minimise the loss or change to the data during the process. Whichever method employed during this phase, there still be some degree of interaction with the device required. The manual and logical acquisition technique requires some degree of interaction and physical acquisition technique requires interaction or physical deconstruction of the device.

Examination: however, whichever method is employed to acquire data from the target device, this phase is designed to allow digital forensics personnel to systematically search for potential evidences on a SMART device and create detailed documentation for analysis. This can be archived by filtering and matching the patterns in its characteristics to discover hidden data. It will also enable the visibility and traceability of its originality. This will also help with validating the evidence and revealing hidden information in the data which is vital in proving the case.

PRECAUTION:

Extra cautiousness is advised if the software application or operating system of the digital mobile SMART device encountered is suspected of being modified such as jailbreaking. However, particular types of modifications might affect the way it is handled such as add-on security mechanisms in order to enhance the security features of the device. This might add extra login features to the device such as a token-based authentication mechanisms or biometric login feature. Inappropriate dealings with the device might cause lock down or even cause the device to destroy its contents. Another reason is, some SMART device might contain malware. Depending on the type of malware on the SMART device, it might try to spread itself over the network if the suspected device is connecting to the network's wireless connection. The infected application might contain functions that could trigger carrying out actions such as wiping clean the content of the device or modifying the contents. Another modification might be implemented for extra security reasons are usually carried out by security professionals of an organisation is remapping the keys. Pressing a key or combinations of keys that usually for a particular purpose but it might cause disaster with the new key remapping.

6.2.5.2 Virtual/Cloud Forensics:

Performing forensic analysis in virtual or cloud environment is not the same as conducting an analysis on a local or standalone computer. With cloud environment, the forensics personnel needs to trust whatever information provided by the cloud service provider. These information can be complete, partial or false however, these information are evidence and still have to be presented in court of law. In that case, the process of acquiring data, preserving and examining it plays a very important part as a result; every process including chain of custody must be documented.

Identification: the process of conducting forensics investigation in virtual and/or cloud environment, the process begins with the identification phase. This phase involves searching, documenting and recognition of potential evidence. This phase also includes determining the tool to use, obtaining a search warrant, identify the type of the cloud environment and also any other potential sources of evidence. As mentioned earlier, the cloud environment is very complicated as it is expected to be impractical or even impossible to have access to the physical crime scene. However, it is much easier to have access to the client side of the cloud such as a SMART device or consider collecting the non-digital information such as interviewing individuals or suspects to obtain username or password.

Data Acquisition: after the identification phase, potential evidences have been identified. In this phase, the identified potential evidence needs to be either collected or acquire the data. However, due to the multi-tenant nature of the cloud environment, acquiring the data is recommended rather than collecting the potential evidence. The purpose of avoiding potential evidence collection is to minimise disrupting other applications and customers that are using the service. The directives of the law is very clear, the collection of digital evidence can only be conducted by the cloud service provider not by the user. To acquire data from the cloud environment must focus on the logical items only and not the devices that hold the logical items. Based on the nature and the scope of the investigation, the integrity of the image or data acquired must be maintained. As a result, the method employed must be well-understood, defensible and well-documented.

Preservation: after potential evidence has been acquired, it must be preserved as well as the chain of custody. Preservation is defined as the process of maintaining and safeguarding the integrity and/or its original condition. This is a complex and very important procedure because it provides assurances with regards to the admissibility of potential evidences in the court of law.

6.2.5.3 Network Forensics:

As mentioned earlier (section 3.1.2), network forensics is under the umbrella of digital forensics. Network forensics is about monitoring of network traffics, collecting information for the purpose of intrusion detection and legal advice. Network forensics deals with volatile data and dynamic information. It captures, stores, analyse and record all network activities from e-mails, database queries to web browsing. Network forensics can reveal from communication level such as the user, time of the activity to the address and protocol levels. This information is vital to forensic personnel in terms of reconstructing the event and tracing back to the origin of the crime.

Identification: in a network environment, it is a challenge to establish where to locate the potential evidence. However, with this framework, the investigation started with the SMART device forensics and a link can be found on the device to other forensic domain such as cloud and network forensics. As a result, forensics personnel will not waste time but go directly to the device with information showing up on the mobile SMART device involved. There are also other tasks involved in this phase such as preparing appropriate tools for the case, obtain search warrant, documentation of the physical crime scene and preserve the status of any potential digital device. This documentation should include sketching, taking video footages and photographs. It should also include details about the physical device involved as potential evidence such as the PIN number, password, model, and type of device, what is its role in the network and so on.

Collection/Acquisition: after creating a detailed documentation of the crime scene in the identification phase, the forensic personnel need to make a decision whether to collect potential evidences or acquire the data. If the decision is to acquire the data, the device should be kept but a decision whether to isolate it from the network or keep monitoring the system. If the decision is to isolate the device then a logical acquisition should be conducted before isolating it. If the device has a wireless capability, block it so there will be further communication via the wireless connection.

Preservation: in the network environment, in order to maintain the integrity of the acquired data, it needs to verify with verification functions such as hash or digital signatures to confirm that the acquired image is no different to the original.

Examination: after the data has been acquired, this phase is designed to examine the acquired image which includes an in-depth and systematic search for information which is vital for proving the case.

Analysis: this phase is designed to determine the significance of the examination phase's results. This phase is also designed to provide evidence for the case by identifying the relationships between fragments of data so the conclusion can be based on the evidence found. Therefore, a systematic approach should always be adopted to ensure consistency. This may involve analysing the time, hidden data, the applications and the files of the acquired data. The analysis should also include identifying people, places and events and so on. The analysis should also define their characteristics and relationships. It is also recommended that a complete documentation of the analysis phase be completed. As mentioned earlier (section 4.4), to analyse the extracted data, a systematic and methodical approach should always be adopted. This will help forensic personnel to reach a well informed decision based on the data.

Presentation: after analysing the acquired data, the conclusion and the results will need to be presented. This phase is designed to present a summary and an explanation of the results. Audience varied depending on the nature of the incident under investigation but the findings must be presented in the court of law. Therefore, the audience ranges from law enforcement officials and legal experts to corporate management, the general counsel and families and friends of the victims. However, it will be based solely on each country's law, as a result, carefully planned presentation of the case in the court of law is vital to the successful outcome of a trial.

Reporting: this phase involves writing a report to summarise the processes and various steps of the investigation to show how the conclusion was reached. This report will also include information such as the expertise and knowledge of the digital forensics examiner, the methodology, tools and techniques employed and the chain of custody documents, any problems and any procedural error should be included, any supporting materials should all be submitted together. Therefore, a good report wholly depends on if a careful record of all actions and processes during the investigation was well maintained. Reporting come about when the acquired data has been searched and analysed and potential evidences has been found. Most of the digital forensic tools come with built-in reporting feature that can be customised. Such customisation for instance, it allows the organisation to re-structure the report template, insert the organisation logo and so on. SMART devices allow its user to capture audio or video recordings of an event. Such evidence cannot be presented in a printed hard-copy reporting format. Therefore, removable media such as CD-ROM or DVD-ROM or a flash drive can be used for such evidence.

Returning evidence: this phase is designed to ensure that all physical and digital property is returned to its rightful owners.

6.3 CONCLUSION

Figure 3.17 illustrated the STRAW MAN model, the first attempt in developing a digital forensic investigation process model derived from the theories gained from the literature. The data collected during the pilot study and the test case scenarios provided a basis to evaluate the performance of the STRAW MAN. The evaluation results were then used with reference to the relevant standards and best practice guidelines in the field to make improvements to the STRAW MAN. A new name was given to the STRAW MAN after the improvements "Multi-disciplinary Digital Forensic Investigation Process Model (MDFIPM)".

This highlights the new digital investigation framework known as the Multi-disciplinary Digital Investigation Framework and also the recommendation of best practice guidelines for forensic practitioners. The new investigation framework was developed based on the knowledge and experiences gained during this study. Due to the fact that forensic experts believed that models are just an abstraction of a process employed to examine the evidence, an abstract representation of reality. They just generalise an informal procedure to deliver a framework. That framework provides a detailed understanding of what each process is to do and not do.

The new investigation framework is objective based. This means that each phase has an objective and tasks to complete. This is followed by the recommendation to digital forensic practitioners in a best practice guideline also developed during this study. This guideline is applicable to both the Multi-disciplinary Digital Forensic Investigation Process Model and the Multi-disciplinary Digital Forensic Investigation Framework.

In the next chapter, chapter seven provides a detailed discussion of the findings. This also leads in to the results of the hypotheses tests and the answering of the research question.

Chapter Seven

Discussions of Findings

7.0 INTRODUCTION

This chapter is to test the hypotheses based on the evidence presented in the previous chapters, answer the research question and to discuss the implications. In addition the effectiveness of the selected methodology is to be evaluated and the limitations noted. Chapter four described and explained the design of the study and each of its phases. The Design Science (DS) research methodology was chosen to guide this study. DS provides an iterative methodology to fill the gap and address the problem found in the literature. Two fictitious case studies were also outlined and the test-bed was designed and documented. DS research methodology provides special emphasis on the artefact creation and improvement, its evaluation and a refining of the solution for the problem identified in the literature. The outcome of chapter four was an artefact, the STRAW MAN model. Importantly in chapters 5 and 6 the model was improved and two related artefacts developed; the framework and the practitioners guide.

Chapter seven has five main sections. Section 7.1 will be focusing on the hypotheses, testing and the decision whether to reject or accept them. Section 7.2 will be focusing on answering the research question, while section 7.3 provides a discussion of these conclusions. Section 7.4 evaluates the effectiveness of the methodology and the limitations. The final section, section 7.5 provides the conclusion for this chapter.

7.1 HYPOTHESIS TEST AND THE RESEARCH QUESTION

As it shown in section 4.6, there are four hypotheses developed in order to test the strength of the findings of this study. The four hypotheses are: H1: the network forensic investigation process model will be suitable for mobile forensic investigation. H2: the computer forensic investigation process model will be suitable for cloud forensic investigation. H3: a multi-disciplinary digital forensic investigation process model will improve the effectiveness and efficiency of digital forensic investigation. H4: a comprehensive framework to guide the investigator on best practices will improve the effectiveness and efficiency of digital forensic investigation. These hypotheses were tested by following the evaluation methodology showed in section 4.5 and in table 4.2.

Each hypothesis was evaluated with the help of the evaluation method mentioned earlier in table 4.2. The attributes and properties of the straw man model were also brought in to the evaluation process. In addition to these data, the principles, and standards from reputable organisations such as NIJ, Daubert, DoJ, the ISO/IEC 27037, the IOCE and the ACPO were applied. Some of the existing digital investigation process models were used while running the two case studies during the data collection phase on the test-bed shown in figure 4.6. The results from this evaluation process were used to test the validity of the hypotheses and also to answer the research question.

Table 7.1: Hypothesis testing criteria.

Evaluation Methods	Attributes	Properties
Observational	• Completeness • Consistency • Accuracy • Performance • Reliability • Usability • Fit with the Organization	• Efficiency • Effectiveness • Efficacy • Ethicality • Elegance
Analytical		
Experimental		
Testing		
Descriptive		

In order to test whether a network forensic approach is suitable for forensic investigation in a multi-disciplinary environment, an evaluation methodology is required to guide the process. Table 7.1 shows the processes, the attributes and the properties that a model with a multi-disciplinary capability should have. The design evaluation method also defines five main phases as showed in figure 7.1.

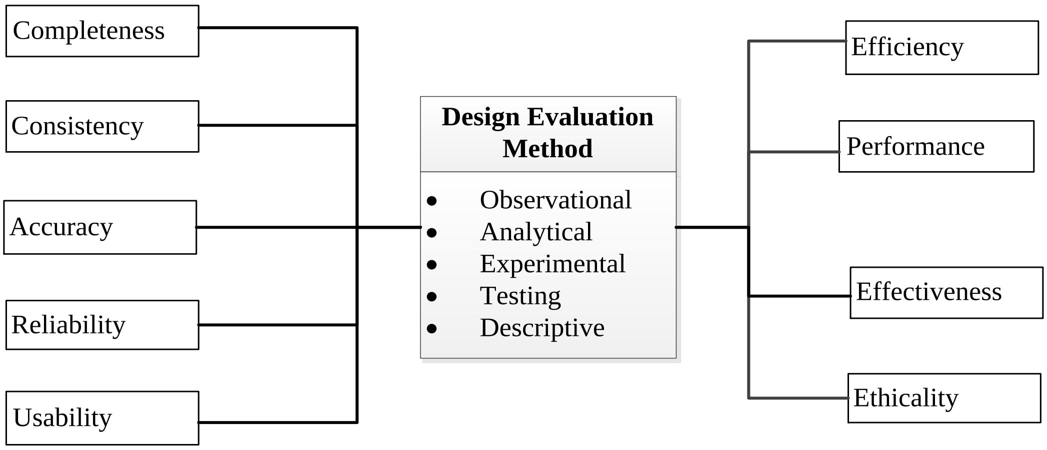


Figure 7.1: Relationships between attributes and properties of a model.

The DS evaluation methodology shown in table 4.2 will be used to evaluate the artefacts and also in the testing of the hypotheses and to answer the research question. Following in table 7.2 is the decision matrix table developed to illustrate how the ratings used in the evaluation were reached.

Table 7.2: Evaluation decision matrix.

	Observational 1	Analytical 4	Experimental 1	Testing 1	Descriptive 2	Possible total
Attributes 6	6	24	6	6	12	54/3=18
Properties 5	5	20	5	5	10	45/3=15
Total	**11**	**44**	**11**	**11**	**22**	**99/3=33**

1 – 33 = Low; 34 – 66 = Medium; 67 – 99 = High

As it shows in table 4.2, only one criterion under observational - Study the artefact in depth in a test case environment. Analytical there are four criteria which are - Examine structure of artefact for static qualities; Study fit of artefact into technical IS architecture; Demonstrate inherent optimal properties of artefact or provide optimality bounds on artefact behaviour and then Study artefact in use for dynamic qualities (e.g., performance). Only one under experimental which concerns with the usability of the artefact while testing concerns with Executing the artefact interfaces to discover failures and identify defects. The final criteria concerns with two – the use of the information from the knowledge base (e.g., relevant research) to build a convincing argument for the artefact's value (effectiveness & efficiency) and also, construct detailed scenarios around the artefact to demonstrate its value (effectiveness & efficiency).

Table 7.1 showed that the model has six attributes and five properties. The decision matrix works by observing the underlying structure of the data and its behaviour during the experimental phase. The evaluation criterion of DS research is then used to evaluate the artefacts against its attributes and properties. The results will then run through the decision matrix and the results will be the rating applied for that particular field in the testing table.

The following tables are the discussion of the outcomes of the evaluation used to test the hypotheses developed for this study.

Table 7.3: Hypothesis one testing.

H1: ***network forensic investigation process model is suitable for forensic investigation in a multi-disciplinary environment.***

Attributes/ Properties	Observational	Analytical	Experimental	Testing	Descriptive
Completeness	Low	Low	Medium	Medium	High
Consistency	Low	Low	Low	Low	High
Accuracy	Low	Low	Low	Low	High
Performance	Low	Low	Low	Low	High
Reliability	Medium	Medium	Medium	Medium	High
Usability	Medium	Medium	Medium	Medium	High
Efficiency	Low	Low	Low	Low	High
Effectiveness	Low	Low	Low	Low	High
Ethicality	High	High	High	High	High

The hypothesis one was designed to test the current network forensics investigation procedures whether it is suitable to conduct a forensic investigation in a multi-disciplinary environment. When the network forensic investigation process model was applied on the two case studies, it was observed to have low performance on six criteria and two on medium and one high performance which was on the ethical criteria. This is because, in the very first phase of the model involved in chapter three - figure 3.13, it is known as the preparation phase. It was designed to acquire authorizations and legal warrants so that privacy of the network users is not violated.

The model was found to be low on some criteria such as completeness, consistency and performance. This is because, it is only complete and consistent when it is used in a network environment but not to investigate a SMART device that is crime related. With regards to the analytical phase, this is designed to evaluate the complexity of the artefact, behaviour of the artefact and the fitness of the artefact when applied in this multi-disciplinary environment. Table 7.2 showed very similar results to the observational phase. For instance, the performance is low on effectiveness and efficiency because the model involved is found not be very effective in such architecture. However, it is still usable since the model contains the main four phases such as collection, preservation, analysis and presentation.

With regards to the experimental and testing phases of the design evaluation method, the completeness attribute showed a medium performance in the scenario tests. However, the last phase descriptive has high performance on all criteria. This is because; information from academic knowledge base can be applied and used to build an informed argument for the artefact in this study. As a result, it can be concluded that hypothesis one is rejected.

Table 7.4: Hypothesis two testing.

H2: ***computer forensic investigation process model is suitable for a forensic investigation in a multi-disciplinary environment***

Attributes /Properties	Observational	Analytical	Experimental	Testing	Descriptive
Completeness	Low	Low	Medium	Medium	High
Consistency	Low	Low	Low	Low	High
Accuracy	Low	Low	Low	Low	High
Performance	Low	Low	Low	Low	High
Reliability	Medium	Medium	Medium	Medium	High
Usability	Medium	Medium	Medium	Medium	High
Efficiency	Low	Low	Low	Low	High
Effectiveness	Low	Low	Low	Low	High
Ethicality	Low	Low	High	High	High

Hypothesis two was designed to test the current computer forensics investigation procedures whether it is suitable to conduct a forensic investigation in a multi-disciplinary environment. When the computer forensic investigation process model was applied on the two case studies, it was observed to have low performance on seven criteria and two on medium. This is not only a change from the results showed in table 7.2 but the performance regarding the ethical criteria is low. The model involved has five phases as illustrated in chapter three - figure 3.15. The first phase is known as the pre-process phase which has provision for acquiring proper authority but lacks to mention any provisions for owner's or user's privacy.

Additionally, this model was found to be low on some criteria such as completeness, consistency and performance. It can only be complete and consistent when used in a network environment instead of investigating a SMART device and cloud related crime. The analytical phase is designed to evaluate the complexity, behaviour and fitness of the artefact when applied in a multi-disciplinary environment. Table 7.3 showed results similar to the observational phase. For instance, the performance is low on effectiveness and efficiency because the model involved is not effective in such architecture. This is a result of computer forensics being solely focused on standalone or single computer not networked computers. However, it is still usable as the model contains four main phases such as collection/acquisition, preservation, analysis and presentation.

Table 7.5: Hypothesis three testing.

H3: a multi-disciplinary digital forensic investigation process model will improve the effectiveness and efficiency of digital forensic investigation.

Attributes/ Properties	Observational	Analytical	Experimental	Testing	Descriptive
Completeness	High	High	High	Medium	High
Consistency	High	High	High	Medium	High
Accuracy	High	High	High	Medium	High
Performance	High	Medium	High	Medium	High
Reliability	High	Medium	High	Medium	High
Usability	High	Medium	High	Medium	High
Efficiency	High	High	High	High	High
Effectiveness	High	High	High	High	High
Ethicality	High	High	High	High	High

With regards to experimental and testing phases of the design evaluation method, the completeness attribute showed a medium performance in the scenario tests. However, the last phase descriptive has high performance on all criteria. This is because; information from academic knowledge base can be applied and used to build an informed argument for the artefact in this study. As a result, it can be concluded that hypothesis two is rejected.

The hypothesis three was designed to test the suitability of the STRAW MAN forensics investigation process model to conduct a forensic investigation in a multi-disciplinary environment. The STRAW MAN forensic investigation process model was applied on the two case studies. It was observed to have high performance on all phases of the evaluation method, and all performance criteria. This is a change from the results showed in table 7.2 and 7.3.

The model involved consists of 22 phases comprising of 12 main phases for mobile SMART device forensics and five each for cloud/virtual environment and network based investigation. The implication is that for a mobile SMART device - which converges many segregated areas - investigation knowledge from each of the implicated areas is required for effective and efficient investigations. When the STRAW MAN is observed under those two case studies, all criteria were met. Testing under the analytical phase, performance, reliability and usability were rated medium. The analytical phase required the artefact to be tested for qualities, fitness of the artefact into technical information system and its dynamic qualities for performance. However, these tests will not be completed until the artefact will be tested in a real case in the field.

Again, under experimental and testing phases, the artefact needs to be studied under a controlled environment for qualities such as its usability. All the criteria were satisfied however, for functional testing, the top six criteria completeness, consistency, accuracy, performance, reliability and usability were only scored medium. This is again because the STRAW MAN was tested with case studies in the lab and it still requires testing in the field to fully satisfy these criteria. The last phase descriptive has high performance on all criteria. This is because; information from academic knowledge base, guidelines, principles and standards from reputable organisations were all taken into account from the design phase, development and testing of this artefact. As a result, it can be concluded that hypothesis three is accepted.

Table 7.6: Hypothesis four testing.

H4: ***a comprehensive framework to guide the investigator on best practices will improve the effectiveness and efficiency of digital forensic investigation.***

Attributes/ Properties	Observational	Analytical	Experimental	Testing	Descriptive
Completeness	High	High	High	Medium	High
Consistency	High	High	High	Medium	High
Accuracy	High	High	High	Medium	High
Performance	High	Medium	High	Medium	High
Reliability	High	Medium	High	Medium	High
Usability	High	Medium	High	Medium	High
Efficiency	High	High	High	High	High
Effectiveness	High	High	High	High	High
Ethicality	High	High	High	High	High

The hypothesis four was designed to test the suitability of comprehensive framework in guiding forensic practitioner on best practices; it might improve the effectiveness and efficiency of digital forensic investigation. The end results for evaluating of the forensic investigation framework was very similar to STRAW MAN model evaluation results. The framework consists of 22 phases also but with the framework, the tasks for each phase are recommended.

When the investigation framework is observed under those two case studies, all criteria were met. Testing under the analytical phase, performance, reliability and usability were rated medium. The analytical phase required the artefact to be tested for qualities, fitness of the artefact into technical information system and its dynamic qualities for performance. However, these tests will not be completed until the artefact will be tested in a real case in the field.

Again, under experimental and testing phases, the artefact needs to be studied under a controlled environment for qualities such as its usability. All the criteria were satisfied however, for functional testing, the top six criteria completeness, consistency, accuracy, performance, reliability and usability were only scored medium. This is again because the all-inclusive investigation framework was only tested with case studies in the lab, still need to test it in the field to fully satisfy these criteria. The last phase descriptive has high performance on all criteria. This is because; information from academic knowledge base, guidelines, principles and standards from reputable organisations were all taken into account from the design phase, development and testing of this artefact. As a result, it can be concluded that hypothesis three is accepted.

Four hypotheses have been tested as part of this study. The DS research, design evaluation methodology, and the above mentioned nine attributes and properties of an investigation process model were employed for the testing of these four hypotheses. The test results indicated that H1 and H2 were both rejected. The results concluded that a generic investigation process model that was developed for a specific sub-field of digital forensics cannot be used for an investigation in a multi-disciplinary environment. For instance, network forensic, cloud forensics or mobile forensics. Based on the hypothesis test data, effectiveness and efficiency cannot be achieved and the completeness and the integrity of the investigation process might be compromised. As a result, the admissibility of the potential evidence might be questionable in the court of law.

The test results also indicated that H3 and H4 were both accepted. These are the artefacts developed as the solution for problem identified in the literature. The advantage of these artefacts is that there were specifically developed for an investigation in a multi-disciplinary environment. The test results indicated few weaknesses of the artefacts however, these are minors caused by the facts that these two artefacts have not been tested in a real forensic investigation environment.

Table 7.7: Hypothesis test results.

H1	*Network forensic investigation process model will be suitable for mobile forensic investigation.*	Rejected
H2	*Computer forensic investigation process model will be suitable for cloud forensic investigation.*	Rejected
H3	*A multi-disciplinary digital forensic investigation process model will improve the effectiveness and efficiency of digital forensic investigation.*	Accepted
H4	*A comprehensive framework to guide the investigator on best practises will improve the effectiveness and efficiency of digital forensic investigation.*	Accepted

The data provided in table 7.6 charted a summary of the hypotheses developed for this study and the outcomes of the hypotheses tests.

7.2 RESEARCH QUESTION

This section is designed to answer the research question. The research question is *"What can be done to improve the effectiveness and efficiency of digital forensic investigation?"* In chapter 4, the research methodology was chosen for this study, DS research method as discussed in section 4.2.1. The first entry point of DS research method is called problem-centred initiation illustrated in figure 4.2. This entry point focuses on identifying the problem and the motivation for the study. As a result, from the literature reviewed in chapter two and three, the problem was identified. As part of the entry point one of the DS research, the problem also needs to be defined and show its importance; as showed in sections 3.4 and 3.5.

The second entry point is concerned with defining the objective and the solution; this determines what a better artefact does. This was accomplished by the reviewing of the literature in chapter 2 and the critical review provided in chapter 3. The third entry point is concerned with the designed and the development of the artefact. Entry point four is concerned with the demonstration and solving of the problem. Phase number four is concerned with the evaluation of the artefact to observe its effectiveness and efficiency.

Following the guidance of the chosen research methodology, this study managed to find the answer for the research question and also test the hypotheses. This study is aiming at finding a way to improve the effectiveness and the efficiency of digital forensic investigation. After evaluating the artefact, observing its performance while running through two test case studies, the hypotheses were tested. After testing the hypotheses, it can be concluded that the best answer for the research question is the Multi-disciplinary investigation process model/framework. The problem identified in the literature, there is no such investigation process model yet. As a result, the answer is to develop a Multi-disciplinary investigation process model/framework.

7.3 IMPLICATIONS OF THE RESULTS

It is evident in the literature that the advancement in today's communication technologies has changed the way individuals conduct their daily tasks and the way businesses operate. This study focusses on SMART technologies and these devices interact with various types of networks wirelessly. In section 2.2, various types of wireless business information systems found in the literature as illustrated in figure 2.6 were reviewed. This growth introduces more access devices which entail new security vulnerabilities which is a threat to both businesses and private users. These new vulnerabilities have become the main targets for malicious attacks. There has been research in the field in an attempt to prevent intruders and illegal access to the network.

There are many prevention and detection methods and techniques found and implemented but criminals seem to always find a way to break these security mechanisms as explained in chapter two. These security incidents created a new field known as digital forensics because of the need to find the criminals. Digital forensics is defined in section 3.1.2 as the art of employing computer technology in order to identify, preserve, analyse and the presentation of digital evidence gathered from a compromised device. Extracting data from suspected devices can produce vital evidence for any digital crime investigation. However, the growth of communication technologies has created sub-fields within the digital forensic arena. There are four main sub-fields known as computer forensics, mobile forensics, network forensics and cloud forensics as illustrated in figure 3.1.

Section 3.1.2 also explained in detail various ways of extracting data from a mobile SMART device. These devices have the ability to install third party software applications such as games, e-mail clients, online banking application and more. These device also have phone book that stored contact details, also has the ability to access the Internet and social networking sites. As a result, these are vital information to forensic investigators. However, there are challenges of extracting data from a mobile SMART device.

These devices are running on an operating system like computers. However, various manufacturers have developed their own devices and it runs on their own proprietary operating system such as iPhone and other mobile SMART devices from Apple Inc. Section 2.3.2 explained the structure of the Android operating system developed by Google and SMART devices manufactured by companies such Samsung are running on it. There were guidelines explained in detail in sections 3.2.2 and 3.2.3. They both recommended strict policies and procedures to follow in order for potential evidences extracted from suspected devices to be admissible in the court of law. These two guidelines were developed by the ACPO and NIST. The ACPO guidelines focus on ensuring that proper practices and procedures are followed. The NIST guidelines are aiming at aiding forensic practitioners in developing proper policies and procedures and also preparing forensic experts for future technological changes.

Section 3.2.4 provided a review of existing digital forensic investigation process models found in the literature starting from 1995 to 2012. This shows the growth in the importance of digital forensic. However, it also emphasises the fact that forensic practitioners need to use standardised methods and techniques in order for the findings of an investigation to be admissible in the court of law. The literature reviewed in chapter two highlighted the fact that every device was developed differently. The operating systems’ requirements are all different as well. As a result, the requirements for every case are going to be different also.

In addition, section 3.2.4 also highlighted the fact that the existing investigation process models were developed for a particular sub-field. As a result, section 3.4 explained the details and identified the problem found in the literature for this study. It is also highlighted the fact that there is no investigation process model yet for forensic investigators to be used when challenged with a case that more than one sub-field of digital forensics is involves. The scenario test also shows the character of an investigation that is involved a mobile SMART device as a result, the STRAW MAN model was developed as illustrated in figure 3.17 for testing. The proposed model was drafted from the learning of the analysis in this chapter and formulated to fill the gaps and avoid repetition.

7.4 METHODOLOGY EVALUATION

This section is aimed to evaluate the contributions of the employed research methodology (Design Science) to the design of this study, its processes, development of knowledge, innovation and the outcome of the study.

7.4.1 The Adopted Methodology (DS)

The purpose of this study is to find a way to improve the effectiveness and efficiency of digital forensic investigation processes. Section 4.1 discussed the design methodologies of the twelve investigation process models reviewed in 3.2.4. Section 4.1.1 highlighted the findings of the evaluation in 4.1, most of the design methodologies started off by defining the problem with the existing investigation process models. Then analysed selected forensic investigation process models from the literature. However, section 4.1.1 highlighted that most of them focus on the design problems of the existing models. It was also evident that their purposes were to enhance and improve a particular area of the forensic investigation processes. It was also evident from section 4.1.1 that still there is still no digital forensic investigation process model to guide digital forensic practitioners when facing a case that involved more than one sub-field of digital forensics.

The methodology employed by this study is Design Science (DS) research method as explained in section 4.2.1. Figure 4.2 provided a graphical illustration of DS research method and figure 4.3 outlined the criteria for conducting a DS research. It was highlighted in section 4.2.1 one of the differentiation advantages of DS research method which is, DS is solution-oriented. Design methods evaluated in section 4.1.1, some of them were problem-oriented and some were technology-oriented. As a result, DS was employed because it focusses on the solution to a problem and not only that but the perfection of the solution as in figure 4.2. The development of the design of this study as illustrated in figure 4.5 was based on DS method. DS research method and the design both have an iterative feature implemented. The purpose is to keep refining and re-evaluating the new solution until it reaches the desired outcome.

The implementation of the iterative feature between entry point two and the sixth phase of DS research method is evidence that its main focus is on the artefact. As mentioned earlier, the purpose of this study is to find a way to improve the effectiveness and the efficiency of digital forensic investigation processes. DS method guided this study to focus on the artefact, the solution and not just that but, DS also encouraged by providing a way for this study to keep refining the artefact until the desired outcome is reached. Entry point five of DS focusses on evaluating the artefact which is the time to observe how effective and efficient the artefact is.

Even though DS method is solution-oriented but its processes were also designed to warrant the novelty of the study. For instance, entry point number one allowed this study to explore the knowledge base, the literature, in order to make sure that the gap for the study is there. Define the problem and the motivation for and show its importance. Entry point number two focusses on defining the objectives and also identify what would a better solution accomplish. At the end, DS also reminds the researcher to contribute back to the body of knowledge. The final entry point of DS encourages communicating of the findings by utilising both the academic and professional publications.

However, it is believed that DS is best in an environment where the researcher is very experienced researcher. DS can be best applied in a confirmatory study because DS is solution-oriented with and iterative feature. DS implemented an iterative feature on the second entry point which allows the researcher to keep defining or re-defining its objective and solution. This is dangerous when the researcher is not an experience researcher because the researcher can easily fall into an infinite loop. Keep re-defining the objectives and keep re-evaluating the artefact. DS research method can be improved by implementing a phase to help with defining the scope of the study so the boundary can be clearly defined.

7.4.2 Limitations Of This Study

A good literature analysis always facilitates a foundation for understanding of the gaps, issues and the problems for research. However, one of the limitations of this study is the lack of prior research on the chosen topic. Depending on the currency or scope of a research topic, there were very little found in the six databases defined in section 2.1.2 that directly deal with this particular topic. As a result, an exploratory approach was employed during the literature analysis in order to explore an entirely new research typology.

After the evaluation of the STRAW MAN model, it was discovered that the data gathered from the two test case scenarios did not meet the requirements to conduct an empirical evaluation of the artefacts. Two test case scenarios were developed, one was used in the pilot study to confirm the theory and the other was used to evaluate the performance of the artefacts. It is now believed that the measure used to evaluate the artefacts.

The processes of the MDFIPM and the MDFIF were tested and evaluated using test case scenarios specifically designed to illustrate its capabilities to preserve a structured and logical flow. This provides consistency, reliability, usability, efficiency and effectiveness. These ensure that the principles of legitimacy and admissibility are satisfied. Despite the model and the framework being theoretically tested and evaluated in a controlled environment, it has yet to be applied on a real case environment.

7.5 CONCLUSION

An in-depth and methodical understanding of the findings has been discussed in chapter five. However, this chapter includes five sections that further discuss these findings. The first section focussed on discussing the testing of the hypotheses and how this study arrived at the decision to reject or accept each of them. The second section discussed the answer for the main research question while the third section provided a detailed discussion of those decisions. The fourth section discussed the evaluation results based on the effectiveness of the chosen methodology for this study and also the limitations of this work.

The discussions in this chapter have led to the discovery of the strengths and weaknesses of the solution (artefact). The discussions also helped to identify the limitations of this study and an approach leading to the improvements and an area for further research. The following chapter will summarise and conclude this thesis.

Chapter Eight

Conclusion

8.0 INTRODUCTION

Chapter one provides a brief overview of the problem areas for this study. In chapter two, these problem areas were defined in detail by focusing on the technical aspects and mechanisms of the digital mobile SMART devices. Chapter two also defined the network context that a mobile SMART device utilises. Chapter three was designed to expand the literature reviewed in chapter two from technical environments to look directly at guidelines and investigation process models that are currently employed by forensic investigators. Chapter three highlighted the problems further, by looking at the various sub-fields of digital forensics.

Therefore, the main research question is concerned with improving the effectiveness and the efficiency of an investigation that involves more than one of the digital forensic sub-fields. The study was aimed to fill this identified gap in the literature by developing an investigation process model initially known as the STRAW MAN model that an investigator can use in such an investigation environment. This new STRAW MAN model is a resolved model from analysis of the existing models. At the same time, the phases of the STRAW MAN model were aligned to the existing standards and principles developed by reputable organisations in the field such as the ACPO, NIST and the ISO related standards. A test-bed was designed covering the three different sub-fields of digital forensics and implemented. The Mobile device forensics, Network forensics and Cloud forensics were used. Two fictitious case studies were developed then the STRAW MAN model was used to investigate these cases.

A full report of the results was reported in chapter 5 and the requirements for improvements to the STRAW MAN model were identified. The test case results identified the character of digital forensics investigation and areas that need improvements. Table 5.31 illustrated the process used to measure the performance of the STRAW MAN model and in figure 5.32 showed the new digital forensic investigation model.

The sections of this chapter are designed to conclude this study. Section 8.1 summarises the contributions of this study to the body of knowledge. In section 8.2, the areas for further research are explained.

8.1 CONTRIBUTIONS

In order to evaluate the contributions that this study has made to the body of knowledge, this section is divided into three sub-sections. First is to look at findings based on initial development of the STRAW MAN model. Second is to look at the results of the performance evaluation of the STRAW MAN model. Finally, it looks at the development of the recommendations for digital forensic practitioners in chapter six.

8.1.1 The STRAW MAN model

An important contribution of this study is the development of a new digital forensic investigation process model. The problem identified in the literature established that the rapid growth of communication technologies creates more sub-fields in the digital forensic domain. Researchers in the field developed various investigation process models to gather for each of the sub-fields. However, this study identified the gap in the literature and the STRAW MAN model is one investigation process model that has the ability to gather evidence for an investigation in a multi-disciplinary environment. At the same time, without compromising the effectiveness and the efficiency of the investigation while maintaining the integrity of the evidence.

The case studies indicated that digital forensics has a complex nature therefore it requires multi-disciplinary skills and abilities. Thus, this study has found that the solution to the problem identified should meet those requirements. The solution should have multi-disciplinary skills and abilities. Reputable organisations such as ACPO, ISO/IEC, NIST have developed principles, standards and guidelines. Those are imperative with regards to the integrity and admissibility of the evidence in the court of law. Those standards and principles together with the Daubert criteria, NIJ and the DoJ guidelines were employed in the design, development and the evaluation of the new investigation process model.

8.1.2 The STRAW MAN Model Improvements

The case studies showed that the gap identified in the literature exists and also verified the character of digital forensic investigation on mobile SMART device. The case studies also indicated areas of the STRAW MAN model that needs to be improved. As it was mentioned in section 5.2.1, a model is only an abstraction. Forensic personnel think that a model is just a recipe. However, the performance evaluation of the model indicated that, the investigation processes of the model were not in control of the whole investigation processes. It showed that we are doing the right thing but we are not doing it right.

As a result, the improvements made to the investigation process model was, that an objective was given to each of the phases. Out of that, an investigation framework was developed. This Multi-disciplinary investigation framework has been tested on the same case studies also. The test results for the framework indicated the all criteria were met. Results from the analytical phase of the evaluation method employed, the performance, reliability and usability were all rated medium. The framework was developed based on the model as an improvement to the STRAW MAN model. Same as the STRAW MAN model, the framework comprises of three different disciplines and consists of 22 phases. However, with the framework, an objective was allocated to each of the 22 phases so, to archive the objective, recommended tasks or steps for each phase are recommended.

It is evident in the evaluation results that the multi-disciplinary framework has made big improvements from the model. However, the analytical phase of the evaluation method requires the artefact to be tested for qualities. This is to determine its fitness and dynamic qualities for performance. However, these tests cannot be concluded until the artefact is being tested in a real case environment. Chapter four and in section 4.6 outlined four hypotheses that were developed for this study. In section 7.1 of chapter seven showed the hypotheses testing results. Two of the four hypotheses were rejected. This confirmed that an investigation process model that was developed for a specific sub-field of the digital forensic arena is not suitable for an investigation in a multi-disciplinary environment. The results indicated that the completeness, effectiveness and efficiency of the investigation are compromised. As a result, the integrity of the evidence is also affected. Consequently, the admissibility of the evidence in the court of law is also uncertain.

8.1.3 The Best Practice Guidelines for Practitioners

Chapter six of this document provides recommendations for best practice guidelines for practitioners. These recommendations were results of the learning developed from the findings of this study. The technological advancements in the communication arena have direct impact on digital forensics. As a result, practitioners in the field need to re-evaluate their status and adapt. However, there will always be a need to extract and analyse digital data from digital devices as evidence in an investigation.

The guideline was developed to be employed in conjunction with the multi-disciplinary investigation process model and the framework. The purpose of the guideline is to provide in-depth understanding into the processes of the model and the framework. It also explains the processes involved in each of the phases from mobile SMART devices to an investigation involving virtual/cloud technologies and private organisation network environment.

The guideline has two objectives: it can be very helpful in developing policies and procedures on how to deal with multi-disciplinary fields of investigation. Digital forensic experts will also find the guideline useful when facing such investigation environment. The intended audience for the guideline can be varied, from first responders to digital forensic practitioners in the field. The main concern within the digital forensic communities is that, various sub-fields of digital forensic require different methods and procedures. Not only that but every device has its own structure, architecture and operating system.

The model and the framework have particular goals; to maximise the effectiveness and efficiency of the investigation and the integrity of the evidence. The guideline was developed to help digital forensic personnel in order to archive the model’s and the framework’s goals. The guideline explains the phases involved and their relationship to digital forensic processes of the multi-disciplinary investigation framework’s phases.

8.2 AREAS FOR FURTHER RESEARCH

The rapid growth in the digital communication technology’s domain has posed significant concerns for digital forensic personnel. The evaluation methodology employed consists of five phases which was used together with the artefact’s attributes and properties to test the hypothesis. The results confirmed the performance, reliability and usability of the artefact.

The new digital forensic investigation process model and framework were designed and developed for an investigation in a multi-disciplinary environment.

The recent introduction of SMART watches is an enhancement in the area of wearable digital mobile devices. SMART watches are capable of more than telling time, monitoring your heart rate and motivation for exercise. A SMART watch now has the ability to make phone calls, surf the internet and accessing private networks. These new tools have changed the way daily tasks and businesses are conducted. SMART watch technology is a new addition to the WBAN family discussed in section 2.5.3 as its ability to access the internet increases its potential to be involved in criminal activities. For instance, some Universities do not allow SMART watches in the exam rooms because students can access the Internet and look for answers.

These devices need to be studied further for a better understanding of their properties, attributes and how they behave. In addition, the technology used for their memory and storage, connection mechanisms and the architecture of their hardware and software need to be studied further. A better understanding of their features allows the investigation model and framework to be more adaptable to future technological changes. Future technological changes include the ‘Internet of Things (IoT)’ which is expected to advance the connectivity of devices, systems and services on a wireless level. The technological changes introduced by the IoT also referred to as ‘Internet of Everything (IoE)’ is in the networking domain. The interconnectivity of these embedded devices includes a variety of protocols, domains and applications.

This new technology also aids the enabling of the use of advanced applications such as Smart Grid which can expand to areas such as Smart city. The IoT also expands to the healthcare systems and includes applications heart monitoring implants, biochip transponders and the automotive field such as built-in sensors on vehicles. These devices alongside various technologies such as

SMART thermostat systems and washer/dryer systems that utilise Wi-Fi technologies have been used to collect numerous amounts of useful data. However, these devices have been known to involve criminal activities such as hacking heart monitoring implants and commit murder. As mentioned earlier, this new network structure and technology entails a variety of protocols, domains and applications that needs to be studied in more depth.

In order for the new artefact to be adaptable and better fit with future technological changes, the new artefact needs to have a quick revision feature implemented. However, the phases of the new framework developed in this study have objectives with individually set of tasks to guide the investigator in order to achieve the objective. An in-depth understanding of these new networking technologies might require a quick revision of the tasks. As a result, adding new task(s) to a phase(s) might be required in order to achieve the same objective.

8.3 CONCLUSION

This study found a gap in the literature and developed an artefact as the solution to fill the gap. The model and the framework have been tested in the lab on case studies however; the hypotheses test indicated that the artefact still needs to be tested on a real case in the field. Similar to any area of the information communication technology arena, administrators, managers and practitioners still need to keep themselves up-to-date with current technologies. Every assessment made based on security threats, risks or vulnerability test report have major contributions to the knowledge base.

Similarly, digital forensic practitioners and researchers need to keep themselves up-to-date with technological changes, any changes with regards to principles and standards in the digital forensic arena. The multi-disciplinary model and framework have been developed with various standardised processes, principles from reputable organisations such as ACPO, NIST and so on implemented to its phases. However, it still needs to be tested on a real case. Researchers and digital forensic professionals also need to stay up-to-date with any technological change or changes in the standards, principles or regulations with regards to digital forensic especially in mobile SMART device domain.

References

Abhishek, K., & Mahasweta, S. (2011). Cloud Computing. In L. Wang, R. Ranjan, J. Chen, & B. Bentatallah (Eds.), *Cloud Computing: Methodology, Systems, and Applications* (pp. 3-29). UK: CRC Press.

Achi, H., Hellany, A., & Nagrial, M. (2008c). Network security approach for digital forensics analysis. *Proceedings of the ICCES 2008 International Conference on Computer Engineering & Systems*, *2008* (pp. 263-267). Cairo: IEEE.

Achi, H., Hellany, A., & Nagrial, M. (2009a). Methodology and challenges in digital security forensics of wireless systems and devices. *Proceedings of the ICCES 2009. International Conference on Computer Engineering & Systems, 2009* (pp.43-46). Alexandria: IEEE.

Achi, H., Hellany, A., & Nagrial, M. (2009b). Digital forensics of wireless systems and devices technical and legal challenges. *Proceedings of the 6th International Symposium on High-Capacity Optical Networks and Enabling Technologies (HONET), 2009* (pp.43-46). Alexandria: IEEE.

ACPO. (2007). ACPO Good Practice Guide for Computer-Based Evidence. *Official release version*, *4*(1), 72.

Ademu, I. O., Imafidon, C. O., & Preston, D. S. (2011). A New Approach of Digital Forensic Model for Digital Forensic Investigation. *IJACSA International Journal of Advanced Computer Science and Applications, 2*(12), 175-178.

Ajijola, A., Zavarsky, P., & Ruhl, R. (2014). A review and comparative evaluation of forensics guidelines of NIST SP 800-101 Rev.1:2014 and ISO/IEC 27037:2012. *Proceedings of the 2014 World Congress on the Internet Security (WorldCIS)* (pp. 66-73). London: IEEE.

Akers, P., McGrew, W., & Dampier, D. (2011). WiFi Stakeout: A network forensics tool for reconnaissance and first responders. *Proceedings of the 2011 International Conference on the Engineering and Industries (ICEI)* (pp. 1-4). Jeju: IEEE.

Albano, P., Castiglione, A., Cattaneo, G., & De Santis, A. (2011b). A Novel Anti-Forensics Technique for the Android OS. *Proceedings of the 2011*

International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA) (pp. 380-385). Maui: IEEE.

Albano, P., Castiglione, A., Cattaneo, G., De Maio, G., & De Santis, A. (2011). On the Construction of a False Digital Alibi on the Android OS. *Proceedings of the 2011 Third International Conference on Intelligent Networking and Collaborative Systems (INCoS)* (pp. 685-690). Fukuoka: IEEE.

Aldhaban, F. (2012). Exploring the adoption of Smartphone technology: Literature review. *Proceedings of PICMET '12: Technology Management for Emerging Technologies (PICMET), 2012* (pp. 2758 - 2770). Vancouver: IEEE.

Alghafli, K. A., Jones, A., & Martin, T. A. (2011). Guidelines for the digital forensic processing of smartphones. *Proceedings of the 9th Australian Digital Forensics Conference* (pp. 1-8). WA: ECU.

Ali, K. A., & Mouftah, H. T. (2011). Wireless personal area networks architecture and protocols for multimedia applications. *Ad Hoc Networks, 9*(4), 675-686.

Allen, S., Graupera, V., & Lundrigan, L. (2010). Android. In *Pro Smartphone Cross-Platform Development* (pp. 35-50). NY: Apress.

Allen, S., Graupera, V., & Lundrigan, L. (2010). Windows Mobile. In *Pro Smartphone Cross-Platform Development* (pp. 65-80). NY: Apress.

Almulla, S., Iraqi, Y., & Jones, A. (2013). Cloud forensics: A research perspective. *Proceedings of the 2013 9th International Conference on Innovations in Information Technology (IIT)* (pp. 66-71). Abu Dhabi: IEEE.

Apple Developer. (2012). *iOS technology overview.* Retrieved June 18, 2013, from https://developer.apple.com/library/ios/documentation/Miscellaneous/Conceptual/iPhoneOSTechOverview/iPhoneOSTechOverview.pdf

Apple.Inc. (2013). *iPhone user guide: For iOS 6.1*. Retrieved April 24, 2013, from http://manuals.info.apple.com/en_US/iphone_user_guide.pdf

Apple.Inc. (2013). *iPhone*. Retrieved April 24, 2013, from http://www.apple.com/iphone/specs.html

Arabo, A., & El-Mousa, F. (2012). Security framework for smart devices. *Proceedings of the 2012 International Conference on Cyber Security, Cyber*

Warfare and Digital Forensic (CyberSec) (pp. 82 - 87). Kuala Lumpur: IEEE.

Arpee, J. (2001). Designing the cellular network infrastructure. *R. F. Design, 24*(5), 26-26.

Ashcroft, J. (2001). Crime Scene Investigation: A Guide for First Responders. *US Department of Justice, NCJ, 1*(1), 1-93.

Astuti, D., Nyrhinen, A., Jarvinen, I., & Kojo, M. (2008). SLACP: A Novel Link-Layer Protocol for Wireless WANs. *Proceedings of the ICN 2008, Seventh International Conference on Networking.* (pp. 121 - 130). Cancun: IEEE.

Ayers, R. (2007). *Cell phone forensic tools: An overview and analysis update*: Computer Security Division, Information Technology Laboratory. Maryland: NIST.

Azadegan, S., Yu, W., Liu, H., Sistani, M., & Acharya, S. (2012). Novel Anti-forensics Approaches for Smart Phones. *Proceedings of the 2012 45th Hawaii International Conference on System Science (HICSS)* (pp. 5424-5431). Maui: IEEE.

Bader, M., & Baggili, I. (2010). iPhone 3GS forensics: Logical analysis using apple iTunes backup utility. *Small Scale Digital Device Forensics Journal, 4*(1), 15.

Ballagas, R., Borchers, J., Rohs, M., & Sheridan, J. G. (2006). The smart phone: a ubiquitous input device. *Pervasive Computing, IEEE, 5*(1), 70-77.

Banuri, H., Alam, M., Khan, S., Manzoor, J., Ali, B., Khan, Y., Yaseen, M., Tahir, M., Ali, T., Alam, Q., Zhang, X. (2012). An Android runtime security policy enforcement framework. *Personal and Ubiquitous Computing, 16*(6), 631-641.

Baranov, A. V., & Lyakhov, A. I. (2005). Estimating Performance of Arbitrarily Loaded Wireless Local-area Networks with IEEE 802.11 Protocol. *Automation and Remote Control, 66*(7), 1101-1114.

Baryamureeba, V., & Tushabe, F. (2004). The enhanced digital investigation process model. *Proceedings of the Fourth Digital Forensic Research Workshop* (pp. 1-9). Citeseer: DFRW.

Becher, M., Freiling, F. C., Hoffmann, J., Holz, T., Uellenbeck, S., & Wolf, C. (2011). Mobile Security Catching Up? Revealing the Nuts and Bolts of the

Security of Mobile Devices. *Proceedings of the 2011 IEEE Symposium on Security and Privacy (SP)* (pp.96-111). CA: IEEE.

Bednar, P. M., Katos, V., & Hennell, C. (2008). Cyber-Crime Investigations: Complex Collaborative Decision Making. *Proceedings of the third International Annual Workshop on Digital Forensics and Incident Analysis, 2008. WDFIA '08.* (pp. 3-11). Malaga: IEEE.

Beebe, N. L., & Clark, J. G. (2005). A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation, 2*(2), 147-167.

Bhargava, B., Wu, X., Lu, Y., & Wang, W. (2004). Integrating heterogeneous wireless technologies: a cellular aided mobile Ad Hoc network (CAMA). *Mob. Netw. Appl., 9*(4), 393-408.

Birk, D., & Wegener, C. (2011). Technical Issues of Forensic Investigations in Cloud Computing Environments. *Proceedings of the 2011 IEEE Sixth International Workshop on the Systematic Approaches to Digital Forensic Engineering (SADFE)* (pp. 1-10). CA: IEEE.

Bosch, P., Samuel, L., Mullender, S., Polakos, P., & Rittenhouse, G. (2007). Flat Cellular (UMTS) Networks. *Proceedings of the WCNC 2007 IEEE Conference of the Wireless Communications and Networking.* (pp. 3861 - 3866). Kowloon: IEEE.

Bosomworth, D. (2013). *Mobile marketing statistics 2013*. Retrieved April 23, 2013, from http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/

Botta, A., Pescapé, A., & Karrer, R. (2009). Wireless Networks Test-beds: When Heterogeneity Plays with Us. In E. Hossain (Ed.), *Heterogeneous Wireless Access Networks* (pp. 1-17). US: Springer.

Braley, R. C., Gifford, I. C., & Heile, R. F. (2000). Wireless personal area networks: an overview of the IEEE P802.15 working group. *SIGMOBILE Mob. Comput. Commun. Rev., 4*(1), 26-33.

Brown, T. A. (2006). *Confirmatory factor analysis for applied research*. NY: Guilford Press.

Bu Sung, L., Shixing, Y., Ding, M., & Guopeng, Z. (2011). Aggregating IaaS Service. Proceedings of the 2011 Annual Conference of the SRII Global Conference (SRII). (pp. 335-338). San Jose: IEEE.

Callaway, E., Gorday, P., Hester, L., Gutierrez, J. A., Naeve, M., Heile, B., & Bahl, V. (2002). Home networking with IEEE 802.15.4: a developing standard for low-rate wireless personal area networks. *Communications Magazine, IEEE, 40*(8), 70-77.

Calvet, J. C. L., & Noll, J. (2010). *Subscriber Identity Module*: EP Patent 1,733,581.

Carrier, B., & Spafford, E. H. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence, 2*(2), 1-20.

Casey, E. (2011). Foundations of digital forensic, *Digital evidence and computer crime: Forensic science, computers, and the internet* (3rd ed.). (pp. 1-34). MA: Academic.

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

Casey, E., & Turnbull, B. (2011). Digital evidence on mobile devices. *Eoghan Casey, Digital Evidence and Computer Crime. Third Edition. Forensic Science, Computers, and the Internet, Academic Pres*.

Chadha, S. (2012). *Nano-SIM cards vs Micro SIM cards- All you need to know*. Retrieved April 29, 2013, from http://www.gadgec.com/nano-sim-cards-vs-micro-sim-cards/

Cheema, A., Iqbal, M., & Ali, W. (2014). An Open Source Toolkit for iOS Filesystem Forensics. In G. Peterson & S. Shenoi (Eds.), *Advances in Digital Forensics X* (Vol. 433, pp. 227-235). Heidelberg: Springer.

Chen, J., Pang, A.-C., Sheu, S.-T., & Tseng, H.-W. (2005). High Performance Wireless Switch Protocol for IEEE 802.11 Wireless Networks. *Mobile Networks and Applications, 10*(5), 741-751.

Chen, M., Gonzalez, S., Vasilakos, A., Cao, H., & Leung, V. M. (2011). Body Area Networks: A Survey. *Mobile Networks and Applications, 16*(2), 171-193.

Cinque, M., Cotroneo, D., Kalbarczyk, Z., & Iyer, R. K. (2007). How Do Mobile Phones Fail? A Failure Data Analysis of Symbian OS Smart Phones. *Proceedings of the DSN '07. 37th Annual IEEE/IFIP International Conference Dependable Systems and Networks, 2007* (pp. 585 - 594). Edinburgh: IEEE.

Cloud Security Alliance (2013). *White paper analysing cloud vulnerability incidents from 2008-2012 released by the CSA Cloud Vulnerabilities Working Group*. Retrieved June 5, 2013, from https://cloudsecurityalliance.org/csa-news/white-paper-cloud-vulnerability-released/

CSA. (2013). Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing. *CLOUD SECURITY ALLIANCE: Incident Management and Forensics Working Group, 1*(1), 1-31.

Cusack, B., & Lutui, R. (2013). Including Network Routers In Forensic Investigation. *Proceedings of the 11th Australian Digital Forensics Conference* (pp. 59-70). WA: ECU.

Dailey, M. (2012). Digital forensic tools. ***SC** Magazine, 23*(5), 50-51.

Dalkey, N., & Helmer, O. (1963). An Experimental Application of the Delphi Method to the use of Experts. *Management Science, 9*(3), 458-458.

Da-Yu, K., Shiuh-Jeng, W., Sharma, A., & Huang, F. F.-Y. (2009). A Case-Oriented Model of Digital Forensics on Infected Zombie Computers. *Proceedings of the 2nd International Conference on Computer Science and its Applications, 2009*. CSA '09. (pp. 1-6). Korea (South): IEEE.

Delphi Technique. (2003). In *Capstone Encyclopaedia of Business.* Retrieved April 15, 2013, from http://ezproxy.aut.ac.nz/login?qurl=http%3A%2F%2Fwww.credoreference.com/entry/capstonebus/delphi_technique

De Marco, L., Kechadi, M. T., & Ferrucci, F. (2014). Cloud Forensic Readiness: Foundations. In P. Gladyshev, A. Marrington, & I. Baggili (Eds.), *Digital Forensics and Cyber Crime* (Vol. 132, pp. 237-244). Moscow: Springer.

De Montford University. (1999). How to undertake a literature search and review - for dissertation and final year proects. *DMU Libraries & Learning Services. Publication No. 23041, 8*(13), 1-8.

Derr, K. W. (2007). Nightmares with Mobile Devices are Just around the Corner! *Proceedings of the IEEE International Conference on Portable Information Devices, 2007.* (pp. 1-5). FL: IEEE.

Deyan, C., & Hong, Z. (2012). Data Security and Privacy Protection Issues in Cloud Computing. *Proceedings of the 2012 International Conference on*

Computer Science and Electronics Engineering (ICCSEE) (pp. 647-651). Hangzhou: IEEE.

Dezfouli, F. N., Dehghantanha, A., Mahmoud, R., Sani, N. F. B. M., & bin Shamsuddin, S. (2012). Volatile memory acquisition using backup for forensic investigation. *Proceedings of the 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)* (pp. 186-189). Kuala Lumpur: IEEE.

Donghyuk, Y., Jae-Yoon, L., Seunghwan, Y., Sun-Hee, L., Okyeon, Y., & Jongin, L. (2008). The Evidence Collection of DoS Attack in WLAN by Using WLAN Forensic Profiling System. *Proceedings of the ICISS. International Conference on Information Science and Security, 2008* (pp. 197-204). Seoul: IEEE.

Donohoe, H., Stellefson, M., & Tennant, B. (2012). Advantages and Limitations of the e-Delphi Technique: Implications for Health Education Researchers. *American Journal of Health Education, 43*(1), 38-46.

Dresch, A., Lacerda, D., & Antunes, J., Jr. (2015). Design Science Research. In *Design Science Research* (pp. 67-102). Switzerland: Springer.

Elyas, M., Ahmad, A., Maynard, S. B., & Lonie, A. (2015). Digital forensic readiness: Expert perspectives on a theoretical framework. *Computers & Security, 52*(0), 70-89.

Engadget Mobile. (2012). Samsung Galaxy S Blaze 4G making its way into T-Mobile stores in March for $150 (pp. 1-2). Chatham: Newstex.

Enticknap, N. (2003). Companies are looking up to wireless Wan. *Computer Weekly*, 44-44.

Ergen, M. (2009). Ultra Mobile Broadband of 3GPP2. In *Mobile Broadband* (pp. 417-446). CA: Springer.

Eul, H. (2010). Wireless communication - successful differentiation on standard technology by innovation. *Proceedings of the 2010 Design, Automation & Test in Europe Conference & Exhibition (DATE)* (pp. 2). Dresden: IEEE.

Fang, J., Jiang, Z., Chow, K.-P., Yiu, S.-M., Hui, L., Zhou, G., He, M., Tang, Y. (2012). Forensic Analysis of Pirated Chinese Shanzhai Mobile Phones. In G. Peterson & S. Shenoi (Eds.), *Advances in Digital Forensics VIII* (Vol. 383, pp. 129-142). Heidelberg: Springer.

Foltin, C. (2012). Going Mobile. (cover story). *Strategic Finance, 93*(9), 29-36.

Furht, B. (2010). Cloud Computing Fundamentals. In B. Furht & A. Escalante (Eds.), *Handbook of Cloud Computing* (pp. 3-19). FL: Springer.

Franklin, K., & Hart, J. (2007). Idea Generation and Exploration: Benefits and Limitations of the Policy Delphi Research Method. *Innovative Higher Education, 31*(4), 237-246.

Freiling, F. C., & Schwittay, B. (2007). A Common Process Model for Incident Response and Computer Forensics. *IMF, 7*, 19-40.

Garg, V. (2010). Wireless Communications & Networking: an introduction. CA: Elsevier.

Gartner. (2013). *Gartner Says Worldwide PC, Tablet and Mobile Phone Combined Shipments to Reach 2.4 Billion Units in 2013*. Retrieved April 23, 2013, from http://www.gartner.com/newsroom/id/2408515

Gizmodo. (2012). *Apple's New A6 Chip Is Smaller, Lighter, and Mightier A6,* Chatham: Newstex.

Glisson, W. B., Storer, T., & Buchanan-Wollaston, J. (2013). An empirical comparison of data recovered from mobile forensic toolkits. *Digital Investigation, 10*(1), 44-55.

Gomez-Miralles, L., & Arnedo-Moreno, J. (2011). Universal, Fast Method for iPad Forensics Imaging via USB Adapter. *Proceeding of the 2011 Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS).* (pp. 200 - 207). Seoul: IEEE.

Goodman, C. M. (1987). The Delphi technique: a critique. *Journal of Advanced Nursing, 12*(6), 729-734.

Gorunescu, F. (2011). Exploratory Data Analysis. In *Data Mining* (Vol. 12, pp. 57-157). Heidelberg: Springer.

Graubner, P., Schmidt, M., & Freisleben, B. (2011). Energy-Efficient Management of Virtual Machines in Eucalyptus. *Proceedings of the 2011 IEEE International Conference on Cloud Computing (CLOUD).* (pp. 243 - 250). Washington: IEEE.

Gregor, S. (2006). The Nature of Theory in Information Systems. *MIS Quarterly, 30*(3), 611-642.

Grispos, G., Glisson, W. B., & Storer, T. (2013). Using Smartphones as a Proxy for Forensic Evidence Contained in Cloud Storage Services. *Proceedings* *of the 2013 46th Hawaii International Conference on System Sciences (HICSS)* (pp. 4910-4919). HI: IEEE.

Grispos, G., Storer, T., & Glisson, W. B. (2011). A comparison of forensic evidence recovery techniques for a windows mobile smart phone. *Digital Investigation, 8*(1), 23-36.

Gronli, T.-M., Hansen, J., & Ghinea, G. (2010) Android vs Windows Mobile vs Java ME: a comparative study of mobile development environments. *Proceedings of the 3rd International Conference on P Ervasive Technologies Related to Assistive Environments, Samos, Greece.* (pp. 635 - 641). Victoria: IEEE.

Gunasekera, S. (2012). Android Architecture. In *Android Apps Security* (pp. 1-12). NY:Apress.

Gutierrez, A., Dreslinski, R. G., Wenisch, T. F., Mudge, T., Saidi, A., Emmons, C., & Paver, N. (2011). Full-system analysis and characterization of interactive smartphone applications. *Proceedings of the 2011 IEEE International Symposium on Workload Characterisation (IISWC).* (pp. 81-90). TX: IEEE.

Hankins, R., Uehara, T., & Jigang, L. (2009). A Comparative Study of Forensic Science and Computer Forensics. *Proceedings of the Third IEEE International Conference on Secure Software Integration and Reliability Improvement, 2009. SSIRI 2009* (pp. 230-239). Shanghai: IEEE.

Hansen, H. (2012). *Big wire globe FC clip art*. Retrieved July 21,, 2015, from http://www.clker.com/clipart-big-wire-globe-fc.html

Hartt, B. (2012). Apple iPhone 5. *Buckle down for the iPhone 5 teardown: the biggest thing to happen to teardowns since teardowns., 21*(1), 1-10.

Havard, L. (2007). How to conduct an effective and valid literature search. *Nursing times, 103*(45), 32-33.

Hasteer, N., Bansal, A., & Murthy, B. K. (2013). Pragmatic assessment of research intensive areas in cloud: a systematic review. *SIGSOFT Softw. Eng. Notes, 38*(3).

Hayes, B. (2008). Cloud computing. *Commun. ACM, 51*(7), 9-11.

HBR. (2013). How People Really Use Mobile. *Harvard Business Review, 91*(1), 30-31.

Hevner, A., & Chatterjee, S. (2010). Introduction to design science research. In *Design Research in Information Systems* (pp. 1-8). NY: Springer.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly, 28*(1), 75-105.

Holt, A., & Huang, C.-Y. (2010). Introduction. In *802.11 Wireless Networks* (pp. 1-13). London: Springer.

Hoog, A., & Strzempka, K. (2011). *iPhone and iPad data security*. iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices (pp. 79-105). Burlington: Elsevier.

Hoog, A. (2011). *Android Forensics: Investigation, Analysis and Mobile Security for Google Android*. Retrieved September 4, 2013, from http://AUT.eblib.com.au/patron/FullRecord.aspx?p=776188

Hou, R., Jin Zhi, G., & Wang Bao, L. (2012). Security mechanism analysis of open-source: Andriod OS & Symbian OS. *Proceedings of the 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet*). (pp. 3497-3501). Yichang: IEEE.

Howitt, I., & Gutierrez, J. A. (2003). IEEE 802.15.4 low rate - wireless personal area network coexistence issues. *Proceedings of the WCNC 2003 IEEE Conference on the Wireless Communications and Networking.* (pp. 1481 - 1486 vol.3). New Orleans: IEEE.

IDC. (2015). *Smartphone OS Market Share, 2015 Q2*. Retrieved November 12, 2015, from http://www.idc.com/getdoc.jsp?containerId=prUS23946013#.UR1AM1pASJV

Itani, W., Kayssi, A., & Chehab, A. (2009). Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures. *Proceedings of the Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing*. (pp. 711-716). Chengdu: IEEE.

Jaeger, R. G., & Halliday, T. R. (1998). On confirmatory versus exploratory research. *Herpetologists' League, 54*(1), 64-66.

Jankun-Kelly, T. J., Kwan-Liu, M., & Gertz, M. (2007). A Model and Framework for Visualization Exploration. *Visualization and Computer Graphics, IEEE Transactions on, 13*(2), 357-369.

Jansen, W., & Ayers, R. (2006). Forensic software tools for cell phone subscriber identity modules. *Proceedings of the International Conference on Digital Forensics, Security, and Law (ADFSL)* (pp. 101-113). Pennsylvania: CiteSeer.

Jansen, W., & Ayers, R. (2007). Guidelines on cell phone forensics. *NIST Special Publication, 800*, 101.

Jansen, W., & Scarfone, K. (2008). Guidelines on Cell Phone and PDA Security (Draft). *NIST Special Publication, 800*, 124.

Jain, R. (2006). *Wireless personal area networks (WPANs).* Retrieved May 21, 2013, from http://www.cse.wustl.edu/~jain/cse574-06/ftp/j_4pan/index.htm

Jha, U. (2002). Wireless Landscape – Need for Seamless Connectivity. *Wireless Personal Communications, 22*(2), 275-283.

Johannesson, P., & Perjons, E. (2014). A Method Framework for Design Science Research. In *An Introduction to Design Science* (pp. 75-89). Switzerland: Springer.

Johansson, P., Kazantzidis, M., Kapoor, R., & Gerla, M. (2001). Bluetooth: an enabler for personal area networking. *Network, IEEE, 15*(5), 28-37.

Juanru, L., Dawu, G., & Yuhao, L. (2012). Android Malware Forensics: Reconstruction of Malicious Events. *(ICDCSW), Proceedings of the 32nd International Conference on distributed computing systems* (pp. 552-558). Macau: IEEE.

Jung, W., Kang, C., Yoon, C., Kim, D., & Cha, H. (2012) DevScope: a nonintrusive and online power analysis tool for smartphone hardware components. *Proceedings of the eighth IEEE/ACM/IFIP international conference on Hardware/software codesign and system synthesis,* (pp. 353-362). Tampere Finland: IEEE.

Junjie, P., Xuejun, Z., Zhou, L., Bofeng, Z., Wu, Z., & Qing, L. (2009). Comparison of Several Cloud Computing Platforms. *Proceedings of the 2009 Second International Conference of the Information Science and Engineering (ISISE),* (pp. 23-27). Shanghai: IEEE.

Junseok, P., Hyokyung, B., & Kern, K. (2009). Buffer Cache Management for Combined MLC and SLC Flash Memories Using both Volatile and Nonvolatile RAMs. *Proceedings of the 2009. RTCSA '09 15th IEEE*

International Conference on Embedded and Real-Time Computing Systems and Applications. (pp. 228 - 235). Beijing: IEEE.

Kabir, M. (2009). *GSM network architecture*. Paper presented at the Cellular Mobile Systems and Services (TCOM1010). Retrieved April 26, 2013, from, http://www6.conestogac.on.ca/~mkabir/TCOM1010_ConEd_Cellular/Day-02_GSM%20Network%20Architecture.pdf

Keckler, S. W., Dally, W. J., Khailany, B., Garland, M., & Glasco, D. (2011). GPUs and the Future of Parallel Computing. *Micro, IEEE, 31*(5), 7-17.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to Integrating Forensic Techniques into Incident Response. *NIST Special Publication 800-86,* 121.

Kevan, T. (2004). Wireless Wide-Area Networks Pick Up the Pace. *Frontline Solutions, 5*(11), 20-25.

Kim, D., Lee, S., Chung, J., Kim, D. H., Woo, D. H., Yoo, S., & Lee, S. (2012a). Hybrid DRAM/PRAM-based main memory for single-chip CPU/GPU. *Proceedings of the 49th Annual Design Automation Conference* (pp. 888 - 896). San Francisco: IEEE.

Kim, D., Park, J., Lee, Keun-gi Lee., & Lee, S. (2012b). Forensic Analysis of Android Phone Using Ext4 File System Journal Log. In J. J. Park, V. C. M. Leung, C.-L. Wang, & T. Shon (Eds.), *Future Information Technology, Application, and Service* (Vol. 164, pp. 435-446). Springer Netherlands.

Klaver, C. (2010). Windows Mobile advanced forensics. *Digital Investigation, 6*(3–4), 147-167.

Kok Seng, T., Gee Keng, E., Chee Kyun, N., Noordin, N. K., & Ali, B. M. (2011). The performance evaluation of IEEE 802.11 against IEEE 802.15.4 with low transmission power. *Proceedings of the 2011 17th Asia-Pacific Conference on the Communications (APCC).* (pp. 850 - 855). Sabah: IEEE.

Kolios, P., Friderikos, V., & Papadaki, K. (2011). Future Wireless Mobile Networks. *Vehicular Technology Magazine, IEEE, 6*(1), 24-30.

Kotsch, T. J. (1996). Wireless LAN over microwave. *Proceedings of the Northcon/96.* (pp. 125 - 133). Seattle: IEEE.

Kotsopoulos, P. A., & Stamatiou, Y. C. (2012). Uncovering Mobile Phone Users' Malicious Activities Using Open Source Tools. *Proceedings of the 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)* (927-933). Istanbul: IEEE.

Kubi, A. K., Saleem, S., & Popov, O. (2011). Evaluation of some tools for extracting e-evidence from mobile devices. *Proceedings of the 2011 5th International Conference on Application of Information and Communication Technologies (AICT)* (pp.1-6). Baku: IEEE.

Kumar, R. (1998). *Research methodology: A step-by-step guide for beginners*. Melbourne: Addison Wesley Longman.

Kumar, A., Byung Gook, L., HoonJae, L., & Kumari, A. (2012). Secure storage and access of data in cloud computing. *Proceedings of the 2012 International Conference on ICT Convergence (ICTC)* (pp. 336-339). Jeju Island: IEEE.

Lagerspetz, E., & Tarkoma, S. (2010). Cloud-assisted mobile desktop search. *Proceedings of the 2010 8th IEEE International Conference on Pervasive Computing and Communication Workshops (PERCOM Workshops)* (pp. 826-828). Mannheim: IEEE.

Lagerspetz, E., & Tarkoma, S. (2011). Mobile search and the cloud: The benefits of offloading. *Proceedings of the 2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops).* (pp. 117-122). Seattle: IEEE.

Lammle, T. (2010). *CCNA Wireless Study Guide: IUWNE Exam 640-721* Indianapolis: Wiley.

Latré, B., Braem, B., Moerman, I., Blondia, C., & Demeester, P. (2011). A survey on wireless body area networks. *Wireless Networks, 17*(1), 1-18.

Lee, M. J., Jianliang, Z., Young-Bae, K., & Shrestha, D. M. (2006). Emerging standards for wireless mesh technology. *Wireless Communications, IEEE, 13*(2), 56-63.

Leavitt, N. (2011). Mobile Security: Finally a Serious Problem? *Computer, 44*(6), 11-14.

Lee, H., & Chuvyrov, E. (2012). Security. In *Beginning Windows Phone App Development* (pp. 479-512). NY: Apress.

Lin, R., Dor-Shifer, D., Rosenberg, S., Kraus, S., & Sarne, D. (2006). Towards the fourth generation of cellular networks: improving performance using distributed negotiation. *Proceedings of the 9th ACM international symposium on Modeling analysis and simulation of wireless and mobile systems* (pp. 347-356). Terromolinos: ACM.

Lin, I. L., Han-Chieh, C., & Shih-Hao, P. (2011). Research of Digital Evidence Forensics Standard Operating Procedure with Comparison and Analysis Based on Smart Phone. *Proceedings of the 2011 International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA)* (pp.386-391). Barcelona: IEEE.

Liu, H., Azadegan, S., Yu, W., Acharya, S., & Sistani, A. (2012). Are We Relying Too Much on Forensics Tools? In R. Lee (Ed.), *Software Engineering Research, Management and Applications 2011* (Vol. 377, pp. 145-156). Heidelberg: Springer.

Lu, J., Sundaram, A., Meng, Z., A, P., Lu, G., & Stav, J. B. (2012). Mobile Exam System – MES: Architecture for Database Management System. In *Learning with Mobile Technologies, Handheld Devices, and Smart Phones: Innovative Methods* (pp. 1-20). Hershey: IGI Global.

Mahajan, A., Dahiya, M. S., & Sanghvi, H. P. (2013). Forensic Analysis of Instant Messenger Applications on Android Devices. *International Journal of Computer Applications (0975 – 8887), 68*(8), 38-44.

Malhotra, N. K. (2007). *Exploratory, descriptive and causal research designs*. Retrieved September 4, 2013, from http://www.monroecollege.edu/AcademicResources/ebooks/9781111532406_lores_p01_ch03.pdf

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision support systems*, *15*(4), 251-266.

March, S. T., & Storey, V. C. (2008). Design science in the information systems discipline: an introduction to the special issue on design science research. *Management Information Systems Quarterly*, *32*(4), 6.

Marshall, P., Keahey, K., & Freeman, T. (2010). Elastic Site: Using Clouds to Elastically Extend Site Resources. *Proceedings of the 2010 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing (CCGrid).* (pp. 43-52). Melbourne: IEEE.

Martini, B., & Choo, K.-K. R. (2012). An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation, 9*(2), 71-80.

Martino, J. P. (1976). The Delphi method: Techniques and applications: Linstone, Harold A., and Murray Turoff, Addison-Wesley. *Technological Forecasting and Social Change, 8*(4), 441-442.

Mazzini, F. F., Mateus, G. R., & Smith, J. M. (2003). Lagrangean based methods for solving large-scale cellular network design problems. *Wirel. Netw., 9*(6), 659-672.

McDermott-Wells, P. (2004). What is Bluetooth? *Potentials, IEEE, 23*(5), 33-35.

McKemmish, R. (1999). *What is forensic computing?* Canberra: Australian Institute of Criminology.

Mehbodniya, A., Kaleem, F., Yen, K. K., & Adachi, F. (2013). A novel wireless network access selection scheme for heterogeneous multimedia traffic. *Proceedings of the 2013 IEEE Conference on the Consumer Communications and Networking Conference (CCNC).* (pp. 485 - 489). Las Vegas: IEEE.

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing (draft). *NIST Special Publication, 800*, 145.

Mellars, B. (2004). Forensic examination of mobile phones. *Digital Investigation, 1*(4), 266-272.

Menard, T., Miller, J., Nowak, M., & Norris, D. (2011). Comparing the GPS capabilities of the Samsung Galaxy S, Motorola Droid X, and the Apple iPhone for vehicle tracking using FreeSim_Mobile. *Proceedings of the 2011 14th International IEEE Conference on the Intelligent Transportation Systems (ITSC).* (pp. 985 - 990). DC: IEEE.

Merriam-Webster. (2011). *Methodology*. Retrieved April 5, 2014, from http://www.merriam-webster.com/dictionary/methodology?show=0&t=1300577597

Microsoft. (2007). *Microsoft white paper on the architectural overview of windows mobile infrastructure components* [White paper]. Retrieved June 23, 2013 from download.microsoft.com/.../Windows_Mobile_Architecture_Overview.pdf

Miller, T., & Monaghan, C. (2013). *App store tops 40 billion downloads with almost half in 2012*. Retrieved April 30, 2013, from http://www.apple.com/pr/library/2013/01/07App-Store-Tops-40-Billion-Downloads-with-Almost-Half-in-2012.html

Mislan, R. (2010). Cellphone crime solvers. *Spectrum, IEEE, 47*(7), 34-39.

Miyahara, Y. (2011). Next-generation wireless technologies trends for ultra low energy. *Proceedings of the 17th IEEE/ACM international symposium on Low-power electronics and design* (p. 345). Fukuoka: IEEE.

Mohtasebi, S., & Dehghantanha, A. (2013). Towards a Unified Forensic Investigation Framework of Smartphones. *International Journal of Computer Theory and Engineering, 5*(2), 351-355.

Molisch, A. F. (Ed.). (2010). *Wireless Communications* (2 ed.). Chicester: Wiley. Retrieved January 6, 2015, from http://AUT.eblib.com.au/patron/FullRecord.aspx?p=875742

Mollah, M. B., Islam, K. R., & Islam, S. S. (2012). Next generation of computing through cloud computing technology. *Proceedings of the 2012 25th IEEE Canadian Conference on Electrical & Computer Engineering (CCECE).* (pp. 1-6). Montreal: IEEE.

Moren, D. (2010). iOS 4. *Macworld, 27*(9), 46-49

Morrissey, S. (2010). iOS Operating and File System Analysis. In *iOS Forensic Analysis for iPhone, iPad, and iPod touch* (pp. 25-66). NY: Apress.

Mshvidobadze, T. (2012). Evolution mobile wireless communication and LTE networks. *Proceedings of the 2012 6th International Conference on the Application of Information and Communication Technologies (AICT)* (1-7). Tbilisi: IEEE.

Nair, V. (2008). Heterogeneous wireless communication devices- present and future. *Proceedings of the MICROWAVE 2008 International Conference on Recent Advances in Microwave Theory and Applications.* (pp. 8). Singapore: IEEE.

Nicopolitidis, P., Obaidat, M. S., Papadimitriou, G. I., & Pomportsis, A. S. (2003). Personal Area Networks (PANs). In *Wireless Networks* (pp. 299-325). NJ: John Wiley & Sons.

NIJ. (2001). Electronic Crime Scene Investigation: A Guide for First Responders. *National Institute of Justice, 4*(1), 1-81.

NIST. (2013a). *Test Results for Mobile Device Acquisition Tool: Device Seizure v5.0 build 4582.15907*. Retrieved January 17, 2014, from https://www.ncjrs.gov/pdffiles1/nij/241153.pdf

NIST. (2013b). Exploratory Data Analysis. In *NIST/SEMATECH e-Handbook of Statistical Methods*. Retrieved January 17, 2014, from http://www.itl.nist.gov/div898/handbook/index.htm

Nurmi, D., Wolski, R., Grzegorczyk, C., Obertelli, G., Soman, S., Youseff, L., & Zagorodnov, D. (2009). The Eucalyptus Open-Source Cloud-Computing System. *Proceedings of the 9th IEEE.ACM International Symposium on the Cluster Computing and the Grid* (pp. 124-131). Shanghai: IEEE.

Nworie, J. (2011). Using the Delphi Technique in Educational Technology Research. *TechTrends, 55*(5), 24-30.

Offermann, P., Levina, O., Schonherr, M., & Bub, U. (2009). Outline of a design science research process. *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology* (pp. 1-11). US: ACM.

Ogunsola, L. (2005). Information and Communication Technologies and the Effects of Globalization: Twenty-First Century “Digital Slavery” for Developing Countries--Myth or Reality. *Electronic Journal of Academic and Special Librarianship, 6*(1-2), 1-10.

Okoli, C., & Pawlowski, S. D. (2004a). The Delphi method as a research tool: an example, design considerations and applications. *Information & Management*, *42*(1), 15-29.

Okoli, C., & Pawlowski, S. D. (2004b). The Delphi method as a research tool: an example, design considerations and applications. *Information & Management*, *42*(1), 15-29.

Oliver, E. (2009). A survey of platforms for mobile networks research. *SIGMOBILE Mobile Computing and Communications Review, 12*(4), 56-63.

Owen, P., & Thomas, P. (2011). An analysis of digital forensic examinations: Mobile devices versus hard disk drives utilising ACPO & NIST guidelines. *Digital Investigation, 8*(2), 135-140.

Özyiğit, Ö., Ulusoy, G., Özlale, Ü., & Yaveroğlu, T. (2012). Information and Communication Technologies on the Road to 2023. *YASED Information and Communication Technologies Working Group, 1*(1), 1-168.

Palmer, G., & Corporation, M. (2001). *A Road Map for Digital Forensic Research*. Retrieved July 6, 2014, from http://isis.poly.edu/kulesh/forensics/docs/DFRWS_RM_Final.pdf

Pareek, D. (2006). *WiMAX: Taking Wireless to the MAX*. Retrieved July 7, 2014, from http://dx.doi.org/10.1201/9781420013436.ch1.

Pattron, D. D. (2009). *Research methodology*. Retrieved March 22, 2011, from http://www.authorstream.com/Presentation/drpattron68-138583-Research-Methodology-CONTENTS-Constitutes-Topic-Select-Limitations-method-Entertainment-ppt-powerpoint/

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems, 24*(3), 45-77.

Peisert, S., Bishop, M., & Marzullo, K. (2008). Computer forensics in forensis. *SIGOPS Oper. Syst. Rev., 42*(3), 112-122.

Pelton, J. (2012). The Future of Communications Satellites. In *Satellite Communications* (pp. 95-104). NY: Springer.

Peng-Ting, C., Hsin-Pei, H., Cheng, J. Z., & Yu-Sheng, L. (2009). Broadband mobile advertisement: What are the right ingredient and attributes for mobile subscribers. *Proceedings of the Portland International Conference on Management of Engineering & Technology.* (pp. 625-632). Portland: IEEE.

Perrucci, G. P., Fitzek, F. H. P., & Widmer, J. (2011). Survey on Energy Consumption Entities on the Smartphone Platform. *Proceedings of the 2011 IEEE 73rd Vehicular Technology Conference (VTC Spring)* (pp. 1-8). Yokohama: IEEE.

Perumal, S. (2009). Digital forensic model based on Malaysian investigation process. *International Journal of Computer Science and Network Security, 9*(8), 38-44.

Pilli, E. S., Joshi, R. C., & Niyogi, R. (2010). Network forensic frameworks: Survey and research challenges. *Digital Investigation*, *7*(1–2), 14-27.

Pocatilu, P. (2011). Android Applications Security. *Informatica Economica, 15*(3), 163-171.

Pokharel, M., YoungHyun, Y., & Jong Sou, P. (2009). Cloud Computing in System Architecture. *Proceedings of the CNMT 2009 International*

Conference of the Computer Network and Multimedia Technology. (pp. 1-5). Wuhan: IEEE.

Pollitt, M. (1995). Computer forensics: An approach to evidence in cyberspace. *Proceedings of the National Information Systems Security Conference* (Vol. 2, pp. 487-491). Washington: Citeseer.

Potter, R. (1999). Squeezing the cellular network. *Telecommunications, 33*(2), 63-66.

Puder, A., & Antebi, O. (2013). Cross-Compiling Android Applications to iOS and Windows Phone 7. *Mobile Networks and Applications, 18*(1), 3-21.

Punja, S. G., & Mislan, R. P. (2008). Mobile device analysis. *Small Scale Digital Device Forensics Journal, 2*(1), 1-16.

Raghav, S., & Saxena, A. K. (2009). Mobile forensics: Guidelines and challenges in data preservation and acquisition. *Proceedings of the 2009 IEEE Student Conference on Research and Development (SCOReD)* (pp. 5-8). Serdang: IEEE.

Rajan, D. (2011). Introduction to Wireless Communications. In J. Kennington, E. Olinick & D. Rajan (Eds.), *Wireless Network Design* (Vol. 158, pp. 9-46): NY: Springer.

Rehault, F. (2010). Windows mobile advanced forensics: An alternative to existing tools. *Digital Investigation, 7*(1–2), 38-47.

Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence, 1*(3), 1-12.

Rizvi, S., Aziz, A., Saad, N. M., & Samir, B. B. (2010). A comparative analysis of integration schemes for UMTS and WLAN networks. *Proceedings of the 2010 IEEE Asia Pacific Conference on the Circuits and Systems (APCCAS).* (pp. 92 - 95). Kuala Lumpur: IEEE.

Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer Forensics Field Triage Process Model. *Journal of Digital Forensics, Security and Law, 1*(2), 19-38.

Rowlingson, R. (2004). A ten step process for forensic readiness. *International Journal of Digital Evidence, 2*(3), 1-28.

Ruan, K., Carthy, J., Kechadi, T., & Baggili, I. (2013). Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results. *Digital Investigation, 10*(1), 34-43.

Sabat, H. K. (2002). The evolving mobile wireless value chain and market structure. *Telecommunications Policy, 26*(9–10), 505-535.

Said, H., Yousif, A., & Humaid, H. (2011). IPhone forensics techniques and crime investigation. *Proceedings of the 2011 International Conference and Workshop on Current Trends in Information Technology (CTIT).* (pp. 120-125). Dubai: IEEE.

Sakr, S., Liu, A., & Fayoumi, A. G. (2013). The family of mapreduce and large-scale data processing systems. *ACM Comput. Surv., 46*(1), 1-44.

Sangani, K. (2013). Space race. *Engineering & Technology, 8*(2), 82-83.

Sang-Rock, Y., Sung-Kyu, L., Ki-Seob, L., On-Sik, C., Nam-deog, K., Tae-Hong, K., & Yong-Wan, P. (2008). A study for grounding effect to improve performance of WWAN. *Proceedings of the EMC 2008 IEEE International Conference on the Electromagnetic Compatibility.* (pp. 125 - 133). Detroit: IEEE.

Sauter, M. (2010). From GSM to LTE: An Introduction to Mobile Networks and Mobile Broadband Retrieved from July 17, 2012, from http://AUT.eblib.com.au/patron/FullRecord.aspx?p=645005

Savoldi, A., Gubian, P., & Echizen, I. (2009). A Comparison between Windows Mobile and Symbian S60 Embedded Forensics. *Proceedings of the Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2009. IIH-MSP '09* (pp. 546-550). Kyoto: IEEE.

Sayrac, B., Riihijärvi, J., Mähönen, P., Jemaa, S. B., Moulines, E., & Grimoud, S. (2012). Improving coverage estimation for cellular networks with spatial bayesian prediction based on measurements. *Proceedings of the 2012 ACM SIGCOMM workshop on Cellular networks: operations, challenges, and future design* (pp. 43-48). NY: ACM.

Selamat, S. R., Yusof, R., & Sahib, S. (2008). Mapping process of digital forensic investigation framework. *International Journal of Computer Science and Network Security, 8*(10), 163-169.

Seltman, H. J. (2014). Exploratory Data Analysis: A first look at the data. In *Experimental design and analysis* (pp. 61-100).

Selvakumar, C., Rathanam, G. J., & Sumalatha, M. R. (2013). PDDS - Improving cloud data storage security using data partitioning technique. *Proceedings* *of the 2013 IEEE 3rd International on Advance Computing Conference (IACC).* (pp.7-11). Ghaziabad: IEEE.

Sharma, H., & Sabharwal, N. (2012). Investigating the implications of virtual forensics. *Proceedings of the 2012 International Conference on the Advances in Engineering, Science and Management (ICAESM)* (pp. 617-620). Tamil Nadu: IEEE.

Siep, T. M., Gifford, I. C., Braley, R. C., & Heile, R. F. (2000). Paving the way for personal area network standards: an overview of the IEEE P802.15 Working Group for Wireless Personal Area Networks. *Personal Communications, IEEE, 7*(1), 37-43.

Siewiorek, D. (2012). Generation smartphone. *Spectrum, IEEE, 49*(9), 54-58.

Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *The Communications of the Association for Information Systems, 13*(1), 63.

Sturniolo, E. (2001). Wireless wide area networks: Looking for the right solution. *SunServer, 15*(1), 12-12,19.

Sugiki, A., & Kato, K. (2011). An Extensible Cloud Platform Inspired by Operating Systems. *Proceedings of the 2011 Fourth IEEE International Conference on Utility and Cloud Computing (UCC).* (pp. 306 - 311). NSW: IEEE.

Talib, A. M., Atan, R., Abdullah, R., & Azrifah, M. (2011). CloudZone: Towards an integrity layer of cloud data storage based on multi agent system architecture. *Proceedings of the 2011 IEEE Conference on Open Systems (ICOS).* (pp. 127-132). Langkawi: IEEE.

Tamilarasi, S. (2013). Forensic Investigative Methodologies for Digital Crime. *International Journal of Computer Science & Applications (TIJCSA), 2*(03), 58-65.

Targeted News Service. (2012). DRAM Content Rises and Becomes More Uniform in Smartphones, *Targeted News Service*. Retrieved May 25, 2012, from http://ezproxy.aut.ac.nz/login?url=http://search.proquest.com/docview/108 ay 0611610?accountid=8440

Thakur, A., Gormish, M., & Erol, B. (2011). Mobile phones and information capture in the workplace. *Proceedings of the CHI '11 Extended Abstracts on Human Factors in Computing Systems* (pp. 1513-1518). BC: ACM.

Theoharidou, M., Mylonas, A., & Gritzalis, D. (2012). A Risk Assessment Method for Smartphones. In D. Gritzalis, S. Furnell & M. Theoharidou (Eds.), *Information Security and Privacy Research* (Vol. 376, pp. 443-456). Heidelberg: Springer.

Tilson, D., Sorensen, C., & Lyytinen, K. (2011). The Paradoxes of Change and Control in Digital Infrastructures: The Mobile Operating Systems Case. *Proceedings of the 2011 Tenth International Conference on Mobile Business (ICMB).* (pp. 26 - 35). Como: IEEE.

Tipper, D., Rezgui, A., Krishnamurthy, P., & Pacharintanakul, P. (2010). Dimming Cellular Networks. *Proceedings of the 2010 IEEE G;obal Telecommunications Conference.* (pp. 1-8). Miami: IEEE.

Tudzarov, A., & Janevski, T. (2011). Design for 5G Mobile Network Architecture. *International Journal of Communication Networks and Information Security, 3*(2), 112-123.

Ullah, S., Higgins, H., Braem, B., Latre, B., Blondia, C., Moerman, I., Saleem, S., Rahman, Z., Kwak, K. (2012). A Comprehensive Survey of Wireless Body Area Networks. *Journal of Medical Systems, 36*(3), 1065-1094.

Unwin, A. (2010). Exploratory Data Analysis. In P. P. B. McGaw (Ed.), *International Encyclopaedia of Education (Third Edition)* (pp. 156-161). Oxford: Elsevier.

Valjarevic, A., & Venter, H. S. (2012). Harmonised digital forensic investigation process model. *Proceedings of the 2012 Information Security for South Africa (ISSA).* (pp. 1-10). Johannesburg: IEEE.

Van der Linde, E., & Hancke, G. P. (2008). An Investigation of Bluetooth Mergence with Ultra Wideband. *Proceedings of the 2008 Third International Conference on the meeting of the Broadband Communications, Information Technology & Biomedical Applications* (pp. 451-457). Gauteng: IEEE.

Van Hal, T. J. (2013). Taming the Golden Goose: Private Companies, Consumer Geolocation Data, and the Need for a Class Action Regime for Privacy

Protection. *Vanderbilt Journal of Entertainment & Technology Law., 15*, 713-713.

Venable, J., Pries-Heje, J., & Baskerville, R. (2012). A Comprehensive Framework for Evaluation in Design Science Research. In K. Peffers, M. Rothenberger, & B. Kuechler (Eds.), *Design Science Research in Information Systems. Advances in Theory and Practice* (Vol. 7286, pp. 423-438). Berlin: Springer.

von Solms, S., Louwrens, C., Reekie, C., & Grobler, T. (2006). A Control Framework for Digital Forensics. In M. Olivier & S. Shenoi (Eds.), *Advances in Digital Forensics II* (Vol. 222, pp. 343-355). NY: Springer.

Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common Phases Of Computer Forensics Investigation Models. *International Journal of Computer Science & Information Technology, 3*(3), 17-31.

Walls, J. G., Widermeyer, G. R., & El Sawy, O. A. (2004). Assessing information system design theory in perspective: how useful was our 1992 initial rendition? *Journal of Information Technology Theory and Application (JITTA), 6*(2), 6.

Wang, Y., Streff, K., & Raman, S. (2012). Smartphone Security Challenges. *Computer*, *45*(12), 52-58.

Wei-Tek, T., Xin, S., & Balasooriya, J. (2010). Service-Oriented Cloud Computing Architecture. *Proceedings of the Seventh International Conference on Information Technology: New Generations (ITNG), 2010* (pp. 684 - 689). Las Vegas: IEEE.

Welte, H. (2010). Anatomy of contemporary GSM cellphone hardware. *Unpublished paper, c*, 1-15.

Wenbo, Z., Xiang, H., Ningjiang, C., Wei, W., & Hua, Z. (2012). PaaS-Oriented Performance Modeling for Cloud Computing. *Proceedings of the 2012 IEEE 36th Annual on Computer Software and Applications Conference (COMPSAC).* (pp. 395-404). Izmir: IEEE.

Wright, D. (2009). Wireless Technologies for Mobile Computing and Commerce *Mobile Computing: Concepts, Methodologies, Tools, and Applications* (pp. 1175-1182). Pennsylvania: IGI Global.

Yadav, S., Ahmad, K., & Shekhar, J. (2011). Analysis of Digital Forensic Tools and Investigation Process. In A. Mantri, S. Nandi, G. Kumar & S. Kumar

(Eds.), *High Performance Architecture and Grid Computing* (Vol. 169, pp. 435-441). Heidelberg: Springer.

Yates, I. I. (2010). Practical investigations of digital forensics tools for mobile devices. *Proceedings of the 2010 Information Security Curriculum Development Conference* (pp. 156-162). NY: ACM.

Yin, Z., & Leung, V. M. (2006). Third-Party Handshake Protocol for Efficient Peer Discovery and Route Optimization in IEEE 802.15.3 WPANs. *Mobile Networks and Applications, 11*(5), 681-695.

Yusoh, Z. I. M., & Maolin, T. (2012). Clustering composite SaaS components in Cloud computing using a Grouping Genetic Algorithm. *Proceedings of the 2012 IEEE Congress on Evolutionary Computation (CEC).* (pp. 1-8). Brisbane: IEEE.

Zheng, P., & Ni, L. M. (2006). Spotlight: the rise of the smart phone. *Distributed Systems Online, IEEE, 7*(3), 1-14.