UNIVERSITI PUTRA MALAYSIA

A GENERIC SMARTPHONE FORENSIC INVESTIGATION PROCESS MODEL

ANAHITA FARJAMFAR

FSKTM 2016 33

A GENERIC SMARTPHONE FORENSIC INVESTIGATION PROCESS MODEL

By

ANAHITA FARJAMFAR

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Doctor of Philosophy

December 2016

DEDICATION

This thesis is dedicated to my beloved husband and family. To my husband because his love, acceptance, patience and encouragement has accompanied us through the years of this project. I am truly thankful for having you in my life. A special feeling of gratitude to my loving parents, whose faithful prayers, support, love and words of encouragement carried and inspired me through ‘thick and thin’. The support from all of you kept me to work hard for the things that I aspire to achieve.

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

A GENERIC SMARTPHONE FORENSIC INVESTIGATION PROCESS MODEL

By

ANAHITA FARJAMFAR

December 2016

Chairman : Mohd Taufik Abdullah, PhD
Faculty : Computer Science and Information Technology

Smartphones are sources of digital evidence and repository for considerable amount of personal and work-related information about the phone users, their network of contacts and activities. Investigations involving various such devices have been identified as growing challenges to digital forensic researchers and practitioners. Similar to other areas of digital forensic practice, the process models developed for smartphones do not consider satisfying any scientific requirement of a digital investigation process models to make such models reliable and admissible in court. They have also been criticized for their tendency to focus on one particular type of devices and failure to embrace the level of practicality and generality needed to be applied in the investigation of all smartphones, independent of their platforms. In addition, the common challenge associated with these models is that they tried to encompass all aspects of digital forensic activities in a single-tier, high level process models. This makes such models too unwieldy, impractical and unlikely to be adopted.

This research proposes a new forensic process model for digital investigation of smartphones, called Generic Smartphone Forensic Investigation Process Model (GSFIPM), which addresses both the practical needs of practitioners and the expectations of legal domain for a reliable and structured process model to be followed. The proposed model is a multi-tier, objective-based, iterative process model that is generically applicable in investigation of any type of smartphones. GSFIPM is integrated with Encompassing Proceedings as principles that have a wider scope than a single process in the course of an investigation. The second tier of the GSFIPM focuses on the evidence collection and preservation process since this process is arguably the most critical process in the course of a digital investigation. Any doubt cast upon this process makes the output of other processes moot. A two-stage formal model called Formal Evidence Collection Model for Smartphones (FECMS) is designed, comprising of two UML Activity Diagrams, two Implementation Guidelines and the Overarching Principles.

This research employed the Design Science Research Process (DSRP) methodology on the basis that it is an ‘ideal approach’ in the problem domain of digital forensic and especially appropriate for creating a new process model. The effectiveness of the GSFIPM and FECMS to satisfy the intended requirements are independently evaluated by a group of digital forensic experts. Feedbacks from these experts are taken into account and amendments are applied as appropriately as possible. The feedbacks received from experts, regarding the GSFIPM, are generally positive in fulfilling the scientific requirements. GSFIPM is also believed to hold new features in the design, namely being multi-tier and iterative, and containing overarching principles and stratification in roles and responsibilities. The feedbacks are also optimist for FECMS, in terms of utility and usability. This research demonstrates how GSFIPM and FECMS can be practically applicable in smartphone investigations and beneficial to the digital forensic practitioners in various environments.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

MODEL GENERIK PROSES PENYIASATAN FORENSIK TELEFON PINTAR

Oleh

ANAHITA FARJAMFAR

Disember 2016

Pengerusi : Mohd Taufik Abdullah, PhD
Fakulti : Sains Komputer dan Teknologi Maklumat

Telefon pintar merupakan sumber bagi bukti digital dan repositori bagi sejumlah besar maklumat peribadi dan maklumat berkaitan kerja tentang pengguna telefon, rangkaian kenalan dan aktiviti mereka. Penyiasatan melibatkan pelbagai peranti sedemikian telah dikenal pasti sebagai cabaran yang sentiasa berkembang bagi penyelidik dan pengamal forensik digital. Sebagaimana amalan sesetengah bidang forensik digital, model proses forensik yang telah dibangunkan untuk telefon pintar tidak memenuhi keperluan saintifik model proses penyiasatan digital untuk menjadikan model tersebut boleh percaya dan boleh diterima di mahkamah. Model-model ini telah dikritik kerana kecenderungannya untuk tertumpu kepada satu jenis peranti dan ianya tidak meliputi tahap praktikal dan sifat umum yang diperlukan untuk membolehkannya digunakan dalam penyiasatan ke atas semua jenis telefon pintar tanpa bersandar kepada platfom masing-masing. Tambahan pula, cabaran biasa yang dikaitkan dengan model-model ini adalah mereka cuba untuk merangkumi semua aspek aktiviti forensik digital dalam satu model proses tingkat-tunggal bertahap tinggi. Ini menjadikan model itu sukar dikawal, tidak praktikal dan mungkin tidak diguna pakai.

Kajian ini mencadangkan satu model proses forensik baharu bagi penyiasatan digital telefon pintar, yang dipanggil Model Generik Proses Penyiasatan Forensik Telefon Pintar (GSFIPM), yang menumpukan kepada kedua-dua keperluan praktikal bagi pengamal forensik digital dan juga memenuhi keperluan dalam domain undang-undang yang mengharapkan model proses yang boleh dipercayai dan berstruktur untuk diikuti.

Model Generik Proses Penyiasatan Forensik Telefon Pintar (GSFIPM) ini dicadangkan untuk mengatasi kelemahan yang telah dinyatakan sebelum ini. Model yang dicadangkan ini adalah pelbagai-tingkat, berasaskan objektif dan model proses berlelar yang bersifat umum dan boleh digunakan dalam penyiasatan sebarang jenis telefon pintar. GSFIPM disepadukan dengan Prosedur Perangkuman sebagai prinsip yang mempunyai skop yang lebih luas berbanding proses tunggal dalam aliran sesuatu penyiasatan. Tingkat kedua GSFIPM memberi tumpuan kepada pengumpulan bukti dan proses pemuliharaan, memandangkan proses ini boleh dikatakan proses yang paling kritikal dalam proses penyiasatan digital. Sebarang keraguan di peringkat proses ini akan mengakibatkan hasil output bagi proses lain dipertikaikan. Satu model formal dua peringkat yang dipanggil Model Pengumpulan Bukti Formal Telefon Pintar (FECMS) telah direka bentuk, yang terdiri daripada dua Rajah Aktiviti UML, dua Garis Panduan Pelaksanaan dan Prinsip Perlengkungan.

Kajian ini mengguna pakai metodologi Proses Penyelidikan Sains Reka Bentuk (DSRP) atas dasar bahawa ia adalah satu pendekatan yang ideal dalam masalah domain digital forensik dan khususnya sesuai untuk mencipta satu model proses baharu. Keberkesanan GSFIPM dan FECMS bagi memenuhi keperluan yang dihasratkan telah dinilai secara bebas oleh sekumpulan pakar forensik digital. Maklum balas daripada pakar ini telah diambil kira dan pindaan telah dilaksanakan ke atas kedua-dua model sewajar yang mungkin. Maklum balas yang diterima daripada pakar mengenai GSFIPM, secara umumnya adalah positif dalam memenuhi keperluan saintifik. GSFIPM juga dipercayai mempunyai ciri-ciri baharu dalam rekabentuknya, seperti bersifat pelbagai-tingkat dan berlelar, dan mengandungi prinsip perlengkungan serta perlapisan dalam peranan dan tanggungjawab. Maklum balas juga optimis terhadap FECMS, dari segi utiliti dan kebolehgunaan. Kajian ini menunjukkan bagaimana GSFIPM dan FECMS boleh digunakan secara praktikal dalam penyiasatan telefon pintar dan memberi manfaat kepada pengamal forensik digital dalam pelbagai persekitaran.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank Allah for giving me strength and determination to finish this thesis. May his merciful and supportive grace be upon all and me forever.

I wish to express my sincere gratitude to my supervisor Dr. Mohd Taufik Abdullah and my committee members Prof. Ramlan Mahmod and Associate Prof. Dr. Nur Izura Udzir, for their insightful comments, valuable advice, and guidance throughout this research. I really appreciate the freedom they provided while I was working on my research and their openness to new ideas.

My special thanks go to my dearest friends who were always willing to help and share their ideas and knowledge even when they were busy with their own research. I will always treasure their friendship.

Most of all, I would like to express my delightful appreciation to my husband, my parents and family for their affectionate support, understanding, and encouragement. Their prayers and good wishes constantly helped me to be strong, especially in difficult times. I am forever grateful and indebted to them.

I certify that a Thesis Examination Committee has met on 20 December 2016 to conduct the final examination of Anahita Farjamfar on her thesis entitled "A Generic Smartphone Forensic Investigation Process Model" in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Doctor of Philosophy.

Members of the Thesis Examination Committee were as follows:

Nor Fazlida binti Mohd Sani, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Azizol bin Hj Abdullah, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Shukor Abd Razak, PhD
Associate Professor
Universiti Teknologi Malaysia
Malaysia
(External Examiner)

Nathan Luke Clarke, PhD
Professor
Plymouth Unversity
United Kingdom
(External Examiner)

NOR AINI AB. SHUKOR, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 28 February 2017

This thesis was submitted to the Senate of the Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

Mohd Taufik Abdullah, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Ramlan Mahmod, PhD
Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Nur Izura Udzir, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

ROBIAH BINTI YUNUS, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustration and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/ fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: ____________________ Date: ____________________

Name and Matric No.: Anahita Farjamfar, GS31872

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature: ______________________________
Name of
Chairman of
Supervisory
Committee: Dr. Mohd Taufik Abdullah

Signature: ______________________________
Name of
Member of
Supervisory
Committee: Professor Dr. Ramlan Mahmod

Signature: ______________________________
Name of
Member of
Supervisory
Committee: Associate Professor Dr. Nur Izura Udzir

TABLE OF CONTENTS

	Page
ABSTRACT	i
ABSTRAK	iii
ACKNOWLEDGEMENTS	v
APPROVAL	vi
DECLARATION	viii
LIST OF TABLES	xiii
LIST OF FIGURES	xiv
LIST OF ABBREVATIONS	xviii

CHAPTER

1	**INTRODUCTION**			
	1.1	Background		1
	1.2	Research Motivation		2
	1.3	Research Problems		4
	1.4	Research Objectives		6
	1.5	Research Scopes		6
	1.6	Research Contributions		7
	1.7	Thesis Organization		8
2	**LITRATURE REVIEW**			
	2.1	Digital Forensics		10
	2.2	Digital Evidence		11
	2.3	Standards and Guidelines for Smartphones Forensics		14
		2.3.1	Locard's Exchange Principle	14
		2.3.2	Principle of Electronic Evidence (ACPO)	15
		2.3.3	Principles Applying To The Recovery of Digital Evidence (IOCE)	15
		2.3.4	Guidelines for the Management of IT Evidence	16
		2.3.5	Electronic Crime Scene Investigation: A Guide for First Responders	16
		2.3.6	Best Practices for Seizing Electronic Evidence	16
		2.3.7	Handling Instructions for Mobile Phones	17
	2.4	Related Works		18
		2.4.1	Assessment Criteria for Previous Models	18
		2.4.2	Related Works on Conventional Computer-Based Digital Forensics Process Models	20
		2.4.3	Related Works on Smartphones Digital Forensics Process Mod	30
		2.4.4	Related works on Unified Modelling Language (UML)	40
	2.5	Summary		44
3	**RESEARCHMETHODOLOGY**			
	3.1	Design Science		45
	3.2	DSRP Activity 1-Problem Identification and Motivation		47
	3.3	DSRP Activity 2-Objectives of a Solution		47
	3.4	DSRP Activity 3-Design and Development		47

3.4.1 Identifying Criteria against which Previous Works 48
3.4.2 Identifying Requirements of the new Models 49
3.4.3 Identifying Roles and Responsibilities 49
3.4.4 Proposing the new Artefacts 49
3.5 DSRP Activity 4 and 5-Demonstration and Evaluation 49
3.6 DSRP Activity 6-Communication 53
3.7 Summary 53

4 MODEL DESIGN AND DEVELOPMENT
4.1 Model Requirements 54
4.2 Roles and Responsibilities 56
4.3 Generic Smartphone Forensic Investigation Process Model (GSFIPM) 57
4.3.1 Perimeter Establishing 59
4.3.2 Planning 59
4.3.3 Preparation 61
4.3.4 Collection and Preservation 62
4.3.5 Analysis 65
4.3.6 Reconstruction 66
4.3.7 Presentation 67
4.3.8 Case Closure 67
4.3.9 Encompassing Proceedings 68
4.4 Formal Evidence Collection Model for Smartphones (FECMS) 72
4.4.1 ECMS Principles 73
4.4.2 Assumption 73
4.4.3 The FECMS Representation 74
4.5 Summary 75

5 EVALUATION
5.1 valuation of Models through Survey 80
5.2 GSFIPM Evaluation 81
5.2.1 Feedbacks from Experts and the Researcher's Comments 81
5.2.2 Survey Discussion 82
5.3 FECMS Evaluation 83
5.3.1 Feedbacks from Experts and the Researcher's Comments (Utility and Usability) 83
5.3.2 Survey Discussion 87
5.3.3 FECMS Amendments in Response to the External Evaluation 88
5.3.4 Completed FECMS 94
5.3.5 Feedbacks from Experts (Comparison with ADAM) 95
5.4 Summary 96

6 CONCLUSIONS AND FUTURE WORK
6.1 Conclusion 97
6.2 Contributions of the Work 98
6.3 Future Work 99

REFERENCES 100
APPENDICES 104
BIODATA OF STUDENT 108
LIST OF PUBLICATIONS 109

LIST OF TABLES

Table		Page
2.1	The NIST Categorization of Smartphone Digital Evidence after (Lin et al., 2011)	13
2.2	Forensically Significant Data per OS after (Barmpatsalou et al., 2013)	13
2.3	Summary of Models Score based on Model Requirements Adapted from (Adams, 2012)	20
2.4	Summary of Previous Process Models Score based on Model Scientific Requirements	30
2.5	Summary of Smartphones Process Models Score	37
2.6	Summary of Weaknesses Identified in Previous Process Models	39
2.7	Summary of Previous Studies Applying Modelling Technique	43
4.1	A Harmonized Comparison of Previous Models with the Proposed Generic Model (GSFIPM)	55
5.1	Comparison between Features of GSFIPM with Previous Smartphone Models	83

LIST OF FIGURES

Figure		Page
1.1	Number of Smartphone Users Worldwide from 2014 to 2019 (in millions)	2
1.2	Surveyed Organization's Overall Security Posture (Ability to Defend Cyber Threats) on a scale of 1 to 5	3
2.1	A Three-Level Hierarchical Model for Developing Guidelines for Computer Forensic Evidence after (Noblett et al., 2000)	14
2.2	The Integrated Digital Investigation Process after (Carrier and Spafford,2004)	21
2.3	The Digital Crime Scene Investigation Phase after (Carrier and Spafford,2004)	21
2.4	Framework Structure Proposed by (Beebe and Clark, 2005)	22
2.5	Two-Dimensional Evidence Reliability Amplification Process Diagram after (Khatir et al., 2008)	24
2.6	Comprehensive Harmonized Digital Forensic Investigation process after (Valjarevic and Venter, 2015)	28
2.7	Phases of the Windows Mobile Device Forensic Model after (Ramabhadran, 2007)	32
2.8	Smartphone Forensic Investigation Process Model after (Goel et al., 2012)	35
2.9	Smart Technologies Digital Forensic Investigation Model after (Cusack and Lutui, 2014)	37
2.10	The Interaction Overview Diagram for the Computer Forensics Process after (Ruan and Huebner, 2009)	41
2.11	Activity Diagrams for Collection after (Ruan and Huebner, 2009)	41
3.1	Design Science Research Process adopted from (Peffers et al., 2006)	46
4.1	The Proposed Generic Smartphone Forensic Investigation Process Model (GSFIPM)	58
4.2	The FECMS Stage 1- On the Scene (version 1)	76
4.3	The FECMS Stage 2- In The Lab (version 1)	76
4.4	The FECMS Implementation Guideline for Collection of Physical Evidence (version1)	78
4.5	The FECMS Implementation Guideline for Collection of Digital Evidence (version1)	79
5.1	Percentages of Yes/No Answers of Participant Experts in Rating Each Individual Model Requirement	83
5.2	Percentages of Positive Answers of Participant Experts in Comparing the GSFIPM with previous Models	84
5.3	The FECMS Stage 1- On the Scene (version 2)	89
5.4	The FECMS Stage 2- In the Lab (version 2)	90
5.5	The FECMS Stage 2- In the Lab (version 3)	91
5.6	The FECMS Stage 2- In the Lab (version 4)	92
5.7	The FECMS Implementation Guideline for Collection of Physical Evidence (version2)	93
5.8	Comparison between FECMS with ADAMS in terms of Structure	94
5.9	Comparison between FECMS with ADAMS in terms of Completeness	95
5.10	Comparison between FECMS with ADAMS in terms of Easiness	95
A1	The FECMS Stage 1- On the Scene	104
A2	The FECMS Stage 2- In the Lab	105

A3 The FECMS Implementation Guideline for Collection of Physical Evidence 106
A4 The FECMS Implementation Guideline for Collection of Digital Evidence 107

LIST OF ABBREVATIONS

ACPO	Association of Chief Police Officer
ADAM	Advanced Data Acquisition Model
ASCII	American Standard Code for Information Interchange
BYOD	Bring Your Own Device
CHDFIP	Comprehensive Harmonized Digital Forensic Investigation Process
DFFFCHK	Digital Forensic Framework using Feedback and Case History Keeper
DFRWS	Digital Forensic Research Workshop
DSRP	Design Science Research Process
FECMS	Formal Evidence Collection Model for Smartphones
GSFIPM	Generic Smartphones Forensics Investigation Process Model
GSM	Global System for Mobile
HOFDIP	Hierarchical, Objectives-Based Framework for the Digital Investigations Process
ID	Identifier
IDIP	Integrated Digital Investigation Process
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IOCE	International Organization of Computer Evidence
IT	Information Technology
JTAG	Joint Test Action Group
NIJ	National Institute of Justice
NIST	National Institute of Standards and Technology
OS	Operating System
PC	Personal Computer
PCB	Printed Circuit Board
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PUK	Personal Unlocking Key
SD	Secure Digital
SFIPM	Smartphone Forensic Investigation Process Model
SIM	Subscriber Identity Module
SMS	Short Message Service
SSFPM	Symbian Smartphones Forensic Process Model
STDFIM	Smart Technologies Digital Forensic Investigation Model
SWGDE	Scientific Working Group on Digital Evidence
TCB	Trusted Computing Base
TDERAPM	Two-Dimensional Evidence Reliability Amplification Process Model
UML	Unified Modelling Language
USB	Universal Serial Bus
USSS	United States Secret Service
VOIP	Voice over IP
WMDFM	Windows Mobile Devices Forensics Model

CHAPTER 1

INTRODUCTION

This chapter presents the introduction and the overall structure of the thesis. The aim of this chapter is to define the main objectives of the research into the smartphone forensics and to describe the particular research problem and explain the value of a solution.

1.1 Background

A smartphone can be defined as a mobile phone which is equipped with an operating system. Smartphones typically include all of the features included in a normal mobile phone with those of another popular consumer device like personal digital assistants, media players, digital cameras and/or GPS navigation units. Later, smartphones were equipped with all of those plus the features of a touch screen computer (can come with QWERTY keypad also), including web browsing, Wi-Fi, 3rd-party applications, motion sensor, mobile payment, 3G/4G and so on. Mobile phones can be utilized by criminals as a tool for assistance in daily operations as well as for controlling the organized crimes. Practitioners of law have been attempting continually to act against criminals active in regard to the application of digital technologies. Nowadays, the increase in the utilization of smartphones resulted in considering these devices as sources of digital evidence. While the amount of data retained in such devices is to a great extent less in comparison to the amount of data that can be stored in computers, still this small volume of data can be greatly valuable in the process of revealing information about its user. Nevertheless, unfortunately, in the case of digital forensics practitioners as well as law enforcement agents there is still a huge gap in regard to handling the digital evidence obtained from smartphones. Digital forensic science was defined by The First Digital Forensic Research Workshop (DFRWS) 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 facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations,(Palmer, 2001, p. 16).

There are a number of challenges in the course of presenting the digital evidence to the involved courts. Such challenges are related to the evidence reliability which is in fact the requirement of the application of reliable principles and methods. Edmond (2010) believes that although the real and proper meaning of “demonstrable reliability” (or “sufficiently reliable”) is still a debatable issue, assessments of reliability must be concentrated on the techniques applied and the accuracy of them (in addition to the proficiency of the operator and/or the analyst) (Edmond, 2010). A number of digital forensic process models for smartphones have been developed worldwide with the purpose of defining the vital steps that should be followed to make sure that the investigation is being performed in a reliable way and forensically sound manner. (Forensically sound is a common term in the field of digital forensics when trying to qualify or justify the application of a specific technology or a relevant method. A great number of practitioners utilize this term in description of the capabilities of a piece of software or forensic analysis approach (McKemmish, 2008)). These process models are developed with the perspective to work well with one particular type of devices. Also despite the presence of basic principles relevant to the process of handling the digital evidence, different jurisdictional as well as technological nature of the involved cases encourages a different application of these principles by courts in different ways. Thus, the processes utilized by the digital forensic practitioners are always under meticulous scrutiny.

1.2 Research Motivation

Users of mobile phones are switching to smartphones in a high rate as these devices have become more affordable and equipped with 3G and 4G networks facilities. Data from eMarketer[1] show that over one-quarter of the world's total population have used smartphones in 2015. eMarketer's latest mobile user forecast estimates more than half, i.e. 51.7%, of all mobile phone users will use smartphones in 2018. It means that eventually, feature phones will have become the minority in the world of telecommunications. According to a forecast by Statista.com[2], number of smartphones users will surpass 2.2 billion in 2017, and the number is expected to increase over 2.6 billion by 2019. Figure 1.1 depicts the statistics anticipating the usage of smartphones from 2014 to 2019.

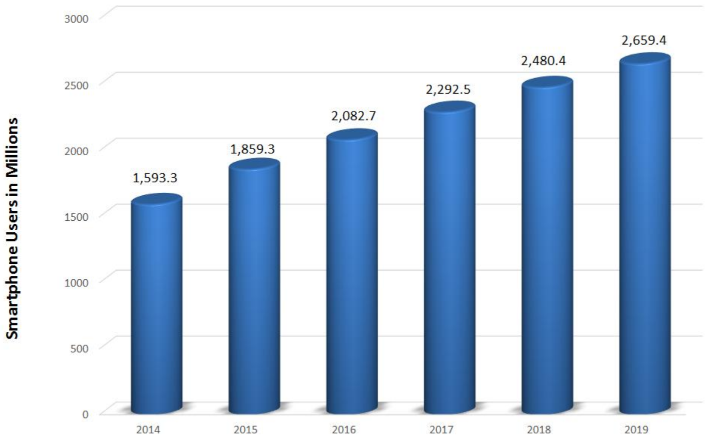

Figure 1.1: [2]Number of Smartphone Users Worldwide, 2014 to 2019 (in millions)

[1] http://www.emarketer.com/Article/2-Billion-Consumers-Worldwide-Smartphones-by-2016/1011694.

[2] http://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

Based on a survey of more than 800 IT security decision makers and practitioners across North America and Europe, the CyberEdge Group[3] report that 71% of surveyed organizations were victims of successful cyber-attacks in 2015. The report ("Cyberthreat Defense Report," 2015) highlights that "mobile devices (smartphones and tablets) are perceived as IT security's weakest link, closely followed by social media applications" (p. 5) as it is shown in Figure 1.2.

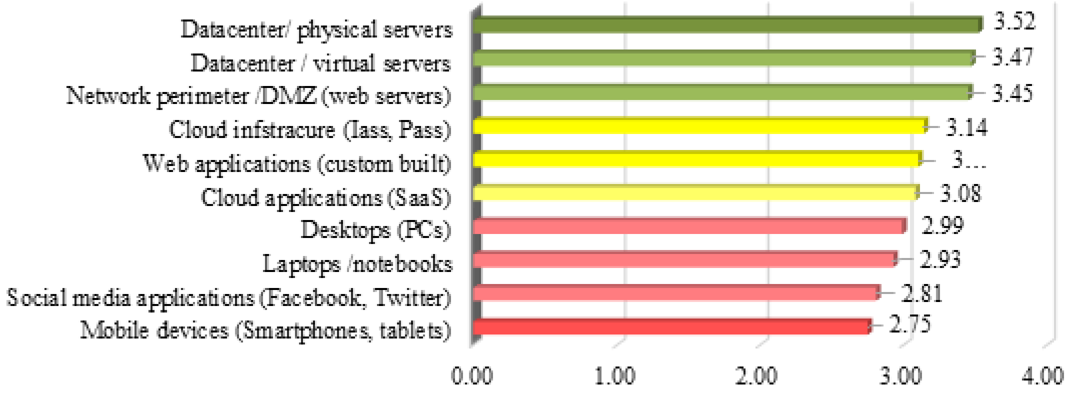

Figure 1.2: [3]Surveyed Organization's Overall Security Posture (Ability to Defend Cyber Threats) on a scale of 1 to 5

It is worth mentioning that the BYOD (Bring Your Own Device) policy trend in companies and firms only adds to the security and privacy problem for corporations. Security breaches and failed perimeter controls are followed immediately by digital forensics. In using a smartphone, surprisingly large amount of personal or corporate data is supplied and transmitted by the user. Digital evidence is defined by the SWGDE, Scientific Working Group on Digital Evidence as "information of probative value that is stored or transmitted in binary form" (*SWGDE and SWGIT Digital and Multimedia Evidence Glossary*, 2011, p. 6). Accordingly, any piece of useful information transferred or stored in digital mode is evidence irrespective of the devices or interfaces used to transfer or store it. Thus smartphones can be seen as a "promising site" for collecting such evidence (Goel, Tyagi, and Agarwal, 2012).

Electronic devices could be either as objects of crime, instruments used to commit a crime or repositories of evidence relevant to a crime, while smartphones can be involved in all these cases; they are anyhow repository for considerable amount of personal information about the phone user and their network of contacts. In this case, it is critical to obtain evidence reliably and in a forensically sound manner by applying a proven digital forensic method and following a trustworthy process model. The need for a proper guidance and reliable process model for digital forensic practitioners to be used in unfamiliar areas of technology, such as smartphones, is the motivation for this research.

[3] CyberEdge Group is an award-winning research, marketing, and publishing firm which serves the needs of information security service providers and vendors.

1.3 Research Problems

In Daubert, which is named after *Daubert v Merrell Dow Pharmaceuticals (U.S.)* (1993), court charged trial judges with the responsibility to scrutinise evidence in order to make sure that the requirements set by the Federal Rules of Evidence rule 702 are all met. In accordance to these rules, determination of the admissibility of an involved evidence depends on the fact that (1) expert testimony has been produced based on reliable methods and procedures; and (2) the fact that the expert has reliably utilized the principles and methods in dealing with the facts included and involved in the case at hand.

To comply with second condition, reliably application of the principles and methods, some researchers in the field of digital forensics realized the lack of reliable process models and admissible procedures for mobile phones and proposed forensic investigation process models specifically intended for smartphones. However, rather than being general, these models have often been intended for specific types of mobile phones such as Windows phones (Goel et al., 2012;Ramabhadran, 2007), Symbian smartphones (Yu, Jiang, Shu, Yin, and Liu, 2009) or Android smartphones (Simão, Sícoli, Melo, Deus, and Sousa Júnior, 2011).In addition, the common weakness associated with these models is that in designing the models they did not consider requirements of any scientific discipline. While scientific disciplines aid the courts in the assessment of the reliability of digital evidence produced using such models. Besides, previous models tried to encompass all aspects of digital forensic activities in a single-tier, high level process model that focus on the abstract level rather than the more details needed by various model users, models such as those proposed by(Lutui, 2016;Cusack and Lutui, 2014;Goel et al., 2012; Ramabhadran, 2007).As (Rogers, 2004) states, this feature has made such models too unwieldy and complicated and therefore make these models impractical and unlikely to be adopted.

Whereas some of the mentioned models include descriptions in a high level that in fact provide no applicable guidance,(Reith, Carr, and Gunsch, 2002)criticises other models for being involved with a focus on the details of the technology and without consideration for a generalized and technology independent process, models such as the one proposed by (Yu et al., 2009). A list of low-level prescriptive actions might entangle forensic practitioners in complex legal challenges since there is a possibility that they have to provide explanation for the reason why they hadn't followed every individual item from the list in which a lot of items may be inappropriate in specific situations. There are weaknesses in most of the previously developed models in terms of target audience on the basis that these models are overwhelmed by tasks that are mostly concerned with those working in physical crime investigation units, as well as in terms of stratification of roles and responsibilities.

Moreover, of particular concern regarding the evidence reliability and expert testimony is the manner in which digital evidence has been acquired. The general principle that courts implement for copies of documents offered as evidence is to consider the copy of the involved document as equivalent to the original version of the document. This principle is applied to the case of digital records too. Same as other kinds of evidence, the presented evidence of this type is not presumed as reliable by courts, unless some proof is provided that indicates the empirical testing in regard to the techniques, theories and procedures which are associated with the process of producing the presented copy (Mason, 2007). The matter of reliability entails that a court pays a great deal of attention to the manner in which digital evidence was obtained and especially the process of capturing and storing the data. As Rogers (2004)points out "If doubt is cast on the initial collection and management of evidence, output from the other phases is moot" (p.12), which indicates that the evidence collection process is arguably the most critical process in the course of digital investigation. However, few researchers or practitioners have focused on it while they were developing prior models. Consequently, it is extremely important to develop a comprehensive description for the process of evidence collection during smartphones investigation which formally describes the processes adopted to collect digital and physical evidence.

This research addresses the fundamental issue that practitioners operating in the field of digital forensic need to claim in the court that during an investigation involving smartphones a reliable process model and admissible procedure has been used. Specifically, this thesis addresses the following issues:

1. A number of efforts have developed digital forensics process models against the need of practitioners to follow a reliable procedure and admissible approach in dealing with smartphones. The major drawback of these models is that they do not consider satisfying any scientific requirement of a digital investigation process models. The requirements that make such models reliable and admissible. They have also been criticized for their representations in a single tier, linear approach which lack overarching principles and stratification of roles and responsibilities. Overwhelming the models with unrelated activities and the biased towards incident response has made them unwieldy and impractical.

2. Evidence collection as the most critical phases of the digital investigation process model may come under scrutiny. Thus, digital forensic practitioners may need a formal model of a process to describe the employed procedures in such a way that it can be understood by courts and juries or management team whose knowledge and understanding is different. Currently, there is no formal description of the processes adopted for the collection of physical and digital evidence in the investigation of smartphones. The current processes are described rather informal and intuitive that overlook understanding of those who need to act upon thus hinder corresponding audience to determine the reliability of the collection process employed to collect potential evidence from smartphones.

1.4 Research Objectives

The main objective of this research is to propose a generic smartphone forensic investigation process model which expands upon significant contributions of earlier models, increases practicality and applicability and meets scientific requirements. What this study intends to propose is a process model that is in line with the ACPO guidelines and contains appropriate instructions to help practitioners in successfully implementing the proposed model and properly and consistently applying digital forensic principles.

To achieve the goals of the research to bridge the gap faced by forensics investigators, the specific objectives are to:

1. Propose a generic multi-tier digital forensics investigation process model that meets the scientific requirements for a digital investigation process model and it is generic in that it can be applied in the investigation of all smartphones. Such process model should be iterative and includes overarching principles and stratification of roles and responsibilities in the design.

2. Propose a formal model of a process, to describe the evidence collection and preservation process in an investigation involving smartphones, in a way that it is cross-platform and capable of helping practitioners properly follow and formally describe the employed processes to various audience whose knowledge and understanding is different. Such model should have a straightforward process flow and be comprehensive of all processes in evidence collection.

1.5 Research Scopes

- Mobile device forensics: generally, digital forensics can be classified into six different branches that are network forensics, software forensics, computer forensics, data forensics, cloud forensics and mobile device forensics. The scope of this research is mainly narrowed down to the subdivision of mobile device forensics which covers investigation of a smartphone, using accepted methods in forensically sound manner and following reliable process model. As regular phones can be seen as the subset of smartphones in terms of features and capabilities, the developed process model and the data acquisition model can also be employed in cases involving these types of phones. Nonetheless we focus on smartphones with wider range of features and capabilities.

- Although all processes of Generic Smartphones Forensics Investigation Process Model (GSFIPM) may or should consist of sub-processes, in the case of the present research, at the second tier we focus on the context of evidence collection and preservation. The introduction of this limitation was based on the fact that reviewing the relevant literature demonstrated the process of incorporating other major elements, especially the phase of analysis, is beyond the limitations of a research thesis, specifically in the light of the criticism presented for the case of many other models. The criticism is that they attempted to embrace a huge task which has made their model complex and unwieldy (Rogers, 2004).

- In terms of the ‘target audience’, this process model applies to both corporate investigators (third- parties that provide digital forensic services and perform their task on behalf of external clients, usually lawyers) and law enforcement investigators who already have enough backgrounds and experience for undertaking digital investigation. However the model is designed with sufficient guidelines and details to be practical even for novice digital investigator with proper knowledge and expertise in the field. Furthermore, despite incorporating the physical crime scene standard theories in the process of designing our model to be consistence with other models such as (Carrier and Spafford, 2003) and despite presenting the principle of *Interaction with the Case Coordinator* (including physical investigator of the actual crime scene), this model’s concentration is at the unit’s operating in the field of digital investigation as their roles and responsibilities are defined. Thus, some activities such as securing the physical crime scene from unauthorized access or surveying witnesses at the physical crime scene are excluded from the scope of our proposed process model since digital investigator can obtain necessary information through interactions with physical crime scene investigator.

- The development of new technology, constantly changes the field of digital forensics either as the focus of activities of digital forensic practitioners or in regard to the tools which are available during the process of undertaking such activities. As the result, NIST, the U.S. National Institute of Standards and Technology faces some difficulties in progressing at the same speed as new digital forensic software which are released or even the updates made to the current software. However, this study doesn’t intend to deal with the reliability of the wide range of tools and computer systems available to the digital forensic practitioners in order to apply in the process of their work. In addition, the new model for evidence collection and preservation is meant to assist in structuring current processes formally (in a way that can be described and presented to the court or respective audience), instead of totally replacing them.

1.6 Research Contributions

The major contribution of this research is the creation of a Generic Smartphones Forensic Investigation Process Model (GSFIP) that will assist investigators, law enforcements, examiners and researchers to follow a reliable procedure and apply a consistent and admissible process model for the investigation of a smartphone. As such, Formal Evidence Collection Model for Smartphones (FECMS) is designed to address both the real needs of the involved practitioners in the area of digital forensics and the expectation of law courts for a formal description of the process adopted to collect digital and physical evidence.

The following are the contributions of this research:

1. Developing a multi-tier, objective based, iterative Generic Smartphones Forensics Investigation Process Model that is generically applicable in investigation of any type of smartphone. The model is supported by Encompassing Proceedings as Principles that span across several processes and sub processes, usually during the entire timeline related to the process model. This process model has shown to be satisfactory in fulfilling the scientific requirements for a digital forensics process model.

2. Developing a Formal Evidence Collection Model for Smartphones which is generic in the sense that it is capable of being employed by the practitioners of digital forensic for all smartphones regardless of the platform. The model comprises of two UML (Unified Modelling Language) Activity diagrams and two Implementation Guidelines. Feedbacks from experts of the field recommend that the FECMS is successful in furthering adoption of the Unified Modelling Language in the digital forensic field which brings scientific merit to the process of evidence collection and preservation.

1.7 Thesis Organization

This section presents an outline of the entire thesis which is organized as follows:

Chapter 1 presents the introduction and includes, among other contents, the motivation, problem statement, research objectives and scopes, and contributions of the thesis.

Chapter 2 reviews digital forensics and digital evidence definitions, relevant standards and guidelines for smartphones forensics, related studies of the subject matter which includes conventional computer-based digital forensics models, smartphone-based digital forensics models, and the unified modelling language.

Chapter 3 provides a brief explanation of the research methodologies adopted in this research, the Design Science Research Process, DSRP. Each specific activity involved in the research process is detailed out. This chapter also describes how the proposed models are demonstrated and evaluated. The evaluation criteria used to evaluate the models are also highlighted.

Chapter 4 describes the proposed Generic Smartphone Forensic Investigation Process Model (GSFIPM). An inclusive discussion is provided on the components of GSFIPM which includes vital processes and Encompassing Proceedings governing implementation of the model. Implementation guidelines for each specific process are briefly explained in this chapter. The Design activity for the FECMS is also described along with its Principles, two UML Activity diagrams and two Implementation Guidelines.

Chapter 5 describes the composition of the Experts who incorporated in the survey, the tasks they were set to and the results of their feedbacks including detailed amendments to the FECMS.

Chapter 6 summarizes the entire thesis together with the recommendations on possible extensions of this research as future works. The research is also summarised with respect to the research contributions to the field of digital forensics.

REFERENCES

Adams, R. (2012). *The Advanced Data Acquisition Model (ADAM): A Process Model for Digital Forensic Practice*. Doctor of Philosophy Thesis , Murdoch University.

Adams, R., Hobbs, V., & Mann, G. (2013). The Advanced Data Acquisition Model (Adam): a Process Model for Digital Forensic Practice. *Journal of Digital Forensics, Security and Law*, *8*(4), 25–48.

Agarwal, R., & Kothari, S. (2015). Review of Digital Forensic Investigation Frameworks. In *Information Science and Applications* (Vol. 339, pp. 561–571).

Ahmed, R., & Dharaskar, R. V. (2009). Mobile forensics: An introduction from indian law enforcement perspective. *Communications in Computer and Information Science*, *31*, 173–184.

Al-Zarouni, M. (2006). Mobile Handset Forensic Evidence : a challenge for Law Enforcement. In *Proceedings of the 4th Australian Digital Forensics Conference*.

Aleksandar, V., & Venter, H. S. (2012). Harmonised Digital Forensic Investigation Process Model. *Information Security for South Africa (ISSA)*, 1--10.

Armstrong, C., & Armstrong, H. (2010). Modeling Forensic Evidence Systems Using Design Science, 282–300.

Ayers, R., Jansen, W., & Brothers, S. (2014). *Guidelines on mobile device forensics (NIST Special Publication 800-101 Revision 1)*.

Barmpatsalou, K., Damopoulos, D., Kambourakis, G., & Katos, V. (2013a). A critical review of 7 years of Mobile Device Forensics. *Digital Investigation*, *10*(4), 323–349.

Barmpatsalou, K., Damopoulos, D., Kambourakis, G., & Katos, V. (2013b). A Critical Review of 7 Years of Mobile Device Forensics. *Digital Investigation*, *10*(4), 323–349.

Baryamureeba, V., & Florence, T. (2006). The Enhanced Digital Investigation Process Model. *Asian Journal of Information Technology*, *5*, 790–794.

Beebe, N. L., & Clark, J. G. (2005). A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation*, *2*(2), 147–167.

Best Practices For Seizing Electronic Evidence. (2009). *United States Secret Service*.

Bogen, A. C., & Dampier, D. A. (2005). Unifying Computer Forensics Modeling Approaches: A Software Engineering Perspective. In *First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05)* (Vol. 1, pp. 27–39).

Carrier, B. D. (2006). *A Hypothesis-Based Approach To Digital Forensic Investigations*. Purdue University.

Carrier, B., & Spafford, E. (2004). An event-based digital forensic investigation framework. *Digital Forensic Research Workshop*, 1–12.

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 Forensics. In *Digital evidence and computer crime: Forensic science, computers, and the internet* (pp. 3–34).

Chan, E. M. (2011). *A framework for live forensics*. *ProQuest Dissertations and Theses*. University of Illinois at Urbana.

Ciardhuáin, S. (2004). An extended model of cybercrime investigations. *International Journal of Digital Evidence, 3*(1), 1–22.

Cleven, A., Gubler, P., & Hüner, K. M. (2009). Design alternatives for the evaluation of design science research artifacts. *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology*, 19.

Cusack, B., & Lutui, R. (2014). Up-dating Investigation Models for Smartphone Procedures. In *Proceedings of the 12th Australian Digital Forensics Conference* (pp. 53–63). Perth, Australia, 1-3 December, 2014.

Cyberthreat Defense Report. (2015). *CyberEdge Group*.

Digital Evidence: Standards and Principles. (2000).

Edmond, G. (2010). Impartiality, efficiency or reliability? A critical response to expert evidence law and procedure in Australia. *Australian Journal of Forensic Sciences*, *42*(2), 83–99.

Elyas, M., Maynard, S. B., Ahmad, A., & Lonie, A. (2014). Towards a Systemic Framework for Digital Forensic Readiness. *The Journal of Computer Information Systems*, *543*, 97–105.

Ghosh, A. (2004). Guidelines for the Management of IT Evidence, (March), 0–26.

Goel, A., Tyagi, A., & Agarwal, A. (2012). Smartphone Forensic Investigation Process Model. *International Journal of Computer Science & Security (IJCSS), 5*(5), 322–341.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75–105.

Hoog, A. (2011). Android forensic techniques. In *Android forensics: investigation, analysis and mobile security for Google Android* (pp. 195–284).

I.O.C.E. (2009). *Guidelines For Best Practice In The Forensic Examination Of Digital Technology*. *Working group Forensic IT ENFSI*.

Jain, N., & Kalbande, D. (2015). Digital Forensic Framework using Feedback and Case History Keeper. In *International Conference on Communication, Information & Computing Technology (ICCICT)*.

Jansen, W., & Ayers, R. (2007). Guidelines on Cell Phone Forensics. *NIST Special Publication*.

Khatir, M., Hejazi, S. M., & Sneiders, E. (2008). Two-Dimensional Evidence Reliability Amplification Process Model for Digital Forensics. In *Proceedings of 3rd International Annual Workshop on Digital Forensics and Incidents Analysis* (pp. 21–29).

Kipper, G. (2007). *Wireless Crime And Forensic Investigation*. CRC Press.

Kohn, M., Eloff, J. H. P., & Olivier, M. S. (2008). UML modelling of digital forensic process models (DFPMs). In *Proceedings of the ISSA Innovative Minds Conference, Pretoria, South Africa* (pp. 1–13).

Lessard, J., & Kessler, G. C. (2010). Android Forensics : Simplifying Cell Phone Examinations. *Small Scale Digital Device Forensics Journal*, *4*(1), 1–12.

Lin, I.-L., Chao, H.-C., & Peng, S.-H. (2011). Research of Digital Evidence Forensics Standard Operating Procedure with Comparison and Analysis Based on Smart Phone. In *2011 International Conference on Broadband and Wireless Computing, Communication and Applications* (pp. 386–391). Ieee.

Lutui, R. (2016). A multidisciplinary digital forensic investigation process model. *Business Horizons*, *59*(6), 593–604. https://doi.org/10.1016/j.bushor.2016.08.001

Martini, B., & Choo, K.-K. R. (2012). An Integrated Conceptual Digital Forensic Framework for Cloud Computing. *Digital Investigation*, *9*(2), 71–80.

Mason, S. (2007). lectronic Evidence: Disclosure, Discovery & Admissibility. *LexisNexis Butterworths*.

McKemmish, R. (1999). What is Forensic Computing? Retrieved from http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi118.pdf

McKemmish, R. (2008). When is Digital Evidence Forensically Sound? In *Advances in Digital Forensics IV* (Vol. 285, pp. 3–15). Springer US.

Miller, C. (2012). Best Evidence Rule. In *Evidence: Best Evidence Rule* (pp. 1–31). CALI eLangdell Press.

Mukasey, M. B., Sedgwick, J. L., & Hagy, D. W. (2008). *Electronic Crime Scene Investigation: A Guide for First Responders*. National Institute of Justice, Washington, DC.

Mumba, E. R., & Venter, H. (2014). Mobile Forensics using the Harmonised Digital Forensic Investigation Process. In *Information Security for South Africa (ISSA)* (pp. 1--10).

Noblett, M. G., Pollitt, M. M., & Presley, L. a. (2000). Recovering and Examining Computer Forensic Evidence. *Forensic Science Communications*, *2*(4), 1–8.

Palmer, G. (2001). *A Road Map for Digital Forensic Research. Technical Report DTR-T001-01, Report From the First Digital Forensic Research Workshop (DFRWS).*

Peffers, K., Tuunanen, T., Gengler, C. E., Rossi, M., Hui, W., Virtanen, V., & Bragge, J. (2006). The Design Science Research Process: A Model for Producing and Presenting Information Systems Research. *The Proceedings of Design Research in Information Systems and Technology DESRIST'06*, *24*, 83–106.

Ramabhadran, A. (2007). Forensic Investigation Process Model For Windows Mobile Devices. *Tata Elxsi Security Group*, 1–16.

Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. *International Journal of Digital Evidence*, *1*(3), 1–12.

Rogers, M. (2004). West Lafayette, Purdue University. *DCSA: A Practical Approach to Digital Crime Scene Analysis*, *3*.

Rogers, M. K., Mislan, R., Goldman, J., Wedge, T., & Debrota, S. (2006). Computer Forensics Field Triage Process Model. *Conference on Digital Forensics, Security and Law*, *1*(2), 27–40.

Ruan, C., & Huebner, E. (2009). Formalizing Computer Forensics Process with UML. In *Lecture Notes in Business Information Processing* (Vol. 20 LNBIP, pp. 184–189).

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.

Simão, A., Sícoli, F., Melo, L., Deus, F., & Sousa Júnior, R. (2011). Acquisition and Analysis of Digital Evidence in Android Smartphones. *The International Journal of Forensic Computer Science*, *6*(1), 28–43.

Spalevic, Z., Bjelajac, Z., & Caric, M. (2012). The Importance and the Role of Forensics of Mobile. *Facta Universitatis - Series: Electronics and Energetics*, *25*(2), 121–136.

SWGDE and SWGIT Digital & Multimedia Evidence Glossary. (2011). *Scientific Working Groups on Digital Evidence and Imaging Technology*. Retrieved from https://www.swgde.org/documents/Archived Documents/2011-01-14_SWGDE-SWGIT_Glossary_v2_4.pdf

Valjarevic, A., & Venter, H. S. (2015). A Comprehensive and Harmonized Digital Forensic Investigation Process Model. *Journal of Forensic Sciences*, 1–17.

Whitcomb, C. M. (2002). An Historical Perspective of Digital Evidence: A Forensic Scientist’s View. *International Journal of Digital Evidence*, *1*(1), 7–15.

Wilkinson, S., & Haagman, D. (2010). Good Practice Guide for Computer Based Evidence. *Association of Chief Police Officers*.

Willassen, S. (2005). Forensic Analysis of Mobile Phone Internal Memory. In *Advances in digital forensics* (Vol. 194, pp. 191–204).

Williams, D. J. (2012). *ACPO Good Practice Guide for Digital Evidence*. Retrieved from http://library.npia.police.uk/docs/acpo/digital-evidence-2012.pdf

Yu, X., Jiang, L., Shu, H., Yin, Q., & Liu, T. (2009). A Process Model for Forensic Analysis of Symbian Smart Phones. In *Advances in Software Engineering* (pp. 86–93).