UNIVERSITI PUTRA MALAYSIA

# *SCIENTIFIC FORENSIC FRAMEWORK FOR SMARTPHONES*

MARYAM SHAHPASAND

# SCIENTIFIC FORENSIC FRAMEWORK FOR SMARTPHONES

**By**

**MARYAM SHAHPASAND**

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

**April 2015**

# DEDICATION

Dedicated to

My wonderful parents whose words of encouragement and never ending support helped me complete this study,

My siblings who have never left my side and are very special, and

My supervisor who taught me to learn.

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

## SCIENTIFIC FORENSIC FRAMEWORK FOR SMARTPHONES

By

**MARYAM SHAHPASAND**

**April 2015**

**Chairman: Prof. Ramlan Mahmod, PhD**

**Faculty: Computer Science and Information Technology**

Main interest in both criminal investigations and security agencies is discovering communications channels by terrorists and criminals. One of the primary challenges faced by law enforcement agencies is the tremendous capacity and capabilities of smartphones as affordable, commonplace and an indispensable part of daily lives. When mobile phone devices are involved in a crime, forensic examiners need methods and tools to properly retrieve and analyze existing data on the digital device based on scientific forensic standards.

Unfortunately, forensic analysis of mobile phone devices is not adequately documented and explored. However to overcome this issue, there has been considerable work in the mobile phone analysis field but forensic science does not apply to forensic remnants determination on newfangled smartphones. Consideration of existing forensic works demonstrates that no formal technique covers verification of valuable forensic evidences on smartphones. Forensic investigators need scientific forensic sound techniques to analyze smartphones and present at court as reliable report. The current standard and open formats for mobile phone forensic describe memory image properties, but do not describe the products of detailed investigations for real-world crime cases and caused to mobile phone forensic investigators are confronting constraints such as time, budget, and the capacity when handling mobile phone forensic cases on a daily basis. So, the strong need felt for plenary framework to investigate smartphones in both digital and scientific forensic part, verify formally and apply to real-world scenarios.

The aim of this study is to propose and develop a scientific forensic framework for smartphones to apply the scientific forensic processes on smartphone investigation. The proposed scientific forensic framework for smartphones helps investigators by considering all artifacts and available digital evidences on these devices. A formal model designed for describing scientific forensic framework to verify examination results for presenting in the court rooms. The developed framework is analyzed for different contexts and conditions, within of real-world smartphone crime scenarios. Based on exploratory research, real-world smartphone crime cases investigate to discover the methods with the acquiring, preserving and analyzing digital evidences on Windows Phone 8 devices. Extracted evidences and forensic methods are examined by content pattern, formalize the extracted evidences in mathematical way and developed applications provided correctness, atomicity, integrity and consistency according to Doubert Standard.

Scientific forensic framework is developed and verified in both formal and experimental aspect of research. Formal model developed for scientific forensic framework based on TLA logic and proof the applicability of model on all smartphones independent of platforms. Formal model devised an expressive and flexible model for representing scientific forensic framework for smartphones. Experimental part done on Windows Phone 8, evaluated based on Doubert standard and approved by panel of experts including academic Committee, Low Enforcement Committee and Digital Investigator Committee. Applicability of proposed framework to real-world scenarios proves the framework correctness and device independency. The results demonstrate how the development framework can cover all steps of scientific and digital investigation process in smartphone crime cases. Scientific forensic framework is conformed to the best practices including: identifying the file sources, extracting files metadata, extracting device information, Network, auditing and reporting system to prepare court reports, file signatures (file carving model), SIM and SD card, Hardware, Phone State and artifacts examination on desktop O.S.

The present study creates a reliable guideline on smartphone investigation process and presented a scientific forensic framework by providing correctness, atomicity, integrity and consistency for smartphone. The proposed scientific forensic framework assists investigators by collecting all possible smartphone evidences to find out the chain of custody, present a court report and detect the criminals. Furthermore, the proposed framework as a scientific reference for smartphones investigators can be used for police agencies, low Enforcements, Incident Response management teams. Moreover, this study can be regarded as pioneering research which has attempted to shed light on smartphone forensic.

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

# RANGKA KERJA FORENSIK SAINTIFIK UNTUK TELEFON PINTAR

Oleh

**MARYAM SHAHPASAND**

**April 2015**

**Pengerusi: Prof. Ramlan Mahmod, PhD**

**Fakulti: Sains Komputer dan Teknologi Maklumat**

Kepentingan tertentu di dalam penyiasatan jenayah dan agensi-agensi keselamatan menjadi saluran komunikasi yang diterokai oleh pengganas dan penjenayah. Salah satu cabaran-cabaran utama yang dihadapi oleh agensi penguatkuasaan undang-undang ialah kapasiti dan kemampuan telefon pintar yang mudah dimiliki, lazim dan menjadi bahagian yang penting dalam kehidupan seharian. Apabila peranti-peranti telefon mudah alih terlibat di dalam sesuatu jenayah, pemeriksa forensik memerlukan kaedah dan peralatan mahupun perkakas untuk mendapat semula dan menganalisa data yang sedia ada pada peranti digital dengan betul berdasarkan piawaian forensik saintifik.

Malangnya, kaedah analisis forensik ke atas telefon mudah alih tidak didokumentasi dan diterokai secukupnya. Walaubagaimanapun, untuk mengatasi masalah ini, banyak usaha/kerja telah dilaksanakan di dalam bidang analisa telefon mudah alih, akan tetapi sains forensik tidak digunakan ke atas saki-baki penentuan forensic terhadap telefon pintar buatan baharu. Perhitungan ke atas kerja-kerja forensik yang sedia ada menunjukkan bahawa tidak ada teknik formal yang meliputi pengesahan bukti-bukti forensik yang bernilai pada telefon pintar. Penyiasat forensik memerlukan teknik bunyi forensik saintifik untuk menganalisis telefon pintar dan mengemukakannya sebagai laporan yang boleh dipercayai di mahkamah. Piawai semasa dan format terbuka bagi forensik telefon mudah alih menghuraikan sifat-sifat imej memori, tetapi tidak memerikan produk siasatan terperinci bagi kes-kes jenayah sebenar dan menyebabkan penyiasat forensik telefon mudah alih menghadapi kekangan seperti masa, bajet dan keupayaan apabila mengedalikan kes-kes forensik telefon mudah alih secara harian. Oleh itu, keperluan untuk rangka kerja tidak terhad untuk menyiasat telefon pintar dalam kedua-dua bahagian, forensik saintifik dan digital, ditentusahkan secara formal dan digunakan ke atas senario-senario sebenar.

Tujuan penyelidikan ini adalah untuk mereka bentuk dan membangun rangka kerja forensik saintifik untuk telefon pintar bagi menggunakan proses forensik saintifik ke atas siasatan telefon pintar. Rangka kerja yang dicadangkan untuk telefon mudah alih membantu para penyiasat dengan mempertimbangkan ke semua artifak dan bukti-bukti digital yang sedia ada di dalam peranti-peranti ini. Satu model formal direka untuk menghuraikan rangka kerja forensik untuk mengesahkan hasil penilaian untuk dibentangkan di dalam bilik mahkamah. Rangka kerja yang dibangunkan dianalisa untuk konteks dan keadaan yang berbeza, di dalam scenario jenayah telefon pintar sebenar. Berdasarkan kepada penyelidikan eksploratori, kes-kes jenayah telefon pintar disiasat untuk meneroka kaedah-kaedah pemerolehan, pemeliharaan dan penganalisaan bukti-bukti digital peranti-peranti telefon mudah alih Windows 8. Bukti-bukti yang diekstrak dan kaedah-kaedah forensik dinilai menerusi bentuk kandungan, memformalkan bukti-bukti yang diekstrak melalui kaedah matematik dan aplikasi yang dibangunkan, yang menyediakan kebenaran, keatoman, integriti dan konsistensi berdasarkan piawaian Doubert.

Rangka kerja forensik saintifik dibangunkan dan disahkan di dalam kedua-dua aspek iaitu formal dan eksperimen penyelidikan. Model formal dibangunkan untuk rangka kerja forensik saintifik berdasarkan logik TLA dan untuk membuktikan kesesuaiannya ke atas sebarang telefon pintar yang bebas platform.
Model formal cipta satu model ekspresif dan fleksibel bagi menggambarkan rangka kerja forensik saintifik untuk telefon pintar. Bahagian exsperimen dilakukan ke atas telefon mudah alih Windows 8, yang dinilai berdasarkan piawaian *Doubert* dan diluluskan oleh panel-panel pakar termasuklah

Jawatankuasa Akademik, Jawatankuasa Penguatkuasaan Rendah dan Jawatankuasa Penyiasat Digital. Kebolehgunaan cadangan rangka kerja kepada senario-senario sebenar membuktikan ketepatan rangka kerja dan kebebasan peranti. Hasil keputusan menunjukkan bagaimana pembangunan rangka kerja dapat merangkumi kesemua langkah-langkah saintifik dan proses penyisatan digital di dalam kes-kes jenayah telefon pintar. Rangka kerja forensik saintifik patuh kepada amalan-amalan terbaik termasuklah mengenalpasti sumber fail, mengekstrak metadata fail, mengekstrak informasi peranti, rangkaian, sistem audit dan laporan untuk menyediakan laporan-laporan mahkamah, fail tanda kenal (model ukiran fail), kad SIM dan SD, perkakasan, pemeriksaan keadaan telefon dan artifak-artifak pada Windows O.S.

Penyelidikan ini mewujudkan garis panduan yang boleh dipercayai ke atas proses siasatan telefon pintar dan membentangkan rangka kerja forensik saintifik dengan membekalkan ketepatan, keatoman, integriti dan konsistensi terhadap telefon pintar. Rangka kerja yang dicadangkan dapat membantu para penyiasat dengan mengumpul ke semua bukti-bukti telefon pintar untuk mengetahui rantaian jagaan, membentangkan laporan mahkamah dan mengesan penjenayah. Tambahan pula, rangka kerja yang dicadangkan sebagai rujukan saintifik untuk penyiasat-penyiasat telefon pintar boleh digunakan untuk agensi-agensi polis, penguatkuasaan rendah dan pihak pengurusan respons insiden. Selain itu, penyelidikan ini boleh dianggap sebagai penyelidikan perintis yang berupaya memberi gambaran yang lebih jelas di dalam forensik telefon pintar.

## ACKNOWLEDGEMENT

I would like to express my gratitude to all those gave me the possibility to complete this thesis. First I would like to express my profound appreciation and sincere thanks to my dear supervisor, Professor Dr. Ramlan Mahmod, whose help, patience, stimulating suggestions and encouragement helped me in all the time of writing this thesis. I am also deeply indebted to my respectable committee members, Associate Professor Dr. Nur Izura Udzir and Dr. Ali Deghantanha, for their insightful guidelines and invaluable specialized suggestions. Last, but by no means least, I would like to thank my family since I would not have been able to complete this thesis without their support.

I certify that a Thesis Examination Committee has met on 27 April 2015 to conduct the final examination of Maryam Shahpasand on her thesis entitled “Scientific Forensic Framework for Smartphones” 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:

**Azmi bin Jaafar, PhD**
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

**Dr. Azizol Abdullah, PhD**
Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

**Azizah binti Abdul Manaf, PhD**
Professor
Advance Informatics School (AIS)
University Technology Malaysia
(External Examiner)

**Jill Slay, PhD**
Professor
Division of Information Technology
University of South Australia
(External Examiner)

**ZULKARNAIN ZAINAL, PhD**
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: .. … 2015

This thesis was submitted to the Senate of University 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:

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

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

**Ali Deghantanha, PhD**
Senior Lecture
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

**BUJANG BIN KIM HUAT, 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, illustrations 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 Universit 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.: Maryam Shahpasand – GS26759

**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:

Signature: ____________________

Name of Member of Supervisory Committee:

Signature: ____________________

Name of Member of Supervisory Committee:

# TABLE OF CONTENTS

## LIST OF TABLES

**Table** **Page**

# LIST OF FIGURES

## LIST OF ABBREVATIONS

| | |
|---|---|
| ACPO | Association Of Chief Police Officers |
| CSI | Crime Scene Investigation |
| DFE | Digital Forensic Evidence |
| DFE | Digital Forensic Evidence |
| GPS | Global Positioning System |
| GSM | Global System For Mobile Communications |
| ICCID | SIM Card Unique Serial Number |
| MMS | Multimedia Message Service |
| MS | Mobile Station |
| MSDN | Microsoft Developer Network |
| NFC | Near Field Communication |
| NIST | National Institute Of Standards And Technology |
| NSP | Network Service Provider |
| O.S | Operating System |
| PIN | Personal Identification Number |
| PRNU | Photo Response Non Uniformity |
| PUK | PIN Unlock Key |
| SDK | Software Development Kit |
| SFFWP8 | Scientific Forensic Framework For Windows Phone 8 |
| SIM | Subscriber Identification Module |
| SMS | Short Message Service |
| SW | Search Warrant |
| SWGDE | Scientific Working Group On Digital Evidence |
| TLA | Temporal Logic of Action |
| UEFI | Unified Extensible Firmware Interface |
| WP8 | Windows Phone 8 |

## TERMS AND DEFINITIONS

| | Term | Definition |
|---|---|---|
| 1. | affidavit | A written sworn statement of fact voluntarily made by an affiant or deponent under an oath or affirmation administered by a person authorized to do so by law. Such statement is witnessed as to the authenticity of the affiant's signature by a taker of oaths, such as a notary public or commissioner of oaths. The name is Medieval Latin for he/she has declared upon oath. An affidavit is a type of verified statement or showing, or in other words, it contains a verification, meaning it is under oath or penalty of perjury, and this serves as evidence to its veracity and is required for court proceedings. |
| 2. | Chain of Custody | A clear, well-documented chain of custody must be maintained from the time the convicted offender / arrestee sample is first received by the CODIS unit (Arkansas State Crime Laboratory, 2010).<br>The continual custody of physical evidence from the time it's received to the time of its release from the State Crime Laboratory (Kermit B. Channell, 2009). |
| 3. | Digital Evidence | Information of probative value that is stored or transmitted in binary form (SWGDE and SWGIT, 2011).<br>Information and data of investigative value that are stored in or transmitted by an electronic device (U.S. Department of Justice 2007). |
| 4. | digital evidence custodian | Administer, maintain and con devices used to store and process digital evidence. |
| 5. | digital forensic examiner | Covers evidence handling, imaging drives and devices, and processing digital evidence. |
| 6. | digital forensic investigator | Determinate the evidence that is relevant to the case. Digital forensic investigators are familiar with digital evidence processing software and either are, or report directly to, case agents. |
| 7. | digital forensics | Tools and techniques to recover, preserve, and examine digital evidence on or transmitted by digital devices (E. Chan, Venkataraman, David, Chaugule, & Campbell, 2011). |
| 8. | Global Positioning System (GPS) | A series of computers and satellites designed to determine the latitude and longitude of a receiver on Earth (Katz, 2010a). |
| 9. | Global System for Mobile Communications (GSM) | Standard for mobile telephone systems. It originated in Europe and is the most common standard worldwide for mobile phones. GSM makes use of SIM cards to identify devices on the network. AT&T and T-Mobile are the largest NSP providers in the U.S. that operates with GSM (Katz, 2010a). |
| 10. | Hash | Numerical values that represent a string of text (search term), generated by hashing functions (algorithms). Hash values are used to query large sums of data such as databases or hard drives for specific terms. In forensics, hash values are also used to substantiate the integrity of digital evidence and/or for inclusion and exclusion comparisons against known value sets. (NFSTC, 2009) |
| 11. | Metadata | Data, frequently embedded within a file, that describes a file or directory, which can include the locations where the content is stored, dates and times, application specific information, and permissions. Examples: Email headers and website source code contain metadata.(NFSTC, 2009) |
| 12. | Multimedia Message Service (MMS) | A standard way to transmit messages that include multimedia content to and from mobile phones (Katz, 2010a). |

|  |  |  |
|---|---|---|
| 13. | Narrative Description | Documentation of the general appearance of the scene as first observed; extreme detail regarding evidence or actual collection of evidence, is normally beyond the scope of the Narrative Description (North Carolina Justice Department, 2010). |
| 14. | Network Service Provider (NSP) | The company that provides communication service to a mobile phone (Katz, 2010a). |
| 15. | Personal Identification Number (PIN) | A 4 to 8 digit code that can be user enabled to lock a SIM card and prevent a phone from functioning until entered (Katz, 2010a). |
| 16. | Search warrant | A written court order authorizing law enforcement to search a defined area and/or seize property specifically described in the warrant. In general, the degree of difficulty for the above authorizations is in the ascending order (Huang & Adviser-Fu, 2013). |
| 17. | Short Message Service (SMS) | A protocol used to transmit text messages to and from mobile phones (Katz, 2010a). |
| 18. | Write Block | Write Protect: Hardware and/or software methods of preventing modification of content on a media storage unit like a CD or thumb drive (NFSTC, 2009) |
| 19. | Scientific forensic | Scientific forensic enables law enforcement to use the new techniques practically and legally in forensically sound manner for whole investigation process (Barbara, 2008) |
| 20. | stand-alone Phone | Not attached to any network or device. |
| 21. | Forensic target | The digital device which uses for investigation and in this thesis the forensic target device is Windows Phone 8. |

# CHAPTER 1

# INTRODUCTION

## 1.1 Introduction

Particular interest in both criminal investigations and security agencies is discovering communications channels by terrorists and criminals. One of the primary challenges faced by law enforcement agencies is the tremendous capacity and capabilities of smartphones as affordable, commonplace and an indispensable part of daily lives. Smartphones provide mobile data storage, computation, network abilities, and innovative features of third party applications. Smart phone sales increased during 2010 with over 60 million units sold in the second quarter of 2010 (Gartner, 2010).

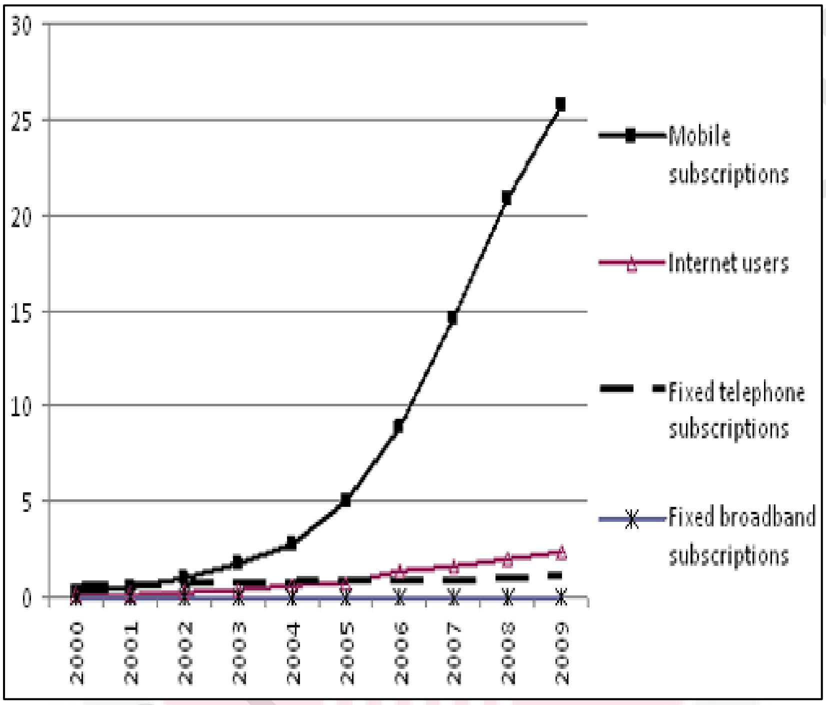

**Figure 1-1. Usage of mobile phones (NATIONS, 2010)**

There are usually three ways in which a mobile phone can be instrumental to the commission of a crime:

1. As a communication tool in the process of committing a crime - e.g. calls on phone related to drug trafficking

2. As a storage device providing evidence of a crime - e.g. images of child pornography created by phone camera

3. As a means of committing a crime - e.g. detonation of a bomb by sending a text message to the bomb

According to the Scientific Working Group on Digital Evidence (SWGDE) “new families of mobile phones are typically manufactured every 3 to 6 months (SWGDE, 2005)”, every new phone has the possibility for new evidence. When mobile phone devices are involved in a crime, forensic examiners need methods and tools to properly retrieve and analyze existing data on the mobile phones based on scientific forensic standards. law enforcement departments establish policies detailing how mobile phones should be treated and they will follow the guidelines established by organizations such as INTERPOL, NIST (NIST, 2005a) and SWGDE (NFSTC, 2009).

There can be an incredible amount of information stored on a mobile phone. When a crime is committed evidence may often be found on a phone if an investigator can find it. This evidence can take many forms such as call histories, contact lists, text messages, and multimedia. Some of the issues unique to the examination of smartphones consist of Memory type, States, Remote Communication, Data-sharing, Lack of Standardization, Technological Advances, Tool Validity (Breeuwsma, De Jongh, Klaver, Van Der Knijff, & Roeloffs, 2007; Distefano & Me, 2008; Jansen, Delaitre, & Moenner, 2008; Punja & Mislan, 2008; Ramabhadran, 2007). These, and other underlying factors, are why there is no investigative process model widely accepted that is independent of platform, manufacturer, or functionality for forensically examining a smartphone (Dancer & Adviser-Dampier, 2012).

These are basic principles of science, yet it is debatable if they are met by current digital investigations (B. Carrier, 2002; Meyers & Rogers, 2005). Digital Forensics is a practical and fast growing science to fight against digital crimes and investigate the criminal. Digital forensics is the occupation to collecting, preserving analyzing and presenting evidence from digital devices which used or accessed for illegal purposes (Kleiman, 2011; Pollitt, 2010). The lack of standardization and the rise in the use of smartphones serve as the main motivations for this research in scientific perspective.

Windows Phone 8 operating system is a relatively new type of digital devices that their usage is raising quickly in the public (Figure 1-2) because of the operating system resemblance to Windows 8 operating system. Moreover, the WP8 firmware interface controls the booting process of these devices, and then passes control to WP8 operating system (Figure 1-3). UEFI is a replacement for the older BIOS firmware interface to make faster boot and resume times (Windows Phone 8). Currently, there is no forensically sound method for analyzing the Windows Phone 8 mobile devices.

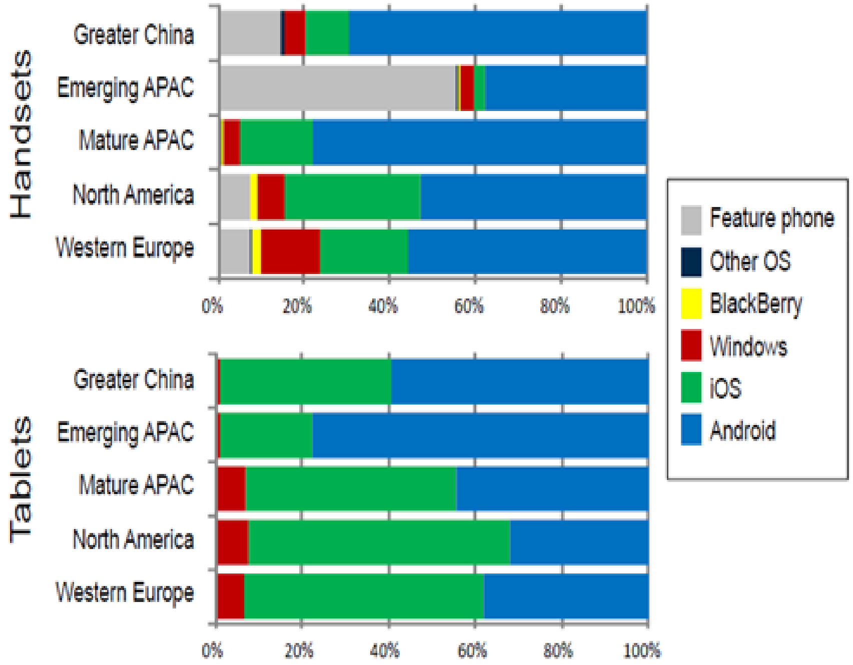

**Figure 1-2. Mobile platform trends 2015 by Gartner Darry Carlton**

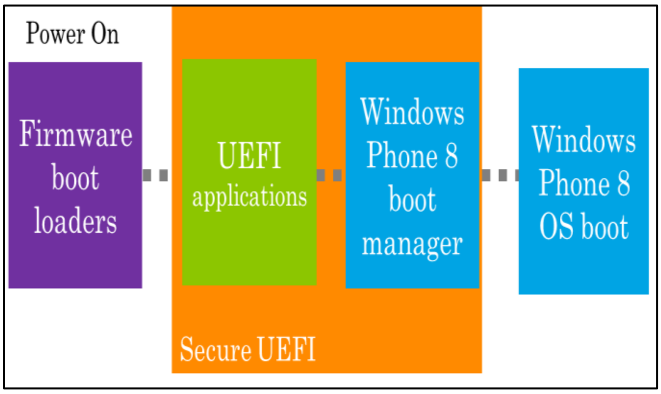

**Figure 1-3. Unified Extensible Firmware Interface (UEFI)**

The latest works on Windows Phone have not been cover Windows Phone 8 investigation process; even they did not support the foundation forensic issues of mobile phones with Windows O.Ss on version 6, 7. Windows Mobile advanced forensics (Klaver, 2010) express that the forensic application of Physical Acquisition can be applied to Windows CE devices and proposed a method to investigate isolated Windows CE database volume files for both active and deleted data. At the same time, usage of smartphones boot loaders to acquire data and preserve the digital evidence integrity has been proved (Rehault, 2010). In 2011, a comparison of information recovery techniques has been present for a single device (Grispos, Storer, & Glisson, 2011). Kaart (2013) define EDB format by using reverse-engineering and implement a parser due to forensic access to Windows Mobile pim.vol and other Embedded Database (EDB) volumes.

Furthermore, there has not been considerable work in the smartphone analysis field to determine forensic remnants on smartphone based on the scientific forensic. This research try to solve the issues associated with digital evidence on smartphone, and provides a forensic sound scientific framework. The aim of this study is developing a forensic sound scientific forensic framework for smartphone to help investigators by considering all artifacts and available digital evidences on these devices. The proposed framework sets the groundwork for smartphone investigation in a forensically sound manner by providing correctness, atomicity, integrity and consistency. This research is based on exploratory research and the goal is discovering ideas, methods and insights to familiarize with the acquiring and analyzing digital evidences on smartphone devices. Moreover, several forensic applications have been implemented on Web and Windows Phone 8 as sample of smartphone platforms to proof the applicability of framework on real-world scenarios.

The results showed that digital evidences are discoverable on smartphone and can be presented as court evidence in concise reports through the proposed forensic reporting system. Research results have been verified by formal model in first part and by Doubert standard in experimental part. Panel of experts included academic Committee, Low Enforcement Committee and Digital Investigator Committee approved the framework. Real-world case studies results demonstrate how the development framework can be covered all steps of scientific and digital investigation process in smartphone crime cases. The proposed framework assists investigators by collecting all possible smartphone evidences to find out the chain of custody and detect the criminals in forensic sound manner.

## 1.2 Problem Statement

With the growth in phone technology, the procedures and techniques used for data acquisition and for the analysis of data must all be modified. The creation and enhancements of digital devices directly affects the law enforcement community. Law enforcement officers know that smartphones as new and high usage devices can contain valuable evidence. They are left with trying to find ways to extract the evidence without altering or damaging it, so that they can develop their criminal cases. The findings of research studies (Barmpatsalou, Damopoulos, Kambourakis, & Katos, 2013; S. Garfinkel, 2012) have indicated that lack of sufficient scientific component of smartphone forensic is one of the main problems during investigation process. The current frameworks do not consider whether law enforcement can use the new technique practically and legally and whether it is forensically sound enough for investigation. Using technologies in investigation process without any law restrictions is not possible and smartphone investigators have been found serious difficulties in using current digital forensic framework during investigation process without scientific components (Barmpatsalou, et al., 2013; S. Garfinkel, 2012; Thomas, Owen, & McPhee, 2010).

Over the last several years, commercial hardware and software vendors who specialize in digital forensic analysis tools and applications have made significant improvements in the methodologies necessary to analyze digital evidence (Huebner, Bem, & Bem, 2007). Forensic examiners should consider the most appropriate combination of certification, education, and real-world experience to gauge the competency of a smartphones investigation process (Garrie, 2014). Current United Kingdom ACPO guidelines and the United States of America NIST guidelines are unclear or insubstantial (Thomas, et al., 2010). Consideration of existing forensic works demonstrates that no formal technique covers verification of valuable forensic evidences on smartphones (Grispos, et al., 2011). Forensic investigators need forensic sound techniques to analyze smartphones and present at court as reliable report. law enforcement, military and other users of smartphones forensics products will be unable to rely on the results of forensic analysis (Al-Zarouni, 2006; S. L. Garfinkel, 2010).

Proportionally, many criminal activities are carried out through the use of or with the aid of mobile phones. For the past five years, DFEs have been forced to keep up with the emerging technologies and growing capacities of mobile phones from the simple phone to the more advanced smartphones of today. Phone evidence storage challenges include acquiring and processing massive amounts of digital evidence, maintaining the integrity of the evidence and storing the evidence for extended periods of time. It is reasonable to believe that a forensic examiner could have evidence from an improperly protected smartphones dismissed from court entirely. Even if that evidence is not dismissed, there is now the problem of explaining to a jury why evidence has potentially changed. For mobile phone forensics to catch up with release cycles of mobile phones, more comprehensive and in depth frameworks for evaluating mobile forensic toolkits should be developed and data on appropriate tools and techniques for each type of phone should be made available at timely manner. These features may not be supported by existing software tools and a release of a new revision of the forensic software will be required to support the device (Owen & Thomas, 2011). The current standard and open formats for mobile phone forensic describe memory image properties, but do not describe the products of detailed investigations for real-world crime cases (Levine & Liberatore, 2009). Current United Kingdom ACPO guidelines and the United States of America NIST guidelines are unclear or insubstantial (Thomas, et al., 2010). Mobile phone forensic specialists and state and local investigators are also confronting constraints such as time, budget, and capacity when handling mobile phone forensic cases on a daily basis (Bennett, 2011). Without a clear strategy, forensic research will fall behind the market, tools will become increasingly obsolete, and law enforcement, military and other users of smartphones forensics products will be unable to rely on the results of forensic analysis (S. L. Garfinkel, 2010).

Scientific forensic enables law enforcement to use the new techniques practically and legally in forensically sound manner for whole investigation process (Barbara, 2008). Many of the recognized areas of digital forensics still lack the kinds of scientific part of forensic. Smartphones have largely been used for business purposes and they have also been used in governmental and military. So, the strong need felt for plenary framework to investigate smartphones in both digital and scientific forensic part, verify formally and apply to real-world scenarios. Therefore, providing the most viable scientific component is absolutely essential to enhance investigation correctness. Formal proof truly protects evidence on smartphones so it can be presented in court. Consequently, the intention of design and development of scientific forensic framework verified formally and tested the applicability of framework to real-world smartphones crime cases are rightly emphasized.

## 1.3 Research Objectives

The objective of this research is to design and develop a scientific forensic framework for smartphones. To achieve this objective, the following processes are fulfilled in this thesis:

1. To propose and develop a scientific forensic framework for smartphones to apply the scientific forensic processes on smartphone investigation.

2. To design a formal model for describing scientific forensic framework to verify examination results for presenting in the court rooms.

3. To design an experimental test to analyze the extendibility of the proposed framework and included methods in investigating of real-world smartphone crime cases within different contexts and different phones conditions.

### 1.4 Research Scope

This research is scoped according to the delimitation that the experiments are performed on stand-alone Windows Phone 8 devices without any chip-off or JTAG on boards. The experiments are adjusted by considering setting on factory reset and built-in applications that are similar on both HTC 8x and Nokia Lumia 820.

### 1.5 Research Contributions

This research aims to address the lack of practices in mobile phone forensics, the examination crimes and illegal activities involving smartphones, and the need for educating and training law enforcement and mobile phone forensic technicians. The contributions of this research lie in the proposed framework consist:

1. Developed framework bridged the gap between scientific forensic and smartphone forensic. The proposed framework can be a quick reference for smartphones investigators and can be used for police agencies, low Enforcements, Incident Response management teams. The scientific part consists of legal standards and rules, hardware identification, digital data identification, scene recognition, affidavit and search warrant, investigator kit, initial scene understanding and documentation.

2. Formal model devised an expressive and flexible method for representing scientific forensic framework for smartphones. Developed methods that can be used to easily share evidential findings and to reuse and manage knowledge acquired about the crime case and evidences.

3. The designed experimental test has been applied to three real-world smartphones crime scene within different phone conditions. Applicability of proposed framework to real-world scenarios verified by Doubert Standard proves the framework correctness and device independency.

Indeed, the present study created a reliable guideline on smartphone investigation process and presented a scientific forensic framework by providing correctness, atomicity, integrity and consistency for smartphone. Moreover, this study can be regarded as pioneering research which has attempted to shed light on smartphone forensic.

### 1.6 Organization of Thesis

The thesis is organized in accordance with the standard structure of thesis at University Putra Malaysia. It is organized in a manner to give detail information on how the research is carried out. As final report of the research, this thesis consists of six chapters.

The first chapter of the thesis, which is an introductory chapter, introduces the background of the research, researcher's motivation and research intention. It describes the rationale of conducting this research that includes the objectives and problem concentration of the research. The research contributions and scope of research are also explained in this chapter.

Chapter two is the Literature Review that provides a review and discussion of past works relevant to this research. In this chapter, resource materials such as journals, conference proceedings, seminar, thesis, books, and online resources are used as the main references.

Next is Chapter 3 justifies the research methodology employed in conducting this research. The methodology consists of design, development and verification of framework.

The details of formal model are presented in chapter 4. The model used to verify the proposed scientific forensic framework for smartphones.

Chapter 5 describes the research experimental findings and discussion. It presents a experiments on Windows Phone 8 with the verifications of the findings.

The final or conclusion chapter of the thesis is Chapter 6. The conclusion of the research and potential future research is presented in this chapter.

Appendices A, B, and C show the result of applying proposed framework to three real-world case studies and demonstrate the correct feature of proposed framework.

# REFERENCES

AccessData-MPE+. http://accessdata.com/solutions/digital-forensics/mpe

AccessData. Forensic Tool Kit (FTK), from http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk

Adelstein, F., & Senior Principal Scientist, A. (2003). MFP: The mobile forensic platform. *International Journal of Digital Evidence, 2*(1).

Ahmad, A. (2002). *The forensic chain of evidence model: Improving the process of evidence collection in incident handling procedures.* Paper presented at the Proceedings of the 6th Pacific Asia Conference on Information Systems, Tokyo, Japan.

Ahmed, R., & Dharaskar, R. V. (2008). *Mobile forensics: an overview, tools, future trends and challenges from law enforcement perspective.* Paper presented at the 6th International Conference on E-Governance, ICEG, Emerging Technologies in E-Government, M-Government.

Al-Zarouni, M. (2006). Mobile handset forensic evidence: a challenge for law enforcement.

Al Mutawa, N., Baggili, I., & Marrington, A. (2012). Forensic analysis of social networking applications on mobile devices. *Digital Investigation, 9*, S24-S33.

Alink, W., Bhoedjang, R., Boncz, P. A., & de Vries, A. P. (2006). XIRAF - XML-based indexing and querying for digital forensics. *Digital Investigation, 3*, 50-58.

Allen, W. H. (2005). Computer forensics. *IEEE security & privacy, 3*(4), 59-62.

Androulidakis, I. I. (2012). Mobile Phone Forensics *Mobile Phone Security and Forensics* (pp. 75-99): Springer.

Arasteh, A. R., Debbabi, M., Sakha, A., & Saleh, M. (2007). Analyzing multiple logs for forensic evidence. *Digital Investigation, 4*, 82-91.

Arkansas State Crime Laboratory (2010). *Quality Assurance Manual*.

Association of Chief Police Officers (2011). ACPO Speed Enforcement Policy Guildline 2011-2015.

Association of Chief Police Officers (ACPO). http://www.acpo.police.uk/

Association of Chief Police Officers (ACPO) (2000). Association of Chief Police Officers (ACPO) Guildline.

Backtrack-Linux ForensicPackage. http://www.backtrack-linux.org/

Baggili, I. M., Mislan, R., & Rogers, M. (2007). Mobile phone forensics tool testing: A database driven approach. *International Journal of Digital Evidence, 6*(2), 168-178.

Barbara, J. J. (2008). *Handbook of digital and multimedia forensic evidence*: Springer.

Barbara, J. J. (2009). Cloud computing: Another digital forensic challenge. *Digital Forensic Investigator News*.

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

Barry AJ Fisher, & David R Fisher (2012). *Techniques of crime scene investigation*: CRC Press.

Baryamureeba, V., & Tushabe, F. (2004). *The enhanced digital investigation process model.* Paper presented at the Proceedings of the Fourth Digital Forensic Research Workshop.

Baum, L. (2012). *The Supreme Court*: CQ Press.

Beckett, J., & Slay, J. (2007). *Digital forensics: Validation and verification in a dynamic work environment.* Paper presented at the System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on.

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

Bennett, D. W. (2011). The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations.

Berghel, H. (2007). Hiding data, forensics, and anti-forensics. *Communications of the ACM, 50*(4), 15-20.

Beverly, R., Garfinkel, S., & Cardwell, G. (2011). Forensic carving of network packets and associated data structures. *Digital Investigation, 8,* S78-S89.

Bhoedjang, R. A., van Ballegooij, A. R., van Beek, H. M., van Schie, J. C., Dillema, F. W., van Baar, R. B., et al. (2012). Engineering an online computer forensic service. *Digital Investigation, 9*(2), 96-108.

Biggs, S., & Vidalis, S. (2009). *Cloud computing: The impact on digital forensic investigations.* Paper presented at the Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for.

Birk, D., & Wegener, C. (2011). *Technical issues of forensic investigations in cloud computing environments.* Paper presented at the Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop on.

BKF-CellPhoneAnalayzer. http://www.bkforensics.com/cpa.html

Bogen, A. C., & Adviser-Dampier, D. A. (2006). *Selecting keyword search terms in computer forensics examinations using domain analysis and modeling.* Mississippi State University.

Bommisetty, S., Tamma, R., & Mahalik, H. (2014). *Practical Mobile Forensics*: Packt Publishing Ltd.

Bradford, P., & Ray, D. (2007). *Models of models: Digital forensics and domain-specific languages.* Paper presented at the Cyber Security and Information Infrastructure Workshop, Oak Ridge National Laboratory.

Breeuwsma, M., De Jongh, M., Klaver, C., Van Der Knijff, R., & Roeloffs, M. (2007). Forensic data recovery from flash memory. *Small Scale Digital Device Forensics Journal, 1*(1), 1-17.

Brezinski, D., & Killalea, T. (2002). Guidelines for evidence collection and archiving. *Request For Comments, 3227*.

Brueckner, S., Guaspari, D., Adelstein, F., & Weeks, J. (2008). Automated computer forensics training in a virtualized environment. *Digital Investigation, 5,* S105-S111.

Burdach, M. (2005). Digital forensics of the physical memory. *Warsaw University*.

Cabinet Office (2010). Data exchange - The legal implications, from http://www.crimereduction

Caine. http://www.caine-live.net/

Carrier, B. (2002). *Open source digital forensics tools: The legal argument*: stake Research Report.

Carrier, B., & Spafford, E. H. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence, 2*(2), 1-20.

Carrier, B., & Spafford, E. H. (2004). *An event-based digital forensic investigation framework.* Paper presented at the Digital forensic research workshop.

Carrier, B. D., & Spafford, E. H. (2006). Categories of digital investigation analysis techniques based on the computer history model. *Digital Investigation, 3*, 121-130.

Case, A., Cristina, A., Marziale, L., Richard, G. G., & Roussev, V. (2008). FACE: Automated digital evidence discovery and correlation. *Digital Investigation, 5*, S65-S75.

CASE, J. R. (2011). Crime-Scene Investigation and Evidence Collection.

Casey, E. (2001). *Handbook of computer crime investigation: forensic tools and technology*: Academic press.

Casey, E. (2007). What does "forensically sound" • really mean? *Digital Investigation, 4*(2), 49-50.

Casey, E. (2011a). *Digital evidence and computer crime: forensic science, computers and the internet*: Academic press.

Casey, E. (2011b). The increasing need for automation and validation in digital forensics. *Digital Investigation, 7*(3), 103-104.

Casey, E., Bann, M., & Doyle, J. (2010). Introduction to windows mobile forensics. *Digital Investigation, 6*(3), 136-146.

Casey, E., Cheval, A., Lee, J. Y., Oxley, D., & Song, Y. J. (2011). Forensic acquisition and analysis of palm webOS on mobile devices. *Digital Investigation, 8*(1), 37-47.

Catanese, S. A., & Fiumara, G. (2010). *A visual tool for forensic analysis of mobile phone traffic.* Paper presented at the Proceedings of the 2nd ACM workshop on Multimedia in forensics, security and intelligence.

Cellebrite-UFED. http://www.cellebrite.com/mobile-forensics/products/standalone/ufed-touch-ultimate

Chan, E., Venkataraman, S., David, F., Chaugule, A., & Campbell, R. (2011). *Forenscope: A framework for live forensics.* Paper presented at the Proceedings of the 26th Annual Computer Security Applications Conference.

Chan, E. M. (2011). *A framework for live forensics.* University of Illinois at Urbana-Champaign.

Chan, E. M., Carlyle, J. C., David, F. M., Farivar, R., & Campbell, R. H. (2008). *Bootjacker: compromising computers using forced restarts.* Paper presented at the Proceedings of the 15th ACM conference on Computer and communications security.

Chen, M., Fridrich, J., Goljan, M., & LukÃ¡s, J. (2008). Determining image origin and integrity using sensor noise. *Information Forensics and Security, IEEE Transactions on, 3*(1), 74-90.

Chung, H., Park, J., Lee, S., & Kang, C. (2012). Digital forensic investigation of cloud storage services. *Digital Investigation, 9*(2), 81-95.

Ciardhuain, S. a. Ã. (2004). An extended model of cybercrime investigations. *International Journal of Digital Evidence, 3*(1), 1-22.

Cornell University Law School. http://www.law.cornell.edu/

Crime, I. E. W. P. o. I. (2006). *Good Practice Guide for Mobile Phone Seizure and Examination*: European Working Party on IT Crime.

Crime Scene Resources, I. http://www.crime-scene-investigator.net

CSA, C. S. A. (2012). Top threats to cloud computing V1.0, from http://www.cloudsecurityalliance.org

Dancer, F. C., & Adviser-Dampier, D. A. (2012). *A platform independent investigative process model for smartphones.*

Daniel, L. E. (2012). *Digital forensics for legal professionals: understanding digital evidence from the warrant to the courtroom*: Elsevier.

Dankner, S., & Gupta, M. (2007). Evidence preservation: RF signal blocking fffiiciency & effect of lack of signal on a sim card: Term Paper.

Datar, T. D., Cole, K. A., & Rogers, M. K. (2014). *AWARENESS OF SCAM E-MAILS: AN EXPLORATORY RESEARCH STUDY.* Paper presented at the Proceedings of the Conference on Digital Forensics, Security and Law.

Davis, C., Cowen, D., & Philipp, A. (2005). *Hacking Exposed Computer Forensics: Secrets & Solutions*: McGraw-Hill/Osborne.

Davis, M. C. (2009). *A Network Based Storage Model for the Processing of Digital Evidence.* University of Tulsa.

Dellutri, F., Ottaviani, V., & Me, G. (2008). *MIAT-WM5: forensic acquisition for Windows mobile PocketPC.* Paper presented at the Proceedings of the workshop on security and high performance computing, as part of the 2008 international conference on high performance computing & simulation.

Digital Discovery. http://www.digitaldiscoveryesi.com/

Distefano, A., & Me, G. (2008). An overall assessment of mobile internal acquisition tool. *Digital Investigation, 5*, S121-S127.

Distefano, A., Me, G., & Pace, F. (2010). Android anti-forensics through a local paradigm. *Digital Investigation, 7*, S83-S94.

Drepper, U. (2007). What every programmer should know about memory. *Red Hat, Inc, 11*.

e-fense Helix3. http://www.e-fense.com/h3-enterprise.php

ENISA, E. N. a. I. S. A. (2011). Security & resilience in governmental clouds, from http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-andresilience-in-governmental-clouds/at_download/fullReport

Evidence, S. W. G. o. D., & America, U. S. o. (2000). Digital Evidence: Standards and Principles.

Fairbanks, K. D. (2012). An analysis of Ext4 for digital forensics. *Digital Investigation, 9*, S118-S130.

Farmer, D., & Venema, W. (2005). *Forensic discovery* (Vol. 6): Addison-Wesley Upper Saddle River.

Farrell, M. G. (1993). Daubert v. Merrell Dow Pharmaceuticals, Inc.: Epistemilogy and Legal Process. *Cardozo L. Rev., 15*, 2183.

Federal Bureau of Investigation. Innocent Images National Initiative, Washington, DC from http://www.fbi.gov/

Federal Judicial Center. Materials on Electronic Discovery: Civil Litigation, Federal Judicial Center Foundation, Washington, DC, from www.fjc.gov/public/home.nsf/pages/196

Feldman, J. E. (2006). Top ten things to do when collecting electronic evidence. *Fam. Advoc., 29*, 9.

Forensics Laboratory *North Texas Regional Computer Forensics Laboratory,* : www.ntrcfl.org/index.cfm, Dallas,Texas

Friendly, H. J. (2012). The" Law of the Circuit" and All That: Foreword to the Second Circuit 1970 Term. *St. John's Law Review, 46*(3), 2.

Garcia, G. L. (2007). *Forensic physical memory analysis: an overview of tools and techniques.* Paper presented at the TKK T-110.5290 Seminar on Network Security.

Garfinkel, S. (2012). Lessons learned writing digital forensics tools and managing a 30TB digital evidence corpus. *Digital Investigation, 9*, S80-S89.

Garfinkel, S., Farrell, P., Roussev, V., & Dinolt, G. (2009). Bringing science to digital forensics with standardized forensic corpora. *Digital Investigation, 6*, S2-S11.

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation, 7*, S64-S73.

Garrie, D. B. (2014). *Digital Forensic Evidence in the Courtroom: Understanding Content and Quality*.

Gartner (2010). worldwide mobile device sales grew 13.8 percent in second quarter of 2010, but competition drove prices down, from http://www.gartner.com/it/page.jsp?id¼41421013

George Stanley Burdynski Jr. The Charley Project, from www.charleyproject.org/cases/b/burdynskigeorge.html

GFI http://www.gfi.com/blog/top-20-free-digital-forensic-investigation-tools-for-sysadmins/.

Gladyshev, P., & Patel, A. (2004). Finite state machine approach to digital event reconstruction. *Digital Investigation, 1*(2), 130-149.

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.

Grove, W. M., & Andreasen, N. C. (1982). Simultaneous tests of many hypotheses in exploratory research. *The Journal of nervous and mental disease, 170*(1), 3-8.

GuidanceSoftware-EnCase. https://www.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx#

Guo, Y., & Slay, J. (2010). *Data recovery function testing for digital forensic tools*: Springer.

Guo, Y., Slay, J., & Beckett, J. (2009). Validation and verification of computer forensic software toolsâ€”Searching Function. *Digital Investigation, 6*, S12-S22.

Hafner, K., & Markoff, J. (1995). *Cyberpunk: Outlaws and Hackers on the Computer Frontier, Revised*: Simon and Schuster.

Halderman, J. A., Schoen, S. D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J. A., et al. (2009). Lest we remember: cold-boot attacks on encryption keys. *Communications of the ACM, 52*(5), 91-98.

HARCFL. Heart of America RCFL, from http://www.harcfl.org/

Hart, S. V., Ashcroft, J., & Daniels, D. J. (2004). Forensic examination of digital evidence: a guide for law enforcement. *National Institute of Justice NIJ-US, Washington DC, USA, Tech. Rep. NCJ, 199408*.

Hejazi, S., Talhi, C., & Debbabi, M. (2009). Extraction of forensically sensitive information from windows physical memory. *Digital Investigation, 6*, S121-S131.

HTC Windows Phone 8 http://www.htc.com/us/smartphones/htc-wp-8x/.

Huang, J., & Adviser-Fu, X. (2013). A comprehensive study of network forensics in terms of laws and technologies.

Huebner, E., Bem, D., & Bem, O. (2007). Computer forensicsâ€“past, present and future. *Information security Technical report, 8*(2), 32-46.

Huebner, E., Bem, D., Henskens, F., & Wallis, M. (2007). Persistent systems techniques in forensic acquisition of memory. *Digital Investigation, 4*(3), 129-137.

Hunton, P. (2011). A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment. *Digital Investigation, 7*(3), 105-113.

Infosec Institute. http://resources.infosecinstitute.com/computer-forensics-tools/

Inoue, H., Adelstein, F., & Joyce, R. A. (2011). Visualization in testing a volatile memory forensic tool. *Digital Investigation, 8*, S42-S51.

Investigation, E. C. S. (2001). A Guide for First Responders. *US Department of Justice, NCJ, 187736*.

James, S. H., Nordby, J. J., & Bell, S. (2005). *Forensic science: an introduction to scientific and investigative techniques*: CRC press.

Jansen, W., & Ayers, R. (2007). Guidelines on cell phone forensics. *NIST Special Publication, 800*, 101.

Jansen, W., Delaitre, A. l., & Moenner, L. (2008). *Overcoming impediments to cell phone forensics.* Paper presented at the Hawaii International Conference on System Sciences, Proceedings of the 41st Annual.

Jarrett, H. M., Bailie, M. W., Hagen, E., & Judish, N. (2009). Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. *Office of Legal Education Executive Office for United States Attorneys*.

Jeon, S., Bang, J., Byun, K., & Lee, S. (2012). A recovery method of deleted record for SQLite database. *Personal and Ubiquitous Computing, 16*(6), 707-715.

Johnson, C., Montanari, M., & Campbell, R. H. (2010). *Automatic management of logging infrastructure.* Paper presented at the CAE Workshop on Insider Threat. CAE.

Kaart, M., Klaver, C., & van Baar, R. (2013). Forensic access to Windows Mobile pim. vol and other Embedded Database (EDB) volumes. *Digital Investigation, 9*(3), 170-192.

Kahved zic, D., & Kechadi, T. (2009). DIALOG: A framework for modeling, analysis and reuse of digital forensic knowledge. *Digital Investigation, 6*, S23-S33.

Katz, E. (2010a). *A field test of mobile phone shielding devices.*

Katz, E. (2010b). A field test of mobile phone shielding devices.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response. *NIST Special Publication*, 800-886.

Kermit B. Channell (2009). *Evidence Receiving Quality Manual*: ARKANSAS STATE CRIME LABORATORY.

King, S. T., & Chen, P. M. (2005). Backtracking intrusions. *ACM Transactions on Computer Systems (TOCS), 23*(1), 51-76.

Klaver, C. (2010). Windows Mobile advanced forensics. *Digital Investigation, 6*(3), 147-167.

Kleiman, D. (2011). *The Official CHFI Study Guide (Exam 312-49): For Computer Hacking Forensic Investigator*: Syngress.

Kornblum, J. (2002). *Preservation of fragile digital evidence by first responders.* Paper presented at the Digital Forensics Research Workshop.

Kruse II, W. G., & Heiser, J. G. (2001). *Computer forensics: incident response essentials*: Pearson Education.

Kuhn, R. (2010). Smart phone tool test assertions and test plan. *National Institute for Science and Technology*.

Laboratory Accreditation Board *American Society of Crime Laboratory Directors - Laboratory Accreditation Board*, : http://www.ascld-lab.org/ , Garner, North Carolina

Laboratory and Scientific Section (2009). *Crime scene and physical evidence awareness for non-forensic personnel*. New York: United Nations Office on Drugs and Crime.

Guidline for evidence submission (2007).

Lai, Y., Yang, C., Lin, C., & Ahn, T. (2011). Design and implementation of mobile forensic tool for android smart phone through cloud computing *Convergence and Hybrid Information Technology* (pp. 196-203): Springer.

Lamport, L. (1994). The temporal logic of actions. *ACM Transactions on Programming Languages and Systems (TOPLAS), 16*(3), 872-923.

Laurie, A. (2006). Digital detective - Bluetooth. *Digital Investigation, 3*(1), 17-19.

Lee, H. C., Palmbach, T., & Miller, M. T. (2001). *Henry Lee's crime scene handbook*: Academic Press.

Lee, X., Yang, C., Chen, S., & Wu, J. (2009). *Design and implementation of forensic system in android smart phone.* Paper presented at the The 5th Joint Workshop on Information Security.

Leigland, R., & Krings, A. W. (2004). A formalization of digital forensics. *International Journal of Digital Evidence, 3*(2), 1-32.

LeMay, M., & Gunter, C. A. (2012). Cumulative attestation kernels for embedded systems. *Smart Grid, IEEE Transactions on, 3*(2), 744-760.

Lesemann, D., & Mahalik, H. (2008). Dialing up and drilling down: Forensic preservation of handheld devices. *ISSA Journal, p. 22l, November*.

Levine, B. N., & Liberatore, M. (2009). Dex: Digital evidence provenance supporting reproducibility and comparison. *Digital Investigation, 6*, S48-S56.

Lewis, D. L. (2009). Examining cellular phones and handheld devices. *Forensics Magazine*.

Libster, E., & Kornblum, J. D. (2008). A proposal for an integrated memory acquisition mechanism. *ACM SIGOPS Operating Systems Review, 42*(3), 14-20.

Lutes, K. D., & Mislan, R. P. (2008). *Challenges in Mobile Phone Forensics.* Paper presented at the Proceeding of the 5th International Conference on Cybernetics and Information Technologies, Systems and Applications.

M. Mason (2007). Congressional Testimony, Statement before the House Judiciary Committee, Federal Bureau of Investigation, Washington, DC from www.fbi.gov/congress/congress07/mason101707.htm

Majors, S. (2009). Ohio justices: Cell phone searches require warrant. *The New York Times*.

Marcinkoski, J. (2008). Re: Cell phones and the fourth amendment.

Mobile Device Forensics (2009).

Martini, B., & Choo, K.-K. R. (2012). An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation, 9*(2), 71-80.

Mattia Epifani (2013). Open source tools for mobile forensics,  sans european digital forensics summit.

McKemmish, R. (1999). *What is forensic computing?* : Australian Institute of Criminology.

Mellars, B. (2004). Forensic examination of mobile phones. *Digital Investigation, 1*(4), 266-272.

Mercuri, R. (2005). Challenges in forensic computing. *Communications of the ACM, 48*(12), 17-21.

Meyers, M., & Rogers, M. (2005). Computer Forensics: Meeting the Challenges of Scientific Evidence. *Research Advances in Digital Forensics*.

Micro Systemation-XRY. https://www.msab.com/

Microsoft. http://msdn.microsoft.com/en-us/windows/desktop/bg162891.aspx

Microsoft Windows Phone 8. http://support2.microsoft.com/ask-community/phone/windows-phone-8/

Mislan, R. P., Casey, E., & Kessler, G. C. (2010). The growing need for on-scene triage of mobile devices. *Digital Investigation*, *6*(3), 112-124.

Mitchell, L. J., Gumley, A., Reilly, E. S., Macbeth, A., Lysaker, P., Carcione, A., et al. (2012). Metacognition in forensic patients with schizophrenia and a past history of interpersonal violence: an exploratory study. *Psychosis*, *4*(1), 42-51.

MOBILedit Forensic. http://www.mobiledit.com/forensic

Mohay, G. (2005). *Technical challenges and directions for digital forensics.* Paper presented at the Systematic Approaches to Digital Forensic Engineering, 2005. First International Workshop on.

MSDN windows Phone 8 https://social.msdn.microsoft.com/Forums/windowsapps/en-US/home?forum=wpdevelop.

Mukasey, M. B., Sedgwick, J. L., & Hagy, D. (2008). Electronic Crime Scene Investigation: A Guide for First Responders. *NCJ, 219941*.

National Institute for Justice (2009). *Test results for mobile device acquisition tool: Cellebrite UFED*: U.S. Department of Justice, 810 Seventh Street N.W. Washington, DC 20531, USA: National Institute for Justice.

NATIONS, U. (2010). *Information Economy Report 2010, ICTs, Enterprises and Poverty Alleviation*.

Nederlands Forensisch Institut (2012). Workflow Mobile Phone Forensic Examinations.

Nelson, B., Phillips, A., & Steuart, C. (2010). *Guide to computer forensics and investigations*: Cengage Learning.

Neubauer, D., & Meinhold, S. (2012). *Judicial process: law, courts, and politics in the United States*: Cengage Learning.

NFSTC (2009). *A Simplified Guide To Digital Evidence* National Forensic Science Technology Center.

NFSTC, N. F. S. T. C. (2013). *Crime Scene Investigation: A Guide for Law Enforcement*: U.S. Department of Justice. .

Ngobeni, S., Venter, H., & Burke, I. (2010). A forensic readiness model for wireless networks *Advances in Digital Forensics VI* (pp. 107-117): Springer.

NIST. National Institute of Standards and Technology, from http://www.nist.gov/

NIST (2005a). *Computer Forensic Tool Testing*, http://www.cftt.nist.gov/

NIST (2005b). *Digital Forensic*: National Institute of Standards and Technology.

Noblett, M. G. (1995). *Report of the Federal Bureau of Investigation on development of forensic tools and examinations for data recovery from computer evidence.* Paper presented at the Proceedings of the 11th INTERPOL Forensic Science Symposium.

Nokia Windows Phone 8 http://www.nokia.com/my-en/.

Evidence Guide (2010).

OHIOPD. http://www.ohiopd.com

Olsen, G. (2012). *Windows phone 8 security*. Paper presented at the Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices.

Olsson, J., & Boldt, M. (2009). Computer forensic timeline visualization tool. *Digital Investigation, 6*, S78-S87.

Overill, R. E., Kwan, Y., Chow, K., Lai, K., & Law, Y. (2009). A cost-effective digital forensics investigation model. *Proc. 5th Annual IFIP WG, 11*, 193-202.

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.

Oxygen Forensics http://www.oxygen-forensic.com/en/.

Palmer, G. (2001). *A road map for digital forensic research*. Utica, New York.

Palmer, G. L. (2002). Forensic analysis in the digital world. *International Journal of Digital Evidence, 1*(1), 1-6.

ParabenForensics-MobileFieldKit https://www.paraben.com/mobile-field-kit.html.

Park, J., Chung, H., & Lee, S. (2012). Forensic analysis techniques for fragmented flash memory pages in smartphones. *Digital Investigation, 9*(2), 109-118.

Park, W., Na, O., & Chang, H. (2014). An exploratory research on advanced smart media security design for sustainable intelligence information system. *Multimedia Tools and Applications*, 1-12.

Petroni Jr, N. L., Walters, A., Fraser, T., & Arbaugh, W. A. (2006). FATKit: A framework for the extraction and analysis of digital forensic data from volatile system memory. *Digital Investigation, 3*(4), 197-210.

Pilli, E. S., Joshi, R. C., & Niyogi, R. (2010). Network forensic frameworks: Survey and research challenges. *Digital Investigation, 7*(1), 14-27.

Pollitt, M. (2010). A history of digital forensics *Advances in Digital Forensics VI* (pp. 3-15): Springer.

Prosise, C., Mandia, K., & Pepe, M. (2003). *Incident response & computer forensics*: McGraw-Hill/Osborne.

Punja, S. G., & Mislan, R. P. (2008). Mobile device analysis. *Small Scale Digital Device Forensics Journal, 2*(1), 1-16.

Ramabhadran, A. (2007). Forensic investigation process model for Windows Mobile devices. *Tata Elxsi Security Group*, 1-16.

RCFL National Program Office Regional Computer Forensics Laboratory, Quantico, Virginia

Rehault, F. (2010). Windows mobile advanced forensics: An alternative to existing tools. *Digital Investigation, 7*(1), 38-47.

Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence, 1*(3), 1-12.

Rekhis, S., & Boudriga, N. (2012). A system for formal digital forensic investigation aware of anti-forensic attacks. *Information Forensics and Security, IEEE Transactions on, 7*(2), 635-650.

Researcher to Recover Mobile Info. http://news.bbc.co.uk/1/hi/wales/7374221.stm

Ruibin, G., Yun, T., & Gaertner, M. (2005). Case-relevance information investigation: binding computer intelligence to the current computer forensic framework. *International Journal of Digital Evidence, 4*(1), 1-13.

Saferstein, R. (2004). Criminalistics: An introduction to forensic science.

SANS-SIFT. http://digital-forensics.sans.org/community/downloads

SANS. SANS Inisititute, from http://www.sans.org/

Shahpasand, M., & Mahmod, R. Windows Phone 8 Crime Case Managment.

Shahpasand, M., Mahmod, R., Dehghantanha, A., & Udzir, N. I. Forensics of Skype on Windows and Windows Phone.

Shahpasand, M., Mahmod, R., Dehghantanha, A., & Udzir, N. I. A quick reference for Windows Phone 8 investigators.

Shahpasand, M., Mahmod, R., Dehghantanha, A., & Udzir, N. I. Set of Location, Time and Date Clues on Mobile Phones.

Shahpasand, M., Mahmod, R., Dehghantanha, A., & Udzir, N. I. Windows Phone 8 Active Data Collection, Examination and Analysis.

Shahpasand, M., Mahmod, R., & Udzir, N. I. An Audit and Report System for Mobile Phone Investigation Process.

Shahpasand, M., Mahmod, R., & Udzir, N. I. Data Acquisition and Preservation on Close Source Phone Operating System

Shahpasand, M., Mahmod, R., & Udzir, N. I. Source identifications, Signatures and metadata in Mobile Phones.

Shahpasand, M., Mahmod, R., & Udzir, N. I. Standard data set for mobile phone forensic.

Shahpasand, M., Mahmod, R., & Udzir, N. I. Standards and Rules Guideline for Mobile Phone Investigation.

Shahpasand, M., Mahmod, R., & Udzir, N. I. Windows Phone 8 Crime Scene Investigation.

Shenoi, S. (2010). *Advances in Digital Forensics VI*: Springer.

Shields, C., Frieder, O., & Maloof, M. (2011). A system for the proactive, continuous, and efficient collection of digital forensic evidence. *Digital Investigation, 8*, S3-S13.

Sleuthkit-Autopcy http://www.sleuthkit.org/.

Smith.Fred, & Bace.Rebecca (2003). *A Guide to Forensic Testimony: The Art and Practice of Presenting Testimony As An Expert Technical Witness*.

Stebbins, R. A. (2001). *Exploratory research in the social sciences* (Vol. 48): Sage.

Sustainable Agriculture Network (2012). *CHAIN OF CUSTODY STANDARD*: www.sanstandards.org – www.rainforest-alliance.org.

Sutherland, I., Evans, J., Tryfonas, T., & Blyth, A. (2008). Acquiring volatile operating system data tools and techniques. *ACM SIGOPS Operating Systems Review, 42*(3), 65-73.

SWGDE (2005). Scientific Working Group on Digital Evidence. *ASCLD Glossary Definitions*, h ttp://www.swgde.org .

SWGDE (2012). *Best Practices for Mobile Phone Examinations* Scientific Working Group on Digital Evidence.

SWGDE and SWGIT (2011). *Digital & Multimedia Evidence Glossary*.

Sylve, J., Case, A., Marziale, L., & Richard, G. G. (2012). Acquisition and analysis of volatile memory from android devices. *Digital Investigation, 8*(3), 175-184.

Tanner, A. L., & Adviser-Dampier, D. A. (2010). *A concept mapping case domain modeling approach for digital forensic investigations.* Mississippi State University.

Thing, V. L., Ng, K.-Y., & Chang, E.-C. (2010). Live memory forensics of mobile phones. *Digital Investigation, 7,* S74-S82.

Thomas, P., Owen, P., & McPhee, D. (2010). *An analysis of the digital forensic examination of mobile phones.* Paper presented at the Next Generation Mobile Applications, Services and Technologies (NGMAST), 2010 Fourth International Conference on.

TrÄ • ek, D., Abie, H., Skomedal, Ã. s., & Starc, I. (2010). Advanced Framework for Digital Forensic Technologies and Procedures*. *Journal of forensic sciences, 55*(6), 1471-1480.

Tsai, L. C. F. (2014). Federal Bureau of Investigation. *The Encyclopedia of Criminology and Criminal Justice*.

Turnbull, B., & Slay, J. (2008). *Wi-Fi network signals as a source of digital evidence: Wireless network forensics.* Paper presented at the Availability, Reliability and Security, 2008. ARES 08. Third International Conference on.

U.S. Department of Justice (2007). *Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors* Office of Justice Programs National Institute of Justice.

U.S. Department of Justice (2009). *Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders* U.S. Department of Justice Office of Justice Programs.

U.S. General Accounting Office. Crime Technology: Department of Defense Assistance to State and Local Law Enforcement Agencies, Report GAO/GGD-00-14, Washington, DC from fas.org/irp/gao/ggd-00-014.htm

United States Secret Service (2010). *Best Practices For Seizing Electronic Evidence v.3, A Pocket Guide for First Responders*: U.S. Department of Homeland Security.

Van Eijk, O., & Roeloffs, M. (2010). Forensic acquisition and analysis of the Random Access Memory of TomTom GPS navigation systems. *Digital Investigation, 6*(3), 179-188.

Vatis, M. (2002). Law enforcement tools and technologies for investigating cyber attacks. *Dartmouth College*.

Venter, J. (2006). Process flow diagrams for training and operations *Advances in Digital Forensics II* (pp. 331-342): Springer.

Vomel, S., & Freiling, F. C. (2011). A survey of main memory acquisition and analysis techniques for the windows operating system. *Digital Investigation, 8*(1), 3-22.

Vomel, S., & Freiling, F. C. (2012). Correctness, atomicity, and integrity: defining criteria for forensically-sound memory acquisition. *Digital Investigation, 9*(2), 125-137.

Vomel, S., & Stuttgen, J. (2013). An evaluation platform for forensic memory acquisition software. *Digital Investigation, 10,* S30-S40.

Wagner, I. (2013). A new jitter-algorithm to quantify hoarseness: an exploratory study. *International Journal of Speech Language and the Law, 2*(1), 18-27.

Walls, R. J., Levine, B. N., Liberatore, M., & Shields, C. (2011). *Effective digital forensics research is investigator-centric.* Paper presented at the Proc. USENIX Workshop on Hot Topics in Security (HotSec).

Ward, A. (2012). *Deciding to leave: The politics of retirement from the United States Supreme Court*: SUNY Press.

Whitcomb, C. M. (2002). An historical perspective of digital evidence: A forensic scientistâ€™s view. *International Journal of Digital Evidence, 1*(1), 7-15.

Wilkinson, S., & Haagman, D. (2010). Good practice guide for computer-based electronic evidence. *Association of Chief Police Officers*.

Willassen, S. (2003). Forensics and the GSM mobile telephone system. *International Journal of Digital Evidence, 2*(1), 1-17.

Williamson, B., Apeldoorn, P., Cheam, B., & Mcdonald, M. (2006). *Forensic analysis of the contents of Nokia mobile phones.* Paper presented at the Australian digital forensics conference.

Windows Phone 8. http://www.windowsphone.com/en-my

Windows Phone 8 Forum. http://forums.windowscentral.com/windows-phone-8/

Windows Phone Forum. http://forum.xda-developers.com/windows-phone-8

Yates, I. (2010). *Practical investigations of digital forensics tools for mobile devices.* Paper presented at the 2010 Information Security Curriculum Development Conference.

Yates, M., & Chi, H. (2011). *A framework for designing benchmarks of investigating digital forensics tools for mobile devices.* Paper presented at the Proceedings of the 49th Annual Southeast Regional Conference.

Yu, X., Jiang, L.-H., Shu, H., Yin, Q., & Liu, T.-M. (2009). A process model for forensic analysis of Symbian smart phones *Advances in Software Engineering* (pp. 86-93): Springer.

Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common phases of computer forensics investigation models. *International Journal of Computer Science & Information Technology (IJCSIT), 3*(3), 17-31.