Research Journal of Applied Sciences, Engineering and Technology 8(3): 358-366, 2014
DOI:10.19026/rjaset.8.981
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: February 25, 2014 Accepted: May 19, 2014 Published: July 15, 2014

Research Article

A Review on Mobile Device's Digital Forensic Process Models

Anahita Farjamfar, Mohd Taufik Abdullah, Ramlan Mahmod and Nur Izura Udzir
Security Research Group, Faculty of Computer Science and Information Technology,
University of Putra Malaysia, Serdang, Selangor, 43400, Malaysia

Abstract: The main purpose of this study is to discuss the different comparative studies on digital forensics process models specially in the field of mobile devices. In order to legally pursue digital criminals, investigation should be conducted in a forensically sound manner so that the acquired evidence would be accepted in the court of law. Digital forensic process models define the important steps that should be followed to assure the investigation is performed successfully. There are a number of digital forensic process models developed by various organizations worldwide, but yet, there is no agreement among forensics investigation and legislative delegation which procedures to adhere to; specially in the case of facing mobile devices with latest technologies. This is vital, as mobile phones and other mobile devices such as PDAs or tablets are becoming ever-present as the main technology platform around the world and people are obtaining and using mobile phones more than ever. In this study we will give a review of the proposed digital forensics process models within last 7 years and to discuss the need for a consensus to follow the same underlying approaches while continually updating digital forensics process models to cover new emerging technologies and devices.

Keywords: Digital evidence, digital forensics, mobile forensic

INTRODUCTION

The majority of organizations rely deeply on digital devices and they are shifting to use mobile devices such as PDAs or tablets to operate and improve their business. Such businesses depend on digital devices to process, store and recover data. A large amount of created information is collected and distributed via mobile devices. Mobile devices despite their small sizes which can be carried around in a pocket, are becoming more functional due to enhancements in semiconductor technologies and computing power. Traditional computers sit on one end of digital forensics spectrum where the methods and processes are reliable and consistent. Cell phones, along with their quick hardware and software alterations, fit on the other end of the spectrum. Smart phones fall somewhere in the middle of this spectrum. Smart phones are mobile phones built on a mobile operating system, with more advanced computing capability and highly developed communication features including Wireless and Bluetooth. Using these new generation of phones, users are able not only to make and receive phone calls, but also browse the Internet, chat, send and receive text/multimedia messages as well as view and edit PDF, Excel and PowerPoint files. They store data almost like a laptop while function like a cell phone. Smartphone's diversity of manufacturers, hardware structure and operating system merged with the regular connection to a network, cause forensically sound methods to lag behind technologies in progress.

On the other hand, the continued growth of the mobile devices market and their advanced features provide the opportunity of utilizing them in criminal activities leading to security risks where these devices are used for carrying out digital crimes or being the target of a security attack due to their predominant use by employees at various enterprises. Ironically, while it has taken decades to convince legal businesses that mobile connectivity can develop their functions, more or less, anyone involved at any level of crime since 1980s have already realized how to take advantage of mobile phones. Therefore, forensic investigators found that mobile devices have become a potential source of digital evidence in criminal investigations which can be essential in capturing critical information to accuse a suspect that compromises a digital device. The objective of this study is to deliver an overview on digital forensic investigation process models especially for mobile devices with the purpose of highlighting that digital forensic community require to reach to a general agreement regarding pursuit of identical fundamental yet flexible approaches which are updatable for new emerging technologies and devices.

Corresponding Author: Mohd Taufik Abdullah, Security Research Group, Faculty of Computer Science and Information Technology, University of Putra Malaysia, Serdang, Selangor, 43400, Malaysia, Tel.: 03-89471724

METHODOLOGY

We are aiming to review different digital forensics process models especially in the field of mobile devices. For this purpose, we have studied different papers related to this topic and we will provide a brief review of these studies. In the area of digital forensics, hundreds of process models have been proposed all over the world. This review will only contain thirteen published papers that represent the Digital Forensics Investigation Framework with their respective processes or activities since 2007, as there are some review papers which already discussed and categorized models proposed from 1995 through 2007; reviews such as Selamat and Yusof (2008) which addressed thirteen digital forensic process models or Pollitt (2007) which presented a brief introduction of fourteen published papers from 1995 to 2006 all on development of digital forensic models.

LITERATURE REVIEW

Digital evidence and its characteristics: According to the Scientific Working Group on Digital Evidence SWGDE (2006), Digital Evidence is "information of probative value that is stored or transmitted in binary form". Based on this definition, digital evidence includes evidence on any digital devices such as portable media players, digital cameras or telecommunication devices and not merely limited to those found on computers. Moreover, digital evidence has been expanded to include every category of crime where digital evidence can be found and be used as the proof; it is not bounded only to traditional computer crimes like hacking and intrusion (Ghosh, 2004). Digital evidence covers any digital data that can confirm that a crime has been committed or can provide a link between a crime and its victim or a crime and its executor. In general, it can be said that digital evidence is a sequence of binary digit numbers on transmission or information files stored on the electronic device. The digital evidence file formats include digital images, text, audio and video, etc., (SWGDE, 2006).

The International Organization on Computer Evidence (IOCE) (2002), defines digital evidence as "any information in digital form with an appropriate attestation or liberating value or value of reasonable doubt and it is stored or transmitted in digital form." The digital evidence can be copied with limitless diversities, can be modified easily and cannot be understood directly without technical process. Identifying original resources of such evidences is very difficult as well. There are five properties the evidence must have in order to be useful: admissibility, authenticity, completeness, reliability and believability.

Digital evidences from a Smartphone may include missed, dialed, received calls, SMS, MMs, phonebook\contacts, calendars, photos, videos and notes. As smart phones have internet connection capability, they may contain web browser history, emails, social networking contacts, messages and vocational information. Digital evidence of a mobile device can be retrieved from the SIM (Subscriber Identity Modules) card, mobile internal flash memory or its SD (Secure Digital) card.

Table 1: The NIST categorization of smart phone digital evidences

Class	Digital evidence
Smart phone memory	Device ID number, date and language setting, address book, pictures, e-mail, browser history, SMS, media
SIM card	PIN code, PUK code, IMEI, IMSI
Memory card	Deleted videos, pictures, files

The National Institute of Standards and Technology (NIST), divides digital evidences of smart phones into three parts based on their storage location in SIM card, smart phone memory and SD card memory as shown in Table 1 (Lin *et al*., 2011).

In mobile device forensics, evidences are divided into several categories based on the type of mobile device and services it provides to the user (Spalevic *et al*., 2012). The categories are as follows.

User ID is utilized in network providers for mobile phones as the user's authentication tool and verification to the types of services available for users. Mobile device is identified by an international number for Identification of Mobile devices (IMEI). The SIM card contains a number labeled as international number for identification of users (IMSI) used for registering to a system, a secret code for verification and other information. IMEI and IMSI numbers are independent, which provides users' mobility. SIM card can be protected from unauthorized access by personal identification number, PIN, or a password.

Diary of mobile devices often contains timely arranged lists of incoming, missed, replied and selected numbers, as well as GPS information, connection moments on appropriate network cells and moment of connection termination with network cells. This information can lead to a very precisely controlled location of the user in a specific moment of time.

Contacts which may contain photos, email addresses, physical addresses, alternative phone numbers and many other useful information on individuals in Contacts, can be considered a list of potential witnesses, victims or accomplices.

Text messages contain segments of evidence and time indicators which are very valuable in an investigation. Modern forensic methods let reconstruction and tracing of damaged or deleted messages.

Calendar can indicate the user's movement, commitments, or individuals they had contacted.

Electronic mail provides information on internet communication of the suspect.

Instant messages are messages exchanged in real time and may contain complete conversations and time indicators.

Images, audio records, multimedia messages: Application documents represent documents that can be

generated in some modern mobile devices in the form of calculation, presentation and other document formats.

SD cards and backup files often serve for data transfer from a computer to a mobile device and vice versa and therefore may contain important evidences to be investigated.

Mobile forensics: Digital forensics is a science concerning identification, collection, preservation, storage, analysis and documenting of digital evidence or data that has been stored, processed or transferred in digital form. In general, digital forensics is divided into five branches namely computer forensics, software forensics, data forensics, network forensics and mobile device forensics. Mobile device forensics covers recovery of digital evidence or data from a mobile device using accepted methods in forensically sound manner which include analysis of both SIM card and phone memory. The phrase 'mobile device' often applies to mobile phones. However, it includes any digital device that has both internal memory and communication capability, including PDA devices, GPS devices and tablet computers. Study of mobile device forensics is a fairly new subject which has been at work approximately since the early 2000s.

According to Ramabhadran (2007), there are some dissimilarities between computer forensics and mobile device forensics. These differences are related to the special features of mobile devices which includes:

- A wide range of hardware models and accessories
- Variety of different embedded operating systems
- Short product cycle with new models emerging very frequently
- Extreme orientation towards mobility
- File system residing in volatile memory on certain devices while in non-volatile on some others
- Hybrid devices with advanced networking and communication features
- Suspending processes when switched off or idle, while the device is active in the background

A comparative study of different mobile operating systems used in various mobile phones has been conducted by Ali (2014). The author has done analysis based on various parameters such as future perspectives, reliability, security, etc. Computer forensics and smart phone forensics are furthermore dissimilar in terms of operating systems and files storing locations. In a computer, the operating system is stored in the secondary memory, while in a smart phone, it is stored in the Read Only Memory (ROM). In a computer, files are stored in the secondary memory, whereas files in a smart phone are stored in the Random Access Memory (RAM). In computer forensics, bit-by-bit-copy methods can be done by isolating the device and removing the hard drive to dump the memory to a image file. While in a mobile device, isolating the phone from any radio signal could result in draining the battery. This is because the phone tries unsuccessfully to connect to a network which leads to power consumption. Besides, the smart phone forensics process must be done in the power-on state.

Some difficulties faced by forensic investigators dealing with mobile phones come from proprietary hardware, a wide array of chargers and connection socket and cable types for connecting a mobile phone to a computer and discrepancy of particular versions of an OS on different manufacturer's hardware according to Daware *et al*. (2012). Smart phones are equipped with a comprehensive architecture, containing ROM, RAM, memory controller, CPU, data bus, Digital Signal Processor (DSP), radio frequency hardware, a range of hardware keyboard and interface, LCD, etc. Many types of mobile phones are embedded with the flash memory. Flash memory is a non-volatile memory i.e., it is erasable and rewritable and, therefore, making it easier for developers of smart phones OS to upgrade or port. Flash has special properties which could be important from forensics point of view. For example, as data has to be copied from flash to RAM to be updated and then copied back to another empty location in flash, data prior to change could be accessible using some acquisition methods. NOR and NAND are two types of flash memory. NOR flash is faster, although it takes longer to erase and write new data. This kind of flash memory is also more expensive. So far, NOR has been used mostly in mobile phones. This kind of flash is mapped in the memory space of the processor and processor code can directly be executed from NOR, but it can also be used as user data storage. NAND, which is almost corresponding to a hard disk, has significantly higher storage capacity than NOR. This kind is not mapped in the processor's memory map. Therefore, the code stored in it cannot be executed directly and needs to be loaded first into RAM. A number of devices could use both these flashes. For instance a Smartphone may be equipped with NOR for booting the operating system while using a removable NAND card for its other memory or storage requirements.

Basic hardware diagram of a smart phones device is shown in Fig. 1.

Digital devices mainly have only two different states On or Off, whereas mobile devices can be in any of the states explained below, at a given point of time. These states and the transition mediums have been shown in Fig. 2.

Nascent state: The device is in factory configuration settings and contains no user data. For entering into this state the device must be charged for a minimum amount of time. By allowing the battery to discharge totally or by doing a hard reset of the device at any time, this state can be achieved but any user action will convert the state to another one.

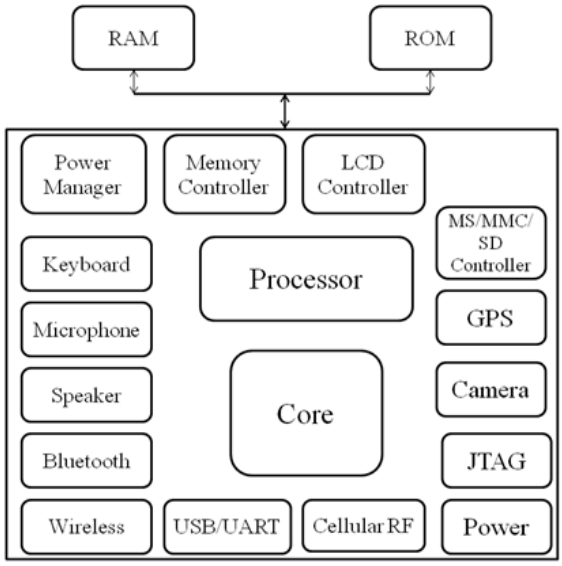

Fig. 1: Smartphone generic hardware diagram

Active state: Whenever the device is powered on and the user is performing some tasks and the file system has data, it means that the device is in this state. Clearing the working memory by doing a soft reset, will result in a transition to this state.

Quiescent state: This state is achieved when the power button is pressed either in active or semi-active state. Also a transition to this state occurs when the inactivity timer expires while in semi-active state. In this state, background tasks are being executed and all user data are being preserved while conserving battery life. However, it seems that device is in the inactive mode. Generally, the device is considered to be 'off', if it is in the quiescent state and 'on' if it is in any other state.

Semi-active state: This state is reached when a timer is triggered after some inactivity duration. In this state, the device is between active and quiescent states. Button pressing, screen tapping or soft reset performing will result in the transition to this state. In this state, battery life is conserved by reducing the backlight and other similar functions.

Digital forensic procedures: During the execution of cyber crime, digital device may be used as the:

- Aim or target of the attack (computer intrusion, theft, data destruction)
- Means of the attack (credit card fraud, sending spam or images)
- Link to regular crime (drug or human trafficking, child pornography)
- Repository of digital evidence of cyber crime

Forensic procedures must be prescribed through legislation and by laws at national level for computer generated and memorized digital evidence to be acceptable by judicial practice. These procedures include:

- Handling, storing and preserving of digital evidence
- Forensic acquisition of evidence
- Examining and analysis of evidence
- Expert opinions and testimonies on digital evidence

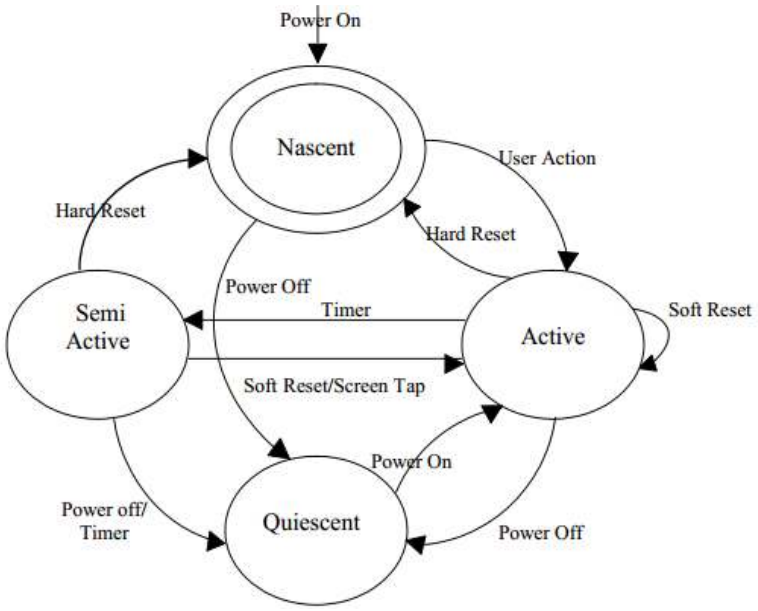

Fig. 2: Generic state of a mobile device (Ramabhadran, 2007)

Digital forensic investigation is commonly categorized into official (public) and corporate (private) investigation as stated by Spalevic *et al*. (2012).

Official digital forensic investigation is conducted by police investigative bodies and special prosecution for cyber crime. This kind of investigation is conducted on the basis of law on criminal procedure, law on combating cyber crime, law on electronic communication, law on protection of information and information systems, law on digital evidence, law on electronic signature and law on electronic commerce. On the basis of "step-by-step" model, the process of official digital forensic investigation, generally involves four phases: initial investigation, tracking the perpetrator, discovering identity of the perpetrator and arrest.

In real cases of cyber crime, at the beginning stages of the investigation, the investigative bodies collect reasonable evidence and put in a claim against the suspect who can also be unknown individual. Official investigation is initiated after a warrant for investigation from investigative judge is provided by the prosecutor and on the basis of police findings. Suspicious computer or communication system can be temporarily seized based on a valid court order, including physical image of the hard disk or memory content of IT system and devices for the purpose of forensic acquisition and data analysis.

Corporate digital forensic investigation is conducted within a corporation and consists of the initial three phases of public investigation. This form of investigation involves corporate digital forensics and administrator of computer networks assisted by experts on physical transfer and data protection in the corporation.

Determining the type of network within which a mobile phone has functioned is essential prior to commencing the investigation. Nowadays, three types of mobile networks are defined according to Yates and Chi (2011):

- CDMA (Code Division Multiple Access) network does not have the SIM module, which means that all the data are saved on the mobile phone. These networks are prevalent in the United State of America (USA).
- GSM (Global System for Mobile communication) networks use SIM module as separate components designed as a transferable element from one to the other device. GSM networks are dominant in Europe.
- IDEN (Integrated Digital Enhanced Network) networks use a system of advanced SIM cards (USIMs) developed by Motorola.

GSM technology has been the most prominent mobile phone technology in the world. Although there are other technologies that are competing with GSM such as 3G, the third generation of mobile technology. From the other perspective mobile phone technologies can be categories as 2G, 3G and 4G.

2G first introduced in 1991, is the second-generation of cellular telephone technology which were commercially launched on the GSM standard and the first to use digital encryption of conversations. 2G networks were the first to offer data services and SMS text messaging, but their data transfer rates are lower than those of their successors.

3G networks succeed 2G ones, offering faster data transfer rates and are the first to enable video calls. This makes them especially suitable for use in modern smart phones, which require constant high-speed internet connection for many of their applications.

4G is the fourth generation of mobile phone communications standards. It is a successor of the 3G and provides ultra-broadband internet access for mobile devices. The high data transfer rates make 4G networks suitable for use in USB wireless modems for laptops and even home internet access.

COMPARATIVE ANALYSIS OF DIGITAL FORENSICS PROCESS MODELS

Early in 2007, Freiling and Schwittay (2007) suggested a new process model for inspecting computer security incidents. To improve the overall investigation process, this model combines the two notions of Incident Response and Computer Forensics. The focus of this model is mostly on analysis. Thus its steps include Pre-Incident Preparation, Pre-Analysis, Analysis and Post-Analysis. All steps and activities which are executed before the real analysis starts are included in Pre-Analysis phase while the Post-Analysis phase is about documenting the written report of the entire actions performed throughout the investigation. In the Analysis Phase, the real analysis occurs. This model integrates the forensic analysis into an Incident Response framework.

Ramabhadran (2007) believe that investigating Windows mobile devices have become challenging for investigators and forensic community due to their technological advancements and popularity. Thus, the author describes a twelve-stage model contacting various processes involved in the forensic investigation of Windows mobile devices, helping forensic practitioners and organizations in setting up appropriate policies and procedures. Preparation, Securing the Scene, Survey and Recognition, Documenting the Scene, Communication Shielding, Volatile Evidence Collection, Non-Volatile Evidence Collection, Preservation, Examination, Analysis, Presentation and Review are the stages in the proposed model. The primary crime investigation relating to Windows mobile devices and those relating to computers has been distinguished in this model. It also divided volatile

and non-volatile evidence collection, each to be done depending on the situation either in crime scene or later at a secure forensic lab. The author has emphasized on Communication Shielding as an important step prior to evidence collection.

Later, Perumal (2009) introduced a new digital forensic process model which covers the complete range of an investigation procedures according to the Malaysian Cyber Law. In order to lead to a better prosecution, the authors have distinguished the live data acquisition stage from the static data acquisition stage in order to focus on fragile evidence. The proposed model consists of seven stages, which are Planning, Identification, Reconnaissance, Analysis, Result, Proof and Defense and Diffusion of Information. Besides that, the Identification stage contain two sub-procedures namely Identifying seized items, Identifying fragile evidence and live acquisition.

The Symbian OSv9.x's security mechanism, which is based on the Trusted Computing, makes many existing smart phones forensics process models inapplicable to Symbian smart phones. Therefore, based on various versions of Symbian smart phones an adaptive process model has been provided by Yu *et al*. (2009) which contains five different stages: Preparation and Version Identification, Remote Evidence Acquisition, Internal Evidence Acquisition, Analysis and Presentation and Review. The Evidence Acquisition stage is adaptive depending on the existence of TCB (Trusted Computing Base), either remote for advanced Symbian smart phones with TCB or internal for early Symbian smart phone without TCB. This model has neglected some important steps such as preservation or transfering of the collected evidences.

Ademu *et al*. (2011) proposed a four-tier iterative approach where the first tier includes four rules for digital forensic investigation which involves Preparation, Identification, Authorization and Communication. The second tier has rules such as Collection, Preservation and Documentation, the third tier has rules consisting Examination, Exploratory Testing and Analysis and the fourth tier which is the Presentation phase has rules such as Result, Review and Report. The model identifies the need for interaction of investigator with available sources and tools. Exploratory testing has been named as another advantage of the model.

The integrated process model proposed by Ademu and Imafidon (2012) has introduced a new step to the digital forensic investigation process. The idea of the model is to add the security mechanism to the layers of digital investigation process, which are Preparation, Interaction, Reconstruction and Presentation, to assist reviewing the security needs and requirements of any digital forensic investigation and to ensure they are met during the investigation.

Cohen (2010) proposed a process model that includes the following phases: Identification, Collection, Preservation, Transportation, Storage, Analysis, Interpretation, Attribution, Reconstruction, Presentation and Destruction.

Casey (2009) defines phases of digital forensic investigation process as: Gathering Information and Making Observations to form a hypothesis explaining observations, Evaluating the Hypothesis, Drawing Conclusions and Communicating the Findings.

Cohen *et al*. (2011) discussed the state of the science of digital evidence examination and consensus in digital evidence examination. They recognize that numerous calls have been made for scientific approaches and formal methods in the field of digital forensics (Cohen *et al*., 2011; Leigland and Krings, 2004; Hankins *et al*., 2009; National Research Council, 2009; SWGDE, 2009; Garfinkel *et al*., 2009).

Valjarevic and Venter (2012) discussed the need for an international standard formalizing the digital forensic investigation process and consequently proposed an iterative, multi-tier harmonized digital forensic investigation process model. In order to achieve the highest efficiency of the investigation and admissibility of the digital evidence, the authors have introduced the term "parallel actions". These are principles that should be translated into actions within the digital forensic investigation process and should be run parallel with the phases and span across several or all phases and not to be limited to a specific phase. This harmonized model contains the following twelve phases: Incident Detection, First Response, Planning, Preparation, Incident Scene Documentation, Potential Evidence Identification, Potential Evidence Collection, Potential Evidence Transportation, Potential Evidence Storage, Potential Evidence Analysis, Presentation and Conclusion. The defined parallel actions comprise obtaining authorization, documentation, defining the information flow, preserving the chain of evidence, preserving evidence and interaction with the physical investigation.

According to Owen and Thomas (2011) guidelines and research into the forensic examination of hard disk drives are much more established compared with those related to mobile devices. The NIST guidelines by Jansen and Ayers (2007) can be used as a starting point for forensic capabilities development rather than legal advice. On the other hand, the ACPO (2007) guidelines give the lawful principles and considerations to ensure the integrity of evidences while they need some updated guidance on how mobile devices should be handled by law enforcements during an investigation. Both these prominent guidelines require modernizing as mobile devices are continuously evolving and their features become more pervasive.

Research conducted by Parvez *et al*. (2011) argues the need for model specific frameworks for investigation of mobile devices and thus a proper framework for investigating Samsung Star 3G has been proposed. Also the framework is claimed to be quite useful such that some of its procedure could be proposed for the investigation of other phones and portable devices. Authorization, First Response, Device Transportation, Live Acquisition, Maintenance and Evidence Analysis are the procedure components of this framework. Besides that, the authors have conducted an experiment to determine if aluminum foil is an alternative solution for signal isolation in the cases when isolation bags are not available and their results confirm the claim.

The operating procedure introduced by Lin *et al*. (2011) has been discussed and compared to the Standard Operating Procedures proposed by NIST in Lin *et al*. (2011). The Smart-Phone Digital Evidence Forensics Standard Operating Procedure (Smart-Phone DEFSOP) is divided into four phases, comprising of Conception, Preparation, Operation and Reporting. The Operation phase is divided into three processes, including collection, analysis and forensics. The model has considered law and principles as the first phase in order to assist other phases and legitimate digital evidences. Contrary to NIST, it also includes training and preparation prior to the forensics procedure. The authors believe that Acquisition and Examination/ Analysis are technical, so it is essential to put them in a single phase (Operation phase). They strongly believe that this model is more reliable than NIST as digital evidence legitimacy is considered.

Goel *et al*. (2012) exploits a fourteen stage model to explore the forensic investigation of Smartphone and its involved processes. Keeping in mind that the standard techniques and methods in the digital investigation world are incorporated to those in physical investigation world, the paper proposed the stages as Preparation, Securing the scene, Documentation, PDA Mode, Communication Shielding, Volatile Evidence Collection, non-Volatile Evidence Collection, Off Set, Cell Site Analysis, Preservation, Examination, Analysis, Presentation and Review. This model has facilitated mode selection, to decide if the device is in the On mode then it should be moved to communication shielding so that potential vulnerable volatile evidences remain intact, else if the device is in Off mode it is advised not to turn it On and avoid any data overwriting. Thus the investigator should shift to the collection stage. One of the newly introduced stages of the model is Off Set analysis. Smart phones are now equipped with cloud computing which is an advantage to store their personal data online to overcome mobile storage limits and access the data anywhere anytime from any device. This could raise the likelihood of hiding the criminal evidence online which is not easy to be tracked from the device. Special consideration needs to be given to see what online data transactions have been made to have a track of activities performed. Cell Site Analysis is associated with the science of locating the geographical area of the phone whenever calls, SMS or downloads are made or received, either in real time or historically. However, this information is part of evidence collection and examination in every investigation.

Three core matters which can be recognized from the mentioned models include repetitiveness in some processes, proposed focus area and characteristics of models. To name a few, Ramabhadran (2007) and Ademu *et al*. (2011) have process redundancies in their proposed model. The focus of Perumal (2009) and Goel *et al*. (2012) were on the issue of evidence acquisition, whereas Perumal (2009) on analysis process. Frameworks by Valjarevic and Venter (2012) and Parvez *et al*. (2011) have practicality and specificity as their characteristics which are essential for the process of investigation. The focus of existing guidelines and procedures are mostly on the collection of digital evidence, while provide less guidance on the forensic analysis of the evidences that these systems and devices may contain. Each model has its own strong points; however, from the variety of proposed frameworks it is unclear that the forensics procedures should be in general and standard form or should be model/OS specific, especially in the mobile device arena with the wide variety of models and proprietary operating systems.

CONCLUSION

The facts revealed by reviewing previous models have shown some redundancies in performing the steps of various phases even if different terminologies have been used. The study also revealed the focus area of proposed models in addition to their characteristics. The varying frameworks developed are such that they mostly work well with one particular type of investigation. There is still disagreement among forensic practitioners and law enforcement officials, whether investigation procedures should be model specific for each device, or should be comprehensive enough to be used as a standardized set of guidelines in the order of events for expediting investigations. What is generally accepted is that in order to be able to claim in the court that a trusted process has been used during a digital forensic investigation a proven digital forensic investigation process model should be adhered to. Daubert Rule (2001), most prominently used in the USA for expert witness testimony, including digital forensics experts, clearly states that theories and techniques used to draw conclusions on a case must give positive answers to the following questions: whether the theories and techniques employed by the

scientific expert have been tested, whether they have been subjected to peer review and publication, whether the techniques employed by the expert have a known error rate, whether they are subject to standards governing their application and whether the theories and techniques employed by the expert enjoy widespread acceptance. On the other hand, lately new technologies and devices are released which no guidelines or procedures precisely covers them. In the reviewed models there was no explicit model for Android or iphone mobile devices while as they are the predominant in the market. Therefore, authors believe that in order to ensure thoroughness and consistency of forensic procedures, underlying approaches for evidence handling, should remain the same while forensics process models should constantly be updated to cover high technology evidences.

REFERENCES

ACPO (The Association of Chief Police Officers), 2007. Good Practice Guide for Computer-based Electronic Evidence Version 4. England, Wales and N. Ireland. Retrieved form: http://www.acpo.police.uk.

Ademu, I.O. and C.O. Imafidon, 2012. Applying security mechanism to digital forensic investigation process. Int. J. Emerg. Trends Eng. Dev., 7(2): 128-133.

Ademu, I.O., C.O. Imafidon and D.S. Preston, 2011. A new approach of digital forensic model for digital forensic investigation. Int. J. Adv. Comput. Sci. Appl., 2(12): 175-178.

Ali, A., 2014. A review of different comparative studies on mobile operating system. Res. J. Appl. Sci. Eng. Technol., 7(12): 2578-2582.

Casey, E., 2009. Handbook of Digital Forensics and Investigation. Access Online via Elsevier, Forensic Analysis.

Cohen, F.B., 2010. Fundamental of digital forensic evidence. In: Stavroulakis, P.P. and M. Stamp (Eds.), 1st Edn., Handbook of Information and Communication Security. Springer, pp: 789-808, 10.1007/978-1-84882-684-7.

Cohen, F.B., J. Lowrie and C. Preston, 2011. The state of the science of digital evidence examination. Int. Fed. Info. Proc., 7: 3-21.

Daubert Rule, 2001. Merrell Dow Pharmaceuticals. Inc., 509 U. S. 579 (1993), Federal Rules of Evidence, as amended, 28 U.S.C., Rule 702.

Daware, S., S. Dahake and V.M. Thakare, 2012. Mobile forensics : Overview of digital forensic, computer forensics vs. mobile forensics and tools. Int. J. Comput. Appl., 2012: 7-8.

Freiling, F.C. and B. Schwittay, 2007. A common process model for incident response and computer forensics. Journal = {IMF}, 7: 19-40.

Garfinkel, S., P. Farrell, V. Roussev and G. Dinolt, 2009. Bringing science to digital forensics with standardized forensic corpora. Digit. Invest., 6: S2-S11.

Ghosh, A., 2004. Guidelines for the management of IT evidence. Incident Response and Forensics Workshop, Document No telwg29/ IRF/04a.

Goel, A., A. Tyagi and A. Agarwal, 2012. Smartphone forensic investigation process model. Int. J. Comput. Sci. Secur. (IJCSS), 6(5): 322-341.

Hankins, R., T. Uehara and J. Liu, 2009. A comparative study of forensic science and computer forensics. Proceeding of 3rd IEEE International Conference on Secure Software Integration and Reliability Improvement, pp: 230-239.

International Organization on Computer Evidence (IOCE), 2002. Guidelines for Best Practice in the Forensic Examination of Digital Technology. Retrieved form: http://www.ioce.org/fileadmin/user_upload/2002/ioce_bp_exam_digit_tech.html.

Jansen, W. and R. Ayers, 2007. Guidelines on cell phone forensics. NIST Special Publication (SP) 800-101, Gaithersburg, MD.

Leigland, R. and A.W. Krings, 2004. A formalization of digital forensics. Int. J. Digit. Evidence, 3(2): 1-32.

Lin, I.L., H.C. Chao and S.H. Peng, 2011. Research of digital evidence forensics standard operating procedure with comparison and analysis based on smart phone. Proceeding of International Conference on Broadband and Wireless Computing, Communication and Applications, pp: 386-391.

National Research Council, 2009. Strengthening Forensic Science in the United States: A Path Forward. ISBN: 0-309-13131-6, pp: 352.

Owen, P. and P. Thomas, 2011. An analysis of digital forensic examinations: Mobile devices versus hard disk drives utilising ACPO and NIST guidelines. Digit. Invest., 8(2): 135-140.

Parvez, S., A. Dehghantanha and H.G. Broujerdi, 2011. Framework of digital forensics for the Samsung star series phone. Proceeding of 3rd International Conference on Electronics Computer Technology (ICECT, 2011), 2: 264-267.

Perumal, S., 2009. Digital forensic model based on Malaysian investigation process. Int. J. Comput. Sci. Network Secur., 9(8): 38-44.

Pollitt, M.M., 2007. An ad hoc review of digital forensic models. Proceeding of 2nd International Workshop on Systematic Approaches to Digital Forensic Engineering, pp: 43-54.

Ramabhadran, A., 2007. Forensic investigation process model for windows mobile devices. Tata Elxsi Security Group, pp: 1-16.

Selamat, S. and R. Yusof, 2008. Mapping process of digital forensic investigation framework. Int. J. Comput. Sci. Network Secur., 8(10): 163-169.

Spalevic, Z., Z. Bjelajac and M. Caric, 2012. The importance and the role of forensics of mobile. FACTA Univ., Ser. Electr. Energ., 25(2): 121-136.

SWGDE, 2006. SWGDE and SWGIT Digital and Multimedia Evidence Glossary. [Online]. Retrieved form: https://www.swgde.org/documents/swgde2005/SWGDEandSWGITCombinedM (Accessed on: Aug. 18, 2008).

SWGDE, 2009. Scientific Working Group on Digital Evidence (SWGDE). Retrieved form: https://www.swgde.org/documents/Archived%20Documents/2009-05-22%20SWGDE- SWGIT%20Digital%20and%20Multimedia%20Evidence%20Glossary%20v2.3. pp: 1-6.

Valjarevic, A. and H.S. Venter, 2012. Harmonised digital forensic investigation process model. Proceeding of Information Security for South Africa (ISSA, 2012), pp: 1-10.

Yates, M. and H. Chi, 2011. A framework for designing benchmarks of investigating digital forensics tools for mobile devices. Proceedings of the 49th Annual Southeast Regional Conference on ACM-SE '11, pp: 179-184.

Yu, X., L.H. Jiang, H. Shu, Q. Yin and T.M. Liu, 2009. A process model for forensic analysis of Symbian smart phones. In: Slezak, D. *et al*. (Eds.), ASEA 2009. CCIS 59, Springer-Verlag, Berlin, Heidelberg, pp: 86-93.