Impact Factor:	ISRA (India) = 1.344	SIS (USA) = 0.912	ICV (Poland) = 6.630
	ISI (Dubai, UAE) = 0.829	РИНЦ (Russia) = 0.179	PIF (India) = 1.940
	GIF (Australia) = 0.564	ESJI (KZ) = 1.042	
	JIF = 1.500	SJIF (Morocco) = 2.031	

SOI: 1.1/TAS DOI: 10.15863/TAS

International Scientific Journal

Theoretical & Applied Science

p-ISSN: 2308-4944 (print) **e-ISSN:** 2409-0085 (online)

Year: 2016 **Issue:** 1 **Volume:** 33

Published: 30.01.2016 **http://T-Science.org**

SECTION 5. Innovative technologies in science.

Muhammad Sadiq
CRIDS (Center for Research in Distributed and Supercomputing) RIU.
muhammad.sadiq@crids.org

Muhammad Shahid Iqbal
School of Computer Science, Anhui University, Hefei, China
nawabishahid@yahoo.com

Khawar Naveed
CRIDS (Center for Research in Distributed and Supercomputing) RIU.
knaveedpak@yahoo.co.uk

Muhammad Sajad
CRIDS (Center for Research in Distributed and Supercomputing) RIU.
muhammad.sajad@crids.org

MOBILE DEVICES FORENSICS INVESTIGATION: PROCESS MODELS AND COMPARISON

Abstract: *The new era of smart devices have evolved in the last few years which has facilitated general public in fulfilling their need with fast and efficient communication devices. These devices in the hands of antisocial activists can cause great harm to public. Due to wide range of smart phones available in the market, an ultimate forensics investigation framework is very difficult to reach. This paper outlines a review of some of the previously used mobile forensics investigation models and also compares the NIST guidelines of cell phone forensics with the other SOPs and available models. Also important stages of the data acquisition as well as for further investigation are identified and used in the new unified mobile devices forensics investigation model.*

Key words: *Forensics, investigation, cell phones, SOP.*

Language: *English*

Citation: Sadiq M, Iqbal MS, Naveed K, Sajad M (2016) MOBILE DEVICES FORENSICS INVESTIGATION: PROCESS MODELS AND COMPARISON. ISJ Theoretical & Applied Science, 01 (33): 164-168.

Soi: http://s-o-i.org/1.1/TAS-01-33-29 ***Doi***: crossref http://dx.doi.org/10.15863/TAS.2016.01.33.29

I. INTRODUCTION

Mobile phone technology is basically a complicated technology. Innovation in the technology of mobile phones make forensics of mobile devices more complex and complicated. A major contributor that increase complexity of the forensics of mobile devices is variety of mobile manufactures in the market each having its proprietary software and hardware formats and standards.

Presently, mobile devices are used by millions people. The advancements in the technology not only focus features but also, its design and size, which attract the common public. Advanced features of mobiles have not only made it convenient in use for common public, but on other hand, criminals use it for their illicit purposes. Therefore, this device has become a part of investigation to reach the miscreants.

The mobile forensics is challenging and requires the recovering of the evidence from the device in a manner acceptable in forensically sound manner. The challenge in mobile forensics is compounded by different processor types, limited processing and memory resources of the mobile phones and different vendor specific OS with some level of security implementation. The power supply in the mobile devices is also an important aspect while investigating the mobile device.

While keeping in view the use of mobile devices and the constraints playing role in the investigation of the devices, a need to develop and model an investigating process. The factors involved in making the mobile forensics challenging could be; variety of available operating systems, short life cycle of the product and new models develop very rapidly, the file system is robust, device introduces new communication technologies and efficient performance.

II. LITERATURE REVIEW

The main and important Components of mobile forensics are as follows:

Appropriate method for data acquisition; examining the collected data and analyzing it, and most important is to adapt an investigation process model.

A. Forensics Survey:

Konstantia *et. al.* [1] has presented a critical review of forensics of mobile devices in the last 7 years. The mobile forensics as mobile devices have undergone a revolutionary

growth in the last decade. It also describes the decision to concentrate on the last 7 year is to elaborate the interdependence of the contributions and efforts made in the field during this period. [1] also presents a schematic outline as well as details picture of significant developments in this field so far. An effort for new comers in the field to have a quick and complete picture of the domain. The topics of Data Acquisition, Operating Systems, and Data types, Standardization in the field, Android forensics, Blackberry forensics, iOS forensics, Maemo forensics, Shanzahi forensics, Symbian forensics, WebOS forensics, Windows mobile forensics and multiple OS forensics have been highlighted. Also a chronological representation of major contributions is outlined.

Authors describes in the survey paper that provides a succinct review of the mobile forensics and security, also the attack vectors by using back end systems and web browsers[2]. The difference between normal security and mobile security is also discussed. A further elaboration is done on the attack models and hardware security aspects. Performance can be also measured through defined parameters [12].

B. Data Acquisition:

Two well-known methods for mobile phone data acquisition are referred to as Remote data acquisition Local data acquisition. Considering it as the most important step in the mobile forensics investigation, data acquisition as well as data analysis data reverse engineering method is shown.[3] It introduces a method named as MIAT (Mobile internal Acquisition Tool) that actually decodes the information that can be used in other areas also. The methodology includes the following mentioned steps, choice of objective, Identification of files on interest, Data hypothesis, sequences similarity discovery, data interpretation, meta-form building and error correction. The final step involves the testing and debugging stage.

Data acquisition and preservation impose a major challenge in mobile forensics [4]. Different steps involved in the process of the mobile forensics, especially the critical stages of the data acquisition and preservation is focused. The forensics analysis of the wireless networking of mobile phones is mention in [5]. The paper presents a method to analyze wireless features of a smart phone forensically, using open source tools. The method introduced in the paper is evaluated with the ACPO (Association of Chief Police Officers') guidelines of good practice for digital electronic based forensics.

C. Investigation Process Models:

Moving forward the Smart phone digital evidence forensics standard operating procedure is proposed by I-Long Lin [6]. I-Long Lin compares the SOP with the one proposed by NIST and also a third party forensics tool is used to collect, examine and analyze the digital evidence. The proposed system defines the steps in SOP as Conception Phase, Preparation Phase, Operation Phase and Reporting Phase.

The challenging and important stages in the investigation process of mobile forensics is discussed by Stacey Omeleze and H. S. Venter [7]. The Harmonised Digital Forensics Investigation process model (HDFI) is in draft version for becoming an internationally recognized standard is tested in this paper using an android smart phone. The paper gives a review of the HDFI and then test the process on an android phone which has shown satisfactory results. As the demand of the investigation may differ for different devices but a generic process may help the investigator to well document and analyze the evidence [8]. The paper identifies the steps of evidence extraction method as Intake, Identification, Preparation, Isolation, Processing, Verification, Documentation, Presentation and Archiving. A comparative matrix is also presented that shows the available tool kits and their functionalities according to different wireless technologies.

Mobile forensics contains some challenges in the data acquisition and preservation due to the variety of models of different vendors available in market[9]. After research and critical analysis of Google's Android, the Windows smart phones are also included in the consideration. Windows smart phones have less market share than android but are competitor of android and also many cases of investigation of windows phones have been observed on routine basis. So, a forensic investigation model is also prepared for the windows phones [10]. Hardware architecture of the windows phone as well as its generic states are presented. After mentioning the detailed challenges in the forensics of windows phones, the author lists the steps involved in the process of investigation for the windows phones.

III. Existing Process Models

As also discussed in the literature review, there are some existing forensics investigation models proposed previously. Some of the forensics investigation models proposed by the different researchers are as follows;

The digital evidences have been divided into three categories i.e. changeable digital information, fixed information and file system digital information [6]. Also NIST has divided the digital evidences into three categories including smart phone memory, memory card and SIM card.

I-Long Lin [6] describes the phases of mobile phone investigation in his proposed model called DEFSOP (Digital Evidence Forensics Standard Operating Procedure) as "Conception", "Preparation", "Operation" and "Reporting". While the NIST SOP states the phases as "Preservation", "Acquisition", "Examination and Analysis" and "Reporting". Both of the SOPs define the same amount of phases with some similarities and some differences. Further 4Ps are also refereed (referred or refreed??) in [6] i.e. Prevention, Protection, Preservation and Presentation. These are considered the crux of the investigation model.

IV. Proposed Mobile Forensics Model

The proposed model for mobile forensics investigation is based on the most important phases identified for the mobile investigation. As there is no unified or any appropriate forensics model among all of the proposed ones. Every model works well in a particular type of case but not all. Also the existing models do not control the information flow.

The proposed model consists of the following phases;

A. Preparation

The most important phase of forensics is the preparation phase because it is the pre-investigation stage and it involves understanding of nature of the case. Setting up the investigation team as well as the forensics lab and the first responder tool kit along with the necessary forensics workstation that can help getting the evidence at the crime scene. Another important factor is the briefing of the situation. The team members should be aware of different types of devices and general hardware and software configurations of the devices that are involved in the case.

After analyzing the initial situation of the case a systematic strategy for carrying out the investigation is to be formulated considering legal constraints..

B. Handling Evidence & Secure the Evidence

All the evidence should be handled according to the strategy mentioned at the start of the investigation. A chain of custody forms?? should be maintained to ensure the integrity of the evidence. An important step is to isolate the device from the network. Also the need of any traditional forensics process should be kept in consideration.

Isolation of the crime scene from the people not required at the crime scene because the integrity of the evidence can be ensured if there is no unauthorized access at the crime scene.

C. Data Acquisition

Data acquisition depends on the nature of the investigation. As described above local acquisitions have many advantages but it cannot be employed wholly in every situation. As a contrasted remote acquisition methods take more resources. To cope with the issues it is recommended that both the methods, local and remote, are to be used according to the situation of the case. The type of acquisitions could be Manual, logical, file system, physical, chip-off and micro-read.

The data acquisition of the mobile devices are different for power off devices and power on devices.

- For power off devices, first, obtain the manual of the device. Second, remove the removal memory cards etc from the device, if any. Ensure that the power of the mobile is maintained for the examination. Also acquire the internal memory of the device. Non-volatile evidence could be acquired.
- For power on devices, the most important step is to cut off the network communication of the device. Maintain the power of the device. Remove the memory card from the device, if any. And at last switch off the device. Collecting volatile evidence required the power on state of the mobile device.

D. Documentation

The phase documentation is inter connected with all the other devices as the documentation is to be done at all the stages of the investigation. Chain of custody is an important document to maintain from the starting of the investigation till the representation of the evidence in court. Further the whole crime scene is to be documented. The documentation should include the following;

- Legal authority letter.
- Chain of custody.
- Photographs and manual documents of the visible as well as digital evidence.
- Information about the mobile device if obtained from the owner.
- All the carried out investigation should be documented as if to be handed over to any other examiner.
- Formulated strategy to carry out the investigation.
- Report of the findings.

E. Preservation

This phase deal with the bagging, tagging concept of the evidence. The transportation and storage of the evidence is also covered in this phase. A proper procedure is to be followed to ensure the integrity of the collected evidence. All the collected evidence should be tagged according to the procedure and packed in the evidence bags. For mobile devices the bags should be anti-static and radio blockers. So that the digital evidence could not be altered with the radio wave and electric field. Being electronic devices, the humidity and temperature could have an adverse effect on the devices, so special arrangements may be required to avoid environmental effects. The transportation of the evidences should be secure to ensure the integrity. On reaching the forensics lab, the evidence should be placed in the secure containers while maintaining the chain of custody form. The container should be secured from the unauthorized access.

F. Examination and Analysis

This phase deals with the examination of the collected evidence. Before examination of the evidence, extra copies of the evidence should be made. The aim of examination is to make the evidence visible. The formatting of data as well as arranging the data in order to analyze it. Data filtering, specific words key search and validations are the majors of this phase. Detecting and recovering is also part of this phase. Also selection of appropriate tools for forensics is important at this stage. Analysis is the step, rather it should be called as technical review of the examined data or evidence. Recreating the crime scene is the part of the analysis step. The recreation of the crime scene involves getting information from the fragments of recovered evidence. Timeframe analysis is an important task at this stage because at the presentation of the case in the court the timeframe of the crime have significant impact on the judgment. Making a comprehensive report at the end of examination and analysis is the last step.

G. Presentation

Presentation is an important phase in any criminal case because decision of the court depends on this. The report that is prepared about the case at the end of examination and analysis is presented to the court of law or in case of internal company investigation in front of company management. A culprit may be released by the court if the evidences are not properly substantiated. The report should be flexible enough because it could be challenged in the court of law (Seems incorrect). So the supporting documentation should be complete at the time of presentation of the case.

H. Review

The final phase is the review phase. This phase is specifically for the investigator. The review phase gives the examiner an opportunity to improve his expertise as well as analytical skills. All the steps followed before are analyzed in this phase and a peer review of the investigation is carried out. This results in efficient investigation and facilitates to reach the criminals.

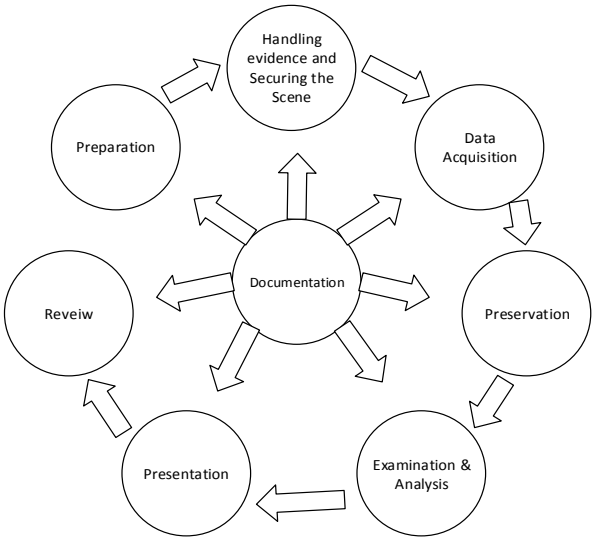

Fig. 1. **Phases of the proposed model**

Fig. 1 explains the process flow of the proposed system mentioning the phases and their linkwith other phases. It can be seen that great emphasis has been put on the documentation phase as it used throughout the investigation process. This phase is interlinked with all the other phase as the documentation is to be maintained at every stage of the investigation as well as it is the most important step at the time of the presentation of the case in the court of law. Fig.1 shows that the mobile forensics investigation starts at Preparation phase, following evidence handling and its securing process at the crime scene. Later data acquisition that depends on the case situation as it can be at the crime scene as well as at the forensics lab after the seizure of the evidence. Next, the process leads toward Preservation of the evidence. Examination and Analysis of the evidence is the important phase as it is the core of the investigation. These phases results in proving the allegations and bring the criminal to justice.

V. Comparison with Some Existing Models

Table.1 below gives comparison of the proposed model with the existing models. It also gives a comparison between the phases of the proposed model and other models' phases. As mentioned earlier, t the existing model is generalized model for all the handheld devices' investigations. Therefore, the phases are also generalized accordingly.

Proposed Model	NIST Guidelines	DEFSOP	Model for Windows devices	HDFI model
Preparation	×	✓	✓	✓
Handling Evidence & Secure the Evidence	✓	×	×	×
Data Acquisition	✓	✓	✓	✓
Documentation	✓	×	✓	✓
Preservation	✓	×	✓	✓
Examination and Analysis	✓	✓	✓	✓
Presentation	✓	✓	✓	✓
Review	×	×	✓	×

VI. Conclusion

A new unified forensics investigation model for mobile devices has been proposed. An effort has been made to make a model that could be used for every kind and type of mobile device investigation. This model is inspired by the previous works in this domain and also the NIST guidelines for cell phone forensics are kept in consideration while designing of the process model. The advantage of the proposed model is that the extra and repeated phases and stages of the previous models were merged and the phases are made more concise and to the point. Furthermore some recommendations are also made in the phases of the process.

In future work, the practical implementation of the work is to be analyzed and limitations in the practical scenario are to be measured.

References:

1. Konstantia Barmpatsalou, Dimitrios Damopoulos, Georgios Kambourakis, Vasilios Katos (2013) "A critical review of 7 years of Mobile Device Forensics", 2013.
2. Michael Becher, Felix C. Freiling, Johannes Hoffmann, Thorsten Holz, Sebastian Uellenbeck, Christopher Wolf (2011) "Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices", 2011 IEEE Symposium on Security and Privacy.
3. Fabio Dellutri, Vittorio Ottaviani, Daniele Bocci, Giuseppe F. Italiano (2009) "Data reverse engineering on a smartphone", 2009 IEEE.
4. Vinod Patil, Sulabha V. Patil (2012) "Survey on Mobile Phone Forensics: Guidelines and Challenges in Data Preservation and Acquisition", MPGI National Multi Conference 2012.
5. Panagiotis Andriotis, George Oikonomou, Theo Tryfonas (2012) "Forensic Analysis of Wireless Networking Evidence of Android Smartphones", 2012 IEEE.
6. I-Long Lin, Han-Chieh Chao, Shih-Hao Peng (2011) "Research of Digital Evidence Forensics Standard Operating Procedure with Comparison and Analysis based on Smart Phone", 2011 International Conference on Broadband and Wireless Computing, Communication and Applications.
7. Stacey Omeleze and H. S. Venter (2013) "Testing the Harmonised Digital Forensic Investigation Process Model-Using an Android Mobile Phone", 2013 IEEE.
8. Det. Cynthia A. Murphy (2015) "Developing Process for Mobile Device Forensics".
9. Shivankar Raghav and Ashish Kumar Saxena (2009) "Mobile Forensics: Guidelines and Challenges in Data Preservation and Acquisition", 2009 Student conference on Research and Development.
10. Anup Ramabhadran (2015) "Forensics Investigation Process Model for Windows Mobile Devices", Security Group-Tata Elxsi.
11. (2012) NIST Guidelines for cell phone forensics.
12. Muhammad Sadiq, Muhammad Shahid Iqbal, A. Malip and W. A. Mior Othman (2015) A Survey of Most Common Referred Automated Performance Testing Tools. ARPN Journal of Science and Technology, 5(11):525- 536, (2015)