# NEW RESEARCH DIRECTIONS IN THE AREA OF SMART PHONE FORENSIC ANALYSIS

Firdous Kausar

Department of Computer Science, College of Computer and Information Sciences, Imam University, Riyadh, Saudi Arabia.

***ABSTRACT***

*The proliferation of smart mobile phones with diverse features makes it possible to increase their use in criminal activities. The fast technological evolution and presence of different smart phones and their proprietary operating systems pose great difficulties for investigators and law enforcement officials to choose the best tool for forensics examination, accurate recovery and speedy analysis of data present on smart phones. This paper presents a literature review on smart phone forensic techniques for different platform. As a result of comprehensive analysis of these techniques, it has been found that there is no generic forensic technique or tool available which can perform the forensic analysis of all currently available different smart phones. Further, there is a need to develop a generic technique for forensic analysis of a variety of different smart phones. This generic technique should perform the forensic of currently available different smart phones on the crime scene without need to attach the smart phone with computer. Further, it will help the investigators to do their jobs easily and more efficiently. The proposed technique need to be implemented and tested on different smart phones to validate its performance and accuracy.*

***KEYWORDS***

*Smart phone Forensic, Digital Forensic, Analysis, Tools, Digital Evidence, Internal Memory*

## 1. INTRODUCTION

In these days, the smart phones are integral part of our daily lives and these are used because of their enhanced features e.g. web connectivity, increased storage capacity, computing power, upload capabilities, and attractive interface.

The smart phones have combination of functionality and storage space as like business laptops of just few years back and make them a prime target for forensic analysts and security specialists. A significant data of forensic value based on e-mails, call-history, addresses, contact numbers, notes, voice records, web history, videos, photos, calendar events, tasks, SMS, MMS, GPS navigators, browsing history and voicemail recording is very important for forensic professionals. The smart phones have become a vital part in criminal investigations. The smart phones are a potential source of digital evidences. The forensics investigators solve criminal cases via stored data in the phone applications. Even if the data is erased or deleted from the phone, evidence may still be restored and can be retrieved through forensic tools. Further, increasing rate of stored data in smart-phones makes the speedy, convenient and detailed data analysis by law enforcement units, police departments, incident response team members, security agencies, tax and customs services, army, and other government authorities.

DOI : 10.5121/ijcnc.2014.6409 

Nowadays, the smart phones are providing a major part in digital evidences of crimes. In criminal cases, the combination of several capabilities of smart phones through which the user information are extracted as evidences. On the transmission, the digital evidences are series of binary digit numbers on the transmission. Further, the files of information are stored on the electronic devices. Furthermore, the audio, video, images etc. are the file formats of digital evidences. The digital evidences can be copied and modified. Due to this, it is very difficult to find out the original resource. In data verification, some technical resources are required to find the actual picture.

Due to massively utilization of the smart phones technologies, the social security issues have been increased tremendously. The digital forensics provides the facility to produce the evidences for the court and other rule & regulation authorities. New digital equipment are coming in the market rapidly. At present, the digital forensics are used widely in the fields of memory forensics, network forensics, computer forensics, and mobile forensics etc.

There is a need to present a generic forensic technique for smart phones which will provide solutions of problems in current forensic tools with the features i.e. generic, usability, comprehensive, accuracy, deterministic, capability, affordability, and backup.

There are lot of limitations and deficiencies with current tools for smart phones forensics, which are as under:

1. Some forensic tools are worked perfectly with one type of smart phones but not with others.
2. Some tools are unable to create the physical image in the absence of jailbreaking the devise after the advent of IOS 4.x for the iPhone.
3. Due to some programming errors, out of date specification (which are used to translate the encoded bits into data understandable for the investigator) and incorrect protocol structure for the input of cellular device, the forensic results are not accurate.

## 2. GOAL OF RESEARCH

The objective of this research is to have a detailed review and in depth analysis of currently available several forensic analysis techniques and tools for different smart phones and find out the problems, weaknesses and technical shortcomings of these techniques. The focus of this research is to address their limitations by developing new technique and tool for forensic analysis of different smart phones. Further, there should be given the comprehensive analysis of proposed technique and comparison with the existing techniques of forensic analysis for different smart phones. Implementation and testing of the proposed technique should be done in variety of different smart phones to show its practical usage and efficiency.

Following important guidelines and requirements specified in [21] [22] should be taken into consideration during the development of forensic analysis technique for smart phones.

- **Generic** – the tool should have ability to use with all type of smart phones without any limitation with any type of operating system.
- **Usability** – the tool should have capability to give the results in the form of different reports that will be useful for forensic professional and enforcement authorities
- **Comprehensive** – the tool should have capability to produce the required data to forensic professionals, as a result, the evidences related to inspection, which can be recognized and presented to courts.
- **Accuracy** – the tool should have ability that the output in the form of verified reports.

- **Deterministic** – the tool should have facility to provide the exact output as per given the same input data and set of instructions.
- **Capability** – the tool must have feature set, supported devices, performance and diversity of features with customization and flexibility.
- **Backup** – the tool must have ability to make backup and reports when needed.
- **Affordability** – the tool should be feasible regarding cost versus benefits.

## 3. EXISTING SMART PHONE FORENSIC TECHNIQUES

There are many researchers currently working in the area of smart phone forensic investigation. These techniques can be divided in to broader categories of following smart phone platforms 1) Android based techniques, 2) iPhone based Techniques 3) Blackberry based techniques and 4) Others.

This section discusses some of the state of art research in this area.

F. Rehault [1] presents a method to retrieve the erased information from Windows Mobile smart phone using bootloader instead of ActiveSync in order to prevent the alteration of data on flash memory of smart phones to perform forensic investigation. Once the smart phone has been set into the "bootloader mode", it has to be connected through USB cable to computer and run the rbmc command in CommTTy program to dump the flash memory of smart phone to some output file on the computer hard disk. This dump file is then use to reconstruct file system on flash memory. A python script is given by author to reconstructs all the messages folders per email accounts, SMS/MMS accounts and un-compresses the stored compressed data.

Y.Gao et al [2] discuss the importance of on-the-spot digital forensics tools and particular user and software engineering requirements for these tools. They propose the Bluepipe architecture for on-the-spot investigation and the Bluepipe remote forensics protocol.

C.K. Wee et al [3] provide the analysis of integrity of the images of iPAQ type PDA's JFFS2 file system, acquired at two different times. They also attempt to recover the files on JFFS2. It is shown that if no soft or hard reset is performed then image integrity remains maintained. Also, it is possible to recover the deleted files from ROM.

F.Dellutri et al [4] presents a method for acquisition of data from a PcketPC internal storage memory by copying it to an external removable memory without connecting PocketPC to desktop or laptop computer. In order to seize data from PocketPC, first put it in Faraday cage, if there is memory card already present in the device remove it and insert the new memory card with installed MIAT-WM5 application default set to autorunnable. MIAT-WM5 copies the hash of each file in a log, before and after copy in order to assure its image integrity.

F. Li et al [5] explore the currently available open source digital forensic tools that can be used for forensic of Android smart phones. A comparison of common forensic system with developed forensic system is given. It shows that developed forensic systems are able to acquire the data from smart phone through forensic SD card. There is no need to switch off the smart phone or connecting it to PC as done with common forensic systems. It also provides the comparison of forensic tool function for Android Forensic and research developed system.
P.M. Mokhonoana et al [6] present a method to acquire from Symbian smart phones contents using an on-phone forensic tool. They develop on-phone tool using native Symbian C++ with auto-start property. This tool can be placed on SD memory card and retrieved data also resides on same memory card. This tool can copy SMS, MMS, emails, audio, video, pictures, applications,

internet cache and user files. Some of the important information about recently made calls and stores contact information cannot be copied using this on-phone tool.

L. Thing et al[7] describe an automated techniques to conduct the live memory forensic of Android based smart phone's. It also performs the experiments on different interactive based applications to show its dynamic properties analysis. The automated system consist of Message Script Generator, UI/Application Exerciser Monkey, Chat Bot, Memory Acquisition Tool, and Memory Dump Analyzer. Each of these components performs specific tasks to acquire data from the volatile memory of phone. Several experiments are carried out to perform real-time evidence acquisition and it shows that the there is elevated persistency for outgoing messages than the incoming messages.

Hoog [8] [9] provides a detailed survey of the forensic analysis tools for the Android phone. The Android Debug Bridge (ADB) allows communication with the phone by using the USB connection. The "adb pull" command can be used to recover active file from the memory of phone. Nandroid backup and Paraben Device Seizure are some of the other available tools that help in the retrieving the file from Android smart phone.

J.Lessard et al [10] explore the steps of the forensic analysis of an Android device. They use Sprint HTC Hero running Android v1.5 phone to conduct their experiments. The phone is connected with PC through USB data cable. FTK Imager is used to get the image of data from memory card by using export disk image option after connecting phone with PC. Root access is acquired by enabling the USB debugging option and dd command is used to image the memory. It is possible to retrieve deleted messages and contacts by analyzing these images. It also recover call history, Web and search history, pictures, MMS/SMS messages, e-mail data with complete messages, and even GPS data, voice mail and passwords, if root access is available.
A. Morum et al [11] presents a method to perform data acquisition of Android smartphones for forensic analysis by connecting to computer using data cables. The first step is to get image of data from the memory card by running a disk dump and then generate the hash of the image data to preserve its integrity. Then take the copy of the system partitions stored in phone's internal memory by using the USB debugging tool ADB with super user privilege. They also provide method on acquisition of data from locked device and how to bypass the passwords.

MI Husain et al[12] propose a method for forensic analysis of client based version of AIM, Yahoo! Messenger and web based version of Google Talk, instant messages on Apple iPhone. iTunes Backup is used to get data logically from the phone. Significant digital evidence are found from AIM and Yahoo messenger IM but no important evidence is found for Google Talk except the particular accessed time.

S. Y. Willassen[13] discusses two different method of imaging the internal memory of mobile phones. It also describes the digital evidence that can be extracted from the internal memory of different mobile phones like Nokia[14], Sony Ericson [15] and Siemens [16]. The presence of specialized embedded memory manager is discovered in the internal memory of [14], [15] and [16] which may cause the overwriting of the deleted data in case of its reorganization.

Other commercially available software and hardware for forensics analysis in market are Oxygen Forensic Suite [17], MOBILedit! Forensic [18], EnCase®, Neutrino® [19] and .XRY [20].

M. Bader et al [23] use the Apple iTunes backup utility to acquire to logical backup of iPhone 3GS . They retrieved the significant data like e-mail messages, text and multimedia messages, browsing history, GPRS locations, contacts, call history and voicemail recording, that can be utilize as digital evidence by analyzing the logical backup.

N. Al Mutawa et al [24] perform a forensic analysis study to keep track of user activities on Facebook, Twitter and Myspace social networking applications by using three different platforms of BlackBerrys, iPhones, and Android. The results show that it is possible to retrieve a significant amount of data related to user activities from android and iPhone but blackberry does not give access to user data for forensic investigation.

J. Park et al [25] describe a technique to reconstruct the smart phone flash memory pages area of the file system. The process of fragmented flash memory analysis is done in two steps where first page classification is done and then page analysis is performed.

J. Sylve et al [26] present the technique for obtaining a total memory captures from Android based smart phones. A code is provided to perform analysis of kernel data structures, and scripts which permit examination of a number of activities based on land and file system. They successfully able to retrieve the evidences including the objects related to running processes, terminated processes, open files, network activity, and memory mappings.

## 4. COMPARATIVE ANALYSIS OF FORENSIC TECHNIQUES

The comparative analysis of above discussed forensic techniques is shown in Table 1. This comparison is done based on different parameters specified in [21] [22]. It can be seen that most of the work in this area is conducted for android based smart phone as compare to other platforms. This choice of platform for conducting research for android is because of its open source feature. Further, it can be concluded that most of the current research focus on logical acquisition of data which requires the phone to connect with computer as compared to physical acquisition of data from phone. Physical acquisition does not requires phone to connect with computer instead SD card is mounted into phone for acquisition of data. The most important finding after comparative analysis of these techniques is that there is no one generic forensic technique is available that can be used for forensic analysis of all available platforms of smart phone.

Table 1. Comparative Analysis of Forensic Techniques

| Technique | Generic | Comprehensive | Accuracy | Need Connection with Computer | Platform |
|---|---|---|---|---|---|
| [1] | No | Yes | Average | Yes | Windows |
| [3] | No | Yes | Good | No | iPAQ |
| [4] | No | | Average | No | PocketPC |
| [5] | No | | Average | No | Android |
| [6] | No | Yes | Good | No | Symbians |
| [7] | No | Yes | Good | Yes | Android |
| [8][9] | No | No | Average | Yes | Android |
| [10] | No | Yes | Good | Yes | Android |
| [11] | No | No | Good | Yes | Android |
| [12] | No | No | Average | Yes | Social Networking Application |

| | | | | | |
|---|---|---|---|---|---|
| [13] | No | No | Average | Yes | Nokia, Sony Ericson, Siemens |
| [23] | No | Yes | Good | Yes | iPhone |
| [24] | No | No | Average | Yes | Blackberry, iPhone, Android |
| [26] | No | Yes | Good | No | Android |
| [25] | No | No | Average | No | Android |

## 4.1 COMPARISON OF COMMERCIAL FORENSIC SYSTEM WITH GENERIC FORENSIC SYSTEM

The variation between commercial forensic system and generic forensic system is the basic steps need to be followed during the forensic investigation process. In the generic forensic system, the acquisition of evidence from smart phone can be done by using SD card instead of a desktop or PC, and saved evidences in forensic SD card on crime scene efficiently with no use of extra hardware.

The comparison of the process of forensic digital investigation between commercial forensic system and generic forensic system is given below in Table-2.

Comparison of Forensic Process (Table-2)

| **Forensic Process** | **Commercial Forensic System** | **Generic Forensic System** |
|---|---|---|
| Crime Scene Exploration | Document the details of the crime scene evidences of smart-phone around the state of affairs, and power-off the smart-phone. Put it into evidences bag to present it in the digital forensic laboratory. | Un-mount user SD card without switching off the power and document the details of the crime scene outside condition |
| Acquisition of Evidences | Hook up to the desktop or PC, progress the acquisition of evidences by use of forensic toolkit. | The smart phone is Mounted with the forensic SD card, progress the acquisition of evidences by use of forensic software, and collected data is saved in the forensic SD card. |
| Forensic Analysis of | Perform analysis by using | Perform analysis by using |

| | | |
|---|---|---|
| Collected Evidences | desktop or PC | desktop or PC |
| Report Generation | Produce the report of result of analysis by using desktop or PC | Produce the report of result of analysis by using desktop or PC |

## 5. CONCLUSIONS

The availability of a variety of type of smart phones', their proprietary operating systems, various applications and local forensic laws makes the smart phone forensic a challenging task. The approach of this research is basically studying the internal architecture and operating systems of different smart phones available in market either using GSM or CDMA. The variety of operating systems needs to be focused for this research includes: Android, iOS, Symbian, RIM, Bada, BlackBerry OS and, others. The generic techniques will retrieve the evidence items present in Subscriber Identity Module (SIM), Mobile Phone Internal/flash Memory, external and internal Memory Cards and memory sticks. There is also need to propose a method for blocking RF signals of mobile phone during forensic analysis. A generic technique is required that can acquire data from different smart phones by inserting the memory card with installed auto-run forensic application. As a result the forensic investigator can perform fast acquisition of data from phone without the need of attaching it to computer with data cable. It should also perform the analysis of following acquired digital data for digital evidences in investigation:

- Basic information of Phone and SIM-card data
- E-mail Messages and attachments
- Call history (Incoming, outgoing and missed calls)
- Contact information
- Multimedia Gallery
- Multimedia Messages with attachments
- Web-browsing session logs
- Video films and clips
- Caller Groups
- Text notes
- GPRS and Wi-Fi traffic
- Voice records
- Organizer (call reminders, memos, appointments, calendar meetings, to-do tasks, birthdays and adversaries)
- The complete data e.g. installed applications on the phone with their data, all files from phone memory and flash card.
- SMS
- Virus intrusion

## REFERENCES

[1]. F. Rehault, Windows mobile advanced forensics: An alternative to existing tools, in Digital Investigation, Volume 7, Issues 1–2, October 2010, Pages 38–47

[2]. Y. Gao, G. G. Richard, V. Roussev, Bluepipe: A Scalable Architecture for On-the-Spot Digital Forensics, International Journal of Digital Evidence Summer 2004, Volume 3, Issue 1

[3]. C. K. Wee , L. W. Wong, Forensic Image Analysis of Familiar-based iPAQ, May 12, 2007, from http://www.forensicfocus.com/downloads/familiar-ipaq-forensic-analysis.pdf

[4]. F.Dellutri, V. Ottaviani, G.Me, MIAT-WM5: Forensic Acquisition for Windows Mobile PocketPC, in Proc. of the Workshop on Security and High Performance Computing Systems, part of the 2008 International Conference on High performance Computing & Simulation(HPCS 2008)
[5]. P. X. F. Li, C.H. Yang, S. J. Chen, J. S. Wu, Design and Implementation of Forensic System in Android Smart, The fifth joint workshop on Information Security, China, August 5- 6, 2010.
[6]. P. M. Mokhonoana, M. S. Olivier, Acquisition of a Symbian Smart phone's Content with an On-Phone Forensic Tool, Proceedings of the Southern African Telecommunication Networks and Applications Conference 2007, Mauritius, September 2007.
[7]. V. L. L. Thing, K. Y. Ng, E. C. Chang, Live memory forensics of mobile phones, in Digital Investigation, Volume 7, 2010, Pages 74-82.
[8]. Hoog A, Gaffaney K. iPhone forensics. via Forensics Whitepaper; June 2009.
[9]. Hoog A. Android forensics, presented at Mobile Forensics World 2009; May 2009.
[10]. J. Lessard, G.C. Kessler, Android Forensics: Simplifying Cell Phone Examinations, Small Scale Digital Device Forensics Journal Vol. 4, no.1, September 2010.
[11]. A. L. Simao, F. C. Sicoli, L. P. de Melo, F. E. de Deus, R. T. de Sousa Junior, Acquisition of Digital Evidence in Android Smartphones , Proceedings of The 9th Australian Digital Forensics Conference, Perth, Western Australia, 5th -7th December, 2011.
[12]. MI Husain, R. Sridhar, Forensics: forensic analysis of instant messaging on smart phones. Digital Forensics and Cyber Crime, vol. 31; January 2010. pp. 9-18.
[13]. S. Y. Willassen, Forensic analysis of mobile phone internal memory, Advances in Digital Forensics, IFIP International Federation for Information Processing, 2005, Volume 194/2005, pp. 191-204.
[14]. Nokia, http://www.nokia.com
[15]. Sony Ericsson, www.sonyericsson.com
[16]. Siemens , www.siemens.com
[17]. MOBILedit! Forensic, http://www.mobiledit.com/forensic/
[18]. EnCase®, and Neutrino®, http://www.encaseondemand.com/Home/tabid/632/Default.aspx
[19]. Oxygen Forensic Suite, http://www.oxygen-forensic.com/us/
[20]. .XRY, http://www.msab.com/
[21]. NIST Guidelines on Cell Phone Forensics, Special Publication 800-101
[22]. NIST Smart Phone Toll Specification, April 10, 2010.
[23]. M. Bader, I. Baggili, iPhone 3GS Forensics: Logical analysis using Apple iTunes Backup Utility, Small Scale Digital Device Forensics Journal, Vol. 4, no.1, September 2010.
[24]. N. Al Mutawa, I. Baggili, A. Marrington, "Forensic analysis of social networking applications on mobile devices", Digital Investigation, Volume 9, Pages S24–S33, August 2012.
[25]. J.Park, H. Chung, S. Lee, "Forensic analysis techniques for fragmented flash memory pages in smartphones", Digital Investigation, Volume 9, Issue 2, Pages 109–118, November 2012.
[26]. J. Sylve , A .Case , L. Marziale , G. G. Richard , Acquisition and analysis of volatile memory from android devices , in Digital Investigation, Volume 8 , 2012, Pages 175–184.

**Authors**

Firdous Kausar is currently working as an Assistant Professor in the Department o f Computer Science, College of Computer and Information Sciences, Imam University, Riyadh, Saudi Arabia. She received her Ph.D. in Information Security from National University of Sciences and Technology, Pakistan in 2009. Dr. Kausar has served as a reviewer of several international conferences and journals. She is editorial board member of Future Technology Research Association Publishing. In addition, she served as a Guest Editor for Special Issue on: Advances in Communication Networks for Pervasive and Ubiquitous Applications, Journal of Supercomputing, Springer, 2011. Her research interests are in Cryptography, Cryptanalysis, Information Security Management, Ubiquitous Computing, Network Security, Digital Forensics, Sensor Networks, Mobile and Ad hoc Networks.