ISSN No. 0976-5697

Volume 5, No. 4, April 2014 (Special Issue)

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Forensic Presevation of Digital Evidence on Mobile Devices from the Perspective of Efficient Generalized Forensics Framework for Mobile Devices (EGFFMD)

Rizwan Ahmed
G. H. Raisoni College of Engineering, Nagpur, India
rizwanmailbox@gmail.com

Rajiv V. Dharaskar
Matoshri Prathisthan Group of Institution, Nanded, India
rvdharaskar@rediffmail.com

Vilas M. Thakare
SGB Amravati University, Amravati, India
vilthakare@yahoo.co.in

Abstract: The extraordinary development of mobile communications is a source of new security challenges. Today, mobile phones have become ubiquitous in nature involving their use in many daily activities, and sometimes those activities might be criminal in nature. The remarkable advancements in the technology and increase in computing power of these devices over last few years, has led to an increase of their functionality while keeping the size of such devices small enough to fit in a pocket. The use of mobile phones in criminal activities has led to the need of recovering the digital evidence data in them for the further investigations. It is therefore essential for investigators to be able to extract digital evidence quickly and accurately. The digital forensic examiner must know how to preserve and acquire digital evidence effectively from mobile devices. This paper provides an overview of digital evidence preservation issues, relevant solutions for digital forensics examiners, and tips for successful preservation of digital evidence on mobile devices.

Keywords: Digital Evidence, Mobile Forensics, Mobile Forensic tools, Smartphone

I. INTRODUCTION

Mobile phones, Smartphones and other Personal Digital Assistants (PDAs) provide people with the ability to surf the web, send/receive emails, capture and exchange pictures/videos, listen to music, or watch movies in the palm of their hand. The future holds even greater promises as these devices are being used as "digital wallets" to pay bills, check account balances, and store other forms of data. Due to these varying and always increasing capabilities, however, a mobile device can become the focus of litigation, investigation, or law enforcement action. At that point, a tool of convenience becomes a source of digital evidence. Digital Forensic Examiners may be called upon to preserve a wide variety of mobile devices that can produce critical evidence, including email, call logs, pictures, password, videos, user-created documents, and text messages [1].

As mobile phones, and other handheld devices integrate new technologies for communications and data storage, they will continue to emerge as sources of additional evidence in criminal and civil investigations. Consequently, Digital Forensic Examiners must know how to preserve and acquire data effectively on mobile devices. This paper provides an overview of digital evidence preservation issues, relevant solutions for digital forensics examiners, and tips for successful preservation of digital evidence on mobile devices. The identified methods are already incorporated in Efficient Generalized Forensics Framework for Mobile Devices (EGFFMD) [3, 6, 7, 8, 13].

II. BACKGROUND

Currently, numbers of researchers had addressed to the security issues of the smartphone, and developed various technologies for the investigative features. In this section, we have analyzed the definitions of digital evidence, mobile forensics and smartphone, and also introduced some studies that had down in Android smart phone operating system architectures, and mobile phone forensic tools area.

A. *Digital Evidence:*

The digital evidence is a series of binary digit numbers on transmission [9], or stored information files on the electronic device. Moreover, the digital evidence file formats includes audio, video, images, and digital, etc. The digital evidence is not virtual exist, but there are some other features to look for, the digital evidence can be copied with unlimited differences, can be modified easily, hard to be identified the original resource, can be integrated data verification, and cannot be understood directly without technical process.

B. *Mobile Forensics:*

With the increased emphasis on social security issue, crime issue is considerable when it comes to the utilization of smart phone technologies, digital forensics provide the technical skills to collect evidences for the court to review and judge cases. Digital equipment has changed daily, people has pervasive use some common digital devices such as computers, Internet, mobile phones, digital cameras, hardware, storage devices, etc. Currently, digital forensics has widely used in the areas of network forensics, mobile forensics, computer forensics, and memory forensics, etc. According to NIST definition of mobile phone forensics process is preservation, acquisition, examination and analysis, and then reporting [10].

The various aspects of mobile forensics have been discussed in our previous research work [1, 2, 3, 4, 5, 6, 7, 8, 13].

CONFERENCE PAPER
Two day National Conference on Innovation and Advancement in Computing
Organized by: Department of IT, GITAM UNIVERSITY Hyderabad (A.P.) India
Schedule: 28-29 March 2014

C. Smartphone:

Due to the advanced technological development, mobile phone's selling was decreased in 2009; smart phones' selling is increased, and the commercial demand cannot be sacrificed by the smart phone. In Table 1 [11] shows definition of smart phone, the various categories of smart phones' forensic, different operating systems and the disordered domestic laws for forensic procedures result in the difficulty of smart phone forensics [12].

Table 1. Definition of Smart Phone

Item	Definition
Capability	With voice and data wireless communication personal management (PIM), such as contacts, calendar, alarm clock, etc.
Input Mode	Common with push-button, voice input, touch and multi-touch
Wireless Transmission	IrDA, Bluetooth and Wi-Fi
Operating System	Symbian, iphone, Windows Mobile, Android, Palm, RIM, etc.
Processor	Embedded multi-task microprocessor

III. LOCATION OF DATA ON MOBILE DEVICES

Mobile devices contain various data and potential evidence items which can be of interest for a Forensics Examiner. Sources of evidence on Mobile devices may include: Subscriber Identity Module (SIM), Mobile Phone Internal Memory, Memory Cards and Network Service Providers. Typically the data on mobile devices can be stored at following places:

A. Memory:

Memory can either be volatile or non-volatile. Volatile memory, such as "Random Access Memory" (RAM) offers fast read and write access. However, RAM can be lost when a device loses power. Non-volatile memory, which includes "read only memory" (ROM), is not lost when a device loses power.

PDA's typically use RAM to store their operating system and data for applications and files. As a result, if the device loses power, this information will be lost. Unless the device uses alkaline batteries, replacing the battery may also render data unrecoverable. Digital Examiners must therefore check that all requisite power cords are available when acquiring evidence from Mobile Device to ensure that there is sufficient power to complete the acquisition.

Mobile phones, on the other hand, use non-volatile memory to store data, which is similar to a hard drive on a computer, but on a smaller scale. The operating system on a mobile phone is stored in ROM and it normally does not lose data if its battery loses power.

B. Media:

A mobile device may consist of several pieces of media, each which may be subject to digital evidence preservation during chain of custody. Depending on the model, a mobile device may consist of:

(i) "Subscriber Identity Module" (SIM) card
(ii) An internal memory module
(iii) Additional modules for such services as GPS positioning
(iv) Memory cards.

All components that may contain data relevant to the investigations should be preserved. SIM cards are thumbnail-sized smart cards that contain a user's contacts or "address book," SMS (text) messages, last dialed numbers, network information, the owner's phone number, the subscriber ID, SIM card serial number and integrated circuit card ID or "ICC-ID." They typically hold 64 KB or 12 8KB of data, although 256 KB size cards are also available. The SIM card is not, however, typically used for data storage. Examiners should acquire the SIM card only after acquiring the data on the device; accessing the SIM card before imaging the device requires removing the battery and doing so could reset the date and time stamps of messages. Powering on a device with a different SIM card could delete some or all of the data in the device's memory. The best option is to create a "Safety SIM" using a tool that allows the user's data to be copied to a sterile SIM card. The safety SIM can be used to acquire data without altering the device's date and time stamps. While a safety SIM contains a copy of the original SIM card's user data it does not have the file system needed for the phone to function or receive any data. Memory cards can range from 32 MB up to 8 GB in size. Memory cards contain file systems, such as File Allocation Table (FAT) and examiners should preserve the media in the same way they would a hard disk using the same forensic hardware and software. Both SIM and memory cards should be write-protected during the acquisition process to prevent the modification or deletion of data. Hardware and software tools are available that will allow examiners to acquire data from SIM cards [5].

The examiner's goal should be to preserve completely the internal memory of the mobile device. The internal memory is essentially the storage space of the handheld. Applications and add-ons such as Global Position Services (GPS) may reside as part of the handheld's internal memory. Evidence pertaining to a GPS device stored internally will be captured during the preservation of the handheld's internal memory. Examiners should be aware that a GPS device may also be a module inserted in the handheld. All pieces of media attached to the handheld should be preserved.

IV. CHALLENGES OF MOBILE FORENSICS

The field of Mobile forensics has lots challenges associated with it and some of the prominent challenges are listed below:

a. Mobile forensics is challenging field due to continuous advancements in relevant technologies. Currently, we have several models of mobile devices with different mobile operating systems, manufactured by various companies. Since these devices are manufactured by different manufacturers, they mostly lack standardized methods of storing data. Currently, most of these mobile devices use closed operating systems with proprietary interfaces. In order to counter this challenge, there is constant race to identify new methods and techniques which can be employed for mobile forensics.
b. Different mobile devices have different variety of data cables which might be required for evidence extraction or data transfer. In order to support more number of mobile devices during digital investigation, identification and collection of data cables is challenging task. In order to address this challenge, we

CONFERENCE PAPER
Two day National Conference on Innovation and Advancement in Computing
Organized by: Department of IT, GITAM UNIVERSITY Hyderabad (A.P.) India
Schedule: 28-29 March 2014

can create a small database for defining mobile devices, their relevant models and their associated data cables.

c. Due to different mobile operating systems from different vendors having various versions, conflicts may occur due to version specific device drivers. This challenge can be addressed by designating individual machines for each type of forensic software or by using Virtual Machines to achieve the same.
d. During investigation of mobile devices, live network signals need to be blocked which may result in battery being drained quickly. We can make use of various shielding methods such as EMI/EMC protection.
e. Due to volatile nature of mobile devices, data on them keeps on changing constantly due to lack of conventional write-blocking mechanism. In order to avoid any inadvertent changes to evidence during analysis of mobile devices that are powered ON, we need to ensure that the device does not receive any calls, text messages, or other communications. We can address this by doing these investigations in shielded labs.
f. In case of mobile device being shut down or restarted, we may lose volatile data as well as based on security measures the device may ask for security code to get the access. We can make use of relevant techniques to get past this or ask the device owner (if available) for relevant security codes.
g. In case of physically damaged mobile devices, most of the commercially available forensic tools do not provide solutions to extract evidence from them. Digital investigators need to be trained and equipped to handle such situations.
h. Different mobile devices employ different authentication mechanisms in order to do access management. In order to carry out digital investigation, identifying of Personal Identification Number (PIN), Phone Unlock Key (PUK), and handset and memory card passwords can become difficult and time consuming process.
i. Currently, all the trainings available in the field of forensics are vender specific. Ideally, we need to come with standard and neutral trainings.
j. During digital investigation, status of unopened emails and messages might change so we need to take proper care to handle such evidence.
k. For most of the mobile devices, the data on them can be remotely destroyed or changed. In order to avoid this, during digital investigation the mobile devices should be shielded in lab environments. Proper precautions must be taken in this regards, to protect the data on mobile devices during digital investigations.
l. Sometimes the data on mobile device's internal memory is restricted without the use of SIM card. If another SIM is inserted, then it may result in loss of mobile device data. So, appropriate precautions must be taken this regards.
m. Most of the commercial mobile forensic tools may only provide logical acquisition of digital evidence. In order to recover, deleted evidence only physical acquisition can be used.
n. Future introduction of Mobile Number Portability (MNP) might result into invalid identification of subscriber. Mobile network operators need to be consulted for identification of relevant subscriber.
o. Flashing tools like Universal Flasher UFS-3 can be used for changing the mobile device IMEI. This may result in improper identification of mobile devices. We may need to look at banning this illegal activity to curb this practice.

V. MOBILE FORENSICS: ADDITIONAL CONSIDERATIONS

Traditional Computer Forensics involving acquisition of a computer hard drive presents digital investigators with relatively few hardware configurations considering limited number of prominent operating systems, most of which are regularly encountered. On the other hand, mobile devices have lots of variations in terms of their software and hardware configurations due to multiple manufacturers. This results in a scenario in which not all forensics tools work for all the mobile devices. Digital investigators need to use multiple tools in order to do acquisition of evidence from mobile devices. Most of these tools do the digital evidence extraction from mobile devices using either physical acquisition, or logical acquisition or both. A physical acquisition of mobile device helps in capturing the unallocated space of the device which helps in identifying the deleted file fragments that may reside device. Thus physical acquisition helps in recovering the deleted data such as SMS messages, email, voice mail, and pictures etc. based on availability of the same from relevant devices.

We have lots of commercial tools available in market for forensic analysis of mobile devices which may involve making physical and logical copies. All these forensic tools have their own unique advantages and disadvantages. As an example, if a forensic tool allows user to do logical acquisition only then the digital investigator probably might not be able to acquire complete deleted data. In most of the scenarios, logical acquisition using forensic tools should be able to recover data such as call logs, active contacts, calendars entries, SMS and MMS messages, emails, memos, photos, videos, tasks and ringtones/audio files. Based on studies, it has been found that when a forensic acquisition tool is used on mobile devices, it may not work always as intended. These forensic tools claim to make forensics image of mobile devices but sometimes they only are able create logical image of target mobile device rather than physical image. Indeed, on some occasions these forensic acquisition tools fail to capture any digital evidence.

VI. PRESERVING DIGITAL EVIDENCE ON MOBILE DEVICES

Preserving data on mobile devices presents lots of unique challenges. Some mobile devices may require special cables and even may require additional equipment in order to connect them to a digital forensic workstation. In some other scenarios, digital forensic workstations or forensic software applications probably might not have all the necessary drivers installed to establish communication with the target mobile devices. Sometimes, in order to preserve the digital evidence on mobile devices, some specific software may be needed to be customized to work on a particular model. In some cases, the digital examiners need to install an application "agent" on the target mobile device in order to

allow the forensic tool to recognize device during the acquisition process. While installing these external applications, a precaution must be exercised from forensic perspective so that this does not introduce of new data on target mobile device along with preserving the existing data on target mobile device. This is really important considering the fact that, when all forensic acquisition methods fail, then best method of digital evidence examination of mobile devices might be scroll analysis which simply involves taking photographs of each screen on the target mobile device.

A. Cryptographic Hashing for Ensuring Digital Evidence Integrity:

Following best practices, a forensic hash is used for identification, verification, and authentication of file data. A forensic hash is a form of a checksum. A checksum is a mathematical calculation, which in its simplest form, adds up the assorted bits in a data string and provides a value. MD5 (Message Digest 5) and SHA-1 (Secure Hash Algorithm 1) are more complex forms of checksum algorithms. A forensic hash is the process of using a mathematical function and applying it to the collected data, which results in a hash value that is a unique identifier for the acquired (collected) data (similar to a DNA sequence or a fingerprint of the data). When a hash algorithm is used, it computes a string of numbers for a digital file. Any change to the data will result in a change to the hash value. Both MD5 and SHA-1 algorithms are commonly used on forensic image files. The hash process is normally used during acquisition of the evidence, during verification of the forensic image (duplicate of the evidence), and again at the end of the examination to ensure the integrity of the data and forensic processing. MD5 and SHA-1 hash values are also currently used to validate the integrity of downloaded files in information technology applications. They have been accepted by the scientific and consumer community to confirm that the files that are downloaded are the same and complete files that are requested to be downloaded [13].

B. Forensic Validity of Hash Algorithms:

The compromise of the MD5 and SHA-1 hash algorithms is vastly more complex. While it is possible to cause two files to have matching hash values, it is a complex process. The person creating the compromised files must have physical possession of the files to be altered. The affected/compromised files must be altered prior to the hash algorithm being run so that a matching hash value is produced. Research by Stevens, et al. has shown [14], in their vulnerability assessment, that a known hash value cannot be targeted to produce a duplicate hash of a known file. “We cannot target a given hash value, and produce a (meaningful) input bit string hashing to that given value colliding files have to be specially prepared by the attacker. Existing files with a known hash that have not been prepared in this way are not vulnerable.” This is important in the use of hash sets to identify known files.

VII. CONCLUSION AND FUTURE WORK

Mobile Phones are becoming even more sophisticated with day by day increase in capabilities. Both law enforcement and the private sector need to invest time and money into learning about new mobile operating systems and developing new digital forensic methods.

This paper outlined the various forensic evidence preservation approaches from the perspective of Efficient Generalized Forensics Framework for extraction and documentation of evidence from mobile devices. The approaches outlined will ensure that during forensic acquisition, a complete and consistent snapshot of mobile devices will be maintained through integrity verification using hashing algorithms.

VIII.REFERENCES

[1] Rizwan Ahmed, and Rajiv V. Dharaskar. "Mobile forensics: an overview, tools, future trends and challenges from law enforcement perspective." In 6th International Conference on E-Governance, ICEG, Emerging Technologies in E-Government, M-Government, pp. 312-23. 2008.. http://www.iceg.net/2008/books/2/34_312-323.pdf

[2] Rizwan Ahmed, and Rajiv V. Dharaskar. "Mobile forensics: an introduction from Indian law enforcement perspective." In Information Systems, Technology and Management, pp. 173-184. Springer Berlin Heidelberg, 2009. http://link.springer.com/chapter/10.1007%2F978-3-642-00405-6_21?LI=true#

[3] Rizwan Ahmed, R. Dharaskar, and V. Thakare, “Digital evidence extraction and documentation from mobile devices,” ijarcce.com, vol. 2, no. 1, pp. 1019–1024, 2013.

[4] Rizwan Ahmed, and R. V. Dharaskar. "MFL3G: An Open Source Mobile Forensics Library For Digital Analysis And Reporting Of Mobile Devices For Collecting Digital Evidence, An Overview From Windows Mobile OS Perspective." In International Conference on Advanced Computing Technologies (ICACT 2008), GRIET, Hyderabad, India. 2008. http://www.gbv.de/dms/tib-ub-hannover/61808083x.pdf

[5] Rizwan Ahmed, Dr. R. V. Dharaskar, “Mobile Forensics: the roadblocks ahead, proposed solutions using Protocol Filtering and SIM programming”, International Journal Of Computer Science And Applications Vol. 2, No. 2. pp. 109-115.

http://www.researchpublications.org/IJCSA/issue5/2009-IJCSA-5-5.pdf

[6] Rizwan Ahmed, Rajiv V Dharaskar, “Study of Mobile Botnets: An Analysis from the Perspective of Efficient Generalized Forensics Framework for Mobile Devices”, IJCA Proceedings on National Conference on Innovative Paradigms in Engineering and Technology (NCIPET 2012) ncipet(15):5-8, March 2012. Published by Foundation of Computer Science, New York, USA. http://www.ijcaonline.org/proceedings/ncipet/number15/5302-1114

[7] Rizwan Ahmed, Dr RV Dharaskar, and Dr VM Thakare. "Mobile Forensics: the study of collecting digital evidence from mobile devices." In International Conference on Computer Networks and Security (ICCNS 2008), VIT, Pune, Sept, pp. 27-28, 2008.

[8] Rizwan Ahmed, and Rajiv V. Dharaskar. "Mobile Forensics: Process guidelines for analysis and design of efficient

generalized forensics framework for extraction and documentation of evidence from legal admissibility perspective." In First International Conference of the South Asian Society [of] Criminology and Victimology (SASCV), 15-17 January 2011, Jaipur, Rajasthan, India: SASCV 2011: Conference Proceedings, p. 132. K. Jaishankar, 2011.

[9] SWGDE and SWGIT Digital & Multimedia Evidence Glossary, SWGIT Digital & Multimedia Evidence Glossary Version: 2.3, 2009.

[10] Jansen, W., Ayers, R.: Guidelines on Cell Phone Forensics, NIST, SP 800-101, 2007).

[11] Zhang, Z.H., Luo, H.Y., Chen, L.X., Chen J.Y., "Digital home appliances industry trends, Ministry of Economic Affairs", R.O.C. (in Chinese), 2002.

[12] Ayers, R., Jansen, W., Moenner, L., Delaitre A., "Cell Phone Forensic Tools: An Overview and Analysis update", NISTIR 7387, 2007.

[13] Rizwan Ahmed and Dr. R. V. Dharaskar, "Study of Cryptographi Hashing: An Analysis From The Perspective of Developing Effiecient Generalized Forensics Framework for the Mobile Devices," International Journal of Innovative Research in Science and Techniques, vol. 3, no. June, pp. 5–9, 2012.

[14] Marc Stevens, Arjen Lenstra, Benne de Weger, "Vulnerability of software integrity and code signing applications to chosen-prefix collisions for MD5", http://www.win.tue.nl/hashclash/SoftIntCodeSign/

CONFERENCE PAPER
Two day National Conference on Innovation and Advancement in Computing
Organized by: Department of IT, GITAM UNIVERSITY Hyderabad (A.P.) India
Schedule: 28-29 March 2014