Mobile forensics: Problems and Possibilities

Jasmeen Kaur

Department of Computer Science & Engg
Swami Vivekanand Institute of Engg. and Tech., Banur, Punjab, India.

Abstract: **The mobile phones have revolutionized communications along with which their use in criminal activities is also increasing. The remarkable advancements in technology and computing power of these devices have increased their functionality. The increased functionality of mobile devices has led to it being used in various criminal activities, which arises the need of recovering the data in them. The information derived can be used as forensic evidence in various investigations. The aim of this paper is to examine the current methods involved in the forensic examination of mobile phones that can be used for proper recovery and speedy analysis of data present in mobiles.**

Keywords: **Mobile Forensics, Cell Phone Forensics, Forensic process, Evidence, Data Acquisition**

I. INTRODUCTION

Mobile Forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods [2]. Mobile phone forensic includes the methods that show how evidences are taken from mobile phones. It includes analysis of both SIM and Phone memory. Evidence items contained in mobile phones are fragile and can be easily deleted or can be overwritten. Main aim for carrying research in the field of mobile phone forensics is to extract useful information from these devices and present it as evidence in the court of law [1].

Mobile phones have become an integral part of life and are essential personal data storage and communication phones. These phones are often seized as part of criminal investigations due to the amount and nature of data stored in them. Mobile phone forensics is a relatively new and emerging field of forensics that is closely associated with computer forensics as the forensic examination is concerned primarily with digital media [3]. Mobile forensics offers many possibilities and a huge potential but there are many issues before this potential can be realized. This paper discusses various issues faced and the different methods that can be used for forensic examination of mobile phones.

II. EVIDENCE ITEMS PRESENT IN MOBILE PHONES

Mobile phones contain various evidence items which can be of interest for a Forensic Examiner. Sources of evidence in a Mobile phone may include: SIM cards, Internal Memory, Memory Cards and Network Service Providers. Other items of evidence [7] include:

- multimedia files
- messages
- e-mails
- browser history/bookmarks/cookies
- personal information
- log files
- maps
- connection information
- GPS positions
- Running processes
- Routing tables
- Network and connectivity statistics
- Boot sequence, default libraries

III. CHALLENGES ASSOCIATED WITH MOBILE FORENSICS

- Several phone models exist
- Lack of standardization while storing data
- Diverse operating systems exist
- Signals need to be blocked while carrying forensics analysis
- Blocking signals drains the battery quickly
- Large variety of data cables exist whose identification and collection is a difficult task
- No software exists for extracting data from physically damaged mobile phones
- Data tends to change due to lack of write-blocking mechanism
- Status of unopened emails and messages change after opening them
- Mobile phones may lose data on next restart once shut down
- Authentication mechanisms can confine access to data
- Data from mobile phone internal memory is restricted without the use of SIM card. Inserting another SIM can cause loss of data

IV. DATA EXTRACTION METHODS

- *Manual Extraction*- extraction carried out by the forensic examiner.
- *Logical Extraction*- extraction of information from the device using software tools.
- *Physical Extraction*- extraction of information from the device by direct access to the flash memories.

V. MOBILE FORENSIC PROCESS

The Mobile Forensic Process [7] is divided into five tages:

- *Preservation*- is the process of seizing and securing suspect property without altering or changing the contents of the data that reside on devices or removable media. It is important to document every action taken when searching for and collecting evidence.
- *Acquisition*- is the process of obtaining information from a digital device and its peripheral equipment and media.
- *Examination*- involves applying tools to uncover digital evidence including that which may be hidden or obscured. The results are gained through applying established scientifically based methods, and should describe the content and state of the data fully, including the source and the potential significance.
- *Analysis*- is the process of looking at the results of the examination for its direct significance and probative value to the case.
- *Reporting*- is the process of preparing a detailed summary of all the steps taken and conclusions reached in the investigations. It depends on maintaining a careful record of all actions and observations, describing the results of tests and examinations, and explaining the inferences drawn from the evidence.

IV. LEVELS OF ANALYSIS FOR DATA ACQUISITION

Methods for data acquisition from mobile phones depend upon their condition, model, time and nature. There is currently no standard method for analyzing internal memory of mobile phones. Based on various extraction methods, different levels of analysis can be logically made for evidence acquisition from mobile phones as shown in figure-1[1].

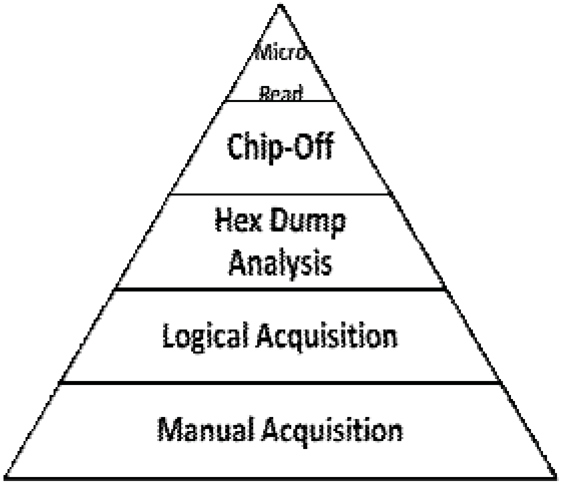

Figure-1: Levels of Analysis

• *Manual Acquisition*- involves reviewing phone documentation and browsing manually using the keypad and display of mobile phone. It will not get all data and will not recover deleted files.
• *Logical Acquisition*- involves access to the user files while connecting data cable to the handset and extracting data using software tools. It does not provide access to deleted data.
• *Hex Dump analysis*- involves physical acquisition of a mobile phone's file system. It involves either a cable connection and specific software or removing chips from circuit board and dumping contents. Data is obtained in a raw form which requires interpretation. This method provides access to deleted data from mobile phone's internal memory which is not overwritten and extracts data hidden from handset menus.
• *Chip-Off method*- involves the removal of a memory chip from mobile phone and read it in either second phone or EEprom reader to conduct forensic analysis. It extracts all data from mobile phone memory however, data is not contiguous which is hard to interpret and convert.
• *Micro Read*- involves the use of a high power microscope to provide a physical view of the electronic circuitry of mobile phone memory. This method can be used while acquiring data from physically damaged memory chips. It extracts and verify all data from mobile phone memory and is most forensically sound.

V. AVAILABLE FORENSIC TOOLS AND TOOLKITS

Forensic toolkits are intended to facilitate the work of examiners, allowing them to perform the forensic process in a timely and structured manner, and to improve the quality of the results. Forensic software tools strive to address a wide range of applicable devices and handle the most common investigative situations with modest skill level requirements. These tools typically perform logical acquisitions using common protocols for synchronization, debugging and communications. However, for the recovery of deleted data, highly specialized hardware based tools and expertise is required [5]. The variety of forensic toolkits for cell phones is diverse. The tools require the examiner to have full access to the device i.e. the device should not be protected by some authentication mechanism. While most toolkits support a full range of acquisition, examination and reporting functions, some focus on a subset. Different tools may be capable of using different interfaces like infrared, Bluetooth or serial cable to acquire device contents. Information present on a cell phone can vary depending on:
• The inherent capabilities of the phone implemented by the manufacturer
• The modifications made to the phone by the service provider or network operator
• The network services subscribed to and used by the user
• The modifications made to the phone by the user
Commercially available Cell phone and SIM tools with their functions:
• *PDA Seizure*- Acquisition, Examination, Reporting
• *Pilot-link*- Acquisition
• *Cell Seizure*- Acquisition, Examination, Reporting
• *MOBILedit! Forensic*- Acquisition, Examination, Reporting

- *BitPIM-* Acquisition, Examination
- *TULP 2G-* Acquisition, Reporting
- *GSM .XRY-* Acquisition, Examination, Reporting
- *Oxygen PM-* Acquisition, Examination, Reporting
- *SIMIS-* Acquisition, Examination, Reporting
- *ForensicSIM-* Acquisition, Examination, Reporting
- *Forensic Card Reader-* Acquisition, Examination, Reporting
- *SIMCon-* Acquisition, Examination, Reporting

Forensic software tools acquire data from a device in one of the two ways: Physical acquisition or Logical acquisition. Physical acquisition implies a bit-by-bit copy of an entire physical store, while logical acquisition implies a bit-by-bit copy of logical storage objects that reside on a logical store. In general, physical acquisition is preferable, since it allows any data remnants present to be examined, which otherwise would go unaccounted in a logical acquisition.

VI. CONCLUSIONS

Mobile forensics is a new area for research and development. To recover data from mobile phones various methods are applied. This paper summarizes the problems faced in mobile forensics and also discusses the various tools and toolkits that can be used in the mobile forensic process, so as to extract data which could be used as evidence in investigations.

VII. REFERENCES

[1] Amjad Zareen, Dr. Shamim Baig, Centre for Advance Studies in Engineering, Islamabad, Pakistan, “Mobile Phone Forensics Challenges, Analysis and Tools Classification”, 2010.

[2]Shivankar Raghav, Ashish Kumar Saxena, “Mobile Forensics: Guidelines and Challenges in Data Preservation and Acquisition”, IEEE Student Conference on Research and Development, 2009.

[3] Paul Owen, Paula Thomas and Duncan McPhee, Information Security Research Group, University of Glamorgan, UK, “An Analysis of the Digital Forensic Examination of Mobile Phones”, 2010.

[4] Jingshan Huang, Alec Yasinsac, Patrick J. Hayes, University of South Alabama, USA, “Knowledge Sharing and Reuse in Digital Forensics”, 2010.

[5] Rick Ayers, Wayne Jansen, Nicolas Cilleros, Ronan Daniellou, National Institute of Standards and Technology, USA, “Cell Phone Forensic Tools: An Overview and Analysis”.

[6] Rizwan Ahmed, Rajiv V. Dharaskar, “Mobile Forensics: an Overview, Tools, Future Trends and challenges from Law Enforcement Perspective”.

[7] http://en.wikipedia.org/wiki/Mobile_device_forensics

[8] http://en.wikipedia.org/wiki/Mobile_forensic