Major Challenges of Mobile Forensics

Mayuri Goel[1], *Vimal Kumar*[2]

Computer Science and Engineering
[1,2]*Meerut Institute of Engineering and Technology,* Meerut, Uttar Pradesh, India
[1]mayurigoel99@gmail.com, [2]vimal.kumar@miet.ac.in

Email ID- **serviceheb@gmail.com**

ABSTRACT:

With the rapid growth of mobile devices, chances of usage of mobile phones in criminal activities has also increased. Mobile phones nowadays offers wide range of functionality and services, such as Short Message Service, Multimedia Messaging Service, Internet connectivity, online transactions, location service etc. which in turn make the device more potential of providing evidence in criminal cases. There are many tools available to examine evidence from mobile device. Also, proper knowledge of forensic tools is required to identify and collect relevant information. This paper discusses about the types of digital forensics, digital evidences, challenges, mobile forensic process and tools available for mobile forensics. Identification and extraction of appropriate information from mobile phone is the objective of proceeding with mobile forensics.

Keywords: Digital forensics, mobile forensics, mobile phone, evidence

Access this Article Online	**Quick Response Code:**
Website: http://heb-nic.in/cass-studies	
Received on 23/05/2019	
Accepted on 29/05/2019 © HEB All rights reserved	

1. INTRODUCTION

Use of scientifically derived methods for the preservation of data, collection of evidence, identification of relevant information, analysis of those evidences, interpretation, documentation of investigation process and submission of evidences obtained from various sources to facilitate criminal investigation process is known as digital forensics. Digital forensics deals with the detection and prevention of cybercrime. Mobile phones are used extensively nowadays due to lower cost and ease of portability. The concept of computer forensics started back in late 1990s and early 2000s. By 2019, the count of users of mobile phone across the globe is expected to reach five billion. The count of mobile phone users in India is forecast to be skyrocketed from 524.9million in 2013 to 813.2million in year 2019.The count of subscribers of mobile phone is expected to reach 4.68billion in 2019. By 2020, almost 75% of the global population is expected to be connected by mobile phone. Digital device is not limited to computer but also includes computer, mobile phones, tablet or any electronic device.

The paper is divided into following sections: Section I explains digital forensics and mobile phone usage statistics. Section II discusses the types of digital forensics, Section III deals with mobile phones usage and evidences. Section IV tells about some challenges associated with the forensic process. Section V discusses the tools and techniques available to perform forensic investigation process. Section VI discusses how the forensic process is carried out and what steps are taken in order to preserve the evidence. Section VII concludes the paper.

Digital forensics is divided into five branches as shown in Figure 1.

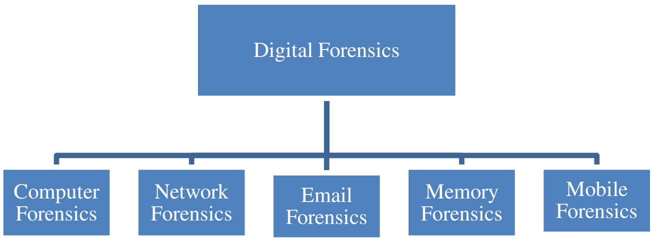

Figure 1: Classification of Digital Forensics

Computer Forensics: Collection of evidence from mobile device was easier in the early days. This field of forensics deals with questions like how to preserve data, identify relevant information, extract that information, documenting the appropriate steps taken in the process and what result can be drawn from the investigation process.

Network Forensics extracts the information about the port from where the network was accessed. The investigator and the adversary may use the same tool i.e. for investigation purpose and committing crime respectively. It identifies who gained access to the network and how they did it.

E-mail Forensics answers following questions: identity of email sender and receiver, at what time the message was sent and received which helps in knowing the source of the email. With the increased usage of email services, investigators need to identify the scams and fraud attempts made by the adversary.

Memory forensics is the analysis of computer's memory block. Memory forensics tools are used in order to extract text from the memory dump.

Mobile forensics deals with which method can be used in order to collect evidence from the devices and how evidence can be collected from those devices. Recovering potential evidences under forensically good condition from mobile phone is the known as mobile phone forensics. In order to complete the forensic process, understanding of tools and their limitation is necessary [9].

2. MOBILE PHONE USAGE AND EVIDENCES

Mobile phones contain potential evidences that can help in carrying out the investigation process. Storage capacity of mobile phones has increased from 1GB to 64GB as per the need of "mini-computer" sort of device. Now, there are mobile phones which provide storage capacity of 64GB which can further be increased by contacting the service providers. So, mobile devices are no less than computers in today's scenario. Mobile devices not only provide large storage capacity but also provide services like taking pictures, sending text messages, video calls, internet connectivity, mobile browser, wireless synchronization with other devices, and the ability to sync more than one email account to a device etc. Mobile phone size is declining while their storage capacity is increasing. Some factors that increase the need of mobile forensics are [1]:

- Mobile phones are used not only to save and share personal as well as corporate data: mobile based applications such as word processors, spreadsheets, office suite has led to increased usage of mobile phones. Newer mobile devices are incorporated with the functionality of viewing and printing documents from device making them more efficient. 'Push e-mail' service notifies the user about the new e-mail received and allows them to view and download it on mobile device only.
- Use of mobiles in online transactions like net banking, online transfer of payment etc. Enhanced connectivity and security enabled more online transactions such as using E-wallet services, shopping from online portals, hotel and flight reservations, trading in stock exchange etc.

Digital evidence is the information that is of utmost value for the investigator and is stored on a digital device. Since mobile phones provide so much services and facilities, therefore they are the evidences too. Evidence can be call logs, contact list, social networking website/application post, memory card, Subscriber Identity Module (SIM), multimedia messages, text messages, notes, browser history etc. Currently, there is no single tool available for the complete process, so investigator need to use combination of various tools for the successful completion of forensic process.

3. CHALLENGES ASSOCIATED WITH FORENSIC PROCESS

Mobile devices perform various functions ranging from a simple telephony service to providing internet connectivity etc. Mobile phones are designed for mobility that is compact in size, lightweight and ease of portability. Mobile phones have a basic set of functionality and capability including a microprocessor, microphone, speaker, memory unit, hardware components, display screen, an input interface, a radio module and an interface for providing input to the device. The internal storage capacity of mobile phones has been extended to 64GB, which can further be increased using external memory chips like memory card with maximum capacity of 2TB.

Computers are made for a general set of application whereas mobile phones perform only a specific set of functions. Mobile forensics is a challenging field due to rapid rise and change in technology. Following are some challenges associated with mobile forensics:

a) There are various mobile network carriers and device manufacturers present in the market, thus making identification of mobile phone difficult. The true hardware model can be identified once its battery is removed which may result in loss of information stored in volatile memory [2].

b) Preserving power of mobile phone is great challenge in itself as there is no standard for cable connectors. Mobile device may lose its power completely if left unplugged that is not charged for considerable time duration which may result in loss of information stored in volatile memory i.e. loss of crucial evidence[2].

c) Mobile forensic tools currently available in the market have no solution to deal with broken or damaged phone [7].

d) Newer mobile phones allow user to remotely lock their device or wipe its data. So, isolating the mobile device is necessary to prevent contamination of existing data [3].

e) In order to preserve the evidence, if the device seized is in ON state then it should be transported to the lab in the same state to avoid changes to mobile data.

f) Carrying device in ON state can allow the device to make network/cellular connections. So device should be carried in a Faraday cage.

g) Mobile device when seized should be kept in Faraday bag or other kind of blocking material, set on airplane mode in order to avoid external cellular tower connection. Turning the device off preserves its cell tower location information and call logs.

h) Analysis must be done when device is powered on, but to do it precisely, write-blocking software must be installed in order to prevent contamination of evidence. But unfortunately no standard for write-blocking mechanism is present [3].

i) Currently, there is no single tool available to perform the forensic process. So, investigator has to use combination of various tools in order to extract and analyze the data.

j) Mobile device needs to be protected from incoming communications. Text messages and call logs are stored in ‘First In, First Out’ order which on establishing connection can delete the older text messages and call logs. The device should be placed in wireless preservation container.

k) As mobile phones are more like a ‘mini- computer’, operating system used can be Blackberry, Symbian, Android, iOS, Windows Mobile etc. The challenge is having knowledge of all these operating systems and their protocols for analysis of device [2].

l) Unlocking the mobile phone is a great task too [7].

4. MOBILE FORENSIC TECHNIQUES AND TOOLS

Mobile phones and computers provide similar functionality but their software, hardware components and physical features are different. Collection of various forensic and non-forensic tools are used by the investigator for the investigation process completion. Forensic tools are associated with the data acquired from internal memory of the phone by maintaining the integrity value of data. Non-forensic tools compromise integrity of data [8].The main objective of mobile device tool classification system is to make classification and comparison of extraction method of tools easy. In Figure 2, the tool classification system is shown. The pyramid when accessed from bottom to top that is from Level1 to Level5, features offered are [4]:

- Methods get more technical
- Tools get more expensive
- Methods get more time consuming
- Methods get more ‘forensically sound'

Level 1: Manual Extraction: Here, acquisition of data is done from mobile phone and photographic documentation of data displayed on the display screen. The contents displayed on the LCD display require human intervention to operate the touch screen, keyboard or buttons to get the information. In this case, recovery of deleted information is not possible. It becomes difficult to retrieve data if the display is damaged or broken [3].

Level 2: Logical Extraction: This method is accomplished by providing connectivity between a mobile phone and forensic workstation i.e. server using either a wired (USB) or wireless (Wi-Fi or Bluetooth) connection [5].

Level 3: Hex Dump Analysis: This method deals with the acquisition of a mobile’s file system physically.

Level 4: Chip-Off: In this method, memory chip is removed from the device and is put into any other phone to perform analysis process. . This method allows extraction of complete data from device but is not cost effective [3].

Level 5: Micro Read: This method provides a physical look out of the circuit unit or say circuit of mobile phone’s memory by using a high-power microscope. This method is the most forensically sound method. This method can acquire data from physically damaged memory chip.

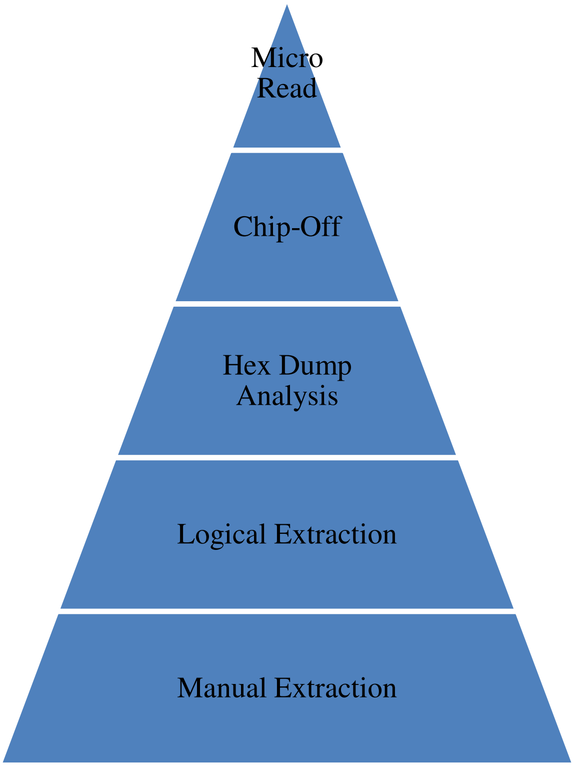

Figure 2: Mobile Device Tool Classification System

Tools available to carry out forensic process are [12] [13]:

Open source tools-

- The Sleuth Kit
- SANS Investigative Forensic Toolkit (SIFT)

Commercial tools:

- EnCase
- PDA Seizure

iOS- based tools:

- iPhone Analyzer
- XRY

Android-based tools:

- Autopsy
- MOBILEdit

5. FORENSIC PROCESS

Questions raised when mobile device is obtained during investigation are [8]:

a) How should relevant data be extracted from the device?

b) Which method is best to preserve the evidence?

c) How device should be handled?

Forensic process can be broken down into following main categories: seizure and preservation of data, acquisition of data, examination and analysis of evidences and reporting of process [5] [6].

A. *Seizure and Preservation*

This is the first and the basic step of forensic process. Mobiles when recovered in power on state should be transported in same state to avoid contamination of data and ensure data preservation. If the device is kept in ON state then the device might make cellular connection which can overwrite the existing data that's why devices are often carried in Faraday bag or any other kind of blocking material. But keeping device in Faraday bag can make the device unusable and deplete its battery very fast. Set of rules as stated under the USSS document are [1] [10]:

a) Do not turn the mobile OFF, if it is ON.

b) Note information displayed on screen.

c) Don't switch the device OFF as it can make the device lock active.

d) Power off the device before transporting the device.

e) Do not turn the mobile ON, if it is OFF as it can overwrite or modify existing data.

Preservation of evidence is done by keeping the device isolated so that contamination of data can't take place. It is very important to preserve data so as to ensure that it is successfully presented in the court of law. There are three basic steps involved [5]:

i. **Securing and evaluating the scene:** Digital data may get lost if the mobile device isn't handled with care while seizure, also physical evidence may get contaminated.

ii. **Documenting the scene:** Visible data should be recorded. All digital devices like mobile phones, removable media, power connectors are photographed along with display screen's contents.

iii. **Isolation:** There is a possibility of remotely locking the device or wiping its data. So, isolating the device from other devices to avoid contamination of data is important. This can be done by enabling 'airplane mode' or keeping the device in Faraday bag.

B. Data Acquisition: Data acquisition is the next step in the process. Acquisition is the process of cloning the device or generating its mirror image in order to gather the information from mobile device. This method has an advantage that it saves information loss caused by depletion of mobile battery. The forensic process begins with the identification of the mobile phone.

***C Examination and Analysis*:** The process of examining the evidence reveals the hidden evidence. Data reduction is done by separating relevant information from irrelevant information as soon as data is obtained. Process of analysis and examination are different in nature. Analysis process looks at the results of the examination process while examination is a more technical process. In examination, copy of data acquired from mobile device is made. With the help of features provided by mobile phone manufacturers like messaging, internet connectivity following potential evidences may be collected:

- Customer name and address
- Billing details

- Call logs
- Phonebook or Contact information
- Text messages
- Location information
- Multi-media data
- Web browsing activities
- Social media related information

D. Reporting**:** Preparing a document containing summary of steps taken out during investigation process and conclusion drawn from the investigation of a case is known as documenting or reporting. Reports contain information of case like case number, investigator name, types of evidences and relevant evidence found.

6. CONCLUSION

Technology of mobile phone is growing at a rapid pace so the need of mobile forensics has also increased as they provide crucial evidence for criminal investigation. Mobile phones reveal a lot of information such as list of incoming, outgoing and missed calls, messages sent and received, internet history, location of mobile etc. Tools like The Sleuth Kit for Ubuntu is available free of cost while EnCase is a commercial tool available for investigation process. Autopsy and MOBILEdit are tools that work efficiently for android mobile phones while iPhone Analyzer is effective for iOS mobiles. However, one tool is not sufficient to successfully complete the investigation process. So, investigators use various tools in combination for the process completion.

REFERENCES

[1]. Ahmed, Rizwan, and Rajiv V. Dharaskar. "Mobile forensics: an overview, tools, future trends and challenges from law enforcement perspective." 6th international conference on e-governance, iceg, emerging technologies in e-government, m-government. 2008.

[2]. Lutes, Kyle D., and Richard P. Mislan. "Challenges in mobile phone forensics." Proceeding of the 5th International Conference on Cybernetics and Information Technologies, Systems and Applications (CITSA). 2008.

[3]. Zareen, Amjad, and Shamim Baig. "Notice of Violation of IEEE Publication Principles Mobile Phone Forensics: Challenges, Analysis and Tools Classification." Systematic Approaches to Digital Forensic Engineering (SADFE), 2010 Fifth IEEE International Workshop on. IEEE, 2010.

[4]. Murphy, Cynthia A. "Developing process for mobile device forensics." Accessed on 11 (2009).

[5]. Lohiya, Ritika, Priya John, and Pooja Shah. "Survey on mobile forensics." International Journal of Computer Applications118.16 (2015).

[6]. Daware, Shubhangi, Sandhya Dahake, and V. M. Thakare. "Mobile forensics: Overview of digital forensic, computer forensics vs. mobile forensics and tools." International Journal of Computing Applications (2012): 7-8.

[7]. Osho, Oluwafemi, and SefiyatOyizaOhida. "Comparative evaluation of mobile forensic tools." IJ Inf. Technol. Comput. Sci (2016): 74-83.

[8]. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-101r1.pdf

[9]. https://hub.packtpub.com/introduction-mobile-forensics/

[10]. https://www.researchgate.net/publication/256460734_Mobile_Forensics_Opportunities_and_Challenges_in_Data_Preservation

[11]. https://en.wikipedia.org/wiki/Mobile_device_forensics

[12]. https://h11dfs.com/the-best-open-source-digital-forensic-tools/

[13]. Kumari, Noble, and A. K. Mohapatra. "An insight into digital forensics branches and tools." *Computational Techniques in Information and Communication Technologies (ICCTICT), 2016 International Conference on*. IEEE, 2016.