Data Acquisition From Mobile Phone using Mobiledit

Mayuri Goel, Vimal Kumar

Abstract- Mobile forensic is a subsidiary of digital forensic that is flourishing constantly. As per current scenario, mobile phones not only mean traditional mobile phones that were developed and used in late 1990s but also include smart phones that offer an array of functionality. Mobile phones developed in 1990s also known as feature phones provided limited functionality such as calling and messaging as they were subjected to provide communication facility. But at present, mobile phones are used not only for communication but also for executing face to face interactions, shopping using various applications, trading and internet surfing, etc thus making mobile more feature-variant and making them smart. Since, mobile phone market is constantly rising because of increased and improved features; usage of mobile phones in criminal activities or illegal activities has also increased. The crime scene can be re-created by identifying the series of actions that has taken place when crime was committed by using compatible mobile forensic tools. Current attack could not be prevented, but the investigator can attain all crucial evidences present on the crime scene in order to reduce similar kind of attacks in future. The capturing and recording of crime scene, collecting and analyzing the evidence and finding the culprit and reason of committing crime is the art of mobile forensics. In this paper, we are going to discuss the implementation of proposed framework by using tool MOBILedit.

Keywords: mobile phones, mobile forensic, smart phones

I INTRODUCTION

In late 1990s and early 2000s, mobile phones were introduced to provide communication facility to people. The mobile phones that were developed were bulky and heavy, comprising of antenna used to send and receive signals attached with the tower of corresponding service providing company. But at that time, usage of mobile phone was limited as they were not only expensive but cost of making calls was high [1]. In fact, not only making calls was costly, but calls received were also charged. First non-commercial mobile phone was launched in India in year 1995 in Delhi. Therefore, traditional mobile phones were just a handheld devices aimed to provide communication facility whenever needed.

Introduction of smart phones has led to a new era in itself. As per current scenario, it is not about only making calls, but about interacting with people on one to one basis. Mobile phone usage is all about staying connected with family, friends and acquaintances via social media. Mobile users just need to install these kinds of applications, place an order, fill in the shipping address, pay using various options and order is at your door step. Not only this, but mobile phones can directly be connected to printer as well. Evolution of technology led to the possibility of printing using mobile phone. Increased usage of mobile phones has made working of various departments paperless. As we all know, everything has both pros and cons. Advantage of mobile phone technology has solved the problem of taking time out from offices and standing in queues to deposit bills. They can do it on phone anywhere and anytime. In case, if mobile phone is lost or stolen and user is logged in to banking credentials, then he may lose all his personal data and money that is kept in his/her account. That's why it is recommended to sign out your account after use to avoid such mishappenings. Reduced cost and ease of portability has led to increased demand and usage of mobile phone. Everything is good in limits and anything beyond limit is harmful. Mobile is like an integral part of human life. So, there is a need of knowing the limits upto which the content must be shared. One must remember what to share, when to share and limit to share. As if not kept in mind, one can misuse your personal information and whereabouts. So, maintaining privacy and secrecy is in one's own hand and the person himself/ herself is responsible for the same.

Mobile forensics [2] deals with which method can be used in order to collect evidence [3] from the devices and how evidence can be collected from those devices. The object that is most obvious to be involved in committing crime and solving a case is mobile phone. Mobile phones possess some unique features as compared to other digital devices such as ease of portability, battery backup, volatile memory, wireless communication facility etc just to name a few. In general, mobiles are always found in active state. Recovering potential evidences under forensically good condition from mobile phone is known as mobile phone forensics [4]. In order to complete the forensic process, understanding of tools and their limitation is necessary [5].

The paper is organized as follows: section II discusses the background, literature review, potential evidences and areas of concern for collecting digital evidences while section III discusses the proposed framework which is the basis of implementation. Section IV explains the implementation of framework by using tool MOBILedit. Section V concludes the paper along with future scope.

II. BACKGROUND

Mobile phones are the handheld devices that are capable of performing every task that computers can do; this is why mobile phones act as 'mini computers' [6]. With the use of appropriate forensic tools, potential evidences can be collected and analyzed.

Revised Manuscript Received on July 18, 2019.

Mayuri Goel , Student, Computer Science at Meerut Institute of Engineering and Technology, Meerut,U.P, India.

Vimal Kumar, Associate Professor in the Department of Computer Science & Engineering at MIET, Meerut, (U.P), India.

A. *Literature review*

Lohiya et al, 2015 [7] performed survey on mobile forensics. Mobile forensic is the art of retrieving data from mobile device under forensically sound condition as mobile phones are capable of storing enormous amount of data just like laptops and personal computers and also recovery of deleted information can be done from phone just like it is done from a hard disk. Investigation steps included are:

1. Preservation of data to present it in the court of law
   a. Securing and evaluating the crime scene involves careful handling of device
   b. Documenting the scene by keeping photographic record of crime scene
   c. Isolation of mobile device from the cellular tower
2. Acquisition is the process of generating a mirror image of the device to prevent data loss.
3. Examination and Analysis is done to reveal hidden data and identify relevant information.
4. Reporting is done to summarize actions performed in the forensic process.

B. *Potential Evidences*

Useful information needs to be extracted very carefully as evidences present in mobiles are very delicate and can be easily overwritten [3]. While performing forensic process, investigator needs to be very cautious. Potential evidences can be recovered from phone by using appropriate and compatible tools. Not every tool is compatible with all types of mobile phones. Due to diversity in operating system platforms, one tool cannot work for two different operating system based devices [8] [9]. Collecting evidences is a crucial task in itself as evidence can be in many forms. For example, images can be in the format .jpg, .jpeg, .png, .gif etc. as there is no standard format for storage of images and similarly, videos can be in MP4 format for android phones while MOV format is used for iOS phones. Table I shows evidences and their sources.

C. *Evidence availability*

Evidences in mobile phone can be stored primarily at various locations i.e. in phone's internal memory, SIM card memory, external memory as maximum capacity of internal memory [10] is 512GB which is provided in latest smart phone, SIM card holds storage capacity up to 128GB while external memory chip allows 2TB of data storage capacity respectively.

- Internal memory allows maximum storage capacity of 512GB data as given in latest model of smart phone named 'Samsung Galaxy Fold' with RAM of 12GB. This smart phone is not only a phone with 4.6inch screen, but also serves as tablet with screen size of 7.3inches. Samsung is the first company that has launched a foldable smart phone cum tablet. The user can access three applications at once when used as a tablet but if used as a smart phone, the thickness of phone increases which is a negative point for Mobile Phone Company.
- SIM cards [11] that were used back in 1990s and 2000s provided limited storage capacity. The old SIM cards could store only 500 contacts while at present, they can store any number of contacts by raising the storage limit to 128GB.
- External memory chips are used to store information where storage capacity ranges from 2GB to 2TB which is very high and can store ample amount of data.

III. PROPOSED FRAMEWORK

Generally, mobile forensic process is broadly divided into four phases, named as collection, examination, analysis and reporting. We have proposed the layered architecture for mobile forensics analysis such that every layer is independent of their functionality. The layered framework is proposed in order to ease the investigation process as shown in Figure 1. Figure 2 and Figure 3 shows sub phases of layer 2 and layer 3 respectively. Proposed layered framework consists of seven layers, such that some layers are divided in subparts:

Layer 1: Prepare and strategize
Layer 2: Crime scene detection
a) Secure the crime scene
b) Photographic recording of crime scene
c) Evidence intake
Layer 3: Seizure and preservation
a) Power preservation
b) Isolation from cellular network
Layer 4: Extraction and acquisition
Layer 5: Examination and Analysis
Layer 6: Reporting and documentation
Layer 7: Close the case

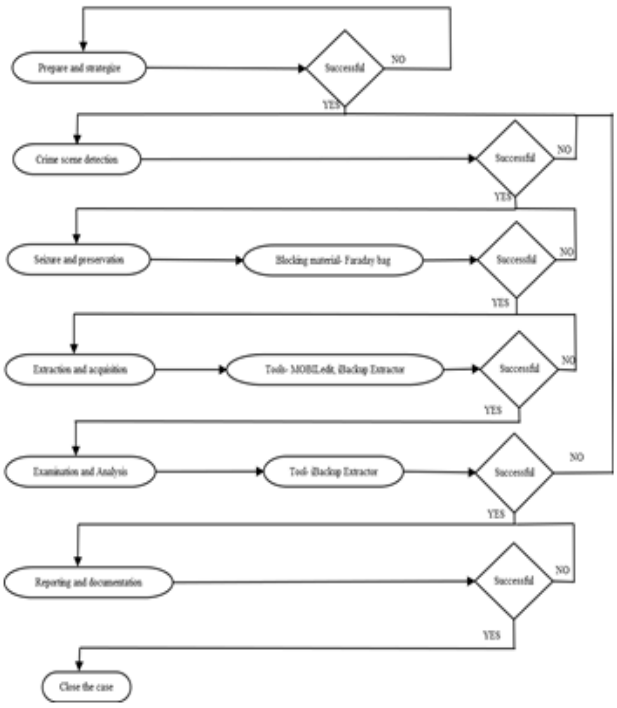

Figure 1: Layered Framework for Mobile Forensics Analysis

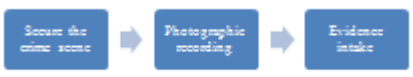

Figure 2: Subparts of Layer 2 Crime scene detection

Figure 3: Subparts of Layer 3 Seizure and preservation

A. Working

Step 1: Start from layer 1 to at least layer 5.
If successful, go to step 2
Else
Repeat step 1.
Step 2: Detect the crime scene.
If successful, go to step 3
Else
Repeat step 2.
Step 3: Seize the device and preserve it.
If successful, go to step 4
Else
Repeat step 3.
Step 4: Extract and acquire data from the device.
If successful, go to step 5
Else
Repeat step 4.
Step 5: Examine and analyze the evidences.
If successful, go to step 6
Else
Repeat step 2.
Step 6: Report and document every activity of the process.
If successful, go to step 7
Else
Repeat step 5.
Step 7: Close the case i.e. EXIT.

IV. IMPLEMENTATION OF PROPOSED FRAMEWORK & RESULTS

The above framework works on seven layers where every layer has its own functionality. This framework is implemented by using tool MOBILedit [12]. Some key features of MOBILedit are:

MOBILedit: MOBILedit version 10.0.1.25088 is used for the forensic process. This tool supports wide range of mobile phones such as Apple, Blackberry, HTC, Nokia, OnePlus and Sony to name a few. Data of mobile can be extracted by connecting via cable or by using backup, also cloud can be accessed using this tool. This tool is capable of identifying device id, device name, model and manufacturer of the device, display and wallpaper resolution. Also IMEI number is also discoverable. It allows extraction of call logs, messages, phonebook, calendar and notes entries, applications installed and multimedia files stored on the device as shown in Table II.

Table II: Data extraction comparison using MOBILedit

Attributes	MOBILedit	MOBILedit
Backup type	Without encryption	Encrypted
Manufacturer	Apple	Apple
Model	iPhone 6	iPhone 6
IMEI Number	Available	Available
Device Name	Unknown	Unknown
Device Id	Available	Available
Device Type	-	-
Version	12.1.2	12.1.4
Operator	Not available	Not available
Backup date and time	1/2/2019 12:48:50 PM	3/5/2019 3:19:28 PM
Call logs	404	202
Contacts	1017	619
Messages	137	203
Notes	No records available	No records available
Calendar	275	273
Internet	-	-
Reminders	Not supported	Not supported
Voice mail	Not supported	Not supported
Applications installed	16	17
Media	Available	Available

V. CONCLUSION AND FUTURE SCOPE

Here, layered framework for mobile forensics is proposed, which is based on the existing process and models. This framework is implemented using tool MOBILedit to complete the acquisition process. In proposed framework, number of layers can be increased or reduced as per the case type. Mobile forensics framework is of utmost value for investigation purpose in order to identify the culprit and reason of committing crime.

Future scope may be understood as to build a comprehensive framework where the proposed framework can be integrated with existing open source tools for forensic analysis. The proposed framework will facilitate ease of working and investigating as every layer has its own functionality. The layered framework can be used efficiently as it is very flexible since every layer has its own functionality and can be extended as per situation. Just like deleted data for text messages and phone calls has been recovered, the same can be done for whatsapp messages by extending functionality of this work.

REFERENCES

1. Aziz, N. A., Mokhti, F., & Nozri, M. N. M. "Mobile Device Forensics: Extracting and Analysing Data from an Android-Based Smartphone." In Fourth International

Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec), (pp. 123-128). IEEE (2015).
2. Osho, O., & Ohida, S. O. "Comparative evaluation of mobile forensic tools." IJ Inf. Technol. Comput. Sci, 74-83, (2016).
3. Kubi, A. K., Saleem, S., & Popov, O. "Evaluation of some tools for extracting e-evidence from mobile devices." In 5th International Conference on Application of Information and Communication Technologies (AICT), (pp. 1-6). IEEE (2011).
4. Daware, S., Dahake, S., & Thakare, V. M. "Mobile forensics: Overview of digital forensic, computer forensics vs. mobile forensics and tools." International Journal of Computer Applications (2012).
5. Murphy, Cynthia A. "Developing process for mobile device forensics." Accessed on 11 (2009).
6. Alhassan, M. M., & Adjei-Quaye, A. "Computer & Cyber Forensics: A Case Study of Ghana." American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS), 28(1), 167-176 (2017).
7. Lohiya, R., John, P., & Shah, P. "Survey on mobile forensics." International Journal of Computer Applications, 118(16) (2015).
8. Zareen, A., & Baig, S. "Mobile Phone Forensics Challenges. Analysis and Tools Classification." Fifth (2010).
9. Lutes, K. D., & Mislan, R. P. "Challenges in mobile phone forensics." In Proceeding of the 5th International Conference on Cybernetics and Information Technologies, Systems and Applications (CITSA) (2008).
10. Tassone, C., Martini, B., Choo, K. K. R., & Slay, J. "Mobile device forensics: A snapshot." Trends and Issues in Crime and Criminal Justice, (460), 1 (2013).
11. Raghav, S., & Saxena, A. K.. Mobile forensics: "Guidelines and challenges in data preservation and acquisition." In Student Conference on Research and Development (SCOReD), IEEE (pp. 5-8) (2009).
12. Wazid, M., Katal, A., Goudar, R. H., & Rao, S. "Hacktivism trends, digital forensic tools and challenges: A survey." In 2013 IEEE Conference on Information & Communication Technologies (pp. 138-144). IEEE (2013).
13. Ahmed, R., & Dharaskar, R. V. "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).

AUTHORS PROFILE

Mayuri Goel, currently undertaking a Masters degree in Computer Science at Meerut Institute of Engineering and Technology, Meerut. Studied B. tech in Computer Science & Engineering from Bharat Institute of Technology, Meerut, Uttar Pradesh, India. Research paper on 'Layered framework for mobile forensics analysis' has been published in 2nd International Conference on Advanced Computing and Software Engineering.

Dr. Vimal Kumar is a Associate Professor in the Department of Computer Science & Engineering at MIET, Meerut, (U.P), India. He received his B.Tech Degree in 2007 from Uttar Pradesh Technicial University, Lucknow and M.Tech degree in Information Security from Motilal Nehru National Institute of Technology, Allahabad, India in 2011. He did his Ph.D in Computer Science and Engineering from AKTU, Lucknow, India in 2017. He has published a large number of various research papers in International and National journals and conferences of high repute. His research interests lie in Mobile Ad hoc Network, Network Security and Network Forensics