A Review on Activity Extraction from Mobile Devices And Analyzing User Behavior

Ms. Thara Draupadi R
M.Tech Cyber Forensics & Information Security
College of Engineering, Kallooppara,
Pathanamthitta, Kerala, India tharar28@gmail.com

Asst. Prof. Ajoy Thomas
Department of Computer Science and Engineering
College of Engineering, Kallooppara,
Pathanamthitta, Kerala, India ajoythomas@cek.ac.in

Abstract

Mobile devices store user's personal information and even more data, becoming a personal tracker for daily activities that provides important information about the user. The present work proposes a review on tools and techniques that allows investigators to obtain a complete report and timeline of the activities that were performed on the device. This report incorporates the information provided by many sources into a unique set of data. Using this report the users with same behaviors are identified and kept in a class.
Using these data identical users are saved from different types of attacks and malwares.

Keywords: **Smartphones, Mobile forensics, Forensic tools, Acquisition techniques**

1.INTRODUCTION

Mobile devices have become an important part of person's day to day life. It made a revolution in communication nearly every population including youth and adults connecting them to internet and to each other in different places. The development of social media applications [1] made an easy way to communicate each other. According to the rapid advancement in technology, mobile devices that provided the basic functionalities of making calls and messages emerged in the form of portable mini computers. Mobile phones now have the ability to store and process data, create multimedia files, carry out high level computational tasks and access any information in the world with the vast use of Internet.

Also, a remarkable growth happened in the criminal activities along with the increased usage of mobile devices and they became main source of crimes such as harassment, sending pornographic content, trafficking, terror attacks and so on. Nowadays, mobile phones are used for performing a variety of tasks. As a result of this, they store a lot of information related to the user´s behavior. Therefore, they can be considered as an important source of evidence for forensics analysis. Also, the forensic analysis uses a set of techniques that allow the collection and extraction of data from different devices without making any changes to their original state. For example, it can recover deleted files, instant messaging information, browsing history, login data, among others, all these types of information are known as digital evidence. Three aspects should be considered during the forensics analysis: i) avoid the contamination of evidence to prevent misinterpretations; ii) act methodically, that is, all the results of the forensics process must be well documented; and iii) control the chain

of custody by using a protocol. Also, certain legal aspects are to be considered during the performance of forensics investigation [2], or otherwise, these leads to the misuse of applications, fraud, theft, dissemination of copyrighted materials, etc. Therefore, it is necessary to follow all the legal guidelines corresponding to the jurisdiction, to avoid undue exposure of personal information. Also, a variety of applications (e.g., Encase, DFF, FTK, Helix, Oxygen, MOBILEdit, UFED) are used for forensic analysis to perform the inspection of various elements of mobile phones (e.g., internal memory, applications, messages).

Now, the so-called suites take all the previous points and join them in a single analysis creating a powerful and useful tool. A method of generating unique report with all the information about the mobile device user's behavior, after collection of information from different applications that are installed on it, which runs on Android OS. Using that information, a track of the users' activities while using the mobile device are obtained.

2.MOBILE FORENSICS

Mobile forensics is the process of recovering digital evidence from mobile devices under forensically sound conditions with the help of acceptable procedures [3]. It is a new field of interest in digital forensics offering many possibilities and has huge potential. The forensic analysis of mobile phones is challenging on a number of evidential and technical levels. There requires a careful gathering and analysis of evidence that exists in a mobile phone in the form of text messages, chats, call logs, multimedia files, browsing history, GPS location and so on without compromising on the integrity of the data. Also, a step-by-step plan is needed for conducting a forensic examination. The steps involved in mobile forensics are [4]:

- Identification: This step deals with physical identification of the mobile device that can prove to be a potential source of investigation activity.
- Preservation: This step includes the seizing and security suspect property without making any alterations in the contents of data that residing in the device
- Acquisition: This is the process of imaging or obtaining information from digital evidence and its peripheral equipment and media.
- Examination and Analysis: In this step several tools are applied to obtain digital evidence including hidden data.
- Reporting: It is the preparation of detailed summary of all steps followed and conclusions obtained during investigation procedure
- Presentation: This is the final step which is the presentation of the evidence in front of court proceedings to get accepted in front of the judiciary.

3.FORENSIC TOOLS

Forensics plays a crucial role in today's data driven world. Therefore, it is essential to explore different types of mobile device forensic tools those are available now [4]. There occurs an exponential growth on cybercrimes related to mobile devices, due to uncontrolled usage in different everyday activities like storage and transmission of personal and corporate data. Online transactions are most important among them. There are two domains like open source and commercial tools with contrasting consideration including security and accessibility. These tools may differ in according to security, accessibility, quality, easiness in usage and freedom in development of software. Using well defined forensic procedures, data is extracted from mobile devices by using these tools and produce customized reports. Some forensic tools widely used are:

- **Andriller**

This is the most common tool used for android forensics due to its wide range of functionality and free cost. It contains a hoard of forensic tools used in modern smart phones. Also, it follows a forensically sound, non-destructive and read only data acquisition process. It can also crack Password, lock screen for Pattern, PIN code and also contains custom decoders for decoding communications.

- **UFED Touch**

Universal Forensic Extraction Device (UFED)Touch is a commercial GUI based tool from Cellebrit's series of products. Also, it is easy to use in touch screen. By using this tool, extraction of file system, other data and passwords from the phone is possible. The extraction of deleted data, from the widest range of mobile devices can be done. Extraction reports can be viewed on screen with the HTML report viewer. No need for PC for data extraction and reports can be viewed in the kit itself. Two versions of UFED are available:

a. **UFED Ultimate-** It is used for Physical extraction and decoding while bypassing pattern lock / password / PIN from Android devices including Samsung Galaxy S family, LG, HTC, Motorola, and more.

b. **UFED Logical-** is used for Logical extraction of data: Apps data, passwords, IM (instant messaging), contacts, SMS & MMS, emails, calendar, multimedia, call logs, phone details (IMEI/ESN), ICCID and IMSI, SIM location information (TMIS, MCC, MNC, LAC). It also supports forensic cloning of SIM ID to isolate the phone from network activity during analysis.

- **OXYGEN Forensic**

There are two versions of Oxygen Forensics and they are: OXYGEN Forensics Analyst and OXYGEN Forensics Detective. The factor that makes the tool attractive is the Zero footprint operation., i.e., leaving no traces and making no modifications to the phone content. And it is also capable to detect malicious and spyware apps installed on Android and Apple devices, discover and process their logs and configuration files. It has a property of extensive reporting with variety of graphs, which includes social networking. Also, extraction of geolocation data from alla sources are possible.

- **XRY**

It is used to perform secure forensic extraction of data from a wide variety of mobile devices, such as smartphones, satellite navigation units, modems, music players and tablets. It runs on windows operating Systemax Logical,XRY, PinPoint and XRY Physical are the three versions available.

- **MobilEdit Forensic**

This tool enables the extraction and viewing data from different sources like Contact book, call history, text and multimedia messages, files, calendars, notes, reminders, raw application data, IMEI, operating systems, firmware including SIM details (IMSI), ICCID and location area information. And also have the ability to retrieve data deleted from phone memory and can bypass the passcode, PIN and phone backup encryption techniques. Physical acquisition of Android phones and memory cards are possible using this tool.

- **Droidspotter**

Droidspotter is a tool written entirely in Java. SQL database is used to store all its data. It can be used for finding possible locations of location data from unanalyzed android applications. It also allow the extraction of data from apk files through easily available navigation pane.

- **Mobile phone Examiner Plus (MPE+)**

It owns most intuitive and user-friendly GUI Interface in the market. And also includes graphically visualization tools that allows its user to easily see communication relationships among contacts and automatically construct graphical data timelines. MPE+ is also available on a preconfigured touch-screen tablet for on-scene mobile forensics triage. MPE+ supports latest mobile device profiles and features advanced carving, deleted data recovery, SQLite database browsing, advanced analysis, filtering options and has inbuilt support for query and script building.

- **VIAEXTRACT/Now Secure**

It is one among the powerful analysis and reporting tools for Android smart phones and devices. And it supports all the three types of data acquisition; Logical, Physical and File System. And have two versions; commercial and noncommercial. The noncommercial version has as features like screen lock bypass tool, automated data parsing, deleted data recovery, artifact viewer, global search, timeline, android filesystem, logical, backup extraction. Commercial version has all the features of noncommercial with android physical extraction, file carving and reporting.

4. ACQUISITION TECHNIQUES

The most important step in Mobile Forensics is the data acquisition [5]. It is necessary to acquire both deleted and undeleted data present in mobile phones in order to discover relevant artifacts and find meaningful insights from them. Manual examination of the mobile devices is done in Manual acquisition. This is a simplest technique and is suitable when there is an immediate need to obtain evidence from the device. Another acquisition methods are: Logical acquisition and Physical acquisition.

4.1 Logical acquisition

A bit-by-bit copy of logical storage objects are obtained from the allocated spaces in the memory of the mobile device. These techniques will fail in the recovering of data from the slack spaces and hence cannot obtain the deleted data. These are best suitable for unrooted devices even though the data recovered is less as compared to physical acquisition. USB debugging mode enabled on the mobile device is the only requirement for performing logical acquisition.

- **ADB Pull**

The ADB daemon running on the device runs with the shell permissions on unrooted. As a result, maximum evidential files are not accessible. They can still access useful files such as unencrypted apps, most of the tmpfs file systems that can include user data such as browser history, and system information. However, if there are root privileges, then ADB pull method is effective to analyze the files of interest from the workstation.

- **Backup analysis**

A lot of backup options are available to store the mobile device data in a particular location and restore it back as needed. Many of the backup utilities have a SD Card option as well as options to save data to the cloud. a backup image obtained from the phone is utilized to carry out the investigation.

- **AFLogical**

It is an Android forensics logical technique which is distributed free to law enforcement and government agencies. These takes advantage of the Content Provider architecture to gain access to data stored on the device. Some of the Content Providers are:SMS/MMS,Contacts,Calender.

- **Commercial providers**

Many of the commercial mobile forensic software vendors now support Android based acquisition.It is very helpful for a forensic analyst to understand how each of the forensic software vendors implement Android support. Some Commercial

Providers are Cellebrite UFED, CompelsonMOBILedit and viaForensic's viaExtract

4.2 Physical acquisition

Physical acquisition is based on bit-by-bit copy of an entire physical storage [6]. It allows extracting deleted, obsolete data along with the other contents from a mobile device. It can be performed after gaining the root level access of mobile devices so as to get complete control to the system.

- **Hardware based Acquisition**

There are methods which connect a hardware to the device or physically extract device components. These types of methods work specially on unrooted devices but require forensic analysts who have expertise training in forensic.

1) **JTAG**: Joint Test Action Group has specified specifications for printed circuit boards (PCB) testing and

debugging called boundary scan. Investigators use JTAG to access and retrieve content of memory chips and create forensic images of these chips.

2) **Chip-off:** This method allows the recovery of damaged devices and also circumvent pass code-protected devices. However, the physical removal of NAND chips often damages the connectors on the bottom of the chip, and as a result damage the data.

• **Software based Acquisition**

This method uses a software on devices to obtain digital artifacts. There is no physical removal of the hardware components so, it does not cause permanent damage to the device. Therefore, this acquisition works only with root privileges with USB debugging enabled. From a forensics standpoint, temporary root privileges or root access via a custom recovery mode are preferred. Many commercial and open-source vendors are available who provide physical acquisition software such as:

a. Cellebrite UFED

b. Oxygen Forensic Suite

c. Wondershare Dr. Fone for Android

5. LITERATURE SURVEY

5.1 Forensic investigation and analysis on digital evidence discovery through physical Acquisition on smartphone

Users give less concerns on the smartphone and social networks security risks, this paved way for cybercriminals to change their strategies. The security risk includes spams, that will threaten them as they are more dependent on the smartphone. Therefore, it is necessary to perform the smartphone forensics analysis to retrieve and analyzed the potentially great amounts and extremely valuable information on these devices.

This paper investigates about personal and sensitive data by types of digital information as evidence and conducted forensic analysis on a popular smartphone Samsung Galaxy Note III. Physical acquisition technique [6]is used for the data extraction and analysis is done using Cellebrite UFED. The evidence discovered include files, contacts, events of smartphone and social network data storage and location. Performing the extraction and analysis of digital evidence over smartphone activities show the possibility of identifying potential suspects that could assist the forensic investigators in crime investigations.

5.2 The next generation for the forensic extraction of electronic evidence from mobile telephones

A wealth of information about the user can be extracted from a mobile phone.

Before a court considering the electronic evidence, the court must ensure that the subject matter, testimony of which is to be given, is scientific. Therefore, at the investigation stage, be given to fulfill the requirements of science and law, including international standards. Such compliance also moves the extraction of electronic evidence from mobile telephones into the next generation, by being able to give in court well- reasoned and concrete claims about the accuracy and validity of conclusions [3].

5.3 A critical review of 7 years of Mobile Device Forensics

Mobile Device Forensics (MF) is an interdisciplinary field consisting of variety of techniques applied to a wide range of computing devices, including smart phones. From the last few years, a significant amount of research has been conducted in various mobile device platforms, data acquisition schemes, and information extraction methods. This work presents a detailed assessment of the actions and methodologies taken throughout the last seven years. This categorization chart also serves as an analytic progress report, with regards to the evolution of MF [7].

5.4 Android Phone Forensic: Tools and Techniques

Now a days mobile phones have become so intrusive in our daily lives because they can give huge amount of information to forensic examiners. This work aims to bring them together under a comparative study so that this paper could serve as a starting point for several android users, future forensic examiners and investigators. After conducting various survey, scarcity for papers on tools for android forensic were found. In this paper an analysis of different tools and techniques used in android forensic and at the end tabulated the results and findings [4].

6. METHODOLOGY

During the forensic investigation, the investigator needs to deal with different types of files. All these files are stored in a folder. Also, all the files are sorted and arranged in chronological order. And the redundant data are eliminated. The forensic investigator [8] logins and gives start and end date. At that time activities happened at particular time period will be displayed. Through this investigator can access data. After the analysis, the person having same behavior are classified into various groups i.e, those having same type of browsing history, downloads, applications. Therefore, investigator can easily detect those performing illegal activities. Moreover, the investigator can filter the information relevant to the case.

7. CONCLUSION

It is necessary to select right tools for the acquisition of evidence that serves as input to the application represents a crucial piece of research; however, none of them possess the ability to acquire all the information of a mobile device. And also, suitable acquisition technics are required it is essential to obtain a desired result. The evidence has to be carefully manipulated, because if the information is altered in any way, this will not be valid for the investigation. It is necessary to follow all the legal guidelines corresponding to the jurisdiction where the conflict is generated, to avoid undue exposure of personal information.

REFERENCES

[1] D. Walnycky, I. Baggili, A. Marrington, J. Moore, and F. Breitinger,"Network and device forensic analysis of Android social-messaging applications," Digit. Investig., vol. 14, no. S1, pp. S77–S84, 2015

[2] M. Taylor, G. Hughes, J. Haggerty, D. Gresty, and P. Almond, "Digital evidence from mobile telephone applications," Comput. Law Secur. Rev.,vol. 28, no. 3, pp. 335–339, 2012.

[3] H. K. S. Tse, K. P. Chow, and M. Y. K. Kwan, "The next generation for the forensic extraction of electronic evidence from mobile telephones,"Int. Work. Syst. Approaches Digit. Forensics Eng., SADFE, 2014.

[4] S. Yadav, K. Ahmad, and J. Shekhar, "Analysis of Digital Forensic Tools and Investigation Process," High Perform. Archit. Grid …, pp. 435–441,2011

[5] Shalini,Vibhuti Narayan Singh,Mukesh Yadav and Pooja Rastogi: "A Forensic Approach for Data Acquisition of Smart Phones to Meet the Challenges of Law Enforcement Perspective", J Indian Acad Forensic Med.,vol.37,No.2,April-June 2015.

[6] Tanizia Binti Tajuddin and Azizah Abd Manaf:"Forensic Investigation and Analysis on Digital Evidence Discovery through Physical Acquisition on

Smartphone", World Congress on Internet

[7] K. Barmpatsalou, D. Damopoulos, G. Kambourakis, and V. Katos, "A critical review of 7 years of Mobile Device Forensics," Digit. Investig.,vol. 10, no. 4, pp. 323–349, 2013.

[8] Security(WorldCIS-2015)."ISO/IEC 27037:2012 - Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence. [Online]. Available:https://www.iso.org/standard/44381.html. [Accessed: 30-Aug-2018].