Review of Forensic Analysis of Android Smartphones

Chayal Narendrakumar M.[1], Dr.Ravi K. Sheth [2]
[2]Assistant Professor, Dept of IT
[1, 2] Raksha Shakti University, Ahmedabad

Abstract- *Cybercrime is spreading day by day and now become a part of routine life of users. With ease of smartphones and internet, which creates opportunity for the cyber criminals to commit such cybercrimes by utilizing smartphones.Theyprovide all-most similar features and functionality which are available in Computers and Laptops. The mobility and flexibility of smartphones leverages accessibility of user to store their personal and confidential information. Easy communication via internet technology provides feasibility to share and communicate on social media, Emails, internet banking, and web browsing. Android, ios and windows are the major operating systems for smartphones. Among them Android and ios (iphones) are most popular. This paper proposed forensic analysis of android based smartphones specified with different tools and techniques. Forensic investigation plays crucial role to prove and testify the impact of crime in court proceeding. Author has proposed memory analysis, data acquisition and extraction, call history, application history, chat, History etc. Author has explored the existing literature of the mobile forensic and focused on the core area of the android mobile operating systems.*

Keywords- Mobile forensic, Smartphone forensic, Android forensic, Ios forensic, Digital Forensic, Cyber Forensic

I. INTRODUCTION

Smartphones are the prima facia evidence for the forensic expert to analysis[1]. Number of mobile users are increasing Day by day which generates new threats and sophisticated crime in the field of cyber forensics. Further, new research in field of cyber forensics reveal new methods and technique. There are numerous tools available for gathering relevant information from a mobile phone and few of them are specific with their advantages and limitations. Apart from personal use smartphones play critical role in the business and corporate world. Mobile phone technology is changing rapidly, new technological innovations in field enhancing security features of smartphones and tablets. Corporates, business persons, bankers, doctors etc are spending at least 35 to 40 % of working time by using smartphones with their personal and confidential information. The big two rivals Android and IOS operating system have occupied most of the smartphone users with numerous applications and communication technology[2].These mobile applications provide superior features like, sms, mms, audio video chatting and calling, Email, internet banking, GPS, calendars, personal diary and notes, social media, etc. But criminalsuses these resources to perform such crime like harassment and stalking through social media (Facebook, Whatsapp, Instragram, Hike, Twitter, etc), email frauds. Terrorists' uses social media applications to perform mind wash of people to involve them in criminal activities. Illegal gambling, betting, and tricky games like Blue whale with easy accessibility via smartphones and tablets leverage criminal activities in our society. Forensic investigation of smartphones are the post criminal activity to identify such criminal activity and useful in court of law against criminal.

Here these smartphones are source of very important information during course of forensic investigation like call history, chat history, images, which may be deleted from the mobile device[3]. This paper proposes forensics methodology of acquiring image and data from the Android devices. This review paper is divide in 5 section, Section 2 includes existing research work on particular problem with android system overview and architecture. Section 3 includes forensic methodology along with forensic tools for data analysis and recovery. Section 4 includes future recommendation and last section is conclusion.

II. EXISTING WORK

All smartphones and tablets runs using a specific software called operating system. These operating systems are responsible to manage hardware and software resources of the smartphones. All the supported application software runs on the operating system. There are numerous operating systems available in the market like Android, ios, Symbian, blackberry, Bada, windowsetc and some specific operating system for specific device. But Android andIos are the most popular operating systems. This paper proposes study of existing literature based on Android operating system. Further part of paper elaborates android operating system overview, architecture and forensic methodology.

III. ANDROID OPERATING SYSTEM OVERVIEW

Android operating system is developed on linux kernel 2.6 [4] which is responsible for hardware and software abstraction. Android operating system consist of a Dalvik Virtual Machine which is internal sandbox framework for executing multiple application at a same time with privilege control mechanism. Android application generally consist of .apk (android package) extension, along with manifest and resource file. Apart from that important system files, core libraries and configuration files are stored in the main memory. Deep knowledge of android operating system and memory architecture is must for forensic investigator.

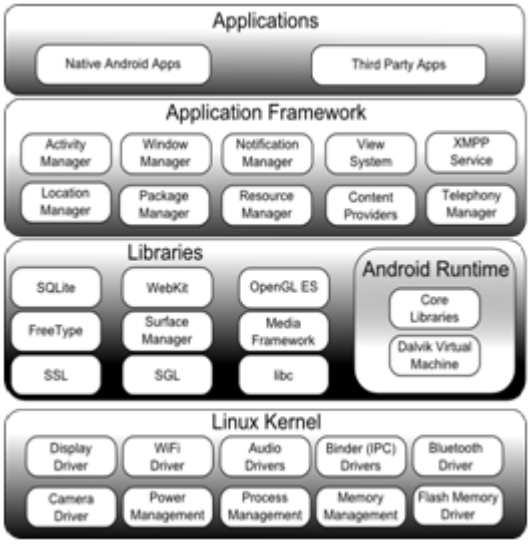
Android Architecture

Android architecture consists of mainly five layers shows in Fig1. Android architecture is consist of a five layers which are application, application framework, libraries, Linux kernel and android runtime. The Linux kernel is responsible for providing abstraction between software and hardware such as display driver, audio Wi-Fi driver etc. Applications are developed by third party in java.

IV. FORENSIC METHODOLOGY

Existing study regarding mobile forensic deals with five phases. But process of data acquisition, file system, rooting mechanism, operating system and application structures is different. Some mobile manufacturing companies have their own GUI and other application installed which restrict from taking a root privilege[5]. In some special cases experts write new rooting script to gain root access for smartphone. The most normal methodology is to use adb(android debug bridge) for making a backup of device. DD command is also utilized to make backup of device in Linux operating system[6].

Forensic researchers has found another methodology based on yaffs2 file system. By using this critical information has been recovered and analysed [7].We can also make backup of android phone using clockworkmod(CWM)which is a custom full data backup and recovery by using sdcard. Backup file is stored in sdcard and we can perform forensic operations on that backup file.Fig.1 [10]



There are few commercial tools like UFED, Encase, and Oxygen Forensic suite for recovering and analysing android device. In smartphones data can be gathered by three ways manual data extraction, logical data extraction and physical data extraction. Generally forensic expert focuses on mainly device logs, network traffic, file system, memory and applications.Further we will discuss about logical and physical extraction of data.

V. LOGICAL EXTRACTION OF DATA

Logical extraction consist of a bit by bit copy of data or storage in to memory card or forensic workstation. This consist of android system directories and related files. This method allows us to extract and recover deleted data also but for that some special tools are required. There are few tools available which are open source and commercial version. Few tools are as follows

1. SAFT

SAFT is freeware mobile forensic tool which is used to extract important information from mobile device like call detail, sms/mms, contact list, browser history, notes, social media detail like whatsapp, facebook, twitter, Instagram, email, calendar details etc.

2. LiME (live memory extractor)

This tools is used to extract volatile memory (RAM) from the mobile device which is useful to analyse recent activity of the mobile user. It provides facility to dump memory in sdcard& on network as well. Live memory or ram dump can be analysed with volatility tool to extract social

media application password, email password, bank application password etc[8].

3. Andriller

This tool is used to crack the PIN, pattern lock andpassword applied on the mobile device. Furthermore, it is used to decrypt the backup files

VI. PHYSICAL EXTRACTION OF DATA

In this process data are extracted bit for bit from the entire storage media of device. This is a traditional forensic method and it allows us to recover deleted data smoothly with maximum output. This is not an easy task for forensic examiner because of a device's manufacture security. Sometimes forensic expert has to develop custom boot loader to get the root permission of mobile device.

Here is the step by step procedure to acquire image of the android smartphone

1. Getting root access:

In some cases expert needs to root the smartphone to get the root permission but there are some other open source tools available which extract data without rooting a device as well but with some limitations. (AFLogic) To root the android device experts generally use authenticate source like kingoroot, srsroot,iroot etc.

2. Memory acquisition of smartphone

For windows, expert uses android tool kit with jdk (java developer kit) and adb(android debug bridge) with some specific command. Expert needs to enable usb debugging option from the developer options of the phone and connect phone to workstation. Now it needs to open android SDK tool from the program file in windows and use command adb devices.

It will show you a connected android device with serial number.

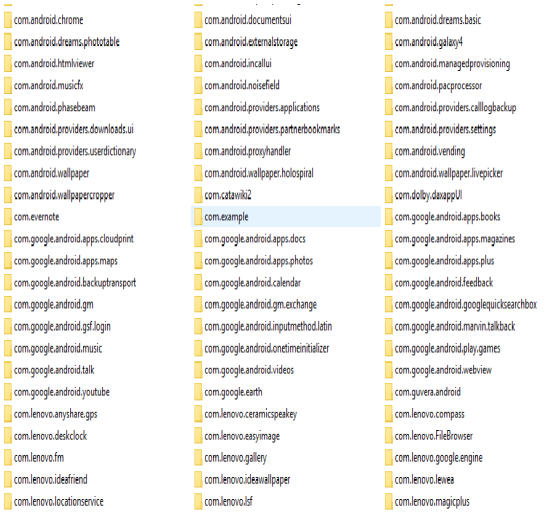
Use command adb backup [-f <file>] [-apk|-noapk] [-shared|-noshared] [-all] [-system|nosystem] [<packages...>].

Phone screen shows option to perform full backup option. For linux user expert needs to install adb tool kit after that dd tools should be used along with ddif=/emmc@usrdata of=/storage/sdcard1/data-image.dd this command and copy all the extracted data to forensic workstation[9].

Forensic analysis of acquired image

Acquired image should be keep safe and can be analysed with the help of different forensic tools such as FTK, Volatility etc. The image contains different folders like /data, /cache, /media, /system etc can be analysed by FTK imager. The key evidence like call history, chat history, sms detail, browsing history, system and network logs etc can be analysed to present in court of law. Apart from that expert can use android image extractor tool to extract the backup image of smartphone which shows android complete file structure with database. For example contact list is stored in /data/data/com.android.providers.contacts/contactlist.db. This .db is database filer which can be viewed in Sqllite database browser. Same way all the system files contains .db files which shows the data.Some of the android phone supports auto call records enabled by default so in this case /data/data/com.android.providers.media with .db file. Here figure -1 shows some of extracted data with android system files.

Extracted android system files



VII. FUTURE RECOMMENDATIONS

Android is open source operating system and it is not limited. So in future new version of android operating system like version 7 and upcoming versions will create challenge for forensic analyst. Some smartphones companies like Samsung and google nexus has improved there security by using some specific security software.Smartphone makers are increasing security by using high level encryption algorithm to encrypt user data, PIN, pattern, passwords, biometric face recognition, WhatsApp data encryption. To decrypt and find relative evidence from data which is a big challenge for forensic analyst.

VIII. CONCLUSION

Android smartphones are increasing security constantly and leveraging computing, communication and user functionality. The open source nature of android smartphones increased complexity and raised questions against integrity of smartphones. But provides and supports various open source forensic analysis tools. Forensic analysis of android smartphones has identified modern smartphone crimes with suitable evidence to justify it in court of law. Author has discussed artefacts finds during forensic analysis with some open source tools.

REFERENCES

[1] Smartphone Forensics Analysis: A Case Study, Mubarak Al-Hadadi and Ali AlShidhani , International Journal of Computer and Electrical Engineering, Vol. 5, No. 6, December 2013
[2] Forensic Analysis of Android Mobile Devices,V. Venkateswara Rao, Dr. A.S.N Chakravarthy, IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2016), December 23-25, 2016, Jaipur, India
[3] Forensic Analysis on iOS Devices, Tim Proffitt, HamedKhiabani , SANS Institute
[4] Forensic Analysis of Android Mobile Devices,V. Venkateswara Rao, Dr. A.S.NChakravarthy, IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2016), December 23-25, 2016, Jaipur, India
[5] Mobile Forensics: an Overview, Tools, Future trendsand Challenges from Law Enforcement perspective, Rizwan Ahmed1* and Rajiv V. Dharaskar1, *Emerging Technologies in E-Government*, G. H. Raisoni College of Engineering and Technology, HingnaRoada, Nagpur.
[6] Mobile Forensics:Comparison of extraction and analyzing methods of iOS and Android, DmitrijsAbalenkovs, Petro Bondarenko, Vijay KumarrajuPathapati, Andre Nordb,Gjovik university college, Dec 2012.
[7] A. M. Noora Al Mutawa, Ibrahim Baggili, \Forensic analysis of social networking applications on mobiledevices," Elsevier, 2012.
[8] E. Arvidson, \Encryption on the android." http://www.ehow.com/info_12183909_ Encryption-android.html. (Accessed on 14/12/2017)
[9] C.-T. L. Sheng-Wen Chen, Chung-Huang Yang, Design and implementation of live sd acquisition tool in android smart phone," IEEEXplore, 2011.
[10] http://www.techotopia.com/index.php/An_Overview_of_the_Android_Architecture