A Review of Forensic Data Analysis and Recovery of Android Devices

Khushboo Malakar[1], Dr.Priyanka Sharma[2]
[1]Student, Raksha Shakti University, Ahmedabad
[2]H.O.D, Department of IT, Raksha Shakti University, Ahmedabad

Abstract*-As mobile devices grow in popularity and ubiquity in everyday life, they are often involved in digital crimes and digital investigation as well. While doing forensic investigation of the digital devices which are involved in the crime needs special tools and techniques to seize, acquire and analysis of the android devices. The methodology encompasses the tools, techniques and procedures needed to gather data from a variety of common devices. Author has proposed memory analysis, data acquisition and extraction, call history, application history, chat, History, browser history etc. Author has explored the existing literature of the mobile forensic and focused on the core area of the android mobile operating systems.*

This paper proposed forensic analysis of android based smartphones specified with different open source tools, commercial tools, techniques and paper highlights various techniques available in the market in terms of logical acquisition, physical acquisition and analysis, commands File system acquisition and File system extraction.

Keywords-Mobile Phone Forensics, Handheld devices, Smartphone forensic, Android forensic, Cyber Forensic

I. INTRODUCTION

Many of the portable devices like Smartphone, tables, PDAs and many other electronic handheld gadgets are running using software program called operating system to manage the hardware and applications.

The mobile operating system is the software platform on top of which other programs, called application programs, can run on mobile devices. Many mobile operating systems are available in the market such as Apple iOS, Google Android, BlackBerry OS, Nokia's Symbian, Hewlett-Packard's webOS (formerly Palm OS) and Microsoft's Windows Phone OS. Out of these Google Android is the popular and mostly used. As Mobile Device use becomes more widespread, Mobile Device forensics becomes more and more important as Mobile Devices are often found in crime scenes. Mobile Device forensics, being part of digital forensics, aims at the retrieval or gathering of data and evidence from mobile phones and similar devices used in daily life.

The purpose of a Mobile Device forensic tool is to obtain data from a Mobile Device without modifying the data. The tool should provide critical updates in time to keep pace of the rapid changes of Mobile Device hardware and software. The tools can be either forensic or non-forensic, which each of them providing different challenges as well as allowing for different solutions.

Forensic tools are tools that are designed primarily for uncovering data from Mobile Devices, while non-forensic tools are not designed for uncovering data but can be manipulated for that purpose.

In the below sections android architecture and various forensics methods available and various tools features are discussed. This paper discussed about Android OS, architecture, Kinds of anti-forensics, Forensic Methodology, in Section 1, presented literature review of existing work carried out in the area of android forensics in Section 2, Various methods and tools existing for conducting forensic activity on android OS are discussed in Section 3,Section 4 includes future recommendation and last section is conclusion.

Android operating system overview

Android operating system is developed on linux kernel 2.6 [1] 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.

II. 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

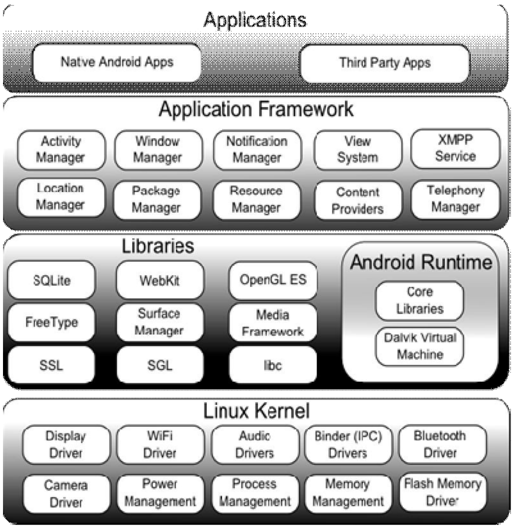
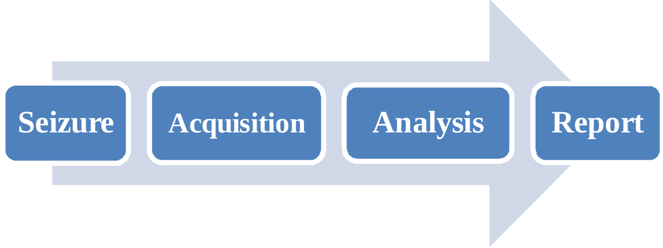


Fig.1 [9]

III. FORENSIC METHODOLOGY

Mobile forensics is the process to analyses the mobile phone to detect and collect the evidences related to the crime. A method is proposed to analyse the mobile phone to detect crime, main focus of the method is to analyse mobile phone internal and external memory and SIM card. Mobile forensic process of mobile devices [2].

There are four phases in mobile forensic process:-



IV. LITERATURE REVIEW

The National Institute of Standards and Technology defines mobile phone forensics as, “the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods”. Several works have been published for carrying out forensic activity on android OS in terms of file system analysis, study of OS architectures, processes, kernel module, rooting mechanisms, analysis of various applications, analysis of instant messaging applications, android malicious application detection and analysis and many more. In the initial study of existing android forensics methods, it is observed that special rooting scripts and methods have been used for gaining root user privileges on the device. With the gained super user privilege, imaging of required partitions and disks of the device using dd command through Android Debug Bridge (ADB). The acquired images are analysed using traditional forensic tools or other commercial tools [3]. A general method for digital forensics collection on android devices has been discussed through special boot methods enabling the use of custom recovery booting, data on Android Several more works have been published with respect to various social networking applications, instant messaging applications, web browsers and many other categories of applications [4].

V. ANDROID FORENSIC METHODS

Currently, this paper discusses about four major types of acquisition methods namely logical acquisition, physical acquisition, Command Line Tools System and File system acquisition.

Logical Acquisition methods and tools

In logical data acquisition data stored in the memory are acquired by using the file system or the protocol of a chip provider. It is a process of bit-by-bit copying of logical storage objects such as file system, directories and files.

Andriller

It is a utility which consists of various tools for serving various purposes which includes cracking of screen lock pattern, PIN and passwords, decoding of encrypted databases and files, data extraction automatically and unpacking of android backups.

WhatsappXtract

WhatsappXtract is a WhatsApp Backup Messages Extractor for Android and iPhone devices. These tools are able to read whatsapp chats using a backup file. In this it will read older messages, chats and other information in whatsapp backup file and can display on the computer. This tool is specifically used for Whatsapp application.

LiME Module

LiME or formerly called as DMD module used to dump RAM contents of the phone which will give details about recent user activities, process details, memory structures and many more volatile content.

AFLogical

AFLogical is a logical memory acquisition tool for Android devices. The user installed in the device will acquire the contact list, call logs, SMS, MMS and MMSParts and info.xml file details are send to the forensics workstation. Tool acquires logical memory details of the device.

Nandroid Backups

Nandroid Backups is another method for extracting the total file system of the device using NANDroid backup.

SAFT

SAFT is easy-to-use mobile forensic tool used to extract valuable information from the device such as Call logs, SMS/MMS logs, contacts list, file browser logs, browser history, bookmarks, facebook and twitter logs, Youtube and instagram logs, Viber, Whatsapp and Skype logs, Email messages, location history and calendar.

Physical Acquisition and tools

A physical data acquisition from a mobile device means that a bit-for-bit copy of physical storage is extracted. This would give a forensic examiner a bit-for-bit copy of the mobile device’s flash memory; this is similar to the way data is acquired in traditional computer forensics. [7]

Cellebrite UFED Physical analyser

Unified Forensic Examination Device is hardware forensic examination device for extraction of evidences from mobile devices. CelleBrite (UFED) Communicates with a cell phone via a data cable, infrared (IR), or BlueTooth (BT). UFED can acquire data (logically and physically). UFED physical analyzer which analyzes every segment of a device’s memory using advanced logical, file system and physical extractions. Using simple stand-alone method with UFED, an examiner can recover MMS/SMS messages, call logs, photos, video, and contact information [9]. UFED mainly focuses on logical extraction only. It does not recover emails, browser or search history.

Oxygen Forensics Suite

Oxygen mobile forensic Suite is used for logical acquisition and analysis of cell phones, PDAs and Smartphone’s. This software kit is a proprietary and having registration key for forensics workstation.

XRY Complete with PinPoint and Cloud

XRY is a purpose built, software based solution, complete with all necessary hardware for recovering data from mobile devices in a forensically complete secure manner.

MOBILedit Forensic Express

MOBILedit Forensic Express, you can extract all the data from a phone with only a few clicks. This includes deleted data, call history, contacts, text messages, multimedia messages, photos, videos, recordings, calendar items, reminders, notes, data files, passwords, and data from apps such as Skype, Dropbox, Evernote, Facebook, WhatsApp, Viber, Signal, WeChat and many others.

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.

Command line tools system

Mobile devices don't offer the chance to run or boot from a CD, connecting to a network share or another device with clean tools. System commands square measure the most cost effective technique; however imply some risks of knowledge loss. Each command usage with choices and output should be documented.

dd command

For external memory and also the USB flash drive, acceptable package, e.g., the UNIX operating system command DD, is required to create the bit-level copy. What are more USB flash drives with memory protection don't would like special hardware and may be connected to any pc.

AT commands

AT commands square measure recent electronic equipment commands, e.g., Hayes command set and Motorola phone AT commands, and might so solely be used on a tool that has electronic equipment support. Exploitation these commands one will solely acquire data through the software package, such no deleted information will be extracted.

File system acquisition

Logical extraction usually does not produce any deleted information, due to it normally being removed from the phone's file system. However, in some cases—particularly with platforms built on SQLite, such as iOS and Android—the phone may keep a database file of information which does not overwrite the information but simply marks it as deleted and available for later overwriting. In such cases, if the device allows file system access through its synchronization interface, it is possible to recover deleted information. File system extraction is useful for understanding the file structure, web browsing history, or app usage, as well as providing the examiner with the ability to perform an analysis with traditional computer forensic tools. [8]

VI. CONCLUSION

This paper also studied various free and commercial mobile forensics tools directed on Android devices specifically. Due to availability of vast number of models and manufacturer specific customizations many of existing tools does not support all the devices and does not have the same steps to carry out digital investigation process. Each tool is having its own procedure to acquire and analyse the data in forensically sound manner. A forensic investigator should have knowledge of hardware and software and detailed understating of the architecture to select appropriate tool for the required task. The fastest growing and increased use of Android platform urging the digital forensics community to develop a standard framework to facilitate digital investigation of mobile device, PDAs, tablets and other Android enable devices.

ACKNOWLEDGEMENT

We would like to thank our institute to grant permission to perform our research work on such topics and providing all the required materials to us. I would like to thank my parents and friends for their constant support and encouragement.

REFERENCES

[1] 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

[2] Mobile Forensics: an Overview, Tools, Future trends and Challenges from Law Enforcement perspective, Rizwan Ahmed1* and Rajiv V. Dharaskar1, Emerging Technologies in E-Government, G. H. Raisoni College of Engineering and Technology, Hingna Roada, Nagpur.

[3] Jeff Lessard and Gary Kessler, “Android Forensics: Simplifying Cell Phone Examinations”, Small Scale Digital Device Forensics Journal Vol. 4, No.1, ISSN# 1941-6164, September 2010.

[4] Noora Al Mutawa, Ibrahim Baggili and Andrew Marrington, “Forensic analysis of social networking applications on mobile devices”, Digital Investigation 9, S24–S33, 2012.

[5] Mobile device forensics: Wikipedia, the free encyclopedia.

[6] Andri P Heriyanto,”Procedures and Tools for Acquisition and Analysis of Volatile Memory on Android smartphones”.

[7] Henry, Paul. "Quick Look – Cellebrite UFED Using Extract Phone Data & File System Dump".Retrieved 21 July 2012.

[8] Howard Chivers, “Private browsing: A window of forensic opportunity”, Digital Investigation 11, 20–29, 2014.

[9] http://www.techotopia.com/index.php/An_Overview_of_the_Android_Architecture