International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Mobile Device Forensics: Extracting Data from Unallocated Space

Goka Madhuri[*1], Dr. Ravi k Sheth[2]

[*1]Student M.Tech Second Year, Department of IT & Telecommunication, Raksha Shakti University, Ahmedabad, Gujarat, India

[2]Asst. Professor, Department of IT & Telecommunication, Raksha Shakti University, Ahmedabad, Gujarat, India

ABSTRACT

The number of smartphone users are increasing day by day and majority of people rely on it for communication and business related matters With ease of smartphones and internet, which creates opportunity for the cyber criminals to commit such cybercrimes by utilizing smartphones. Therefore, The mobility and flexibility of smartphones leverages accessibility of user to store their personal and confidential information. However, investigators may face problems in extracting crucial information and the vital data stored in the smartphone. The aim of this work is to explain how to extract the data from an unallocated space in android mobiles using tools like autopsy,santoku , Encase.

Keywords: Android Mobiles, Extracting Data, Unallocated Space, Autopsy, Santoku.

I. INTRODUCTION

Smartphone is the most common mobile device own by many people to communicate, organise and coordinate tasks with others. The capability and the users of these devices increase each year. Based on statistics from 2009 to 2016, the number of smartphones sold worldwide increased rapidly. With the huge availability of smartphones, there is also high rise of it being used for crime purposes. The process of gathering digital evidence from a mobile phone, under forensically sound conditions, using well accepted methods is defined as mobile forensics.

A digital forensic investigation process comprises of four main steps. Firstly, preservation involves identifying, documenting and seizure of mobile device. Data collection is the process of obtaining raw data from mobile device. Analysis phase is where meaningful digital evidence relevant to the case will be extracted from raw data using scientific methods. The reporting phase presents examined and analysed evidence conducted in the previous step in a meaningful way.

Conducting a mobile forensic investigation on smartphone is a difficult task without proper supportive tools. Forensic investigation processes and methods involved vary across mobile platforms, device model and manufacturers. There is a lack of knowledge and supportive forensic tools for Android based smartphones in the forensics field. Continuous rapid growth of Android smartphone market share necessitates the existence of an Android forensic framework that supports all phases of the forensic investigation process.

Extracting data from unallocated space from smartphones is challenging. Unlike personal computers that have limited number of major operating vendors, there are no countless manufacturers of smartphones and mobile devices with their own proprietary technology and formats. At the same time, there are mobile-device forensic tools available, such as Bulk Extractor, Yodot, Wondershare Dr.Fone. but these tools needs a rooted mobiles for extracting the data.

There are commercial mobile devices forensics tools (among them are highlighted above) that are highly capable but may be too expensive to some users. However, this paper is based on extracting the data from unallocated spac. In order to discover these methods of extracting data from unallocated space, the

architecture of the Android smartphones is studied as well to understand its structure, operating system and how it works. The complexity and the diversity of Android smartphones vary based on their architecture models and their manufacturer proprietary design.

II. BACKGROUND

1) Android System Architecture:

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.

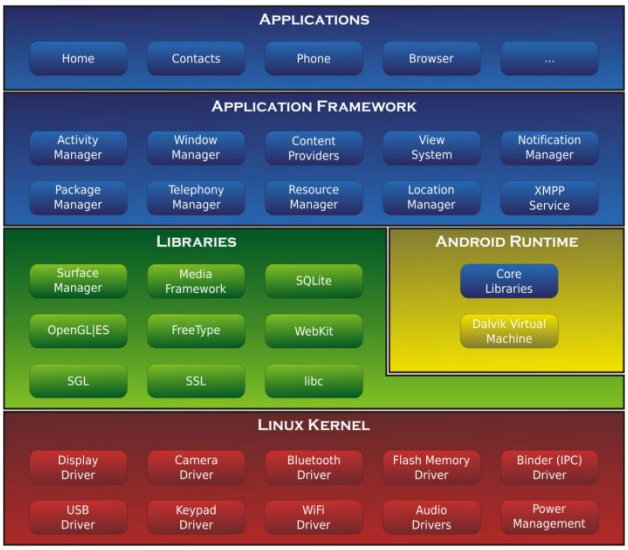
Android Architecture:

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.

2) Android Developer Bridge(ADB):

Android Debug Bridge (ADB) is a command line tool that allows your local computer to communicate with a connected Android-powered device or an emulator. It is a client-server program that includes a client, a daemon, and a server. ADB makes a connection between your telephone or other personal wireless devices and a local computer, creating the possibility to interact with your telephone or tablets on your desktop through the command line.

An attacker can obtain privileged access through physical access to a device that has ADB enabled. If the attacker can access the physical computer, he/her can easily determine whether ADB is enabled or not by executing adb get-serialno on the computer. The device's serial number would be returned if the ADB is enabled. Once the attacker knows that ADB is enabled on the device, he can use ADB's push command to implant an exploit on the device, and use ADB's shell command to launch the exploit and escalate his privilege.



An attack on an ADB enabled device does not require any action from the user and it is more cleanly compared with remote attacks. Privilege escalation using ADB has a drawback that depends on the availability of an enabled debug bridge. However, if the device is not password-protected, the attacker could simply connect with the common device Interface and enable ADB. For instance, Super One-Click desktop application in paper can gain privileged access from Android devices with enabled ADB and give the user privileged access. ADB-based attacks do not need install new application and reboot.

The lack of device modification in ADB-based attacks makes it much more difficult to trace than other attacks. It is unlikely to be detected by security applications on unrooted devices.

3) Autopsy:

Autopsy is a digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. You can even use it to recover photos from your camera's memory card.

Smart phones are basically small computers and Autopsy can parse and analyze the contents of Android and iOS devices. This includes both the official databases and third-party app database.

The ingest module has a basic flow of

- ✓ Query for files using the org.sleuthkit.autopsy.casemodule.services.FileManager service
- ✓ Parse them or open them with SQLite (you'll need to bring along a SQLite JAR file)
- ✓ Create Blackboard Artifacts (see The Blackboard)

The BlackBoard has standard artifacts for the standard cell phone forensics data types, such as BlackboardArtifact.TSK_CALLLOG.

Autopsy comes with an Android module, as defined in various classes in the org.sleuthkit.autopsy.modules.android package.

III. LITERATURE REVIEW

A. ANDROPHSY- Forensic Framework for Android:

Authors: Indeewari U. Akarawita, Amila B. Perera, Ajantha Atukorale
Published in: International Conference on Advances in ICT for Emerging Regions
Year: 2015

Forensic investigators who do not have access to expensive commercial Android forensic tools need lot of efforts to accomplish their job. Though there are impressive research findings, the Android forensic field lacks collaboration among findings, and has reduced their worth. In this study we implemented an open source forensic framework for Android smartphones - ANDROPHSY to serve the open source Android forensic community with the powerful features that are not available on any free solutions. ANDROPHSY supports forensic investigator in all four phases of a mobile forensic investigation.

B. Mobile Device Forensics: Extracting and Analysing Data from an Android-based Smartphone

Authors: Normaziah A. Aziz, Fakhrulrazi Mokti, Mohd Nadhar M. Nozri
Published in: 2015 Fourth International Conference on Cyber Security, Cyber Warfare and Digital Forensic
Year: 2015

Implementing digital forensics on mobile devices that are in various platform and proprietary is indeed a challenge for forensics analyst. Data residing on Android based smartphones can be extracted using the right tools and processes. It is important to understand the phone architecture, operating systems, computer forensic process and forensic tools prior to do the data extraction and recovery of files. Data from the Contact List, Call Logs, Calendar, Image, Emails, SMS and GPS TrackPoint are managed to be extracted. Related data can be singled out and analyzed for the law enforcement to relate these evidences to the case. Such digital evidences can then be brought to the court. The data extraction for different android smartphones varies based on their architecture models and their manufacturer proprietary design.

C. IE Internet Information Forensics Technology in Unallocated Disk Space

Authors: Chen Haiping, Luo Delin, Gao Qinquan, Qian Zhicong, Wu Shunxiang
Published in: IEEE conference
Year: 2010

In this paper, they did a detailed analysis and comparison on the data stream of IE Internet Cookie records, history records and cache records. And develop an analyzing system of the websites records information in unallocated space based on a string pattern matching algorithm. This system can be used as a part of computer forensics software.

IV. PROBLEM STATEMENT

In today's market Android play a vital role in business and more in entertainment but as demand is more for these devices market launches more product due to rise in business. If any one lost there data or forgot there password they can backup or extract the data from the mobile devices with the help of tools but they don't know that the data is also stored in unallocated space. The main problem is unable to find which data is stored in unallocated space and unable to extract the data from the unallocated space in android devices.

V. METHODOLOGY

If someone try to extract data from an Android device, the possible cases for succesful extraction are:

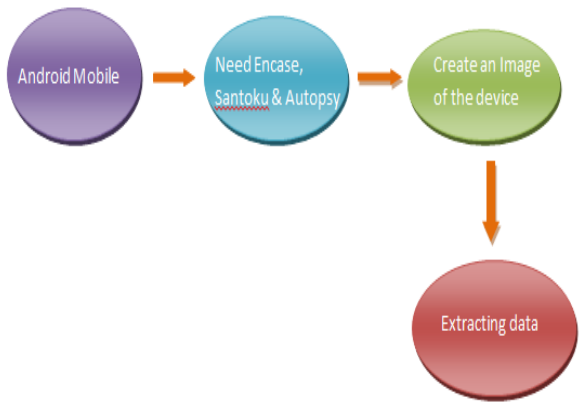
- ✓ The Android phone should be Rooted,
- ✓ USB- Debugging should be turned ON, or
- ✓ The data should be in extrenal SD card.

They extract the data from the devices but they cant extract the data from unallocated space.

In this research the main agenda is to extract the data from unallocated space in android devices.

i. Install Encase in your sysytem which is used for the forensic purpose. Encase is the best platform for mobile devices forensic for extracting data.
ii. Now connect the mobile device to the system and make an image of the mobile with the help of Encase.
iii. And now extract the data from it using autopsy.

FLOW CHART:



VI. CONCLUSION

Data situated in Android smartphones can be extracted by using the suitable tools and processes. It is important to understand the device anatomy, operating systems, computer forensic process and forensic tools prior to do the data extraction and recovery of files. Data from unallocated space are managed to be extracted. Related data can be singled out and analyzed for the law enforcement to relate these evidences to the case. Such digital evidences can then be brought to the court. The data extraction for different android smartphones varies based on their architecture models and their manufacturer proprietary design.

VII. REFERENCES

[1]. Normaziah A. Aziz, Fakhrulrazi Mokti, Mohd Nadhar M. Nozri Extracting and Analysing
[2]. Data from an Android-based Smartphone, 2015 Fourth International Conference on Cyber Security, Cyber Warfare and Digital Forensic.
[3]. Chen Haiping, Luo Delin, Gao Qinquan, IE Internet Information Forensics Technology in Unallocated Disk Space, in IEEE conference in 2010
[4]. Mubarak Al-Hadadi and Ali Al-Shidhani, Smartphone Forensics Analysis: A case study, International Journal of Computer and Electrical Engineering, Vol. 5, No. 6, December 2013.
[5]. Alexios Mylonas, Vasilis Meletiadis, Bill Tsoumas, Lilian Mitrou and Dimitris Gritzalis, "Smartphone Forensics: A Proactive Investigation Scheme for Evidence Acquisition.", a chapter in Information Security and Privacy Research, Vol 376, pp 249-260, Springer Berlin Heidelberg, 2012.
[6]. Jeff Lessard, Gary C. Kessler, "Android Forensics: Simplifying Cell Phone Examinations", Scale Digital Evidence Forensics Journal Vol.4, September 2010
[7]. Muhammad Faheem, N-A. Le-Khac, Tahar Kechadi, "Smartphone Forensic Analysis: A Case Study for Obtaining Root Access of an Android Samsung S3 Device and Analyse the Image without an Expensive Commercial Tool", Journal of Information Security, 2014.
[8]. The Sleuth Kit, Retrieved on 5 March 2015 from http://www.sleuthkit.org/sleuthkit/
[9]. The Statistics Portal Website, Retrieve on 4 May 2015 from http://www.statista.com
[10]. Jackson, W., Can digital forensics keep up with Smartphone Tech Retrieved on 2 April from http://gcn.com/Articles/2014/06/16/forensics-technologyrace.aspx?Page=2
[11]. Networkworld.com, 2015 "Getting Forensics data off Smartphones and Tablets can be Tough" http://www.networkworld.com/article/2160656/smartphones/gettingforensics-data-off-smartphones--tablets-can-be-tough--experts-say.html Retrieve 12 March 2015
[12]. https://www.sleuthkit.org/autopsy/v2/https://digital-forensics.sans.org/blog/2009/05/11/a-step-by-step-introduction-to-using-the-autopsy-forensic-browser