I J C T A, 9(15), 2016, pp. 7111-7117

Performing Digital Autopsy on an Android Device: An "Open Source" Approach

Rajan Fasra* and A.R. Nagoor Meeran**

ABSTRACT

In this evolving digital era, the use and misuse of data found on smart phones has grown significantly. In the event of a cyber-incident, when the major role is played by a smart phone, it is imperative to unearth evidence residing on the device, in a forensically sound manner. The recovery of evidence from electronic devices is now firmly a part of investigative activity in both public and private domains. According to the reports published by the International Data Corporation (IDC) in Q1 2015 [1], it has been found that Android smart phones monopolize the smart phone market by 78%. Due to the radical increase in the use of android smart phones in the course of time, exploitation of the same has increased exponentially. Currently, forensic experts are facing the challenge of forensically recovering all the required data/evidence like artifacts left by Wi-Fi, Bluetooth, Browsers, Sim-card, Device details and more from an android smart phone, efficiently at one go. I intend to develop an Open Source tool that would recover all crucial evidence residing on the android smart phone and also correlate the various events of forensic interest; in order to facilitate an investigation, reduce the cognitive load on the analyst side and display all the recovered results in a precise, coherent manner. We claim that this way of finding not only saves an investigator's time and effort, but can also reveal the interrelationship between the artifacts, providing a more robust and comprehensive approach. The plethora of information recovered from the smart phone, organized categorically, can be used to corroborate any finding in an investigation, by providing solid evidence in a court of law.

Keywords: Android, Open-Source, Forensics, Smart Phones, Autopsy.

1. INTRODUCTION

The smart phone market is growing exponentially [current statistics shows 167.9 million smart phones alone in India and India will Overtake US in 2016, says dazeinfo.com][2]. Along with the increased availability of these powerful devices, there is also a potential inflation in criminals to misuse this technology as well. Criminals misuse smart phones for activities like text message and email harassment, child pornography, illegal dealing of narcotics, etc [3]. The data nested on smart phones proved to be immensely useful to analysts through the furtherance of an investigation. Indeed, mobile devices have already proven that they contain a large volume of probative information, that aids an investigator to link an individual with basic text message data, call logs and contacts; but they also contain even more fruitful information such as chat logs, e-mail, browser history and lot more sensitive data which is of an investigator's interest. And as Android is one of the dominant players in the smart phone market, it is important for a forensics investigator to have knowledge of Android forensics.

2. RESEARCH OVERVIEW

2.1. Research Problem

The accelerated growth of a variety of smart phones in the market, demands exemplary skill from a digital forensics expert. The forensic investigator should be skilled enough to adopt different forensic

* SRM University, Kattankulathur, Chennai, India, *Email: rajfasra@gmail.com*

** SRM University, Kattankulathur, Chennai, India, *Email: nagooris@gmail.com*

procedures on a seized device, depending on its features. He should be able to extract all the data on the device, with minimal damage to it. Some challenges that a digital forensics expert is faced with are as follows:

1. Understanding the inner working of the operating system and file system for a smart phone.
2. Choosing what acquisition techniques can be applied for a device.
3. Choosing a tool from the plethora of utilities available.
4. Acquiring all possible data from the device.

Understanding these facts, if a digital forensic expert has one utility, that could be operated across a multitude of devices which would automate the acquisition of all data, then the utility provides access to a gold mine of information in the smart phone. In addition to this, if the tool is "open source" then forensic experts can tweak the tool to cater to their needs.

Currently there is "no open-source software tool" that can extract all data from an android device. This research aims to develop an "open-source" for the same [4].

2.2. PROPOSED SOLUTION

A forensic examiner handling mobile devices will have knowledge about where evidence resides on the device. But only an adept forensic examiner will have the capability to acquire the evidence in a forensically sound manner. He will be aware of the internal working and cabling of the device and would be able to choose which software or tools are needed to acquire data from the device, with minimal changes to it. While handling mobile devices, it is always advisable to allow only skilled forensic experts to handle valuable evidence. Once an expert is identified our objective is as explained further in the section. The mobile forensics process is broken into three main categories: seizure, acquisition, and examination/ analysis. Our objective here is to administer: "Acquisition" of the evidence which is populated on mobile device.

The tool I intend to develop, exemplifies this fact, demonstrating that open source tools which are capable of exfiltrating and revealing evidence buried deep down in mobile devices, are needed greatly in the current era to bridge the divergence between the growth of crime and the case being solved, within a specific time window as put forth by the law. As the tool which is proposed here flows with the impulse of open source, its sole purpose is to contribute to the open source forensic community. It will assist forensics analysts to delve better into the committed crime and yield most out of the device which is assumed to be involved in the criminal activity. The "Acquisition Tool" developed, would acquire data in a forensically sound manner, keeping in tune with conventional techniques like logical acquisition, file-system acquisition and physical acquisition [5].

3. IMPLEMENTATION

3.1. Developing Acquisition Tool

The project flow begins with developing an android application which behaves as an acquisition tool at the time of forensic investigation.

Table 1
Tools Required for Developing Acquisition Tool

Operating System	:	Ubuntu 15.10 (64-Bit Recommended)
IDE	:	Android Studio 1.5.1
Test Device	:	Samsung Galaxy Grand i9082 (Rooted)

The acquisition tool is called Android Digital Autopsy (ADA), it performs:

1. Logical Acquisition,
2. File System Acquisition,
3. Physical Acquisition.

3.1.1. Logical Acquisition

Logical Acquisition is the simplest among the three acquisition methods. It acquires data that is visible to the user who is operating the device. The Android Operating System makes use of Content Providers, which is an interface that allows applications to share data between them and provides access to data of other applications [6]. Logical Acquisition can be done by using Content Providers to acquire the data that belongs to an application, that is visible to the end user.

During logical acquisition, details like:

1. Contacts Or Phone-book
2. Call History
3. Messages : SMS and MMS

are recovered from the seized device, the details are displayed to the forensic examiner on the screen and are also saved to a specific location on the device which is mentioned below.

[default_location]: /<internal_storage>/ADA/ADA-Logical/

The forensic examiner is given the choice of acquiring any or all of the above mentioned data. The acquired files are stored with a predefined formatted name which is as below:

[default_filename]: adacontacts-<timestamp>.csv

3.1.2. File System Acquisition

In this acquisition technique, the Android device uses Application Program Interface (API) to interact with the file system and makes it possible to extract the data listed below. ADA performs File System acquisition by gaining ROOT access to the file system of the seized device.

During File System acquisition, details like:

Wi-Fi details.

BSSID or SSID

Password

Address of Wi-Fi

Security protocol

Bluetooth(BT) details.

Name of BT

Address of BT

Direction of transfer-sent/receive

Application details.

Apps using other apps.

Apps installed time.
Apps updated time.
Apps using Process
Apps using Services.

SIM details.
IMEI Number (Device ID)
IMSI Number (Subscriber ID)
SIM Serial Number
Network Connection like GSM, CDMA, iDEN and more.

Account details.
Account existing on the phones associated with Google, WhatsApp and Facebook.

Browser related details.
Browser Bookmarks
Browser history

Miscellaneous details.
Phone Uptime
Meta-Data about File-System (OS, ROM build,Model,Serial.)
Screen Display Resolution, Display Colours
Files related to account's on device (Gmail, Facebook, etc.)
User Dictionary entries
Calendar events

are recovered from the seized device, the details are displayed to the forensic examiner on the screen and are also saved to a specific location on the device which is mentioned below.

[default_location]: /<internal_storage>/ADA/ADA-FileSystem/

The forensic examiner is given the choice of acquiring any or all of the above mentioned data. The acquired files are stored with a predefined formatted name which is as below:

[default_filename]: bluetooth_details-<timestamp>.<db/txt>

3.1.3. Physical Acquisition

The technique of physical acquisition aids in extracting deleted files from the internal storage, by accessing the storage medium independent of the underlying file system [7]. For physical acquisition knowledge about the file system and its inner-working is recommended. The Android File System is divided into partitions to represent data like data, cache, boot, system, recovery, etc, which are mapped to block devices which might look like: /dev/block/mmcblkXpY [here X and Y range from 0 to number of partitions you have on your android device]. Example of block: "/dev/block/mmcblk0p17".This mapping will vary according to phone's make and model.

The partition layout can be any one of the following three types:

1. Memory Technology Device (MTD)

2. Multimedia Card (MMC)
3. Extended Multimedia Card (EMMC)

In this research, a device with MMC partition layout has been used. To understand the layout of partitions in a device, it is imperative to first find out the number of blocks in it. These details are stored in a file in the Android file system, the location of which depends on the type of partition layout.

For MMC devices, the number of block devices in the file system can be found by accessing the file in the location, "/proc/partitions".

This file only gives details about the number of block devices. We need to know what data is stored in each block in order to assist in data recovery from corresponding partitions. This information can be found in a file in the following location for an MMC device,"/dev/block/platform/sdhci.1/by-name/".

By acquiring the RAW images of the blocks using "dd" command, after knowing what data is stored in which block, it is possible to recover deleted evidence from the phone in a forensically sound manner.

A script file - "ada-cloner.sh", has been developed for a smart phone, to automate the process of physical acquisition. It performs the following steps:

1. Identify the blocks in a device
2. Map the data blocks to the partitions
3. Acquire RAW images of each block along with its MD5 hash value.
4. Store the RAW images in the ROOT directory of an External Storage Card formatted with NTFS File System. This storage card belongs to the Forensic Investigator and is to be inserted into the device for the purpose of Physical Acquisition.

This script file is effective across all MMC devices. The following steps are done to acquire RAW images of all the blocks in a seized device.

1. Connect the device via ADB.
2. Gain ROOT access to the device.
3. Execute the script file by typing the command on FWS terminal.

root@hostname#: sh /<root-directory-of-externalcard>/ada-cloner.sh

4. Wait until the process is completed (approx 2 hours for 8GB INTERNAL storage) to view the acquired raw images which are stored in the External Storage Card.

The "dd" image is saved to a specific location on the phone which is mentioned below.

[default_location]: /<external_storage>/ADA/ADA-Physical/

The acquired "dd" image file with MD5 hash file is stored with a predefined formatted name which is as below:

[default_image_filename]: mmcblkXpY.dd

[default_MD5hash_filename]: mmcblkXpY.md5

ADA also transfers the acquired files from device to FWS by instructing the forensic examiner to gain ROOT access and execute the following command in the command line terminal of the FWS.

After Logical and FileSystem acquisition, we can transfer the files stored in Internal storage by:

Command: adb pull /<internal_storage>/ADA/* /home/<username>/ADA/

After Physical acquisition, we can transfer the files stored in External storage by:

Command: adb pull /<external_storage>/ADA/* /home/<username>/ADA/

3.2. Deploying Acquisition Tool

All the tests are performed on a rooted android device by deploying the Android Application Package (APK) of the developed acquisition tool "Android Digital Autopsy", using the following procedure:

1. Connect the Test device to the FWS using a USB cable.
2. Now execute the following command in linux terminal to install APK.

   Command: "adb install ADA.apk".
3. Now you can further interact with the device to acquire the needed evidence.

In conventional digital forensics, a skilled examiner is supposed to make only minimal changes to the seized device. Any interaction with the device from the time of the crime, like unplugging the computer from power or accessing data when the computer is running modifies the state of the device, thereby altering volatile data. In mobile device forensics, it is impossible to analyze a device, without minimal change or impact to the device [8]. If a forensic examiner aims to have minimal interaction with the device, then a lot of probative information would go uncollected. Some analysts argue that exploiting the device, would provide more valuable information to the investigation. Andrew Hoog's "AFLogical OSE" is a perfect example of a tool following this approach. This tool when installed on a seized device, performs logical acquisition in an efficient manner [9].

In the next stage of deployment we can proceed with performing

1. Logical acquisition;
2. File System acquisition;
3. Physical acquisition

The acquired data is then stored on the device in the internal storage directory under the folder with name "ADA". Once acquisition is performed, the data collected can be sent to the forensic workstation (FWS) for further analysis.

3.3. Timeline Analysis

In digital forensics, the amount of acquired data is enormous. It is difficult to perform a brute force approach on all data collected to find data relevant to the scope of investigation. If a tool provides a forensic investigator the option to filter acquired data to relevant data, it would greatly help to accelerate the investigative process. Keeping in tune with this idea, an ADA Analysis Tool was developed, that operates on the data acquired via Logical Acquisition and performs "Timeline analysis". The tool takes as input the call logs and message inbox files generated by Logical Acquisition, two dates- one behaving as start date and another as end date. This helps to narrow down the entries from the files, that fall between the ranges of the dates provided, which can then be displayed to the investigator. This aids the investigator by eliminating the display of irrelevant entries.

4. OPEN SOURCE NATURE OF ADA

Open Source is fabricating its threads not only in the Commercial Market but also in areas like Government Agencies, Infrastructure software, Military, Education, Healthcare, that depend highly on technology. The purpose of open source is to provide software that is cheaper, reliable and is of good quality. According to a latest survey "81% of recruiters say getting 'LINUX' talent is priority".

The impact of open source in the field of digital forensic is very vast. Open source forensic tools are more advantageous than proprietary (closed source) forensic tools. Some facts to substantiate the same are given below: [10]

1. Reviewing source code is an added advantage to debug each step as the program gets executed.
2. Sharing the improvements and enhancements to the software is easy with open source community.
3. The overall quality of the product is maintained by the open source community.
4. Open source products are mostly available with no price tag attached to it.
5. Linux is the backbone of Android and can be used as a powerful forensic tool too.

5. FUTURE WORK

The extension to the project can be viewed as follows. In physical acquisition, once the location of deleted data is found, data recovery can be done to recover the deleted data. The analysis tool can be made to also chronologically relate the events of File System Acquisition [11], falling within a specific timeline.

REFERENCES

[1] http://www.idc.com/prodserv/smartphone-os-market-share.jsp (As on March 23, 2016).

[2] http://www. dazeinfo.com/2015/07/04/global-smartphone-sales-2015-2017-india-will-surpass-us-report/ (As on March 23, 2016).

[3] Yoon. S., Jeon. Y., (2014) "Security threats analysis for Android based Mobile Device" in International Conference on Information and Communication Technology Convergence. 775-776.

[4] Manson.D., Carlin.A., Ramos. S., Gyger. A., Kaufman. M., Treichelt. T., (2007)." Is the Open Way a Better Way? Digital Forensics Using Open Source Tools" in Annual Hawaii International Conference, 266b.

[5] https://en.wikipedia.org/wiki/Mobile_device_forensics#Acquisition (As on March 23, 2016).

[6] Jackson.W. (2014). Android Content Providers: Providing Data to Applications. In Android Apps for Absolute Beginners. Apress. 505-550.

[7] Tsai. Y., Yang. C., (2013). Physical Forensic Acquisition and Pattern Unlock on Android Smart Phones. In Future Information Communication Technology and Applications. Lecture Notes in Electrical Engineering, Volume 235. Springer. 871-881.

[8] Hoog. A., (2011). Android forensic techniques. In McCash. J., (Ed) Android Forensics. 197-198. Syngress Publications.

[9] Hoog. A., (2011). Android forensic techniques. In McCash. J., (Ed) Android Forensics. 220-228. Syngress Publications.

[10] Hoog. A., (2011). Android device, data and app security. In McCash. J., (Ed) Android Forensics. 174-175. Syngress Publications.

[11] Kasiaras D.; Zafeiropoulos T.; Clarke N.; Kambourakis G.,(2014). "Android Forensics: Correlation Analysis" in Internet Technology and Secured Transactions (ICITST). 157-162.