Collection of Evidence Data with Physical Acquisition of Root Access of an Android Samsung J7 Prime and Analysing on Open Source Tool Autopsy 4.15.0

Aye Thida Tun
University of Computer Studies, Yangon, Myanmar
ayethidatun@ucsy.edu.mm

Ciin Zam Man
University of Computer Studies, Yangon, Myanmar
ciinzamman@ucsy.edu.mm

Ei Cho Zin
University of Computer Studies, Yangon, Myanmar
eichozin@ucsy.edu.mm

Ei Ei Kay Khaing
University of Computer Studies, Pyay, Myanmar
eieikaykhaing@ucsy.edu.mm

Zun Myat Myat Soe
University of Computer Studies, Yangon, Myanmar
zunmyatmyatsoe@ucsy.edu.mm

Mie Mie Su Thwin
Cyber Security Research Lab
University of Computer Studies, Yangon, Myanmar
drmiemiesuthwin@ucsy.edu.mm

Abstract – Today, the smartphone market is growing rapidly and then it is essential in daily life. The smartphone is the most useful device in the world. Most of the people use it instead of a laptop for their daily work and to store personal data and information. This paper is intended to know how to get root access in non-rooting device. The interesting point in this paper is how to acquire data using dd command. In this paper, evidence data from external sdcard are analysed using autopsy tools. This tools extract contacts, image, and song and so on. This paper is presented in three main sections. These sections are (1) background theory, (2) data acquisition from device (3) analysing data using autopsy. The second section is subdivided into two parts such as rooting and physical acquisition.

Keywords – android forensics, physical acquisition, Android Debug Bridge (ADB)

I.INTRODUCTION

In this era, the word forensics is a well-known word in many fields. A lot of criminal cases are being caused by using digital devices. Digital forensics is used to prevent crime by collecting and analysing digital data. Digital forensics can be divided into many groups such as computer forensics, mobile forensics, database forensics, network forensics.

In the market, mobile devices are developed as many kinds of technology by the various factories. As smart devices, it can be used as a tool in many criminal cases. Android forensics is becoming a crucial section for reducing criminal cases.

In mobile devices, the mobile operating system is differed by Manufacturers. For example, Nokia introduces Maemo OS, Apple introduces iOS and Google introduces android OS, and so on. Table I shows the versions of the Android mobile operation system [1].

TABLE I. ANDROID MOBILE OPERATNG SYSTEM

Name	Version	Supported (security fixes)
Cupcake	1.5	No
Donut	1.6	No
Éclair	2.0 – 2.1	No
Froyo	2.2 – 2.2.3	No
Gingerbread	2.3 – 2.3.7	No
Honeycomb	3.0 – 3.2.6	No
Ice Cream Sandwich	4.0 – 4.0.4	No
Jelly Bean	4.1 – 4.3.1	No
KitKat	4.4 – 4.4.4	No
Lollipop	5.0 – 5.1.1	No
Marshmallow	6.0 – 6.0.1	No
Nougat	7.0 -7.1.2	No
Oreo	8.0 -8.1	Yes
Pie	9	Yes
Android 10	10	Yes
Android 11	11	Yes

Android is developed on Linux kernel which supports many file systems. The Android File Systems can be classified into two groups such as flash memory file systems and media-based file systems. Flash memory android file systems can be sub-classified as YAFFS2, JFFS2, F2FS and exFAT. And media-based android file

systems consist of EXT2, EXT3, EXT4, and MSDOS, and VFAT.

II. RELATED WORK

In [2], the android device partitions can be divided into five partitions. These are /boot, /system, /recovery, /userdata, /cache. This paper involves two forensics investigations that are proactive forensics investigations and reactive forensics investigations. Proactive Forensics is to collect evidence and monitor suspects in real-time. Reactive Forensics is an investigation process by law-enforcement authorities. Android forensics can face many challenges, which are application-based, permission-based, and extraction based challenges.

In [3], the researcher review forensics on android device. The acquisition is one of the forensics steps and involves file system acquisition, memory acquisition, and environmental acquisition. And the author discusses the main characteristics of mobile devices. This paper review many acquisition techniques; for example, AccessData FTK and dd Image and so on.

In [4], the researcher presented four acquisition tools that are used to acquire data. These tools are ADB Backup, DD tool, Magnet Acquire, and Belkasoft. The author surveyed two forensics analysing tools on Samsung and Oppo phones. One of the forensics analysis tools is Autopsy, free and open-source tools. And another tool is Belkasoft which is the flagship digital forensic suite. This tool is a commercial tool but the author used a trial version. Both of these tools are GUI tools as well as user friendly.

In [5], the author discussed the growth of android smartphones and the architecture of the android operating system. And then discuss with a case study using UFED Physical Analyzer. For analysing, the researcher used the Samsung S3 phone, Android OS version 4.1.2. The author presented rooting access on android phone using Android Development Tool.

III. BACKGROUND THEORY

Android operating system was developed by Google based on Linux kernel in 2005. Android device consists of six partitions and are boot, system, recovery, data, cache, and mics. Each partition performs its function.

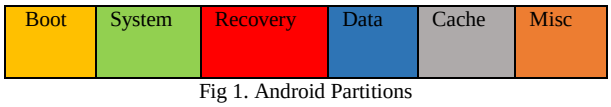

Fig 1. Android Partitions

Boot partition consists of an Android kernel and ramdisk. This is important for booting the phone. System partition involves operating system including GUI and default system applications. Recover partition is designed for backup. Data partition is an interesting partition for the investigator. It can be stored user data like sms, contacts, and so on. Cache partition can be stored repeated access application and data. Misc partition contains miscellaneous system settings for hardware setting, USB configuration, etc. And another partition is sdcard, which is used to store data [6].

The android operating system architecture is developed by four main parts that are application, application framework, libraries, and Linux kernel. All low-level device drivers consist of a Linux kernel. Android Libraries provide the main features of the Android operating system.

Two steps of android forensics are data acquisition and analysing. In data acquisition, three acquisition methods are Physical, Logical, and Manual Acquisition. Manual Acquisition can be performed either not locked phone or the PIN/Password/Pattern lock is known by the investigator. In this way, every data available to the user is available to the examiner via the usual user interface (UI). It is neither access system files nor system logs. This method reduces access time.

Logical acquisition is a bit-by-bit copy of given logical storage. This acquisition method produces, in general, a relatively manageable file which can be analysed and parsed by forensic tools. It back-up the whole device, for instance, logically acquired image. Santoku Linux is a logical acquisition of an android emulator.

Physical acquisition acquires data directly from hardware by direct access to a given disk or flash memory. Physically acquiring can get a headache but if successfully done, the produced copy can be used to recover deleted fragments and allows the examiner to put his hands on data remnants. Physical acquisition creates a copy file that includes not only the deleted data but also unallocated space. The well-known data acquisition tools are FTK Imager, SANS SIFT, Magnet RAM capture, and so on. FTK Imager collects data for any change of the original evidence and Magnet RAM capture records data from the memory of a suspected device.

In analysing step, the investigator needs to know which tools analyse what kinds of data. Many open-source tools and commercial tools are developed in the forensics world. The popular tools are ProDiscover, Sleuth Kit (+Autopsy), EnCase, ProDiscover provide to see the history of the internet. These tools accept to import or export .dd images file. Autopsy is open-source and user-friendly forensics tool. The investigator is allowed to investigate hard drive and smartphone. EnCase can perform deep and triage analysis. This tool also acquires data from the smartphone.

IV. DATA ACQUISITION FROM DEVICE

In physical acquisition step, evidence data are collected from the mobile device which has root access. The specification of the device is shown in table II.

TABLE II. SPECIFICATION OF TESTING DEVICE

Brand	Samsung
Device Name	Galaxy j7 prime
Model Number	SM-G610F/DS
Android Version	8.1.0
Kernel Version	3.18.14-14381225
Build Number	M1AJQ.610FDXS1CTE1
Micro SD Card	16 GB

A. Rooting

Firstly, the investigator must check the tested device which has root access or not. The investigator can use the root checker application. Another checking method is accessing data partition. If the device does not have root access, the result will show permission denied.

Shell access to the tested device: adb –d shell

Fig 2. Device without root access

In the rooting process, Odin, TWRP is downloaded on the computer. SuperSu file is download and copied in tested device internal memory. Firstly the investigator enables USB debugging and OEM mode. TWRP Manager, a root application, provide for backup and restore. Secondly, the tested device's volume down, power and home button are pressed to reach the download mode. Thirdly, open Odin flashing tool and connect the mobile device using a USB cable. When Odin and device are successfully connected, the investigator clicks the AP or PDA button for choosing the TWRP recovery file. And then that file is installed into the tested device. Finally, SuperSu file, which manages root permission, is installed to the phone. After that, the examiner needs to reboot the tested phone. If the device has root access, the investigator can access /data/data partition.

Enable root permission (switch user): su

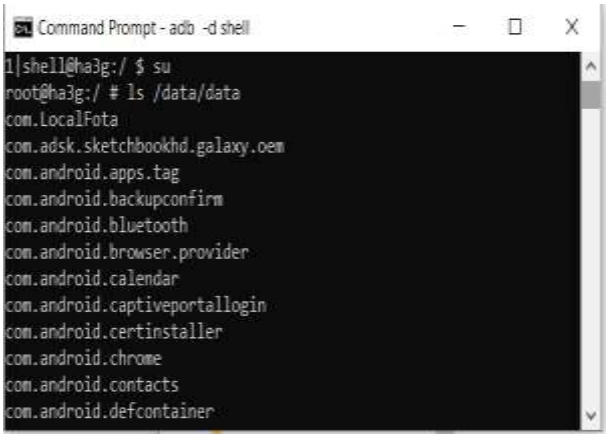

Fig 3. Device with root access

B. Physical Acquisition

In forensics workstation, Android SDK, the Android Debugging Bridge (ADB), and platform-tools are required for physical acquisition. Platform tools consist of net cat and adb.exe file. If Window does not have net cat, the examiner will need to download net cat application. And then it is copied into the platform-tools folder. Firstly, the examiner opens a command window and checks that the tested device is already connected to the forensics workstation or not.

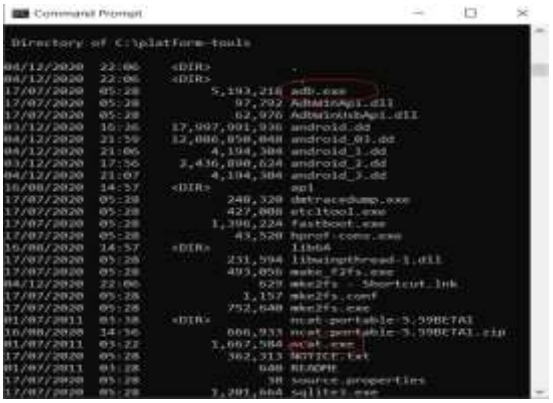

Fig 4. Adb.exe and ncat.exe in platform-tools folder

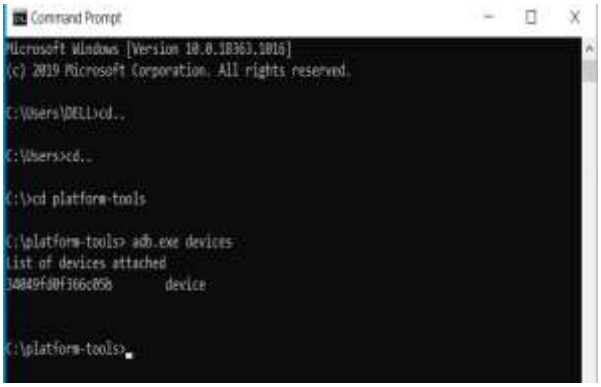

Fig 5. Running adb daemon and connected tested device

In figure5, the tested device is connected to the localhost forensics workstation. The investigator can see the partition of the device using the command below.

Show partition in file system: df

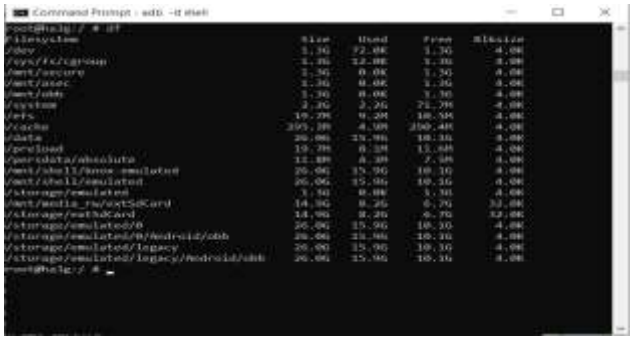

Fig 6. Output of df command

Busybox utility application is needed to run on the tested phone. One of the partitions is mmcblk0, the physical disk of the tested device. And the investigator can analyse the interesting partition from the phone. The interesting partition means the information that is essential data for forensics. In tested phone, mmcblk1p1 is an external sdcard that consists of the song files, contact files, images and so on.

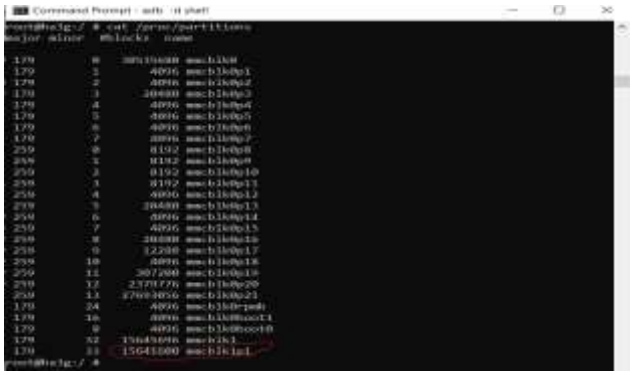

Fig 7. Show partition of tested device

In the tested device, the investigator chooses the external sdcard as an interesting partition. For analysing evidence, this partition is created as image/ dd files. The investigator opens another command line and then go to platform-tools partition in local forensic (window) workstation. In this workstation, tcp port 8888 is opened for accepting any forward traffic that port to and from the phone using ADB. Ncat makes a connection between the localhost and phone. All the data from sdcard are sent to android_02.dd file. DD is an extension for a raw disk.

Command: adb forward tcp:8888 tcp:8888

ncat.exe 127.0.0.1 8888 > android_02.dd

Fig 8. Local Forensics Workstation

Port 8888 is set up on the phone for listening connection. Netcat listens on port 8888 any connection which comes all the data from mmcblk0p1 on the port.5dd if=/dev/block/mmcblk1p1 | busybox nc –l –p 8888

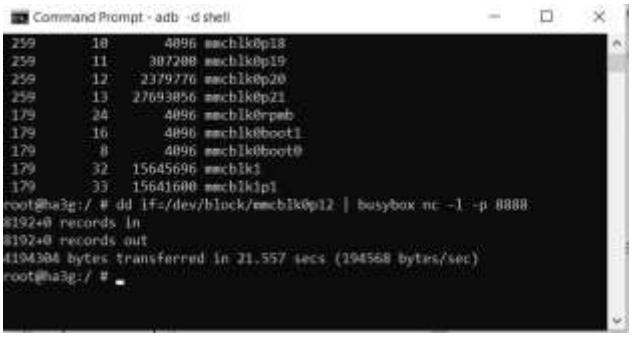

Fig 9. Acquiring Evidence Data

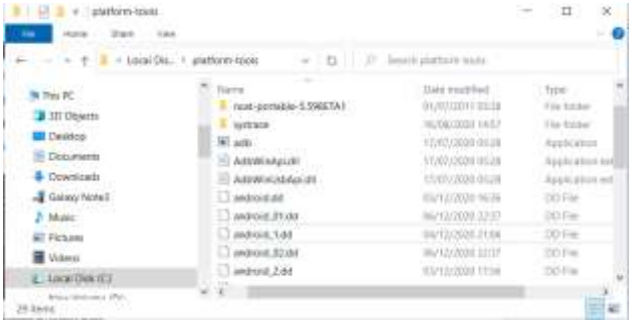

Fig 10. Creating DD Files

V. ANALYSIING DATA USING AUTOPSY

Autopsy is one of the well-known user-friendly forensics tools. It can clarify using the graphical user interface (GUI). And then it can provide email analysis and display thumbnail of images and extract information from call logs, SMS, contact, etc.

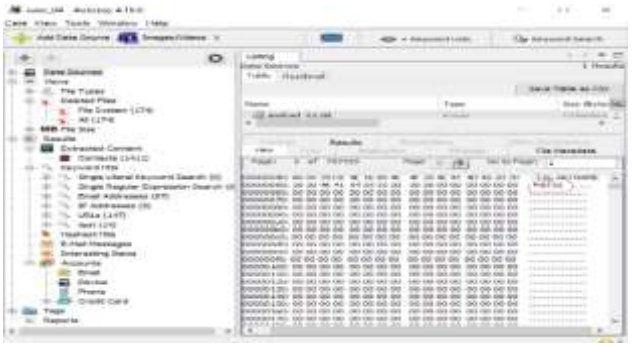

Fig 11. File System of External sdCard

Firstly, the forensics examiner creates a new case using Autopsy 4.15.0. In previous data acquisition step, raw data file (android_03.dd) was created by using dd command. The data source or tested file is collected from external sdCard. In figure11, FAT32 is the file system of android_03.dd.

Figure12 presented the result of analysing data on evidence and show artifact of the android media card.

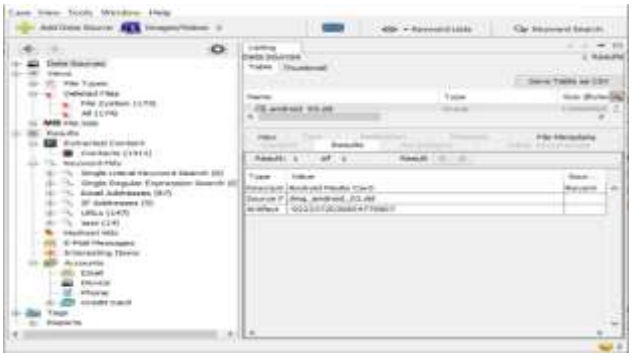

Fig 12. Results of Data Source

This data source has one thousand four hundred and eleven contacts lists, one hundred and seventy-four deleted file systems.

Figure13 shows the timestamp of analysis. This analysis took nearly ten minutes.

Fig 13. Timestamp of Analysis

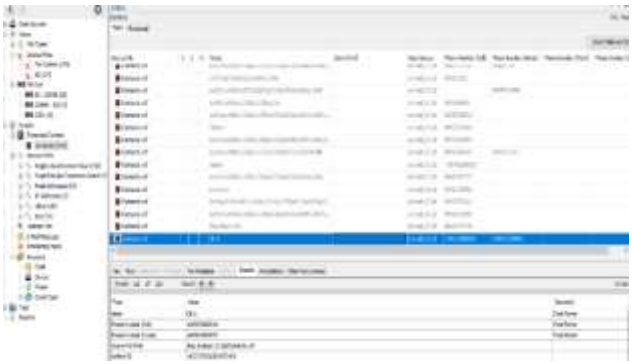

Fig 14. Contacts List

Figure14 shows the result of contact list file from analysing data source. The investigator can see detail information of contacts book.

Fig 15. Phone Number form Deleted File

In figure15 gave a collection of deleted information that is deleted by someone. It concludes song file, phone number, and movie file and so on.

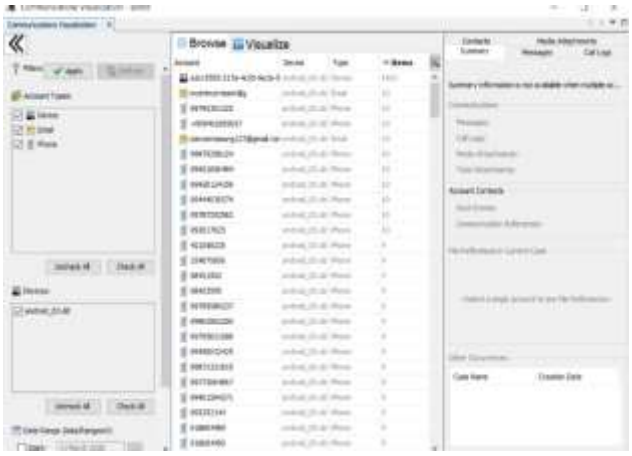

Fig 16. Evidence Data from External sdCard

Detail information of android_03.dd can be seen by using autopsy. Figure16 represent summary data of email, phone from device. In autopsy, the investigator can acquire related information using a keyword. In figure17, the forensics examiner investigates information using create keyword.

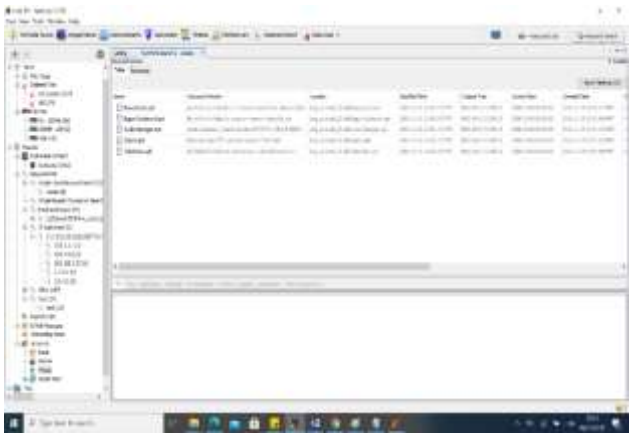

Fig 17. Keyword Search with test

(a)

(b)

(c)

Fig 18. Timeline (a) Count (b) Detail (c) List

Figure18 (a), (b) and (c) present the timeline of data from the data source. In this paper, the external sdCard of the tested device is used from 2016 to 2020. Figure18 (a) shows yearly data usage and (b) illustrates the detail events from the data source and (c) shows detail lists with event type and description In the analysing step, the investigator can see essential evidence data from the data source.

VI. CONCLUSION

In this paper, the author select external sdCard, one of the interesting partition from tested device. In acquisition process, physical acquisition method is used to collect all evidence data. The author presented how to acquire data using adb, ncat and dd. Some require application are discussed when android phone rooting. Some data acquisition tools and analysing tool are generally discussed in this area. Moreover, the paper presents detail analysis information using autopsy.

VII. REFERENCES

[1] https://en.wikipedia.org/wiki/Android_version_history

[2] Sudip Hazra and Prabhaker Mateti, "Challenges in Android Forensics", Communications in Computer and Information Science, November 2017.

[3] Hussein Farooq Tayeb and Cihan Varol, "Android Mobile Device Forensics: A Review"

[4] Htar Htar Lwin, Wai Phyo Aung and Kyaw Kyaw Lin, "Comparative Analysis of Android Mobile Forensics Tools"

[5] Muhammad Faheem, N.-A.Le-Khac and Tahar Kechadi, "Smartphone Forensics Analysis: A Case Study for Obtaining Root Access of an Android Samsung S3 Device and Analyse the Image without an Expensive Commercial Tool

[6] https://www.dataforensics.org

[7] https://medium.com/@tusharcool118/autopsy-tutorial-for-digital-forensics-707ea5d5994d