A Comparison Study of Android Mobile Forensics for Retrieving Files System

Aiman Al-Sabaawi *a.alsabaawi@student.qut.edu.au*
[a] *School of Electrical Engineering and Computer Science*
Queensland University of Technology
Brisbane, Australia
[b] *Department of Computer Science*
Al-Nahrain University
Baghdad, Iraq

Ernest Foo *e.foo@griffith.edu.au*
School of Information and Communication Technology
Griffith University
Brisbane, Australia

Abstract

A comparison study of the Android forensic field in terms of Android forensic process for acquiring and analysing an Android disk image is presented. The challenges of Android forensics, including the complexity of the Android application, different procedures and tools for obtaining data, difficulties with hardware set up, using expensive commercial tools for acquiring logical data that fail to retrieve physical data acquisition are described in this paper. To solve these challenges and achieve high accuracy and integrity in Android forensic processes, a new open source technique is investigated. Manual, Logical and physical acquisition techniques are used to acquire data from an Android mobile device (Samsung Android 4.2.2). The mobile phone is identified by taking photos of the device and its individual components, including the memory expansion card, and labelling them with identifying information. Following the manual acquisition, logical acquisition is conducted using the AFLogical application in the ViaExtract tool (by Now secure) installed on a Santoku Linux Virtual Machine. The image file is then created using the AccessData FTK imager tool for physical acquisition. Four tools are utilized to analyse recovered data: one using ViaExtract on a Santoku Linux Virtual Machine, two using the AccessData FTK Imager, and one using file carving in Autopsy on a Kali Linux Virtual Machine. The results of the analysis demonstrate that the technique can retrieve Contacts, photos, Videos, Call Logs, and SMSs. Also, the EaseUS Data Recovery Wizard Free tool is used for the recovery of files from the LOST.DIRon external memory.

Keywords: Mobile Forensics, Android Forensics, Digital Forensics, Mobile Security.

1. INTRODUCTION

Androids OS was developed by Google for mobile devices, including smart phones and tablets. Since 2008, the Android mobile platform has been increasingly used and it became the most common mobile operating system in the world in early 2011. The increasing availability of Android devices with greater flexibility and the rapid development and huge growth of the Android platform have resulted in them becoming important devices for users, particularly regarding their range of features and applications. The Android architecture consists of four levels: Applications level; Application framework level; Libraries and Android Runtime level; and the Linux Kernel Level, as shown in figure 1 [1,2]. Therefore, lack of knowledge and supported techniques to investigate and retrieve data from these devices are key issues for forensics investigators. Crimes, including harassment using text messages, communications related to narcotics and threats using email could occur using Android devices. Recovering the data stored on these

Android devices could be quite useful for analysts and researchers in tracking these activities in the course of an investigation [3].

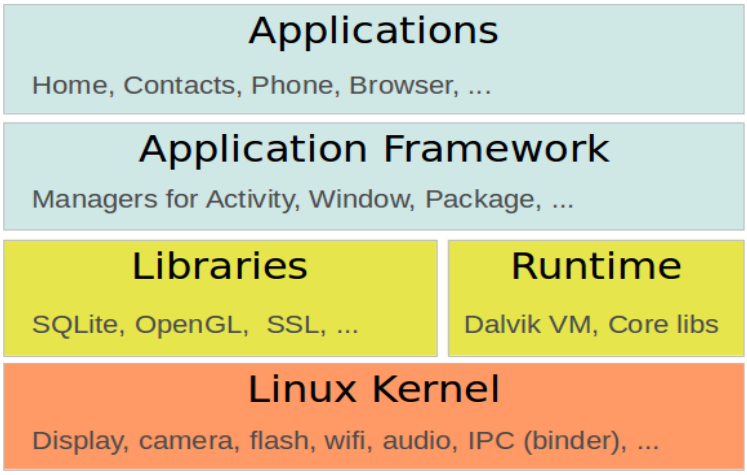

FIGURE 1: The Android Platform Architecture includes Applications, Application Framework, Libraries, Runtime, and Linux Kernel [4].

In recent years, many researchers have worked in the area of Android forensic investigation based on open source, commercial techniques and android applications. The steps in the forensic analysis of an Android device were explained in [5,6]. They used "Sprint HTC Hero running Android v1.5, v2.2 (Froyo) and v3.0 (Gingerbread) and the AccessData ForensicTool Kit (FTK) v1.81" to gain root access through the USB debugging option and Cellbrite UFED to create a logical DD image to conduct logical examination and analysis. In another study [7], the authors aimed to investigate the tools and techniques used for Android device forensics and they compared the tools according to their function in the investigation process. These tools included Open Source Android Forensics (OSAF), Android DebugBridge, Andriller, AFLogical, SKYPE extractor and WHATSAPP extract. In another study [8], existing android forensic methods were presented and the methods that have been utilized for obtaining root user on the Android mobile were explained [2]. Open source software was used to obtain a logical image of the required partitions of the device [1]. However, there are many tools and techniques developed in this field which can extract and analyze data using Open Source Android Forensics (OSAF), commercial and manual techniques. These techniques have drawbacks and there are many challenges, identified in the following sub-section.

1.1 Challenges of Acquisition and Analysis of Data on Android Devices

- The complexity and the diversity of Android applications and devices are based on their architecture models and their factory proprietary technology and formats; for example, Android version 6.0 has a new application permission that can give the users more control over data sharing.
- The commercial tools that are used to acquire a logical image are highly capable, but they are too expensive.
- There are different procedures and techniques used to obtain and verify data. The Android platform has developed rapidly. Therefore, it is difficult for examiners to adapt to the new devices and to choose a technique that will be suitable for their investigations and produce the most data from the simplest technique.
- It is difficult to disconnect Android devices from surrounding networks.
- The hardware of the Android interface is difficult to set up and work upon.
- It is difficult to acquire the data from the Android devices which are running custom ROMs.

Furthermore, data which can be obtained from Android devices using logical analysis differs from data that forensic investigators can obtain in the lab using physical analysis (manually). Forensic examiners need to obtain more detailed analysis of the data from a cell phone. In physical analysis, all data in the storage of a mobile phone can be obtained, including deleted contacts, deleted messages and more. This type of software is difficult to use and interpreting the data requires time, effort and special training. Data can include not only numbers called and received but, as mobile phones and their memory become more complex, they can also include internet web pages and video images. Retrieving data from the storage of mobile phones may include: Accessing data which are stored on SIM cards; Retrieving SMS/MMS outbox, inbox, and sent items; Reading the contents of mobile phones; Internet history, etc. [9].

1.2 Motivation and Contribution

The Android forensic challenges are related to the storage and files system of the phone and the data that can be synchronized, stored, and accessed across multiple devices. Examiners require more effort to preserve data because these data are volatile and can be deleted remotely or quickly transformed. There are a number of reasons that law execution and forensic investigators often face difficulties in obtaining, extracting and documenting digital data and evidence from an Android device [10].

The main contribution of this paper is to investigate Android mobile file system forensics. We investigate how Android mobile file system forensics will help investigators and examiners to provide them with advanced skills to decode, detect, decrypt, correctly interpreted data recovered data from the file system of an Android mobile device. This paper will identify Android mobile applications and tools to enable organizations to develop suitable procedures and policies for dealing with the acquisition and analysis of data. This is one branch of digital forensics and becomes important when identifying a suspect and the most damning evidence based on scientifically derived procedures and techniques, for preserving, validating, identifying, analyzing, interpreting, documenting and presenting the data, images and videos obtained from the Android mobile devices to help or further the reconstruction of events. It will help investigators save information on these devices, preventing changes to dates and time, location data and other associated data even if these devices are damaged and to improve an application with searching and indexing capability for locating private content on the Android mobile devices, including credit card numbers,postal and email addresses, etc. We will also focus on logical and physical data acquisition tools and their features, analytic techniques of the Android phone files system and recovery files from “LOST.DIR directory”.

2. PROPOSED METHOD FOR ANDROID MOBILE FORENSIC

Further investigation is necessary to determine what data will be used in the future and the new techniques that will be required and to examine the difference between the proposed technique and existing forensic tools. The advantages and disadvantages of physical and logical [11] extraction require the examiner to select the type of data to be extracted based on each forensic scenario. In some cases, investigators use only certain and important data while in other cases full extraction of the physical memory and/or the embedded file system of the mobile is desirable for the potential recovery of deleted data and a full forensic examination [12]. Therefore, the development of guidelines and processes for the extraction and collecting of data from Android mobiles is especially important, and researchers must periodically review and improve those processes according to Android technology development. In this paper, we will present an overview of processes for the recovery and documentation of data from Android mobiles, as shown in figure 2.

2.1 Evidence Intake Phase

The process of file and data extraction from Android devices requires the evidence intake phase to involve: request form and intake paperwork to document the chain of custody; ownership of the Android device; the circumstances in which the Android device was found; and requesting general information related to the type of data. The critical step in this process is the development

of specific objectives for extracting data. This will serve to explain and document the target of an examiner and help in the documentation of the testing procedure for each Android device examined [13].

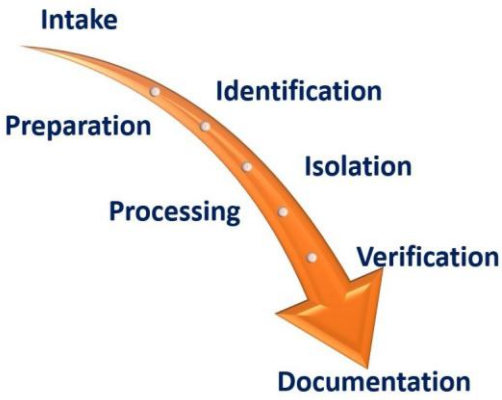

FIGURE 2: A Diagram of Digital Forensics Process Phases, including Intake, Preparation, Identification, Isolation, Processing, Verification and Documentation.

2.2 Identification Phase

To examine an Android mobile, the examiner has to identify the following steps:

- Proper Legal authority for conducting a forensic testing for Android devices;
- The purpose of the forensic examination;
- The information regarding manufacture, model and type of the Android devices should be identified;
- Removing stored data to external storage;
- Checking other sources that may be considered as potential evidence [13].

2.3 Preparation Phase

Based on the identification phase, the preparation phase requires a particular search related to the specific Android devices that require testing, the proper tools to be used in the examination and a preparation process to check that all of the necessary tools, cables, drivers and software are at the site for the test. When the information regarding the manufacture, model and type of the Android devices are identified, the examiners can then obtain the specific devices with the capability of retrieving the desired data from the Android device. These resources include “mobileforensicscentral.com" and “phonescoop.com". The SEARCH toolbar, “available as a free download from www.search.org", includes updated sources for mobile phone examinations. The tools should be suitable for the analysis of a mobile device and be capable of determining factors such as the target of the testing, the model of Android devices to be examined and the presence of any external storage capabilities. The tools available for an examination should be compatible with the phone technology and include iDEN, SIM Card, GSM and CDMA [13].

2.4 Isolation Phase

Before the examination, Android devices should be isolated from networks that can be connected with Android devices via wireless (Wi-Fi), infrared and Bluetooth network capabilities. Isolation of the mobile from these communication sources is a significant phase before examination because it prevents the adding of new data to the phone during new calls and texting. Remote wiping or remote access via a \kill signal can result in the potential destruction of data being high, and can also result in a high possibility of accidental overwriting of current data such as text messages and new calls. If the examiner isolates the Android devices from the network, the email, Internet browsing history, voice-mail or other data that may be stored on the service providers network instead of the device itself cannot be accessed accidently [13].

2.5 Processing Phase

After examiners have identified the proper tools to achieve the goal of the examination in the phases previously described, and Android devices have been isolated from the network and other communication devices, the desired data can be extracted. Removable data storage cards should be processed separately from the Android devices when that is possible, as accessing data stored on these cards may change the data on the data storage card during the device examination step. Any installed data storage/memory cards should be removed from the devices before the examination process, and they should be processed separately using traditional computer forensics techniques. This ensures that the date, time information and files stored on the memory card/data storage are not changed during the examination. In some cases, it may not be possible to process a removable data storage card separately from the devices, for example, when the examiners lack the tools for this process, or if the user locks or encrypts the data card to the Android device, examiners cannot access the data card except through the device. In this situation, the documentation and data card processing are especially important [13,14].

2.6 Verification Phase

After the previous phases, the examiner should verify the accuracy of the data extracted from the devices. There are several ways that can assist in verification of extracted data. Matching the data extracted from the Android device with the data displayed by the device itself is the only legal way to ensure that the data are the same [13].

2.7 Documentation and Reporting Phase

The examiner should document the process of the examination in the form of contemporaneous notes related to each step and what was done during the examination. The benefit of these notes is to ensure that the examiner records the basic information in the examination process. These notes and documentation may address the following:

1. When was the examination begun (date and time)?
2. What was the physical condition of the device?
3. Taking photos of the device and individual components, including SIM card and memory expansion card and labeling them with identifying information.
4. What was the status of the device when they received it (on or off)?
5. Determining the model, manufacturer, and identifying information tools used during the examination.
6. What data were documented through the examination? [13].

3. EXPERIMENTS AND RESULTS

3.1 Evidence Intake Phase

The proposed technique was implemented using an Android mobile device which was found at a crime scene.

3.2 Identification Phase

It was necessary to check whether or not the Android mobile device was associated with the crime. In this experiment, the specifications of all data that required extraction from this mobile are shown in Table 1.

Brand	Samsung
Device Name/ Model number	Galaxy Grand/ GT-I9082
Android Version	4.2.2
Baseband version	I9082XXUBNA3
Kernel Version	3.0.31-1257343
Build Number	JDQ39.I9082XXUBNC1
Serial Number	41002716872f6000
MicroSD Card	16 GB, Toshiba brand

Table 1: Data specification of Android mobile device.

3.3. Preparation Phase

Hardware and software preparation. The hardware requirements were the host machine (computer), Samsung USB Cable, USB Memory Storage, and SD Adapter. The software required to include Santoka Linux VM, Kali Linux VM, AccessData FTK imager, Android Studio, and EaseUS Data Recovery Wizard Free tool.

3.4. Isolation Phase

The Bluetooth and wireless network (Wi-Fi) were switched off in the mobile device. As there was no SIM card used, we did not need to perform extra steps.

.

3.5. Processing Phase

The practical steps and tools which were used in the processing and verification phases are summarized in figure 3.

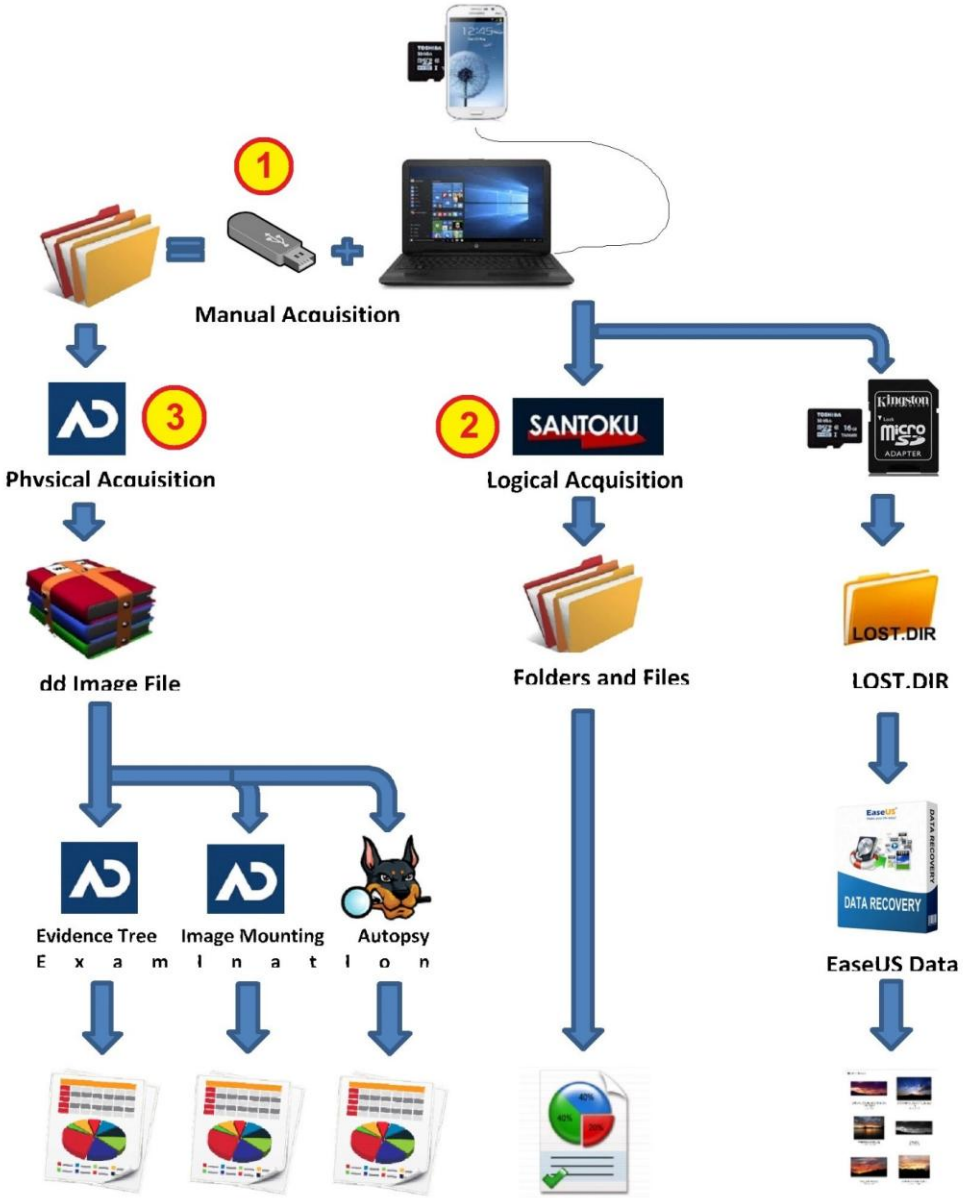

FIGURE 3: A Diagram for Processing Phases, including Manual, Logical and Physical Acquisition; and Verification Phase.

There were two extra steps used in this phase:

Step 1: Connection and Backup (Manual Acquisition) The USB driver (Google USB driver) of mobile phone applications was installed after installing Android Studio (SDK manager) to connect the mobile device with the computer [15]. Then, the mobile device files were moved to the USB Memory Drive in the computer using manual full backup, which is called “Manual Direct Acquisition”

Step 2: Unlock the mobile device using the Santoku Linux Alpha tool, which is sponsored by ViaForensics (NowSecure Company), the mobile device can be unlocked to access the root of the devices file system.

1. The mobile device should be enabled for USB debugging by Settings => Developer Options, then checking (Allow mock locations), (Stay awake) and (USB debugging), as shown in figure 4. If the Developer Options setting is not visible, go to Settings => About devices => Tap on (Build Number) seven times, then Developer Options will appear.
2. The mobile device was then connected to the computer using Santoku Linux in VirtualBox, by going to Devices => USB Devices => Click on the mobile device name, making a check mark next to the mobile device, as shown in figure 6. Then, we should agree in the mobile to allow debugging with the computer by choosing OK such in figure 5.
3. We could then open the mobile device in File Manager in Santoku Linux after revealing the interface, and then copy the mobile files manually to the Santoku Linux or to the host machine, as shown in figure 7.
4. In the Santoku Linux Virtual Machine => Device Forensics => AFLogical OSE command prompt, the command (sudo adb devices) was used to show the serial number of the mobile device before typing the command (adb reboot bootloader) to reboot the mobile device into recovery mode, as shown in figure 8.

The mobile device will be rebooted to start again after being unlocked successfully.

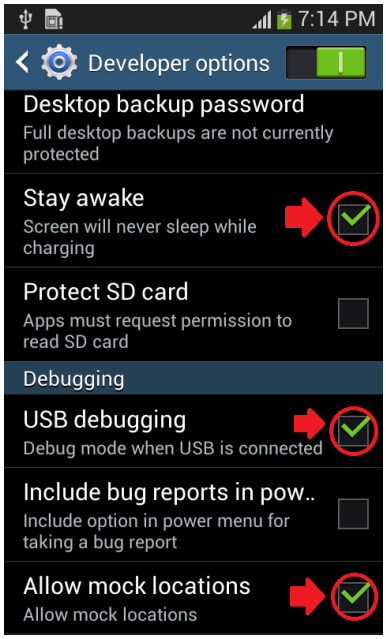

FIGURE 4: Setting Developer Options by Enabling Mobile USB Debugging.

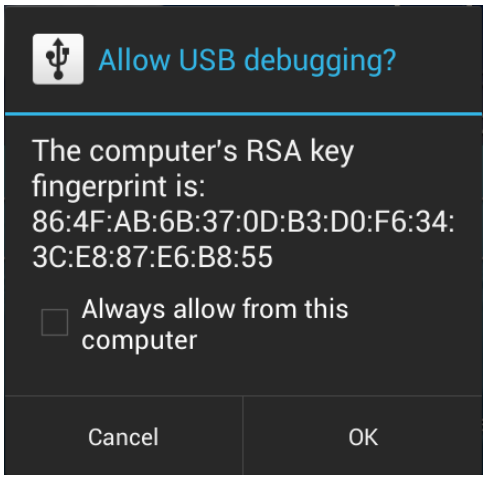

FIGURE 5: USB Debugging Agreement at Mobile.

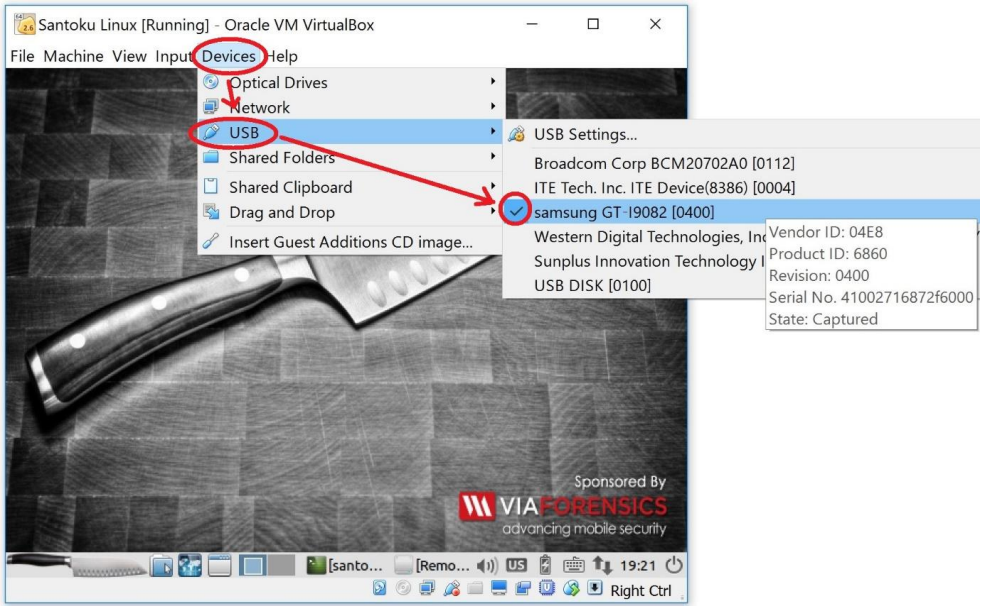

FIGURE 6: A Process of Connecting the Mobile Device to the Computer.

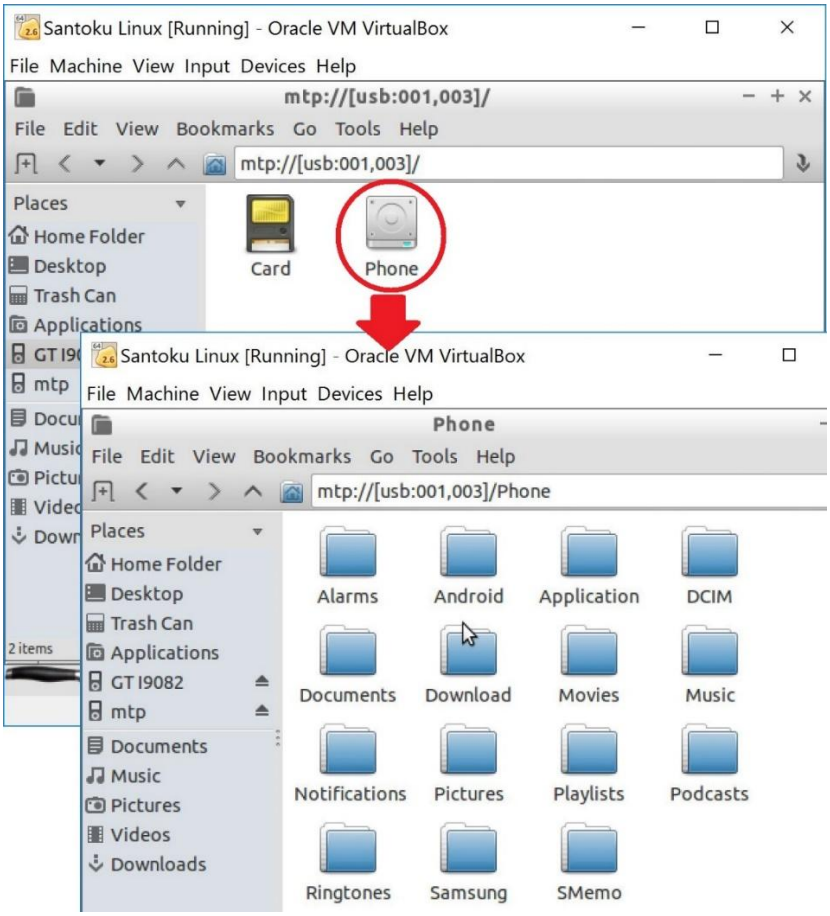

FIGURE 7: An Interface of Santoku Linux File Manager that includes Mobile Phone Data, such as Pictures, Music files and, etc.

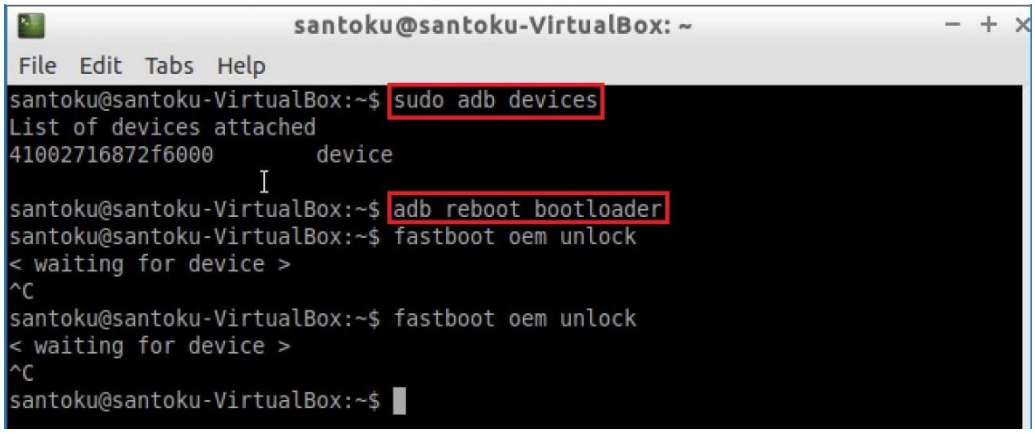

FIGURE 8: Enable Connection and Rebooting the Mobile.

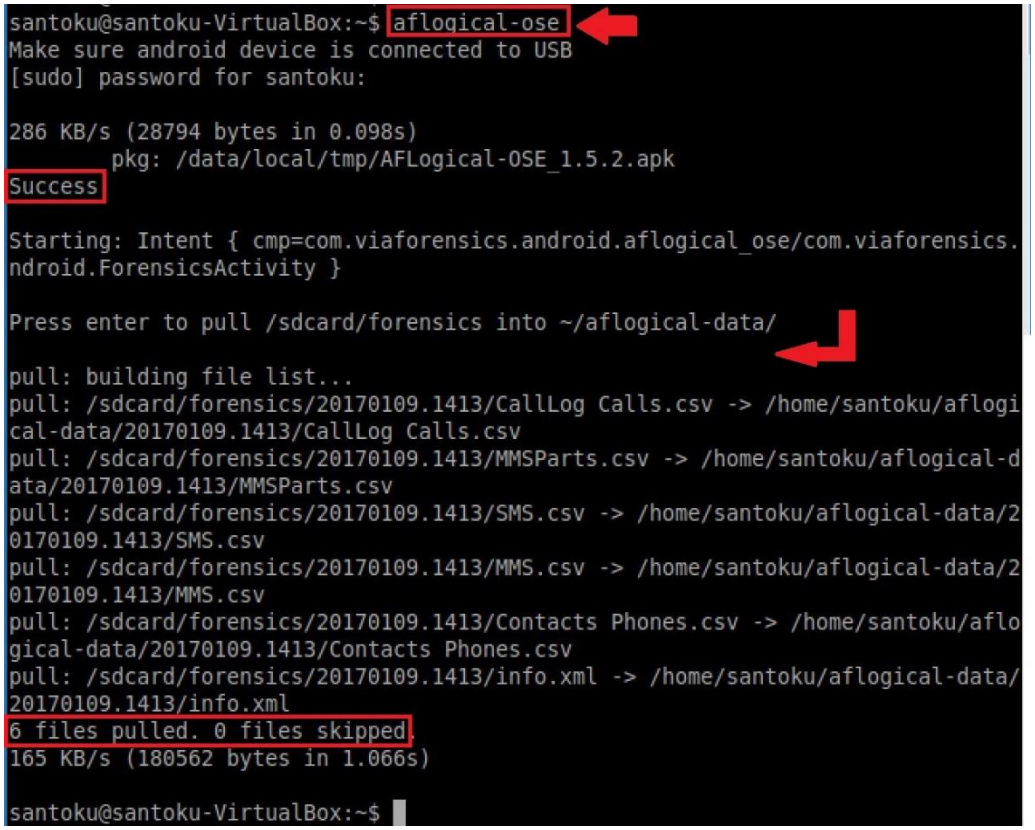

FIGURE 9: An Interface of AFLogical Command.

Step 3: Logical acquisition this process obtained particular data which contains device information, Contacts Phones, MMS, SMS, MMS Parts, and call logs by using the AFLogical application in the ViaExtract tool on the Santoku Linux Virtual Machine (Nowsecure Company). ViaExtract comes with a powerful application (AFLogical) capable of extracting data at the logical level Tahiri (2016). AFLogical is the tool which can assist in pushing the device application which downloads data from the mobile device by using the command (aflogical-ose) [17], as shown in figure 9. Therefore, we can recognise the AFLogical OSE application on the mobile device and we can select which data we want. Select all and the data will be extracted inside a folder named

according to the date and time of this process in figure 10. We must have an SD card installed on the mobile device (or built in) to extract the data. Next, we pulled the data from the SD card to the Santoku Linux Desktop by typing the following command as shown in figure 11 and figure 12:

$ mkdir ~/Desktop/AFLogical_Phone_Data
$ adb pull /sdcard/forensics/ ~/Desktop/AFLogical_Phone_Data

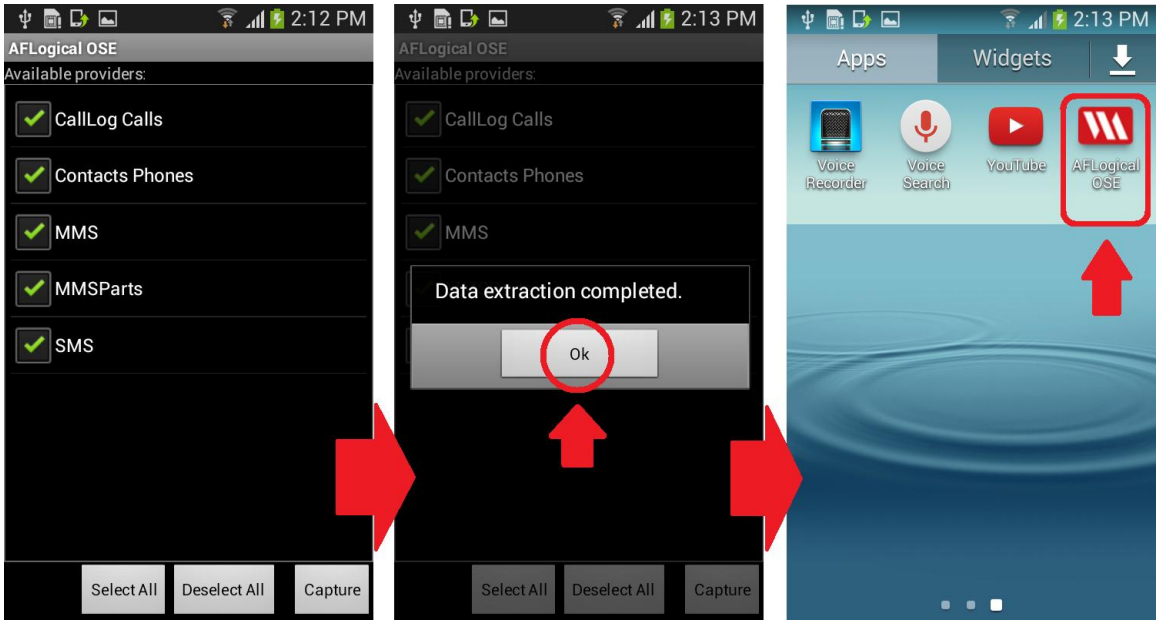

FIGURE 10: Data Extraction from the Android Mobile Device, including Calling Calls, Contacts Phones, MMS, MMSparts and SMS.

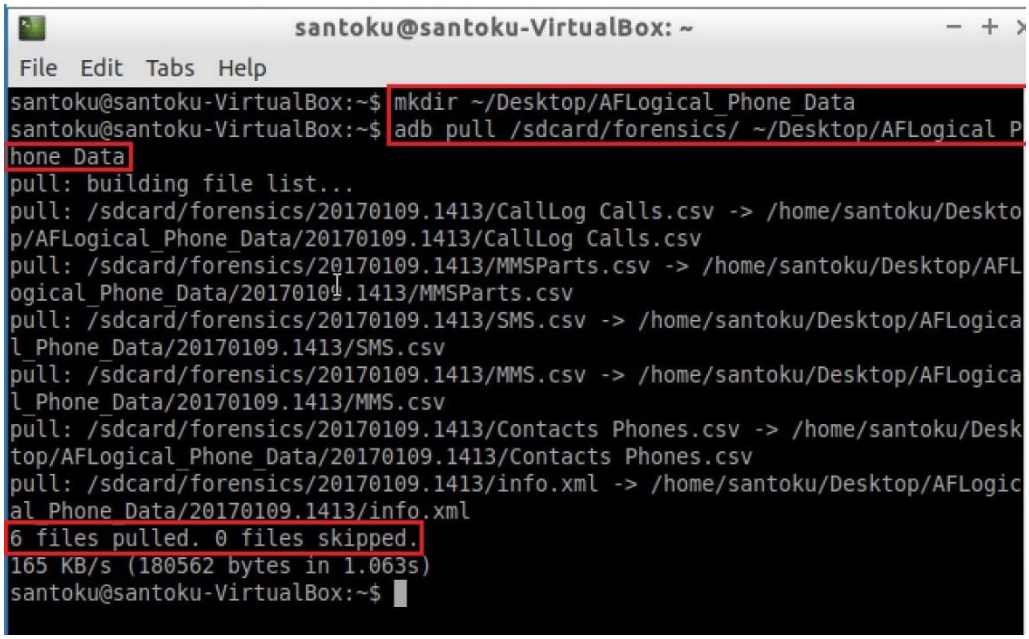

FIGURE 11: Pulling the Data to the Santoku Machine (Command).

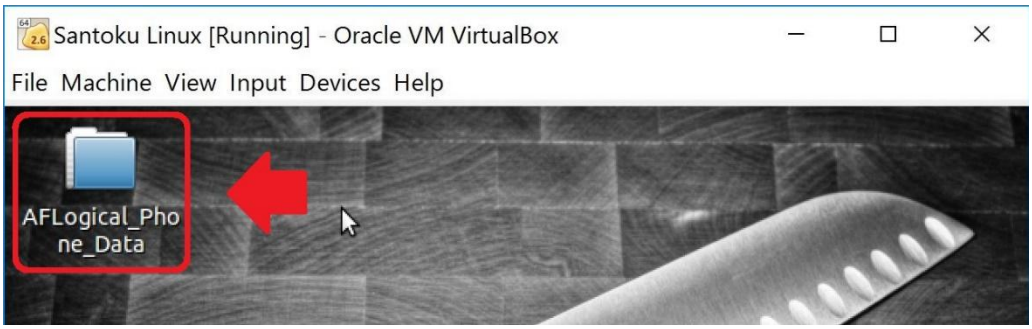

FIGURE 12: Create AFLogical of Mobile in the Santoku Linux Desktop.

Step 4: Physical acquisition this process was used to extract the data of the full contents of memory chips from the mobile device. The Access data FTK Imager tool was used to obtain a Raw (dd) image of the mobile devices backup, which is located on the USB memory Drive, and save it on the computer, as shown in figure 13.

1. Run AccessData FTK Imager => File => Create Disk Image => Physical Drive (because we have the data in USB Memory drive) => Select the Backup drive.
2. Select image type Raw (dd) which is a pure bit-for-bit copy of the source media => Write Evidence Item Information (optional) => Determine the image name (SD Backup) and destination (H:), as well as, inserting zero as the Image Formation Size to create the image as one file (do not fragment), as shown in figure 14.

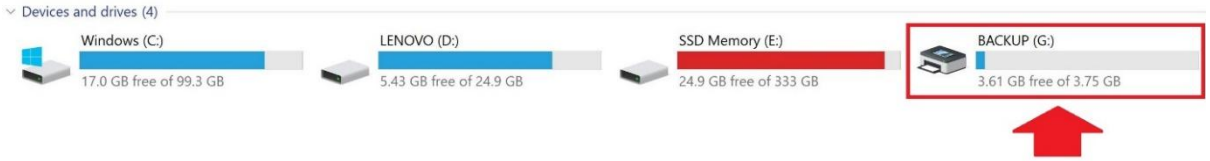

FIGURE 13: Mobile Device Backup.

As a result, we have three files:

1. SD Backup:001: Big dd file image, which is about 3.75 GB, because the raw image file is an uncompressed file format.
2. SD Backup:001:csv: Microsoft Excel Comma Separated Values File, which has all files and folders with their details.
3. SD Backup:001:txt: Text Document, which has all raw image file information, such as case information, Source Type, Cylinders, Heads,MD5, SHA1, etc. See figure 15.

3.6. Verification Phase

This experiment (one logical examination and three physical examinations) were implemented to obtain several results in order to compare with them.

Logical Examination using AFLogical ViaExtract tool in Santoku. For the final steps, we extracted data using Santoku, as shown figure 16 and figure 17. Data were extracted to the AFLogicalP honeData directory on the Santoku machine desktop. Device information, Contacts, Phones, MMS, SMS, MMS Parts, and Call Logs were found in figure 18.

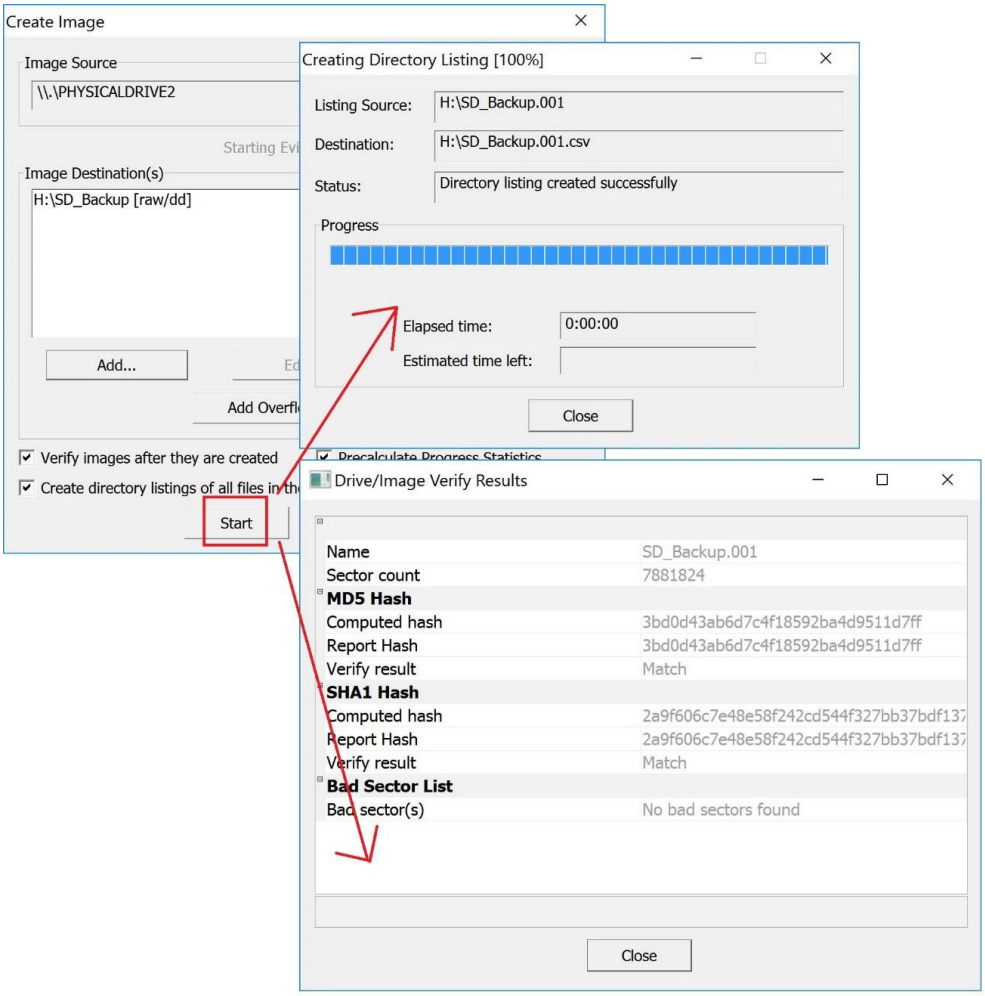

FIGURE 14: The Result of Image Acquisition.

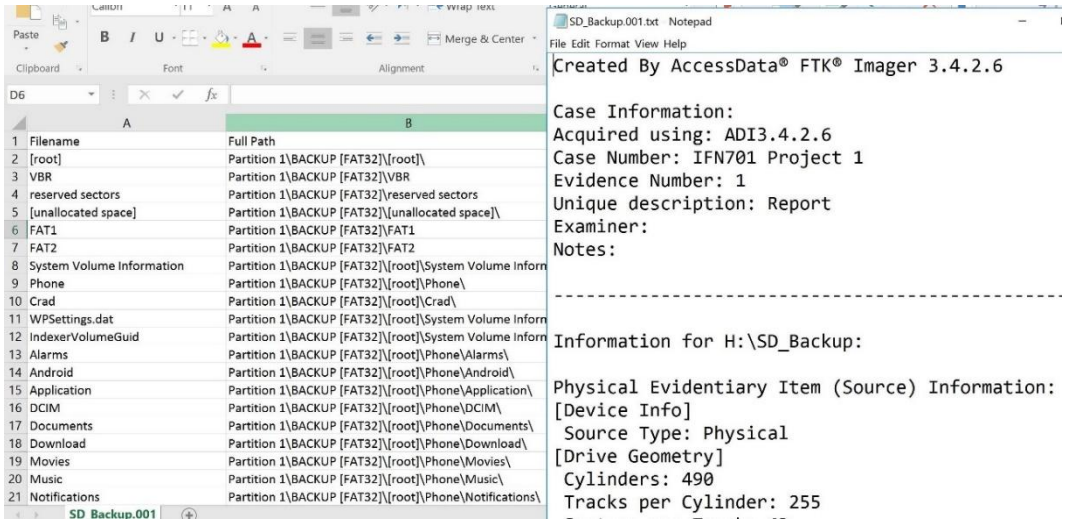

FIGURE 15: Two Final Reports Show the Details of all Files and Folders and their Containing Information.

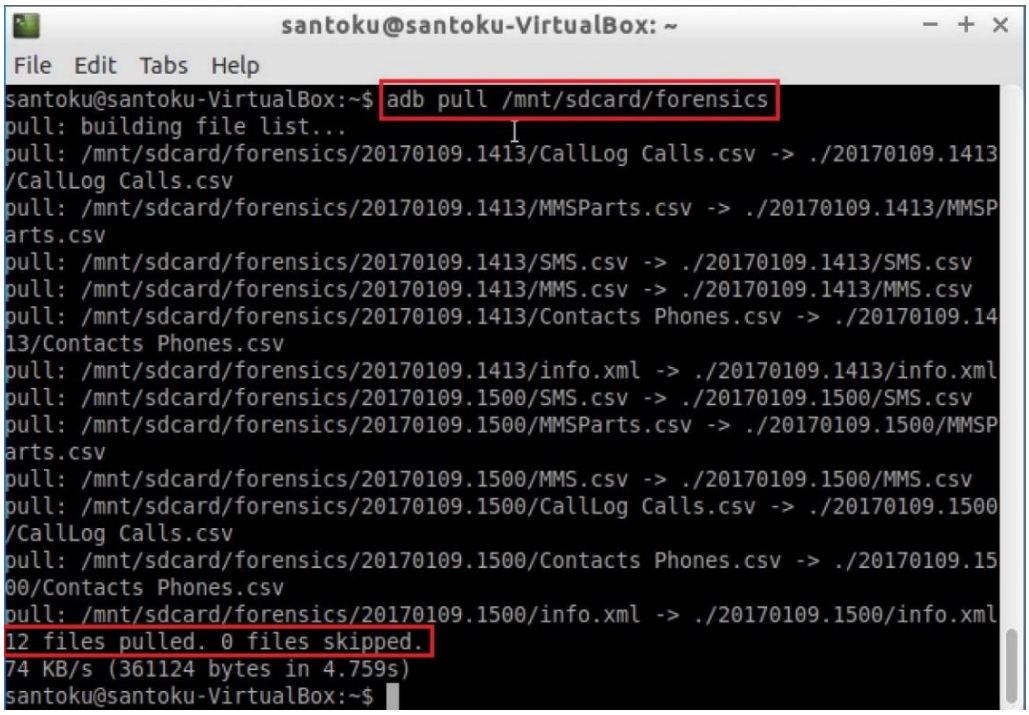

FIGURE 16: Santoku Extracting Data.

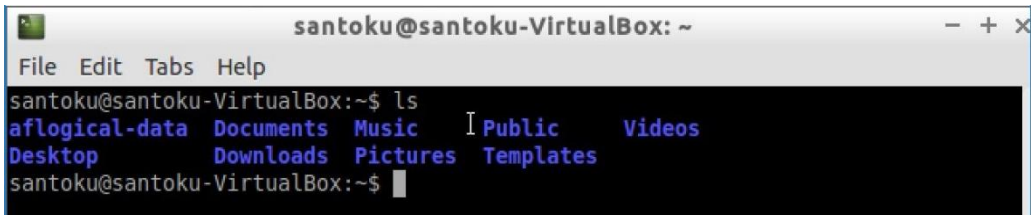

FIGURE 17: Directories After Aflogical-Data was Created.

Physical Examination using dd Image Evidence Tree in AccessData FTK Imager

1. Run AccessData FTK Imager tool => File => Add Evidence Item => Image File => Enter Source Path (Raw dd Image file location) => Finish.
2. This enables exploration of the image files in the Evidence tree. The full contents of the memory chips on the phone can be found. Contacts phone numbers, MMS, SMS, MMS Parts, Call Logs, Photos, and Video in the Android device were revealed. See figure 19

Physical Examination using Image Mounting in AccessData FTK Imager

1. Run AccessData FTK Imager tool => File => image Mounting => Browse the Backup Image (Raw dd Image file location) => Mount. A new partition, (F:), appears in Drive, as shown in figure 20. This partition is created as a temporary partition to look like the mobile device storage.
2. Mobile device files can then be explored in the new partition (F:). The full contents of memory chips on the phone can be found. Contacts Phones, MMS, SMS, MMS Parts, Call Logs, Photos, and Video in the Android device were revealed. See figure 21.

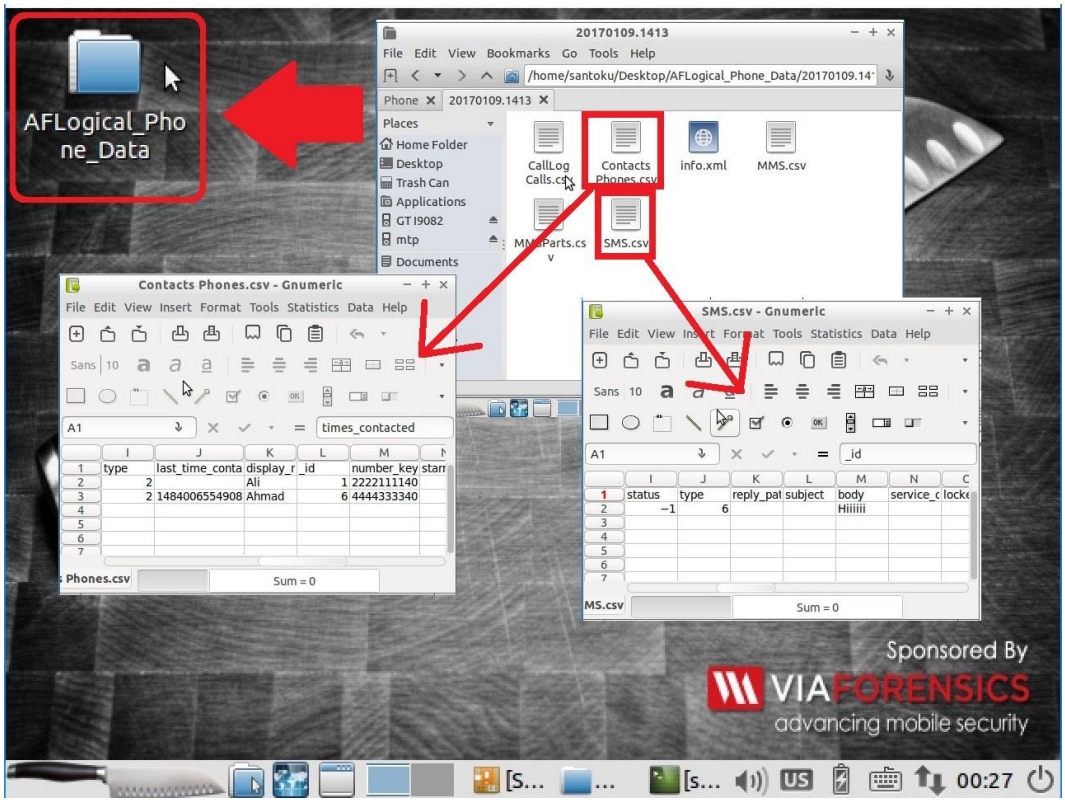

FIGURE 18: Data at The Santoku Machine.

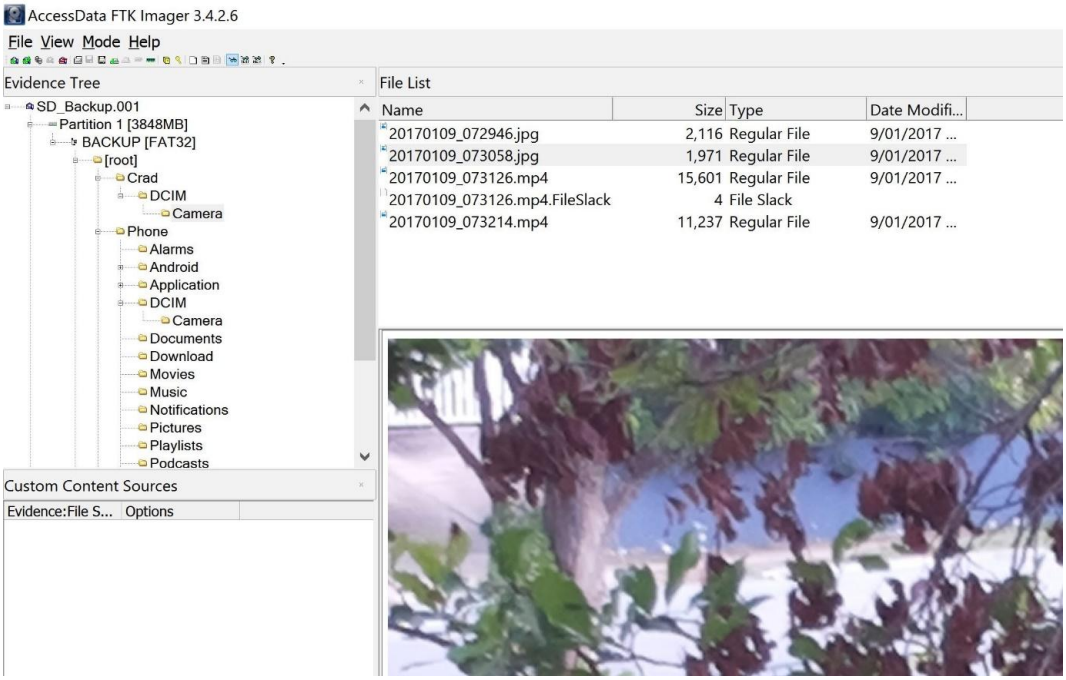

FIGURE 19: Image File Evidence Tree.

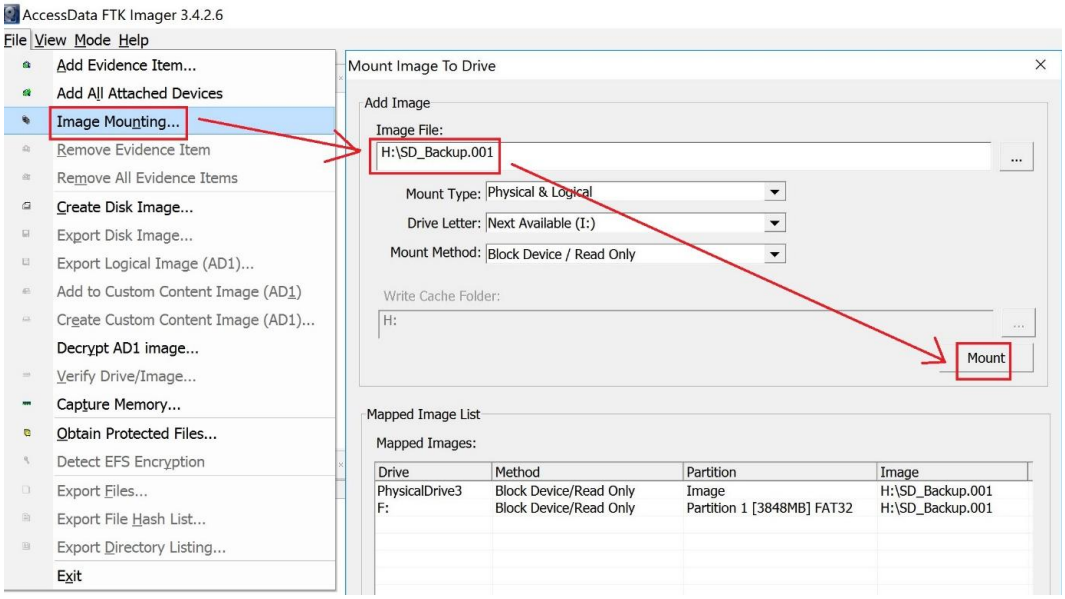

FIGURE 20: Image Mounting Examination.

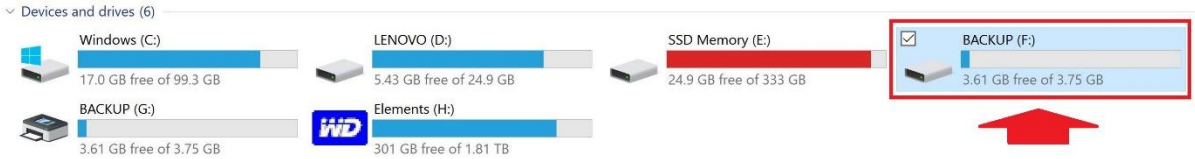

FIGURE 21: Backup Location.

Physical Examination using File Carving in Autopsy Autopsy is an open sourceend-to-end digital forensics platform. Its uses include creation of a file carving tool. It is a command line forensics tools with a html based graphical interface. Kali Linux has an Autopsy tool which can run from the desktop => Applications => Forensics => autopsy.

After the browser is opened and http : //localhost : 9999/autopsy is typed,a New Case is created and the image file is selected. After a few steps, the file analysis of the image file is displayed and the full contents of memory chips on the phone can be identified. ContactsPhones, MMS, SMS, MMS Parts, Call Logs, Photos, and Video in the Android device were identified, as shown in figure 22.

There were similar results for all examination methods. Contacts Phones,MMS, SMS, MMS Parts, CallLog Calls were found in the Android device using logical examination. As well as the same Contacts Phones, MMS, SMS, MMS Parts, and CallLog Calls, Photos and Videos were found in the Android device using the three physical examination methods Recovery of Deleted Files fromLost.DIR Directory. There is a folder named lost.dir in the SD card. This Lost.DIR is a folder to collect the accidentally lost files, as the Android operating system is running. It includes all kinds of accidentally unsaved cache data and other files. Once an accident happens in the system, the unsaved or corrupted files will be moved to this folder. The file name extensions of these files are removed and named as random numbers.

The function of this LOST.DIR in Android devices is similar to the recycle bin in Windows. Therefore, if you have accidentally lost files, you can restore them from the LOST.DIR folder.

It is necessary to recover files from the lost.dir file folder as soon as possible, otherwise they can be overwritten by new data. EaseUS Data Recovery Wizard Free tool for recovery of files from LOST.DIR

1. The external MicroSD card of the Android device is connected with the computer, after EaseUS Data Recovery Wizard Free software is downloaded.
2. Run the application and select the Local Disk for External SD card =>click “Scan" button.
3. After the scan, all the listed recoverable files in LOST.DIR folder can be previewed. Three photos are found, check list them and select \recover to recover them, then select a destination. All deleted Photos in the Android device are found,as shown in figure 23. We can recover only 2 GB using the free version of this application. To recover more than 2 GB, the application must be bought.

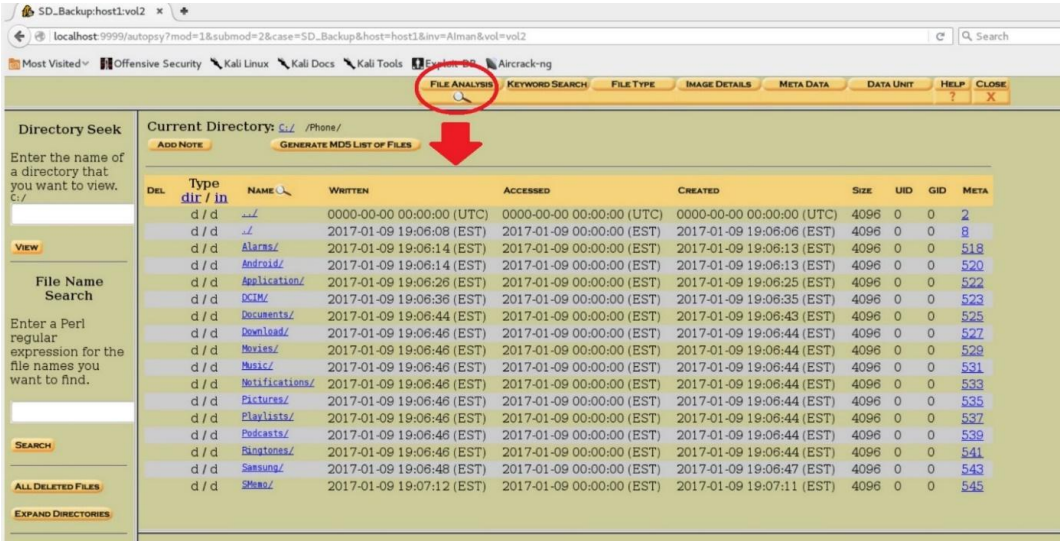

FIGURE 22: Image File Analysis by Autopsy.

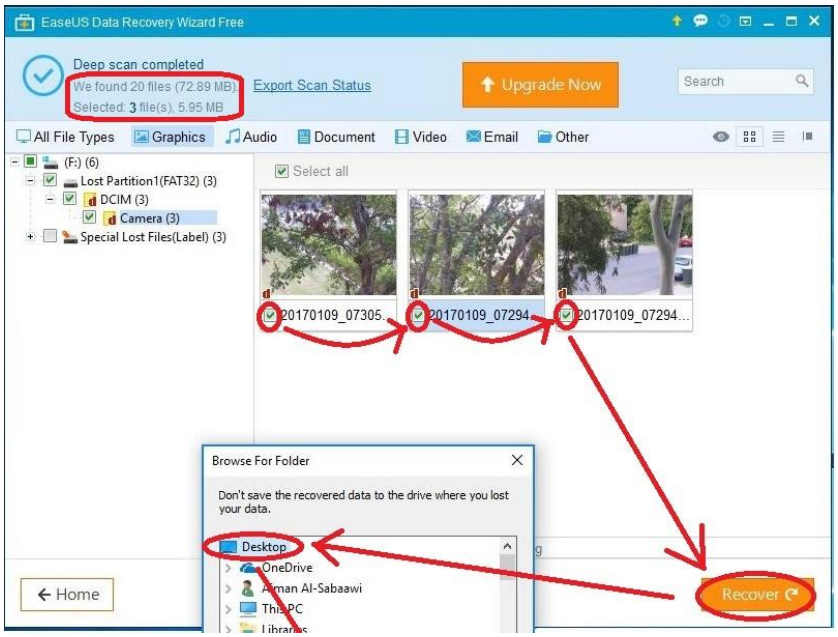

FIGURE 23: Recovering Deleted Files.

3.7. Documentation and Reporting Phase

The Final Report includes the following:

1. The examination began on 9 January 2017, 19:04.
2. The physical condition of the device was very good.
3. The photo of the device and the SD storage is shown in figure 24.
4. The status of the device when it was received was ON.
5. We required the following hardware: computer, Samsung USB Cable, USBMemory Storage, and SD Adapter. In addition, we required the following software: Santoka Linux VM, Kali Linux VM, AccessData FTK imager,Android Studio, and EaseUS Data Recovery Wizard Free tools (see Table-2 for device details).
6. For the data documented through the examination, as shown in Table 2.

FIGURE 24: The Samsung Android 4.2.2 Mobile and SD Storage Evidences

Evidences Type	Quantity	File name
Raw dd File	1	SDBackup.001
Microsoft Excel Comma Separated Values File	1	SDBackup.001.csv
Text File	1	SDBackup.001.txt
All mobile folders and files/ USB	1	folders and files
Contacts Phones	2	Contacts Phones.csv
SMS	1	SMS.csv
MMS	1	MMS.csv
CallLog Calls	1	CallLog Calls.csv
MMSParts	1	MMSParts.csv
Device Info	1	Info.xml
Photos	4	Photos
Videos	3	Videos

TABLE 2: Files of Evidentiary Value to the Case that Retrieving from Android Mobile Device.

4. CONCLUSION & CONCLUSION

Doing this acquisitions and analysis technical methods by Open Source Android Forensics tools (OSAF) was challenges, so doing these tasks by commercial tool, it will save time and will outcome accurate results. A variety of Android devices are available in the market. Their proprietary operating systems, different software and applications and commercial forensic tools make Android device forensics a challenging task for a forensics analyst. It is important to understand the Android architecture, forensic process and tools prior to data extraction and recovery of files. This paper presents the design of the Android platform to choose the appropriate tools for manual, logical and physical acquisition, as well as data analysis. We used a technique to retrieve evidence from items in the file system for both damaged and undamaged

Android devices in crime settings. There is also a need to use commercial methods for analysis of Android devices and Android device data. We propose two methods by AccessData FTK Imager, namely, dd Image Evidence Tree and Image mounting, as well as File Carving in Autopsy using a Kali Linux Virtual Machine for analyzing data. Also, we propose the use of the EaseUS Data Recovery Wizard Free tool for recovery of deleted files from the LOST.DIR. As a result, forensic investigators can achieve fast acquisition of data from an Android device that requires a USB cable to attach it to a computer. It should also produce the documentation and reporting of digital data for digital evidence in investigations. Furthermore, there is advice for researchers that arose from this work:

- The best way to recover data on an Android SD card is to use data recovery software.
- Before recovery, avoid overwriting any data on the SD card. If data are lost due to accidental deletion or improper operations, they should be recovered as soon as possible.
- To avoid permanent data loss, use data recovery software the first time. We will use this technique to obtain the data from a broken Android device for further investigation. A study will be done to compare the proposed tool for logical acquisition and analysis of data with other commercial and manual tools to achieve the best results in an investigation.

In future work, A study will be considered to compare the proposed tool for logical acquisition and analysis of data with other commercial and manual tools in [16][18][19][20] to get the best result for investigation. In addition, we will use the technique in [21] to retrieve handprint from android mobile device. To obtain the data from broken Android device, as shown in figure 25, we recommend to use hardware or software tool to access this mobile.

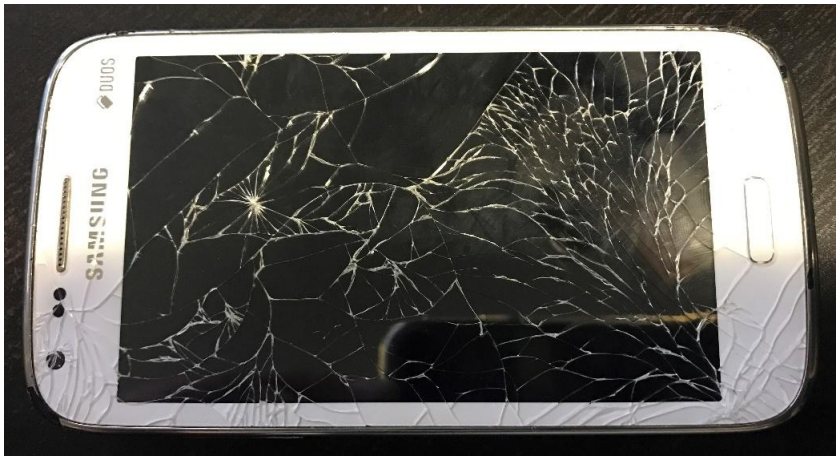

FIGURE 25: Broken Android Mobile

5. REFERENCES

[1] L. Xiaodong, C. Ting, Z. Tong, Y. Kun and F. Wei. “Automated forensic of mobile applications on android devices.” Digital Investigation, vol. 26, pp. S59-S66, 2018.

[2] A.A.-R.F. Al-Sabaawi and E. Foo. “Android mobile forensics for files system,” presented at the International Conference on Cybercrime and Computer Forensics, Gold Coast, Australia, 2017.

[3] N. Mace, S. Perica, C. Du_san, F. Igor and B. Mitko. “Android forensic and anti-forensic techniques: a survey,” in The Eighth International Conference on Business Information Security, (BISEC2016), 2016.

[4] L. Vogel. “Getting started with android development – tutorial.” Internet: www.vogella.com/tutorials/Android/article.html, 2009.

[5] F. Kausar. “New research directions in the area of smart phone forensicanalysis.” International Journal of Computer Networks & Communications, vol. 6, pp. 99, 2014.

[6] A. Gunnar, D.G. Olav and S. Axelsson. “Forensics acquisition analysis and circumvention of samsung secure boot enforced common criteria mode,” in Digital Investigation 24, 2018, pp. S60-S67.

[7] A.A.M. Alamin and A.B.A. Mustafa. “A Survey on Mobile Forensic for Android Smartphones.” IOSR Journal of Computer Engineering (IOSR-JCE), 17(2), pp. 15-19, 2015.

[8] R. Venkateswara and C. ASN. “Survey on android forensic tools and methodologies.” International Journal of Computer Applications, vol. 154, pp. 17-21, 2016.

[9] R. Ayers. “Mobile device forensics,” in NIST Mobile Forensics Workshopand Webcast, 2014.

[10] C.A. Murphy. “Developing process for mobile device forensics”. Accessed on, 11, 2009.

[11] F. Peijun, L. Qingbao, Z. Ping and C. Zhifeng. “Logical acquisition method based on data migration for android mobile devices,” in Digital Investigation, 2018.

[12] L. Xue, C. Qian, H. Zhou, X. Luo, Y. Zhou, Y. Shao and A.T. Chan. “NDroid: Toward tracking information flows across multiple Android contexts.” IEEE Transactions on Information Forensics and Security, 14(3), pp. 814-828, 2018.

[13] S. Bommisetty, R. Tamma and H. Mahalik. “Practical mobile forensics.” Packt Publishing Ltd, 2014.

[14] L. Rocha. “Computer forensics and investigation methodology – 8 steps.” Internet: www.countuponsecurity.com/2014/08/06/computer-forensics-and-investigation-methodology-8-steps, 2014.

[15] Developers. “Get the Google USB Driver.” Internet: www.developer.android.com/425 studio/run/winusb.html, 2016.

[16] S. Tahiri. “Android Forensic Logical Acquisition.” Internet: www.resources.infosecinstitute.com/android-forensic-logical-acquisition, 2016.

[17] Santoku. “How to use aogical ose for logical forensics of an android device.” Internet: www.santoku-linux.com/howto/howto-use-aflogical-ose-logical-forensics-android/, 2016.

[18] H. Srivastava and S. Tapaswi. “Logical acquisition and analysis of data from android mobile devices.” Information & Computer Security. 23(5), pp. 450-475, 2015.

[19] Sunphinx. “Mobile Device Forensics. Retrieved from Sunphinx Mobilite & Ceber Securite.” Internet: www.sunphinx.com/en/mobile-device-forensics.html, 2016.

[20] C. Tassone, B. Martini, K. Raymon and J. Slay. “Mobile device forensics: A snapshot.” Trends and Issues in Crime and Criminal Justice, (460), pp. 1-7, 2013.

[21] K.A. Al-Dulaimi and A.A.R. Al-Saba’awi. “Handprint Recognition Technique Based in Image Segmentation for Recognize.” International Journal of Computer Information Systems, 2(6), pp. 7-12, 2011.