International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Framework for Data Extraction and Analysis of Damaged Android Mobile Device

Nibedita Chakraborty[1], Dr Ravi K Sheth[2], Dr Sunil B Mane[3]
[1]*Student Master in Technology Cyber Security Raksha Shakti University*
[2]*Assistant Professor Raksha Shakti University*
[3]*Associate Professor College of Engineering Pune*

Abstract: ***Nowadays, Android Mobile phone device users were spreading vastly. Mobile device is the most crucial media of digital evidence for the law enforcements, but the investigation process of the mobile device forensics system is absolutely inefficient as compared to digital forensics. Mobile forensics depends on the operating system of the device, model number of the seized device and the condition of the mobile device when it is seized from the crime scene. If the seized mobile device is logically damaged (Screen damage) but it is in chargeable mode and can be detected by the forensic workstation. Sometimes, the device is locked with some PIN / Pattern or Passcode, that time forensic experts faced some problems to extract data from such device. On the above ground, this paper will show how the data, what types of data can be extracted and analyzed the limitations of the data from a screen damaged android device through manual extraction, logical extraction and physical extraction tools normally available. After that this paper will implements a framework for the damaged android mobile device, where all types of data extraction can be done under one roof and it will make the forensic investigation efficient and smooth.***
Keywords: Mobile Forensics, Digital Forensics, Damaged state, Extraction, Digital Evidence, Acquisition

I. INTRODUCTION.

In modernized culture, carrying a mobile phone is about a fundamental element to the moderate individual. With this expansion of modernized technology, mobile phone device have grown into a portable exclusive computer, having the capability to handle the maps, interact, and stock immense chunk of information and data. Mobile phone gives facility to common people to do work by less consuming time. Mobile phone device has countless features such as mobile incoming and outgoing calls, short message services (SMS), multimedia message service (MMS), and What Sapp messages that because it becomes simple to circulate data to the people or class of people. Apart that it can be usable to record difficult position. Moreover, the usage of mobile phone device does not appear beyond any drawbacks.

Mobile phone device is a practical device which used SMD peripheral, Microprocessor and microcontroller, Flash memory, Circuit board. Mobile phone contain antenna, LCD screen, Microphone, speaker etc.

The main part of the Mobile device is the circuit board. Circuit board contain analog to digital translator chip as well as digital to analog translator chip which translate going out audile from analog to digital and translate coming in audile from digital to analog.

1) The chips which present in the mobile phone device are follows
a) Digital signal processor
b) Microprocessor & Microcontroller
c) Flash Memory and ROM

When Examining the Seized Mobile phone, the Forensic Investigator found records in the following sections of the Mobile phone: 1) SIM Card 2) Micro SD Card

2) SIM card normally stores the following data:
a) Contact details
b) SMS Messages history
c) Dialed Call details

External storage of a mobile phone is also called the SD card or USB driver that is externally embedded into the mobile phone. It is also called auxiliary storage of the device.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

II. BACKGROUND

Digital forensics is a subsidiary of forensic discipline which consists of the recognition, retrieval; examination, verification, and submission of details about the digital clue erect from a computer or related digital repository disclosure gadgets. Digital forensics is generally being used to aid to examine the electronic corruption or integrity explicit clue of a computer based fraud. Digital forensics is generally being usable in twain illegitimately act and non-governmental inspection. The objective of this mechanism is to protect the clue in its maximum authentic pattern when operating an analytical analysis by gathering, determining and justifying making the binary data for the objective of recreating the former affair. Among the different branches, Mobile Phone forensics is the freshest upcoming divisions of digital forensics describing to retrieve the digital clue from a seized mobile phone device. Investigation is typically performed either on digital resource such as computer, or server that was used to commit the crime, or was a target of crime. Digital forensics is carried out only to recover, restore, validating the digital evidence. The digital evidence is all the data carrying out, transferred or gathered digitally, and this data contain the probative rate. It can be recovered from the hard drive, mobile phone device, flash drives, routers, tablets, e-mails, laptops. Android Mobile device forensics is the branch of retrieving the binary clue from a seized mobile phone under forensically stable situation using authorized process. The most important problems deal by mobile forensics investigators during the examination process are explained given below:

A. Platform Independent
B. Builder
C. Adapter
D. Operating Systems
E. Applications
F. Security
G. Picking Right Mobile Forensic Tool

III. MOBILE FORENSICS INVESTIGATION PROCESS

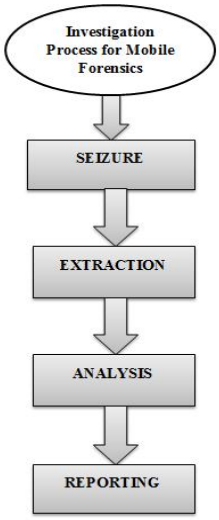

Fig. 1. Mobile Forensics Investigation Process

There are mainly four parts in mobile forensic investigation process as follows:-

A. Seizure

Investigators seized the mobile device from the crime scene and insulate it from outside networks so that no one can modify, delete or tamper the data.

There is a big challenge that is passcode recovery faced by the investigators during this process as follows:-

1) From a forensic examiner opinion, breaking the seized device is the fundamental point while doing acquisition. Therefore several technical processes can be used to breach the security on the android based operating system.

There are two processes to break the code PIN/Pattern/Password Break Code (Rooted Condition) as follows:-

a) For Pattern Break – adb shell rm/data/system/gesture. Key For Password/PIN Break- adb shell rm/data/system/password. Key

b) To breach the Pattern/PIN/Password (Give enter after every command) –

```
adb shell
cd data/system
su
rm *. Key
```

B. Extraction

The objective of this step is to retrieve the data from the seized mobile phone device. There are two methods of data extraction in mobile forensic investigation are follows:-

1) Non Invasive Method

2) Invasive Method

C. Reporting

Save and make record of the extracted digital evidence in a simple document format so that it could be understandable by technical as well as non-technical personnel.

IV. ROOTED AND UN- ROOTED DEVICE

Forensic job needs to get the android mobile device should have root privileges to get the actual and erased digital clue from the seized device.

A. Rooting is the most important word regarding Android Forensics. With the help of this, Forensic Analyst can earn knowledge about the private structure of the seized device. To recover data in depth from the seized device, forensic investigators himself rooted the device in forensic sound manner so that no data will tampered.

B. Un-rooted mobile devices provide the user to access the internal and external memory repository median that permits a forensic examiner to run Logical Acquisition of the seized mobile device. The system details, memory of the seized device and system memory of the mobile device are normally visible by the users. Moreover, entire device backup or adb backup can be employ to run logical acquisition of the mobile device. Partitions and System Folders are stored secret with no access.

But nowadays, Mobile manufacturer don't allow the rooting process for the latest Android version as it may changes / modified the software as well as the hardware of the mobile device. In case of a short- term (Temporary) root, the modification is vanished when the device is reboots. Non-permanent roots are always being referred in forensic cases. In case of rooted devices the entire mobile device extraction can be executed using data definition (dd) command or automatic tools. Root privilege provides a forensic examiner to run data retrieval and carving that crack the erased digital clue reserved in the mobile device.

V. RESEARCH METHODOLOGY

Here, we will explain the methodology which is used for the research. Simultaneously we focused on the data extraction approach, different tools and techniques which are applied in this research and all the hardware and software requirements that are needed for the observation.

For Manual data Extraction, used adb tool, resourceful command based tool which helps to connect to a device. The vital location for a mobile forensic investigator that can be retrieved using adb tool are /system, /data, /sdcard.

1) */System:* It consist of operating system data. The directory holds several subdirectories that contain data related to the system, applications, fonts, libraries, and executable.

2) */Data:* It consist of user related data like SMS applications. It needs root access that means a user without a rooted mobile device couldn't access the data of the particular directory.

3) */Sdcard:* It is used for external storage. It is mostly used to store user data such as images, music files, videos etc.

Here, by using DD command we will dump a memory partition from the android seized mobile device to do the forensic investigation. We used Netcat for receiving the output of the memory dump. When the DD finished the job, we can analysis the image by using Belk soft evidence center. From a forensic perspective, using several adb commands we can extract data like SMS,

MMS, Photos, Account Credentials etc. For Logical Extraction, used AFLogical tool used to extract call logs, phone contact details, MMS messages, MMS parts, SMS messages from the target device. It is available totally in free of cost for law enforcement person. Here, we have used Santoku Linux where AFLogical OSE is already installed. For Logical extraction, Physical Extraction, Capture image, and Capture Screenshot, we used Cellebrite UFED Version 7.15, it extracts the content types like phonebook data, apps data, pictures, email data, Ringtones, Call logs, Browsing data, Calendar etc. But the tool is unable to detect the test subject (YU YUREKA PLUS). In order to overcome the hindrance, we have used UFED Chinex through which detection was feasible.
The following are the important specification in this paper:

TABLE I. MOBILE DEVICE USED

Damaged Android Mobile Device	Operating System	Types Of Device
Yu Yureka Plus	Android 5.1.1	Un-Rooted Condition

TABLE II. PROGRAMMING LANGUAGE USED

Programming Language Used
Hypertext Markup Language(HTML)
Cascading Style Sheets(CSS)
JavaScript(js)

TABLE III. TECHNICAL FRAMEWORK USED

Framework Applied
Electron js for the Desktop GUI Application

VI. IMPLEMENTATION

In this, we will explain how the data is being collected from a damaged seized mobile device where the mobile device is in charging condition but its display is not working. To achieve all the digital evidence from a mobile phone, it is mandatory to make the Mobile device attached to the forensic workstation with the USB cable or Wi-Fi or Bluetooth.

If the seized mobile device has a damaged USB Cable port then USB connection is not imaginable that time we have to connect it with the help of Wireless fidelity or Bluetooth. But USB connection is required if we are trying to achieve ultimate data. When we are trying to connect the device using Wi-Fi that time we should remember one thing that both the mobile phone and the forensic workstation has to be attached within the equivalent Wi-Fi network.

Here, the seized device USB cable port is totally fine so we can connect it by using USB cable with the Forensic workstation.
If the Display of the seized mobile device is no more active, we can apply three approaches as follows:

1) Using an OTG CABLE, it denotes USB On-The-Go, where we can attach a Computer mouse to the mobile device. Then we can use the mouse on the mobile device to navigate the settings for enable the USB debugging. After that install adb to connect with the forensic workstation.
2) Change the screen from any service center. Until the charging port as well as the USB connection port is active, we can extract any data from the seized device.
3) Once the adb is installed, we can apply the Android Screen Mirroring Technique where we used Vysor that Allows the Android users to supervise their mobile device direct from the forensic workstation.

Therefore in this paper, Authors going to implement the above said framework. Using this framework, forensic experts can easily extract different digital evidence in a single roof. The framework is very easy-to-handle, easy to understand Android device extraction desktop application. Mostly, the Data extraction module explained above is only applicable for data retrieval on rooted Android mobile device.

a) It is developed in electron framework to design a desktop application. Electron is a freeware library introduced by GitHub for developing platform independent desktop applications with the help of HTML, CSS, and JavaScript. It normally executes by connecting Chromium and Node.js into an individual runtime and application for windows, Linux etc. Electron enables us to develop desktop applications with core JavaScript by creating a runtime with an application programming interface. It mainly used the main file prescribed in the file named package.json and runs it.

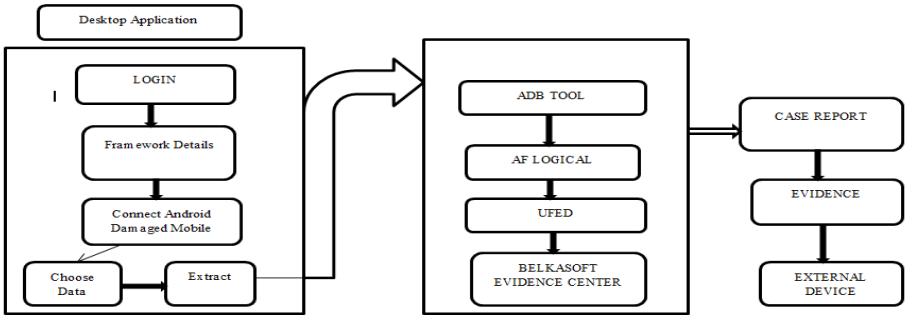

Fig. 2. Damaged Android Mobile Forensics Framework

As the above diagram, the framework contained the authorization process(LOGIN), details of the framework designed by the developers, connecting stage, choose data for extraction , analysis procedures, documentation steps and last of all storing the evidence into an external device. This framework can be accessible by authorized forensic experts only so in future we are going to attach a database with this that will store all the login details of the accessing investigators. This Study is planted on a modernized way where we need to root the seized damaged android device to recover the compact piece of digital evidence. This paper explained the integrated framework of the mobile device forensics investigation process, evaluating its functioning fundamental, recommending forensic procedure of the targeted system. In this paper, authors want to build up the examination of mobile device forensic process. Nevertheless, this forensics framework can be used for greater achievements which are a crucial factor in a time consuming forensic investigation.

VII. RESULT

This framework was figure out for different factors using open source & paid versions of Android forensic tools as the extraction source. The individual tools give different digital evidence as follows:

TABLE IV. FEATURE & EVIDENCE EXTRACTED

FEATURE	ADB TOOL	AF LOGICAL	UFED Chinex	BELKASOFT EVIDENCE CENTER
Root Needed?	Yes	No	No	Yes
Physical Extraction	Yes	No	Yes	Yes
PIN/PATTERN Break	Yes	Yes	No	Yes
Call log	No	Yes	Yes	No
Contacts	No	Yes	Yes	Yes
MMS	Yes	Yes	Yes	No
MMS Parts	No	Yes	Yes	No
SMS	Yes	Yes	Yes	No
Partition list Extraction	Yes	No	Yes	No
Application Data	Yes	No	Yes	No
Downloaded Data	Yes	No	Yes	No
SD Card Data	Yes	No	Yes	Yes
Hangout Messages	Yes	No	No	No
Facebook Data	No	No	Yes	No
Whatsapp Data	Yes	No	Yes	No
Voice Recording	Yes	No	Yes	No
Creating Image	Yes	No	Yes	No
Pictures	Yes	No	Yes	Yes
Browser Details	No	No	Yes	Yes
URL	No	No	Yes	Yes
Documents	Yes	No	Yes	Yes
Video	No	No	Yes	Yes
Timeline Details	No	No	Yes	Yes

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

VIII.CONCLUSION AND FUTURE WORK

This Framework is for those Android Forensic examiners who do not wants to use costly paid Android forensic tools to fulfill their jobs. With this above research work, the Android forensic experts do their work very quickly and efficiently. In the above paper, authors developed a mobile forensic framework for damaged Android mobile device which provides combined solutions which is not generally available in one single tool. The desktop application of the framework is already implemented but as some of the tools source code is not available so backend of the framework is yet to be implemented in future. This framework can be accessible by authorized forensic experts only so in future we are going to attach a database with this that will store all the login details of the accessing investigators. This Study is planted on a modernized way where we need to root the seized damaged android device to recover the compact piece of digital evidence. The achieved outputs are correlated and inspected to contribute a complete outlook of the present mobile device forensics scene. If the modern methods are not being approached, it would be result with the rise of mobile crimes which do not have evidence to be proven and give chance for crime committers to consider these loop holes and hike the mobile crime rate.

REFERENCES

[1] S Kumar Reddy Mallid , Parimala Palli, A Comprehensive Analysis of Smartphone Forensics & Data Acquisitions, 2016 International Journal of Advanced Research in Computer Science and Software Engineering.
[2] Common Investigation Process Model for Database Forensic Investigation Discipline, Arafat Aldhaqm, ShukorAbdRazak, SitiHajar Othman, 1st ICRIL-International Conference on Innovation in Science and Technology (IICIST-2015).
[3] Shivankar Raghav , Asish kumar Saxena, Mobile Forensics: Guidelines and Challenges in Data Preservation and Acquisition, IEEE Student Conference on Research and Development 2009.
[4] Research on the Data Recovery Method of Deleted SMS for iPhone, ZHANG Kai-xiang; ZHOU An-min, Modern Computer 2015.
[5] Forensic Investigation and Analysis on Digital Evidence Discovery through Physical Acquisition on Smartphone**,** Taniza Binti Tajuddin , Azizah Abd Manaf, World Congress on Internet Security (WorldCIS-2015)