International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Modified Model for Mobile Forensic

Prachi Ankush Zinge[1], Late Dr. Madhumita Chatterjee[2], Dr. Prashant Nitnaware[3]

[1]Computer Engineering, Pillai College of Engineering New Panvel, India
Email: *prachiz.2987[at]gmail.com*

[2]Computer Engineering, Pillai College of Engineering New Panvel, India

[3]Computer Engineering, Pillai College of Engineering New Panvel, India
Email: *pnitnaware[at]mes.ac.in*

Abstract: ***Mobile phone is a combination of various components including the computer, camera, calculator, play station and music system etc. Though mobile has been proved to be a boon for human beings which has multiple functions useful for people of all age groups and beyond gender, race, cast or country, it can be used by cybercriminals also. A cybercriminal can delete, hide data from mobile phone or transfer data on another system through social media applications or in other words you can say as hacking. Mobile forensic is a branch of knowledge which helps to detect and analyses any malicious activity performed by criminal on mobile device. Though different mobile forensic tools are available, but not a single integrated tool has been found which creates image of mobile device as well as does a complete analysis. We are going to present a mobile forensic framework which solves this problem by creating image from android mobile phone as well as extract deleted data, hidden data, contacts, multimedia files (images, audio and videos. The mobile forensic acquires image and will be extracted in order to get any evidences if there be and generates reports. Based on these extracted data, multiple reports can be generating that will help entire cybercrime. Our framework would be a generic framework and we will test it using android mobile device.***

Keywords: Mobile Forensics, Mobile Forensics tool, Mobile Forensic Framework.

1. Introduction

In today's modern era, we can't imagine a world without computers. The computers are omnipresent and their usage is covering our universe. There is not a single field of life where computers are not used. While explaining the inevitability of computers in our life, a drawback must be mentioned. Our basic subject is itself about this drawback and its study to avoid it. As computers have captured our entire life space, unfortunately it is useful to cyber criminals also. Cyber criminals can also exploit its speedy and accurate functioning which can be a huge loss to mankind. With the universal use of computers, cybercrimes are also on increase rapidly. The design of computers is such that they are interconnected with each other in the form of networks and exchange huge amount of data which is the main reason for cyber fraud and cybercrimes that take place. Cyber criminals use IT infrastructure or technology which has given birth to the branch of knowledge which is called as Digital Forensic which deals with cybercrimes.

Mobile phones have created another revolution in our life. There is no need to explain its importance as they have become integral part of our life. They are the most personal electronic devices a user accesses. The functions of a mobile phone include simple communication tasks, such as calling and messaging, connecting one person to another, still providing support for Internet browsing, e-mail, taking photos and videos, creating and storing documents, identifying locations with GPS services, and managing business tasks [11], i. e. it performs all functions that a computer can perform. But they also have not been escaped from the clutches of cyber criminals. Almost, every digital forensic investigation conducted basically includes a mobile phone. The science of recovering digital evidence of any cybercrime from mobile phones is called as mobile forensics. Digital evidence is defined as the information and data that is stored in, received, or transmitted by an electronic device that is used for investigations. Or in other words, it can be said that digital or electronic evidence which is probative information stored or transmitted in digital form which can be used in a court trial.

2. Methodology

There are several tools available for mobile forensic which are open source and commercial. They can be classified as physical acquisition and logical acquisition. Physical acquisition is making an identical replica of original and logical acquisition is creating a copy of information and data stored in a device. There is no denial of the fact that mobile phone or smart phones play a vital role in investigating a cybercrime. So, mobile forensic tools are most important in investigating the cybercrime. Each tool has different functionality with respect to different mobile devices. But problem with available mobile forensic tools is that they are not easily available. Also the installation and working of mobile forensic tools is not handy. Another problem that persists with mobile forensic tools is that single integrated open source mobile forensic tool, which will perform all phases of investigation i. e. from identification of device, creating an image to analysis to generating report is not available. Different tools for different phases have to be used. It makes investigation lengthy and difficult. Therefore, to overcome these problems following figure shows proposed architecture of mobile forensic framework.

A. Framework

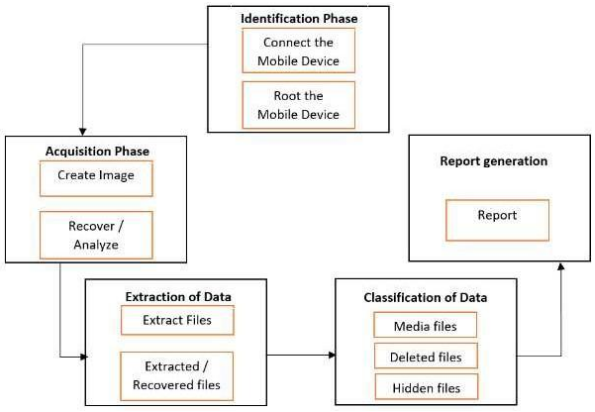

Figure 1: Architecture of proposed mobile forensic framework

3. Experimentation

a) Identification phase

As the evidence is stored in device, identification of device is the first step. The first step of proposed mobile forensic framework is crucial because this phase performs identification of device to check whether evidences can be gathered or not. The market is flooded with different models of different manufactures. So the examiner has to be updated with new models available in the market.

b) Acquisition phase

Acquisition is the process of cloning or copying digital data evidence from mobile devices. It can be stored in different formats which can be used for further analysis. The image of mobile device will be created. It is called as imaging. During the process of image creation there is requirement of write block which will permit read-only access to data storage devices without compromising the integrity of the data. For creation of the image, the mobile device should be rooted so that investigator will have privileges to access all the folders in mobile phone. The image of the entire device can be created or also it in parts, according to the requirement. The resultant image can be saved in various formats including DD and Raw.

c) Extraction of data

The goal of this phase is to retrieve data from the mobile device. The extraction of data is the process that involves retrieval of data from various sources. The extraction module performs the function of logical acquisition of data from the mobile device running on Android OS. The logical extraction of data is a technique for extracting all the files and folders without any of deleted data from the mobile device. All the data can be extracted from the mobile device since rooting has been done, so it enables investigator to view all the files available in the device. This process is done with the goal of preserving any evidence in its most original form while performing a structured investigation by collecting, identifying and classifying the digital evidence. Even a locked screen can be unlocked using a PIN.

d) Classification of data

After extraction of data is completed, now the investigator has to classify the data in order to categorize exactly what types of files are present in the internal memory of mobile device. This is most important step in the investigation of cybercrime. The tool will classify the files into six categories

- Call logs, SMS, Contacts
- IMEI number, SIM number
- Multimedia files such as images, audio and video.
- Deleted data
- Hidden data which was not visible before rooting.
- Stegano data or concealed data that is hidden image or audio within another image or audio.
- WhatsApp data stored in database folder of mobile phone.

SQLite-In this, we need not create physical image but can extract data by generating the file system dump. File system dump is a copy of all files. Only those files which are currently present in the mobile device are contained in file system dump. It will not show deleted files of slack space. All the user activities like installing an application from Playstore, call logs, SMS, Contacts, locations etc are stored in these database files which in turn are embodied in these files.

Deleted data-The data which is deleted intentionally or unknowingly can be recovered through the image we have created. When a file is deleted from a specific device means that file is not destroyed. But the physical location or the address which has been allocated to the file is deleted. The actual file remains there. When a new file is to be stored, it is stored on that physical location of the file. Eventually the old file is overwritten. So there is a scope for the recovery of deleted file if it is not overwritten by some other file. The most basic evidence in the mobile forensic is in the form of deleted data. It is very crucial to recover the deleted data.

Hidden data-Hidden data is a data which was not visible before rooting. Even WhatsApp messages are not secure and saved from various attacks by cyber criminals.

WhatsApp databases always have a backup feature associated with WhatsApp. WhatsApp databases are located on the WhatsApp folder which is created on the device. These databases can be used to extract WhatsApp chats and these are SQLite3 databases. Location for the database is, /sdcard/WhatsApp/Databases

The database only is not sufficient to retrieve tha chats of WhatsApp without the application available on the device. We need a key file to encrypt the database, which is vital. Key file can't be seen in the database folder on the device. It can be seen only if the mobile device is rooted. Key file is basically an encryption key which is used to decrypt the databases, means we can open the chats. The location of this key file is, /data/data/com. WhatsApp/files/key

With the use of this key, we can any type of chats on Whats app.

e) Recovery of data

Once classification is complete, the toolkit will also be able to recover deleted files if found in the internal memory of mobile device. Toolkit is a powerful data recovery to recover lost or deleted data. Every android mobile phone in the market is provided three storage means, that includes SIM card, internal memory and external memory. Even data

is deleted from external memory; it is stored in internal memory.

f) Analysis of data and report generation

The final step in mobile forensic investigation is the analysis of data, which is performed to find out which part of data is required as evidence and is stored for further investigation. The analysis if large volumes of data is performed in separate database system run by analysis team. The analysis focuses more often on the content of the data, than on the database in which is contained, once data analysis is completed, investigator can generate a detailed report with the findings of the investigation. This report can be presented in actual trial of the case where the court examines the report. The report will include notes taken by the specialist in charge of the particular case, details of the hardware examined, the procedures and software used in the examination and any evidence or findings found.

4. Result and Discussion

Algorithm:

1) Root the device. (it is the process of allowing the investigator to attain privileged control over various android subsystems.
2) Unlock Bootloader of Mobile Phone (only if Locked).
3) Install mobile drivers from the respective website. Download and Install Minimal ADB and Fastboot Tool).
4) Download the Latest Super SU zip file.
5) Installing TWRP in the mobile device.
6) Generate the image of the device.
7) Transfer the image from Device to PC

Steps for the execution of mobile forensics and the toolkit:

a) Root the device

Rooting basically grants you handling of core permissions of your device which lets you customize it as per your wish. In proposed mobile forensic tool, we root and use Moto G 2nd generation device running on Android OS version 6.0. However, the rooting process may be different for different types of devices. It may vary depending on the device in consideration as well as the Android OS running the device. Following are the steps for rooting a device:

b) Unlock Bootloader of Mobile Phone (only if Locked)

The bootloader of our Moto G 2nd Generation device was locked. It has to be unlocked. One has to unlock device using Bootloader which gives all developer rights to access the mobile phone. The following figure explains how mobile phone can be unlocked.

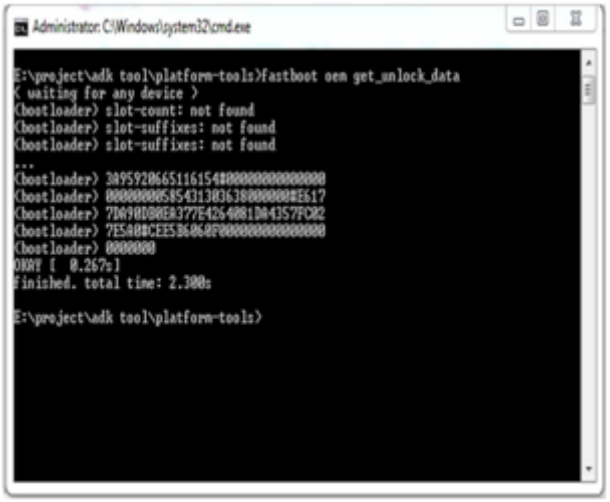

Figure 2: Code to unlock bootloader

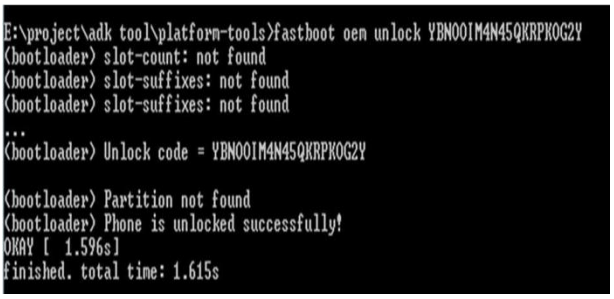

Figure 3: Unlock the device

1) **Install mobile drivers**
   You have to install mobile drivers of their respective mobile phones from the respective websites.
2) **Download and Install Minimal ADB and Fastboot Tool**
   ADB and Fastboot are one of the most important tools used when working with Android devices. It acts as a facilitator which allows you to push, modify, debug, and tweak system files very easily. It plays the role of a middle man.
3) **Download the Latest Super SU zip file.**
   In this step, root permissions for application is allowed.
4) **Installing TWRP in the mobile device:**
   TWRP gives access to all the features that one would expect from any custom recovery.
5) **Rooting MOTOROLA Moto G 2nd Gen**

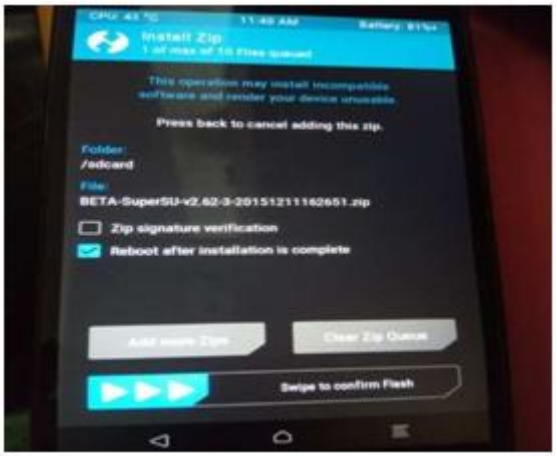

Figure 4: Flashing the SuperSu. zip file

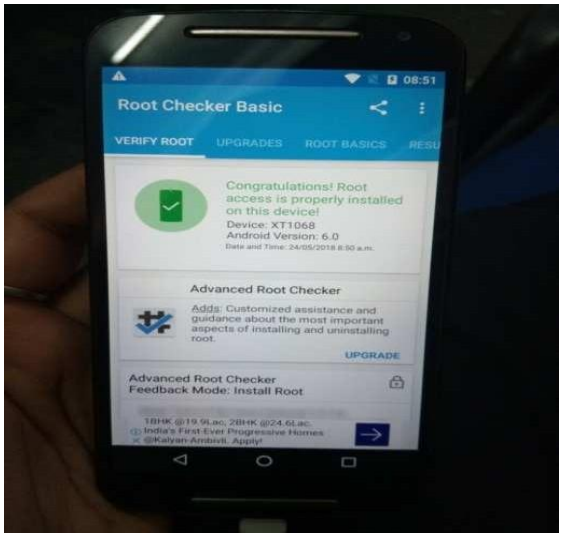

Figure 5: Successfully rooted the device

c) Acquisition phase-Create the image of the device

Once the device is rooted successfully, you can create the image of mobile device. The created image of device must be secured as it contains all the required data. Created image need to be transferred from mobile device to PC. The following figure shows how connection can be done between mobile device and PC.

```
root@osprey_ud2:/ # dd if=/dev/block/mmcblk0 | busybox nc -l -p 8888
30777344+0 records in
30777344+0 records out
15758000128 bytes transferred in 37852.774 secs (416297 bytes/sec)
root@osprey_ud2:/ #
```

Figure 6: Transferring image from Device to PC

Once the transferring of image on PC is done, extraction of data can be performed. The data collected by this method then can be classified according to messages, images, videos, contacts, hidden data. Once the classification is completed a report can be generated which helps for investigation.

Acknowledgment

This paper would not have come into reality without the able guidance, support and wishes of all those who stand by me in the development. I wish to give my special thanks to my guide, **Dr. Prashant Nitnaware**, for his timely advice and guidance.

I would like to thank our Principal, **Dr. Sandeep Joshi** for his constant encouragement throughout the course. I humbly thank our M. E Coordinator, **Dr. Prashant Nitnaware** and our Head of Department, **Dr. Sharvari Govilkar**, for their valuable guidance & unending support despite a very busy work schedule. The cheerful spirit they radiated all the time fueled our desire to excel in the work that I had undertaken.

I acknowledge all the staff members of the department of Computer Engineering for their help and suggestions during various phases of this project work. It's difficult to forget my eminent supporters that are my Friends and Family members who are always there encouraging me in my every deed.

References

[1] Rob Witteman, Arjen Meijer, M-T Kechadi, Nhien-An Le-Khac, 2016, "Toward a new tool to extract the Evidence from a Memory Card of Mobile phones", 4th International Symposium on Digital Forencis and Security (ISDFS'6), IEEE.
[2] D. Hamdi, F, Iqbal, T. Baker, B, Shah, 2016, "Multimedia File Signature Analysis for Smartphone Forensics", 9th International Conference on Development in eSystems Engineering, IEEE.
[3] Walter. T. Mambodza, NagoorMeeran A. R, 2015, "Android Mobile Forencis Analyzer for Stegano data", International Conference on Circuit, Power and Computing Technologies [ICCPCT], IEEE.
[4] Nihar Ranjan Joy, Anshul Kanchan Khanna, Leesha Aneja, 2016, "Android Phone Forensic: Tools And Techniques", International Conference on computing, Communication and Automation (ICCCA2016), IEEE.
[5] Venkateswara Rao V., A. S. N. Chakravarthy, November 2016, "Survey on Android Forensic Tools and Methodologies", International Journal of Computer Applications.
[6] Ritika Lohiya, Priya John, Pooja Shah, May 2015, "Survey on Mobile Forensics", International Journal of Computer Application.
[7] Lutta Pantaleon, Mohamed Hassan, 2017, "An Investigation into the Imapact of Rooting Android Deviceon User Data Integrity", 7th IEEE International Conference on Emerging Security Technologies, IEEE.
[8] Radhika Padmanabhan, Karen Lobo, Mrunali Ghelani, Dhanika Sujan and Mahesh Shirole, 2016, "Comparative Analysis of Commercial and Open Source Mobile Device Forensic Tools", IEEE.
[9] http: //resources. infosecinstitute. com/category/computerforensics
[10] /introduction/mobile-forensics/the-mobile-forensics-process-steps-types/#gref
[11] https: //hub. packtpub. com/introduction-mobile-forensics/
[12] https: //testdisk. en. softonic. com/