DESIGN AND IMPLEMENTATION OF MOBENSIC TOOL TO AID MOBILE FORENSICS

Shahana Shamim[1], Sumit Sharma[2], Queeny Priyangel Srivastava[3], Shivani Thakare[4], Madhumita Chatterjee[5]
Computer Engineering, Pillai College of Engineering, Mumbai, India

Abstract
Mobile phones have become an integral part of our daily lives. Today it is difficult to think of a life without a mobile phone because it is not only a phone but also a calculator, camera, computer, email, a storehouse of information, PlayStation and a music system too. But the advancement of mobile has led to a subsequent increase in the rate of cyber crimes through mobiles. Mobile forensics is used to detect and analyze any malicious activity that might have been performed using the device. Our objective is to help reduce the criminal activities by creating a toolkit to aid mobile forensics for android devices. Currently, there is no single compiled tool available to perform mobile forensics, hence we propose to design a toolkit for the same. The process of mobile forensics includes three major steps, image acquisition, data extraction and data analysis. The toolkit will help to create an image of the entire device, extract deleted and hidden files and perform analysis of video, audio and multimedia files.
Keywords: Android Live Imaging, Android Debug Bridge, Kali Linux, Mobile Forensics, Rooting, Forensic Toolkit Imager, Autopsy.

I. INTRODUCTION

Digital Forensics is the process of uncovering and interpreting electronic data. The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying and validating the digital information for the purpose of reconstructing past events.
The context is most often for usage of data in a court of law, though digital forensics can be used in other instances.
The term "forensics" implies that digital forensics is used to recover evidence to be used in the court of law against some offender. This is very useful to detect corporate frauds, perhaps an employee stole a valuable data or even for the analysis of mobiles recovered at a crime site. The contents of the device, like chats, images etc. can be used to provide evidence against such crimes.

Mobile forensics is a branch of digital forensics which deals with the recovery of digital evidence or data from a mobile device under forensically sound conditions. The use of mobile phones/devices in crime has widely increased for few years, but the forensic study of mobile devices is a new field, from the early 2000s. There are various challenges that are faced while recovering data from mobile due to many reasons. To remain competitive the manufacturers change the original equipment file structures, data storage etc. and hence forensics examiner has to find out alternative ways than used in computer forensics. The storage capacity of devices grows continuously. These are some of the challenges faced in mobile forensics.

Kali Linux is a Debian-derived Open Source L inux distribution designed for digital forensics and p enetration testing. It is maintained and funded by O ffensive Security Ltd. Kali has more than 600 penetration testing tools along with multi-language support. The Kali Linux operating system is completely customizable all the way down to the kernel and is developed in a secure environment. It is specifically tailored to the needs of penetration testing professionals, thus providing a secure environment to carry out various forensic activities.

Android is a mobile-based operating system developed and maintained by Google. It is based on modified version of the Linux operating system and other open source software. Android is available for devices such as smartphones and tablets. Google has also developed Android TV for television and Android Wear for wrist watches. There are various versions of Android available ranging from earliest Gingerbread (2.3) to the latest Oreo (8.0).

II. LITERATURE SURVEY

In paper[1] The Author gives us a tool to extract data from memory card and analysis of WhatsApp application installed on the memory card from different models of mobile phone. There are many mobile forensics tools that can retrieve information from both internal and external memory. Because of the complexity of using different forensics tools and processing time, there is a requirement of one tool that automates the process. The methods followed are File Extraction, File Recovering, File Converting and Decrypting and Reporting and GUI.

In File Extraction, the input to the tool is disk image file and OS relevant file categories will be extracted like pictures, video, audio, and documents.

In File Recovering process the deleted files are extracted and recovered files are sorted in various categories.

In File Converting and Decrypting the audio, video, thumb files containing pictures and additional information and WhatsApp databases are decrypted into a readable format. The last method which is Reporting and GUI offer UI and final report to the investigator.

In paper[2] the author proposes a solution to the anti-forensic technique of steganography by designing and developing an application that will detect the presence of stegno data within the Android device and then perform logical data acquisition of images, audio, and videos. The application proposed by the author that is Mobile forensic Analyser is developed with the hash function and buttons like extract and report. The analysis of stegno data will be in png, mp3, mp4. The tool is also used for detecting hidden data on an image, audio, video. It maintains the integrity of data by using strong tools like hash.

The authors of the paper[3] have proposed file signature analysis which is used to detect if the file extension has tampered or not. The two methods used by them are multimedia file signature acquisition in which they have extracted and compared multimedia file signature of different mobile phones using hex editor, whereas in second method that contents inspection there are two steps the first step is similar to the above and the second step is to compare content and metadata of original and amended multimedia files in order to detect changes. The results obtained by the authors after smartphone multimedia file signature analysis on camera images examined has a file extension .jpg. The camera videos file extension observed are .mp4 (Samsung, Blackberry, Lenovo, Nokia) and .mov. The audio file extensions examined are .wav(Samsung, Nokia), m4a(iPhone) and .amr(Blackberry and Lenovo). The results obtained after content examination for camera images/videos/audio contains metadata which has information such as a timestamp(creation time and date) and company name (manufacturer name, device name, OS).

The content examination of application video obtained multimedia files extracted from WhatsApp have different file extension such as .jpg, .mp4, .mov etc.

III. EXISTING SYSTEM

Mobile forensic is a vast field with a lot of exploration that needs to be performed. The number of mobile phones keeps on increasing day by day with newer versions of a certain phone being released biannually. This has led to an increase of data being produced in a day, this has, in turn, led to increasing of cybercrime at an alarming rate ultimately resulting in a high demand for a complete mobile forensic tool. Currently, there are some tools available for performing image creation process like FTK Imager and for analysis of the created image like Autopsy.

FTK Imager is a Forensic Toolkit Imager w hich is distributed by AccessData used for forensic imaging. It is a commercial software package. FTK Imager is often used for creating images of disks and portable devices**.** T his image is stored as a single file or as segments that may later be reconstructed to obtain the full disk image. It offers MD5 hash calculation and hence confirms the integrity of the data. The resulting image file can be saved in several formats including the DD raw format.

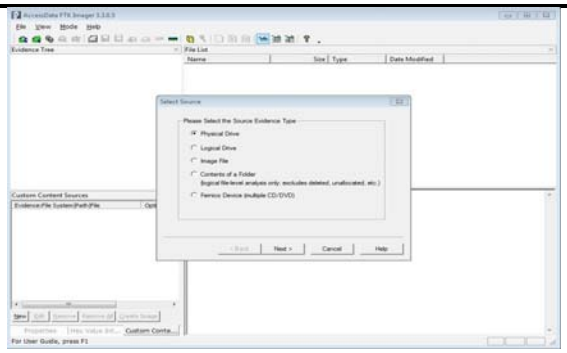

Fig. 1. Forensic toolkit Imager.

An autopsy is a computer software that is used for the forensic analysis process, making it easier for the investigators to carry out their analysis in a secure and efficient manner. This tool is designed with three principles in mind: extensible, framework and ease of use. Extensibility states that the user should be able to add new functionality that can analyze the underlying data source. Frameworks offer standard approaches for investigation, analysis, and reporting. Ease of use makes it easier for users to repeat their steps without reconfiguration.

To initiate the process of analysis we provide the image of the concerned device to the tool in formats such as dd, raw etc. The autopsy software then begins the analysis process, segregating the files on the image into various suitable formats such as documents, multimedia, deleted as well as emails etc. The autopsy GUI provides a simple way to access, analyze and extract the files that are required by the forensic expert.

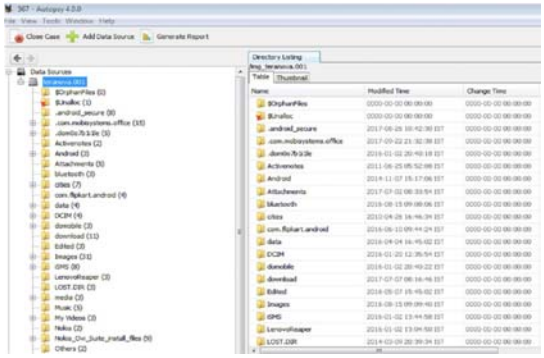

Fig. 2. Autopsy.

Thus we observe that even when we have such tools available for forensic analysis in the market, these do not provide a complete tool to carry out the process of forensic analysis. Each tool provides the functionality to perform one part of the complete task. Hence we propose a complete mobile forensic analysis toolkit called as **Mobensic**. This will help us in performing the various tasks of image creation and data analysis in one platform itself.

IV. PROPOSED SYSTEM

As we have observed that from the existing tools available for mobile forensics the procedure to get all the usable information from the internal memory of the mobile phone is a time-consuming process. There is a need for developing a single tool that simplifies the forensic process. So we propose to design a single toolkit to aid mobile forensics and simplify the investigation of internal memory of the mobile phone. The important thing is that with the help of new toolkit digital investigators can start with the investigation without searching all kinds of tools. Proposed tool will be user-friendly, simple and time-saving. The Mobensic tool works in the Kali Linux environment. The entire process from image creation to the analysis and report generation will be provided by a single tool which will make the process of collecting evidence from the mobile phone much easier.

Figure (a), gives the architecture of our proposed **Mobensic Tool.** It includes the process of creating an image of the mobile device, extracting the required data from the created image and finally performing analysis on the data extracted. Once the data analysis is completed, a detailed report of the entire forensic process is generated for the expert to view.

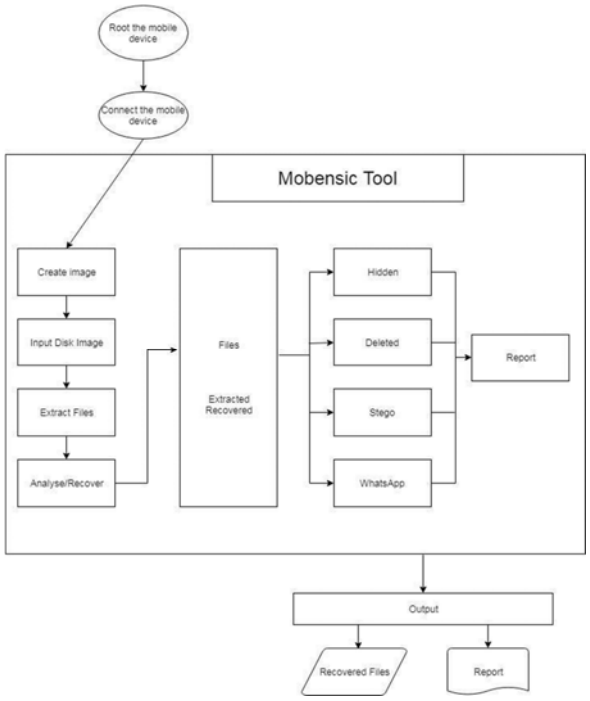

Fig. 1. The architecture of Proposed System.

1. Rooting the device:

The process of rooting allows the user of smartphones, tablets and other devices running on the Android operating system to gain root access to the android subsystems. The Android operating system uses the Linux kernel and hence rooting gives similar administrative permissions as on Linux or any other Unix like operating system.

For the designing of Mobensic toolkit, a Moto G 3rd Generation device running on Android OS version 6.0.1 was used. For the Moto G 3rd generation device, first, unlock the bootloader on the device(if locked) and install the necessary device drivers. Next, install ADB and Fastboot tools along with the latest version of SuperuserSu and TWRP manager.Now make use of the necessary drivers and tools to root the device and attain administrative(Superuser) access.

However, the rooting process may not be the same for each and every device. It may vary depending on the device in consideration as well as the Android OS running on the device.

2. Image creation

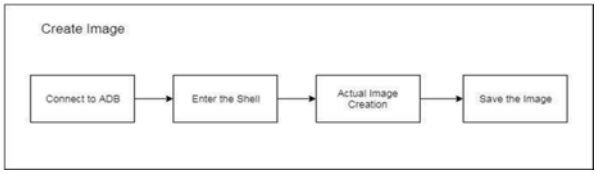

Fig. 2. Internal working of Image creation.

Figure 2, further elaborates the image creation module from the proposed architecture. To create an image of the mobile device, very first step is to activate the write blocker function. Write blocker is a function that will disable all the write access rights on the device, making sure that the device and its contents have not been tampered with. A write blocker will help the forensic expert to prove that the device and its contents have not been manipulated, which is a very important aspect in the court of law to use a mobile device as a proof. After write blocker has been activated, the forensic expert now connects the device to the toolkit using Android Debug Bridge (ADB). The user now enters the ADB Shell. In the shell, perform the actual function of creating the image using Android live Imaging process. This process creates a complete image of the internal memory of the device. The image is then saved for further analysis.

3. Data extraction

Once the image of the entire device has been created, move towards extraction of data from the image. The data extracted is stored in a folder format for easy retrieval and analysis. Mobensic tool will be able to extract the hidden files from, stegno data files, deleted files and also the WhatsApp conversation details from the device.

4. *D ata analysis and Reporting*

After performing the action of data extraction, the expert will need to analyze the data extracted. This will be done in the data analysis and the reporting module of the tool. The forensic expert will be able to classify and analyze the data into different formats like Whats App data, stegno data, multimedia files, and Documents.
The toolkit will further also generate a report on the data that is extracted and classified.

V. RESULTS ACHIEVED

In this section, we deploy our Mobensic tool for analysis and testing. It is difficult to build one tool that can perform all Forensic process as mentioned in section III. This Mobensic tool can simplify the process by integrating all Forensic steps in one single tool.In this section, we test Mobensic tool by analyzing internal memory of mobile devices.

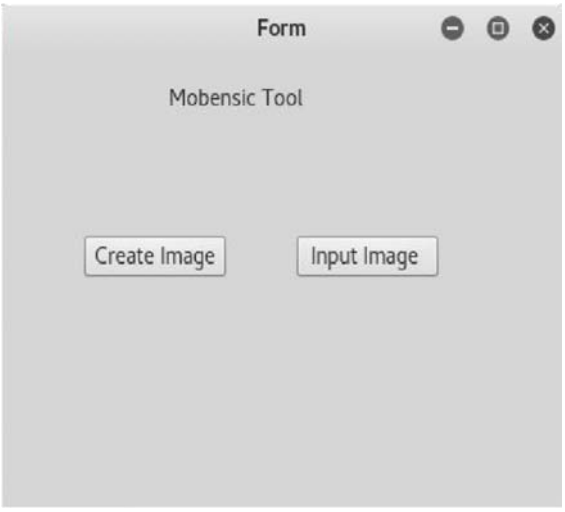

Fig. 1. GUI for Mobensic Tool.

The toolkit provides two options one is to create an image of the internal memory of the mobile device or to directly input the image of the mobile device. In creating image option the image of the mobile device connected is created and stored on your machine whereas in input image option the image of the device is loaded for further analysis.

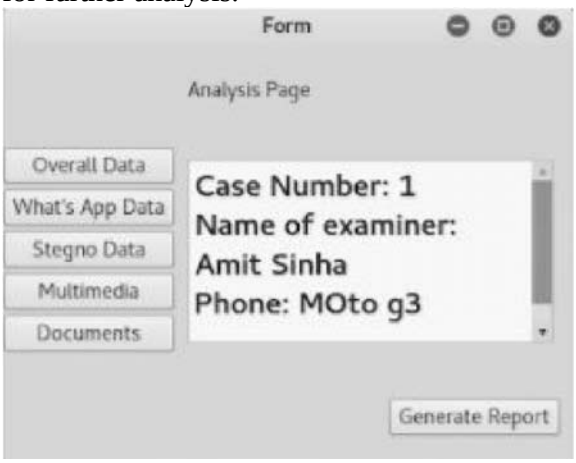

Fig. 2. Analysis screen for Mobensic Tool.

The figure 2 above shows the analysis screen where the input image is analyzed and the data which is recorded is classified as Whatsapp data, Stegno data, Multimedia, Documents. The toolkit also provides a report generation option for a summary of all the extracted data. Now from this, the user can click on any of the options to view and analyze the various data extracted.

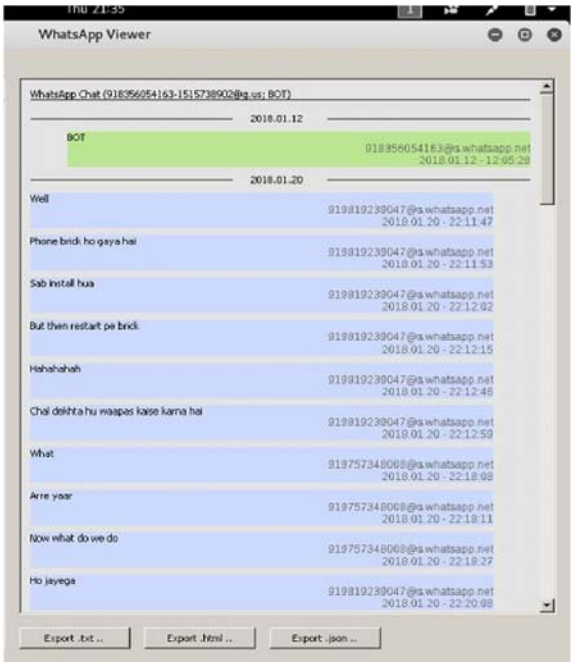

Fig. 3.Whatsapp Viewer.

The above figure 3 shows Whatsapp Viewer which display the Whatsapp chats which were recovered during the analysis phase. When the user clicks on "WhatsApp data" option the conversations stored in the mobile device are displayed to the user.

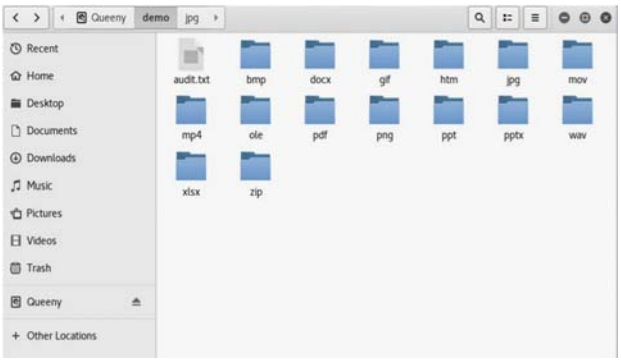

Fig. 4.Data Recovered

Figure 4 above shows the classification output in the extraction of the data from the image of the device. Once the user clicks on the "Overall data" option, the tool gives a complete view of the various sub-folders containing data like jpg files, png files, pdf files, text files etc. which have been recovered in the extraction module.

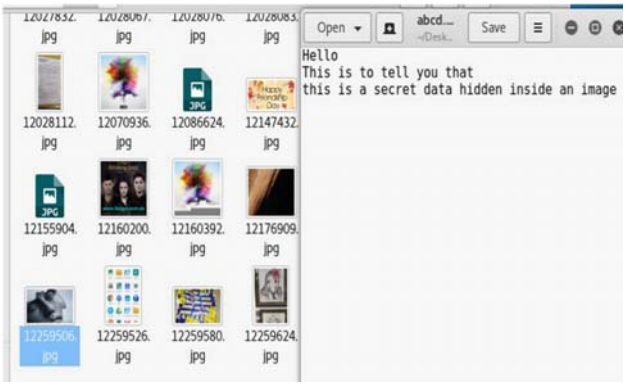

Fig. 5.Stegno Image.

The figure 5 above depicts an example of the stegno image that has been extracted using the Mobensic tool. When the user clicks on “Stegno data” option, the stegno image stored in the mobile device along with its hidden text is recovered by the tool and displayed to the expert.

VI. CONCLUSION

In the past decade, advancement in technology has made us more and more dependent on our mobile devices for day to day activities. This in turn has led to an increase in the number of frauds and malicious activities being performed with the help of the mobile phones. A tool like ours

can help in analyzing the matter and further reach conclusions. Mobensic tool can be used in a vast frame of applications like,

- Military intelligence
- Corporate investigations
- Private investigations
- Criminal and civil defense
- Electronic discovery

In future, the Mobensic tool can be further be enhanced to extract and analyze Call Logs, Contact Information, text messages, and Email. Further, the toolkit can also be available for other operating systems like iOS. The rooting process can also be incorporated into the toolkit, making the process even easier for the forensic expert.

VII. ACKNOWLEDGMENT

We would like to take this opportunity to express our profound gratitude and deep regard to Prof. Dr. Madhumita Chatterjee for her guidance and constant encouragement throughout the course of this project. We are immensely obliged for her cordial support, supervision and providing necessary information.

We remain immensely obliged to Dr. Madhumita Chatterjee for introducing this topic, and for her invaluable support in garnering resources for us either by way of information or computers also her guidance and supervision which made this project happen. We are thankful to our college, Pillai College of Engineering for providing us healthy competitive environment and outstanding educational facilities that played an important role in keeping us highly motivated to achieve our goals.

VIII. REFERENCES

[1] Rob Witteman, Arjen Meijer, T oward a new Tool to Extract the Evidence from a Memory Card of Mobile Phones, 2016, School of Computer Science, University of Dublin, Ireland

[2] Walter T. Mambodza, Nagoor Meeran A.R, A ndroid Mobile Forensic Analyzer for Stegno Data, 2015, Department of Information Technology, SRM University

[3] T. Baker, B. Shah, Multimedia File Signature Analysis for Smartphone Forensics, 2016, Department of Computer Science, Liverpool John Moores University, UK

[4] Neha S Thakur, Forensic Analysis of WhatsApp on Android Smartphones, 2013, Master of Science in Computer Science Information Assurance University of Pune

[5] Mark Lohrum, Live imaging an Android device, 2014, http://freeandroidforensics.blogspot.in/2014/08/live-imagi ng-android-device.html

[6] Qt Designer, Qt Designer Manual (Documentation Archives) http://doc.qt.io/archives/qt-4.8/designer-manual. html

[7] Ajinkya, How to install TWRP and root Motorola Moto G 3rd Gen(2015) https://devsjournal.com/how- to- install-twrp -root-motorola-moto-g-3rd-gen.html

[8] Ajinkya, How to easily unlock bootloader in Moto G 3rd Gen(2015) https://devsjournal.com/how-to-easily-unlockbootloader-in-moto-g-3rd-gen-2015.html

[9] Satish Bommisetty, Rohit Tamma, Heather Mahalik, Practical Mobile Forensics , 1st ed, 2014, Livery Place, 35 Livery Street, Birmingham B3 2PB, UK

[10] Kevin Mandia, Chris Prosise, Matt Pepe, Incident Response and Computer Forensics, 2nd ed, 2014, McGraw-Hill, Inc. New York

[11] Andrew Hogg, Android Forensics Investigation, Analysis and Mobile Security for Google Android, 1st ed, 2011,Oak Park Illinois,USA