DATA EXTRACTION AND ANALYSIS OF ANDROID MOBILE DEVICE: A REVIEW

[1]Nibedita Chakraborty, [2]Dr Ravi K Sheth, [3]Dr Sunil B Mane
[1]Student Master in Technology Cyber Security, [2]Assistant Professor Raksha Shakti University, [3]Associate Professor COEP
[1]Department of Information Technology and Telecommunication.
[1]Raksha Shakti University, Ahmedabad, India

Abstract: Nowadays Mobile phones have become the heartbeat for all human being. As the technology is growing up, people utilize the mobile phone as their portable computer where they can interact with others, share & exchange their unique ideas, information, images and videos at a very high speed. The exponential growth of mobile users worldwide adds to its challenge against security breach and keeping a check on cyber related crime activities. In today's era digital medium can be used extensively communicate through SMS, emails to form a network so that illegal activities can be formulated. Therefore there are various commercial as well as open source tools available in the market to extract and analysis of data from various mobile devices. This paper review that if the display of the android device is cracked or no longer approachable the touch screen that time it is little bit problematic to extract the data though the tools having individual drawbacks. So, there should be a proper framework which can combines all the tools together and prepare a combined solution for the drawbacks and make the forensic investigation efficient and smooth.

Keywords- Mobile Device, Extraction, Evidence, Acquisitions, Mobile Forensics, Damaged mobile device.

I. INTRODUCTION

Nowadays mobile phone becomes a necessity to the maximum people. Mobile phones have become the heartbeat for all human being. Without access to cell phone our lives become a nightmare. The access to cell phone has become part and parcel of us. As the technology is growing up, people utilize the mobile phone as their portable computer where they can interact with others, share & exchange their unique ideas, information, images and videos at a very high speed. Technology is growing gradually and people cannot imagine a life without it. In the past decennary, mobile phone has grown exponentially and increased its virtual presence by getting people hooked into its world. In simple devices People can only dial and accept calls and back & forth messages. But in Smart devices people also have the provision to avail the internet with the above two amenity. Mobile phones is among the marvelous inventions that mankind has gifted to its own kind. This spectacular technology has made one's life easy and comforting. But one should be cautious enough as to not to use that in bad light as because the consequences may get us into trouble. Fraud and prank calls are very common now-a-days which not only makes us lose our valuable time but also brings about mental anxieties. The female sections of our society are the prime targets in most of cases. Many victims approach mobile operators seeking help but the responses are very generic in nature, which include suggestions to block calls or avoid taking unknown calls. Many people have even alleged that mobile operators are in monetary engagements with such groups. Nevertheless, it is to be pointed out here that the lack of action from the operator's side to tackle such occurrences is not appreciable at all. Mobile phones today have become easy prone to software threats globally. This in turn has made the tasks of forensic science quite daunting. Nowadays Smartphone such as Apple iPhone, Samsung Galaxy Series are a packed form of personal computers which offers top performance, vast storage capacity, and other facilities. Mobile phones are the most movable device which can hold machine readable data in a disk and keep an eye on every movement of the user. In 2010, Mobile call records and GPS information are the vital evidence for the investigation of Terrorist attack in Times Square, New York. The exponential growth of mobile users worldwide adds to its challenge against security breach and keeping a check on cyber related crime activities. In today's era digital medium can be used extensively communicate through SMS, emails to form a network so that illegal activities can be formulated. Technological advancement and development in the discipline of information technology and communication has left open variety of software applications each working on its own operating system, programming logics, system and kernel architectures which complicates the task of digital forensic specialists to examine the evidences that may be reserved in a digital device. To make things more complex each mobile manufacturer has their own proprietary technology and formats which are time consuming to break through. The forensic tools that are available today are not sufficient enough to examine and analysis devices which are subjected to regular updates and changes. Nowadays mobile device forensic is very important domain in Digital forensic only because this portable device may contain miscellaneous data about the crime scene, which is very crucial for the inspection. Before investing any damaged mobile device, forensic investigators should aware about the architecture of the mobile device. Mobile phones have three segments as baseband is characteristics into two functions that are analog and Digital.

II. BACKGROUND

Mobile forensics is a part of digital forensics of retrieving and examining data from a portable phone or personal digital assistant which are forensically accepted. The study which supports to retrieve binary proof from a mobile device is known as Mobile Forensics. Mobile phone forensic investigation includes one of two methods which generally performed by the analyzer: Manual and Automatic data extraction. Compatibility with additional pieces of forensic software can help us to achieve automatic extractions from devices. Manual extraction is needed when no compatible software is present. Mobile forensic technique is classified into five steps: seizure, acquisition, identification, evaluation, presentation.

Forensic investigators handle some opposition while seizing the mobile phone as an origin of proof. At the scene of offence, if the mobile phone is found disconnect the investigator should put the gadget in a faraday bag to stop distortion should the device automatically turned on. Faraday bags are specially constructed to detach the device from the network. If the phone is found turned on, turning it off has a lot of concerns hook up to it. If the device is sealed by a PIN or password or encrypted code, the investigator will be needed to detour the clamp or regulate the PIN to enter to the device. Mobile devices are inter-connected devices and can back and forth the information via various mediums, such as telecommunication systems, Wi-Fi access points, and Bluetooth. Therefore if the mobile phone is in the operational state, a lawbreaker can securely delete the information reserved on the mobile phone by performing a remote wipe command. When a device is turned on, it is need to put in a faraday bag. If manageable, prior to putting the mobile phone in the faraday bag, detached it from the network to preserve the digital proof by turning on the flight mode and turning off all network connections (Wi-Fi, GPS, Hotspots, and so on). Once the mobile phone is captured properly, the investigators may use various forensic tools to gain and evaluate the information preserved on the mobile phone.

III. RELATED WORKS

In [1], the authors did a detailed study of different procedures in which smartphones data could be taken out and examined using the sleuth kit autopsy. They applied these tools to get email, contact details, messages, images, call logs and calendar types of data which could be deploy for digital evidence in investigation. Tools used in this paper are either freeware or trial versions. Before extracting and recovery of files we need to have idea regarding the mobile architecture, computer forensics process and different tools used.

In [2], the authors explain two types of acquisition i.e. logical acquisition and physical acquisition by using different forensics tools obtainable in the market and shown the comparing results of these acquisition methods on three different smartphones. They also explained how the different smartphone forensics tools are working and by using this tools how we can take out details from the smartphones. After this research, new and latest functionality as well as limitations of the mobile forensics tools were identified.

In [3], the authors discovered a one way method to analyse the android smartphone. The main target to apply this method is to collect data like video, messages, audio, images etc. the proposed model consists of three steps: seizure (it should be done in front of experienced forensics experts to present the evidence in the court of law) , first analysis (initial extraction step before the phone is seized), data extraction(sending the seized device to the forensics lab and applying different tools to extract data from the device).

In [4], the authors described an open source toolkit which will be helpful for forensics analysis purpose and also can extract the data very quickly and accurately. The advantages of this toolkit are described by the author in this paper. With the help of this toolkit, investigators can also identify about the criminal connections publicly attached with the crime happen. This toolkit can be used to extract data like call logs, Facebook, twitter, Whatsapp data, contact numbers etc.

In [5], the authors are using Cellebrite UFED to extract data from mobile phones through physical acquisition including deleted data. But this research is limited to Samsung Galaxy Note III with Android OS and the system should be in charging mode. The new advantage of using this tool described is to extract data regarding Geographical data of the video, image and text messages so that we can identify when and where the user was located when he/she updated his/her status that will be useful for present the evidence in the court.

In [6], the authors described how criminals use cell phones to accomplish their mission. So it becomes more challenging to extract data from that. There are overall five steps to proceed the forensic over a cell phone: Preservation, Acquisition, Examination, Analysis and Reporting. In this paper they describe the step wise process of doing the mobile forensics and put the focal point on the fault finding of Acquisition and Preservation from a cell phone which can be used as documentation in future cases. It also reports how to deal with this above said two processes. They deliberate about different affair which may arise during accomplish them.

IV. PROPOSED WORK

For the last few years we have successfully extracted data from various mobile devices, such as cell phones, smartphones, tablets, etc. There are various ways through which anyone can extract and analyse data whether it’s deleted or SIM is not available from a smartphone using various commercial tools like UFED, MOBILedit, Oxygen PM etc. Among devices to be examined, some defective mobile devices whether it is in live or dead condition(damaged mechanically, by fire or water) are also come from which digital evidence should also be extracted. The main problem is that how we can extract data from a damaged (live or dead) system when the display is broken and the system is in charging mode. As per the literature survey which we have observed, there are lots of open source and proprietary Mobile Forensics tools available in the market. With the help of these tools Experts can extract data, analysed data and acquisition of the seized. However the seized mobile can be in functional or non-functional condition. As discussed in the above that when a mobile device is seized, forensic experts facing some problems regarding the broken display of the device as the data is not visible in that as well as every forensic tool are having some restrictions on extraction of data. So there should be a framework which will be proposed to get combined outcomes from different tools, which will help Forensic investigator to solve the case efficiently as every commercial as well as open source tools are having individual drawback

V. FUTURE WORK AND CONCLUTION

Forensic examination of damaged mobile phones and computing devices is a growing subject area in computer forensics. Mobile phone forensic tools are a relatively recent development and in the early stages of maturity. Forensic examination tools translate data to a format and structure that is understandable by the examiner and can be effectively used to identify and recover evidence for civil and criminal litigation. It is possible that some forensic tools may contain a degree of inaccuracies, requiring the examiner to employ several tools to verify the accuracy of the examination. The tool may contain a software programming error generated by the mobile device as input may be incorrect, causing the tool to function improperly. In addition, a suspect may tamper with device information to foil the workings of a tool or apply a wiping tool to remove or eliminate data. Over time, experience with a tool provides an understanding of its limitations. New versions of these forensic tools are expected to improve and provide a higher quality result for investigative requirements. There are number of mobile phone forensic tool available in the commercial market. All of these tools provide some level of evidence identification and retrieval from the damaged mobile phone. Note that GSM mobile phones are logically and physically partitioned into handset and SIM , resulting in some forensic tools that deal exclusively with SIM. .XRY, MOBILedit! Forensic tool supports internal and external SIM access. But Oxygen PM supports only internal SIM acquisition. During extraction any data from mobile phones investigator should know the advanced features and limitations of the usable tools and the available tools in the commercial market. It is better to use different tools for performing the examination so that each and every data can be extracted. And from the above framework we can assume the advanced and new features as well as limitations of mobile forensic tools while extracting different data from a damaged device.

REFERENCES

[1] Normaziah A. Aziz, Fakhrulrazi Mokti, Mohd Nadhar M.Nozri, Mobile Device Forensics: Extracting and Analysing Data from an Android-based Smartphone, 2015 Fourth International Conference on Cyber
Security, cyber warfare, and Digital forensics.
[2] 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.
[3] Santos MRP, Alves TF, Neto RPC, Forensic Simplified Methodology for Android Data Extraction, 2016 International Journal of Advanced Research in Computer Science and Software Engineering.
[4] Patrick Dibb and Mohammad Hammoudeh, Forensic Data Recovery from Android OS Devices: An Open Source Toolkit, 2013 European Intelligence and Security Informatics Conference.
[5] Taniza Binti Tajuddin , Azizah Abd Manaf, Forensic Investigation and Analysis on Digital Evidence Discovery through Physical Acquisition on Smartphone, World Congress on Internet Security (WorldCIS-2015).
[6] Shivankar Raghav , Asish kumar Saxena, Mobile Forensics: Guidelines and Challenges in Data Preservation and Acquisition, IEEE Student Conference on Research and Development 2009.