International Journal of Computational Intelligence Research
ISSN 0973-1873 Volume 13, Number 8 (2017), pp. 1859-1869
© Research India Publications
http://www.ripublication.com

Forensics Analysis On Smart Phones Using Mobile Forensics Tools

G Maria Jones*[1] **and S Godfrey Winster***[2]

**[1] PG Scholar, *[2] Professor*
Department of Computer Science and Engineering,
Saveetha Engineering College, Chennai, Tamil Nadu, India.

Abstract

The role of mobile devices (cell phones and smart phones) becomes an integral part of everyone's life, which also leads to criminal activities like hacking, Smishing, SMS spoofing etc. Digital evidence in mobile phone has attempted to delete the data by criminal. Information from mobile phones is useful for investigators to learn about user information. In this paper, a novel method is performing a data acquisition of digital evidence from compromised device which will be useful for digital investigators and court proceedings. This data acquisition method provides better understanding to identify the criminals who misused the mobile devices for cybercrime.

Keywords: Digital evidence ; compromised device; hacking; forensics; cyber crime

I. INTRODUCTION

Digital forensics is the branch of forensics science in which we can able to reconstruct the past events by forensics tools for legal proceedings in court. Generally, digital forensics is divided into 5 major groups. They are computer forensics, mobile forensics, network forensics, forensics data analysis and database forensics. Each division in digital forensics helps to find out the criminals who have done the cyber-attacks, phishers, fraudsters etc. According to CTIA in United States, more than 6 billion text messages and 330 million multimedia messages occur each day (as of December 2013,). In 2016, Apple announced that users send an average of 200,000 messages per second [21]. Mobile phones are tiny computers which can store an immense amount of data. The continuous evolution of mobile device technology

increases everyday which leads to criminal investigations. Several digital toolkits have supported the recovery of data from mobile devices. Forensic tools are mainly to acquire mobile phone data and to generate report of the acquired data. Mobile forensic toolkits are available in the market, including Oxygen forensics, Cellebrite's Universal Forensic Extraction Device (UFED), XRY Forensic Examiner's Kit. These tools help to extract certain informative data. Like personal computers, the mobile devices has also lot of information's like SMS, MMS, audio and video. While analyzing suspected mobile devices, the potential evidences such as, location information, subscriber and equipment identifiers, date/time, language, phonebook information, call logs (Incoming, Outgoing, Deleted), text messages (Incoming/Outgoing/Deleted), MMS (Multimedia messages), video, audio Files, e-mails, web browsing activities, files are need to be checked. There are two standard extraction methods for mobile forensics analysis. They are Logical and Physical analysis. The mobile forensics challenges include; many different types of hardware and software, huge number of mobile operating systems and Security features.

Investigator can get sufficient information from their mobile devices. The significant amount of evidence is possible to retrieve by extracting, locating and analysing the mobile devices. There are three ways that the mobile devices can be linked with a crime. 1) It is used for communication Purposes 2) It also contain details of a victim 3) Extracting of data can be done. Social networking services like Wechat used for a criminals to communicate and coordinate their criminal acts for selling illegal items, defrauding etc [2].

In case of turned-on mobile phone, it is necessary to have a faraday bag to ensure that mobile devices are not connected remotely and also to prevent from tracking the mobile device, remote wiping of data. It is necessary to prevent the digital evidence from the time of seizure until it is submitted as evidence in court. The rapid growth of developing mobile devices, there is a chance of happening crime. In order to access and retrieve older/deleted copies of data, it is necessary to use mobile forensics tools. The extractable data from devices varies from devices to other devices. It is not necessary for all devices are able to extract full device storage data. In recent years, text messages is important digital evidence in high profile cases [1].

The mobile forensics process is categorized as Seizure, Acquisition and examination/Analysis. There are some unique Challenges faced by Examiners.

1. Malicious Programs
2. Lack of availability of tools.
3. Password Recovery.
4. Accidental Reset.
5. Anti-Forensics Technique.

The rest of the paper is organized as follows. Section 2 details the related work, which give the survey of the mobile forensics. Section 3 describes the flow process of mobile forensics. Section 4 proposes methodology to reconstruct the past events using oxygen forensics tool and section 5 gives conclusion and future work.

II. RELATED WORK

Daniel and Ibrahim [1] tested 16 of 20 applications in order to reconstruct the past events of messages that could be useful to forensics examiners and also evaluated the security in sending/receiving the data. They have shown that many messaging application have vulnerabilities during storing and transmitting the data. Songyang et.al [2] explored some questions that arise during forensics examination of weChat and gives technical methods that are useful to these questions. They are 1) Acquisition of user data 2) Investigating the communication and which was shared by user. Cosimo [3] analysed the forensics artifacts in smartphone whatsapp which provide evidentiary information and also shown how to reconstruct messages and contacts from chat database.

Edington and Kishore [4] deals with cloud forensics challenges and proposed a centralised forensics server in which investigator need not to depend on Cloud Service Provider (CSP) for collecting the data for investigation purpose. Cosimo et.al [5] analysed the chatSecure which stores local copies to send and receive messages; they also decrypted the database from secret passphrase which was given by the user at initial encryption process. Finally they concluded that, by using the standardized query language (SQL) cipher deletion technique, one cannot reconstruct the data from database. Karpisek et.al [6] created a tool called command line which is used for the analysis of whatsapp protocol. They can decrypt the network traffic and provides whatsapp artifacts and also able to view messages exchanged through it. Andrew and Richard [7] analysed memory forensics of volatile memory and also described the changes that happens in Operating System Design.

Kevin et.al [8] created a data set which would be helpful for digital forensics by collected and organisation of 308 anti-forensics tools and also created an anti-forensics taxonomy for the purpose of encapsulating within the domain of anti-forensics. Hyunji et.al [9] proposed a model for forensics investigation of cloud storage service due to malicious activities in cloud service and also analysed artiacts for windows, Macintosh Computer (MAC), (iphone operating system) IOS and Android OS. Josiah and Alan [10] demonstrated forensics tools that capable of remote acquisition of data in Amazon EC2 and also shown that some of the technologies are not sufficient to produce trustworthy data and also to solve the problems in cloud forensics acquisition. Darren and Raymond [11] explored that the file contents is as same as the collected data from cloud server and also downloading files using client

software were not altered during the process of uploading, storing and downloading files by using three popular cloud storage providers like Microsoft Skydrve, Dropbox and Google Drive.

Shiek and Lalitha [12] discussed a model based on trusted third party (TTP) that helps in finding the location and IP address which are useful to trap cyber attackers with the collection of evidences which might help for investigation team. Ameer et.al [13] discussed possible solution of cloud forensics challenges with detailed process of recommended solution and also provided brief summary of forensics-as-a-service models. Ben and Raymond [14] demonstrated and discussed on cloud storage-as-a-service forensics from server and client perspective. Vassil et.al [15] developed cloud forensics tools called kumodd, kumodocs and kumofs that work with private and public services, they also provided new capabilities that cannot be achieved by examining of client side artifacts. Amna and Derar [16] Presented a forensics process as a services using BPEL which combines four phases i) Identification ii) Collection iii) Analysis iv) Results into another services called FPaaS. Edington and Kishore [17] discussed the challenges faced by the investigator during the process in which CSP collects the evidence from outside of cloud environment. Saad et.al [18] examined the challenges that are identified in current and also explored technical solution in research respective. Jason [19] introduced two perl scripts that help to retrieve the information from amazon cloud drive.

III. MOBILE FORENSICS FLOW PROCESS

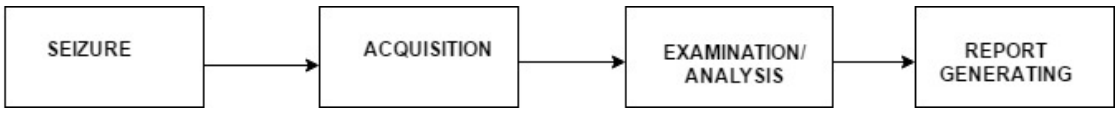

Figure 1: Basic Framework of Digital Forensics

A. Seizure

The main goal of seizing the mobile device during crime scene is to preserve the evidence. So it's necessary to seize the mobile devices on crime scene. Device seizure is an advanced forensic acquisition and analysis tool for examining mobile devices, personal digital assistants (PDA), and global positioning system (GPS) devices.

B. Acquisition

The second process in mobile forensics is acquisition and it is usually meant to retrieve the data from device. Most mobile acquisition is performed live because it is not possible to acquire the data when the power is down.

C. Examination/analysis

Different forensics tools are used to extract the data from seized devices. It is not possible to extract the all possible information so we can use two or more tools for examination.

D. Report Generating

When an investigation is finished the information is often reported in a form nontechnical. Reports may also include audit information and also i) when the examination has beginned? ii) What tools were used? iii) Status of the phone. Finally, it will be processed for a criminal court with a written expert conclusion of the evidence.

IV. MOBILE FORENSICS ANALYSIS

We can able to extract the necessary data like call logs, SMS, MMS, E-mails, Photos, Videos, audio files, Geo location and various application information from fraudster mobile by using oxygen forensics. This tool has the ability to acquire data from volatile memory of the mobile devices. The following information can acquire:

- Device information
- Contacts
- Call Logs (Missed/Outgoing/Incoming Calls)
- Organizer Data (Memos/Tasks/Notes)
- SMS, MMS, E-Mails
- Photos, Videos, Audio and video files
- Deleted Data

With the help of these information's, it is easy to find out the criminals who has played the significant role by law enforcement units, Examiners and other government authorities.

1. EVENT LOGS

Event log Section contains user voice calls: dialled, received and missed calls. Forensics experts are able to find the call time, duration and remote party. Recovering deleted calls is also possible from particular mobile devices by using oxygen forensics tool.

All incoming, outing, missed Call logs placed on the mobile device will appear in this part. It is possible to view the timestamp of the event, Remote party, duration of the call, Number of the call and MD5 hash for each log. Deleted Calls from android

(Samsung Galaxy Grand II) device is displayed with blue color and noticeable by "recycle bin" icon. The call log events are helpful for the examiners, who are all related with particular crime incident.

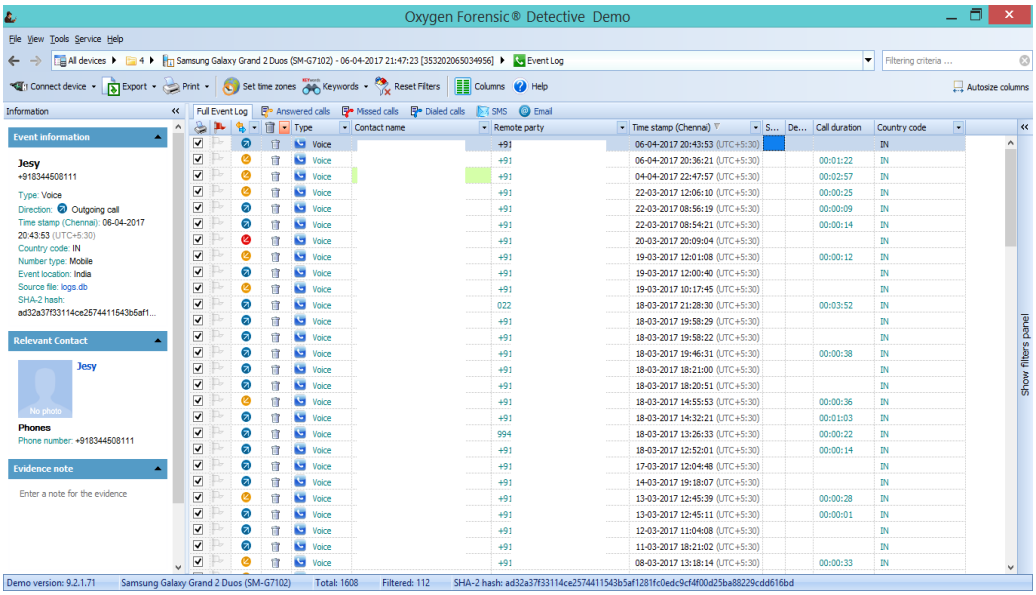

Figure 2: Display of deleted logs (Incoming, Outing, Missed Call)

2. ORGANISER DATA

It gives the information about memos, notes, and tasks etc. Some important information can be gathered from this section. We can able to view the data with data/time. SH2 hash function, Event type, start Time and end time information can be gathered from here.

3. WIFI CONNECTION, WIFI HOTSPOT

Web connections and Geo location reveals suspect visited places and routes. Examiners can analyse several sources of Geo data like Wi-Fi connections, IP connections and Locations databases. With the help of internet connection, forensic examiners are able to determine when and where suspect used Wi-Fi access (public or even private) and accessed his location. It extracts, what are the websites sited and also with possible passwords used by the user. Hotspot connection gives the certain parameters of service set identifier (SSID), basic service set identifier (BSSID), received signal strength indicator (RSSI) which gives the information about when the suspect lastly connected. It allows the examiner to view the location places where the mobile devices used.

Geo location may reveal suspect visualized places and also it determine when and where suspect enabling his location or sharing his location to others. The co-ordinates of the map show the location of the suspect. The history of Web connections and their details are shown in IP address tab: Media Access Control (MAC) and (virtual Private Network) VPN addresses, device and router IPs, (Domain Name Service) DNS name, region, time stamp, etc. Examiner can able to tract the device and find out the device owner location.

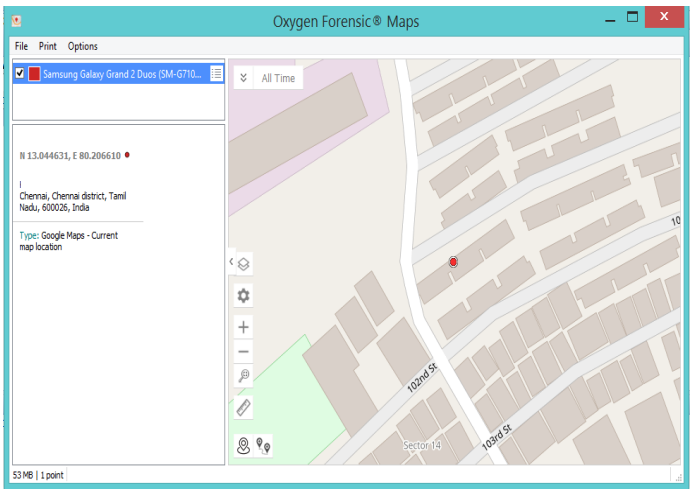

Figure 3: Geo location reveals suspect visited places and routes

4. SOCIAL GRAPH

Social graph visualizes complex connections inside crime groups. This is a highly adjustable workplace that allows forensic experts to review connections between mobile device owners and their contacts, pinpoint connections between multiple device owners, and detect their common contacts.

5. CHATLOGS FROM MOBILE DEVICES

Examiners can able to retrieve all possible data from chat logs. Depending on the mobile device the feature set may vary:

- Chat history with individuals and groups
- Contact list with photos, all fields and notes
- Sent SMS, MMS, recipient mobile number, timestamp and Country Code
- Complete calls information
- Geo-location where the action took place.

Quickly it reveals social connections between user mobile phones and their contacts. Communication statistics provides to explore social connections between device users by analysing calls, text, multimedia, e-mail messages and social messengers.

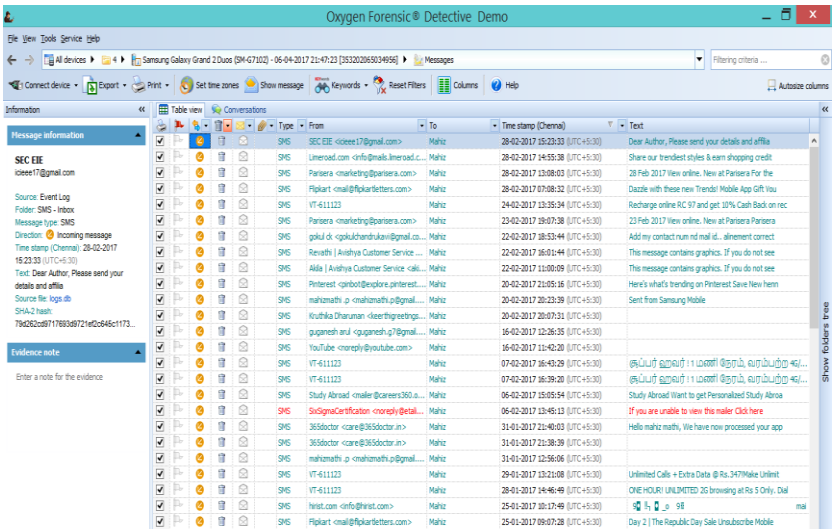

Figure 4: Displaying the deleted chat logs

TABLE 1: DEVICE DATA AND ELEMENTS ARE RECOVERED BY OXYGEN FORENSICS TOOL.

Device Data	**Data Elements**
CALL LOGS	Incoming Outgoing Missed Incoming-deleted Outgoing-deleted Missed-deleted
TEXT MESSAGES	Incoming SMS-Read Outgoing SMS-Read Incoming SMS-deleted Outgoing SMS-deleted

INTERNET DATA	History Visited Sites E-mails Bookmarks
GEO LOCATION	GPS co-ordinates
APPLICATIONS	Devices apps
SOCIAL MEDIA DATA	Facebook Instagram Whatsap

V. CONCLUSION

This paper focused on the reconstructing the past events in mobile using forensics tool. The data can be retrieved from the device, as well as backup files on personal computers and also the sent and received messages from both individuals and groups, varying message types and attachments, message, and device states, e.g., offline, online, blocked, removed, deleted which are useful for the criminal investigation. This data was then analysed by an examiner during the forensic investigation.

REFERENCES

[1] Daniel Walnycky, Ibrahim Baggili, Andrew Marrington, Jason Moore, "Network and device forensics analysis of Android Social messaging application", Digital Investigation 14(2015) S77-S84

[2] Songyang Wu, Yong Zhang, Xupeng Wang, Xiong Xiong, Lin Du, "Forensics analysis of we chat on android smartphones", Digital investigation (2017) 1-8.

[3] Cosimo Anglano, "Forensics analysis of Whatsapp Messenger on Android Smartphones", Digital Investigation 11 (2014) 201-213

[4] M.Edington Alex, R. Kishore, "forensics framework for cloud computing",

computers and Electrical Engineering (2017) 1-13

[5] Cosimo Angano*, Massimo Canonico, Marco Guazzone, "Forensics analysis of the chatsecure instant messaging application on android smartphones", Digital investigation 19 (2016) 44-59

[6] F.Karpisek, I. Baggili, F.Breitinger, "Whatsapp network forensics: Decrypting and understanding the whatsApp call signalling messages", Digital Investigation 15 (2015) 110-118

[7] Andrew Case, Golden G. Richard III, "Memory forensics: The Path forward", Digital investigation (2016) 1-11

[8] Kevin Conlan*, Ibrahi, Baggili, Frank Breitinger, "Anti-forensics: Furthering digital forensics science through a new extended, granular taxonomy" Digital investigation 18 (2016) S66-S75

[9] Hyunji Chung, Jungheum park, Sangjin Lee, Cheulhoon Kang, "Digital forensics investigation of cloud storage services", Digital investigation 9 (2012) 81-95

[10] Josiah Dykstra*, Alan T. Sherman, "Acquiring forensics evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques", Digital investigation 9 (2012) S90-S98

[11] Darren Quick*, Kim-Kwang Raymond Choo, "Forensics collection of cloud storage data: Does the act of collection result in changes to the data or its metadata?" Digital investigation 10 (2013) 266-277

[12] Sheik Khadar Ahmad Manoj*, D. Lalitha Bhaskari, "Cloud Forensics-A Framework for investigating Cyber Attacks in cloud environment", Procedia computer Science 85 (2016) 149-154

[13] Ameer Pichan*, Mihai Lazarescu, Sie Teng Soh, "Cloud Forensics: Technical Challenges, Solutions and Comparative analysis", Digital investigation 13 (2015) 38-57

[14] Ben Martini*, Kim-Kwang Raymond Choo, "Cloud Storage Forensics: owncloud as a case study" Digital investigation 10 (2013) 287-299

[15] Vassil Roussev*, Irfan Ahmed, Andres Barreto, Shane Mcculley, Vivek Shanmughan, "Cloud forensics-Tool development studies and future outlook" Digital investigation (2016) 1-17

[16] Amna Eleyan, Derar Eleyan, "Forensics Process as a Service (FPaaS) for cloud computing", 2015 European Intelligence and Security Information Confernece.

[17] M. Edington Alex, R. Kishore, "Forensics Model for cloud computing: An

Overview”

[18] Saad Alqahtany, Nathan Clarke, Steven Furnell, Christoph Reich, “Cloud Forensics: A Review of challenges, Solutions and Open problems”

[19] Jason S. Hale, “Amazon Cloud Drive forensics analysis”, Digital investigation 10 (2013) 259-265

[20] https://en.wikipedia.org/wiki/Digital_forensics

[21] http://www.bucks.edu/media/bcccmedialibrary/con-ed/itacademy/Intro ToMobileForensics.pdf