Section A-Research paper
ISSN 2063-5346

Forensic Investigation of Mobile Phones Utilizing Mobile Forensics Tools

1. ASLAM.J.KARJAGI *
Asssitant Professor
Department of Computer Science & Engineering
Secab. Institute of Engineering & Technology, Vijayapura 586101
Karnataka, India
*Corresponding author: aslamkarjagi88@gmail.com

2. S. A.QUADRI
Professor
Department of Computer Science & Engineering
Secab. Institute of Engineering & Technology, Vijayapura 586101
Karnataka, India

3. RAFEEDA .A.KARJAGI
Asssitant Professor
Department of Master of Application
Secab. Institute of Engineering & Technology, Vijayapura 586101
Karnataka, India

Abstract:

Mobile devices (cell phones and smart phones) play an increasingly important role in everyone's life, which also encourages illegal activities like SMS spoofing, hacking, and Smishing. Digital evidence from a mobile phone shows that a crook tried to erase the data. Investigators can discover about user information via information from mobile phones. In this study, a novel method is used to gather digital evidence from a compromised device that can be used in court cases and by digital investigators. This data collection technique offers a clearer picture of the offenders using mobile devices inappropriately for cybercrime.

Keywords: Digital investigators, Digital evidence, mobile forensics

I. Introduction:

Digital forensics is the area of forensic science where we can use forensic technologies to reconstruct historical events for use in court cases. Digital forensics is often separated into five main categories. They are database forensics, network forensics, mobile forensics, and forensic data analysis. Each category in digital forensics aids in identifying the cybercriminals, phishers, fraudsters, and other wrongdoers. As of December 2013, more than 6 billion text messages and 330 million multimedia communications were sent daily in the United States, according to CTIA. Apple reported in 2016 that consumers send 200,000 messages on average every second [21]. Mobile devices are tiny computers that have enormous data storage capacities. Criminal investigations are prompted by the daily development in the technology advancement of mobile devices. The recovery of data from mobile devices has been enabled by a number of digital toolkits. Forensic tools are mostly used to collect data from mobile phones and to provide reports on the collected data. There are several mobile forensic toolkits on the market, including XRY Forensic Examiner's Kit, Oxygen Forensics, and Cellebrite's Universal Forensic Extraction Device (UFED). These devices aid in the extraction of specific valuable data. Mobile devices, like personal computers, have access to a wide variety of information, including SMS, MMS, audio, and video. Potential evidence includes location data, subscriber and equipment identifiers, date/time, language, phonebook information, call logs (incoming, outgoing, deleted), text messages (incoming, outgoing, deleted), MMS (Multimedia messaging), video, audio Files, e-mails, and phonebook information, the need to review files and engage in online browsing.

For mobile forensics investigation, there are two common extraction techniques. Both logical and physical analyses are used. There are many different kinds of hardware and software, a sizable number of mobile operating systems, and security features that present obstacles for mobile forensics.

The information an investigator can obtain on their mobile devices is sufficient. By extracting, locating, and analyzing the mobile devices, a sizable amount of evidence can be retrieved. The mobile gadgets might be connected to crime in three different ways. 1) It serves as a communication tool 2) It also includes information on a victim.

3) Data extraction is possible. Social networking sites like Wechat are used by criminals to plan and communicate their illicit activities, such as the sale of illegal goods and fraud, among other things [2].

To make sure mobile phones are not remotely connected and to avoid tracking the mobile device and remote data wiping, it is required to carry a faraday bag when the mobile phone is turned on. From the moment of seizure until it is presented as evidence in court, digital evidence must be prevented. There is a possibility of crime occurring due to the rapid development of mobile devices. Mobile forensics technologies are required with the aim of access and recover older or erased data copies.

The data that can be extracted from different devices varies. Not all devices must have the ability to extract the entirety of their storage data. Text messages have become significant digital evidence in recent years.

The three steps of mobile forensics are seizure, acquisition, and examination/analysis. Examiners encounter certain particular challenges.

1. Negative Programs

2. A lack of tools.

3. Recovery of passwords.

4. Inadvertent Reset.

5. The anti-forensics method

The remainder of the essay is structured as follows. Section 2 describes the associated research that provides a survey of mobile forensics. The flow procedure of mobile forensics is described in Section 3. Section 4 offers a method to use an oxygen forensics tool to recreate historical events, and Section 5 provides a conclusion and suggestions for further work.

II. Related Work

To facilitate restoring of the previous occurrences of messages that could be helpful to forensics examiners, Daniel and Ibrahim [1] tested 16 of 20 applications. They also assessed the “security in sending and receiving the data”. They have demonstrated that numerous messaging applications contain flaws when storing and sending data. WeChat forensics analysis raises several questions, which Songyang et al [2] studied and addressed with technical solutions. They are: 1) gathering user information; and 2) looking into user-shared communications. Cosimo [3] examined the forensic evidence found in smartphone WhatsApp that can be used to reassemble messages and contacts from chat databases.

Edington and Kishore [4] discuss the difficulties of cloud forensics and offer a centralised forensics server that eliminates the requirement for an investigator to rely on a Cloud Service Provider (CSP) to collect data for an investigation. Cosimo et alanalysis .'s of chatSecure, which keeps local copies of messages sent and received, allowed them to decrypt the database using the secret passphrase the user provided during the original encryption procedure. Finally, they came to the conclusion that it is impossible to recreate database data using the SQL cypher deletion technique. A tool named command line was developed by Karpisek et al [6] and is used to analyse the WhatsApp protocol. They are able to decode network traffic, provide WhatsApp artefacts, and examine messages sent and received via it. In addition to analysing volatile memory's memory forensics, Andrew and Richard [7] also described the changes that occur in operating system design.

By gathering and organizing anti-forensics tools and developing an anti-forensics taxonomy with the aim of encapsulating within the field of anti-forensics, Kevin et al. [8] developed a data collection that would be useful for digital forensics. In response to malicious actions in cloud services, Hyunji et al. [9] established a methodology for forensics analysis of cloud storage service and also analysed artefacts for Windows, Macintosh Computer (MAC), (iPhone operating system), IOS, and Android OS. Josiah and Alan [10] showed how to use forensics tools for remote data acquisition in Amazon EC2, as well as how some technologies are insufficient for producing reliable data and for resolving issues with cloud forensics acquisition. By using three well-known cloud storage providers, including Microsoft SkyDrive, Dropbox, and Google Drive, Darren and Raymond [11] investigated whether the contents of the files were the same as the data collected from the cloud server and whether downloading files using client software resulted in any changes.

Shiek and Lalitha [12] discussed a trusted third party (TTP) model that aids in locating the location and IP address that are helpful to trap online criminals with the gathering of evidence that might aid the investigation team. Ameer et al[13] .'s discussion of potential solutions to the problems with cloud forensics included a full explanation of the suggested solution and a succinct description of forensics-as-a-service models. From a server and client standpoint, Ben and Raymond [14] presented and explored cloud storage-as-a-service forensics. Kumodd, Kumoddocs, and Kumofs are cloud forensics tools created by Vassil et al. [15] that function with both private and public services. They also provided new capabilities that cannot be obtained simply looking at client side artefacts. Using BPEL, Amna and Derar [16] presented a forensics method that incorporates four steps. Identification, Collection, Analysis, and Results into another service called FPaaS are the first four steps. The difficulties posed by the investigator when CSP gathers evidence from outside of a cloud environment were highlighted by Edington and Kishore [17]. Saad et al. [18] evaluated the issues that have been noted in recent studies as well as the technical solutions. Two perl scripts introduced by Jason [19] assist in retrieving data from Amazon Cloud Drive.

III. Flow Process of Mobile Forensics

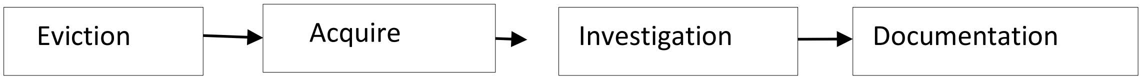

Figure 1: Flow process of Mobile forensics

a) Eviction
   To preserve the evidence, mobile phones are typically seized at crime scenes. Therefore, it's important to confiscate mobile phones at the crime scene. The examination of “mobile phones, personal digital assistants (PDAs), and global positioning system (GPS) devices can be done using the device seizure method”, which is a sophisticated forensic collection and analysis tool.
b) Acquire
   Acquiring, the second step in mobile forensics, typically involves retrieving data from the device. Because data gathering is impossible while the power is out, the majority of mobile acquisition is done live.
c) Investigation
   The data from seized devices is extracted using various forensics technologies. Since it is impossible to extract every piece of information, we must employ two or more instruments to look things over.
d) Documentation

When an inquiry is complete, the results are frequently conveyed in a nontechnical format. Reports may also contain audit details and information on I the start of the examination. ii) What tools were used? iii) The phone's status. The evidence will then be prepared for a criminal court with a documented expert conclusion.

IV. Analysis of Mobile Forensics

Using oxygen forensics, we are able to retrieve the essential information from the fraudster's mobile device, including call logs, SMS, MMS, emails, photos, videos, audio files, geolocation, and details about numerous applications. This tool has the capacity to collect data from mobile devices' volatile memory. You can learn the following information:

Contacts, Device Information, Call Logs (Missed/Outgoing/Incoming Calls), Organizer Data (Memos/Tasks/Notes), SMS, MMS, E-Mails, Photos, Videos, Audio and Video Files, and Device Information, Removed Data.

These details make it simple to identify the criminals who have been actively involved with police enforcement, examiners, and other government agencies.

1. ACTIVITY LOGS

User voice calls are listed in the event log section, including missed and dialed calls.Experts in forensics can identify the call time, duration, and remote party. Utilizing the oxygen forensics tool, it is also possible to recover deleted calls from specific mobile devices.

This section will display every incoming, outgoing, and missed Call logs placed on the mobile device. For each log, it is able to read the timestamp of the event, the Remote party, the length of the call, the call number, and the MD5 hash. Deleted Calls from an Android handset (Samsung Galaxy Grand II) are primarily shown in blue and are distinguishable by the "recycle bin" icon. The examiners who are all connected to a specific crime incident can benefit from the call log events.

2. ORGANISER DATA

It provides information on tasks, memos, and notes, among other things. This section contains some significant information. We have the ability to view the data across time. Information such as the SH2 hash function, Event type, start Time, and finish Time can be obtained from this.

3. WIFI ACCESS, WIFI HOTSPOT

Geolocation and web connections indicate suspiciously frequented locations and routes. Examiners can analyze geo data from a variety of sources, including Wi-Fi connections, IP connections, and databases of locations. Using an internet connection, forensic investigators can pinpoint when and where a suspect utilized public or even private Wi-Fi to access his location. It retrieves information about websites visited as well as potential passwords entered by the user. The specifications of a hotspot connection, such as the service set identifier (SSID), basic service set identifier (BSSID), and received signal strength indicator (RSSI), provide information about the last time the suspect connected. The examiner is able to see the locations where the mobile devices were used.

When and where a suspect enables his location or shares it with others, geolocation can expose suspect-visualized locations. The coordinates on the map display the suspect's whereabouts. The IP address page displays the history of Web connections together with their specifics, such as Media Access Control (MAC) and VPN addresses, device and router IP addresses DNS names, region, and time stamp. The location of the device owner can be tracked by the examiner.

4. COMMUNITY GRAPH

The social graph illustrates intricate relationships within criminal organizations. This highly adaptable setting enables forensic specialists to examine relationships between users of mobile devices and their contacts, identify links between users of different devices, and identify their shared contacts.

5. LOGS FROM MOBILE DEVICES FOR CHAT

Examiners are able to extract all relevant information from chat logs. The feature set of a mobile device may change:

- Previous conversations with individuals and groups
- Contacts list includes photographs, notes, and all fields
- SMS and MMS sent, receiver mobile number, timestamp, and country code
- Complete call details.
- The geographic location of the incident.

It quickly makes social connections between contacts on a user's mobile phone and those users.

By examining calls, texts, multimedia, e-mails, and social messengers, communication statistics enables researchers to investigate the social ties between device users.

Table 1: Oxygen Forensics Tool Receives Device Data and Elements

Device Data	Data Elements
CALL LOGS	Incoming Outgoing Missed Incoming-deleted Outgoing-deleted

	Missed-deleted
SMS	Incoming SMS-Read Outgoing SMS-Read Incoming SMS-deleted Outgoing SMS-deleted
E- History	History Visited Sites E-mails Bookmarks
Geographic location	Co-ordinates
Application	Device Apps
Data of social media	Facebook Instagram Whatsap

V. Conclusion

This research concentrated on applying forensic tools to reconstruct historical events on mobile devices. The" data, backup files on computers, sent and received messages from both individuals and groups", various message types and attachments, and message and device states, such as offline, online, blocked, removed, and deleted, can all be retrieved from the device and are helpful for a criminal investigation. During the forensic inquiry, an examiner then examined this data.

VI. 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 investigation13 (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 Conference.

[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