Mobile Forensics Approaches and Challenges

Asadullah
Department of Computer Science and
Technology, Central University of Punjab
Bathinda 151001,India
asad.nu.it@gmail.com
Tel (+91)8826914076

Abstract *– Nowadays, mobile phones and other handheld devices are everywhere. Cell phones and other cellular devices may be used in the commission of a crime or other incident. For successful recovery and analysis of data contained on mobile phones, digital forensic specialists will require specific instruments for forensics investigation of mobile phones. For this type of investigation, there are some tools and techniques available; nevertheless, there is presently still no good solution. The purpose of this paper is to explore into the difficulties that arise while conducting forensic analysis on mobile phones, to concentrate on numerous analytical techniques, and to illustrate a pyramid of forensic techniques and tools.*

Keywords *– mobile forensics, investigation, evidence, analysis, technique, tools.*

1. INTRODUCTION

Since everyday life and business are moves at the speed of electrons across the air, most civil and criminal investigations involve some sort of digital element. As mobile phones become so ubiquitous and play such a large societal role, there is a high probability that these same devices will be part of those investigations. A mobile phone can be linked to crime in four different ways:

- It can be used as a communication tool in the process of committing a crime.
- It can be a storage device providing evidence of a crime.
- It can contain victim information.
- It can be a means of committing a crime.

The procedures for extracting evidence from mobile phones are referred to as mobile phone forensics It is the science of recovering digital evidence from a mobile phone using approved procedures under forensically sound conditions. It examines both the SIM card and the phone's memory. Mobile phones, like any other digital medium, have the ability to save evidence. The process of retrieving deleted data from a mobile phone is similar to that of recovering data from a hard drive. Evidence items stored on mobile phones, like any other digital media, are fragile and can be easily erased or overwritten. Information can be found in abundance on mobile phones. Call logs, contact lists, and text messages are the most obvious types of data that may be accessed from a phone. Other capabilities of a modern phone, such as ring tones, dictionaries, stored responses, video files, still picture files, calendar events, random papers and data files, and location information, might all be useful in an investigation. Given the wide range of data types available, it's critical to analyze each one with greatest care, especially sensitive data, especially since it is entirely possible, with the use of specialized tools, too often recover deleted information. The main goal of doing mobile phone forensics research is to extract usable information from these devices and submit it as evidence in court. Before trying to study data on a mobile phone device, one must be well prepared. Mobile device forensics necessitates a thorough understanding of technology, as well as familiarity with tools and their limits. Using different tools and personally

confirming the data can be beneficial. Non-forensic tools are ineffective, but forensic methods produce a wide range of results. A forensic examiner must have a clear understanding of what will be acquired and how it will be acquired.

2. APPROACHES IN MOBILE FORENSIC INVESTIGATION

Data on mobile devices can be stored in a variety of locations, including the SIM card, the device's embedded memory, and external memory. The service provider also keeps data related to calls and subscribers. On mobile devices, evidence can be found in the following places:

- Provider information—IMSI, IMEI, and PIN/PUK
- Phone information—Calls, MMS, SMS, and pictures
- SIM card—phone numbers, text messages
- Removable card—pictures

Manual, physical, and logical approaches can all be used to extract data from mobile devices. A manual method is usually used when investigators need only to extract specific evidence from the mobile device. When using the manual approach on a mobile device, the investigator may overlook digital evidence, especially if the investigator is new to or unfamiliar with mobile device extraction. A digital investigator, for example, may overlook a mobile device application that shares secret messages. By failing to analyze the substance of such an application, digital evidence that could be crucial to the case. To decrease the possibility of overlooking important data on a mobile device, the investigator should look at each screen and application systematically and document the outcomes. The physical technique uses low-level data extraction, whereas the logical method uses higher-level communication protocols available on the mobile device. There are benefits and drawbacks to each of these approaches. When employing the physical approach to conduct an inquiry, the investigator can obtain the contents of the entire device memory, including deleted things. Furthermore, with damaged mobile devices, physical acquisition methods might be applied. Also, this method makes fewer modifications to the original device during data acquisition. This procedure, on the other hand, takes a long time and necessitates the use of complex and expensive tools. Consequently, the investigator gets a raw image. A raw image is generally encrypted, and, if the investigator is able to decrypt an image, additional investigation can be accomplished only by using particular and sophisticated software tools. On the other hand, using a logical technique, the investigator can gather data instantaneously in a form that is readable. However, the volume of gathered data is considerably lower than in an extraction process using the physical method. Using the logical acquisition method, the investigator may snag evidence such as date and time stamps as well as location inside the file system Evidence obtained via a data cable may differ from evidence obtained via Bluetooth in certain circumstances. The investigator should execute the logical method in various ways to make sure all potential evidence is pulled out In addition, computer forensic tools and procedures such as physical image acquisition are frequently used to analyze memory cards.

3. CHALLENGES ASSOCIATED WITH MOBILE PHONE FORENSICS

Knowing the significance of mobile phone forensics, it's important to be aware of the current obstacles that investigators face. A survey of the current mobile phone landscape produced six general categories of challenges:

i. Carriers and manufacturers
ii. Data preservation
iii. Power and data connectors
iv. Operating systems and communication protocols
v. Security mechanisms
vi. Unique data formats. The following is a realization of these challenges.

3.1. Carriers and Manufacturers

The first step in any inquiry using a mobile phone is to identify the phone. Given that there are multiple network carriers (at least seventeen in the US alone) and device manufacturers (over thirty in the US), identifying a phone by sight alone is extremely difficult even for trained investigators. A single model from a single hardware manufacturer may be marketed under a variety of distinct carrier names. A great example of this is the recently famous Motorola RAZR which is marketed under at least 24 different product names. The exact hardware type of a device cannot be determined until the battery is removed, however removing batteries can cause the phone to lose information saved in volatile memory, or even worse, require a handset lock code on power up.

3.2. Data Preservation

It's critical to restrict the device from receiving any further data or voice communication during a mobile phone investigation. Because text messages are stored in a "First In, First Out" manner, any new incoming text messages may overwrite older ones. Incoming calls can also remove call history logs, and some devices (like the RIM Blackberry) can be remotely wiped of all data if they aren't protected from incoming communications. As a result, when these phones are first purchased, they must be stored in some form of wireless preservation container. This can be accomplished via a variety of methods, with different degrees of success. These tools range from three layers of common aluminum foil, to a tri-weave mesh material shield of nickel, silver, and copper, to an anodized aluminum shielded enclosure made to withstand wireless devices from radio frequencies.

3.3. Power and Data Connectors

Another issue confronting investigators is how to keep the phone powered up. A phone's battery will eventually die if it is kept unplugged for an extended period of time. Because many mobile phones store information in volatile memory, a total loss of power could result in the loss of information, and consequently critical evidence. As a result, it is preferable to maintain a phone charged. Regrettably, there is currently no standard for mobile phone power requirements. This absence of power standards is exacerbated by the fact that there are no cable connector standards. Hundreds of various types of mobile phone power connectors are currently in use. Even if two phones require the same voltage to charge, their power connectors are unlikely to be interoperable. The OMTP (Open Mobile Terminal Platform) intends to reduce the number of connectors in the mobile sector by suggesting that the micro-USB standard be adopted across the board. Even while a standard like this would be beneficial to criminal investigators and end users, it is unlikely to happen anytime soon because hardware makers are continuously altering their designs and will use whichever connector type helps them achieve their design goals.

3.4. Operating Systems and Communication Protocols

The numerous operating systems used on mobile phones are also a barrier to the development of forensics tools. Mobile phones have evolved into full-fledged computer platforms, necessitating the usage of advanced operating systems by vendors in order for various software programs to operate on them RIM's Blackberry, iDEN, Palm, Symbian, Windows Mobile, Macintosh OS X, and various versions of the Linux open-source operating system are among the most popular operating systems. Some operating systems are also exclusive to the hardware manufacturer. For example, Nokia's Series 30 and 40 phones use the ISA platform. Knowing which protocols to utilize for communication between the evidential mobile phone and the forensic investigator's computer is an issue with all of these operating systems. AT, BREW, FBUS, IrMC, MBUS, OBEX, and SyncML are some of the most well-known data communication protocols now in use, and they are largely dependent on the operating system and carrier restrictions. These protocols can be

used to retrieve information from a mobile phone such as its make and model, telephone number, software revisions, serial number, call logs, contacts, text messages, ring tones, videos, images, and other important pieces of data. They are often proprietary, cryptic, and rarely documented. Unfortunately, practically every phone uses a different version of each of these protocols, and they never seem to reply the same way to the same requests. Worse, in order to enable a communications channel so that vital evidence can be obtained, several operating systems require the examiner to first copy software files directly to the device. The process of copying data to a mobile phone, on the other hand, has the potential to delete evidence. Another point to consider is how protocols can occasionally alter data. Using the built-in protocols to access messages in the message storage, for example, will mark the message as read even if the user has never seen it. This need to access information on the phone should be properly examined, even if it changes the phone's condition. Evidence acquired from a phone that involved modifying information on the phone may not be admissible in court in specific situations.

3.5. Security Mechanisms

To protect data, mobile phones have a number of security features. Manufacturer or user handset locks, as well as SIM card PINs and PUKs, are all examples of securing techniques. Depending on the brand and model of the device, whichever sort of security is used, the implications vary. Many mobile phones include a handset lock code that is either set by the manufacturer (Motorola – 000000, Nokia – 1234), or set by the user, which is even more problematic. When a phone is turned on, the handset lock is normally activated, which causes a difficulty for examiners trying to investigate a phone that has been found or seized in a powered off state Global Systems for Mobile Communication is one of the most widely utilized network technologies in the world (GSM). A SIM card, which comprises a light-weight CPU chip and a small quantity of non-volatile memory, is found in most GSM phones. The SIM card is used as a storage device for subscriber data in GSM phones The SIM's processor's sole purpose is to implement the SIM's access mechanism and security features. GSM specifications define the physical and logical aspects of the access mechanism. The SIM can be physically connected to a computer by inserting it into a conventional smart-card reader. To logically access the SIM, software running on the PC is required. The GSM SIM access mechanism requires software to be implemented. Once the user has validated himself with a PIN and/or PUK code, the contents of the SIM card are arranged as a sequence of files containing binary data that may be copied to a PC. A PIN (Personal Identification Number) is not usually required to gain access to the SIM. Since the phone cannot be used without access to the SIM, this number must be entered whenever the phone is turned on. If the user fails to enter a valid PIN through three attempts, the card becomes blocked, and the user must instead enter an 8-digit code, called a PUK (Personal Unblocking Key), to reopen it. If the user fails to enter the correct PUK after ten attempts, the card becomes permanently blocked and cannot be reopened. The user can modify and deactivate the PIN for a card. The PUKs are set in stone and cannot be altered. The network operator normally keeps track of the PUKs for all of its users because the PUK is fixed. As a result, by asking the network operator for the necessary PUK, the investigator may nearly always acquire access to a SIM card. It might, however, be more efficient to ask the owner of the phone to provide correct PIN or PUK codes. During searches, the PUK might also be recovered, since phone owners sometimes keep the PUK in writing in case they forget the PIN. An extra hurdle may exist even after gaining access to the data on the mobile phone. When data is stored in files on mobile devices, it is sometimes encrypted using a proprietary encryption method. Without the assistance of the hardware or operating system

vendor, decrypting the data becomes far more difficult, if not impossible.

3.6. Unique Data Formats

Assuming that the carrier and manufacturer of a phone can be identified, that the phone can be protected from wireless activity, that the correct power and data connector wiring can be found, and that the information is not stored encrypted, it is then theoretically possible to retrieve information from the phone. However, one more obstacle remains. As with the other components that make up a modern mobile phone, there is neither a standard format nor a standard location, for much of the information desired by an investigator. Data files can be stored in a number of locations. As previously stated, some information can be saved in the memory on the SIM card of the phone. Mobile phone hardware also contains random access memory (RAM) that can be segmented as volatile (requires an electrical charge to retain information), or non-volatile (retains information without an electrical charge). Investigators and makers of forensic software need to be aware that information might be hiding in all these types of memory. Many mobile phones also contain read-only memory (ROM). However, ROM is typically used to store the phone's operating The files saved in ROM are unlikely to be of interest to an investigator because the contents of ROM are not easily modified. Textual information such as telephone numbers, address books, email messages, and text messages are stored using proprietary file formats. Makers of forensic software tools will need to be aware of these formats so they can write software that will convert these files to information easily understood by humans. An exception to these proprietary file formats is for image and video files which are typically stored in common JPG and MPEG format

4. CONCLUSION

We analyzed the various problems that a forensic investigator faces while dealing with smartphone forensics in this research and gave a comparative summary of these challenges. While mobile phones provide a wealth of information, a combination of factors such as developing technology, stronger security features, forensic tool limits, communication protocols, customization by multiple device carriers, and the sheer variety of models can prevent effective forensics. As a result, forensic investigators must be fully aware of what data can and should be extracted from the devices in question, the risks associated with the extraction process, and the amount of high-quality data that can be retrieved and processed using the specific forensic tool at hand, given the tool's limitations. No free tools exist that could investigate every single mobile device on the market. Mobile forensics technologies, methodologies, and training are changing and growing more expensive at the same time as mobile device improvements. To sustain professional readiness and to perform quality mobile device forensic investigation, investigators must receive appropriate training and have access to adequate budgets.

5. REFRENSES

[1] Anobah, M., Saleem, S., & Popov, O. (2014). Testing Framework for Mobile Device Forensics Tools. *Journal of Digital Forensics, Security and Law*. Published. https://doi.org/10.15394/jdfsl.2014.1183

[2] Chernyshev, M., Zeadally, S., Baig, Z., & Woodward, A. (2017a). Mobile Forensics: Advances, Challenges, and Research Opportunities. *IEEE Security & Privacy*, *15*(6), 42–51. https://doi.org/10.1109/msp.2017.4251107

[3] Chetry, A., & Sarkar, M. M. (2020). Mobile Forensics And Its Challenges. *Digital Forensics (4n6) Journal*. Published. https://doi.org/10.46293/4n6/2020.02.03.07

[4] Curran, K., Robinson, A., Peacocke, S., & Cassidy, S. (2010). Mobile Phone Forensic Analysis. *International Journal of Digital Crime and Forensics*, *2*(3), 15–27. https://doi.org/10.4018/jdcf.2010070102

[5] Dashti, M. (2013). Mobile Forensics Opportunities and Challenges in Data Preservation. *IOSR Journal of Engineering*, *03*(08), 23–29. https://doi.org/10.9790/3021-03812329

[6] Digital Forensic Investigation and Analysis of Android Mobile. (2015). *International Journal of Science and Research (IJSR)*, *4*(12), 704–707. https://doi.org/10.21275/v4i12.nov152071

[7] Induruwa, A. (2009). Mobile phone forensics: an overview of technical and legal aspects. *International Journal of Electronic Security and Digital Forensics*, *2*(2), 169. https://doi.org/10.1504/ijesdf.2009.024901

[8] Kumar, M. (2021). Mobile phone forensics - a systematic approach, tools, techniques and challenges. *International Journal of Electronic Security and Digital Forensics*, *13*(1), 64. https://doi.org/10.1504/ijesdf.2021.111725

[9] Madiyanto, S., Mubarok, H., & Widiyasono, N. (2017). Mobile Forensics Investigation Proses Investigasi Mobile Forensics Pada Smartphone Berbasis IOS. *Jurnal Rekayasa Sistem & Industri (JRSI)*, *4*(01). https://doi.org/10.25124/jrsi.v4i01.149

[10] Mellars, B. (2004). Forensic examination of mobile phones. *Digital Investigation*, *1*(4), 266–272. https://doi.org/10.1016/j.diin.2004.11.007

[11] S. Waghmare, V., & Meshram, B. B. (2020). Mobile Forensic Process and Associated Key Challenges. *International Journal of Cyber-Security and Digital Forensics*, *9*(1), 42–54. https://doi.org/10.17781/p002651

[12] Through, J., & Cantrell, G. (2017). Varying Instructional Approaches to Physical Extraction of Mobile Device Memory. *The Journal of Digital Forensics, Security and Law*. Published. https://doi.org/10.15394/jdfsl.2017.1420