REVIEW ARTICLE

IJETV Vol. 9, Issue 2, 2023 Print ISSN: 2394–6822 Online ISSN: 2395–4272

Mobile Forensics: A Valuable Instrument or a Challenge in Forensic Industry

Dipti Shukla[1*], KK Parashar[2]

[1]Samarpan Institute of Nursing and Paramedical Sciences, Lucknow, Uttar Pradesh, India.
[2]Sanskriti University, Mathura, Uttar Pradesh, India.

Abstract

Mobile forensics is the science of recovering digital evidence from a mobile device under forensically sound conditions using accepted methods. Mobile device forensics is a subfield of forensic science called "digital forensics" is dedicated to the retrieval and examination of unprocessed data found on electronic or digital devices. The procedure aims to retrieve and extract any data from a digital device without changing the data that is already on the device. Digital forensics expanded throughout time in tandem with the swift expansion of computers and other digital devices. Depending on the kind of digital device involved, there are several subfields of digital forensics, including computer, network, mobile, and so on. The study of recovering data from a mobile phone in a way that complies with forensic standards is known as mobile phone forensics. This covers the whole process of retrieving and analyzing data from the SIM/USIM, the phone body, and any optional memory cards. Call timings, contact numbers, text or SMS messages, photos, videos, and other types of data may all be recovered and analyzed.

Keywords: Digital forensics, Mobile forensics, Media.

Int J Eth Trauma Victimology (2023). DOI: 10.18099/ijetv.v9i02.08

Introduction

The process of extracting digital evidence from mobile devices using recognized techniques is known as mobile forensics. Mobile forensics, in contrast to typical digital forensics procedures, is limited to the recovery of data from mobile devices, including tablets, smartphones, and android phones. Law enforcement may greatly benefit from the wealth of information found on mobile devices, including location data, text message histories, and site search histories.[1]

The gathering of data from mobile devices has become a crucial component of forensic investigations and is frequently utilized as convincing evidence. It is crucial to have a complete grasp of forensic tools and their properties to extract relevant data.[1]

Importance of Mobile Forensics

Mobile forensics are crucial since mobile devices save a lot of data that may be required to comprehend the entire picture and extent of a cyberattack. There were 15 billion mobile devices in use globally in 2021. That comes to almost two per person. [2]

It's incredible how much data is kept on these devices. The fact that systems are no longer absolute and isolated distinguishes mobile computer forensics from traditional computer forensics. Common place electronics can function as a single network thanks to its interconnectivity, including phones, automobiles, cameras, doorbells, and even refrigerators.[2]

Mobile phone forensics may be performed on the cellular network usage of a specific mobile phone to determine the location and time of calls made, as mobile phones are frequently utilized during many types of criminal behavior. This is especially helpful in situations similar to stalking, where someone has been harassed *via* a cell phone.[3]

Corresponding Author: Dipti Shukla, Samarpan Institute of Nursing and Paramedical Sciences, Lucknow, Uttar Pradesh, India, e-mail: Shukladipti7@gmail.com

How to cite this article: Shukla D, Parashar KK. Mobile Forensics: A Valuable Instrument or a Challenge in Forensic Industry. Int J Eth Trauma Victimology. 2023;9(2):36-38.

Source of support: Nil

Conflict of interest: None

Received: 01/12/2023; **Received in revised form:** 15/12/2023;
Accepted: 20/12/2023; **Published:** 20/01/2024;

These days, police officers' first port of call is mobile phone forensics in addition to the computer. Where will you probably keep all of your records? Where will the records of wrongdoings be kept? Human nature dictates that you will notify someone about wrongdoings, even if you are not the kind to document them. [3]

They may be kept on a computer in a variety of locations, including your PST (Microsoft Outlook personal storage file), EDB (Microsoft Exchange storage file), NSS (Lotus Notes), MSG (Microsoft Outlook Express), and EML (generic email files). All of these files are stored digitally on a variety of storage devices, such as SIM cards for mobile phones, maybe 3G USIM cards, and ordinary mobile phone memory, digital copies of all this information are stored on a variety of storage devices, such as subscriber identity module (SIM) cards for mobile phones, maybe 3G USIM cards, standard mobile phone memory, or internal memory cards; they are mostly, though not just, multimedia card (MMC) cards.[4]

To guarantee that a thorough examination of all available data has been completed for the client in a sound and forensically correct manner, a forensic investigator today must possess solid knowledge of evidence handling, write-blocking, and general computer forensics (Figure 1).[5]

They can no longer rely solely on their mobile phone investigative resources.

Preservation and Documentation

It's critical to preserve the crime scene while collecting evidence. The cell phone cannot just be taken off of the crime scene. Other types of evidence, such as fingerprints and DNA traces, must also be preserved with care. Moreover, appropriate documentation is required for every piece of evidence, as well. A minimum of a few photos of the undisturbed/unmoved phone and details on the time and place of the accusation should be included in this evidence. Noting whether the phone was turned on or not is also crucial.[5]

Acquisition

Actual data from the gadget is obtained at this step. This assembly can happen in several ways. Ideally, both the SIM card and the phone's data are forensically duplicated. Sometimes a device's digital accusation can't be made due to technological issues. In the worst situation, all that may be obtained are phone screenshots.[5]

Examination and Analysis

The collected data is currently being examined for any hints about the potential crime. To examine these hints in more detail, refer to Figure 1. Software tools can assist with the examination, or it can be completed by hand. For that goal, a variety of software solutions are available. Utilizing a variety of software tools is essential. Since there is no magic bullet, effort must be made to ensure that no important piece of evidence is overlooked because a certain instrument lacks a necessary characteristic.[6]

Reporting

The final stage is the most crucial. It can take a long time to acquire the evidence and present it in court. Examiners need to be able to provide conclusive evidence and inform the opposing side about the instruments and techniques they used. If the evidence is not permitted into evidence in court, it is worthless. This can occur if the evidence's provenance or acquisition is questioned, raising doubts about its legitimacy.

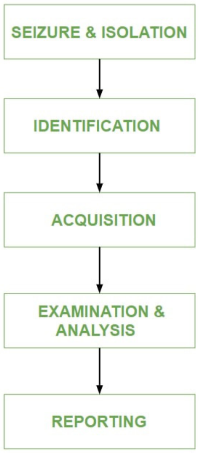

Figure 1: Process of mobile forensics

Types of Evidence

Address book

Various contact details are kept in the address book. An understanding of the suspect's social network can be obtained with the use of the address book. One purpose for it would be to connect a suspect to a victim.[7]

Call history

The call history provides more detail on the owner's actions before the mobile phone was acquired. The duration of the most recent incoming and outgoing calls is visible. Indirect implications can also be drawn from this data.[7]

Short message service (also available in emails on new phones)

While phone histories and address books only provide oblique information, SMS and email communications provide specific information as opposed to the address book and call history, which only provide oblique information. They may include the owner's real writings, either meant for the owner or authored by them, which could be used as evidence in court.[8]

Calendar

The calendar provides a summary of the owner's previous and upcoming activity. It can be used to identify potential witnesses and connect the owner to specific times and locations.

Additional media

Numerous more pieces of information can also be found on more recent mobile phones.

The camera comes first. Films and images can also include proof. Not just in terms of their content, but also in terms of the exchangeable image file format (EXIF) (information contained within files that provides additional details). It's possible that the criminal used the photo as a trophy for their crime. The precise time and date of a photo's capture, as well as its location in some circumstances, can be found using the EXIF data. A global positioning system (GPS) receiver is included with some cell phones. The mobile phone's applications cannot affect the receiver's ability to store location and time data. to connect the owner to potential crime scenes or provide an alibi.[8]

Current problems

Forensics on mobile devices face numerous challenges. They will be examined in this paper in the order that they appear in an examination.[8]

When the cell phone is discovered at the crime site, the first issue arises. Everything works perfectly when the phone is turned off, however, there is a problem when it is turned on. It is feasible to tamper with the evidence if the phone is left on. Some versions have a limited quantity of data storage—20 SMS, for instance. The evidence is gone if the offender decides to delete it by sending 20 pointless texts from a different phone.[8]

Everything works perfectly when the phone is turned off, however, there is a problem when it is turned on. It is feasible to tamper with the evidence if the phone is left on. Some versions have a limited quantity of data storage—20 SMS, for instance. The evidence is gone if the offender decides to delete it by sending 20 pointless texts from a different phone.[9]

Finding the phone is another issue. Numerous manufacturers provide an extensive range of models, with new versions being released on a nearly regular basis. Before the investigation can start, any phone discovered at the scene of a crime must be identified so that the specialist may become acquainted with it. There are various approaches to completing this. Typically, the side of the device displays the logos of the wireless carrier and the manufacturer. However, this is just the beginning. Some websites make an effort to be helpful.[9]

The selection of appropriate software for a given phone presents the next challenge. As was already noted, a wide variety of hardware and software solutions are available. Each of them offers benefits and drawbacks in terms of the software features and supported models. In this case, the investigator must rely on prior knowledge. In a perfect world, he would be familiar with the phone model and its optimal software. The investigator deals with new phones in the real world as well. Here, he must use extreme caution to avoid destroying any evidence.[10]

The SIM lock is another issue. Personal identification numbers (PINs) can be used to secure SIM cards and the data on them. Only three attempts are allowed at the SIM, and ten attempts are allowed for the personal unblocking code (PUK). Asking the owner for the PIN is an excellent practice if a phone is found; if not, calling the manufacturer to get the SPUK is the sole option. One needs to be aware of the integrated circuit card identifier (ICCI) to select the PUK. Usually, this number is printed on the SIM's outside.[10]

Use of Mobile Evidence

The important aspects for which mobile evidence is being presently used are:

- To find out the numbers to which calls have been made from a given mobile with date and time
- To find out the numbers from which the calls have been received in a given mobile with date and time
- To know the contacts through the phone book.
- To know the details of recent SMS messages received
- To know the details of SMS templates
- To know the ring tones and games stored in the instrument
- To know the pictures and video clips stored in the mobile either on the SIM card or a flash memory card.[11]

Cell Phone Forensic Tools

- MOBILedit! Forensic (software)
- Intaforensics - ART – Mobile (software)
- BitPIM (software)
- The.XRY/XACT System Bundle (hardware)
- Cellebrite (UME/UFED-hardware)
- EnCase® Neutrino® (hardware)
- AccessData – MPE (hardware)
- DataPilot SecureView (hardware)
- Paraben's Device Seizure Toolbox (hardware)

Discussion

As can be seen now these days mobile gadgets are all around us and developing into complete computing systems. Therefore, these gadgets are now essential in both criminal and civil investigations as evidence. As was already established, mobile devices—particularly smartphones—produce a wealth of unrelated data that can be quite beneficial to investigators. Even the most well-known manual procedures, nevertheless, might not be able to find this information.

We must be aware as mobile forensic technologies provide a significant solution to the issues. These sophisticated solutions make use of cutting-edge technologies like artificial intelligence and big data to efficiently and forensically soundly expose all of the data on these gadgets. Mobile forensic technologies are crucial for solving crimes of all kinds.

Conclusion

Mobile forensics plays an important role in the forensic industry as it preserves forensic integrity while retrieving pertinent data or digital evidence from a mobile device. To do this, the mobile forensic method needs to create exact guidelines for safely obtaining, separating, moving, storing for further analysis, and verifying digital evidence that comes from mobile devices.

Mobile forensics procedures are typically similar to those of other digital forensics specialities. But it's crucial to remember that the mobile forensics procedure has particulars of its own that need to be considered. If the study of mobile devices is to produce fruitful results, appropriate techniques and guidelines must be followed.

References

1. James SA. An introduction of scientific investigation techniques. 2019
2. Mc Carthy P. Forensic analysis of mobile phones. 2005
3. Reddy KS. Introduction of forensics medicine & toxicology. 2017
4. Majindran, J. Forensic medicine.2021
5. www.ifs india.com
6. Jansen, Wayers, R.: Guidelines on PDA Forensics. 2004
7. Jansen, Wayers, R.: Guidelines on cell phone Forensics, 2004
8. Symbian History. 2008
9. Telecom paper. 2008, http//www.telecompaper.com
10. Ducell. 2008, http://www.diucelk
11. Jansen,Wayers,R.: Guidelines on cell phone Forensics, 2006