International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 1, December 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Conceptual Study of Mobile Forensics

Mr. I. A. Attar, Mr. M. M. Kapale

V.P. Institute of Management Studies and Research, Sangli, Maharashtra, India

ABSTRACT

The use of digital devices in day to day life has increased tremendously. Mobile devices have become an vital part of our day-to-day routine and they are prone to facilitating illegal activity or otherwise being involved when crimes occur. Whereas computers, laptops, servers, and gaming devices might have many users, in the vast majority of cases, mobile devices generally belong to an individual. The science behind recovering digital evidence from mobile phones is called mobile forensics. Digital evidence is defined as data and information that is stored on, received, or transmitted by an electronic device that is used for investigations. Digital evidence encompasses any and all digital data that can be used as evidence in a case. Mobile devices present many challenges from a forensic viewpoint. With new models being developed each day, it is extremely difficult to develop a single process or tool to address all the possibilities an investigator may face. Court cases also need to be taken into consideration as mobile devices are being seized and analyzed.

KEYWORDS: *Mobile forensics, Mobile crime, digital evidence, digital forensics*

How to cite this paper: Mr. I. A. Attar | Mr. M. M. Kapale "Conceptual Study of Mobile Forensics" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-1, December 2019, pp.161-163, URL: https://www.ijtsrd.com/papers/ijtsrd29476.pdf

IJTSRD29476

1. INTRODUCTION

Digital forensics is a branch of forensic science focusing on the recovery and investigation of raw data present in in digital devices. The aim of the process is to extract and recover any information from a digital device without altering the data present on the device. For many years, digital forensics grew along with the rapid growth of computers and various other digital devices. There are different branches of digital forensics depend on the type of digital device involved such as computer forensics, network forensics, mobile forensics, and so on.

Mobile forensic is a part of digital forensics concerning to recovery of digital evidence or data from a mobile device under forensically sound conditions.

2. Objectives:

1. To study the need for mobile forensics
2. To study various challenges in implementation of mobile forensic.

3. Discussion:

Mobile forensics is a collecting electronic data for legal evidence purposes. This is a useful tool for investigators as a method of collecting criminal evidence from a track of digital data, which is often difficult to delete. Extraction of files that deleted mobile phone used as criminal evidence is the primary work of mobile phone forensics investigators.

Need of Mobile Forensic

For crime purpose use of phones was generally recognized for last few years, but the forensic study of mobile devices is a relatively new field, from the early 2000s.

A production of mobile on the consumer market affected a demand for forensic investigation of the devices, which could not be happened by existing computer forensics techniques.

- Mobile devices can be used to save different types of personal data such as contacts, pictures, notes and calendars, SMS and MMS messages.
  Mobiles may additionally contain video, email, web browsing information, location information, and social networking messages and contacts.

Mobile device forensics can be mostly challenging on a number of stages.

- To stay competitive environment, hardware manufacturers frequently alter mobile phone form factors, hardware, operating system, internal file structures, data storage and even connectors and cables.

  As a result, forensic investigator must use a different forensic process compared to computer forensics.

  Storage capacity continues updated so that it demands for more powerful “minicomputer” type devices.

- The types of data and the way mobile devices are used always evolve.
  Finely result of these challenges, a large variety of tackles exist to extract evidence from mobile devices.

Mobile Device Forensic Processing:

In mobile devices challenging things are data recovery and analysis standpoint. Due to increasing functionality and growing data storage, mobile devices have become small size

computers. With security options like password protection and encryption now the norm for lot of these devices, law enforcement continues to struggle to find ways to extract and analyze information from these devices. The Scientific Group on Digital Evidence (SWGDE) and the National Institute for Standards and Technology (NIST) and provide an in-depth look at mobile forensics outlining the benefits and the challenges these devices present to Law enforcement. There are many tools and techniques available in mobile forensics. The selection of tools and techniques during an investigation acts on the type of mobile device and its media.

Tools & Techniques

Forensic software tools are frequently evolving new techniques for the extraction of data from different mobile devices. There are two most common techniques 1) physical and 2) logical extraction. In physical extraction through JTAG or cable connection and logical extraction follows via, infrared, Bluetooth or cable connection.

There are different types of tools available for mobile forensic purposes. They can be classified as commercial, open source and non-forensic tools. Forensic and Non-forensic tools frequently use the same techniques and rules to relate with a mobile device. Forensic analysts must understand the particular types of forensic tools. The tools classification system offers a framework for forensic analysts to compare the acquisition techniques used by different forensic tools to capture data.

Manual Extraction

The manual extraction technique allows investigators to extract and view data through the device's touch screen or keypad. At a later stage, this data is documented photographically. Manual extraction is time wasting and involves a great probability of manmade error. For example, the data may be unintentionally erased or altered during the investigation.

Popular tools for manual extractions include:

- Project-A-Phone
- Fernico ZRT
- EDEC Eclipse

Logical Extraction

In Logical Extraction technique, the investigators connect the mobile to a forensic workstation or hardware via Infrared, RJ-45 connector, or USB cable or Bluetooth. In computer a logical extraction tool—sends a sequence of commands to the mobile device. Due to that, the required data is collected from the phone's storage and sent back to the forensic workstation for examination purposes. The logical extraction include following tools:

- XRY Logical
- Oxygen Forensic Suite
- Lantern

Hex Dump

A hex dump or physical extraction, extracts the raw image in binary format from the mobile device. The forensic expert connects the device to a forensic workstation and pushes the boot-loader into the device, which instructs the device to dump its memory to the computer. This process is cost-effective and supplies more information to the examiners, including the recovery of phone's deleted files and unallocated space. Hex dump include following tools:

- XACT
- Cellebrite UFED Physical Analyzer
- Pandora's Box

Chip-Off

This technique allows the examiner to extract data directly from the flash memory of the mobile device. They remove the phone's memory chip and create its binary format image. This process is costly and requires an ample knowledge of hardware. Incorrect handling may cause physical damage to the chip and renders the data difficult to recover. Chip-off include following tools:

- iSeasamo Phone Opening Tool
- Xytronic 988D Solder Rework Station
- FEITA Digital inspection station
- Chip Epoxy Glue Remover
- Circuit Board Holder

Micro Read

Micro Read process contains interpreting and observing data on memory chips. The examiners use a high-powered electron microscope to analyze the physical gates on the chips and then change the gate level into 1's and 0's to find out the subsequent ASCII code. This process is costly and time-taking. Also, it requires an sufficient knowledge of hardware and file systems.

Challenges in mobile forensics

Most forensic challenges when it comes to the mobile platform is the fact that data can be accessed, stored, and synchronized across multiple devices. Data is volatile and can be rapidly altered or deleted remotely, more struggle is required for the preservation of this data. Mobile forensics is different from computer forensics and presents unique challenges to forensic investigators.

Law implementation and forensic investigator often struggle to obtain digital evidence from mobile devices. The following are some of the reasons:

- **Hardware differences**: As the mobile landscape is varying with passage of time, it is critical for the investigator to adapt to all the challenges and remain updated on mobile device forensic techniques across various devices.
- **Mobile operating system:** There are several versions of mobile Operating systems which make more difficult the task of forensic investigator.
- **Mobile platform security features**: To protect user data and privacy, Modern mobile platforms contain built-in security features which act as a difficulty during the forensic acquisition and analysis.
- **Anti-forensic techniques**: Modern mobile contain different Anti-forensic techniques like data forgery, data hiding, data complication, and secure wiping, make investigations on digital media more difficult.
- **Dynamic nature of evidence**: Digital evidence may be easily modify and delete either purposely or accidentally. For example, browsing an application on the phone might alter the data stored by that application on the device.

- **Accidental reset**: One of features to reset available in mobile which reset everything. During the examine resetting the device accidentally result, data may be loss.
- **Legal issues**: Mobile devices might be involved in crimes, which can cross geographical limits. In order to tackle these multijurisdictional issues, the forensic investigator should be aware of the nature of the crime and the regional laws.

4. Conclusion

Mobile devices store a variety of data such as SMS, call logs, browser history, chat messages, location details, and so on. Mobile device forensics includes many tactics and ideas that fall outside of the boundaries of traditional digital forensics. High care should be taken while handling the device right from evidence intake phase to archiving phase. Investigators responsible for mobile devices must understand the different acquisition methods and the complexities of handling the data during analysis. Extracting data and information from a mobile device is half the battle. The operating system, security features, and type of mobile device will determine the amount of access you have to the data. It is essential to follow sound forensic practices and make sure that the evidence is unchanged during the investigation.

REFERENCES

[1] Digital Evidence, Investigation Manual, Central Board of Direct Taxes, Department of Revenue, Ministry of Finance, Government of India

[2] https://www.iacpcybercenter.org/officers/mobile-forensics/

[3] d3pakblog.wordpress.com

[4] https://subscription.packtpub.com/book/networking_and_servers/9781788839198/1/ch01lvl1sec11/mobile-forensics

[5] https://resources.infosecinstitute.com/category/computerforensics/introduction/mobile-forensics/common-mobile-forensics-tools-and-techniques/

[6] https://booksite.elsevier.com/9780123742681/Chapter_20_Final.pdf

[7] https://riskpro.co.in/mobile-forensic/