Digital Forensic Examination of Mobile phone Data

Dr. Qamar ul Arafeen[1], Najam ul Arifeen[2], Syed Abdul Khaliq Bari[3], M. S. Shamim Ahmed[4]

[1]Department of Computer Science, University of Karachi, Main University Road, Postal code: 75270,
[2]Department of Computer Science, Federal Urdu University of Arts, Science & Technology, Abdul Haq Campus, Karachi, Pakistan
[3]Department of Computer Science, University of Karachi, Main University Road, Pakistan
[4]Additional Registrar, Academics, Shaheed Zulfiqar Ali University of Law, Karachi, Pakistan

Abstract—*Mobile phones are an integral part of our lives since they have played a vital role in bringing people closer together. They have abundantly been used by people all across the globe as they keep them up-to-date about the happenings in the world. However, these mobile phones have also been used in carrying out various criminal activities for the past few decades, therefore, a new discipline of Mobile Phone Forensics has been introduced which will help a lot in curbing the menace of these crimes by locating the whereabouts of the criminals.*

This research paper deals with the introduction of this innovative discipline of mobile phone forensics by throwing light on the importance of this discipline. It also deals with the detailed procedure of conducting a formal forensics analysis with the help of these mobile phones.

Keywords— Mobile Phones, **Digital Forensic, ACPO.**

I. INTRODUCTION

With the invention of mobile phones in the 21st century our lives have been greatly transformed as the whole world has turned into a global village via this invention. Mobile gadgets have played a very pivotal role in connecting people across the globe. The modern man cannot imagine his life without these tiny devices.

On one hand mobile phones have completely revolutionized our lives by providing us with great services of various kinds 24/7 but on the other hand these gadgets are also being used as a vital source of communication in various crimes by the gruesome criminals. With the help of these devices, it has become easy for the terrorists to carry out their heinous activities during the past few decades. For this purpose, a new and innovative discipline of Forensics Science has been introduced in various institutes in Pakistan and abroad which is hoped to greatly assist in encountering these criminals by locating their crimes and places.

Forensics is the discipline which uses various techniques of identifying, recovering and reconstructing the proof by applying scientific principles to legal facts via an argumentative discourse. The investigative authorities of this discipline carry out the arduous task of reconstructing and extracting the evidences in order to apply them on various cases related to crimes for providing solid proofs and analyzing various facts. Similarly, the discipline of Computer Forensics involves the same process but is applicable only on data taken from digital media sources. Thus, we can define Computer Forensics as the process of preserving, identifying, extracting, documenting and interpreting digital data sources. There are available specific forensic guidelines issued by the UK Association of Chief Police Officers (ACPO) and by the US National Institute of Standards Technology (NIST) to make sure that proper policies and processes have been carried out while presenting the forensic criminal case in the court of law.

Over the past few decades, mobile phones have become a vital part of our lives. These gadgets contain essential personal data and are used for communication purposes across the globe. As these phones contain a larger amount of information and data, therefore they often prove to be very helpful in carrying out various criminal investigations. Mobile Phone Forensics is a very novice and innovative discipline of forensics which is very closely associated with the discipline of Computer Forensics as it is also related with the investigation of digital data resources. The UK and US guidelines charter provided by the ACPO and NIST for the examination of digital forensics data contain certain shortcomings and are not applicable to all cases worldwide. Although both guidelines do provide certain solid advices on conducting a forensic analysis of the mobile phones data, yet they do not address certain specific issues and problems related to mobile phone analysis. Therefore, these

guidelines need certain modifications before one can apply them in all forensic cases across the globe.

II. ANALYZING MOBILE PHONES FORENSIC DATA

The investigators of Digital Forensics need certain tools and equipment to help them in their investigation which make it possible for the examiner to examine the computer hard drive effectively in a forensically feasible manner. The forensic investigator works on a digital image/copy of the hard drive of computers and ensure the fact that this drive is not mutilated in any way. The two important software tools named as Guidance Software's EnCase and Access Data's FTK are used to carry out certain functions which help to maintain the integrity of evidence during the analysis of digital data.

It is a challenging task for the examiner to obtain forensically sound data via a mobile device because these software tools are not currently providing this function. Certain software tools like Micro Systemation's .XACT, Paraben's Phone Seizure and BitPim are continuously facing several problems such as:

- Many software only provide a limited section of the report via the mobile phones.
- Interpreting and reconstructing deleted data is difficult because it is ad-hoc, not complete and not easy to grasp.
- The functions and the operational system of the new gadget that has been launched in the market after every four days does not contain any forensic equipment.
- The original mobile phones on which the forensic investigators work often does not maintain integrity of the evidence. For example, the data written on the device during imaging in mobile forensics is contradictory to computer forensics as in this discipline the investigators work with a copy of the digital data rather than with original data.
- The equipment available for mobile phone forensics has limited functions than the equipment available for computer forensics.
- Computer forensics examiners work with the digital copy of the computer hard drive whereas digital copy is not easily available in case of mobile phone forensics because the mobile phone contains various processing layers including:
    1. Hardware layer containing processor, RAM, ROM, signal antennas and input/output hardware.
    2. Original Equipment Manufacturer Vendor (OEM) layer containing boot loading, configuration files and application layer.
    3. Application layer consisting of Microsoft Office, Internet applications, remote wiping and media player.
- A hard drive is left without any power resource when it is taken out from a computer device. This drive can no longer indulge in any sort of communication, thus keeping its evidential integrity intact for further scrutiny.
- Mobile phone data storage consists of various states which make its working more complex. These states include:
    1. Nascent State: No data has been used by the user (Fresh from Factory)
    2. Active State: Powered on mobile performing various tasks.
    3. Quiescent State: Inactive mobile performing various tasks and keeping the date and time accurately on the device.
    4. Semi Active State: Mobile carrying out the task of performing a function like ringing the alarm bell.
- The major problem that mobile phone forensics examiners have to deal with is the enormous number of mobile devices of different kinds made by various manufacturers. For example, cable connection problems, infrared rays' issue, and the availability and connectivity issues of Bluetooth.

All these problems make the mobile phones forensic analysis difficult and lead to alteration in the data of mobile phones. Therefore, it is necessary for the mobile phone examiner to be fully competent and vigilant so that he can handle these arduous tasks efficiently and effectively.

III. CONCLUSION

In order to curb the crimes carried out via the mobile phones, a novice discipline of Mobile Phone Forensics has been introduced in various disciplines across the globe. With the help of this discipline, it becomes easy for the students of this discipline and the concerned authorities to locate and punish such criminals by eradicating and stopping their plans.

It is now the duty of every citizen of Pakistan to locate such criminal activities and inform the concerned authorities as

soon as possible so that these heinous crimes could be stopped immediately.

REFERENCES

[1] ACPO v4.0: Good Practice Guide for Computer-Based Electronic Evidence Internet, http://www.7safe.com/electronic_evidence/
[2] Phone-Forensics Internet, http://www.phoneforensics.com/forum/showthread.php?t=13948&highlight=paraben
[3] Network Working Group Internet, http://www.ietf.org/rfc/rfc1321.txt
[4] Ramabhadran. R, "Forensic Investigation Process Model for Window Mobile Phones"
[5] McCarthy.P, (2005), Forensic Analysis of Mobile Phones, University of South Australia, Australia.
[6] NIST Publication 800-101: Recommendations of the National Institute of Standards and Technology Internet, http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf
[7] Researcher to Recover Mobile Info http://news.bbc.co.uk/1/hi/wales/7374221.stm
[8] Meet the Regulator | Home Office http://police.homeoffice.gov.uk/operationalpolicing/forensic-science-regulator/about-theregulator/meet-the-regulator/