Asian Journal of Convergence in Technology Volume IV Issue I
ISSN NO: 2350-1146 I.F-5.11

Forensic Case Study: Importance and Used of Multiple Tools in Recovery of Vital Evidences from Mobile Devices

Ms. P. B. Binnar , *DFSL Mumbai*, pranita.sadgir@gmail.com,
Ms. N.G. Sonsale , *DFSL Mumbai* , namrata.sonsale@gmail.com and
V. S. Pawade Assistant Director *DFSL Mumbai.*
pranitasadgir@gmail.com

***Abstract*—Now a day's mobile users are increasing worldwide and crimes related to mobile phones are also increasing. Extraction of important evidence from exhibits is also challenging. Different tools give different results depending on type of extraction it supports.**

In this paper, crime involving smartphone, a real case study is discussed. This paper is mainly focused on extraction of digital evidences which can simplify the task of forensic investigator. The main objective of this paper is to study and compare results of different existing forensic tools such as UFED 4PC, XRY, Oxygen Forensic Analyst. Further how tool helped to recover deleted data traces is discussed.

This case study undertakes practical experiments to identified sources for evidence that can later be used in the judiciary system.

Keywords— Digital evidence, Digital Forensics, mobile forensic, Oxygen Forensic, extraction method, UFED 4PC, XRY, data acquisition.

I. INTRODUCTION

Smartphone is the most common mobile device own by many people to communicate, organize and coordinate tasks with others. The capability and the users of these devices increase each year. Based on statistics from 2007 to 2014, the number of smartphones sold worldwide increased rapidly[1]. Android introduced sophisticated communication services over the internet. This facilitates users of various applications on this platform to exchange text messages, voice calls, audio, video and images and much more. The powerful features and technology available in these devices can also be used by the criminals for crimes such as harassment through text messages, committing fraud over e-mail, trafficking of child pornography, communications related to narcotics, etc. Cyber criminals or the persons with malicious intention may use this kind of service for their personal gain or to disturb the user community[2]. Digital forensics is defined as the analysis of data, such as audio, video etc.. obtained after the examination of electronic devices to help the legal process. Today, with the advancement of technology, electronic devices are diversified such as tablet, flash memory, memory cards. At the same time, the storage capacities of devices are increasing day by day. People use these devices widely in many areas such as facilitating their work and following social environment. When forensics analysis is performed, the data on these devices must be evaluated unchanged and not destroyed [3].

Mobile device forensics is a branch of digital forensics relating to recovery of digital evidence or data from a mobile device under forensically sound conditions. Mobile devices can be used to save several types of personal information such as contacts, photos, calendars and notes, SMS and MMS messages. Smartphones may additionally contains video, email, web browsing information, location information, and social networking messages and contacts. Mobile forensics is a new type of gathering digital evidence where the information is retrieved from a mobile phone. It relies on evidence extraction from the internal memory, External memory and service provider logs of a mobile phone when there is the capability to access data[4].

1.1 Types of evidence

As technology advances, the amount and types of data that can be found on a mobile devices is constantly increasing. Evidence that can be potentially recovered from a mobile phones may come from several different sources, including handset's internal memory, SIM cards, and attached memory cards such as SD cards.

Traditionally mobile phone forensics has been associated with recovering SMS and MMS messaging, as well as call logs, contact lists and phone IMEI/ESN information. However, newer generations of smartphones also include wider varieties of information from web browsing, wireless network settings, geo location information (including geotags contained within image metadata), e-mail and other forms of

rich internet media, including important data such as social networking service posts i.e. facebook and Whatsapp.

1.2 Data acquisition types

Mobile device data extraction can be classified as follows:

a. Logical acquisition

Logical acquisition implies a bit-by-bit copy of logical storage objects that reside on a logical storage. Logical acquisition has the advantage that system data structures are easier for a tool to extract and organize. Logical extraction acquires information from the device using the original equipment manufacturer application programming interface for synchronizing the phone's contents with a personal computer. A logical extraction is generally easier to work with as it does not produce a large binary blob. A logical extraction is the "what you see is what you get" process, the easiest and fastest of all the extractions. It relies upon the device's API (Application Programming Interface) to retrieve data, basically extracting whatever data the manufacturer makes available via API[6].

b. File system acquisition

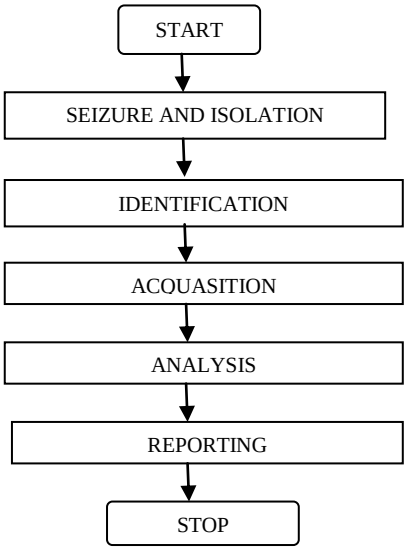
Logical extraction usually does not produce any deleted information, due to it normally being removed from the phone's file system. However, in some cases particularly with platforms built on SQLite, such as IOS and Android the phone may keep a database file of information which does not overwrite the information but simply marks it as deleted and available for later overwriting. In such cases, if the device allows file system access through its synchronization interface, it is possible to recover deleted information. File system extraction is useful for understanding the file structure, web browsing history, or app usage, as well as providing the examiner with the ability to perform an analysis with traditional computer forensic tools. A file system extraction, done on smartphones, goes a bit deeper. It also uses the manufacturer's protocols, though these are different from the API, and are device/family-specific[6].

c. Physical acquisition

Physical acquisition implies a bit-for-bit copy of an entire physical store (e.g. flash memory); therefore, it is the method most similar to the examination of a personal computer. A physical acquisition has the advantage of allowing deleted files and data to be examined. Physical extraction acquires information from the device by direct access to the flash memories. A physical extraction is the most complete (and takes the longest) of all three extractions because it is a bit-for-bit copy of all the data on the device, including data in both allocated and unallocated space on the device's memory. This includes deleted data and metadata[6].

Generally this is harder to achieve because the device original equipment manufacturer needs to secure against arbitrary reading of memory; therefore, a device may be locked to a certain operator. To get around this security, mobile forensics tool vendors often develop their own boot loaders, enabling the forensic tool to access the memory (and often, also to bypass user PIN locks or pattern locks).

II. BASIC DIGITAL FORENSIC INVESTIGATION PROCESS:



The basic digital forensic investigation process is as shown in flowchart.

SEIZRE:- Prior to the actual examination digital media will be seized. In criminal cases this will often be performed by law enforcement personnel trained as technicians to ensure the preservation of evidence.
IDENTIFICATION:- This phase whereby the tasks to identify the digital components from the acquired evidence and converting it to the format understood by human[5].
AQUASITION:- Forensic duplicate of the media is created, usually via a write blocking device, a process referred to as Imaging or Acquisition. The duplicate is created using a hard-drive duplicator or software imaging tools. In Acquisition phase, evidence is acquire in acceptable manner with proper approval from authority[5].
ANALYSIS:- After acquisition the contents of image files are analyzed to identify evidence that either supports or contradicts a hypothesis or for signs of tampering. During the analysis an investigator usually recovers evidence material using a number of different methodologies and tools, often beginning with recovery of deleted material.
REPORTING:- When an investigation is completed the information is often reported in a form suitable for non-technical individuals. Reports may also include audit information and other meta-documentation. In the final phase, the acquired & extracted evidence is presented in the court of law[5].

III. MOBILE FORENSIC TOOLS:

Different software tools are available to retrieve and analyze smartphone data. Each tool has its set of advantages and limitations. These tools are essential for smartphone forensics to extract digital evidence that can be later used in a legal case. There are several computer forensic tools both in the commercial and the open domain. The commonly used forensic toolkits are:

- XRY
- Oxygen Forensic
- UFED 4PC

XRY is a powerful, intuitive and efficient software application that runs on the Windows operating system. It lets you securely extract more high-quality data in less time than ever before, while at all times fully maintaining the integrity of the evidence[7].

Oxygen Forensic is forensic software for data acquisition from mobile devices, their backups and images, memory cards, SIM cards and cloud storages. The program has played a significant role in criminal and other investigations all over the world and is used by Law Enforcement units, Police Departments, army, customs and tax services and other government authorities[8].

UFED 4PC is a new generation application that empowers law enforcement, military, intelligence, corporate security, and e-discovery personnel to capture critical forensic evidence from all mobile devices. This includes mobile phones, handheld tablets, portable GPS devices, and devices manufactured with Chinese chipsets[9].

IV. CASE STUDY SOLVE USING FORENSIC TOOLS:

Evidence collection from Smartphone is very crucial. Extracting data, preserving them, building hypothesis and presenting digital evidences can all aid in solving legal cases. In this paper, a real legal case of Assault from a village is considered. A hypothesis will be established and three different software tools will be used to simulate data extraction to help solve a legal case.

Incident Summary:

A Department(P) received a complaint explaining an incident of intentional insulting or assaulting a boy with intent to dishonor him and voluntarily causing hurt by dangerous weapons by group of people in a village. This incidence was shoot with mobile phone camera. The video was send to some other mobile phone and deleted from phones internal memory. The video was saved in Compact Disk and distributed. This CD and mobile phone were submitted for forensic analysis in an Organization (Q). The mobile phone used in this case was SONY XPERIA running on android 4.4.4 operating system. The investigator were searching for the video which was shoot on dated 13-03-2015. To carry out digital forensics some popular tools available are Cellebrite UFED 4PC, XRY, Oxygen Forensic. Organization (Q) used these tools for searching the video. The video was deleted from mobile phone and memory card was not submitted for analysis. So forensics experts were trying to find some traces of video in database files if available.

When forensic experts extract mobile phone using UFED 4PC and XRY only logical data was extracted but with Oxygen forensic physical extraction was possible. In report generated by Oxygen forensic experts find traces of the reference video given in CD for mentioned date in database file of Mobile's Bluetooth folder. *Result of Analysis:*

Video trace of mentioned date was found which is highlighted in Fig.1. In this image investigators found information about database file, target, timestamp and title. The MAC address of target mobile phone to which video was send also found in Bluetooth folder.

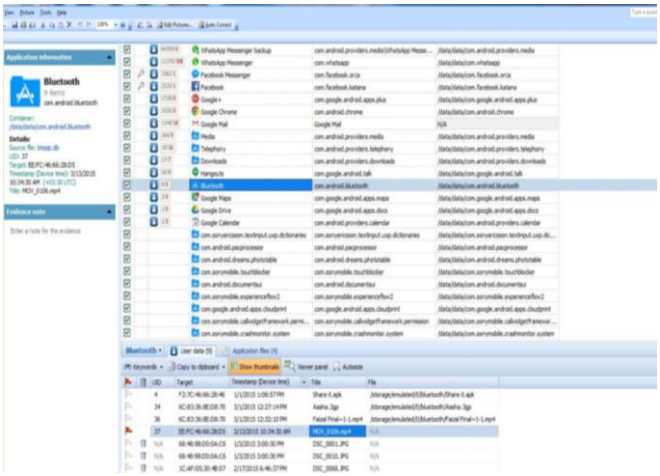


Fig. 1: Trace of the video communicated through Bluetooth to target.

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
   <string name="BC:D1:D3:76:EF:AA">Micromax
A108</string>
   <string name="8C:77:12:B8:2E:9C">GT-
B7722</string>
   <string name="1C:AF:05:30:4B:07">Guru</string>
   <string name="68:48:98:D0:0A:C6">C.K.Grand
2</string>
   <string name="EE:FC:46:66:28:D5">Aqua I-5</string>
   <string name="68:48:98:C0:F8:99">GT-S7392</string>
</map>
```

Fig. 2 :-Trace of Target name found in XML database file.

MAC address found in Fig. 1 was matched with MAC address of target mobile phone found in database file of Bluetooth which is highlighted in Fig. 2. From this investigators got name of target mobile phone i.e. Aqua I-5 to which video was send.

When extraction of mobile phone using oxygen is completed, forensics experts try to search reference video in it but video was deleted and only thumbnail of video frame was recovered which is shown in Fig. 3 with object information. The object information includes name, type, size, status, hash value and location.

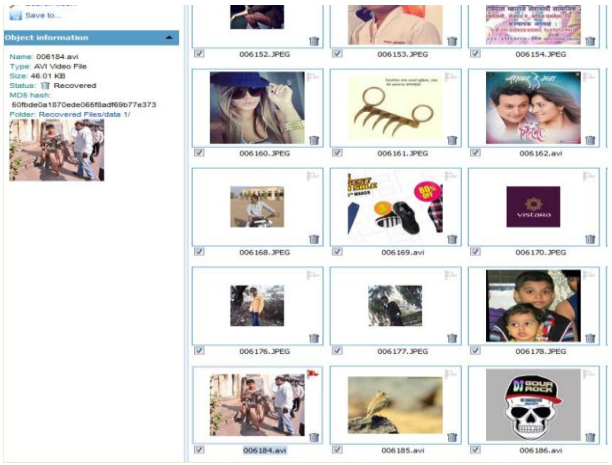


Fig. 3:- Thumbnail of Recovered video frame

V. COMPARATIVE STUDY OF ANALYSIS:

Forensics experts acquire the mobile phone using UFED 4PC, XRY and Oxygen forensics whose comparative result is shown in following table.

TABLE 1 Comparative Results

Parameters	UFED 4PC	XRY	OXY
Device / Network Information	√	√	√
Device / Event Log	√	√	√
Device / Installed Apps	×	√	√
Device / Accounts	×	√	√
Contacts	√	√	√
Calls	√	√	√
Messages / SMS	√	√	√
Messages / MMS	×	√	√
Locations / History	×	√	√
Web / History / Searches	×	√	√
Files / Pictures	√	√	√
Files / Audio	√	√	√
Files / Videos	√	√	√
Files / Documents	×	√	√
Files / Databases	×	√	√
Timeline	×	×	√
WiFi / Bluetooth Connections	×	×	√
WhatsApp Messenger	×	×	√
Facebook Messenger	×	×	√

VI. CONCLUSION:

Method used for forensic analysis should be conducted in accordance with appropriate guidelines, particularly for a case depending on data requirement from evidence. The analysis of the Mobile Phone should be carried out using suitable mobile forensic software tools such as Oxygen Forensic Analyst, XRY and UFED 4PC within a controlled environment while ensuring that evidential and continuity of evidence is maintained. This paper explains overview of tools and methods for forensic data extraction from evidence, basic forensic investigation process, and a real case study is discussed. In this paper results of three tools are compared and result of deleted data traces using better tool is shown.

References

[1] Normaziah A. Aziz, Fakhrulrazi Mokhti, M. Nadhar M. Nozri, " Mobile Device Forensics: Extracting and Analysing Data from an Android-Based Smartphone, ", International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec), Jakarta, Indonesia. 29-31 Oct. 2015. ISBN: 978-1-4673-8499-5.

[2] V. Venkateswara Rao, A.S.N Chakravarthy, "Forensic Analysis of android mobile devices", International Conference on Recent Advances and Innovations in Engineering (ICRAIE), Jaipur, India, Dec.2016.

[3] Sengul Dogan, Erhan Akbal, "Analysis of mobile phones in digital forensics" International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia , May 2017.

[4] Mubarak Al-Hadadi and Ali AlShidhani, " Smartphone Forensics Analysis: A Case Study ", International Journal of Computer and Electrical Engineering, Vol. 5, No. 6, December 2013.

[5] Yunus Yusoff, Roslan Ismail and Zainuddin Hassan,"Comman Phases of Computer Forensics Investigations Model", International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 3, June 2011.

[6] Monique Ferraro (2014) [Online] Available: http://www.law.com/sites/moniqueferraro/2014/07/20/cellebrite-mobile-forensics-tool-q-a/.

[7] (2017) The XRY website. [online] https://www.msab.com/products/xry/

[8] (2017) The Oxygen-Forensic website. [online] https://www.oxygen-forensic.com/download/articles/

[9] (2015) The cellebrite website [online] Available: http://www.mcsira.com/WEB/8888/NSF/Web/3128/UFED/