Comparative analysis of mobile forensic proprietary tools: an application in forensic investigation

Parth Chauhan1*, Tamanna Jaitly2 and Animesh Kumar Agrawal1

1School of Digital Forensic Sciences, NICFS, NFSU (Delhi Campus), Ministry of Home Affairs, Govt. of India
2School of Forensic Sciences, NICFS, NFSU (Delhi Campus), Ministry of Home Affairs, Govt. of India

Abstract

The utilization of the Internet and wireless communication reaches its pinnacle from one side of the planet to the other. Marking the rise of criminal activity in recent years sees enormous growth in security breaches and data theft-related cases in mobile phones. To mitigate them, the implementation of security patches, safety fixes, and updates in mobile devices is of high priority for the organization. The need to foster techniques and procedures in the field to be able to extract and precisely dissect digital crime cases, providing valuable tactical data about the investigation. Mobile forensics is a developing branch assisting the investigator in criminal trials and investigations. Acquisition, Collection, and Analysis of mobile phones settle the purpose of recovering cumulative and corroborative evidence. Upgradation and innovation of mobile devices with time posed a challenge to mobile forensic technology to extract information from such devices. The study aims at extracting comparative and statistical approaches in the analysis of Physical data acquisition utilizing significant versatile mobile criminological proprietary tools. The proposed study also introduces newly developed utility tools along with their characteristic features which help in successful data extraction from mobile devices.

Introduction

Considering the upward trajectory in urbanization results in a remarkable increase in world population crossing 7.91 billion with augmentation of cyberspace to approximately 4.95 billion as per Digital 2022 Global Overview Report. As the number of users increases day by day, the amount of data generated from mobile devices is at high-security risk. Internet activity focus contributes over 5.31 billion and estimates 67.1% of the total population employs smartphones till Jan 2022. Demographical data manifests 4.62 billion of the total population as dynamic web-based media clients which gauge 58.4% till Jan 2022 [1]. Moderation techniques and strides to these unavoidable dangers paves a way for steady data assurance. Certain Smartphone Industries are looking to mitigate these risks by implementing security patches and updates regularly

the Indian smartphone market is pacing upward and reaches 150 Million in 2020 and will increase to 11% with 167 - 168 Million in 2020 with a high prediction of 187 - 190 million market pace in 2022 [1]. This produces a challenge to the forensic investigator to extract useful data from the suspected user’s mobile devices for criminal investigation and trial purposes. Another challenge [2] in mobile forensics is the Boot loop during data extraction which is the device freezing on the startup screen and does not start further, mostly when using a noncompatible mobile forensic tool or the operating system for extraction and acquisition [3]. The scientific process of acquisition, extraction, analysis, and presentation of mobile devices and related evidence in a forensically sound condition is known as Mobile forensics. Mainly [2] mobile forensic tools work on Logical, Physical, and File system acquisition. The application of these acquisition methods mainly depends on the operating system of Mobile devices and the functionality of the tools. The [2] investigator must have an idea about the make & model along with the operating system and its security patch level before choosing any tool for smooth evidence collection for the mobile device. Much research conducted on techniques of data extraction from different mobile devices using open-source and proprietary mobile forensic tools which are now conclusively implemented in forensic labs for extraction purposes. Rusydi Umar, et al. [3] conducted forensic analysis on the WhatsApp application database having
.crypt12 encryption using Belkasoft Evidence (Trial version) and WhatsApp Key/DB Extractor in which Whatsapp key/DB Extractor gave better results in extracting text messages while Belkasoft Evidence gave much better results in extracting the media & documents.

Oluwafemi Osho, et al. [4] conducted an evaluation of mobile forensic tools including AccessData FTK, EnCase, MOBILedlit Forensic Express and Oxygen Forensic Suite on two mobile devices named HTC Desire 300 with android v4.1.2 and Samsung Galaxy GT-S5300 android v2.3.5 focusing on the recovery of deleted data. They concluded that FTK and EnCase are better in recovery than MOBILedlit and Oxygen Forensic Suite. Not only WhatsApp applications, but a previous study [5] was also conducted on forensic analysis of fitness applications in mobile devices using Android Studio and DB browser by manual acquisition. The manual acquisition technique [2] is least considerable due to the fact that the artifact can tamper with while handling the mobile evidence directly. In place of Manual acquisition being considered first [2]. Logical and Physical acquisition is preferable by many forensic laboratories all over the world [6]. The reference study conducted forensic data extraction of five social networking apps using MAGNET AXIOM and MSAB-XRY in three conditions mainly before data deletion, some data deletion from the app, and after uninstallation of the app. The study used logical data acquisition techniques for investigation.

This paper discusses the [7] physical acquisition of an isolated sample mobile device using proprietary tools and the comparative analysis of the recovered artifacts. The study focuses on the practical performance of proprietary tools [8] by testing the artifacts recovery method and its overall features from the acquisition till report generation.

**Methodology**

The experiment was partitioned into stages: experimental setup of sample mobile device; acquisition of sample mobile device using three forensic proprietary tools for artifacts gathering and recovery and comparative result generation from the analysis of artifacts recovered from all three forensic tools. As per the current extraction types, generally, extraction is of three types Physical, Logical, and File system. On the other hand, cloud-based extractions can be performed on a separate basis as the data backup resides on cloud storage which has to be exported using token generation and session IDs Image 1.

The sample mobile device was procured (Table 1) and tested in front of laymen with his consent. Note that the SIM was not part of the experimental setup with the intention to narrow down the study. The physical dump is collected by the acquisition of internal and cloud storage only taking into account that SIM would not give much information as compared to the information stored in the social media database, internal storage media, and cloud.

Logical extraction may not require physically connecting the mobile device in order to extract the data. Such extraction works on the principle of injection of the third-party application which collects the on-device data. The injection of such third-party applications can either be by connecting the device with OTG or using wireless bandwidth. While in the case of iOS Technology, the older version can be partial jailbreak using the vulnerability engagement in the device.

The system and software information is rechecked online for custom ROM installation [9] by providing an IMEI number at https://www.imei.info/. The compatibility of the Sample mobile device is checked before the acquisition using the [10,11] in-built support of manuals of all three mobile forensic tools [2,12]. The mobile used for testing purposes is checked with the latest android version and security patch level to correctly examine the analytical performance of Forensic tools which helps forensic experts for further analysis in forensic laboratories.

Step one is to isolate the mobile device by enabling Flight mode or Airplane mode [13]. Along with this, enable the developer option and check the stay awake option to prevent the screen from locking [13].

The mobile forensic proprietary tools used for the experimental study are shown in Table 2.

Staging towards the acquisition part after completing the experimental setup of the sample device, the mobile device is now connected to the particular tool at a time for the data collection using physical acquisition [2,14]. To complete the step of acquisition, a mobile device is necessary to put in download mode (Image 2).

<p>| Table 2: Mobile forensic tools with their version used in an experimental study. |
|---------------------------------|------------------|</p>
<table>
<thead>
<tr>
<th>Tool Used</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 MSAB-XRY</td>
<td>10.0.0</td>
</tr>
<tr>
<td>2 Cellebrite UFED4PC</td>
<td>7.50.0.137</td>
</tr>
<tr>
<td>3 Oxygen Forensic Detective</td>
<td>13.6.0.47</td>
</tr>
</tbody>
</table>
The mobile phone is made pattern locked with 8 keys in pattern as “729513486” so to check whether these tools were able to bypass or crack the pattern lock and the type of technique they adopt [13] Image 3.

A special booting mode specifically made by Samsung for certified repair technicians to get the root access privilege and debug the system easily for easy maintenance, software, and firmware updates along with recovery of data [13,15,16] Images 4-6.

Results and discussion

The objective of this study is fulfilled by examining the working performance of mobile forensic proprietary tools using Physical acquisition [17-20] with a major focus on the recovery of deleted artifacts. The artifacts collected from the examination using different tools are shown in Tables 3,4.
For dead devices, chipset-based extraction is performed in order to get the physical dump of data. Along with this method, the device was turned into a suitable mode by pressing certain keys which make the tool perform the exploit. However, the chances of getting more amount of deleted data are higher in the case of extraction of the rooted device as compared to the non-rooted one. In order to get the deleted data by physical extraction, the device was made into flashed and made into partial root mode which is called download mode or Emergency Download mode (EDL).

The study highlighted the data extraction using Download mode [13,15,16] which is specifically built for technical support and maintenance in Samsung smartphones. Other factors were also considered for the proper analysis of tools as shown in Table 5.
Conclusion

Data is another challenging task for law enforcement agencies to acquire from cloud-based applications. Capturing evidence from mobile devices, particularly social messaging applications, is more challenging compared to other artifacts. The extraction of artifacts from the latest Android and iOS smartphone modules requires the use of updated tools. Mobile Forensics tools need to be updated with the latest features and capabilities. Comparative analysis of mobile forensic proprietary tools has shown that as we move forward in the development of smartphones, the challenge of unlocking these devices becomes more pronounced.

References

2. Lahesoo P, Mäses S. Forensic Traces of Messaging Applications on Android and iOS Mobile phones.
17. Tajuddin TB, Abd Manaf A. Forensic investigation and analysis on digital evidence discovery through physical acquisition on the

