Mobile device forensics

Asia ALJAHDALI, Nawal ALSAIDI, Maram ALSAFRI, Afnan ALSULAMI, Turkia ALMUTAIRI

College of Computer Science and Engineering, Cybersecurity department,
University of Jeddah, Saudi Arabia

aoaljahdali@uj.edu.sa, nrajealsaidi.stu@uj.edu.sa, malsafri0002.stu@uj.edu.sa,
aalsulami1200.stu@uj.edu.sa, talmotairi0030.stu@uj.edu.sa

Abstract: Globally, the wide-range deployment of smartphones culminated in the expanded collection and sharing of massive amount of data that could be utilized in a forensic investigation as digital evidence. Thus, the mobile industry continues to grow, there is an increase in the probability of its usage in criminal activity. Smartphones are often equipped with a broad variety of applications, emerging technologies and operating systems. Therefore, extracting evidence from a smartphone is difficult for a criminal investigator. To gather relevant evidence, forensic analysis of smartphones and a solid knowledge of forensic tools and their functionality is needed. This study addresses the investigation processes for mobile forensics. The paper presents tools used in investigating smartphone device and the limitations in utilizing forensic techniques. The purpose of this paper is to help investigators to develop further methods to examine all the artifacts for researchers, especially the trial version.

Keywords: Mobile forensics, investigation process, forensic tools.

1. Introduction

Today, smartphones have been more efficient and popular with reduced costs in the production and development of hardware technology (e.g. sensors / processors) and software systems (e.g. Android, IOS). Mobile device forensics is the study of digital evidence recovers in forensic terminology. Forensic investigators can recognize mobile storage locations such as subscriber identification module (SIM), mobile memory, external memory card and networking provider (NSP) with evidence of interest (Naja, 2007). In contrast to computer hard disk extraction techniques, the techniques used to remove the evidence from smartphones are quite different (Garfinkel, 2010). Smart mobile phones utilize a range of operating systems and file structures and file types that are distinct from traditional computers. Since these handheld devices are being used more often, the hacking issue has extended to these devices. Now, every day, hackers probably attack these resources for other mobiles or computers. For such devices, therefore, forensic tools and computers are needed. Compared to the rise in mobile technology, there is relatively little development in automated forensic resources accessible on mobile devices. The usage of handheld forensic devices has two important factors need to be considered, the condition of the system at the moment of acquisition, and the radio isolation. Once the examiners are separated from the power supply because of data in the non-volatile memory, a static analysis may be rendered on a general device and even the existing state of the machine is preserved. Yet that is not feasible on handheld phones, because even the main evidence can be retrieved from fragmented memory until the system is shut off. Moreover, the other aspect which only made live acquisition for mobile devices possible was the locks or passwords disabled when the device was restarted. Another issue is the advancement of mobile technologies, so various solutions were introduced, rendering it very challenging to implement mobile forensic tools (Lokhande & Meshram, 2015).

The remainder of the paper is structured as follows. Section 2 presents a background for the current state-of-the-art in mobile forensic. Section 3 presents forensic techniques used by the investigators to extract required data. Section 4 describes Android and IOS forensic tools. Section 5 discusses anit-forensic tequnichs that would face forensic investigators during the investegation process. The current challenges in mobile forensic is discussed in section 6. Afterword, a study case on one of the forensic tools is presented. Finally, a comparison between IOS and Android forensic tools is presented and discussed.

https://doi.org/10.33436/v31i3y202107

2. Background

This section presents a background for the current state-of-the-art in mobile forensics. Initially, the authors

propose a reference scenario incorporating contemporary aspects. Then, the investigation process of mobile forensic is elaborated. Afterward, data acquisition techniques are presented.

2.1. Mobile forensic process

Mobile forensics are a subpart of the broader field of digital forensics focusing on getting data from a mobile device in order to investigate it (Mchatta, 2018). It is known as the method to analyse the data to collect the evidence linked with the crime. The core of analysing the mobile phone to detect the crime is to analyse the internal and external memory and SIM card in mobile phone. The process of mobile forensics can be summarized into four phases: seizure, acquisition, analysis and reporting (Nelson et al., 2014).

Phaes1: *Seizure*. The law enforcement personnel who are trained to be technicians, is the one who seizes the suspect device in order to preserve the evidence in a criminal state. The majority of private companies have the ability to investigate their own equipment without a warrant. Seizure phase plays an important role in digital forensics, especially in mobile forensics, because the investigators can collect the evidence and preserve the device in the original state. Hence, the main purpose of this stage is to preserve the evidence. When the mobile devices are seized, there should not be any change in the evidences, this means to cut off all the wireless networks. So, if failure occur in this phase, it will affect immediately all other stages (Nelson et al., 2014).

Phase2: *Acquisition.* The process of duplicating the media after the seizure stage is called acquisition. The duplicate can be created using software imaging tools. After that, the original drive will be restored to secure storage to prevent any tampering which may happen during acquisition phase. The duplication will be verified through the SHA-1 or MD5 hash functions. The most crucial part is when the media is verified again during the analysis to insure that the evidence is in the original state. This phase is responsible for choosing the suitable method for analysing and it begins once the investigators receive the device after preservation and they identify the model and type of the received device. So, the challenge in this phase is choosing the right tools because there are many devices available on the market (Nelson et al., 2014).

Phase3: *Analysis.* This phase starts after the acquisition of the media which is going to be analysed to identify the evidence. In this phase, the examiners need to identify the type of mobile device, type of network, carrier and service provider. Despite the diversity of mobile devices, there is no ideal solution for analysing. But AccesssData and SleuthKit are some of the forensic tools which can analyse the data. In general, there are many techniques to analyse the data including that from unallocated space, accessible disk space or cache files in the operating system. Usually, the investigator uses these techniques and types some keywords to search within acquired image files to see whether there is a match. To clarify, the examiners use forensic tools that support hash signatures to identify remarkable files. When an acquired image file is hashed, it will be compared with pre-compiled lists. For example, hashed acquired data has The Reference Data Set which will be compared with The National Software Reference Library. After recovering the evidence, the information will be analysed by the investigator. At the end, the forensic investigator should ensure that the results are accurate (Nelson er al., 2014).

Phase4: *Reporting. The* reporting phase represents the incomes of the previous phase. Generally, there are different desired results based on each case and the investigators should take this into account when they present collected data. The examiners should report the investigated information in an easily understandable for any individual. After completing the investigation, the report passes to the commissions to decide regarding the evidence (Nelson et al., 2014).

2.2. Data acquisition techniques

Generally, data acquisition refers to the procedure used in sampling signals that measure physical conditions as well as converting the results from the digital numeric values. The values should therefore be capable of being manipulated by the computer. In most cases, data acquisition techniques are controlled through the application of the software programs that are established by the use of programming languages like C and C++. Besides, open-source software can be used to provide necessary tools for acquiring data from different hardware equipment. These tools are considered to be flexible, adaptable, and fast in relation to accessing the data. In NIST's Special Publication 800-101 Revision 1, Rick Ayers et al. (Introducing KAPE, 2019) proposed a framework for forensic examiners to compare forensic extraction techniques used by different tools to acquire data, see Figure 1. Forensic investigators may therefore accurately identify and analyze techniques of retrieval, recognizing the equipment limits of each layer.

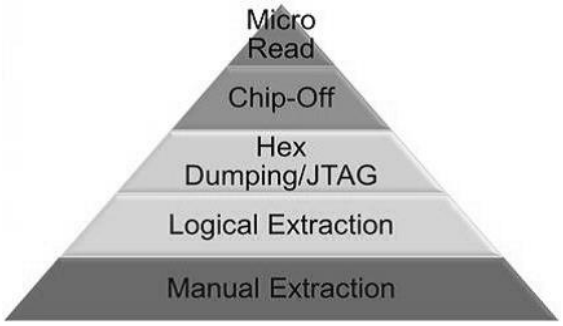

Figure 1. Forensic Extraction Techniques for Data Acquisition

Manual Acquisition. Manual Extraction includes the rendering and documenting of data information processed on a mobile device. This technique does not restore lost data but makes a list of specific displays and user interfaces. This technique is time-intensive and relies on the working state of the system.

Logical Acquisition. This means retrieving the user files via phone and Computer connection through a data cable or Bluetooth and gather evidence through accessible forensic devices. It is fast, simple and trustworthy. Some applications do support a wide range of usable languages and functions such as reporting.

Physical Extraction. Static acquisition of a mobile app file system is also known as the Hex dump analysis. Throughout this type of acquisition analysis, the mobile device connects through the cable or removes cards from the unit and clones the whole directory to retrieve data. Data collected through this technique should be transformed into a raw format and converted into a binary format by using the tool.

Chip-Off. The technique consists of reading the memory using a similar phone or EEprom reader, by removing the chip from the device, and analysing all data retrieved from mobile memory. This technique is efficient but costly.

Micro Read. It is a technique which uses a high-performance electronic microscope to provide physical visibility of the gates on mobile device's electronic chips. Through This technique data can still be retrieved from chemically compromised chips but it is still very expensive. We need to also retrieve the deleted data for full forensic analysis of a mobile device such that both logical acquisition and physical acquisition are needed (KAPE Documenation, n.d.)

3. Mobile forensic techniques for data extraction

The security level in the smartphone is an important aspect as it relates to access to personal information by unauthorized users. Data extraction is the process that entails data retrieval from a smartphone or any other device. Based on this, there are various techniques that are used in extracting data from the smartphones which comprises the following:

Manual data extraction techniques; manual data extraction allows users to have direct interaction with the smartphone user interface. Therefore, users can clearly scroll through the phone and access any document that is considered to be of interest (Sun et al., 2015). Therefore, the data is uncovered by clicking the call log, scanning photos, sorting the data, looking at the history of the web browser, and reading text messages using of third-party applications such as Facebook. Generally, the application of manual data extraction is relatively easy and quick as it is reliable in scanning any required document in the android device.

Logical data extraction technique; this technique helps in providing an in-depth data analysis and can be used in separating any data contained in the Android device.Mainly, this technique involves establishing either a wireless or wired connection between forensic workstation and devices to access the phone's file system as well as retrieving copies that can be used in data back-up. In the utilization of an android device, root access is essential especially when planning to use logical acquisition in data extraction.

File system extraction technique; the file system is used in a situation when the user intends to access a certain file on the internal memory of the mobile with the use of API's associated with each type of the data. This type of extractions is commonly used as the major forensic tool required in retrieving data files from the internal memory like system files, database files, and logs. This technique is effective in examining the web browsing history, app usage, and file structure in mobile device history.

3.1. Mobile forensic evidence

Modern mobile devices including smartphones provide a wealth of knowledge that may be useful. Much of this material is getting more unpredictable, and so live forensics are always required before you can use forensic machine approaches in isolation. Based on the device's working state in some cases, more technical data may be obtained throughout the network. Some examples of relevant forensic data are presented below on a mobile system (Horsman, 2018).

Table 1: Mobile forensic evidence

Mobile evidence types
1. Outgoing, Incoming, missed call history - Call detail records ("CDRs")
2. Phonebook or contact lists
3. SMS text, multimedia messaging content and application based
4. Pictures, audio, videos, files and sometimes voicemail messages
5. Internet browsing history, cookies, content, analytics information, search history
6. Calendar entries, To-do lists, ringtones, notes, memos (notes)
7. Documents, presentation files, spreadsheets and other user-created data
8. Passwords, swipe codes, passcodes, user account credentials
9. Historical geolocation data, Wi-Fi connection information, cell phone tower related location data
10. Data from various installed apps
11. User dictionary content
12. Deleted data from all the above
13. System files, error messages, usage logs, among others.

For certain instances, data from cloud storage of applications may even be retrieved if sufficient security information are present. The following methodologies are used for deciding the geographical position of the app or its user (Arshad et al., 2018):

1. GPS: Satellite Global Positioning System (GPS) is used to assess mobile spot. [Note that the Fed (FCC) E911 legislation include the monitoring of 911 calls by the telephone carrier]
2. Triangulation: The smartphone's positioning can be approximated using three mobile towers in the area.
3. Wireless LAN: Smartphone will monitor Wi-Fi network links even though the GPS has been disabled.
4. Ping: Ping for hardware with mobile number by service provider.
5. Rebel tower (Stingray): Rouge devices cell tower apps will allow smartphones believe they are the provider of services.

Because the usage of devices has become omnipresent in our everyday lives and in our careers, they play a significant role in piracy of IP and other crimes. Although electronic forensics is nearly commonplace, the forensic of smartphones is changing, providing automated forensic examiners with a range of challenges (Pallagani, 2015).

4. Mobile device forensic tools

Due to the increased number of mobile devices, changing in the technology becomes the most complicated issue in the investigation process. Experts may use forensic tools that might be incompatible with the device, so they need to keep up with the latest mobile devices and improving their forensic tool (Mchatta, 2018). This could be a challenge to the investigator which will be discussed in section 7. In investigating a smartphone, the first thing to check is the operating system to see whether it is compatible with the tool or not. In this section, we will introduce mobile forensic tools for both IOS and Android platforms, separately.

4.1. Android dorensic tools

In this part, we will discuss forensics tools of Android, which are used in extraction of evidence from a mobile device's internal memory and getting data. It focuses on identifying data, recording, extracting and examining according to digital forensic standards. Forensics various software tools are available to extract and analyse details on smartphones. Each has a combination of advantages and limitations (Alvarez, 2004).

The label Android image is defined as the physical image that is obtained by performing either of the methods of physical data extraction (also called a forensic image or raw image).

There are many tools used for every mobile app in computer forensics. It should be stressed that all such tools are classified into two types:

- Tools that are not installed on the mobile device. Typically, this software is installed on the computer and displays images of mobile devices participating in this investigation.
- Tools that are installed directly on the mobile device (app) like EaseUS MobiSaver. Such tools are not the same features as the desktop app. This involves apps like Data Recovery, SMS Backups and Recover, etc.

Here, we will focus on the first type including well-known tools such as Oxygen, MOBILedit and Autopsy Forensic. The some of them are commercial and free forensic tools (Beard, 2017).

Oxygen Forensic

Oxygen tool allows reading information from phones including basic phone information, SIM card data, contact list, and reading caller groups and log reports (Missed calls, outgoing calls, and incoming calls), SMS messages, MMS messages, emails, scheduled calendar events, to-do list, text notes, pictures, video files, audio files, Java files, and other files saved in the phone memory or on the memory card snd audio recordings etc.

Investigators can access pre-coordinates, IP addresses, MAC addresses, and credit card numbers. It has the ability to decode and display encrypted applications, noting that this program has full support for Unicode codes, so that it can be read even in Arabic and other languages with Unicode coding in order for the information to be shown correctly. There are more than 500 mobile phone models that are supported by this program. And the list continues to grow rapidly. Oxygen forensic has built-in Social Graph which offers a simple system for exploring social connections between the owners of a phone and their contacts or between multiple devices (CyberRisk Alliance, 2016). Using the Social Graph, aim is to investigate the nearest contacts of device owners. It has the ability to create a Main Evidence area that shows all documents that were bookmarked by the investigator in other pages (Beard, 2017).

Autopsy

Autopsy tool is used to analyze and extract data from Android image files. The tool performs an analysis on the criminal's mobile system so that the digital investigator takes a copy of the accused's system using tools such as the dd tool, (see Figure 2) and then uses the Autopsy tool to perform the analysis. By forensically examining a given amount, Autopsy shows the findings and thus allows investigators to concentrate on specific parts of the data. Using Autopsy, an Android image obtained after physical extraction can be loaded and analyzed. That means in Android data extraction techniques, we can image the full /data / data block or any specific frame that is useful to the investigation, after obtaining the image, an investigator can manually go through the contents and take advantage of the available resources to parse through the contents. It has the ability to analyze call logs, contacts, messages, PS from the browser and Google Maps. Autopsy offers case management capabilities, image integrity checking, keyword search and other automated activities. This tool is used to analyze the items of folders, including lost files by analyzing the file contents; it has the ability to derive parts of files in ASCII or hex format, to track the time series of events set of access time and changes to the application. Autopsy allows you to access the information in the file system of every metadata structure and to retrieve deleted material or carving files to record actions (Alvarez, 2004).

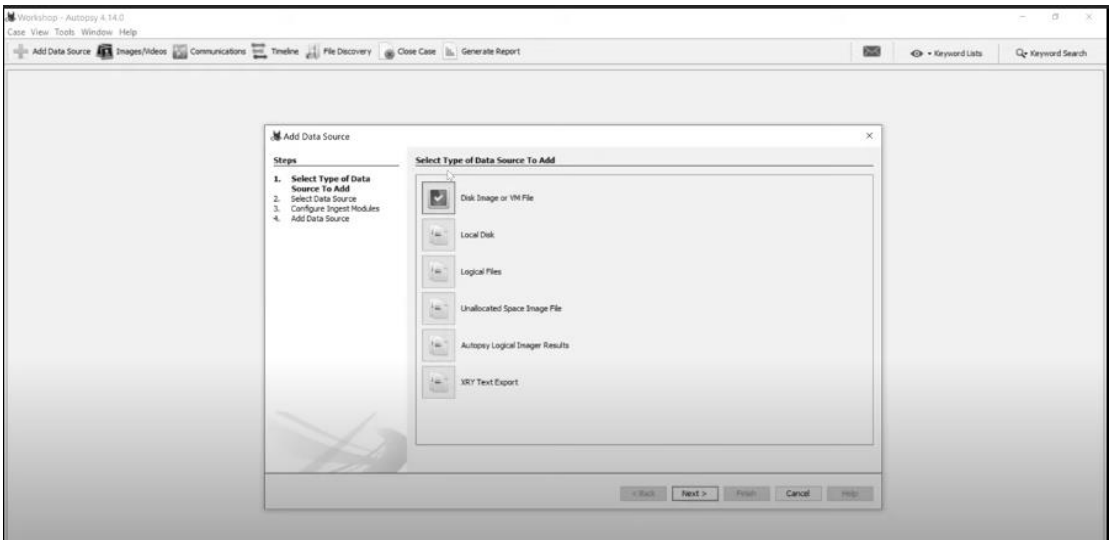

Figure 2. Image the Data Source Using Autopsy (Alvarez, 2004)

MOBILedit

MOBILedit is a logical data acquisition tool for gathering evidence and one of the popular programs with a complete range of tools to extract and analyze smartphone data and information. After the connection has been established, it will show up and give you all the information about the conncted phone like serial number, IMEI, IMSI, ICCID, root status and the operator actual phone number (see Figure 3). Also, it tells how much battery is left on the phone, how much physical memory is on the actual phone, the memory on the SD card and it also shows you the signal on the actual phone. It has the ablility to retrieve from Android devices the accurate location

data. GPS detailed location data can also be provided through application analysis. Mobiledit can collect all the phone contacts whether from facebook or from Google email. It also saves the last 500 missed calls so you can view them all and you can see what number called you as well as the date and time of the call. That's actually the same amount of numbers that your phone itself saves on the actual phone, that means it has the ability to analyze phonebooks, last dialed numbers, missed calls, incoming calls, SMS messages, drafts, multimedia communications, pictures, data ,sound recordings, calendar, other important tasks, notes, files, folders and others . In the Files folder, we can view all different files that are on the phone. At the same time, it allows browsing all the folders that were on the SD card such as applications like Instagram - including images posted on Instagram. It also has the ability to show download images that are saved into SD as adobe reader (PDF) file (DeGrazia, 2019).

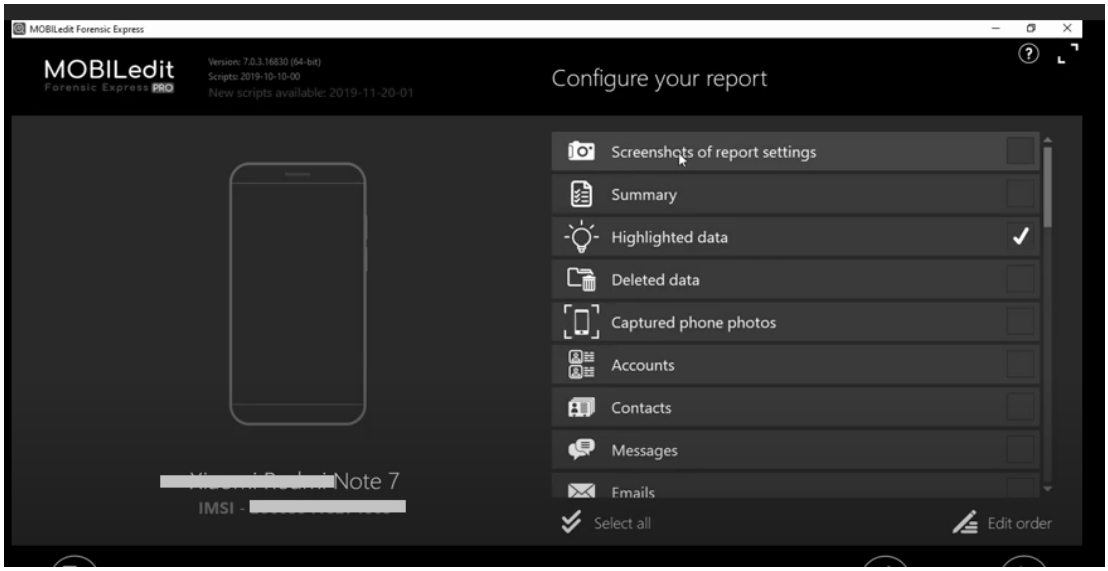

Figure 3. Phone content extracted by MOBILedit (DeGrazia, 2019)

4.2. iOS Forensic tools

Mobile phones are nowadays a target for crime by stealing information and analysing data. Investigation can be done by using tools that ensure the integrity of the evidence. In 2007, Apple made the most effective development in building applications that assist in the investigation and preservation of forensic evidence (Dot C Technologies. ProDiscover Forensics, 2019). iOS devices keep their information secure through a strong protection by encrypting the device's passcode, this would prevent accessing the information by a third party. The closed and secure environment of the Apple system makes it difficult to handle some applications during a mobile forensic examination. The following are two forensic tools that can work on iOS platform.

IPhone Backup Analyzer

Iphone Backup Analyzer is a multi-platform tool that uses Java. Mario Piccinelli created this tool to deal with the difficulty of using iOS to backup and analyse data and files (EC-Council, 2018). In the backup file, all files are logically arranged (Harvey, n.d.). The user can access the files and there is a feature to export all the binary files in the backup files forensic review. Backup contents of an iPhone system or other device using an iOS system can be viewed through the front-end provided by the tool. Archives and databases can be viewed and configuration files read.

Cellebrite Universal Forensic Extraction Device (UFED)

Cellebrite UFED is a mobile forensic investigation software and hardware tool, which is designed to support analysis and acquired data for any type of operating system. UFED enables extraction, decoding, analysis and reporting for mobile data. It is characterized by flexibility and speed while extracting data from smart devices, as the data extraction capacity reaches more than 6800 devices.

Cellebrite UFED provides many versions like Cellebrite UFED Ultimate, Cellebrite UFED Touch Logical, Cellebrite UFED Touch Physical Analyzer and Cellebrite UFED Touch Logical Analyzer (Media, 2020). It supports iOS devices, decoding, recovering deleted data from unallocated space in the device's flash memory and presence of multiple languages. Cellebrite is a popular option among many companies and law enforcement offices. It can provide full PIN bypass & filesystem acquisitions, Locked SIM and Missing SIM Cards, instant messaging application data, SMS, MMS, E-Mails, Calendars, Audios, Videos, Images, Contacts, Call logs, phone Details and SIM Card Details. It enables the examiner to perform logical, physical and files system acquisition along with the password recovery.

5. Mobile device anti-forensic

The presence of an anti-forensic tools is one of the challenges that forensic investigators face in cybercrime as its existence impedes verification work and evidence collection. The primary goal of mobile forensic is to collect and investigate the evidence. An anti-forensic app makes the forensic process more complicated . Peron and Leary define it as "attempt to limit the identification, collection, collation and validation of electronic data" (Miller, 2020). Anti-forensic makes investigation of digital media more difficult and time consuming. As a result of the proliferation and development of smart devices, people now use these devices to store their personal data and important information that increases the rates of theft and hacking crimes.Digital forensic is witnessing a golden age, especially mobile forensic as it provides work on many operating systems, tools and techniques to collect evidence. Some techniques and methods used by anti-forensic make the forensics investigators workmore difficult. Users can use anit-forensic tools to remove or alter evidence of criminal activities. Anti-forensic uses many techniques that can be divided into several categories:data destruction, blocking access to evidence, masking data, and data processing. Anti-forensic tools and methods affect the chances of successful investigation and evidence gathering. Anti-Forensic seeks to increase the time in its favour to try to conceal, destroy, or tamper with evidence so that investigators do not reach it. We will show some of the methods that can be used to anti forensic and the methods used to forge or destroy evidence and prevent access to it.

The general classes for anti-forensic techniques are hiding, obfuscation and data encryption,deletion or data destruction, data falsification, analysis prevention, obstruction of traces collection, and tools subversion (National cyberwatch center, 2018).

Data hiding

The main goal of this technique is to hide file or evidence from forensics tools, . Anti-forensic is often used to trick and manipulate an investigator, especially when the key used for encryption is unknown. Folder encryption is used to prevent unwanted access to data or files. This technique is an outdated and preferred method for hackers. (no sense here) This encryption hides illegal information in many shapes, text, images, and more. There are some applications of different systems that assist in this process, which make it difficult to discover evidence. Steganography is a form of data hiding with all its sub categories (National cyberwatch center, 2018).

Obstruction of traces collection

In this technique, hackers prevent evidence from reaching the investigator by planting false evidence and plagiarism to mislead the forensic tool used. This makes it difficult to obtain forensic evidence. One of the most important methods used here is the header of this file. This tool changes the name of the header of the file and recreates it so that it is not visible to forensic tools (Nextmedia Pty Ltd, 2020).

Evidence source elimination

This technology is one of the best techniques for its users to combat forensic medicine and it eliminates the source of evidence and makes the user invisible when it comes to the system and leaves no trace of it. It uses a set of tools such as source elimination tool (Nextmedia Pty Ltd, 2020).

Artifact wiping

In this approach, the evidence is erased rather than destroyed to prevent it from reaching the crime investigator. Several tools have been developed to ensure that an evidence is erased and not recovered during using forensic tool (Nextmedia Pty Ltd, 2020).

If these techniques are used permanently during listing and research, the researcher must have a deep knowledge of all these techniques and search for tools that enable him to bypass the forensic fight to obtain evidence.

Table 3 presents some of the anti-forensic tools which are are classified according to the used technologies as well as the operating system.

Table 3. Anti-forensic tools (Nextmedia Pty Ltd, 2020)

Application	**Platform**	**Anti-Forensics Technique**	**Classification**
File Shredder	Android	File Wiping	Destroying Data
iShredder	iOS	File Wiping	Destroying Data
LUKS Manager	Android	Encryption	Hiding Data
StegDroid	Android	Steganography	Hiding Data
FakeLocation	iOS	Spoofing	Counterfeiting Data

6. Current challenges in mobile forensic

The rapid growth in mobile technology has been witnessed these days. Therefore, the forensic experts should develop new forensic tools in order to meet the challenges and finalize the investigation of different devices correctly (Sai et al., 2015). In this section, we present some of the current challenges that may face the investigators.

Mobile data extraction

Different forms of data are available on mobile device such as contacts, text messages, call history, photos, etc. These forms of data are considered evidence, too. The challenge here is that when investigators use the evidence, it must be flawless or they cannot use it as an evidence. This means that some investigators face difficulty in extracting mobile data. Server and hard drive are different from mobile devices in the structure of the file system. In cell phone, the structure is diffuse and available across many apps and services (Salama et al., 2012).

Mobile device signals

Another challenge is that the signal of the cell phone must be blocked to ban new access to that device. The core of this challenge is blocking any signals from access that will reduce the efficiency of the battery power. So, the investigators should implement the investigation in an isolated forensic lab in order to prevent the problem of the mobile's energy (Sai et al., 2015).

Obtaining digital evidence

Firstly, the mobile platform security features, these features prohibit the investigation process especially in acquisition phase. New mobiles have advanced built-in security features that provide user privacy . To overcome this point, the examiners need to use special tools with their abilities to extract the evidence. Secondly, using anti-forensic techniques to secure the devices is one of the challenges that face examiners in obtaing digital evidence. These techniques such as data hiding and data forgery will increase the complexity of the investigation process (Nelson et al., 2014).

The volume of data

The amount of data that is relevant to investigation is growing rapidly, this is due to the growth in storage capabilities. However, current smart devices are limited in processing power and storage capacity. As a result of such increased with the volume of data, cloud service have been used to store data, but in cloud it may not be clear to know where the data are actually located, which makes the investigation process more difficult (Saleem et al., 2016).

Tool reliability

The difficulty in choosing an appropriate forensic tool for mobile device is another challenge the investigators may face. This is due to the complexity and diverseness of both mobile devices and investigation tools. As the availability of diverse device models in stores, the forensic tool merchants try to update the compatibility of the devices. Therefore, maintaing the reliability of such tools for evidence acquisition has become more essential (Shakeel, 2019).

7. Study case

These presented results have been extracted for IOS device using Belkasoft Software. This tool allows the investigator collect evidences using Belkasoft Evidence Centre BEC. In this study, acquisition and forensic analysis of tested device (see Figure 4) have been done using image backup to retrieve all the logical data from mobile device of Apple. In BEC, examiners can specify the data types chat, videos, SMS messages, etc. as shown in Figure 5.

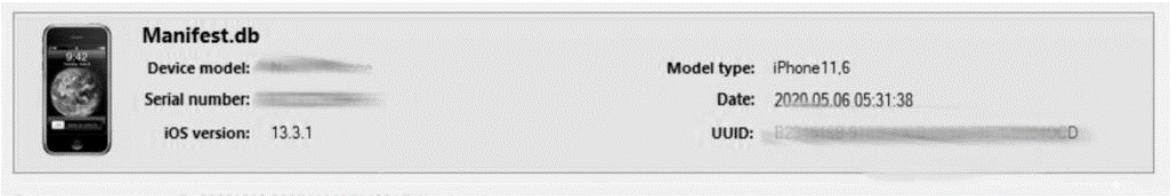

Figure 4. Data of tested device

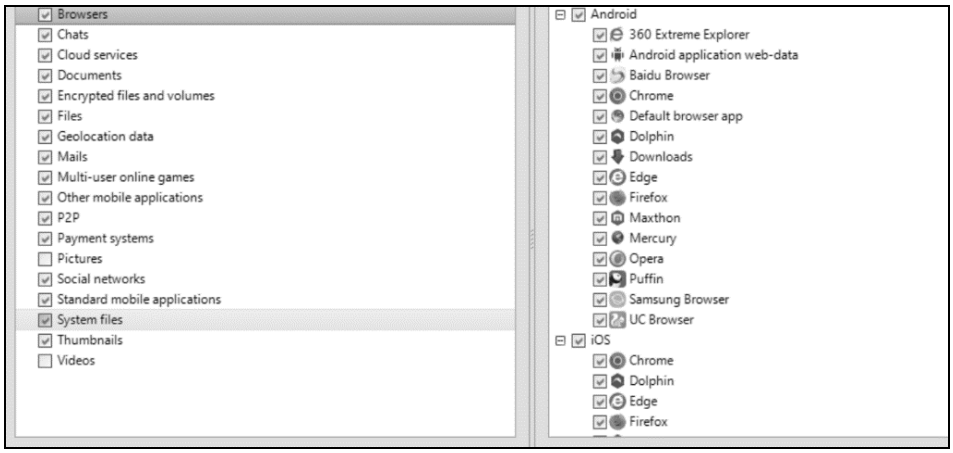

Figure 5. Selecting data type

Once the analysis process is completed, the detected data will be listed as shown in figure 6. The analysis of extracted data source can be summarized and it will be useful for any examiners (see Figure 7).

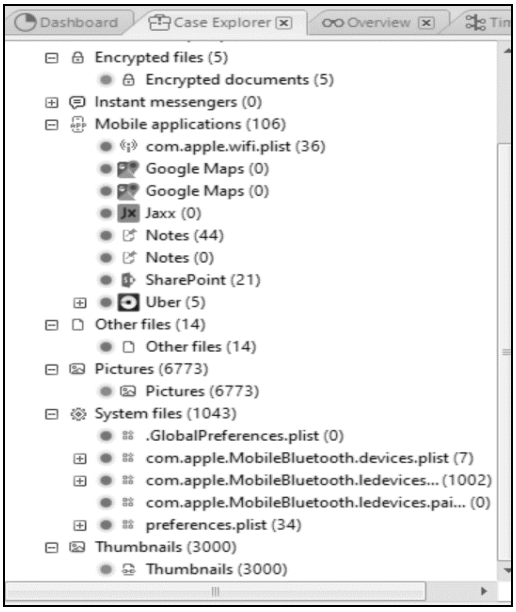

Figure 6. Data Extracted from the Analyzed Device

Figure 7. Summary of extracted data

Also, BEC tool enables the investigators to recover deleted files form ITunes backup. There is also a commercial version which has more advanced features, thus, investigators may visit Belkasoft website to request a trial version.

8. Discussion

In mobile forensics, there are two primary methods of data acquisition: logical and physical. The logical acquisition demands that APIs transfer all files which are not deleted from the file system of the mobile app into a forensic case. The obtained data is an active device material (device accessible), such as addresses, call logs, photos, videos and music, from the memory storage. You may also access partial application data such as configuration files, SQLite files, etc. In addition, a bit/bit file dump for an image of the smartphone device containing deleted data is used in the physical acquisition process. The physical acquisition dump requires both allocated and unallocated space. Please notice that these physically obtained data are in their raw state and require more processing according to the file structure.

Logical retrieval of all data on a smartphone including call logs, contacts, messages, calendar entries and images, photos, are easily, simply, securely and forensically safe.On the other hand, physical acquisition is used to construct a full representation of the memory. . This helps us to remove only deleted data and even the SIM that is not possible through logical acquisition is not present. We can bypass and retrieve passwords on the computer and they are also helpful for the review of removable memory cards.

We are focusing on comparing and analysisng several forensic tools including Oxygen, MOBILedit, Autopsy, Micro Systemation XRY and iPhone Analyzer forensic. In investigating a smartphone as evidence, the first thing to check if that the tool can perform the intended functions. The basis of comparison between these tools includes the level of functions, and the performance of each tool. These functions are as follows: *device Identification*; the capacity of a forensic tool to identify devices. *Data Extraction*; the capacity to retrieve data from the device. *Data decryption*; the capacity to decode data from the device. *MessengerApplication Analysis*; the ability to view messenger application content. *Data Report*; the ability to record information in the form of a text file (.xml,.pdf,.xsl, etc.) *Case management*: case-control throughout a messenger application. *Data recovery deleted*; the ability of a forensic tool to recover some deleted data from the phone. Table 4 compares the tools based on their functions.

Table 4. Fuctions of previous tools (Beard, 2017)

Functions	Autopsy	Oxygen	*MOBILedit*	UFED	iPhone Analyzer
Device Identification		✓	✓	✓	
Data Extraction	✓	✓	✓	✓	✓
Data decryption		✓			✓
Messenger Application Analysis	✓	✓	✓	✓	✓
Data Report		✓	✓	✓	
Data recovery deleted	✓	✓	✓	✓	✓

Tools help in investigating and looking for evidence in forensic. Some of them are free and others require payment. The performance of the free tools is good and serves the purpose, but paid tools have more advantages, the presence of competitive between companies developing such tools leads to develop tools that work in a professional and excellent manner. The investigator needs to determine the type of operating system and the type of evidence that he/she wants to search for in order to avoidusingtools that are not useful to him in the investigation process.

iPhone Backup Analyze is one of the free source tools that enables you to restore unencrypted backups but you will encounter some problems sience the encrypted backups may be more difficult to recover when a complex password was usedand you will have to download other tools for decoding. It is free only for government departments.

XRY is a commercial tool. Commercial tools are usually more durable and easier to use and have features that are not included in the free tools. It was designed to be safe when using extraction to keep the evidence confidential. Evidence reports can be used and submitted in court and elsewhere (Shala & Shala, 2016).

Oxygen supports platform application for Microsoft Windows, MacOS and Linux, it has parsing ability and decoding of applications and databases like WhatSup, cracking. The best feature in Oxygen is that it has social graph, it offers a convenient forum for exploring social connections between a device owner and their contacts or between multiple devices. Using the social graph investigation, the nearest contacts of the device owners can be defined by one click. Also, Oxygen collects information and data from Android devices for physical retrieval. It can be easily recognized the user interface and choices. . Investigators can save the final report in various readable formats, including .xls, .xlsx, .pdf, etc.There are some short falling in Oxygen, one of them is that Oxygen has limited support for the variety of mobile devices . It uses a brute force technique to complete the operation, which is time consuming. Since Oxygen tool is computer-based, there is a high risk that virus/malware would affect the phone that is being analyzed.

Autopsy gives you access to the file system directory tree faster than any commercial tool out there. Also, it supports parsing commonly missed items in Android devices. It supports platform application for Microsoft Windows, MacOS, and Linux (Alvarez, 2004). There are some limitation in Autopsy, one of them is that file carving and extraction is done manually, and do not support decoding or cracking applications and database like Oxygen.

MOBILedit is a commercial tool and can extract the physical and logical acquisition evidence. It supports thousands of phones and SIM analysers through SIM readers. Also it can read deleted messages from the SIM card and supports basic information on the SIM cards and cell phone memory information. MOBILedit does not support the decryption process, consider WhatsApp chat logs that are all encrypted, it cannot be read by MOBILedit database viewer. MOBILedit is compatible with Windows operating system but it may not work properly with Windows 10 without changing the compatibility features of the operating file. Also, the software license does not allow full free use.

9. Conclusion and future work

With the increasing demand for examination of mobile devices, investigators have developed several techniques in order to examine them. The process for any mobile device forensics is composed of different phases, starting with seizure, acquisition, analyses, and ending with reporting. Digital forensics techniques play an essential role in investigation since more and more people are using mobile devices. The techniques can be described in file system, creating an evidence and how the data can be acquired. An observed problem is the availability of techniques that support different platforms. For mobile forensic tools, we have analysed several tools with different platforms, Android and IOS. Oxygen, MOBILedit and Autopsy can be used to extract and analyse data in Android, but Micro Systemation XRY and iPhone Analyzer forensic can be helpful to perform investigation needs. While smartphones provide valuable information for the investigators, dealing with investigated data can be a challenge because of mobile device signals, the way of obtaining the evidence, the volume of data and tool reliability. With the help of open source mobile forensic tools, we performed a study case on Belkasoft software tool to address the result of investigation. For future work, there is a need to develop more tools, especially trial version, in order to explore all artifacts which will be helpful in detecting crimes and collecting evidences.

REFERENCES

1. Alvarez, Paul (2004). *Using extended file information (EXIF) file headers in digital evidence analysis*. International Journal of Digital Evidence 2.3 (2004): 1-5.

2. Arshad, H., Jantan, A. & Isaac A. O. (2018). *Digital Forensics: Review of Issues in ScientificValidation of Digital Evidence* [Ebook]

3. Beard, Isaiah (2017). *Digital Photos, Embedded Metadata, and Personal Privacy*. (2017).

4. *CyberRisk Alliance*. AccessData Forensic Toolkit (FTK). 3 Oct 2016. <https://www.scmagazine.com/review/accessdata-forensic-toolkit-ftk/>.

5. DeGrazia, Mari (2019). *Triage Collection and Timeline Generation with KAPE*. 22 Aug 2019. <https://www.sans.org/blog/triage-collection-and-timeline-generation-with-kape/>.

6. *Dot C Technologies. ProDiscover Forensics*. 2019. <https://www.prodiscover.com/products-services>.

7. EC-Council (2018). *An introduction to computer forensics and how to become a computer hacking forensic investigator*. 25 Mar 2018. <https://blog.eccouncil.org/an-introduction-to-computer-forensics-and-how-to-become-a-computer-hacking-forensic-investigator/>.

8. Garfinkel, Simson L. (2010). *Digital forensics research: The next 10 years*. Digital investigation 7 (2010): S64-S73.

9. Harvey, Phil. Read, *Write and Edit Meta Information!* n.d. <https://exiftool.org/>.

10. Horsman, Graeme (2018). *"I couldn't find it your honour, it mustn't be there!*" *– Tool errors, tool limitations and user error in digital forensics.* Science & Justice 58.6 (2018): 433-440.

11. Horsman, Graeme (2019). *Tool testing and reliability issues in the field of digital forensics*. Digital Investigation 28 (2019): 163-175.

12. *Introducing KAPE – Kroll Artifact Parser and Extractor*. 14 Feb 2019. <https://www.kroll.com/en/insights/publications/cyber/kroll-artifact-parser-extractor-kape>.

13. *KAPE Documenation*. n.d. <https://ericzimmerman.github.io/KapeDocs/#!index.md>.

14. Lokhande, P. S. & B. B Meshram (2015). *Digital forensics analysis for data theft*.

15. Mchatta, Kharim Haji (2018). *MSc Forensics Computing M08CDE: Master Individual Project Project Title: Forensics Tools and Data Hiding Techniques*. Diss. COVENTRY UNIVERSITY, 2018.

16. Media, *Slashdot. AnalogExif.* 2020. <http://analogexif.sourceforge.net/help/>.

17. Miller, Keith (2020). *Forensic Toolkit (FTK)®Digital Investigations*. 2020. <https://accessdata.com/products-services/forensic-toolkit-ftk>.

18. Naja, D. (2007). *Live memory acquisition for windows operating systems*.

19. National cyberwatch center. *Popular forensic software*. 6 Sep 2018. <https://www.cyberstudents.org/blog-post/popular-forensic-software/>.

20. Nelson, B., Phillips, A. & Steuart, C. (2014). *Guide to computer forensics and investigations*. Cengage Learning.

21. Nextmedia Pty Ltd. *ProDiscover Incident Response*. 2020. <https://www.itnews.com.au/feature/review-prodiscover-incident-response-66292>.

22. Pallagani, Avinash (2015). *Implementation of a Prototype for Automated Event Sequence Reconstruction for Web Browsing data in Computer Forensics*. Diss. Texas A&M University-Corpus Christi, 2015.

23. Sai, Dasari Manendra, N. R. G. K. Prasad & Satish Dekka (2015). *The Forensic Process Analysis of Mobile Device.* Int. J. Comput. Sci. Inf. Technol 6.5 (2015): 4847-4850.

24. Salama, Usama, et al. (2012). *Metadata based forensic analysis of digital information in the web*. Annual Symposium on Information Assurance & Secure Knowledge Management. Vol. 7. 2012.

25. Saleem, Shahzad, Oliver Popov & Ibrahim Baggili (2016). *A method and a case study for the selection of the best available tool for mobile device forensics using decision analysis*. Digital Investigation 16 (2016): S55-S64.

26. Shakeel, Irfan (2019). *7 Best Computer Forensics Tools*. 2019. <https://resources.infosecinstitute.com/7-best-computer-forensics-tools/>.

27. Shala, Lavdrim 7 Ahmet Shala (2016). *File Formats-Characterization and Validation*. IFAC - PapersOnLine 49.29 (2016): 253-258.

28. Sun, Xiaoting, et al. (2015). *The detecting system of image forgeries with noise features and EXIF information.* Journal of Systems Science and Complexity 28.5 (2015): 1164-1176.

* * *

Asia Othman ALJAHDALI received her Ph.D. degree in computer science at Florida State University in 2017. And a master's degree in information security in 2013. Later on, she worked at King Abdul-Aziz University as an Assistant Professor. Subsequently, she worked at the University of Jeddah as an Assistant Professor in the cybersecurity department. Currently, beside her academic work, she works as cybersecurity consultant for the administration of cybersecurity at Jeddah University. Her current research interests include information security, cryptography, data hiding, network security, IoT security, and Cloud security.

* * *

Nawal ALSAIDI graduated from King Abdul-Aziz University with a Bachelor of Science in Information Technology. She is currently a master's student enroled in the Cybersecurity programme at Jeddah University. Her research interests include mobile forensic, steganography and vulnerability assessment in IoT device.

* * *

Maram ALSAFRI graduated from King Abdul-Aziz University with a Bachelor of Science in Information Technology. She is currently a master's student enroled in the Cybersecurity programme at Jeddah University. Her research interests include mobile forensics, artificial intelligence, steganography and vulnerability assessment in IoT devices.

* * *

Afnan ALSULAMI graduated from Jeddah University (JU), KAS, in 2016, with a Bachelor of Science in Information Technology. She is currently a master's student enroled in the Cybersecurity programmme at Jeddah University. Her research interests include Distributed Systems Security, Artificial Intelligence, and Machine Learning.

* * *

Turkia ALMUTAIRI graduated from King Abdul-Aziz University with a Bachelor of Science in Information Technology. She is currently a master's student enroled in the Cybersecurity programme at Jeddah University. Her research interests include web application security, Distributed Systems Security, Artificial Intelligence, and Machine Learning.