Mansoura Journal For Computers and Information Sciences

Comparative Study of Different Mobile Forensic Tools for Extracting Evidence from Android Devices

Ramy M. Abou-Elzahab
Faculty of Computers and Information, Computer Science Dept.
Mansoura University, Egypt
ramyzahab@gmail.com

Mohammed F. Al Rahmawy
Faculty of Computers and Information, Computer Science Dept.
Mansoura University, Egypt
mrahmawy@gmail.com

Taher T. Hamza
Faculty of Computers and Information, Computer Science Dept.
Mansoura University, Egypt
taher_hamza@yahoo.com

Abstract
Nowadays there are more than one billion smartphone users all over the world, principally Android smartphone users because of its small size and its ease to help users in most tasks of their daily life. Therefore, smartphones can give huge amount of evidence and information to forensic investigators if a crime has happened. In our research, it has been chosen four forensic tools: MOBILedit, Oxygen forensic, Autopsy and Andriller and made a comparison among them while extracting data from a smartphone and a tablet with different Android versions. On the other hand, it has been examined the extracted data, identified the important extracted data and the unreadable data, so that the evidence can be accepted in a court of law. It has been proved that the free open source tools could extract many evidence data but not as good as the extracted data with a paid tool as MOBILedit forensic tool. There are no any open source tool could extract all important evidence data separately.

Keywords
Criminology, Digital forensics, Mobile forensics, Android platform, Data acquisition methods and Stages of mobile forensics.

1. Introduction
In 2015, according to Numbeo database for crime index [1] the rate of crime index in Egypt was 60.14%. The safety index was 39.86% and the arrangement of Egypt in the crime index was 37th over 117 countries. While in 2019, the crime index rate in Egypt decreased from 60.14% to 48.53%. The safety index is increased from 39.86% to 51.47%. The arrangement of Egypt in the crime index became 43th because of the development of the forensics science especially the digital forensics science. In addition, the digital and mobile forensic tools today have become more affective which helps the investigators to extract evidences from smartphones, tablets, computers and etc. Forensic science is the science that helps the investigators to solve the mystery of crimes by collecting, preserving and analyzing the evidences that found in the crime scene. It combines threads to reveal the criminal or to solve the crime and create a legal integrated report to be approved by the judge in the court of law [2].

The forensic science has over 16 branches in which each branch covers a part of evidence that could be found in the crime scene in our research. Recently, many works had been focused on digital forensic science and especially mobile forensic science [3]. There is no crime without evidence. Nowadays and because of tremendous development in technology, evidence could be some data in a smartphone or in a computer. The scientists developed digital forensic tools which can help investigators to extract evidences from digital devices such as computers, smartphones, smart TVs, servers, etc. [4]. The smartphone users multiplied quickly and many companies produce different software to run on the Smartphone. So, a new branch of digital forensic science has been emerged called mobile forensic science. Android OS spreads much more than IOS platform, Nokia Symbian platform and BB platform. Also, over 80 companies make alliance with Google companies to use Android OS [5].

Digital forensics is a branch of forensic science that includes the recovery, analysis and examination of items that found in digital devices. There are five branches of digital forensics (computer forensics, memory forensics, multimedia forensics, network forensics, and mobile device forensics) [6]. Mobile devices forensics or it`s other name (small scale device forensics) are responsible for the collection and analyzation of the evidences that found in the small devices such as Smartphones, Smart watches and Tablets [7]. The mobile devices use operating systems that make them work. They display GUI to the users when using these devices example of these OS`s include Android, Windows mobile, Mac OS. In our research, it has been focused on Android OS. Android operating system is an open source OS used on mobile devices that are based on Linux kernel, Google Company bought Android in 2005 [8]. On November 5, 2007; the Open Hand set Alliance (OHA) which is alliances of over than 80 companies in the market of mobiles.

These mobiles are such as: Samsung, LG, Motorola, etc. redound and invested to the development of the Android

platform [5]. The Android Platform consists of a kernel, libraries, and a framework.

The software development kits are some tools provided by Google to provide an environment for developing Android software and applications. The Android developer chooses Java programming language in writing Android applications because of its wide spread and its efficiency. Google Company chooses to use the Dalvik virtual machine (DVM) instead of SJP (Standard Java Platform) [9]. The Android software consists of four layers; the application layer, the application framework, the Libraries layer and the Linux kernel.

Android mobile applications have become important for many things in our daily life; for example: real-time communications with family and friends in different countries. They track the location of a shop, do social media activities, play games with friends, send Instant Messages (IMs) and to make voice over IP (VoIP) calls [10]. Android devices data often contain important information that could be extracted to solve a crime. They are such as photos, videos, contacts, the history of (logs, message in instant message applications, internet browser), text messages, e-commerce transaction history and etc.[10]. There are different mobile forensic techniques and tools for data acquisition from mobile devices. However, some of them are in development, and the others need a lot of training to be able to use it. Therefore, the mobile forensic investigator should be aware of the different tools and techniques that are available and be aware to its methodology [11].

Thence, it has been chosen Android Smartphone to focus on in our research. This research work aims to make a comparison of the results obtained from an Android device by using different Mobile forensic tools (paid and open source tools). These Mobile forensic tools can be used to evaluate these tools, compare their qualities, compute the time used to extract data and determine the quality of extracted data.

This paper is organized as follows: Section 2, discusses the related researches and the differences between our research and some other research, Section 3, discusses the basics and challenges of mobile forensics, Section 4, provides an overview of the methodology we use to extract evidence data by different forensic tools and comparing between them, Section 5, presents the result of our research and finally Section 6, shows the conclusion and the recommendations,

2. Related Work

Raji M. *et. al*., in 2018 [12] aimed to make a comparison between commercial and free open source mobile forensic tools. This comparison can be used for extracting, collecting and analyzing data from smartphone that use Android operating system. The authors used two mobile forensic tools: Paraben E3:DS and Autopsy forensic tools. They can be used to compare between them and to know which is better in testing evidence data extracted from smartphones. The research showed that the commercially tool (Paraben E3:DS) is better than the open source forensic tool (Autopsy). In addition, they concluded that investigators should be aware of the legal method to extract evidence data to be accepted in the court of law.

Dogan S. and Akbal E., in 2017 [13] used digital forensic tools to analyze phone devices, they focused on collecting, testing and analyzing phone devices without exposure the data to be damage. They also choose two mobile forensic tools: Oxygen forensic tool and MOBILedit forensic tool for analyzing and testing Android phone. Their research work proved that MOBILedit tool gave faster and better analysis than Oxygen forensic tool.

However, Oxygen forensic tool had some advantages in dump test and wireless protocols over MOBILedit.

Awan F., in 2015 [14] made forensic examination on application of social media on mobile phones. They focused on studying the smartphones internal memory and if it stores the logs and actions that performed by social media applications on different smartphones that uses different operating system. They used the forensic tools to examine social media network application as: Facebook, Twitter. The research work used the Encase forensic tool to examine some smartphones with different operating systems. They proved that tools can`t extract any data from Blackberry phones. Whereas, they can extract a big amount of evidence data from Android, Windows and iPhone smartphones.

Umar R. *et. al*., 2017 [5] work aims to extracting evidence data from WhatsApp application in Android smartphones. This research rated the existing mobile forensic tools in extracting and testing data extracted from WhatsApp. They used WhatsApp Key/DB Extractor tool and Oxygen Forensic tool. They compared between them and showed that important evidence data could be extracted from WhatsApp application that installed on smartphone devices.

Lukito F. *et. al*., in 2016 [15] focused on unrooted Android devices. They used different tools and techniques to extract data and made a comparison among these tools and techniques. This research used different forensics tools such as Android Back up Analysis and Oxygen Forensics. The result shows that the best tool for unrooted android devices is Android Backup Analysis tool.

Aziz, *et. al*. , in 2015 [16] focused on using different methods to find the best method for the elicitation and for testing data extracted from Android smart devices. They put a case scenario of a crime in a company. They tested and examined the relevant data that extracted from the android devices and the result showed the amount of extracted data.

3. Overview of Mobile Forensics

Criminology is the scientific science that studies the nature, management, causes, control, and prevention of criminal behavior, on both social levels and individual. Criminology is a science whose role is before other sciences such as sociology, biology, psychology, psychiatry and social anthropology [17]. There are many types of crimes such as murder, steel, rap, kidnap, privet violation, hack the mobile devices, etc. The forensic investigator is responsible for examining of all types of evidence. The forensic investigators have two jobs. Firstly, they go to the crime scene to collect evidence. Secondly, they examine the evidence in the lab with forensic tools. The forensic science has over 16 branches in which each branch covers a part of evidence that could be found in the crime scene. In the crime scene, the investigator may find five or more types of evidences. He must examine each evidence separately by its own forensic type, for example: if a computer or a mobile device or a memory card or any digital device found they have to be analyzed and examined using digital forensic [6].

Digital forensics is a branch of forensic science that includes the recovery, analysis and examination of items that found in digital devices. Digital forensics isn`t refer to computer forensics only because the use of it has expanded to cover all digital devices investigation with evolving the digital devices which started in early 1980s and continued until today [18].

Digital Forensics is the science interested in examination of digital devices to help investigator to solve the crime and create reports and present it to the judge.
The digital evidence includes Desktop Computers, Laptops, Smart TV, Smart Watches, Smartphones, Tablets, Drones, etc. There are five branches of digital forensics [6], as shown in figure (1).

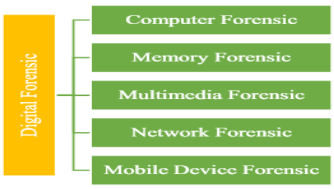


Figure (1), digital forensics branches [6]

Mobile devices forensics are responsible for the collection and analyzation of the evidences that found in the small devices such as Smartphones, Smart watches, Tablets, etc. [7]. The mobile devices use operating systems that make them work and display GUI to the users when they use these devices such as Android, Windows and Mac OS IOS. Android operating system is based on Linux Kernel. Android became the most popular operating system according to its sales in the fourth quarter of 2016 that was about 400 million devices [5].

3.1 Android Platform

The Android software consists of four layers, layer 2 divided into two parts Library layer and Android runtime layer as shown in figure (2) [19] .

- *Linux kernel* acts like an abstraction layer that found between software and hardware and it is in the charge of power management, flash memory management, network management, tools management and security [19].

- *The Libraries layer* is written with C++ programing language and performed through Java interface. The advantage is that the libraries offered can be accessed through the application framework layer [20].

- *The Android runtime* has some libraries that supply all the available features in Java libraries on OS. It is responsible for translating Java code to an understood language to the operating system [21].

- *The application framework* gives an open environment for development that allow the reuse of application functions, it also provides the developer with all available resource [22].

- *The application layer* is the layer that appears to the user in the interface of the device, it consists of some application such as: contacts, SMS programs, web browsers, map service, voice over IP (VOIP) programs [22].

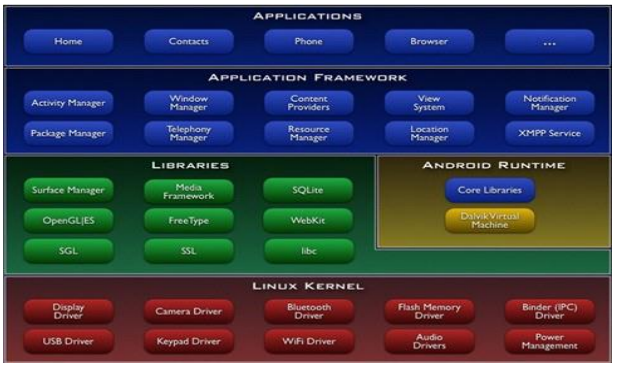


Figure (2), Android platform [19]

3.2 Data Acquisition Technique

There are different mobile forensic techniques and tools for data acquisition from mobile devices [11], as shown in figure [3].

- *Micro read* is one of the techniques that allow the investigator to view data on memory chips via high-power electron microscopes. This technique is expensive, time - consuming, and requires deep knowledge of file systems and hardware [23].

- *Chip-off* is another technique that allows the investigator to extract evidentiary and necessary data from the flash memory module directly. When the memory chip is removed from the device, the investigator generates a binary image for analysis. This technique is extremely expensive and needs wide knowledge of hardware if an untrained investigator tries to use this technique, physical damage could be happen [24].

- *Hex dump* is a technique that enables the data physical extraction from the device. After the investigator connects the device to a forensic workstation, the forensic tools can be used to extract data and to create a raw image of the memory of the device. There are many Hex dump forensic tools for example: UFED Analyzer, XACT, and Pandora's Box [24]. This technique is not expensive and can be used for recovering deleted data and unallocated space. The investigator must be trained to use this technique and must also have good knowledge of hardware and software.

- *Logical extraction* is the most widespread technique; the mobile device is connected to the workstation (forensic lab) via Bluetooth, WIFI or USB. This method is the easiest method for the investigator [24].

Figure (3), data acquisition methods [11]

3.3 The challenges of Extracting Data from Smartphones

There are eight challenges facing investigators when they try to collect data from mobile devices using mobile forensic tools [25].

- *Platform and manufacturers*: Mobile devices have many varieties such as smartphones, tablets, smartwatches,

cameras, navigation device and drones. When the investigator deals with these different devices, he needs to know the features of all these devices so he could extract data from it [26].

- *Data preservations:* It is very important to prevent the mobile device from receiving any communication whether as a text or voice or any other data. Text messages stored in the device "First In, First Out" order, if the device receives new incoming messages it would delete older text messages [27].
- *Power:* Many mobile devices nowadays store data in volatile memory wherefore it is a challenge to investigators to preserve power to the mobile device because the battery of the mobile device lose all its power if it left unplugged for a long period of time. Full loss of power may lead to a loss of data and hence a loss of important evidence [28].
- *Operating system:* There are many manufacturers of mobile devices on the market and there are many OS on the market, these OS are Android, IOS, Symbian, windows mobile, blackberry OS [28].
- *Communication protocols:* The challenge is that there are different protocols used to establish a communication between the evidentiary mobile device and the forensic workstation. There are some good data communication protocols currently in use for example AT, MBUS, OBEX, and Sync ML. Sometimes these protocols are used to restore data from mobile devices such as its model, telephone number, software version, IMEI number, serial number, history call logs, videos, photos, and other important data [29].
- *Security mechanisms:* There are many mechanisms used on mobile phones to provide security to devices and protect data. These security mechanisms range from handset user locks, to PINs of SIM card, PUKs code and full device encryption [30].
- *Android encryption:* Once a device is encrypted all data whether important or not on an Android device is encoded by symmetric encryption keys and became encrypted data that cannot be read without knowing the decrypt key [31].
- *Cloud data:* When user saves important data on cloud storage instead of saving on mobile device the forensic investigations faces a difficulty to extract these data. Although cloud backups can offer the chance to recover deleted data deleted or locked data even from broken devices [32].

These challenges could lead to failure of the investigation so the investigator should know them and take his bin from them.
The encryption considered the hardest challenge may face the investigator because once the device is encrypted all data whether important or not on an Android device is encoded by symmetric encryption keys and became encrypted data that cannot be read without knowing the decrypt key [31].

There are three methods used by Android OS for device encryption.

First: Android version 5.0 and above use **full-disk encryption method**. Full-disk encryption uses a one key protected by device`s password to protect the device's user data partition. Upon boot, the user must open the lock with the password before any part of the disk is accessible [33].

Second: **File-based encryption** release and Android version 7.0 and later supports it. File-based encryption allows different keys to encrypt different files. Mobile devices that support this method can also support Direct Boot that allows encrypted devices to boot to lock screen straightly, so it enable quick access to important features like alarms and web services [34].

Third: **Metadata encryption**. Hardware support is present. Metadata encryption used in Android version 10, it use a single key put at boot time encrypts, such as directory layouts, file sizes, and creation/modification times. This single key is protected by Key master, which is protected by verified boot [35].

3.4 The Steps that should follow once the Investigator Finds a Smartphone

- *If the device is "ON"* [36].

1- Do not turn it "OFF" because switching it "OFF" could activate lock screen feature.

2- The investigator should document all information on the mobile phone display (take photo to it if possible).

3- Put the mobile phone on flight mode.

4- Try to connect mobile device to power to make sure that battery would not drain out,

5- Then the investigator should put the device in isolated box

- *If the device is "OFF" [36].*

Else leave it "OFF" because turning it "ON" could lead to alter evidence on the mobile [36].

4. Methodology

The purpose of the research is to conduct a comparative study between the capabilities of existing examination tools to access their performance, strengths and weaknesses. The goal is not to build new tools, and for this reason a research methodology has been adopted in this research paper similar to that in the following research paper Sudozai, at. Al., (2018) [37]; Rusydi, at. Al., (2017) [5]; Majeed, at. Al., (2018) [12] and Lukito, at. Al., (2016) [15]. In our research, we focused on extracting and analyzing data from Android smart phones with different mobile forensic tools while comparing between the results.

These tools are MOBILedit, Oxygen forensic, Autopsy and Andriller. The extracted data such as call logs, SMS, passwords, web history, cookies, search history, image data, video data, audio data, documents data and all deleted data were tested. The readable, important data and the unreadable data, especially the extracted deleted data can be identified. The steps made by the National Institute of Stanford and Technology (The NIST) can be used to explain research stages from founding the smart phone to extract the important evidence from it and post a report. This step consists of 4 stages as shown in figure (4) [38]. It has been compared the capabilities provided by the studied tools for each step and mentioned the main missing features in each of them.

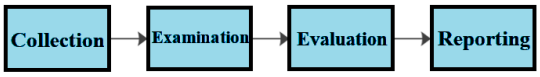


Figure (4). NIST extracting steps [38]

4.1 Stages of Mobile Forensics

4.1.1 Used Tools and Phones in the Collection Step:

It has been chosen four forensic tools (MOBILedit, Oxygen, Autopsy and Andriller).

MOBILedit and oxygen tools are paid commercial tools while Autopsy are open source and free tool and Andriller are free in the trial version so we made a comparisons between the paid and the free tools.

MOBILedit Forensic Express:

MOBILedit Forensic Express is a paid mobile forensic tool that gives us all in one solution. It provides smart phone and cloud extraction, data analyzer and generate (PDF, XML, HTML) report. It is 64-bit application that uses both the physical and logical data acquisition methods. MOBILedit is an excellent tool because of its new and advanced application analyzer; recovery of deleted data, supports of most Android versions includes the latest version and friendly user interface [39].

Oxygen Forensic Suits 2014 v 6.4

Oxygen Forensic tool is a commercial tool that uses logical and physical data acquisition. Oxygen Forensic obtains successfully the information of smartphone devices as IMEI, IMSI, Android version, smartphone name and model.

Oxygen Forensic tool has advantage that it leaves no traces so no footprint would be appeared and makes no changes to the content and extracted data in the smartphone. Oxygen Forensic manages the document, the location tracks, sound, image, and video files. The extracted image has good quality they do not blur when the image is zoomed to see more clearly [40]. Forensic manages to retrieve video files. Oxygen Forensic can play videos files so that can help the investigation to know if the video file is necessary or not before extract it and create report because of its graphic interface.

Autopsy

Autopsy is an open source end-to-end digital forensics tool. It is built by Basic Technology with most of the features available in commercial forensics tools. It is used by forensic investigators and military to extract evidence data from computer. It can be recovered deleted data from device memory or its memory card. It can be used on smartphones after getting physical image from this device by another program (MOBILedit). It is fast, free and easy to use [12].

Andriller

Andriller is an Android forensics tool for Android smartphones only. Due to its wide options and its free of cost trial version, Andriller is one of the most commonly used tools. It can be used in most Android versions to extract important data.

The data acquisition process is logical acquisition followed by read only, non-wasteful and forensically sound. In addition, Andriller can be used to crack several lock screen types such as; Pattern, PIN code, fingerprint or Password. It has decoders for Apps data for decoding communications from databases in the smartphone. Andriller doesn't require root permission to extract data from devices but Andriller extract only the log files, browser history, passwords, contacts so it can`t extract media or audio or image files [41].

These tools can be installed on laptop HP ELITE BOOK, run on it WINDOWS 10 PRO 64 to examine them on one Android smartphone (Samsung Galaxy S5 mini with Android Platform 6.0.1 unrooted and the same smartphone with root permission) and one Android Tablet (Samsung Tablet Note 10.1 with Android Platform 4.4.2). As shown in table (1), (2).

Table (1), Samsung Galaxy S5 minis specifications

1	**Manufacturer**	Samsung	**6**	**IMEI**	355320060564625
2	**Product**	Galaxy S5 Mini	**7**	**IMEI 2**	355321060564623
3	**HW Revision**	MMB29M	**8**	**Rooted**	Yes / No
4	**Platform**	Android	**9**	**SIM Card**	Yes
5	**SW Revision**	6.0.1 (23)	**10**	**Serial Number**	db1c84be

Table (2), Samsung Tablet Note 10.1 specifications

1	**Manufacturer**	Samsung	**6**	**IMEI**	355357058548269
2	**Product**	Note 10.1	**7**	**Operator**	MCC: 602, MNC: 2
3	**HW Revision**	KOT49H	**8**	**Rooted**	No
4	**Platform**	Android	**9**	**SIM Card**	No
5	**SW Revision**	4.4.2 (19)	**10**	**Serial Number**	410764dd39ed314d

4.1.2 Comparing the Examination Step in the Four Tools.

In this step after installing the tools, the smart devices are connected to the laptop by cable and the tools are used for examining them as explained here.

- Examining with MOBILedit Forensic Express

First, connect **Samsung Galaxy S5 mini** with Android platform **version 6.0.1 without root permission** to laptop with cable and allow USB debug in the smart phone. After that, press "Next" the tool demand to install connector application on smartphone. Install it and after that an installation message appears that root permission could help in extracting more important data. Then we choose full content to allow the tool to extract all data in smartphone and press extract. The tool starts examining the smartphone and then begins extracted.

Second, the same previous steps on **Samsung Tablet Note 10.1** have been done with Android platform **version 4.4.6 without root permission.**

Third, connect **Samsung Galaxy S5 mini** Android platform **version 6.0.1 with root permission** to laptop with cable and start MOBILedit forensic tool.

- Examining with Oxygen Forensic Suits

First, connect **Samsung Galaxy S5 mini** with Android platform **version 6.0.1 without root permission** to laptop by cable and allow USB debug in the smart phone. Then press connect device and choose live device acquisition to automatic search and find smartphone. After that the tool starts searching for Smartphone and it finds the device. Then choose a hash algorithm (SHA-2) to be used on the extracted data and press extract. The tool takes about 5 minutes and it failed to extract data because it needs root permission.

Second, the same previous steps with **Samsung Tablet Note 10.1** unrooted and it failed too.

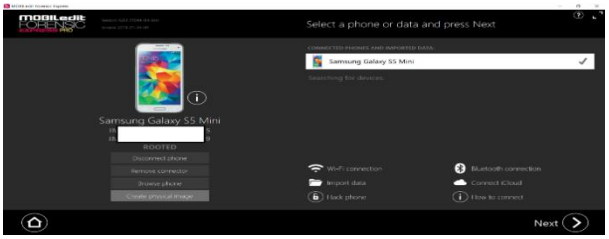
Third, connected **Samsung Galaxy S5 mini** with Android platform **version 6.0.1 with root permission** to laptop by cable and did the same previous steps.

- Examining with Autopsy

Autopsy tool can`t extract data from connected smartphone, it needs a physical image from the smartphone to extract data from it. There are two ways to extract physical image.

First; by Linux .DD command, second by MOBILedit forensic express but it requires root permission.

Physical image can be extracted from **Samsung Galaxy S5 mini** and **Samsung Tablet Note 10.1** by MOBILedit forensic express, as shown in screenshot (1).



Screenshot (1), extraction of physical image

Then start Autopsy tool and create a case, press the button add data source and choose Disk Image. After that browse the physical image of **Samsung Tablet Note 10.1** and start the extraction. The same steps can be done with the physical image of **Samsung S5 mini**.

- Examining with Andriller

Connected **Samsung Galaxy S5 mini without root permission**, **Samsung Galaxy S5 mini with root permission** and **Samsung Tablet Note 10.1 without root permission** to laptop by cable and allow USB debug in them, then we press check, then we press extract.

4.1.3 Comparing the Capabilities for the Evaluation Step.

After the tools finished the extraction of the data, the results e collected by the tools; the performance of each tool and the results produced by each of them has been evaluated.

- MOBILedit Forensic Express

First; the tool took about 2 hours for examining the data in **Samsung Galaxy S5 mini without root permission**. Then the tool demand to allow it to take back up from the smartphone. It has been allowed it and the tool begins to extract data and took about one and half hour to create reports.

Second; the tool took about 1 and half hour to read and 1 hour to extract data from **Samsung Tablet Note 10.1**.

Third; the tool took about 5 hours to read the data and about six and half hour to create reports in **Samsung Galaxy S5 mini with root permission**.

The results showed all the content in the smartphone such as the image files, video files, audio files, log file, all applications and its content in the smartphones, GPS location data, passwords, SMS, contacts, emails, cookies, browsers history, documents and how many files was in each content and if there are deleted files in each content or not. The disadvantage that the tool doesn`t provide hash to the result which is important prove that there is no alter in the extracted evidence data.

- Oxygen Forensic Suits Tool

Oxygen tool took about 2 hour to read data and 2 hours to extract data. Oxygen tool showed the extracted data in graphic interface in shape of buttons, each button opens special data. File Browser icon open all files and data in the smartphone including images, audios, videos, documents and application source. The search button allows us to make search in the extracted files by name or number.

The application button opens all the application in the device and all the data saved in each application and make preview to it as WhatsApp databases, images, videos, documents, browser search and history and etc. The disadvantage of the tool is that it can`t extract the passwords file.

- Autopsy Tool

After Autopsy tool finished the extraction, open the result of **Samsung Galaxy s5 mini** with Android version 6.0.1 in the tool. The tool took about 4 hours to extract call logs, contacts, web browser history, emails, images, deleted files, videos, documents and etc. The tool also could preview the image and videos data in all files in the device. There is button named timeline button showed the web logs and activity and the hidden files in different view mode list, details and charts. The tool showed the email addresses and history together to make it easy to read all sent and received emails.

The disadvantage of the tool.

1- It couldn`t extract the passwords of the accounts or WIFI.
2- That the tool couldn`t extract the information of the smartphone as (IMEI, serial, IMSI, MAC address, SW version).
3- The deleted files couldn`t be read. Autopsy tool took about 2 hours to extract data from **Samsung Tablet Note 10.1**. The tool extract images, videos, emails, deleted files and etc. but it couldn`t extract call logs, contacts and messages.

- Andriller Tool.

First; after Andriller tool finished extraction of data it has created HTML report, open the result of **Samsung Galaxy S5 mini without root permission.** The tool took about 4 minutes to extract data from the smartphone. The extracted data included smartphone information, call log, WIFI password, and accounts of applications and download history.

Second; the tool took about 2 minutes to extract data from **Samsung Tablet Note10.1**. The tool extracted Tablet information, account but the tool here couldn`t extract WIFI passwords, logs and download history.

Third; the tool took about 30 minutes to extract data from **Samsung Galaxy S5 mini with root permission.**

The tool extracted browser history, SMS messages, call logs, WhatsApp messages and calls and contacts, WIFI passwords and accounts.

4.1.4 Capabilities for the Reporting Step

The reporting step is very important step to the investigator because the extracted report will be submitted to the court of law so it must be good report in different formats to be accepted. Table (3) shows the formats that each tool could export. Figure (5) shows illustrator of NIST

. Table (3), the formats that each tool could export.

	HTML	PDF	XLSX	JPG
MOBILedit tool	✓	✓	✓	
Oxygen tool	✓	✓	✓	✓
Autopsy tool	✓		✓	
Andriller tool	✓			

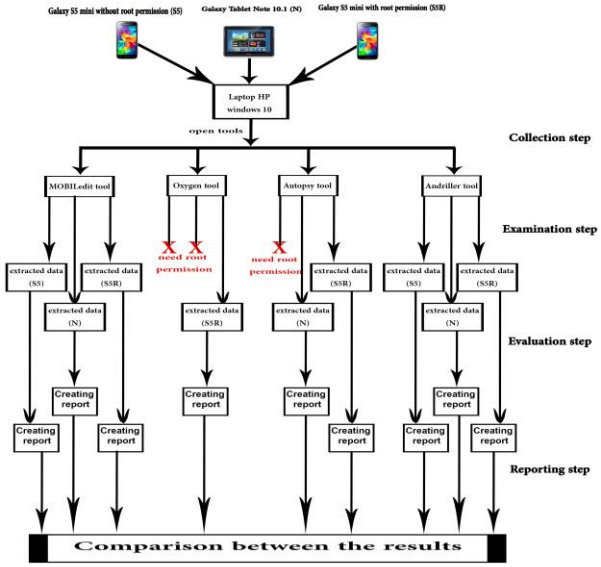


Figure (5), illustrator to NIST steps [38]

5. Results

A comparison between the extracted data has been done by each tool with showing the results in tables and charts.

5.1 Samsung Galaxy S5 mini with Android Version 6.0.1 (rooted)

It finds that Andriller is the fastest tool to read and extract data but this is expected as it only extracts log data and WIFI passwords, information, accounts and some media files, Oxygen tool is fast and it extracts data but require root permission. Autopsy tool extracts deleted data but it is unreadable. MOBILedit is better than the other tools in the number of extracted data especially the deleted data and the password files but unfortunately it doesn`t require Hash to the result. Table (4) shows the number of the extracted data that each tool give and which data are readable and which aren`t. figure (6) shows the extracted media files by each tool.

Table (4), comparison between extracted data from the four tools in Samsung Galaxy S5 rooted.

			MOBILedit	Oxygen detective	Autopsy	Andriller
Hash the result			no	yes	yes	no
The external data	**Call logs**		1546 calls	1050 calls	2012 call logs & SMS	586 calls
	Contacts		1546 calls	612 contacts	167 contacts	113 contacts
	Messages		2123 messages	1965 messages	1982 messages	2124 messages
	Passwords		14 WIFI passwords 2 email passwords 1 account password	--	--	16 WIFI passwords
	Emails		10 emails	6 emails	5 emails	--
	Images	**Media files**	5145 image files	2739 files	5143 image files (4176 unreadable)	263 files
	Audios		927 audio files			
	Videos		769 audio files			
	Documents		643 files			
	Application		285 applications	215 applications	--	--
The ext	**Cookies**		9412 files	--	256 files	
	System logs		88 files	--	--	

	Deleted files	20 web search history 80 downloaded files 81 cookies unreadable 46 calls readable 36 contacts readable 5 accounts readable 7 emails readable 1 image file readable	50 downloaded files 40 calls readable 13 contacts readable 3 emails unreadable	46365 unreadable file	
	Search history	69 URL	51 URL	--	
	Browser history	6 URL	6 URL	17 URL	5 URL
	Download history	549 files	489 files	--	92 files
	Device accounts	26 accounts	6 accounts	3 accounts	6 accounts
	Device information	Product name Android version IMEI IMSI MAC address Serial number SIM card country	Product name Android version IMEI IMSI MAC address Serial number SIM card country	--	Product name Android version MAC address Serial number

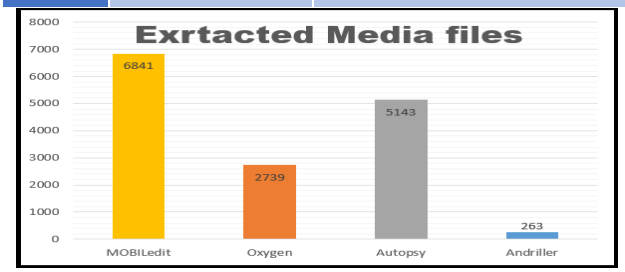


Figure (6), the extracted media files from Samsung Galaxy S5 mini rooted

5.2 Samsung Galaxy S5 mini with Android Version 6.0.1 (without root permission)

Andriller tool extracts few data (call logs, WIFI passwords, device accounts, device information) from the smartphone without root permission than from the smartphone with root permission. Oxygen tool couldn`t extract data because it requires root permission. Autopsy not affected by root permission because it extracts data from physical image not from the Smartphone. It extract media data, call logs, contacts, device accounts and device information. MOBILedit extracted data from unrooted Smartphone are not as good as from the rooted. It extract call logs, contacts, messages, media files, deleted files, accounts, and browser history. MOBILedit forensic tool is better in the number and accuracy of the extracted data from Smartphone than other tools but it could only extract WIFI password files. Table (5) shows the number of the extracted data that each tool give and which data are readable and which aren`t. figure (7) shows the extracted media files by each tool.

Table (5), comparison between extracted data from the tools in Samsung Galaxy S5 unrooted.

			MOBILedit	Autopsy	Andriller
Hash the result			no	yes	no
The extracted data	**Call logs**		1046 calls	2012 for call logs and incoming SMS	500
	Contacts		235 contacts	167 contacts	--
	Messages		2123 messages	1982 messages	--
	Passwords		14 WIFI passwords	--	14 WIFI passwords
	Emails		3 emails	5 emails	1 email
	Images	**Media files**	4401 image files	5143 image files (4176 unreadable)	--
	Audios		627 audio files		
	Videos		389 video files		
	Documents		516 document files		
	Application		285 applications	--	

	Deleted files	1 web search history readable 80 downloaded files readable 11 cookies unreadable 46 calls readable 13 contacts unreadable 13 messages readable 1 image file unreadable	46365 unreadable file	
	Cookies	455 files	256 files	
	System logs	88 files	--	
	Browser history	6 URL	17 URL	
	Search history	65 URL	--	
	Download history	549 files	--	92 files
	Device accounts	6 accounts	3 accounts	6 accounts
	Device information	Product name Android version IMEI IMSI MAC address Serial number SIM card country	--	Product name Android version MAC address Serial number

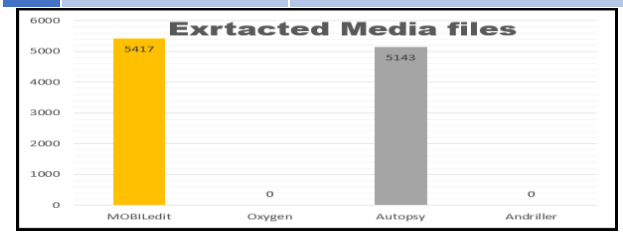


Figure (7), the extracted media files from Samsung Galaxy S5 mini unrooted

5.3 Samsung Tablet Note 10.1 with Android Version 4.4.2 (unrooted)

Andriller tool extracts only smartphone information and accounts. Autopsy extract media files, browser history and unreadable deleted data. MOBILedit tool extract contacts, WIFI passwords, media files, browser history, device accounts and device information. In Android version 4.4.2 all tools couldn`t extract call logs, messages and emails but MOBILedit tool is better than the others in extracted the other data, it can extract WIFI password files. Table (6) shows the number of the extracted data that each tool gives and which data are readable and which aren`t. figure (8) shows the extracted media files by each tool.

Table (6), comparison between extracted data from the tools in Samsung Tablet Note 10.1 unrooted.

		MOBILedit		Autopsy	Andriller
Hash the result		no		yes	no
The extracted data	**Call logs**	--		--	--
	Contacts	8 contacts (7 deleted)			
	Messages	--			
	Passwords	2 WIFI passwords			
	Emails	--			
	Images	**Media files**	532 image files	1724 files	
	Audios		435 audio files		
	Videos		1358 video files		
	Documents	44 document files			
	Application	248 applications		--	

	Deleted files	100 web search history readable 64 browsing history readable 3 cookies unreadable 7 downloaded files readable 7 contacts unreadable 1 image file unreadable	25842 unreadable files	
	Cookies	52 files	--	
	System logs	66 files	--	--
	Browser history	113 URL	11309 URL	
	Web search history	111 files		
	Download history	8 files	--	
	Device accounts	2 accounts	3 accounts	1 account
	Device information	Product name Android version IMEI MAC address Serial number SIM card country	--	Product name Android version IMEI MAC address Serial number

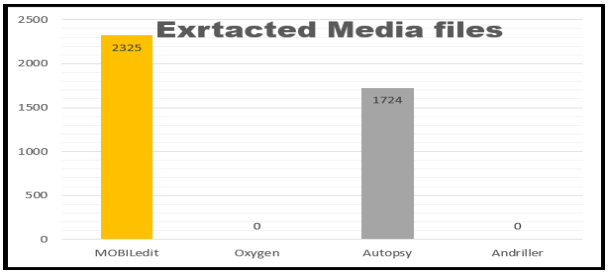


Figure (8), the extracted media files from Samsung

6. Conclusion and Future Work

The purpose pf the research is to conduct a comparative study between the capabilities of existing examination tools to access their performance, strengths and weaknesses. The goal is not to build new tools, and for this reason a research methodology has been adopted in this research paper similar to that in the following research paper From the results, we concluded that MOBILedit forensic tool is better in both the quantity and accuracy of data extracted from Smartphones in both Android version 4.4.2 and version 6.0.1 whether smartphone with root permission or not. MOBILedit PDF, HTML XLSX reports are better than other tools reports in the arrangement, organization and presentation of the extracted data. In addition, oxygen tool is one of the fastest tools but it couldn`t extract password data, system log files, cookies and need root permission. Autopsy tool works with version 6.0.1 better than version 4.4.2 but it need physical image to the smart phone. Andriller tool works in mobile phones with root permission better than without. The best paid tool is MOBILedit forensic tool and that Autopsy tool and Andriller tool are extracting data equivalent to the data extracted by MOBILedit forensic tool from smartphones without root permission. However, MOBILedit forensic tool is more than the rest of the tools in the accuracy and quantity of extracted data from smartphones with root permission. Whereas, the MOBILedit forensic tool has two shortcomings in which the first is slow and the second does not make Hash to the results. MOBILedit reports are the best reports that could be presented to the judge of law after we gave the reports Hash value with other tool.

It has been observed that each of the four tools is purely studied. Therefore, the future study will use other types of tools and study them and know their advantages and disadvantages. As well as trying to design a new forensic tool that avoided the defects in previous tools.

6. References

1- “Numbeo database crime rate” https://www.numbeo.com/crime/rankings_by_country.jsp? [Accessed 9 October 2019].

2- Alldredge, J., (2015). "The 'CSI Effect' and Its Potential Impact on Juror Decisions," Themis: *Research Journal of Justice Studies and Forensic Science*: **3**: (. 1), Article 6

3- Burkhard, M., (4 March 2014). Handbook of Forensic Medicine. Sussex: Wiley Blackwell. p. 10. ISBN 9780470979990.

4- Braithwaite, J. (1 March 2000). "The New Regulatory State and the Transformation of Criminology". British Journal of Criminology. **40** (2): 222–238

5- Umar,R.; Riadi, I. and Zamroni, G. M., (2017). "A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements". *International Journal of Advanced Computer Science and Applications*, **8** (**12**),

6- Roy,N.R.; Khanna, A.K. and Aneja, L., (2016). "Android Phone Forensic: Tools and Techniques" International Conference on Computing, Communication and Automation (ICCCA).

7- Casey, E., (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Academic Press, ELSEVIER, .

8- GADHAVI, B., (2010).Analysis of the Emerging Android Market. The Faculty of the Department of General Engineering, San Jose State University. [S.l.], p. 88. .

9- De L. Simão, A.M.; Sícoli, F. C.; De Melo,L.P. ; De Deus, F.E. and De Sousa Júnior, R.T. ,(2011)."Acquisition and Analysis of Digital Evidence in Android Smartphones" *The International Journal of FORENSIC COMPUTER SCIENCE*, **1**, 28-43.

10- Rastogi, V., Chen, Y., and Jiang, X., (2013). Droid Chameleon: evaluating Android Anti-malware against Transformation Attacks. In: Symposium on Information, Computer and Communications Security (ASIA CCS). March. ACM, 329–334

11- De Jongh, M.; Klaver, C,; Der Knijff, R. and Roeloffs Breeuwsma, M. R. M.(2007). "Forensic Data Recovery from Flash Memory," *Small Scale Digital Forensics Journal*, **1(1)**, PP. 1-17

12- Raji,M. ; Wimmer, H. and Haddad, R. J., (2018). "Analyzing Data from an Android Smartphone while Comparing between Two Forensic Tools" Institute of Electrical and Electronics Engineers.

13- Dogan, S. and Akbal, E.,(2017). "Analysis of mobile phones in digital forensics," in 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 12411244.

14- Awan, (2015)."Forensic examination of social networking applications on smartphones," Conference on Information Assurance and Cyber Security (CIACS), pp. 36-43.

15- Lukito, N. Y. P. ; Yulianto, F. A and Jadied, E., (2016). "Comparison of data acquisition technique using logical extraction method on Unrooted Android Device," in 4th International Conference on Information and Communication Technology (ICoICT), pp. 1-6.

16- Aziz, N. A. ; Mokhti, F. and Nozri, M. N. M., (2015). "Mobile Device Forensics: Extracting and Analysing Data from an Android-based Smartphone," in Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec), pp. 123-128.

17- Bonomi, M.; Rochira, V.; Pasquali, D.; Balercia, G.; Jannini, E. A.and Ferlin, A. (2017). "Klinefelter syndrome (KS): genetics, clinical phenotype and hypogonadism". Journal of Endocrinological Investigation. 40 (2): 123–134.

18- Richard, A., (2013). ""The Advanced Data Acquisition Model (ADAM): A process model for digital forensic practice" (PDF). Murdoch University (2014)

19- BURNETTE, E. H.,(2008). Android. [S.l.]: Pragmatic Bookshelf, ISBN 978-1-934356-17-3

20- HASHIMI, S.; KOMATINENI, S.and MACLEAN, D. ,(2010).Pro Android 2. 1st Editon. ed. [S.l.]: ISBN 978-1-4302-2659-8.

21- EHRINGER, D.,(2017). The Dalvik Virtual Machine Architecture. David Ehringer, março 2008. Available at: <http://davidehringer.com/ software/android/The_Dalvik_Virtual_Machine.pdf>. [Accessed in: 17 February 2017].

22- GOOGLE INC. What is Android? Android Developers, 2011. Available at: http://developer.android.com/guide/basics/what-isandroid.html, Accessed in: 8 April 2017.

23- Ayers, R.; Brothers, S.and Janson, W. (2014). Guidelines on mobile device forensics. NIST Special Publication, Issue 800-101, May 2014, 25-32.

24- INFOSEC (2018). Computer forensics: mobile device hardware and operating system forensics. Retrieved on 2/18/108, from http://resources.infosecinstitute.com/category/computerforensics/introduction/mobile- forensics/mobile-device-hardware-and-operating-system-forensics/ [Accessed 5 August 2019].

25- Lutes, K. D. and Mislan, R. P., (2014). "Challenges in Mobile Phone Forensics" https://www.researchgate.net/publication/264884578.

26- Gratzner, V.; Naccache, D.and Znaty, D.,(2006). Law Enforcement, Forensics and Mobile Communications. Retrieved on Sept. 10, 2007 from http://www.cl.cam.ac.uk/~fms27/persec2006/goodies/2006-Naccache-forensic.pdf

27- Paraben. (n.d.). Paraben's Wireless StrongHold Bag. Retrieved on September 20, 2007 from http://www.parabenforensics.com/catalog/product_info.php?products_id=173

28- Ray, B., (2007). One plug to rule them all. The Register. Retrieved on September 21, 2007 from http://www.theregister.co.uk/2007/09/21/omtp_data_standard/[Accessed 15 August 2019].

29- Ayers, R.; Jansen, R.; Moenner, L.and Delaitre, A., (2007). Cell Phone Forensic Tools: An Overview and Analysis Update. Retrieved on Sept. 10, 2007 from http://csrc.nist.gov/publications/nistir/nistir-7387.pdf

30- Willassen, S., (2003). Forensics and the GSM Mobile Telephone System. International Journal of Digital Evidence. **2**, (1). Retrieved Sept. 10, 2007 from http://www.ijde.org/docs/03_spring_art1.pdf View

31- "Encryption "online https://source.android.com/security/encryption, [Accessed 1 August 2019].

32- http://www.t3k-forensics.com/allgemein-en/10-main-challenges-in-mobile-forensics2/

33- "Encryption full-disk "online https://source.android.com/security/encryption#full-disk, [Accessed 1 August 2019].

34- "Encryption file-based "online https://source.android.com/security/encryption#file-based, [Accessed 1 August 2019].

35- “Encryption metadata “online https://source.android.com/security/encryption#metadata, [Accessed 1 August 2019].

36- Al-Zarouni, M., (2006). "Mobile Handset Forensic Evidence: a challenge for Law Enforcement" Edith Cowan University.

37- Sudozai, M. A. Zk.; Saleem, S.; Buchanan, W. J. and Habib, N., Forensics Study of IMO call and chat app., *Digital Investigation*, 2018, **25**, 5-23

38- Wired, M. C., [Online]. 2016. Available from "https://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-justswitched-encryption-billion-people.

39- "http://www.mobiledit.com/forensic," MobileEdit, [Online]. Available: http://www.mobiledit.com/forensic. [Accessed 5 August 2019].

40- "oxygen-forensic," http://www.oxygen-forensic.com/en/, [Online]. Available: http://www.oxygen-forensic.com/en/. [Accessed 10 August 2019].

41- "Andriller," Andriller, [Online]. Available: http://andriller.com/. [Accessed 14 August 2019]