International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

Android based Mobile Forensic and Comparison using various Tools

Ms. Khyati Gajjar[1], Dr. Priyanka Sharma[2]

[1]Student, School of Information Technology & Cyber Security, Raksha Shakti University, Gujarat, India
[2]Director, Research & Development, Raksha Shakti University, Gujarat, India

---

Abstract: *Evolution in wireless technology and mobile phones are having huge impact on many aspects of daily lives. Number of consumers of this technology are increments and most of the individuals depends on it when correspondence and their uses are not only limited to personal but also in professional agendas. But long with appropriate use of smartphones there is room for its improper or illicit use by crooks as a tool of modus operandi. Consequently, there are confidential and sensitive data stored in smartphones which has potential of being a digital evidence in a process of investigation. But on the other hand investigators may come across many difficulties in extracting critical and vital information contained in an Android-based smartphone. The last segment of the paper presents the factual results of the tools via MOBILedit Forensic Express Dr.Fone, XRY, and Magnet AXIOM. To evaluate information and methodology of an extracting from an Android-based smartphone is the main aim of this work.*

Keywords: Forensics, Forensic Tools, Forensic Investigation.

1. INTRODUCTION

As Mobile Device turns out to be increasingly far reaching, Mobile phone forensics ends up being a consistently expanding number of critical as mobile phones are routinely found in crime scenes. Android-based Mobile phones and mobile's networks interface are becoming used for crime frequently. With the technological progression, forensic science has developed to an excellent extent. Forensic investigation processes usually as a rule consider the evidence gathered by the authorities and these confirmations are frequently inside the digital information and this procedure of analyzing the digital information is known as digital forensics.

Forensics is utilized through sorts of states from inside during a corporate reviewing case to a criminal investigation case regularly observed inside the enforcement world. Numerous crimes and different unfortunate activities make forensics essential as a method for making the world a far superior position. Advanced crime scene investigation is turning out to be significant in light of the fact that our general public is getting increasingly dependent on different computers and media transmission devices and technologies. Smartphone crime scene investigation, being a lot of crime scene investigation, centers around the recovery or gathering of information and evidence from smartphones and similar devices utilized in way of lifestyle.

Nowadays digital device is boundless to 'computer'. Today digital device incorporates mobile phones, PC, tablet or any electronic gadget. The measurable investigation process doesn't rely on the kind of advanced device utilized, rather the procedure of investigation is that the equivalent for each sort of digital devices. The investigation procedure mostly creates three states Data Acquisition which needs to gain the data from the device if it's inside the reliable condition and through a damaged condition the impression of the device is given which is utilized to information recovery. Following stage is that the Analysis during which the data gained is investigated for proof assortment and the last stage is safeguarding which includes having the data and the evidence assembled in secure conditions which further should be possible for the presentation of evidence within the court of law.

The Android-based PDAs are getting the most well-known devices for the latest decade. They're increasing even a progressively conspicuous bit of the pie with the exponential pace of improvement. The technique for thinking for the affirmation of those devices is that they're conservative, cost effective, acceptable and simple to utilize. Android-based mobile phones give a collection of features and data driven information like data records, contact numbers, install applications, games and lots of something different. This data from these devices are as often as possible removed using a couple of measurable devices. Which are both open source and commercial source. In any case, there's nobody comprehensive technique that may be utilized with 100% surety to get data from Android-based smart phones during a forensically strong way. Affirmations from the Android smartphones have accepted an incredibly fundamental activity starting late. The set up approach to manage forensic crime scene investigation is regularly off-base for Android PDAs. In this way, gathering evidence of the Android-based smartphones by set up structures of forensic confirmation is unpredictable and testing.

The present android world can be named as Android World Numerous devices run on Android, however Android is extensively utilized on PDAs. Around 90% operating system of the mobile phones is running on Android, and the vast majority are utilizing Android operating system in a few or the other way. Essentially

three kinds of portable based mobile forensics. For example, Android, iOS, and Windows mobile crime scene investigation. Be that as it may, discussing about mobile forensics legitimately takes us to Android mobile forensics since it is the most famous operating system in the android endeavour. Subsequently, Investigators should know about all the strategies and procedures are utilized for extricating information from Android device. One could extract information like SMS, contacts, installed applications, GPS information and Electronic mails, deleted information.

The purpose of a Mobile Device forensic tool is to assemble data from a Mobile Device without altering the information. The tool should provide crucial updates in time to stay moving with the rapid changes of Mobile Device hardware and software. The tools are often either forensic or non-forensic, all of them providing various challenges also as allowing different solutions.

The purpose for a mobile phone legal instrument is to assemble information from a mobile phone without adjusting the data. The apparatus ought to give essential updates so as to remain moving with the fast changes of mobile phone equipment and programming. The apparatuses are frequently either legal or non-legal, every one of them giving different difficulties additionally as permitting various solutions.

1.1. MOBILE FORENSICS

Mobile phone forensic is a domain of gathering digital evidences from cellular and mobile phones for an investigation or analysis purpose. Mobile Forensics isn't just limited to android based smartphone, but it also covers GPS location traces, tablets and other smartphones. The major objective in Mobile Forensics is recovery and analysis of information from external memory cards, SIM, internal memory with control and integrity of information.

Mobile forensics is considered one important part among the advanced crime scene investigation and also known as digital forensics. Generally regular civil and criminal investigations include a computerized part. Mobile phones become important evidence all over and play such a curious role for data analysis, there's a large chance those mobile phones have footprints and data relevant to the case . There are four different ways a mobile is regularly attached to crime scenes:

- It is majorly utilized as a device in the way of performing a digital attack.
- It's regularly a tool giving evidence and footprints related to crime.
- It will contain vital information regarding the crime and victim.
- It's regularly a method for carrying out a crime.

1.2. ACQUISITION & ANALYSIS OF THE EVIDENCE AND DATA

The Android operating system is based on Linux 2.6 that acts like a middle person between the device and the rest of the device stack. The Linux bit manages the arrangement of various administrations, for example, process, memory, execution and organize convention stack, drivers, and security. The structure and processes utilized in android uses object-situated methodology and permits reuse of existing Framework, Java and C/C++ libraries.

1.2.1. ANDROID ARCHITECTURE

The architecture of the Android system depends on Linux 2.6 kernel. Linux is that core of the android which lives at the android's foundation outline. Controlling the association, relationship of memory and different jobs are there that Linux is capable and is equipped for getting characters. The local libraries is another catalyst to Linux like SQLite is patch for the database. Free type library is utilized for appreciating the sound and media recording. Android runtime comprises of differed libraries. The android structure is additionally perfect because of applications.

1.2.2. CHAIN OF CUSTODY

A common forensics crime scene investigation process must be applied in all legal forensics investigation. The cellular phones or a computer which comprises of recognizing the potential evidence are identified with the case. The investigators will obtain details in a legal and proper way with its appropriate strategies. The evidences and data obtained should be kept in a legitimate cover and location using proper chain of custody.

1.2.3. TYPES OF ACQUISITION

All the data required for a digital forensic case today is present in the memory modules and hardware of the device. The smart devices uses two memory types and storing mechanisms. For example, non-volatile or the secondary storage and volatile or the unstable memory additionally perceived as the RAM. Investigators and the Acquisition of certain two sorts of memory will contribute forensic agents a decent measure of conceivable proof.

Logical acquisition:

This data extraction is done primarily to get basic device data, this extraction do not extracts the unallocated space's data. Without any root of the device it extract's the data which is a main advantage but in this deal with only presented data do not deal with the deleted data. The investigator should know the issue with connection the device then they have to deal with the data extraction in another way.

Physical acquisition:

Physical acquisition techniques of evidence extraction is used to extract the information with the help of access of the flash memory of the device. It creates a mobile device bit-by-bit copy. It further supports the extraction of a deleted record. The local devices that are available in the market usually not support this type of extraction method without the user being accessed to root, to eradicate these problems two different techniques are used i.e., JTAG also known as Joint Test Action Group and Chip-off. These two types of acquisitions can be performed on both rooted and non-rooted mobile devices to fetch the data and information.

Manual Acquisition:

Manual acquisition is an easy method to retrieve data from an Android-based smartphone. The investigator uses the mobile keypad to get the mobile device content. The main advantage of that it is the most convenient and it does not require any training for the investigator to know how to retrieve phone content. It operates with all mobile models and does not require any cables to perform data acquisition. It does not extract all data on the Android-based smartphone such as deleted and hidden files.

2. TOOLS AND METHODOLOGY

The amount in usage of cellular based mobile devices are increasing rapidly. The main challenge to forensic investigation is the change of development and technology at rapid pace. The tools developed today may not be compatible with the devices developed later, so a continuous process is required to update the database and technology used in forensic analysis. The following are a two experimental cases using various mobile devices and forensic tools:

Two physical cellular android based mobile devices Samsung Galaxy J4 plus (unrooted) and VIVO1812 (unrooted) were taken and tested with the different data extraction tools. The results and processes explained in the next section are gathered from MOBILedit Forensic and Dr.Fone for the device Samsung Galaxy J4 plus. Also utilized from XRY and Magnet AXIOM for VIVO1812 Mobile phone.
The following table describes the data that can be fetched from the listed hardware systems:

Table: I List of Mobile forensics Tools

Mobile Forensics Tools (Commercial)	MOBILedit Forensics ,MSAB XRY,Oxygen Forensic Cellebrite UFED, Magnet AXIOM Examine
Mobile Forensics Tools (Free)	MOBILedit Lite , Bitpim, Autopsy, dr.fone MIRACLE THUNDER andriller-master

2.1. PRE-REQUISITES

The primary step for unlocked phones, to get into developer mode and USB Debugging is mentioned below**:

Go to Setting >> About Phone >> Software Information >> 7 times tap on Build Number >> On the Developer Option and display in Settings.

Go to Developer Option >> Allow Development Setting >> Stay Awake >> USB debugging.
USB debugging should be turned ON.

**The steps may change as per different manufacturer and mobile phone model.

2.2. SETUP FOR THE EXPERIMENTS

In order to understand the data extraction techniques used in this project an experimental setup was created. Two physical devices with Android based smartphone Samsung J4 plus (version 9) and VIVO1812. The work is being carried out to do a comparative analysis of the forensic data extracted from the commercially available tools with open source tools.

2.3. EXPERIMENT 1:

In this Experiment, tools used are MOBILedit Forensics Express and Dr.Fone for the device Samsung Galaxy J4 plus.

2.3.1. ANALYSIS WITH MOBILEDIT FORENSICS EXPRESS

MOBILedit Forensic Express is an open-source tool for mobile device forensics which can be used to fetch deleted data, contact details, chats, Graphic files, call details, IMEI, multimedia messages, calendar items, data files, passwords, and data from various installed application such as Skype, Dropbox, Facebook, WhatsApp etc. The extracted files can be analyzed through analyzers. A backup of the seized mobile device can be created for further investigation as experimental basis and to maintain the integrity of the device seized. Features like lock bypass, backup, decryption, Cloning SIM Card and retrieval of Application data are provided in the commercial version tool.

Fig 1: Device Information in MOBILedit Forensic Express

An Android phone can be connected to a PC by USB cable, which transfers data secure and faster.
In this Practical We choose the Full content of the Mobile device for extracted and generated report in MS Excel and PDF Format.

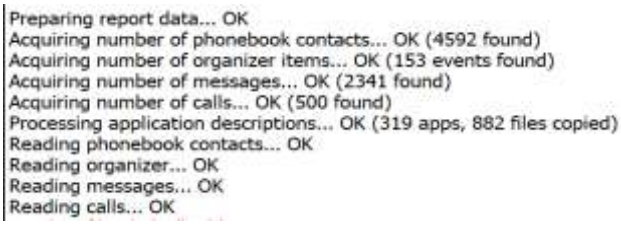

Fig 2: Displays Information about the ongoing extraction process

If you select the Data Extraction Log, you will get a brief resume of the extraction tab in File:

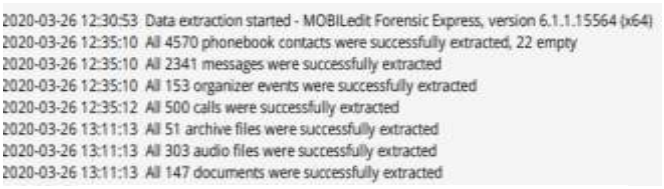

Fig 3. Display information about the extracted data

2.3.2. ANLAYSIS WITH DR.FONE

Dr**.** Fone is an opens source application that, allows you to get back photos and videos are deleted. After investigating your mobile device for photos and videos, it shows the results show in below figures. With ease, data can be recovered all the media content. Available features are Recover, Transfer, Unlock, Root, Erase in paid version of the application.

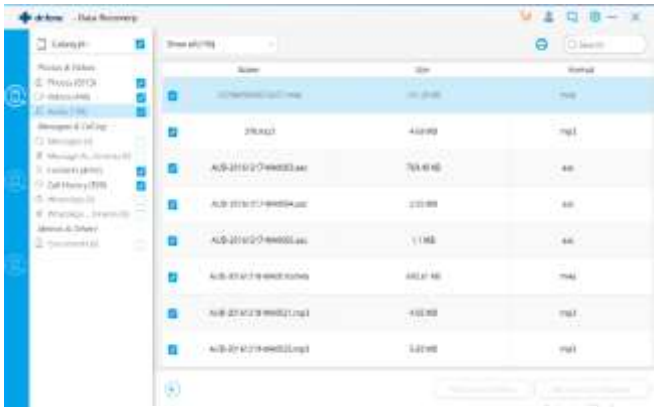

Fig 4. Display information of the Recover Data

2.3.3. COMPARISON OF MOBILEDIT FORENSICS EXPRESS AND DR.FONE

The proposed work in this project has introduced a unique method to extract data from a smartphone in a forensically sound manner which can be produced as evidence. The extraction of data from mobiles is majorly dependent on the available commercial software and tools. In the absence of these expensive commercial tools, it becomes difficult for a forensic investigator to extract data from the mobile based devices. Following are the results of the open source software used for data extraction of the evidence device:

Table-II The result of test data

Experimental parameters	Data extraction by: MOBILedit	Data extraction by :Dr.Fone
IMEI Number	Yes	No
Phonebook Contacts	Present(4570) Unknown(22)	Present(4592)
Call History	Present(500)	Present(500)
Messages	Present(2341)	No
Documents	Present(147)	No
Audio	Present (303)	Present (190)
Videos	Present(721)	Present(498)
Images	Present(11337)	Present(6913)

2.4. EXPERIMENT 2:

In this Experiment, Tools used are XRY and Magnet AXIOM for the mobile device VIVO1812.

2.4.1. ANALYSIS WITH XRY

XRY is a commercial mobile forensic tool. It provides a rapid extraction method to analyses and recover information from smartphones, GPS navigation system and tablets. It is a powerful and efficient system that runs on windows based operating systems which high performance hardware. It

helps to extract more data in less time duration with a great support towards different chipsets.

Following is the result** of extraction of a mobile phone VIVO1812.

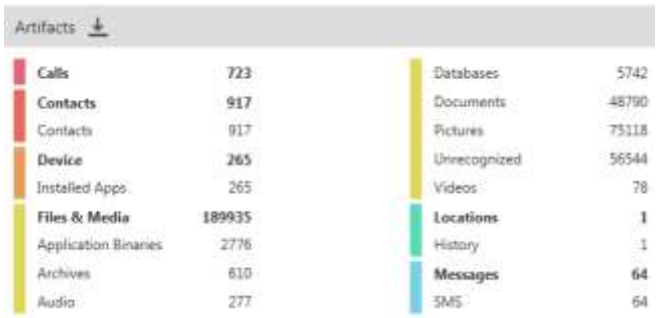

Fig 5: Display information of the Recover Data

**The image here only contains artifacts sections due to copyright protection.

2.4.2. ANALYSIS WITH MAGNET AXIOM

Magnet AXIOM is an intense digital investigation software allowing investigators and agencies to acquire, analyze and report data and evidence files. Image files can also be analyzed as evidence from mobile phones.

Following is the result** of extraction of a mobile phone VIVO1812.

Fig 6. Display information of the Recover Data

**The image here only contains artefacts sections due to copyright protection.

2.4.3 COMPARISION OF XRY AND MAGNET AXIOM

Table-III The result of test data

Experimental parameters	Data extraction by XRY	Data extraction by Magnet AXIOM
Media and Files	189935	36682
Phonebook Contacts	Present(917)	Present(917)
Calls	Present(723)	Present(723)
Messages	Present(64)	Present(64)
Documents	Present(48790)	Present(1532)
Audio	Present (277)	Present (277)
Videos	Present(78)	Present(78)
Images	Present(75118)	Present(75118)

3. COMPARISON OF OPEN SOURCE TOOLS

Table-IV The result of open source data

Parameter	MOBILedit	Dr.Fone
Operating System platform	Windows XP/ 2003/ Vista/ Windows7/8/10	Windows XP/ 2003/ Vista/ Windows7/8/10
Supported OS	iOS, Android Symbian, Windows (Limited to contacts and media files)	iOS, Android Symbian, Windows (Limited to contacts and media files)
Connection via	USB Cable, Wi-Fi, Bluetooth, Infrared	USB Cable
IMEI Number	Yes	No
Physical Data Acquisition	No	Yes
Logical Data Acquisition	Yes	No
Deleted Data Recover	Yes	No
Type of evidence recovered	Full content of mobile device	Contacts, Photos, Videos
Output format	MS Excel, PDF	-

4. COMPARISON OF COMMERCIAL TOOLS

Table-V The result of commercial source data

Parameter	MOBILedit	Dr.Fone
Operating System platform	Windows XP/ 2003/ Vista/ Windows7/8/10	Windows XP/ 2003/ Vista/ Windows7/8/10
Supported OS	iOS, Android Symbian, Windows (Limited to contacts and media files)	iOS, Android Symbian, Windows (Limited to contacts and media files)
Connection via	USB Cable, Wi-Fi, Bluetooth, Infrared	USB Cable
IMEI Number	Yes	Yes
Physical Data Acquisition	Yes – for rooted devices	Yes – for rooted devices
Logical Data Acquisition	Yes	Yes
Deleted Data Recover	Yes	Yes
Type of	Contacts,	Contacts,

evidence recovered	Graphics, messages, System files, Web files, Location history etc.	Graphics, messages, System files, Web files, Location history etc.
Output format	MS Excel, PDF,HTML	MS Excel, PDF,HTML

5. CONCLUSION

With the help of open-source and commercial digital forensic tools like MOBILedit Forensic Express, Dr.Fone, XRY, Magnet AXIOM aspects such as SMS, Calls, Images, Audio, Videos, Contacts, IMEI Number and Documents can be stored for further examination. MOBILedit Forensic Express comes by a write blocker (read-only) feature to ensure the integrity of the mobile phone is maintained and the evidence is not infected. Realizing digital forensics on mobile phone devices that are in different platforms and proprietary is really a challenge for forensics analyst. Data staying on Android-based smartphones can be extracted using the right tools and processes. It is necessary to recognize the phone architecture, operating systems, Mobile forensic process and forensic tools before doing the data extraction and recovery of data. Data from the Contact List, Call, Images, Videos, Audio, Document and SMS are managed to be extracted. Relevant data can be singled out and analysed for law enforcement to relate those evidence to the case. Such digital evidences can then be produced to the court. The data extraction for several android smartphones changes based on their architecture, models and their manufacturer established pattern.

REFERENCES:

[1] Ahmed, Rizwan & Dharaskar, Rajiv. (2008). Mobile Forensics: the study of collecting digital evidence from mobile device.

[2] Aziz, N.A. & Mokti, Fakhrulrazi & Nadhar, Mohd. (2015). Mobile Device Forensics: Extracting and Analysing Data from an Android-Based Smartphone. 10.1109/CyberSec.2015.32.

[3] Lohiya, Ritika & John, Priya & Shah, Pooja. (2015). Survey on Mobile Forensics. International Journal of Computer Applications. 118. 6-11. 10.5120/20827-3476.

[4] Agrawal, Animesh & Khatri, Pallavi & Sinha, Sumitra. (2018). Comparative Study of Mobile Forensic Tools. 10.1007/978-981-10-8360-0_4.

[5] Hazra, Sudip & Mateti, Prabhaker. (2017). Challenges in Android Forensics. 286-299. 10.1007/978-981-10-6898-0_24.

[6] Ahmed, Rizwan. "Mobile Forensics: An Introduction from Indian Law Enforcement Perspective". Retrieved 2 January 2014.

[7] Ahmed, Rizwan & Dharaskar, Rajiv. (2008). Mobile Forensics: an Overview, Tools, Future trends and Challenges from Law Enforcement perspective.

[8] https://resources.infosecinstitute.com/category/computerforensics/introduction/mobile-forensics/the-mobile-forensics-process-steps-types/

[9] Aldolah, Abdulalem & Shukor, Abd & Razak, Shukor & Othman, Siti & Mohammed, Arafat & Saeed, Faisal. (2017). A metamodel for mobile forensics