TALLINN UNIVERSITY OF TECHNOLOGY

School of Information Technologies

Fahad Alamgir - 194335IVCM

A Risk Based Decision Approach for Handling Digital Device at a Crime Scene

Master's Thesis

Supervisor: Dr. Matthew James Sorell, PhD
Center for Digital Forensics
and Cyber Security
Tallinn University of Technology,
Tallinn, Estonia
Co. Supervisor: Alejandro Guerra Manzanares, MSc.
Center for Digital Forensics
and Cyber Security
Tallinn University of Technology,
Tallinn, Estonia

Tallinn 2022

TALLINNA TEHNIKAÜLIKOOL

Infotehnoloogia Teaduskond

Fahad Alamgir - 194335IVCM

Riskipõhine otsus lähenemine jaoks käitlemine digitaalne seade juures kuritegevus stseen

Magistritöö

Juhendaja: Dr. Matthew James Sorell, PhD
Center for Digital Forensics
and Cyber Security
Tallinn University of Technology,
Tallinn, Estonia

Ühine. Juhendaja: Alejandro Guerra Manzanares, MSc.
Center for Digital Forensics
and Cyber Security
Tallinn University of Technology,
Tallinn, Estonia

Tallinn 2022

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Fahad Alamgir

15.04.2022

Abstract

In 21st century, mobile phones have become a primary medium for conducting communication and day to day tasks, such as text and multimedia messaging, audio and video calls, online shopping, online food ordering, online payments etc. Due to increased use of mobile phones, the number of criminal activities via mobile phones have also grown in recent years. When a mobile phone is discovered from a crime scene it always requires an extra amount of care to handle them despite a little unintentional action by first responder while securing a device could permanently destroy the potential digital evidence on it. The focus of this thesis study is to analyze and present the impact on digital evidence, when a first responder arrives to a crime location and attempts to secure a device by performing certain actions on the device i.e. enabling flight mode, remove sim, isolate the device etc. and presents risks associated with them.

List of Abbreviations

GCFIM	Generic Computer Forensic Investigation Model
DEFSOP	Digital Evidence Forensics Standard Operating Procedure
NIST	National institute of Standards & Technology
HDFI	Harmonized Digital Forensics Investigation
ADB	Android Debug Bridge
D.F	Degree of Freedom
JTAG	Joint Test Action Group

Table of Contents

List of Figures

List of Tables

1 Introduction

Since the launch of android devices in the market back in 2007 as an open source project [1]. New features in the android operating system are being continuously developed and released every few months. With new features, functionalities and supporting services, the smart phone has transformed the world into a digital world which has made the lives of the people easy and fast in doing any task. The ever evolving technological advancements also brings threats and safety issues to people in various forms such as phishing attacks, online frauds, contract killing, drugs smuggling, child pornography, terrorism etc. As the mobile phones are a primary medium of communication among people, they can be used as a source of witness to investigate the crime. The mobile phones now a days are very sensitive to intact digital evidence because of their touch and sensors features embedded to them. Whenever the first responder arrives to a crime location they must need to follow a sequence of steps to preserve a digital evidence while seizing a mobile device. The sequence of steps to preserve a digital evidence on the device may vary depending on the situation in which a device is discovered. In this study I have demonstrated the common sequence of steps followed by first responders at a crime scene on the device and analyzed the impact of those sequence of steps to digital evidence present on the device.

After the device is seized and brought to the laboratory an acquisition process is performed to obtain the digital copy of an original image of the phone. In this study I have used an open source android debug platform tools for the data acquisition from a device. Due to availability of wide variety of information collected from the mobile device during acquisition phase, so covering every possible impact on the device is out of the scope of this thesis and that’s why I have specifically analyzed the changes to WhatsApp application based on two reasons. One of them is its popularity among people worldwide and other is its security in terms of end to end encryption of communication. On the other hand, WhatsApp provides various forms of communications, such as One-to-One communication, group messaging, broadcast and multimedia messages as well [2].

1.1 Literature Review (Overview of Digital Forensics Processes)

The idea of conducting this thesis study is to identify impact of actions performed by first responder while securing a device from a crime scene and presents potential risks of choosing certain options over the other to secure a phone. The potential risks are those actions which are performed by a first responder or probably a digital forensics officer on a digital device in order to secure the digital evidence that could harm/corrupt the quality of evidence in such a way that may void its admissibility in a criminal court of justice. The first responder is responsible for making a search and evaluation plan on a scene to obtain the digital evidence [3]. First responder makes sure the security of investigation officers involved in digital forensics investigation process and prevent unauthorized access to the crime location to avoid any possible contamination to digital evidence at a crime scene [3].

Mobile forensics is considered as a branch of digital forensics which involves investigating mobile phones for possible digital evidence in a forensically safe and sound manner by gathering sources of evidence from different aspects [4]. Digital forensics Investigation process consists of a series of actions performed by digital forensics officer to collect, examine, analyze and report the digital evidence in a court [5]. In a similar manner mobile phone forensics process can be defined as a series of actions that a digital forensics investigation officer takes for securing a digital device from a crime scene. In mobile forensics many different kinds of frameworks have been designed to capture the potential digital evidence even when the phones were not common and cheap enough, and internet was not reachable to everyone. In today's age digital forensics is being used at a great scale in domains such as mobile forensics, network forensics, computer forensics, memory forensics etc [7].

The first article in the domain of digital forensics in year 1995 proposed four steps as sequential procedure (Acquisition, Identification, Evaluation, Admission as evidence) for acceptance of digital evidence in court [8]. In 2001 at digital forensics conference in USA Gary Palmer proposed digital forensics investigation standard process, the proposed model had seven steps such as (Identification, Preservation, Collection, Examination, Analysis, Presentation and decision making) [9].

Similarly, in 2002 Reith et al. developed an abstract form of digital forensics consists of nine steps such as (Identification, preparation, approach strategy, preservation, collection, examination, analysis, presentation, and returning evidence) [10]. Up to date many digital forensics process have been proposed i.e. In 2003 integrated digital investigation process (IDIP) was proposed by Carrier and Spafford supporting corporate and legal investigations [11].

In 2004, Baryamureeba and Tushabe presented an Enhanced Integrated Digital Investigation Process (EIDIP) approach which was developed on top of IDIP [12]. Beebe and Clark in 2005 presented multitier digital forensics investigation framework [13]. In 2006, cyber forensics field triage process model was proposed by Rogers et al [14]. In 2007, a framework was proposed from incorporating incident response and computer forensics by Freiling and Schwittay [15]. In 2008, a detailed review and methodology was proposed by Selamat et al. in the field of digital forensics investigation by connecting activities and processes into correct phases [16]. In 2010, a digital forensics readiness framework was proposed by Trček et al. with the use of service oriented architectures, sensor networks, interoperability stipulation [17]. In 2011, a detailed analysis based on literature review was presented by Agarwal et al. by mapping available models and recommended structural based model [18]. In 2012, an integrated digital forensics process model (IDFPM) was proposed by Michael Kohn by comparing the terminologies used in that time of frameworks and tried to standardize the model [19].

In 2013, Dr. Dhananjay and Nilakshi Provided a comparative approach towards digital forensics model (CDFM) [20]. In 2014, a digital forensics framework was presented by Quick et al. based data reduction and data mining technique for large volume of data [21]. In 2015, Jain and Kalbande studied and examined the strengths of twenty-five digital forensics framework and proposed a new framework with additional modules i.e. case registration, history keeper and evidence loader [22]. In 2016, Montasari presented a structured two-stage triage process model on site [23]. In 2018, Verma et al. presented an automated system of digital forensics using machine learning technique in response to data privacy challenge in investigation process [24]. In 2019, Shayau et al. proposed a framework to identify the modified files in a system and verified the integrity of the process with the help of hashing technique [25].

As big data is considered as a big challenge in digital forensics investigation process, in 2020. Song and Li proposed a digital forensics investigation framework focused on big data [26].

1.2 Background Study

In 2004 Barrie Mellars proposed the way a cellular phone network operates and how the data is processed between phone and its network, and he also described some forensics tools i.e. (Oxygen forensics manager, PhoneBase, Cell Seizure Paraben) that can be used during forensics examination and their strengths and weaknesses [27]. In 2005 Svein Willassen studied and experimented two methods for internal memory imaging of a mobile phone, the first method involved in desoldering memory circuits and reading the data off chip, and the other method involved using JTAG for internal memory imaging on several different models of the phone at that time [28]. In 2006, an overview study presented sim card forensics tools which described the efficiency of sim forensics tool and its suitability in digital forensics and introduced an open source *simbrush* tool to digital forensics community [29]. In 2007, a study conducted and proposed the forensics acquisition of Symbian smartphone data with the help of an on-phone forensics tool [30].

In many circumstances during criminal investigation it is very important to obtain and analyze the content on smartphone with less amount of time and the idea behind the on-phone forensics tool was to provide quick forensics facility because it does not require additional equipment and tools for forensics which are only available in forensics laboratory [30]. Although the on-phone forensics tool was not too efficient because of its capability to limited data acquisition so it is not suitable for acquiring complete logical acquisition of files and deleted data on the phone. In 2008, a method for overcoming obstacles in cell phone forensics was introduced [31]. The basic idea behind this study conducted in 2008 was to analyze the phone manager utility inside the phone, as a forensics medium to recover common user data such as pictures and phonebook, because every phone has a phone manager utility from its manufacturer provided for its user’s convenience, and due to the lack in availability of forensics techniques and tools that could suite to every model of mobile phone at that time, the technique was presented to provide a way to accomplish investigation in a smooth way and validating the results of available forensics tools.

In 2009, hashing techniques for mobile device forensics was proposed by comparing the hash values of a set of graphical files when they are transmitted using MMS, Bluetooth, Universal memory exchanger and Micro SD card [32]. This method is very vital in supporting the forensics investigation process and can be very helpful in determining the integrity of acquired evidence in a forensically sound manner. In 2010, android OS was making its place in the market with launch of new updates and features with different versions of software with different mobile phones since then a mobile forensics also expanded to android phones due to its popularity among the users. In 2010, a simplified way to examine the android based phones was proposed, which described the process of logical and physical acquisition of an android phone with the required tools to support the forensics investigation in an understandable format [33]. In 2011, Forensics analysis of android file system showed the extraction of data from a *SonyEricsson* phone in a logical and physical manner using a different methods and tools i.e. NANddump, dd command, xRecovery to understand the structure of available data [34].

In 2012 a study was conducted about forensics analysis of social networking applications on mobile phone manufactured by different companies and i.e. Blackberry, Apple, and google. All three phones had different operating systems i.e. blackberry OS, Apple IOS and Google Android. There were three popular social networking applications tested on these phones i.e. twitter, Facebook and Myspace. As social networking applications contains a certain amount of big information about people that’s why this experiment conducted to find out the information relevant to forensics investigation that can be useful for digital forensics officer [35]. In 2013 a study was conducted to show the data integrity of android based mobile phones during their forensics image acquisition with the help of Android Extractor tool which is developed in C++ and the study involved several experiments with different models of android based popular phones of the time and presents the results of experiments with several repetitions of acquisitions steps [36].

In 2014 a study about interpreting time stamps from a device under investigation described its correlation with events or evidence in real world environment to other devices and a case study was presented with a device whose time zone was set incorrectly and the clock was set in accordance with a time zone where the device was actually found, and in a number of experiments results the time zone database on the device was outdated and does not comply with actual time zone rules for a given period [37] . In 2015 an adversary model for android based mobile devices investigations discussed the possibilities of obtaining digital evidence from a phone by a digital forensics investigation officer as an adversary while ensuring the forensic soundness of the process and integrity of collected evidence [38]. In 2016 a study provided comparison among different mobile devices forensics investigation process models such as NIST guidelines, DEFSOP, Model for windows devices and HDFI model and proposed a model that could be suitable for every kind of mobile devices investigation [39]. In 2017 a study showed the support for mobile forensics in a form of workable process and analysis framework for android based mobile devices for solving cybercrime investigations with the help of open source tools i.e. *Linux command line utility* and Android *ADB* commands [40].

In 2018 a framework was developed aiming at validating the integrity of digital evidence after the digital forensics process completes with the help of comparing results from different mobile forensics investigation tools such as Encase, Oxygen forensics, FTK and Cellibrite namely and this study validates the mobile forensics tools and data stored in a mobile device to ensure the admissibility of evidence in court of law [41]. In 2019 a study showed the digital forensics analysis of android based mobile devices to handle cybercrime cases in the light of dummy cybercrime scenario and discuss the techniques for collecting digital evidence of a crime with forensics tools [42].

In 2020 Forensics analysis on third party mobile applications i.e. (Facebook messenger) demonstrated the methods to recover data items from the phone and categorized the user and application content on the phone, after uninstalling the application from the phone, the research used qualitative and quantitative approaches to accomplish the goal [43].

1.3 Research Question

As we have seen many different approaches for mobile forensics proposed by various researchers and authors based on mobile phones from different models, manufacturers, operating systems and supported features and functionalities and most of the methodologies, frameworks and processes defined above for mobile forensics are quite applicable in real world. In contrast to the previous studies this study demonstrates the impact of different actions on digital evidence present on the device. When the first responder tries to secure the device from a crime scene, and presents the risks involved in different actions performed by first responder on the device over a digital evidence and suggest a sequence of steps for decision making to avoid corruption of digital evidence at its minimum level.

1.4 Android Architecture

Android operating system is an open source platform for mobile phone, initially launched in the year 2007 as an open source project of google. With time and revolutionary features, it became the most popular operating system for mobile phones in the world. Due to increased use of android mobile phones and revolutionary its revolutionary technology stack it has become a common man choice due to cheap price as compare to IOS products. Mobile phones play an important role in our daily lives and it logs basically our every moment or activity on it. Mobile phone can become a companion of the digital forensics investigation officer in tracing a crime and finding a potential evidence about the real situation. The crimes can be online/offline i.e. murder or contract killing can provide useful information about the victim and culprit by analyzing data from the phone in a forensically sound manner. As the android platform is becoming bigger and bigger there is definitely a need for digital forensics investigation skills and expertise to solve critical cases.

Before going deep into the topic it is very essential to first understand the main architecture of the android operating system. Android operating system is based on linux kernel and uses EXT4 file system that contains necessary drivers for different hardware components i.e. Bluetooth, camera, display etc [47].

On top of kernel there is HAL that bridges the hardware with software to allow applications communication with relevant device drivers [47]. On above HAL the android native libraries are used to handle different types of data with the help of C++, C and assembly [47]. Android framework is next layer through which applications communicate directly, On the very top is the applications layer which is very essential to android architecture and for digital forensics as well because application layer contains user data and activities information [47].

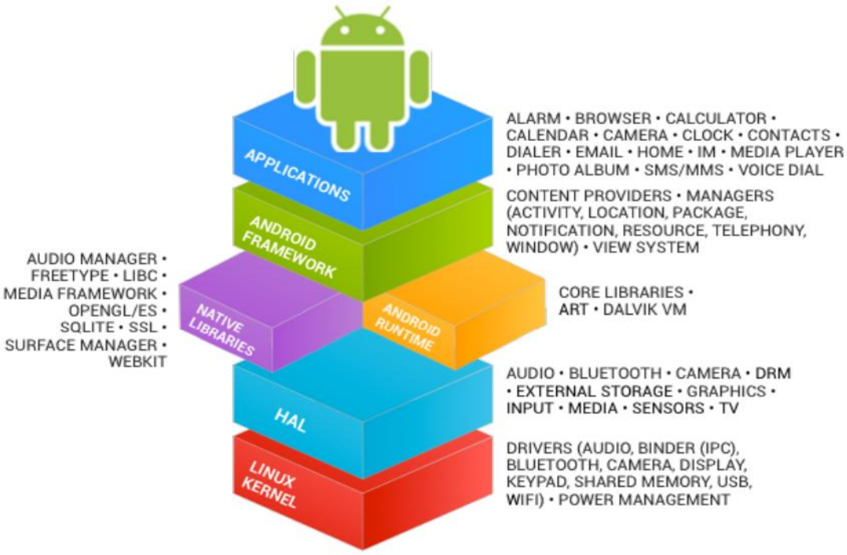

APPLICATIONS
ALARM • BROWSER • CALCULATOR • CALENDAR • CAMERA • CLOCK • CONTACTS • DIALER • EMAIL • HOME • IM • MEDIA PLAYER • PHOTO ALBUM • SMS/MMS • VOICE DIAL
ANDROID FRAMEWORK
CONTENT PROVIDERS • MANAGERS (ACTIVITY, LOCATION, PACKAGE, NOTIFICATION, RESOURCE, TELEPHONY, WINDOW) • VIEW SYSTEM
AUDIO MANAGER • FREETYPE • LIBC • MEDIA FRAMEWORK • OPENGL/ES • SQLITE • SSL • SURFACE MANAGER • WEBKIT
NATIVE LIBRARIES
ANDROID RUNTIME
CORE LIBRARIES • ART • DALVIK VM
HAL
AUDIO • BLUETOOTH • CAMERA • DRM • EXTERNAL STORAGE • GRAPHICS • INPUT • MEDIA • SENSORS • TV
LINUX KERNEL
DRIVERS (AUDIO, BINDER (IPC), BLUETOOTH, CAMERA, DISPLAY, KEYPAD, SHARED MEMORY, USB, WIFI) • POWER MANAGEMENT

Figure 1.0 Android Architecture layers [47]

1.5 Android Device Partitions

There are basically five partitions in android operating system such as.

(1) Boot: This partition contains the boot image which includes kernel and ram disk [47].

(2) System: In this partition we have system files that are installed when rom is flashed [47].

(3) Recovery: This is an alternative type of system partition used for flashing custom rom and this partition is important also for acquiring system partition image during forensics investigation [47].

(4) Userdata: This partition contains all installed applications and user data information and it is very important in forensics investigation [47].

(5) Cache: This partition has frequently access pieces of data [47].

2 Mobile Phone Forensics Triage Process

Mobile phone forensics process typically consists of the following steps in a forward way sequential order from identification of digital evidence to presentation of digital evidence in court.

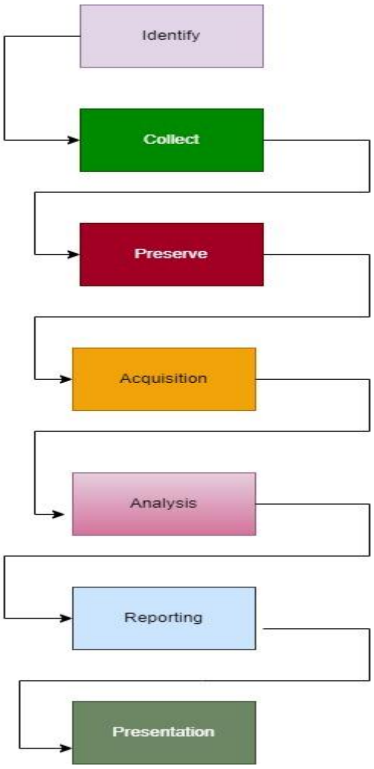


Figure 2.0 Digital Forensics Investigation Process Model

2.1 Identification

In this step a mobile device is being physically identified from a crime location as a helping resource in the criminal investigation process [6].

2.2 Collection

The collection phase involves recording of physical scene and collecting the digital evidence.

2.3 Preservation

In preservation step a mobile device is kept away in a separate box or Faraday bag from the possible sources or communication channels that could contaminate the digital evidence [6].

2.4 Acquisition

In the acquisition process of mobile device, a copy of an original image of a device is obtained in the lab in a forensically sound manner to avoid any possible loss of digital evidence due to certain factors i.e. short battery life or physically breaking the phone [6]. To avoid any kind of

potential damage to the digital evidence, the forensics investigation officers never work on the original image of a device.

2.5 Analysis

In the analysis phase a mobile device data is examined in a very careful manner to obtain relative sources of digital evidence that could provide meaningful insights about it [6]. For analysis phase a good amount of licensed tools are available which are commercially designed and developed for law enforcement.

2.6 Report

The documentation step involves a document which contains information about all kinds of digital evidence obtained from the digital device during an investigation process [6].

2.7 Presentation

The presentation step is the final step, where the evidence is being presented in criminal court of justice to proof the involvement of culprit in a crime [6]. If the evidence does not fulfill the court requirements, then the investigation process cycle can be repeated to identify more concrete proofs which are admissible in court, because sometimes a small mistake can diminish the value of evidence to be accepted in court. After identification of the device from a crime location in the preservation phase of the device, the digital forensics investigation officer tries to secure the phone using one or more options to isolate the device from the outside world to avoid any kind of intentional contamination to a digital evidence.

2.8 Phone Securement Options

There are basically five options available to a digital forensics officer for securing a phone from a crime scene.

(1) Flight mode
(2) Use of Faraday Bag
(3) Remove Sim from the device
(4) Removing the battery from a device
(5) Powered off the device

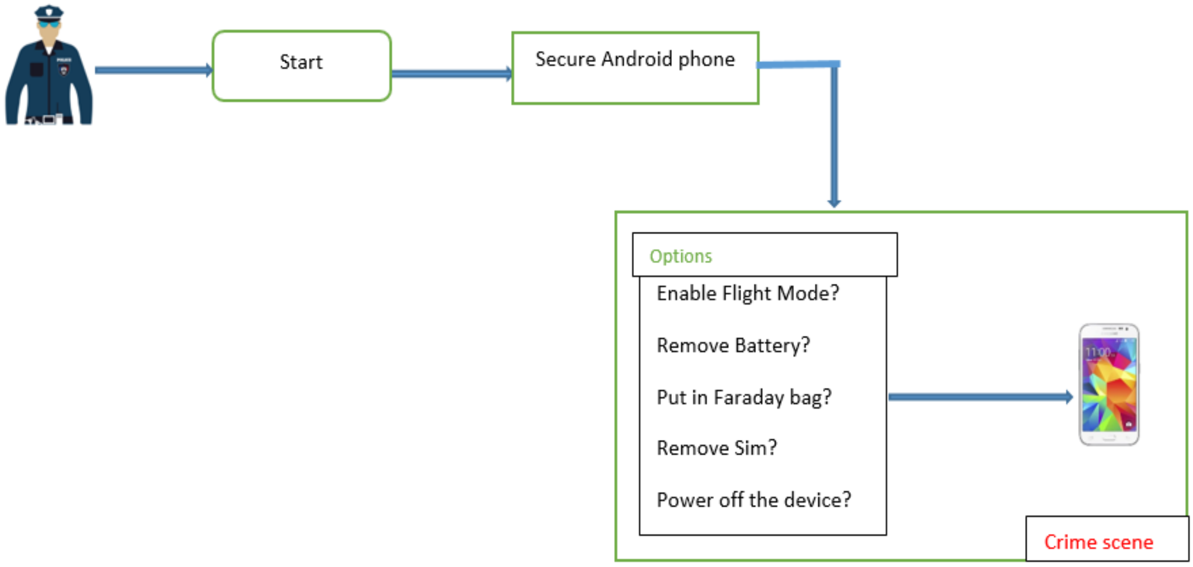


Figure 3.0 Securing a phone from crime scene

In this thesis I have used all five options for securing a phone from a crime location in a manner to cover all the possible sequences of actions such as given in the Table 1.0 below which are applicable to the phone I have used for this research.

A → represents flight mode
B → represents remove battery
C → represents Faraday bag
D → represents remove sim
E → represents power off

Table 1.0 Modes for securing a Phone

3 Digital Forensics Data Acquisition Techniques

The digital evidence is very fragile and it requires the device and forensics workstation to be handled with extraordinary care to avoid any contamination from any source to the data obtained from the device and requires documentation of events to be done throughout the process. Hence there are three popular data acquisition techniques used to gather information from the mobile phones to obtain a digital evidence from it.

3.1 Manual Data Acquisition

In manual data acquisition process, the information related to potential evidence is obtained by interacting with device and from its touch keypad and display screen. The pictures and videos are being taken throughout this process to document each and every aspect of the investigation process.

3.2 Logical Data Acquisition

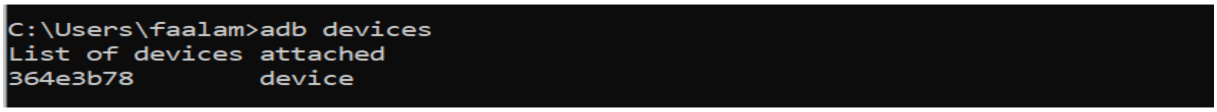
Logical data acquisition process for obtaining digital evidence from the device is considered as a bit-by-bit copy of logical storage objects from the allocated spaces on the device [6]. Logical acquisition of the data provides insights about the various categories such as contacts, pictures, ringtones, downloaded files, documents etc. from the mobile phone under forensics investigation in a limited capacity so that a forensics officer cannot access user data from the applications.

3.3 Physical Data Acquisition

Physical data acquisition process is considered as a bit-by-bit copy of device image which includes deleted data which has not been overwritten and data from unallocated space on the device's internal memory [33]. Physical acquisition of an android mobile phone provides access to a large collection of data on the device. Indeed, physical acquisition process plays an essential role in discovering the potential digital evidence on the device that is acceptable in the court of law. Usually the physically acquired data includes garbage files and certain amount of digital artifacts which cannot be obtained by performing logical and manual acquisition of data on the device. The very first stage of acquiring the physical image of the device involved accessing the super user rights or commonly known as root access to the device. To accomplish the goal of this thesis study, I have performed the logical and physical acquisition of data from the phone with little assistance of manual acquisition and analyzed the acquired data to understand the impact of actions performed by first responder on a digital device to a digital evidence.

3.4 Experimental Setup for Mobile Forensics

In this chapter I have demonstrated the laboratory environment that has been used to perform experiments to conduct this thesis. To setup the lab environment I have used android platform tools for windows which provides the android mobile device connectivity with windows operating system through ADB (Android Debug Bridge) that is a command line utility included in android platform tools. Using ADB we can easily interact with any android phone via ADB shell and can perform various functions such as access to files media and storage, remove files and directories, change permissions of files and directories, logical and physical acquisition of data present on the phone.



```
C:\Users\faalam>adb devices
List of devices attached
364e3b78        device
```

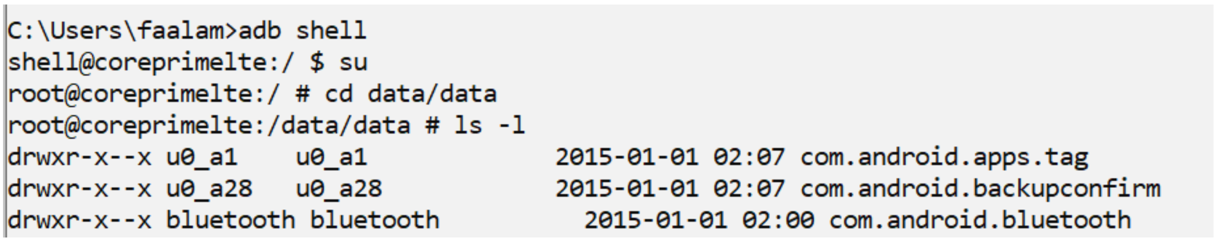
Figure 4.0 Adb command

An android based Samsung phone has been used to perform experiments with the following important specifications given below.

Mobile Phone Specifications	
Released Date	November, 2014. With Android version 5.0.2(Lollipop)
Model number	SM-G360F
Serial Number	364e3b78
IMEI (slot 1)	359360061719683
Android version	5.0.2 (Available since, 4th November, 2014)
Processor	Quad-core 1.2 GHz Cortex-A53
RAM	1GB
Storage memory	8GB
Network Technology	LTE
Battery Life	2000 mAh, removable

Table 2.0 Phone Specifications

Before starting the experiments, the root user access to the phone has been obtained so that access to user personal data from the applications on the phone can also be acquired easily. Because logical acquisition of data does not provide too many insights about the digital evidence as the deleted data is not recovered or obtained from the device.



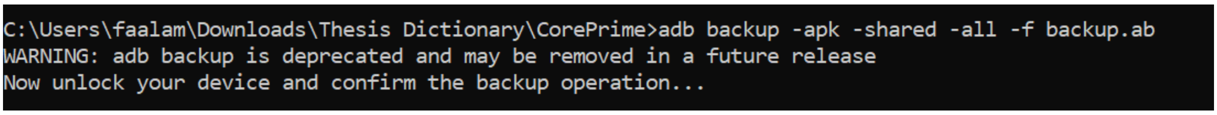
```
C:\Users\faalam>adb shell
shell@coreprimelte:/ $ su
root@coreprimelte:/ # cd data/data
root@coreprimelte:/data/data # ls -l
drwxr-x--x u0_a1     u0_a1             2015-01-01 02:07 com.android.apps.tag
drwxr-x--x u0_a28    u0_a28            2015-01-01 02:07 com.android.backupconfirm
drwxr-x--x bluetooth bluetooth           2015-01-01 02:00 com.android.bluetooth
```

Figure 5.0 Root user command

When the mobile device found at crime scene after identification, collection and preservation phase, it is brought up to digital forensics laboratory, where the digital forensics investigation officer performs data acquisition process on the phone using a forensically safe and sound forensics workstation with a digital forensics tool installed on it.

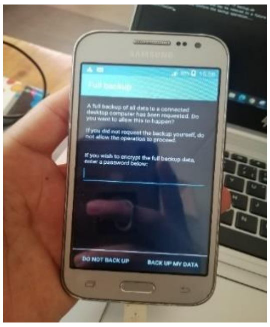
This study is solely relies on android ADB because it’s open source nature and compatibility with android phones despite the licensed tools are expensive and their access is restricted to law enforecement agencies mostly. Below the command to image the phone using android debug bridge is shown in figure 6.0, when the phone is brought to the laboratory a digital forensics investigation officer has mainly two options to obtain digital evidence from the device one is to perform logical acquisition and other is to perform physical acquisition the later one is needed to obtain deleted data artifacts from the phone and this process is very risky as compare to logical acquisition. We can perform logical and physical acquisition of data over the android phone using ADB and any licensed software based tool available in the market i.e. Cellibrite ,Magnet Axiom, Oxygen suite etc.

As we know, we can obtain logical image acquisition of the android phone with the help of android debug bridge. But before this, a usb debugging feature should be enabled on the phone from developer options. This command in figure 6.0, sends a request to image the phone that needs to be confirmed to obtain the image of the phone while it is connected with the forensics work station via a data cable. The image can also be obtained in a protected manner by providing password to encrypt it as shown in figure 7.0.



```
C:\Users\faalam\Downloads\Thesis Dictionary\CorePrime>adb backup -apk -shared -all -f backup.ab
WARNING: adb backup is deprecated and may be removed in a future release
Now unlock your device and confirm the backup operation...
```

Figure 6.0 Phone image command



A full backup of all data to a connected desktop computer has been requested. Do you want to allow this to happen?

If you did not request the backup yourself, do not allow the operation to proceed.

If you wish to encrypt the full backup data, enter a password below:

Figure 7.0 Image confirmation on phone

4 Methodology

To understand the impact on the digital evidence while securing a phone from a crime scene. I have used standard options to secure a phone from a crime scene shown in Table 1.0 and developed their several combinations shown in Table 4.0 and applied them to the android phone used in this study and analyzed and presented the changes to the digital evidence resides inside the phone using experimental research approach, when the phone is secured from a crime scene. This study particularly focuses on WhatsApp application on an android phone to indicate the impact of actions performed by first responder while securing a phone from a crime scene to the digital evidence.

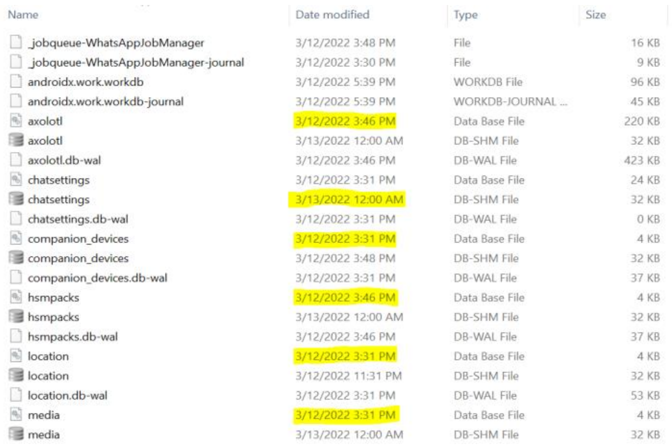
Usually there are six different ways to secure a phone from a crime scene to preserve the digital evidence on the device. But out of six methods, five are used as part of standard procedure to secure a phone from the crime scene which are defined in Table1.0.

4.1 Normal Mode

Normal mode acquisition of the phone is considered as securing a phone from a crime scene without enabling or disabling any feature on the phone. In figures (8-9) WhatsApp acquired database files are shown based on the following scenario-1, when the phone is in normal mode but disconnected from internet.

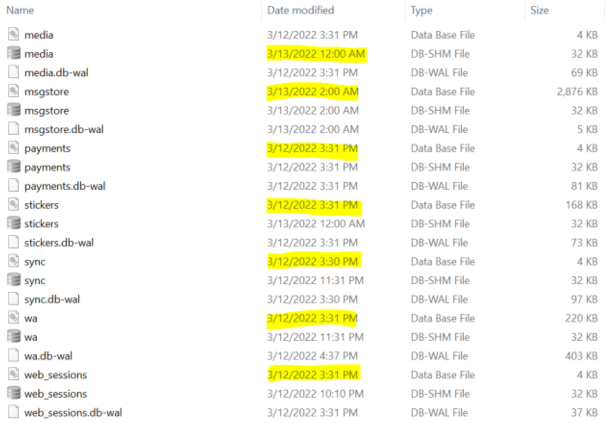
Scenario-1

The phone discovered from the crime scene at 10:30 am on 3/13/2022 and brought to the laboratory in normal mode without using any securement option. The phone image is created at 10:45 am on 3/13/2022 and these are the observed changes to the application database files. The time of database files can be seen to identify recent activities in time by the application itself.



Name	Date modified	Type	Size
_jobqueue-WhatsAppJobManager	3/12/2022 3:48 PM	File	16 KB
_jobqueue-WhatsAppJobManager-journal	3/12/2022 3:30 PM	File	9 KB
androidx.work.workdb	3/12/2022 5:39 PM	WORKDB File	96 KB
androidx.work.workdb-journal	3/12/2022 5:39 PM	WORKDB-JOURNAL ...	45 KB
axolotl	3/12/2022 3:46 PM	Data Base File	220 KB
axolotl	3/13/2022 12:00 AM	DB-SHM File	32 KB
axolotl.db-wal	3/12/2022 3:46 PM	DB-WAL File	423 KB
chatsettings	3/12/2022 3:31 PM	Data Base File	24 KB
chatsettings	3/13/2022 12:00 AM	DB-SHM File	32 KB
chatsettings.db-wal	3/12/2022 3:31 PM	DB-WAL File	0 KB
companion_devices	3/12/2022 3:31 PM	Data Base File	4 KB
companion_devices	3/12/2022 3:48 PM	DB-SHM File	32 KB
companion_devices.db-wal	3/12/2022 3:31 PM	DB-WAL File	37 KB
hsmpacks	3/12/2022 3:46 PM	Data Base File	4 KB
hsmpacks	3/13/2022 12:00 AM	DB-SHM File	32 KB
hsmpacks.db-wal	3/12/2022 3:46 PM	DB-WAL File	37 KB
location	3/12/2022 3:31 PM	Data Base File	4 KB
location	3/12/2022 11:31 PM	DB-SHM File	32 KB
location.db-wal	3/12/2022 3:31 PM	DB-WAL File	53 KB
media	3/12/2022 3:31 PM	Data Base File	4 KB
media	3/13/2022 12:00 AM	DB-SHM File	32 KB

Figure 8.0 WhatsApp Acquired database files



Name	Date modified	Type	Size
media	3/12/2022 3:31 PM	Data Base File	4 KB
media	3/13/2022 12:00 AM	DB-SHM File	32 KB
media.db-wal	3/12/2022 3:31 PM	DB-WAL File	69 KB
msgstore	3/13/2022 2:00 AM	Data Base File	2,876 KB
msgstore	3/13/2022 2:00 AM	DB-SHM File	32 KB
msgstore.db-wal	3/13/2022 2:00 AM	DB-WAL File	5 KB
payments	3/12/2022 3:31 PM	Data Base File	4 KB
payments	3/12/2022 3:31 PM	DB-SHM File	32 KB
payments.db-wal	3/12/2022 3:31 PM	DB-WAL File	81 KB
stickers	3/12/2022 3:31 PM	Data Base File	168 KB
stickers	3/13/2022 12:00 AM	DB-SHM File	32 KB
stickers.db-wal	3/12/2022 3:31 PM	DB-WAL File	73 KB
sync	3/12/2022 3:30 PM	Data Base File	4 KB
sync	3/12/2022 11:31 PM	DB-SHM File	32 KB
sync.db-wal	3/12/2022 3:30 PM	DB-WAL File	97 KB
wa	3/12/2022 3:31 PM	Data Base File	220 KB
wa	3/12/2022 11:31 PM	DB-SHM File	32 KB
wa.db-wal	3/12/2022 4:37 PM	DB-WAL File	403 KB
web_sessions	3/12/2022 3:31 PM	Data Base File	4 KB
web_sessions	3/12/2022 10:10 PM	DB-SHM File	32 KB
web_sessions.db-wal	3/12/2022 3:31 PM	DB-WAL File	37 KB

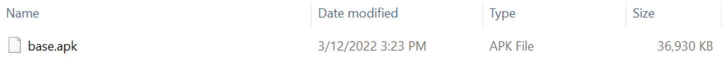
Figure 9.0 WhatsApp Acquired database files

4.2 Flight mode

When the first responder enables the flight mode on the phone to secure it from a crime scene, it will block all incoming and outgoing traffic from the device. In figure 10.0 WhatsApp acquired database files are shown based on scenario-2, when the phone is in flight mode.

Scenario-2

Phone has been discovered at a crime scene at 11:11 am on 3/13/2022 and first responder enables flight mode on the phone immediately after its identification and brought it to the laboratory. The phone's image is created at 11:21 am on 3/13/2022 while the phone remains in flight mode. The changes to the WhatsApp application files can be observed below. As we see in figure 10.0, the database files of WhatsApp do not appear in the phone's image because the backup of the application is not allowed by the application developer, when the phone is in flight mode. The permissions for backup an application are defined in AndroidManifest.xml file.



Name	Date modified	Type	Size
base.apk	3/12/2022 3:23 PM	APK File	36,930 KB

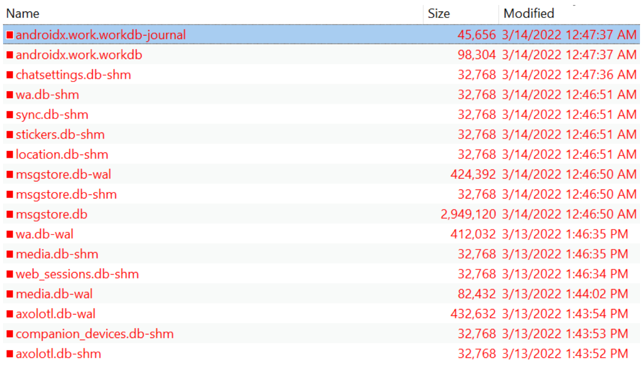
Figure 10.0 WhatsApp Acquired database files

4.3 Remove battery

When the first responder removes the battery from the phone to secure it from a crime scene to avoid battery depletion in Faraday bag. In figure 11.0 WhatsApp acquired database files are shown based on scenario-3.

Scenario-3

Phone has been discovered at a crime scene at 1:00 pm on 3/14/2022 and first responder removes the battery immediately from the phone to secure the digital evidence and brought it to the laboratory. The phone's digital image is taken at 1:30 pm on 3/14/2022 and the following changes to the WhatsApp application files can be observed.



Name	Size	Modified
androidx.work.workdb-journal	45,656	3/14/2022 12:47:37 AM
androidx.work.workdb	98,304	3/14/2022 12:47:37 AM
chatsettings.db-shm	32,768	3/14/2022 12:47:36 AM
wa.db-shm	32,768	3/14/2022 12:46:51 AM
sync.db-shm	32,768	3/14/2022 12:46:51 AM
stickers.db-shm	32,768	3/14/2022 12:46:51 AM
location.db-shm	32,768	3/14/2022 12:46:51 AM
msgstore.db-wal	424,392	3/14/2022 12:46:50 AM
msgstore.db-shm	32,768	3/14/2022 12:46:50 AM
msgstore.db	2,949,120	3/14/2022 12:46:50 AM
wa.db-wal	412,032	3/13/2022 1:46:35 PM
media.db-shm	32,768	3/13/2022 1:46:35 PM
web_sessions.db-shm	32,768	3/13/2022 1:46:34 PM
media.db-wal	82,432	3/13/2022 1:44:02 PM
axolotl.db-wal	432,632	3/13/2022 1:43:54 PM
companion_devices.db-shm	32,768	3/13/2022 1:43:53 PM
axolotl.db-shm	32,768	3/13/2022 1:43:52 PM

Figure 11.0 WhatsApp acquired database files

4.4 Use of Faraday Bag

When the first responder puts the phone in Faraday bag to secure it from a crime scene. It basically isolates the phone from the outside world while blocking any electromagnetic signals to the phone. In figure 11.0 WhatsApp acquisition database files are shown based on scenario-4.

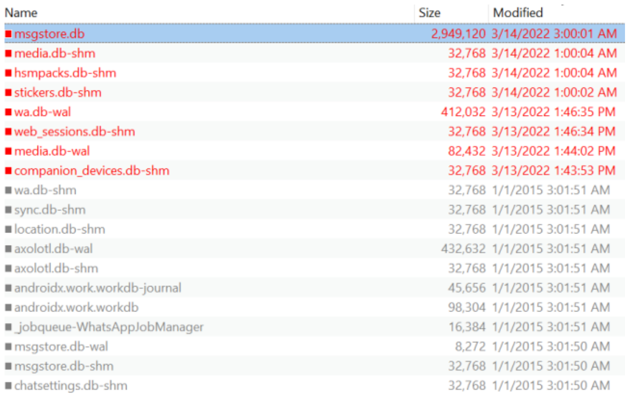
Phone has been discovered at a crime scene at 1:50 pm on 3/14/2022 and first responder removes the battery immediately from the phone to secure the digital evidence and brought it to the laboratory. The phone’s image is created at 2:00 pm on 3/14/2022 and the changes to WhatsApp application database files are similar to the mentioned in figure 11.0.

4.5 Removing SIM

When the first responder removes the battery from the phone to secure it from the crime scene. It will basically block any incoming sim calls and messages on the phone. In figure 12.0 WhatsApp database acquisition files are shown based on scenario-4.

Scenario-4

Phone has been discovered at a crime scene at 3:00 pm on 3/14/2022 and first responder removes the sim immediately from the phone to secure the digital evidence and brought it to the laboratory. The phone’s image is created at 3:30 pm on 3/14/2022 and the changes to WhatsApp application database files can be observed in figure 12.0.



Name	Size	Modified
msgstore.db	2,949,120	3/14/2022 3:00:01 AM
media.db-shm	32,768	3/14/2022 1:00:04 AM
hsmpacks.db-shm	32,768	3/14/2022 1:00:04 AM
stickers.db-shm	32,768	3/14/2022 1:00:02 AM
wa.db-wal	412,032	3/13/2022 1:46:35 PM
web_sessions.db-shm	32,768	3/13/2022 1:46:34 PM
media.db-wal	82,432	3/13/2022 1:44:02 PM
companion_devices.db-shm	32,768	3/13/2022 1:43:53 PM
wa.db-shm	32,768	1/1/2015 3:01:51 AM
sync.db-shm	32,768	1/1/2015 3:01:51 AM
location.db-shm	32,768	1/1/2015 3:01:51 AM
axolotl.db-wal	432,632	1/1/2015 3:01:51 AM
axolotl.db-shm	32,768	1/1/2015 3:01:51 AM
androidx.work.workdb-journal	45,656	1/1/2015 3:01:51 AM
androidx.work.workdb	98,304	1/1/2015 3:01:51 AM
_jobqueue-WhatsAppJobManager	16,384	1/1/2015 3:01:51 AM
msgstore.db-wal	8,272	1/1/2015 3:01:50 AM
msgstore.db-shm	32,768	1/1/2015 3:01:50 AM
chatsettings.db-shm	32,768	1/1/2015 3:01:50 AM

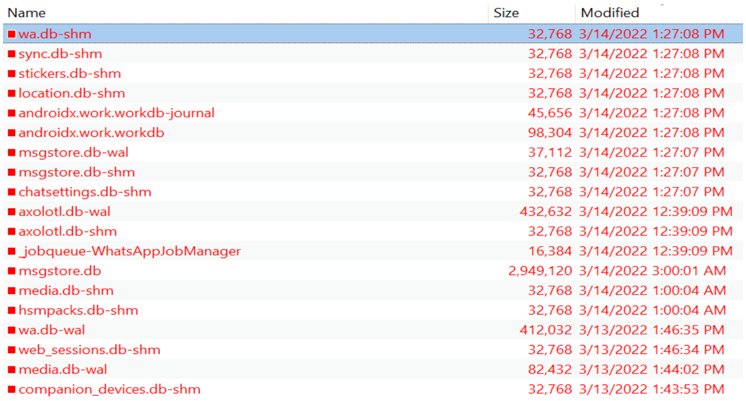
Figure 12.0 WhatsApp acquired database files

4.6 Switch Off the Phone

When the first responder power off the phone to secure it from a crime scene to avoid battery drainage. It will preserve the battery life but would result in loss of volatile data from the memory. In figure 13.0 WhatsApp acquisition database files are shown based on scenario-5.

Scenario-5

Phone has been discovered at a crime scene at 1:50 pm on 3/14/2022 and first responder switched off the phone immediately to secure the digital evidence and brought it to the laboratory. The phone's image is created at 2:00 pm on 3/14/2022 and the changes to WhatsApp application database files can be seen in figure 13.0.



Name	Size	Modified
wa.db-shm	32,768	3/14/2022 1:27:08 PM
sync.db-shm	32,768	3/14/2022 1:27:08 PM
stickers.db-shm	32,768	3/14/2022 1:27:08 PM
location.db-shm	32,768	3/14/2022 1:27:08 PM
androidx.work.workdb-journal	45,656	3/14/2022 1:27:08 PM
androidx.work.workdb	98,304	3/14/2022 1:27:08 PM
msgstore.db-wal	37,112	3/14/2022 1:27:07 PM
msgstore.db-shm	32,768	3/14/2022 1:27:07 PM
chatsettings.db-shm	32,768	3/14/2022 1:27:07 PM
axolotl.db-wal	432,632	3/14/2022 12:39:09 PM
axolotl.db-shm	32,768	3/14/2022 12:39:09 PM
_jobqueue-WhatsAppJobManager	16,384	3/14/2022 12:39:09 PM
msgstore.db	2,949,120	3/14/2022 3:00:01 AM
media.db-shm	32,768	3/14/2022 1:00:04 AM
hsmpacks.db-shm	32,768	3/14/2022 1:00:04 AM
wa.db-wal	412,032	3/13/2022 1:46:35 PM
web_sessions.db-shm	32,768	3/13/2022 1:46:34 PM
media.db-wal	82,432	3/13/2022 1:44:02 PM
companion_devices.db-shm	32,768	3/13/2022 1:43:53 PM

Figure 13.0 WhatsApp acquired database files

Similarly, I have demonstrated changes on WhatsApp application database files if the first responder chooses one or more options in combination to secure a phone from the crime scene. The options to secure a phone from a crime scene are mentioned in Table 3.0 and few possible combinations in figure 14.0

Steps	Options to secure a phone	Symbol representation
1	Flight mode	A
2	Battery remove	B
3	Faraday Bag	C
4	Remove Sim	D
5	Power off	E

Table 3.0 Phone securement options

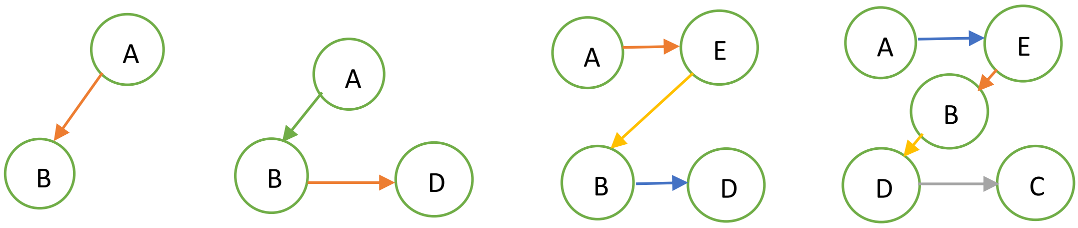


Figure 14.0 Possible combinations to secure a phone

In total, I have taken 45 different images from the phone where each image involves a different sequence of steps to secure a phone to preserve the digital evidence on the device by first responder. Before attempting to acquire each image from the phone, the phone is powered off and Powered on to remove some deep garbage from the system [50]. Since each sequence should have different impact on the digital evidence stored on the device hence at first I compared the size of databases files of WhatsApp application acquired from the phone in each image iteration. The size of database files obtained in each iteration can be seen in the Table 4.0 below.

No. of Image	Actions	Total Size
1	AB	5.35 MB
2	AC	5.35 MB
3	AD	5.36 MB
4	DA	5.36 MB
5	AE	5.37 MB
6	BD	5.39 MB
7	EB	5.39 MB
8	EC	5.40 MB
9	DE	5.40 MB
10	ED	5.41 MB
11	ABD	5.33 MB
12	AEB	5.34 MB
13	ACE	5.34 MB
14	CAE	5.35 MB
15	AEC	5.36 MB
16	ADE	5.36 MB
17	AED	5.37 MB
18	BCD	5.42 MB
19	CBD	5.43 MB
20	BDC	5.44 MB
21	EBC	5.45 MB
22	CEB	5.50 MB
23	ECB	5.50 MB

24	BDE	5.51 MB
25	EBD	5.53 MB
26	CDE	5.55 MB
27	ABCD	5.56 MB
28	ABDC	5.58 MB
29	BDAC	5.58 MB
30	BAEC	5.64 MB
31	ABEC	5.67 MB
32	AEBC	5.65 MB
33	BDAE	5.43 MB
34	AEBD	5.47 MB
35	AEDC	5.48 MB
36	BDCE	5.52 MB
37	EBDC	5.56 MB
38	EBCD	5.60 MB
39	ABCDE	5.62 MB
40	ACBDE	5.65 MB
41	ABDCE	5.70 MB
42	AEBCD	5.65 MB
43	ABCED	5.69 MB
44	AECBD	5.73 MB
45	AEBDC	5.76 MB

Table 4.0 Size in MB's of WhatsApp database files from Phone Image wise

These sequences of image acquisitions in Table 5.0, obtained from phone have similar effect on size of the WhatsApp application database files. As they all possess same size.

Sr. No	Sequence of Images
1	1,2,14
2	3,4,15,16
3	6,7
4	8,9
5	12,13
6	19,33
7	22,23
8	27,37
9	28,29
10	32,40,42

Table 5.0 sequence of Images

4.7 Timeline-I of WhatsApp Database Files Obtained

While the files sizes of most of the images obtained from the device are same. But there is a significant difference between the timestamps of the files. Time plays a very important role in every crime investigation process and digital forensics investigation heavily relies on interpretation of timestamps of the files obtained from a digital device to obtain a potential digital evidence against criminal because timestamps can provide the investigation officer a

chronological order of traces or digital footprints about the activities on the device [44]. From the given below timeline in Table 6.0 and Table 10.0. It can be easily visualized that how certain SQLite database, shared memory and write ahead log files time changes over each iteration. The SQLite files contain sensitive personal data about user such as chat messages, pictures, groups, phone number etc. which is shown in pictures below.

Securement Options	Database Files	Date Modified(AB)	Date Modified(AC)	Date Created(AB)	Date Created(AC)
AB vs AC	msgstore.db	3/19/2022 7:12:37 PM	3/19/2022 7:12:37 PM	3/19/2022 7:23:04 PM	3/19/2022 7:53:06 PM
	wa.db	3/19/2022 7:12:38 PM	3/19/2022 7:12:38 PM	3/19/2022 7:23:04 PM	3/19/2022 7:53:06 PM
	chatsettings.db	3/18/2022 3:54:17 PM	3/18/2022 3:54:17 PM	3/19/2022 7:23:04 PM	3/19/2022 7:53:06 PM
	media.db	3/17/2022 12:39:00 PM	3/17/2022 12:39:00 PM	3/19/2022 7:23:04 PM	3/19/2022 7:53:06 PM
AD vs DA	**Database Files**	**Date Modified(AD)**	**Date Modified(DA)**	**Date Created(AD)**	**Date Created(DA)**
	msgstore.db-shm	1/1/2015 2:00:55 AM	1/1/2015 2:01:22 AM	3/19/2022 8:11:09 PM	3/19/2022 8:30:02 PM
	wa.db-shm	1/1/2015 2:00:55 AM	1/1/2015 2:01:22 AM	3/19/2022 8:11:09 PM	3/19/2022 8:30:02 PM
	chatsettings.db-shm	1/1/2015 2:00:55 AM	1/1/2015 2:01:22 AM	3/19/2022 8:11:09 PM	3/19/2022 8:30:02 PM
	axolotl.db-shm	1/1/2015 2:00:56 AM	1/1/2015 2:01:23 AM	3/19/2022 8:11:09 PM	3/19/2022 8:30:02 PM
AE vs BD	**Database Files**	**Date Modified(AE)**	**Date Modified(BD)**	**Date Created(AE)**	**Date Created(BD)**
	msgstore.db-shm	3/19/2022 8:46:27 PM	1/1/2015 2:01:1 AM	3/19/2022 8:49:20 PM	3/19/2022 8:57:15 PM
	wa.db-shm	3/19/2022 8:46:27 PM	1/1/2015 2:01:01 AM	3/19/2022 8:49:20 PM	3/19/2022 8:57:15 PM
	location.db-shm	3/19/2022 8:46:28 PM	1/1/2015 2:01:02 AM	3/19/2022 8:49:20 PM	3/19/2022 8:57:15 PM
	axolotl.db-shm	3/19/2022 8:44:15 PM	1/1/2015 2:01:02 AM	3/19/2022 8:49:20 PM	3/19/2022 8:57:15 PM
EB vs EC	**Database Files**	**Date Modified(EB)**	**Date Modified(EC)**	**Date Created(EB)**	**Date Created(EC)**
	msgstore.db-shm	3/19/2022 9:02:08 PM	3/19/2022 9:08:57 PM	3/19/2022 9:04:19 PM	3/19/2022 9:12:07 PM
	wa.db-shm	3/19/2022 9:02:08 PM	3/19/2022 9:08:57 PM	3/19/2022 9:04:19 PM	3/19/2022 9:12:07 PM
	location.db-shm	3/19/2022 9:02:08 PM	3/19/2022 9:08:57 PM	3/19/2022 9:04:19 PM	3/19/2022 9:12:07 PM
	sync.db-shm	3/19/2022 9:02:09 PM	3/19/2022 9:08:58 PM	3/19/2022 9:04:19 PM	3/19/2022 9:12:07 PM
DE vs ED	**Database Files**	**Date Modified(DE)**	**Date Modified(ED)**	**Date Created(DE)**	**Date Created(ED)**
	msgstore.db-shm	1/1/2015 2:02:20 AM	1/1/2015 2:01:03 AM	3/19/2022 9:22:25 PM	3/19/2022 9:31:52 PM
	wa.db-shm	1/1/2015 2:02:21 AM	1/1/2015 2:01:04 AM	3/19/2022 9:22:25 PM	3/19/2022 9:31:52 PM
	location.db-shm	1/1/2015 2:02:21 AM	1/1/2015 2:01:04 AM	3/19/2022 9:22:25 PM	3/19/2022 9:31:52 PM
	sync.db-shm	1/1/2015 2:02:22 AM	1/1/2015 2:01:04 AM	3/19/2022 9:22:25 PM	3/19/2022 9:31:52 PM
ABD vs AEB	**Database Files**	**Date Modified(ABD)**	**Date Modified(AEB)**	**Date Created(ABD)**	**Date Created(AEB)**
	msgstore.db-shm	1/1/2015 2:01:41 AM	1/1/2015 2:00:57 AM	3/21/2022 12:57:25 PM	3/21/2022 1:06:07 PM
	wa.db-shm	1/1/2015 2:01:41 AM	1/1/2015 2:00:57 AM	3/21/2022 12:57:25 PM	3/21/2022 1:06:07 PM
	chatsettings.db-shm	1/1/2015 2:01:41 AM	1/1/2015 2:00:57 AM	3/21/2022 12:57:25 PM	3/21/2022 1:06:07 PM
	media.db-shm	1/1/2015 2:18:25 AM	1/1/2015 2:18:25 AM	3/21/2022 12:57:25 PM	3/21/2022 1:06:07 PM
ACE vs CAE	**Database Files**	**Date Modified(ACE)**	**Date Modified(CAE)**	**Date Created(ACE)**	**Date Created(CAE)**
	msgstore.db-shm	3/21/2022 1:27:37 PM	3/21/2022 1:41:05 PM	3/21/2022 1:31:30 PM	3/21/2022 1:56:17 PM
	wa.db-shm	3/21/2022 1:27:37 PM	3/21/2022 1:41:06 PM	3/21/2022 1:31:30 PM	3/21/2022 1:56:17 PM
	chatsettings.db-shm	3/21/2022 1:27:37 PM	3/21/2022 1:41:05 PM	3/21/2022 1:31:30 PM	3/21/2022 1:56:17 PM
	location.db-shm	3/21/2022 1:27:38 PM	3/21/2022 1:41:06 PM	3/21/2022 1:31:30 PM	3/21/2022 1:56:17 PM

	Database Files	Date Modified(AEC)	Date Modified(ADE)	Date Created(AEC)	Date Created(ADE)
AEC vs ADE	msgstore.db-shm	3/21/2022 2:14:02 PM	1/1/2015 2:02:08 AM	3/21/2022 2:17:40 PM	3/21/2022 2:27:15 PM
	wa.db-shm	3/21/2022 2:14:02 PM	1/1/2015 2:02:09 AM	3/21/2022 2:17:40 PM	3/21/2022 2:27:15 PM
	chatsettings.db-shm	3/21/2022 2:14:02 PM	1/1/2015 2:02:09 AM	3/21/2022 2:17:40 PM	3/21/2022 2:27:15 PM
	location.db-shm	3/21/2022 2:14:03 PM	1/1/2015 2:02:09 AM	3/21/2022 2:17:40 PM	3/21/2022 2:27:15 PM
AED VS BCD	**Database Files**	**Date Modified(AED)**	**Date Modified(BCD)**	**Date Created(AED)**	**Date Created(BCD)**
	hsmpacks.db-shm	3/21/2022 1:07:59 PM	1/1/2015 2:16:14 AM	3/21/2022 2:42:45 PM	3/21/2022 3:16:39 PM
	msgstore.db-wal	1/1/2015 2:00:55 AM	1/1/2015 2:00:57 AM	3/21/2022 2:42:45 PM	3/21/2022 3:16:39 PM
	media.db-shm	3/21/2022 1:07:59 PM	1/1/2015 2:16:14 AM	3/21/2022 2:42:45 PM	3/21/2022 3:16:39 PM
	stickers.db-shm	3/21/2022 2:38:34 PM	3/21/2022 3:06:29 PM	3/21/2022 2:42:45 PM	3/21/2022 3:16:39 PM
CBD vs BDC	**Database Files**	**Date Modified(CBD)**	**Date Modified(BDC)**	**Date Created(CBD)**	**Date Created(BDC)**
	msgstore.db-shm	31/1/2015 2:00:58 AM	1/1/2015 2:01:09 AM	3/21/2022 3:34:50 PM	3/21/2022 3:49:55 PM
	wa.db-shm	1/1/2015 2:00:59 AM	1/1/2015 2:01:10 AM	3/21/2022 3:34:50 PM	3/21/2022 3:49:55 PM
	axolotl.db-shm	1/1/2015 2:00:59 AM	1/1/2015 2:01:10 AM	3/21/2022 3:34:50 PM	3/21/2022 3:49:55 PM
	location.db-shm	1/1/2015 2:00:59 AM	1/1/2015 2:01:10 AM	3/21/2022 3:34:50 PM	3/21/2022 3:49:55 PM
EBC VS CEB	**Database Files**	**Date Modified(EBC)**	**Date Modified(CEB)**	**Date Created(EBC)**	**Date Created(CEB)**
	msgstore.db-shm	3/21/2022 4:11:38 PM	3/21/2022 9:02:44 PM	3/21/2022 4:14:40 PM	3/21/2022 9:05:30 PM
	wa.db-shm	3/21/2022 4:11:39 PM	3/21/2022 9:02:45 PM	3/21/2022 4:14:40 PM	3/21/2022 9:05:30 PM
	axolotl.db-shm	3/21/2022 4:03:10 PM	3/21/2022 4:27:45 PM	3/21/2022 4:14:40 PM	3/21/2022 9:05:30 PM
	location.db-shm	3/21/2022 4:11:39 PM	3/21/2022 9:02:45 PM	3/21/2022 4:14:40 PM	3/21/2022 9:05:30 PM
ECB VS BDE	**Database Files**	**Date Modified(ECB)**	**Date Modified(BDE)**	**Date Created(ECB)**	**Date Created(BDE)**
	msgstore.db-shm	3/21/2022 9:20:30 PM	1/1/2015 2:01:15 AM	3/21/2022 9:23:15 PM	3/21/2022 9:33:20 PM
	wa.db-shm	3/21/2022 9:20:30 PM	1/1/2015 2:01:15 AM	3/21/2022 9:23:15 PM	3/21/2022 9:33:20 PM
	axolotl.db-shm	3/21/2022 4:27:45 PM	1/1/2015 2:01:17 AM	3/21/2022 9:23:15 PM	3/21/2022 9:33:20 PM
	location.db-shm	3/21/2022 9:20:32 PM	1/1/2015 2:01:16 AM	3/21/2022 9:23:15 PM	3/21/2022 9:33:20 PM
EBD VS CDE	**Database Files**	**Date Modified(EBD)**	**Date Modified(CDE)**	**Date Created(EBD)**	**Date Created(CDE)**
	msgstore.db-shm	1/1/2015 2:01:09 AM	1/1/2015 2:03:05 AM	3/21/2022 10:14:17 PM	3/21/2022 10:47:24 PM
	wa.db-shm	1/1/2015 2:01:10 AM	1/1/2015 2:03:06 AM	3/21/2022 10:14:17 PM	3/21/2022 10:47:24 PM
	axolotl.db-shm	1/1/2015 2:01:10 AM	1/1/2015 2:01:02 AM	3/21/2022 10:14:17 PM	3/21/2022 10:47:24 PM
	location.db-shm	1/1/2015 2:01:10 AM	1/1/2015 2:03:06 AM	3/21/2022 10:14:17 PM	3/21/2022 10:47:24 PM
ABCD VS ABDC	**Database Files**	**Date Modified(ABCD)**	**Date Modified(ABDC)**	**Date Created(ABCD)**	**Date Created(ABDC)**
	msgstore.db-shm	1/1/2015 2:01:00 AM	1/1/2015 2:00:57 AM	3/21/2022 11:07:19 PM	3/21/2022 11:22:34 PM
	wa.db-shm	1/1/2015 2:01:11 AM	1/1/2015 2:00:57 AM	3/21/2022 11:07:19 PM	3/21/2022 11:22:34 PM
	axolotl.db	1/1/2015 2:01:02 AM	1/1/2015 2:00:58 AM	3/21/2022 11:07:19 PM	3/21/2022 11:22:34 PM
	location.db-shm	1/1/2015 2:01:01 AM	1/1/2015 2:00:57 AM	3/21/2022 11:07:19 PM	3/21/2022 11:22:34 PM
BDAC VS BAEC	**Database Files**	**Date Modified(BDAC)**	**Date Modified(BAEC)**	**Date Created(BDAC)**	**Date Created(BAEC)**
	msgstore.db-shm	1/1/2015 2:00:59 AM	3/21/2022 11:46:48 PM	3/21/2022 11:37:29 PM	3/21/2022 11:49:04 PM
	wa.db-shm	1/1/2015 2:01:00 AM	3/21/2022 11:46:48 PM	3/21/2022 11:37:29 PM	3/21/2022 11:49:04 PM
	axolotl.db	1/1/2015 2:01:01 AM	3/21/2022 11:43:14 PM	3/21/2022 11:37:29 PM	3/21/2022 11:49:04 PM
	location.db-shm	1/1/2015 2:01:00 AM	3/21/2022 11:46:48 PM	3/21/2022 11:37:29 PM	3/21/2022 11:49:04 PM
ABEC VS AEBC	**Database Files**	**Date Modified(ABEC)**	**Date Modified(AEBC)**	**Date Created(ABEC)**	**Date Created(AEBC)**
	msgstore.db-shm	1/1/2015 2:00:57 AM	3/21/2022 11:46:48 PM	3/22/2022 12:00:05 AM	3/22/2022 12:16:28 AM
	wa.db-shm	1/1/2015 2:00:58 AM	1/1/2015 2:01:02 AM	3/22/2022 12:00:05 AM	3/22/2022 12:16:28 AM
	axolotl.db	1/1/2015 2:00:58 AM	3/21/2022 11:43:14 PM	3/22/2022 12:00:05 AM	3/22/2022 12:16:28 AM
	location.db-shm	1/1/2015 2:00:58 AM	3/21/2022 11:46:48 PM	3/22/2022 12:00:05 AM	3/22/2022 12:16:28 AM

BDAE VS AEBD	**Database Files**	**Date Modified(BDAE)**	**Date Modified(AEBD)**	**Date Created(BDAE)**	**Date Created(AEBD)**
	msgstore.db-shm	1/1/2015 2:03:04 AM	1/1/2015 2:01:21 AM	3/22/2022 12:47:10 PM	3/22/2022 12:57:47 PM
	wa.db-shm	1/1/2015 2:03:04 AM	1/1/2015 2:01:02 AM	3/22/2022 12:47:10 PM	3/22/2022 12:57:47 PM
	axolotl.db	1/1/2015 2:03:05 AM	1/1/2015 2:01:22 AM	3/22/2022 12:47:10 PM	3/22/2022 12:57:47 PM
	location.db-shm	1/1/2015 2:03:05 AM	1/1/2015 2:01:21 AM	3/22/2022 12:47:10 PM	3/22/2022 12:57:47 PM
AEDC vs BDCE	**Database Files**	**Date Modified(AEDC)**	**Date Modified(BDCE)**	**Date Created(AEDC)**	**Date Created(BDCE)**
	msgstore.db-shm	1/1/2015 2:04:01 AM	1/1/2015 2:04:01 AM	3/22/2022 1:05:20 PM	3/22/2022 1:26:37 PM
	wa.db-shm	1/1/2015 2:00:56 AM	1/1/2015 2:04:02 AM	3/22/2022 1:05:20 PM	3/22/2022 1:05:20 PM
	axolotl.db	1/1/2015 2:00:56 AM	1/1/2015 2:04:03 AM	3/22/2022 1:05:20 PM	3/22/2022 1:05:20 PM
	location.db-shm	1/1/2015 2:00:56 AM	1/1/2015 2:04:02 AM	3/22/2022 1:05:20 PM	3/22/2022 1:05:20 PM
EBDC VS EBCD	**Database Files**	**Date Modified(EBDC)**	**Date Modified(EBCD)**	**Date Created(EBDC)**	**Date Created(EBCD)**
	_jobqueue-WhatsAppJobManager	1/1/2015 2:01:00 AM	1/1/2015 2:12:09 AM	3/22/2022 1:34:25 PM	3/22/2022 1:56:03 PM
	wa.db-shm	1/1/2015 2:00:59 AM	1/1/2015 2:12:08 AM	3/22/2022 1:34:25 PM	3/22/2022 1:56:03 PM
	axolotl.db	1/1/2015 2:01:00 AM	1/1/2015 2:12:09 AM	3/22/2022 1:34:25 PM	3/22/2022 1:56:03 PM
	location.db-shm	1/1/2015 2:00:59 AM	1/1/2015 2:12:08 AM	3/22/2022 1:34:25 PM	3/22/2022 1:56:03 PM
ABCDE VS ACBDE	**Database Files**	**Date Modified(ABCDE)**	**Date Modified(ACBDE)**	**Date Created(ABCDE)**	**Date Created(ACBDE)**
	_jobqueue-WhatsAppJobManager	1/1/2015 2:02:04 AM	1/1/2015 2:02:56 AM	3/22/2022 2:15:15 PM	3/22/2022 2:25:36 PM
	wa.db-shm	1/1/2015 2:02:03 AM	1/1/2015 2:02:55 AM	3/22/2022 2:15:15 PM	3/22/2022 2:25:36 PM
	axolotl.db	1/1/2015 2:02:03 AM	1/1/2015 2:02:56 AM	3/22/2022 2:15:15 PM	3/22/2022 2:25:36 PM
	location.db-shm	1/1/2015 2:02:03 AM	1/1/2015 2:02:55 AM	3/22/2022 2:15:15 PM	3/22/2022 2:25:36 PM
ABDCE VS AEBCD	**Database Files**	**Date Modified(ABDCE)**	**Date Modified(AEBCD)**	**Date Created(ABDCE)**	**Date Created(AEBCD)**
	_jobqueue-WhatsAppJobManager	1/1/2015 2:00:55 AM	1/1/2015 2:01:52 AM	3/22/2022 3:00:19 PM	3/22/2022 3:22:56 PM
	wa.db-shm	1/1/2015 2:15:31 AM	1/1/2015 2:01:51 AM	3/22/2022 3:00:19 PM	3/22/2022 3:22:56 PM
	axolotl.db	1/1/2015 2:00:55 AM	1/1/2015 2:01:52 AM	3/22/2022 3:00:19 PM	3/22/2022 3:22:56 PM
	location.db-shm	1/1/2015 2:15:31 AM	1/1/2015 2:01:51 AM	3/22/2022 3:00:19 PM	3/22/2022 3:22:56 PM
ABCED VS AECBD	**Database Files**	**Date Modified(ABCED)**	**Date Modified(AECBD)**	**Date Created(ABCED)**	**Date Created(AECBD)**
	_jobqueue-WhatsAppJobManager	1/1/2015 2:02:03 AM	1/1/2015 2:01:04 AM	3/22/2022 3:36:13 PM	3/22/2022 5:38:46 PM
	wa.db-shm	1/1/2015 2:02:02 AM	1/1/2015 2:01:03 AM	3/22/2022 3:36:13 PM	3/22/2022 5:38:46 PM
	axolotl.db	1/1/2015 2:02:03 AM	1/1/2015 2:01:04 AM	3/22/2022 3:36:13 PM	3/22/2022 5:38:46 PM
	location.db-shm	1/1/2015 2:02:02 AM	1/1/2015 2:01:03 AM	3/22/2022 3:36:13 PM	3/22/2022 5:38:46 PM
AECBD VS AEBDC	**Database Files**	**Date Modified(AECBD)**	**Date Modified(AEBDC)**	**Date Created(AECBD)**	**Date Created(AEBDC)**
	_jobqueue-WhatsAppJobManager	1/1/2015 2:01:04 AM	1/1/2015 2:01:01 AM	3/22/2022 3:36:13 PM	3/22/2022 5:57:42 PM
	wa.db-shm	1/1/2015 2:01:03 AM	1/1/2015 2:01:00 AM	3/22/2022 3:36:13 PM	3/22/2022 5:57:42 PM
	axolotl.db	1/1/2015 2:01:01 AM	1/1/2015 2:01:04 AM	3/22/2022 3:36:13 PM	3/22/2022 5:57:42 PM
	location.db-shm	1/1/2015 2:01:03 AM	1/1/2015 2:01:00 AM	3/22/2022 3:36:13 PM	3/22/2022 5:57:42 PM

Table 6.0 Timeline of WhatsApp database files

Apart from the standard procedure actions performed by first responder to secure a device to preserve digital evidence from a crime scene. I have conducted 30 other experiments with different possible methods to secure a device to preserve the digital evidence from the crime scene and presents the impact of those different actions in terms of size of WhatsApp database files obtained from phone’s image acquisition and timeline of files changes in shown in Table 10.0.

Securement Method 1 vs Securement Method 2			
1	First responder discovered a phone from a crime scene, while it has Wi-Fi off and the first responder enable flight mode and usb debug feature on the phone.	2	If the first responder chooses to enable flight mode on the phone and switched it off immediately.
3	If the first responder chooses to switch off the phone directly without enabling any feature on the phone as part of a securement process while assuming the phone was connected to internet during securement process, then when the phone will be turned on phone and gets connected to internet a WhatsApp message could arrive.	4	If the first responder tries to open WhatsApp during securement while the phone was disconnected from the internet.
5	If the first responder chooses to read all the incoming WhatsApp messages on the phone while it is disconnected from the internet.	6	If the first responder chooses to disconnect only internet on the phone while at the same time a WhatsApp messages is sent from another phone.
7	If the first responder chooses to read a single message while the phone is not connected to internet.	8	If the first responder chooses to send a WhatsApp message from the phone discovered at a crime scene and disconnect it from internet.
9	If the first responder chooses to read WhatsApp message on the phone while it is in flight mode.	10	If the first responder chooses to open WhatsApp and deletes one received message from the phone discovered at a crime scene from one to one chat.
11	If the first responder chooses to open WhatsApp and deletes one sent message from the phone discovered at a crime scene from one to one chat.	12	If the first responder chooses to send one WhatsApp message from the phone discovered at a crime scene while it is in flight mode.
13	If the first responder chooses to turn off the phone while it is connected to internet at the time of its discovery from a crime scene. When the phone	14	If the first responder chooses to put the phone in flight mode and tries to send a picture from the phone discovered at a crime scene.

	is turned on in the lab the digital forensics investigation officer disconnects it from the internet and enable flight mode and image the phone.		
15	If the first responder chooses to power off the phone discovered at a crime scene as part of securement procedure to preserve digital evidence. While the phone is powered off a WhatsApp message from another device is sent and when the phone is turned on a message is received.	16	If the first responder chooses to put the phone in flight mode while it has these features enable from swipe down window such as location, screen rotation, Bluetooth, NFC, sync, do not disturb mode
17	If the first responder chooses to write a message on the phone discovered at a crime scene while the phone was connected to the internet and suddenly puts the phone in flight mode as part of securement process and does not close the application.	18	If the first responder chooses to switch off the phone and remove sim while it is in flight mode.
19	If an SMS arrives at the time of image acquisition of the phone under investigation and the phone is in flight mode.	20	If the alarm rings during the time of image acquisition of the phone under investigation and the phone is in flight mode.
21	If the phone is discovered and it is already in flight mode and first responder disables the flight mode and the alarm rings at the time of image acquisition of the phone in the laboratory and digital forensics investigation officer turns it off.	22	If the call arrives to the sim of the phone under investigation during image acquisition process in laboratory while the phone is in flight mode.
23	If first responder chooses to secure a phone by enabling flight mode on the phone under investigation and reads a message.	24	If first responder reads a miscall on the phone and then enable the flight mode to preserve the digital evidence on the phone.
25	If first responder tries to call from the phone under investigation and reads one incoming message and then enable the flight mode to preserve the digital evidence on the phone.	26	If the digital forensics investigation officer tries to call from the phone under investigation when the image acquisition process of the phone under investigation is being conducted and phone is in flight mode. Phone asks to disable the flight mode for making a call and digital

			forensics investigation officer press okay and image acquisition process continues.
27	If the first responder chooses to attend an incoming call immediately after discovering the phone at a crime scene while the phone is in normal mode.	28	If the first responder chooses to cut an incoming call immediately after discovering the phone at a crime scene while the phone is in normal mode.
29	If the digital forensics investigation officer chooses to enable the flight mode on the phone during its image acquisition process in the laboratory.	30	If the digital forensics investigation officer chooses to disable the flight mode on the phone during its image acquisition process in the laboratory.

Table 7.0 Device Securement Methods

The size of WhatsApp application database files obtained in each image iteration which involves device securement methods based on Table 7.0 is given in the Table 8.0 below.

No. of Image	Total Size
1	5.82 MB
2	5.85 MB
3	5.84 MB
4	5.84 MB
5	5.85 MB
6	5.38 MB
7	5.85 MB
8	5.85 MB
9	5.85 MB
10	5.85 MB
11	5.85 MB
12	5.93 MB
13	5.92 MB
14	5.94 MB
15	5.95 MB
16	5.95 MB
17	5.95 MB
18	5.95 MB
19	5.52 MB
20	5.54 MB
21	5.56 MB
22	5.56 MB
23	5.56 MB
24	5.48 MB

25	5.63 MB
26	5.63 MB
27	5.65 MB
28	5.65 MB
29	5.65 MB
30	5.65 MB

Table 8.0 Size in MB’s of WhatsApp database files from Phone Image wise

These sequences of image acquisitions in Table 9.0, obtained from phone have similar effect on size of the WhatsApp application database files. As they all possess same size.

Sr. No	Sequence of Images
1	2,5,7,8,9,10,11
2	3,4
3	15,16,17,18
4	21,22,23
5	25,26
6	27,28,29,30

Table 9.0 sequence of Images

4.8 Timeline-II of WhatsApp Database Files Obtained

Securement Options	**Database Files**	**Date Modified(1)**	**Date Modified(2)**	**Date Created(1)**	**Date Created(2)**
1 vs 2	axolotl.db	4/13/2022 11:32:32 PM	3/28/2022 1:14:27 PM	3/28/2022 2:30:12 PM	3/28/2022 2:54:10 PM
	msgstore.db	4/13/2022 11:39:41 PM	3/28/2022 2:36:47 PM	3/28/2022 2:30:12 PM	3/28/2022 2:54:10 PM
	wa.db	4/13/2022 11:43:06 PM	3/28/2022 1:14:29 PM	3/28/2022 2:30:12 PM	3/28/2022 2:54:10 PM
	web_sessions.db	4/13/2022 11:40:46 PM	3/18/2022 4:58:01 PM	3/28/2022 2:30:12 PM	3/28/2022 2:54:10 PM
3 vs 4	**Database Files**	**Date Modified(3)**	**Date Modified(4)**	**Date Created(3)**	**Date Created(4)**
	web_sessions.db-shm	3/28/2022 3:01:57PM	3/28/2022 3:17:21PM	3/28/2022 3:05:59 PM	3/28/2022 3:22:43 PM
	wa.db-shm	3/28/2022 3:02:10 PM	3/28/2022 3:17:31PM	3/28/2022 3:05:59 PM	3/28/2022 3:22:43 PM
	sync.db-shm	3/28/2022 3:02:11 PM	3/28/2022 3:17:32PM	3/28/2022 3:05:59 PM	3/28/2022 3:22:43 PM
	location.db-shm	3/28/2022 3:02:10 PM	3/28/2022 3:17:32PM	3/28/2022 3:05:59 PM	3/28/2022 3:22:43 PM
5 vs 6	**Database Files**	**Date Modified(5)**	**Date Modified(6)**	**Date Created(5)**	**Date Created(6)**
	web_sessions.db-shm	3/28/2022 3:24:50 PM	3/28/2022 3:51:47 PM	3/28/2022 3:30:51 PM	3/28/2022 3:57:54 PM
	location.db-shm	3/28/2022 3:24:52 PM	3/28/2022 3:50:57 PM	3/28/2022 3:30:51 PM	3/28/2022 3:57:54 PM
	chatsettings.db-shm	3/28/2022 3:24:50 PM	3/28/2022 3:50:59 PM	3/28/2022 3:30:51 PM	3/28/2022 3:57:54 PM
	msgstore.db	3/28/2022 3:25:05 PM	3/28/2022 3:50:57 PM	3/28/2022 3:30:51 PM	3/28/2022 3:57:54 PM
7 vs 8	**Database Files**	**Date Modified(7)**	**Date Modified(8)**	**Date Created(7)**	**Date Created(8)**
	wa.db-shm	3/28/2022 3:58:59 PM	3/28/2022 4:03:40 PM	3/28/2022 4:02:38 PM	3/28/2022 4:21:27 PM
	location.db-shm	3/28/2022 3:59:00 PM	3/28/2022 4:03:40 PM	3/28/2022 4:02:38 PM	3/28/2022 4:21:27 PM
	chatsettings.db-shm	3/28/2022 3:58:59 PM	3/28/2022 4:10:35 PM	3/28/2022 4:02:38 PM	3/28/2022 4:21:27 PM
	axolotl.db-shm	3/28/2022 3:50:58 PM	3/28/2022 4:10:35 PM	3/28/2022 4:02:38 PM	3/28/2022 4:21:27 PM
9 vs 10	**Database Files**	**Date Modified(9)**	**Date Modified(10)**	**Date Created(9)**	**Date Created(10)**
	web_sessions.db-shm	3/28/2022 4:30:47 PM	3/28/2022 5:21:37 PM	3/28/2022 4:34:31 PM	3/28/2022 5:29:18 PM
	msgstore.db-shm	3/28/2022 4:30:51 PM	3/28/2022 5:23:08 PM	3/28/2022 4:34:31 PM	3/28/2022 5:29:18 PM

	chatsettings.db-shm	3/28/2022 4:30:47 PM	3/28/2022 5:21:37 PM	3/28/2022 4:34:31 PM	3/28/2022 5:29:18 PM
	sync.db-shm	3/28/2022 4:30:49 PM	3/28/2022 5:21:39 PM	3/28/2022 4:34:31 PM	3/28/2022 5:29:18 PM
11 vs 12	**Database Files**	**Date Modified(11)**	**Date Modified(12)**	**Date Created(11)**	**Date Created(12)**
	web_sessions.db-shm	3/28/2022 5:32:24 PM	3/28/2022 5:42:19 PM	3/28/2022 5:39:16 PM	3/28/2022 5:46:35 PM
	msgstore.db	3/28/2022 3:50:57 PM	3/28/2022 5:41:44 PM	3/28/2022 5:39:16 PM	3/28/2022 5:46:35 PM
	chatsettings.db-shm	3/28/2022 5:32:24 PM	3/28/2022 5:40:32 PM	3/28/2022 5:39:16 PM	3/28/2022 5:46:35 PM
	_jobqueue-WhatsAppJobManager	3/28/2022 4:30:51 PM	3/28/2022 5:42:15 PM	3/28/2022 5:39:16 PM	3/28/2022 5:46:35 PM
13 vs 14	**Database Files**	**Date Modified(13)**	**Date Modified(14)**	**Date Created(13)**	**Date Created(14)**
	web_sessions.db-shm	3/28/2022 6:13:23 PM	3/28/2022 6:24:10 PM	3/28/2022 6:20:21 PM	3/28/2022 6:30:48 PM
	media.db-shm	1/1/2015 5:02:47 AM	3/28/2022 6:24:54 PM	3/28/2022 6:20:21 PM	3/28/2022 6:30:48 PM
	location.db-shm	3/28/2022 6:13:25 PM	3/28/2022 6:24:12 PM	3/28/2022 6:20:21 PM	3/28/2022 6:30:48 PM
	sync.db-shm	3/28/2022 6:13:25 PM	3/28/2022 6:24:12 PM	3/28/2022 6:20:21 PM	3/28/2022 6:30:48 PM
15 vs 16	**Database Files**	**Date Modified(15)**	**Date Modified(16)**	**Date Created(15)**	**Date Created(16)**
	wa.db	3/28/2022 9:28:48 PM	3/28/2022 1:14:29 PM	3/28/2022 9:33:40 PM	3/28/2022 9:07:20 PM
	location.db-shm	3/28/2022 9:28:45 PM	3/28/2022 8:26:31 PM	3/28/2022 9:33:40 PM	3/28/2022 9:07:20 PM
	msgstore.db	3/28/2022 9:28:48 PM	3/28/2022 8:20:29 PM	3/28/2022 9:33:40 PM	3/28/2022 9:07:20 PM
	sync.db-shm	3/28/2022 9:28:47 PM	3/28/2022 8:26:32 PM	3/28/2022 9:33:40 PM	3/28/2022 9:07:20 PM
17 vs 18	**Database Files**	**Date Modified(17)**	**Date Modified(18)**	**Date Created(17)**	**Date Created(18)**
	wa.db-shm	3/28/2022 9:38:53 PM	1/1/2015 3:01:16 AM	3/28/2022 9:45:47 PM	3/28/2022 10:00:34 PM
	msgstore.db-shm	3/28/2022 9:38:57 PM	1/1/2015 3:01:15 AM	3/28/2022 9:45:47 PM	3/28/2022 10:00:34 PM
	location.db-shm	3/28/2022 9:38:54 PM	1/1/2015 3:01:16 AM	3/28/2022 9:45:47 PM	3/28/2022 10:00:34 PM
	sync.db-shm	3/28/2022 9:38:54 PM	1/1/2015 3:01:16 AM	3/28/2022 9:45:47 PM	3/28/2022 10:00:34 PM
19 vs 20	**Database Files**	**Date Modified(19)**	**Date Modified(20)**	**Date Created(19)**	**Date Created(20)**
	wa.db-shm	3/29/2022 5:43:23 PM	3/29/2022 6:14:59 PM	3/29/2022 5:50:26 PM	3/29/2022 6:30:58 PM
	msgstore.db-shm	3/29/2022 5:43:24 PM	3/29/2022 6:14:58 PM	3/29/2022 5:50:26 PM	3/29/2022 6:30:58 PM
	location.db-shm	3/29/2022 5:43:23 PM	3/29/2022 6:14:58 PM	3/29/2022 5:50:26 PM	3/29/2022 6:30:58 PM
	sync.db-shm	3/29/2022 5:43:24 PM	3/29/2022 6:14:59 PM	3/29/2022 5:50:26 PM	3/29/2022 6:30:58 PM
21 vs 22	**Database Files**	**Date Modified(21)**	**Date Modified(22)**	**Date Created(21)**	**Date Created(22)**
	wa.db-shm	3/29/2022 6:40:14 PM	3/29/2022 6:48:42 PM	3/29/2022 6:50:24 PM	3/29/2022 7:05:49 PM
	msgstore.db-wal	3/29/2022 6:40:14 PM	3/29/2022 6:48:43 PM	3/29/2022 6:50:24 PM	3/29/2022 7:05:49 PM
	location.db-shm	3/29/2022 6:40:14 PM	3/29/2022 6:48:42 PM	3/29/2022 6:50:24 PM	3/29/2022 7:05:49 PM
	sync.db-shm	3/29/2022 6:40:15 PM	3/29/2022 6:48:43 PM	3/29/2022 6:50:24 PM	3/29/2022 7:05:49 PM
23 vs 24	**Database Files**	**Date Modified(23)**	**Date Modified(24)**	**Date Created(23)**	**Date Created(24)**
	web_sessions.db-shm	3/29/2022 5:43:50 PM	3/30/2022 12:15:35 AM	3/29/2022 7:30:17 PM	3/30/2022 12:31:51 AM
	msgstore.db-wal	3/29/2022 6:57:46 PM	3/29/2022 12:15:31 AM	3/29/2022 7:30:17 PM	3/30/2022 12:31:51 AM
	axolotl.db-wal	3/29/2022 5:43:24 PM	3/29/2022 12:15:32 AM	3/29/2022 7:30:17 PM	3/30/2022 12:31:51 AM
	sync.db-shm	3/29/2022 6:57:47 PM	3/29/2022 12:15:32 AM	3/29/2022 7:30:17 PM	3/30/2022 12:31:51 AM
25 vs 26	**Database Files**	**Date Modified(25)**	**Date Modified(26)**	**Date Created(25)**	**Date Created(26)**
	wa.db-shm	3/30/2022 12:34:29 AM	3/30/2022 12:52:18 AM	3/30/2022 12:40:29 AM	3/30/2022 1:00:00 AM
	msgstore.db-shm	3/30/2022 12:34:29 AM	3/30/2022 12:52:18 AM	3/30/2022 12:40:29 AM	3/30/2022 1:00:00 AM
	location.db-shm	3/30/2022 12:34:29 AM	3/30/2022 12:52:18 AM	3/30/2022 12:40:29 AM	3/30/2022 1:00:00 AM
	sync.db-shm	3/30/2022 12:34:30 AM	3/30/2022 12:52:19 AM	3/30/2022 12:40:29 AM	3/30/2022 1:00:00 AM
27 vs 28	**Database Files**	**Date Modified(27)**	**Date Modified(28)**	**Date Created(27)**	**Date Created(28)**
	wa.db	3/28/2022 9:28:48 PM	3/28/2022 9:28:48 PM	3/30/2022 1:30:02 AM	3/30/2022 1:40:06 AM
	msgstore.db	3/29/2022 5:43:24 PM	3/29/2022 5:43:24 PM	3/30/2022 1:30:02 AM	3/30/2022 1:40:06 AM
	axolotl.db	3/28/2022 9:28:48 PM	3/28/2022 9:28:48 PM	3/30/2022 1:30:02 AM	3/30/2022 1:40:06 AM
	sync.db-shm	3/17/2022 1:22:50 PM	3/17/2022 1:22:50 PM	3/30/2022 1:30:02 AM	3/30/2022 1:40:06 AM
29 vs 30	**Database Files**	**Date Modified(29)**	**Date Modified(30)**	**Date Created(29)**	**Date Created(30)**
	wa.db-shm	3/30/2022 1:05:08 AM	3/30/2022 1:36:56 AM	3/30/2022 1:50:09 AM	3/30/2022 2:00:41 AM
	msgstore.db-shm	3/30/2022 1:05:07 AM	3/30/2022 1:36:55 AM	3/30/2022 1:50:09 AM	3/30/2022 2:00:41 AM
	location.db-shm	3/30/2022 1:05:08 AM	3/30/2022 1:36:56 AM	3/30/2022 1:50:09 AM	3/30/2022 2:00:41 AM
	sync.db-shm	3/30/2022 1:05:08 AM	3/30/2022 1:36:56 AM	3/30/2022 1:50:09 AM	3/30/2022 2:00:41 AM

Table 10.0 Timeline of WhatsApp database files

5 Analysis

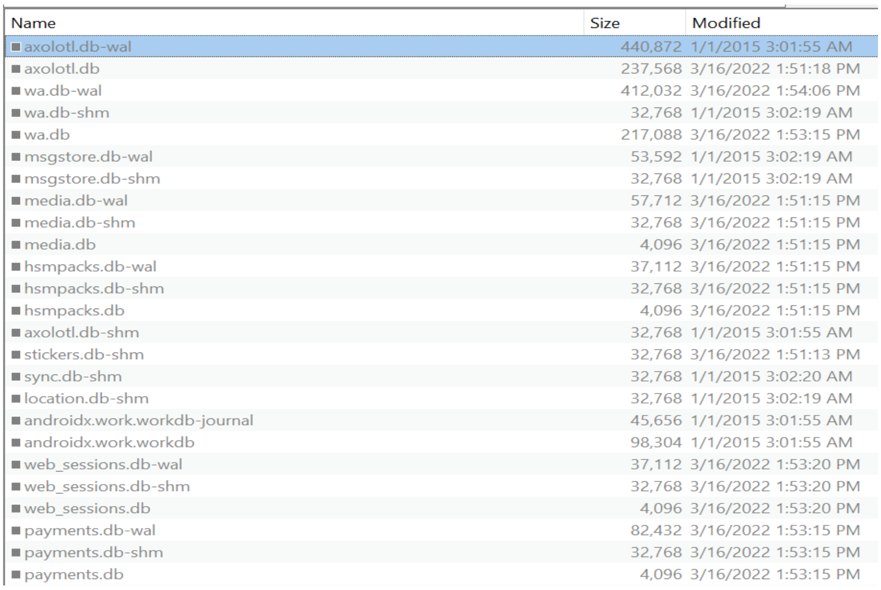
The version of WhatsApp used to conduct this study is 2.22.6.72. WhatsApp is a cross platform application and because of its immense use by a huge population in the world for end to end encrypted communication, so it could be a good option for criminals also to communicate with each other to plan or commit a crime such as robbery, contract killing, child pornography, money laundering, kidnapping, terrorism and drugs smuggling etc. To analyze and understand the WhatsApp application database files from each image taken from the phone after performing the sequence of steps to secure the device and preserve the digital evidence on it at a crime scene, I have examined the results obtained in each image iteration separately and compared them to inspect the actual impact specifically on WhatsApp database acquired files. There are situations when the first responder reaches to a crime scene and found the device in different conditions i.e. password protected, or no password at all, or the phone is ringing due to some call or alarm, the screen is on or may be off. In these different situations each one needs to be handled separately case by case but the ultimate goal of the first responder is to secure a device in such a manner that digital evidence on the device should not get completely vanished. Usually the first responder has these options to secure a device mentioned in Table 1.0. But before this a first responder can check that if the phone's display is on then he/she could quickly disable the passcode because some models of the phone does not ask to re-enter the passcode while disabling it and can enable the usb debug option from developer mode, this will give complete access to the device. In contrast, if the device is password protected then the case would be different such as some phones allow swipe down window to enable flight mode which is also one of the method to secure a device and preserve digital evidence because there is a chance that phone might be connected to internet and a criminal can execute a remote wipe to completely erase the data from the phone. If the battery of the phone is removable then a first responder can also unplug the battery to preserve the digital evidence on the phone in case battery is about to die or attach it to external power source carefully, till the phone reaches to laboratory.

Similarly, there could be a possibility to corrupt the digital evidence on the phone via calls or messages on the phone, so that first responder can also safeguard the device by removing sim or putting the device in a Faraday bag. In this study I have used standard options/methods to secure a digital device to preserve the digital evidence mentioned in Tables (3.0,4.0 and 7.0) to

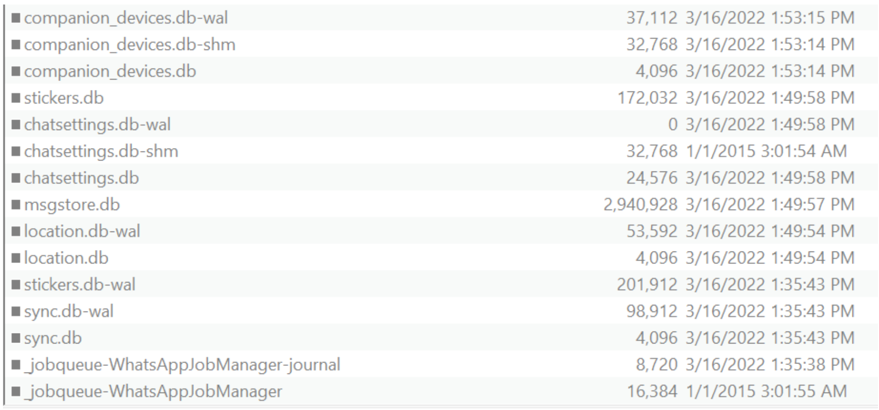
demonstrate the changes/impact on digital evidence on the device followed by actions performed by first responder. As it can be seen in the figure 15.0 and figure 16.0 below. The differences between normal mode image acquisition of the phone and flight mode image acquisition can be seen easily.

The risk of losing a digital evidence from the device is certain at some level. When the adb tool is used to image the phone because adb tool does not provide full backup from the phone and sometimes skips the backups of some apps completely or backup them partially which could result in losing the files that contain highly sensitive information about the user such as phone number, chat messages, call logs, pictures and most importantly the deleted data from the device [48].

To validate this, I have analyzed the behavior of adb tool with several images taken from the phone and observed their differences in terms of files acquired from each along with their timestamps. In figure 15.0 it can be seen that total files acquired from WhatsApp database image acquisition are 40 when the phone in normal mode. While in figure 16.0 it is shown that total files acquired from WhatsApp database image acquisition are 34, when the phone is in flight mode. Since, the missing files from adb backup are shown in figure 17.0.

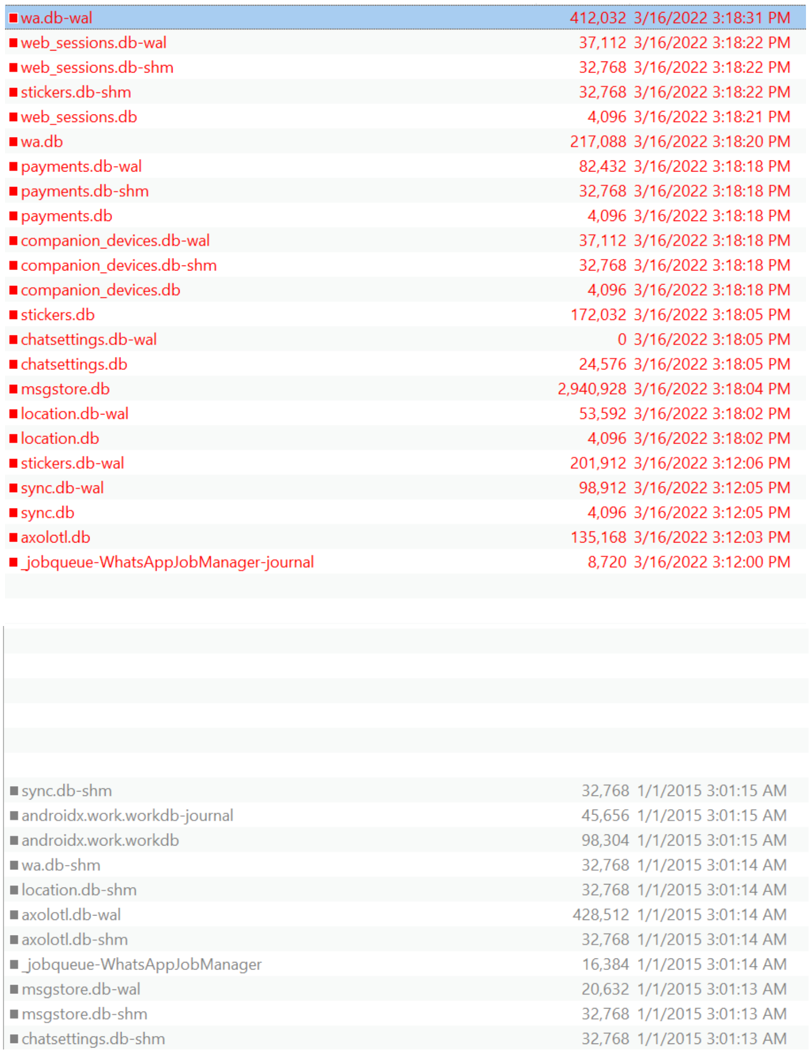


Name	Size	Modified
axolotl.db-wal	440,872	1/1/2015 3:01:55 AM
axolotl.db	237,568	3/16/2022 1:51:18 PM
wa.db-wal	412,032	3/16/2022 1:54:06 PM
wa.db-shm	32,768	1/1/2015 3:02:19 AM
wa.db	217,088	3/16/2022 1:53:15 PM
msgstore.db-wal	53,592	1/1/2015 3:02:19 AM
msgstore.db-shm	32,768	1/1/2015 3:02:19 AM
media.db-wal	57,712	3/16/2022 1:51:15 PM
media.db-shm	32,768	3/16/2022 1:51:15 PM
media.db	4,096	3/16/2022 1:51:15 PM
hsmpacks.db-wal	37,112	3/16/2022 1:51:15 PM
hsmpacks.db-shm	32,768	3/16/2022 1:51:15 PM
hsmpacks.db	4,096	3/16/2022 1:51:15 PM
axolotl.db-shm	32,768	1/1/2015 3:01:55 AM
stickers.db-shm	32,768	3/16/2022 1:51:13 PM
sync.db-shm	32,768	1/1/2015 3:02:20 AM
location.db-shm	32,768	1/1/2015 3:02:19 AM
androidx.work.workdb-journal	45,656	1/1/2015 3:01:55 AM
androidx.work.workdb	98,304	1/1/2015 3:01:55 AM
web_sessions.db-wal	37,112	3/16/2022 1:53:20 PM
web_sessions.db-shm	32,768	3/16/2022 1:53:20 PM
web_sessions.db	4,096	3/16/2022 1:53:20 PM
payments.db-wal	82,432	3/16/2022 1:53:15 PM
payments.db-shm	32,768	3/16/2022 1:53:15 PM
payments.db	4,096	3/16/2022 1:53:15 PM



■ companion_devices.db-wal	37,112	3/16/2022 1:53:15 PM
■ companion_devices.db-shm	32,768	3/16/2022 1:53:14 PM
■ companion_devices.db	4,096	3/16/2022 1:53:14 PM
■ stickers.db	172,032	3/16/2022 1:49:58 PM
■ chatsettings.db-wal	0	3/16/2022 1:49:58 PM
■ chatsettings.db-shm	32,768	1/1/2015 3:01:54 AM
■ chatsettings.db	24,576	3/16/2022 1:49:58 PM
■ msgstore.db	2,940,928	3/16/2022 1:49:57 PM
■ location.db-wal	53,592	3/16/2022 1:49:54 PM
■ location.db	4,096	3/16/2022 1:49:54 PM
■ stickers.db-wal	201,912	3/16/2022 1:35:43 PM
■ sync.db-wal	98,912	3/16/2022 1:35:43 PM
■ sync.db	4,096	3/16/2022 1:35:43 PM
■ _jobqueue-WhatsAppJobManager-journal	8,720	3/16/2022 1:35:38 PM
■ _jobqueue-WhatsAppJobManager	16,384	1/1/2015 3:01:55 AM

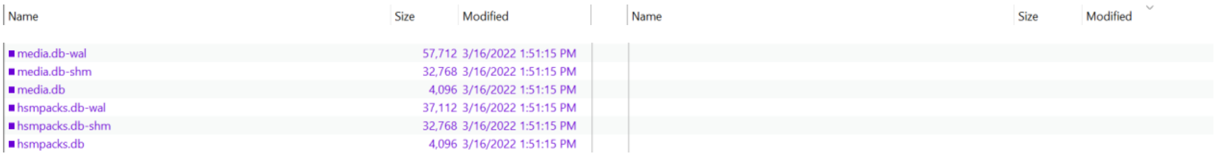
Figure 15.0 WhatsApp database files acquired



■ wa.db-wal	412,032	3/16/2022 3:18:31 PM
■ web_sessions.db-wal	37,112	3/16/2022 3:18:22 PM
■ web_sessions.db-shm	32,768	3/16/2022 3:18:22 PM
■ stickers.db-shm	32,768	3/16/2022 3:18:22 PM
■ web_sessions.db	4,096	3/16/2022 3:18:21 PM
■ wa.db	217,088	3/16/2022 3:18:20 PM
■ payments.db-wal	82,432	3/16/2022 3:18:18 PM
■ payments.db-shm	32,768	3/16/2022 3:18:18 PM
■ payments.db	4,096	3/16/2022 3:18:18 PM
■ companion_devices.db-wal	37,112	3/16/2022 3:18:18 PM
■ companion_devices.db-shm	32,768	3/16/2022 3:18:18 PM
■ companion_devices.db	4,096	3/16/2022 3:18:18 PM
■ stickers.db	172,032	3/16/2022 3:18:05 PM
■ chatsettings.db-wal	0	3/16/2022 3:18:05 PM
■ chatsettings.db	24,576	3/16/2022 3:18:05 PM
■ msgstore.db	2,940,928	3/16/2022 3:18:04 PM
■ location.db-wal	53,592	3/16/2022 3:18:02 PM
■ location.db	4,096	3/16/2022 3:18:02 PM
■ stickers.db-wal	201,912	3/16/2022 3:12:06 PM
■ sync.db-wal	98,912	3/16/2022 3:12:05 PM
■ sync.db	4,096	3/16/2022 3:12:05 PM
■ axolotl.db	135,168	3/16/2022 3:12:03 PM
■ _jobqueue-WhatsAppJobManager-journal	8,720	3/16/2022 3:12:00 PM

■ sync.db-shm	32,768	1/1/2015 3:01:15 AM
■ androidx.work.workdb-journal	45,656	1/1/2015 3:01:15 AM
■ androidx.work.workdb	98,304	1/1/2015 3:01:15 AM
■ wa.db-shm	32,768	1/1/2015 3:01:14 AM
■ location.db-shm	32,768	1/1/2015 3:01:14 AM
■ axolotl.db-wal	428,512	1/1/2015 3:01:14 AM
■ axolotl.db-shm	32,768	1/1/2015 3:01:14 AM
■ _jobqueue-WhatsAppJobManager	16,384	1/1/2015 3:01:14 AM
■ msgstore.db-wal	20,632	1/1/2015 3:01:13 AM
■ msgstore.db-shm	32,768	1/1/2015 3:01:13 AM
■ chatsettings.db-shm	32,768	1/1/2015 3:01:13 AM

Figure 16.0 WhatsApp database files & missing files

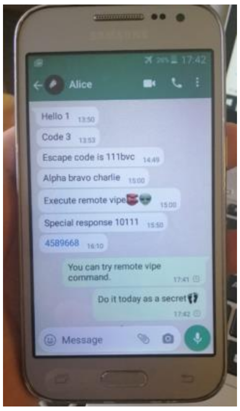


Name	Size	Modified	Name	Size	Modified
media.db-wal	57,712	3/16/2022 1:51:15 PM			
media.db-shm	32,768	3/16/2022 1:51:15 PM			
media.db	4,096	3/16/2022 1:51:15 PM			
hsmpacks.db-wal	37,112	3/16/2022 1:51:15 PM			
hsmpacks.db-shm	32,768	3/16/2022 1:51:15 PM			
hsmpacks.db	4,096	3/16/2022 1:51:15 PM			

Figure 17.0 WhatsApp database missing files

The only solution to work with adb tool is to use the minimum number of apps on the phone or otherwise repeat the image acquisition process until all the files are acquired from the phone or at least the application which is under investigation and compare each image with the previous one in terms of obtained files. The files size change over each iteration of image acquisition process is mainly occurred due to the files with (.) db-wal extensions inside the WhatsApp database folder which are write ahead log files that are used to record the transactions that have been committed but not yet applied to the main database of the WhatsApp such as msgstore.db [49]. These (.) db-wal files will variate in each image iteration and these files will have a direct impact of the actions performed by first responder on the phone to secure it i.e. power off the phone, putting flight mode, remove sim etc.

As the phone used in this research is rooted so we can see a situation where the deleted messages can be seen in figures (18.0-19.0). The rooting is preferred before image the phone because there are high chances from the criminal’s side that the messages have been deleted after crime. So with rooted phone the deleted messages from the phone can be easily recovered. But it is very risky process sometimes and depends on the phone make and model and a wrong rooting process could permanently brick the phone.



Hello 1 13:50

Code 3 13:53

Escape code is 111bvc 14:49

Alpha bravo charlie 15:00

Execute remote vipe👄👽 15:00

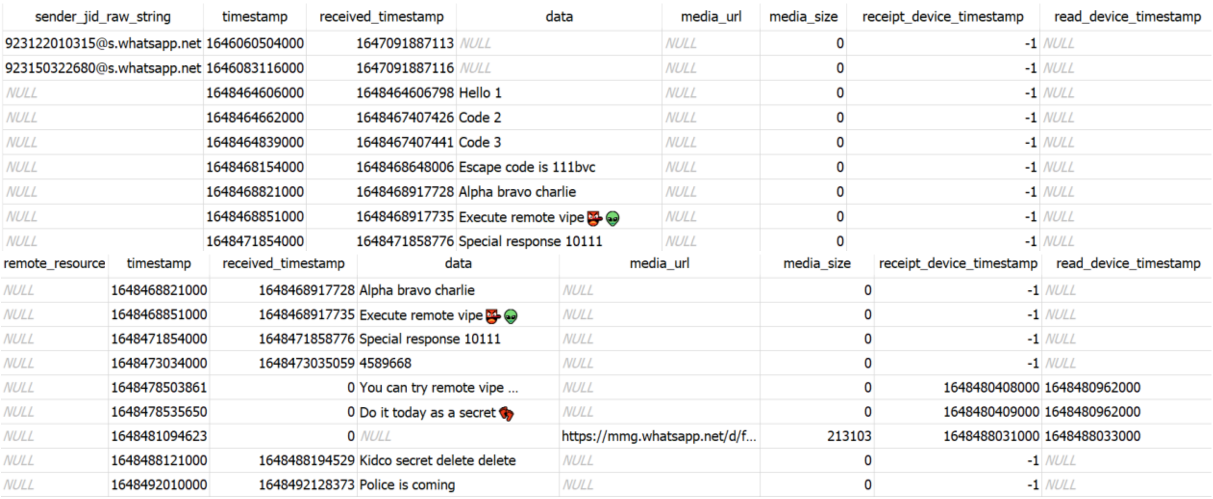
Special response 10111 15:50

4589668 16:10

You can try remote vipe command. 17:41

Do it today as a secret👣 17:42

Figure 18.0 Messages sent and received from the phone

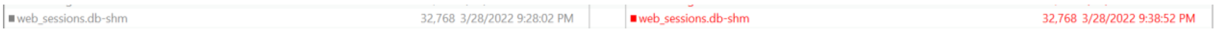


sender_jid_raw_string	timestamp	received_timestamp	data	media_url	media_size	receipt_device_timestamp	read_device_timestamp
923122010315@s.whatsapp.net	1646060504000	1647091887113	NULL	NULL	0	-1	NULL
923150322680@s.whatsapp.net	1646083116000	1647091887116	NULL	NULL	0	-1	NULL
NULL	1648464606000	1648464606798	Hello 1	NULL	0	-1	NULL
NULL	1648464662000	1648467407426	Code 2	NULL	0	-1	NULL
NULL	1648464839000	1648467407441	Code 3	NULL	0	-1	NULL
NULL	1648468154000	1648468648006	Escape code is 111bvc	NULL	0	-1	NULL
NULL	1648468821000	1648468917728	Alpha bravo charlie	NULL	0	-1	NULL
NULL	1648468851000	1648468917735	Execute remote vipe 👺👽	NULL	0	-1	NULL
NULL	1648471854000	1648471858776	Special response 10111	NULL	0	-1	NULL

remote_resource	timestamp	received_timestamp	data	media_url	media_size	receipt_device_timestamp	read_device_timestamp
NULL	1648468821000	1648468917728	Alpha bravo charlie	NULL	0	-1	NULL
NULL	1648468851000	1648468917735	Execute remote vipe 👺👽	NULL	0	-1	NULL
NULL	1648471854000	1648471858776	Special response 10111	NULL	0	-1	NULL
NULL	1648473034000	1648473035059	4589668	NULL	0	-1	NULL
NULL	1648478503861	0	You can try remote vipe ...	NULL	0	1648480408000	1648480962000
NULL	1648478535650	0	Do it today as a secret 👣	NULL	0	1648480409000	1648480962000
NULL	1648481094623	0	NULL	https://mmg.whatsapp.net/d/f...	213103	1648488031000	1648488033000
NULL	1648488121000	1648488194529	Kidco secret delete delete	NULL	0	-1	NULL
NULL	1648492010000	1648492128373	Police is coming	NULL	0	-1	NULL

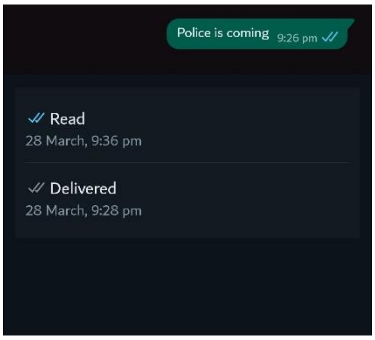
Figure 19.0 Deleted message

The actions of the forensics officer can be distinguished from the database files timestamps of the acquired image from the phone. If we compare the image 15 and 17 from the Table 7.0 where a first responder tries to open the WhatsApp and writes a message but did not send it. It will change the timestamps of web_sessions.db-shm file and mark the message as read in msgstore.db file. The web_sessions.db-shm file shows the last time application opened and used on the phone and from there we can clearly distinguish the actions of first responder on the phone.



web_sessions.db-shm	32,768	3/28/2022 9:28:02 PM
web_sessions.db-shm	32,768	3/28/2022 9:38:52 PM

Figure 20.0 web_sessions.db file



Police is coming 9:26 pm

Read
28 March, 9:36 pm

Delivered
28 March, 9:28 pm

Figure 21.0 Message Timestamps

6 Conclusion

In terms of database file sizes, a risk based decision can be made based on the sequences of images from Table 5.0 and Table 9.0, while the decision making on the time based analysis is complex at some level that needs to be made from the timelines mentioned in Table 6.0 and Table 10.0. Where the challenging part could be the one where the files are not properly backed up from the tool. As the adb tool is not very much efficient in terms of results but it could be utilized in cases where the affordability of licensed commercial tools is restricted to law enforcement and academia. This study gives good results about the digital forensics investigation process of a mobile phone of a specific model of Samsung phone with android version 5.0.2(lollipop). With this research study we can conduct android phone forensics free of cost and we can control the phone via command line terminal and perform actions over the phone without physically interacting with it.

The forensics community can take the benefits of learning from the obtained results in this study about the WhatsApp forensics process on specific phone with specific android version. As mobile forensics is a growing field with the increased number of devices and it requires great expertise from the digital forensics investigation officer to collect, analyze and report the evidence in a timely manner, and every forensics case is different based on the device make and model. The results of this study can also be compared with the results obtained from a commercial tool i.e. Oxygen Forensics, Magnet Axiom, Cellebrite Forensics etc. to find the efficiency tools. Apart from the techniques used in this thesis document there are also available loads of different techniques and procedures for accessing data from mobile phones with a forensics purpose i.e. creating adversarial model for digital forensics, JTAG, sim card forensics, memory forensics etc.

Sometimes the forensics investigation process can sometimes become biased by human error and due to the vulnerable nature of process the decision making could be wrong [45]. To encounter such biasedness NIST manual can also be used as a reference to understand the mobile forensics process in a standard professional way [46].

In real criminal cases the legal aspects of crime are always considered and this study does not cover the legal aspects as they change from country to country. This study can be used as a reference for beginners in the field of digital forensics to understand the mobile forensics of android based phones in a practical way to guide them and demonstrate the changes and impact of certain actions on the device such as timestamps and size of the files which could also be the main players to trace a crime from a digital device. When the first responder tries to secure a phone there are various risks associated with the device and some of them we have observed in this study such as changes in timestamps and files size. The sequence of actions performed by first responder on the device to secure it and preserve the digital evidence, should be in a manner to cover the maximum data from the device which could ease the process of digital forensics and we can see these sequences in the Table 4.0 and Table 8.0. These two tables also show the sequences which have same impact on the amount of data recovered from the phone, but it is possible that timestamps might differ, so we should address both parameters while dealing with digital forensics problem.

References

[1]Brahler, S., 2010. Analysis of the android architecture. *Karlsruhe institute for technology*, *7*(8).

[2] Anglano, C., 2014. Forensic analysis of WhatsApp Messenger on Android smartphones. *Digital Investigation*, *11*(3), pp.201-213.

[3] Jeyamohan, N., 2017, September. Android Digital Forensics–Simplifying Android Forensics Using Regular Expressions. In *2017 Seventeenth International Conference on Advances in ICT for Emerging Regions (ICTer)* (pp. 1-1). IEEE.

[4] Marturana, F., Me, G., Berte, R. and Tacconi, S., 2011, November. A quantitative approach to triaging in mobile forensics. In *2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications* (pp. 582-588). IEEE.

[5] Dogan, S. and Akbal, E., 2017, May. Analysis of mobile phones in digital forensics. In *2017 40th international convention on information and communication technology, electronics and microelectronics (MIPRO)* (pp. 1241-1244). IEEE.

[6] Sathe, S.C. and Dongre, N.M., 2018, January. Data acquisition techniques in mobile forensics. In *2018 2nd International Conference on Inventive Systems and Control (ICISC)* (pp. 280-286). IEEE.

[7] Ahmed, R., Dharaskar, R. and Thakare, V., 2013. Digital evidence extraction and documentation from mobile devices. Int. J. Adv. Res. Comput. Commun. Eng, 2(1), pp.1019-1024.

[8] Pollitt M 1995 Computer Forensics: an Approach to Evidence in Cyberspace Proceeding Natl. Inf. Syst. Secur. Conf. 487–491.

[9] Palmer G 2001 A Road Map for Digital Forensic Research Digital Forensic Research Conference DFRWS USA.

[10] Reith M, Carr C and Gunsch G 2002 An Examination of Digital Forensic Models Int. J. Digit. Evid. 13.

[11] Carrier B and Spafford E H 2003 Getting Physical with the Digital Investigation Process Int. J. Digit. Evid. Fall 2 2.

[12] Baryamureeba V and Tushabe F 2004 The enhanced digital investigation process model Proceedings of the Digital Forensic Research Conference, DFRWS USA 1–9.

[13] Beebe N L and Clark J G 2005 A hierarchical, objectives-based framework for the digital investigations process Digit. Investig. 2 2 147–167.

[14] Rogers M, Goldman J, Mislan R, Wedge T and Debrota S 2006 Computer Forensics Field Triage Process Model J. Digit. Forensics, Secur. Law 1 2 19–38.

[15] Freiling F and Schwittay B 2007 A Common Process Model for Incident Response and Computer Forensics IT-Incidents Management & IT-Forensics – IMF 114 19–40.

[16] Selamat S R, Yusof R and Sahib S 2008 Mapping process of digital forensic investigation framework Int. J. Comput. Sci. Netw. Secur. 8 10 163–169.

[17] Trček D, Abie H, Skomedal Å and Starc I 2010 Advanced framework for digital forensic technologies and procedures J. Forensic Sci. 55 6 1471–80.

[18] Agarwal A, Gupta M, Gupta S and Gupta S C 2011 Systematic Digital Forensic Investigation Model Int. J. Comput. Sci. Secur. 5 1 118–131.

[19] Kohn M D 2012 Integrated Digital Forensic Process Model University of Pretoria.

[20] Kalbande D D and Jain N 2013 Comparative Digital Forensic Model Int. J. Innov. Res. Sci. Eng. Technol. 2 8 3414–19.

[21] Quick D and Choo K K R 2014 Data reduction and data mining framework for digital forensic evidence: Storage, intelligence, review and archive Australia's national research and knowledge centre on crime and justice 480.

[22] Jain N and Kalbande D R 2015 Digital forensic framework using feedback and case history keeper Proceedings Int. Conf. on Communication, Information and Computing Technology, ICCICT.

[23] Montasari R 2016 A Formal Two Stage Triage Process Model (FTSTPM) for Digital Forensic Practice Int. J. Comput. Sci. Secur. 10 2 69–87.

[24] Verma R, Govindaraj J and Gupta G 2018 DF 2.0: Designing an automated, privacy preserving, and effifficient digital forensic framework Annual ADFSL Conference on Digital Forensics, Security and Law 127–150.

[25] Shayau Y H, Asmawi A, Rum S N M and Ariffin N A M 2019 Digital Forensics Investigation Reduction Model (DIFReM) Framework for Windows 10 OS IEEE 9th Int. Conf. Syst. Eng. Technol. 459–464.

[26] Song J and Li J 2020 A Framework for Digital Forensic Investigation of Big Data 3rd International Conference on Artificial Intelligence and Big Data, ICAIBD 96–100.

[27] Mellars, B., 2004. Forensic examination of mobile phones. *Digital Investigation*, *1*(4), pp.266-272.

[28] Willassen, S., 2005, February. Forensic analysis of mobile phone internal memory. In *IFIP International Conference on Digital Forensics* (pp. 191-204). Springer, Boston, MA.

[29] Casadei, F., Savoldi, A. and Gubian, P., 2006. Forensics and SIM cards: an Overview. *International Journal of Digital Evidence*, *5*(1), pp.1-21.

[30] Mokhonoana, P.M. and Olivier, M.S., 2007, September. Acquisition of a Symbian smart phone’s content with an on-phone forensic tool. In *Proceedings of the Southern African Telecommunication Networks and Applications Conference* (Vol. 8).

[31] Jansen, W., Delaitre, A. and Moenner, L., 2008, January. Overcoming impediments to cell phone forensics. In *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)* (pp. 483-483). IEEE.

[32] Danker, S., Ayers, R. and Mislan, R.P., 2009. Hashing techniques for mobile device forensics. *Stress*, *6*(4f16334e774b5c), p.77bebd7fb998797dd.

[33] Lessard, J. and Kessler, G., 2010. Android Forensics: Simplifying Cell Phone Examinations.

[34] D. Quick and M. Alzaabi, ‘‘Forensic analysis of the Android file system YAFFS2,’’ Cowan Univ., Joondalup, WA, Australia, Tech. Rep., 2011, pp. 100–109.

[35] Al Mutawa, N., Baggili, I. and Marrington, A., 2012. Forensic analysis of social networking applications on mobile devices. *Digital investigation*, *9*, pp.S24-S33.

[36] Son, N., Lee, Y., Kim, D., James, J.I., Lee, S. and Lee, K., 2013. A study of user data integrity during acquisition of Android devices. *Digital Investigation*, *10*, pp.S3-S11.

[37] Kaart, M. and Laraghy, S., 2014. Android forensics: Interpretation of timestamps. *Digital Investigation*, *11*(3), pp.234-248.

[38] Do, Q., Martini, B. and Choo, K.K.R., 2015. A forensically sound adversary model for mobile devices. *PloS one*, *10*(9), p.e0138449.

[39] Sadiq, M., Iqbal, M.S., Sajad, M., Naveed, K. and Malip, A., 2016. Mobile devices forensics investigation: process models and comparison. *Theoretical & Applied Science*, (1), pp.164-168.

[40] Htun, N.L. and Thwin, M.M.S., 2017. Proposed Workable Process Flow with Analysis Framework for Android Forensics in Cyber-Crime Investigation. *The International Journal Of Engineering And Science (IJES)*, *6*(1), pp.82-92.

[41] Wilson, R. and Chi, H., 2018, March. A framework for validating aimed mobile digital forensics evidences. In *Proceedings of the ACMSE 2018 Conference* (pp. 1-8).

[42] F. G. Hikmatyar and B. Sugiantoro, ‘‘Digital forensic analysis on Android smartphones for handling cybercrime cases,’’ Int. J. Inform. Develop., vol. 7, no. 2, pp. 19–22, 2019.

[43] Thebaity, M.A., Mishra, S. and Shukla, M.K., 2020. Forensic Analysis of Third-party Mobile Application. *Helix*, *10*(04), pp.32-38.

[44] Kaart, M. and Laraghy, S., 2014. Android forensics: Interpretation of timestamps. *Digital Investigation*, *11*(3), pp.234-248.

[45] Sunde, N. and Dror, I.E., 2019. Cognitive and human factors in digital forensics: Problems, challenges, and the way forward. *Digital investigation*, *29*, pp.101-108.

[46] Jansen, R.A.S.B.W., Ayers, R. and Brothers, S., 2014. Guidelines on mobile device forensics. *NIST Special Publication*, pp.800-101.

[47] “Platform Architecture,” [online]. Available: https://source.android.com/images/android_framework.

[48] “What can and can't be done with adb backup/restore,” [online]. Available: http://dalvikplanet.blogspot.com/2019/05/why-deprecating-adb-backup-and-restore.html.

[49] “WAL-mode file format,” [Online]. Available: https://www.sqlite.org /walformat.html.

[50] “Power off and shutdown,” [Online]. Available: https://www.neway.mobi/news/what-%E2%80%93is-the-difference-between-a-phone-restart-and-a-shutdown.html.