



IJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 Issue: IV Month of publication: April 2020

DOI: <http://doi.org/10.22214/ijraset.2020.4291>

www.ijraset.com

Call:  08813907089

E-mail ID: ijraset@gmail.com

A Forensic approach to Perform Android Mobile Forensic Analysis and Locating Artifacts from Digital Evidence

Laishram Hemanta Singh¹, Dr. Priyanka Sharma², Dr. Tilaka Das³

¹Student Master in Technology Cyber Security, ²Professor Raksha Shakti University, ³Joint Director DFS

¹School of Information Technology & Cyber Security

¹Raksha Shakti University, Gujarat, India

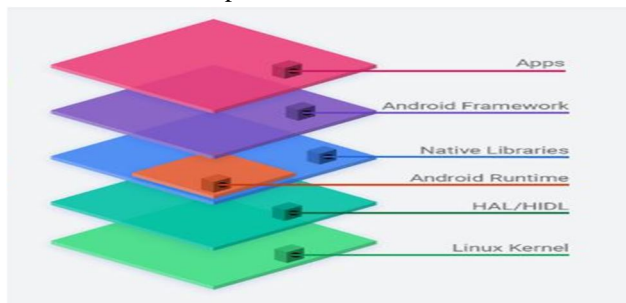
³Directorate of Forensic Science, Guwahati, India.

Abstract: *With the evolving changes in Cyber World, mobile phone platform has risen and become an indispensable tool for crime-fighting and criminal investigation. The no of mobile phone users worldwide today increases three million and is forecast to further, and the majority of people depend on it for communication and business-related matters. While mobile phones are used for the positive developments of our life, it is used by criminals as a communication medium for their modus operandi. We need to understand how to leverage the data from the device in an appropriate method that can make or break your case and your future as an investigator. Therefore, there is prospective information stored in mobile phones that can be used for digital evidence as part of an investigation. However, the investigators may be facing difficulties in extracting crucial data, artifacts, and vital information is stored on the mobile phone. The segregate of mobile forensics knowledge does not only make an investigation problem for new forensic investigators, resulting in a substantial waste of time but also leads to ambiguity in the conceptualization and terminologies of the mobile forensics domain. This work aims to locate the methods of extracting and analyzing data, artifacts from an Android-based mobile phone. We managed to obtain email, contact, messages, calendar, audio, videos, social media (i.e WhatsApp), cache memory, and images data that can be used as digital evidence in an investigation.*

Keywords: *Mobile Device, Extraction, Acquisitions, Mobile Forensics, WhatsApp Forensic, Magnet Acquire, FTK, Autopsy, SQLite*

I. INTRODUCTION

Android platform is an open-source operating system for mobile phone devices and related open source project led by Google only. Android Open Source Project repository offers the vital information and source code needed to create custom variants of the Android Operating System, port devices and accessories to the Android platform, and maintain the ecosystem a healthy environment for millions of Smartphone users. As a project, this platform's goal is to avoid any central point of catastrophe in which an industry competitor can restrict or control the innovations of any other competitors. Android is a fully production-quality operating system for consumer products, complete with customizable code that can be ported to nearly any device and public documentation that is available to everyone. Every time a new phone is released, we have new features, security updates and new ways of doing things. Those new products don't mean more secure ways it just means quicker, more efficient and not necessarily with our best interest at heart. For instance, we have been using facial recognition to unlock our phones, a great idea if executed right. This is an option available to many popular mobile phones but for anyone interested in their privacy, this isn't particularly a good thing. With that, mobiles hold a lot of information about us, on us and for us. We rely heavily on our mobile phones and at this moment in time, it must be hard to find someone who doesn't own a mobile phone.



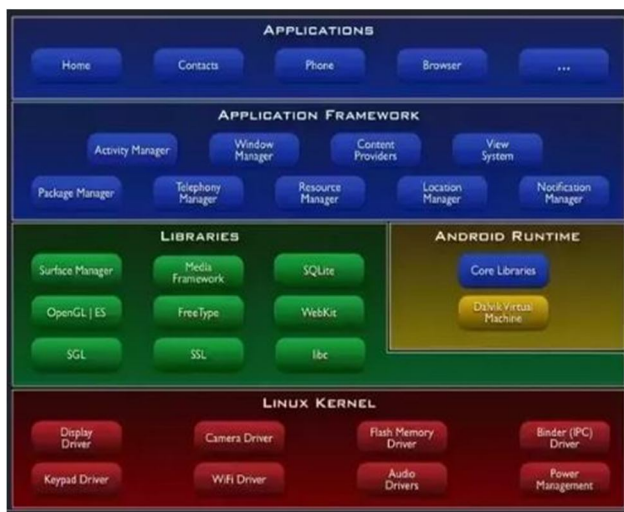


Fig-1: Android Platform Architecture includes Applications, Application Framework, Libraries, Runtime, and Linux Kernel

Without accessing any social media accounts on mobile phones, an investigator can capture a lot of crucial information on a case. The phone holds sensitive information everyone needs to be reminded of and can be aware of, in case of mobile theft. The list of information that can be grabbed off a mobile phone is large but we will be focusing on one of the first places someone will look once they have your phone. We will look at what information can be extracted from a mobile phone from its most basic features and how we can protect ourselves from revealing too much information. If your phone were in the hands of a thief right now, what would he or she find out about you?



Fig-1a: Software Stack for Android Platform

From fig-1 and fig-1a, it shows the layered Architecture with software stack for Android Platform and from fig-2, you can track our lost mobile and you find out the IMEI number, we can permanently erase the device files, images, videos and sensitive data from lost mobile if you know your mobile's login details.

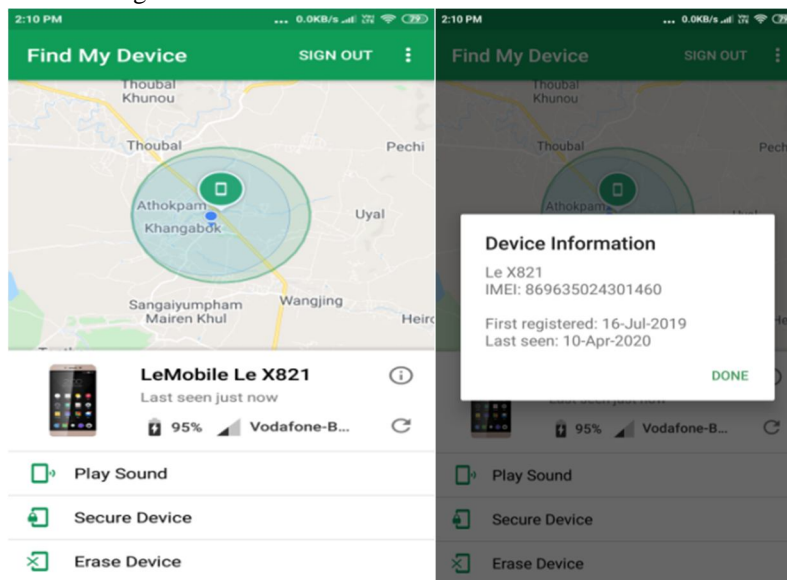


Fig-2: Mobile Location Detection using Find My Device

II. BACKGROUND

Digital forensic is an ancillary of forensic discipline which consists of the identification, retrieval, examination, verification, and submission of data or information as "CHAIN OF CUSTODY" about the digital vital data erect from a computer or related digital repository disclosure gadgets. This forensic concept is generally being used to aid to examine the electronic corruption or integrity explicit clue of a computer-based fraud, criminals. It is also generally being used in twain illegitimately act and non-governmental inspection. The objective of this research is to protect the hint in its maximum authentic pattern when operating an analytical analysis by gathering, determining and justifying making the binary bit-by-bit data for the intention of recreating the former affair. Among the different branches, Mobile Phone forensics is the freshest upcoming division of digital forensics describing to retrieve the digital proof from a seized mobile phone device. The investigation is typically performed either on a digital resource such as a computer, or server that was used to commit the crime or was a target of crime. Digital forensics is accomplished carried out only to recover, restore, validating the digital evidence. It can be recovered from the hard drive, mobile phone device, flash drives, routers, tablets, e-mails, laptops. Android Mobile device forensics is the branch of retrieving the binary clue from a seized mobile phone under a forensically stable situation using authorized processes.

As a part of mobile forensic investigation, we choose Social Media app i.e, WhatsApp is the most popular instant messaging (IM) application worldwide, with over 1.6 billion monthly active users as of July 2019 in over 180 countries (Statista, 2019). WhatsApp allows individuals to communicate with others in real-time through either text, audio, or video calls. WhatsApp also allows individuals to send voice notes, photos, videos, location information, and documents of any type up to 100 MB in size, all through end-to-end encryption (WhatsApp). WhatsApp was first released in 2009 to be an alternative for the traditional short message service (SMS; WhatsApp, 2016). As of 2019, WhatsApp stopped charging one-time and subscription fees, effectively making the application free for users around the world (WhatsApp, 2019). Over time, the capabilities of WhatsApp have increased and thus the relevance to police investigations. In January 2015, the WhatsApp web client was introduced for all major desktop browsers, and the WhatsApp desktop application for Windows was introduced in May 2016 (WhatsApp, 2015; 2016). To use the WhatsApp web client, a user can simply navigate to <https://web.whatsapp.com> on any of the supported browsers on a desktop. Next, the user would scan a quick response (QR) code within the WhatsApp application on a mobile phone to start sending and receiving messages. Supported web browsers include Google Chrome, Mozilla Firefox, Opera, Microsoft Edge. For the desktop application, a user will download the client from <https://www.whatsapp.com/download>, install the application and scan a QR code similar to the web browser client, as seen in Fig-3. Both options are only an extension of a Smartphone and only mirror what is being sent and received on the device. This means if the device is disconnected from a network then no messages can be sent or received on the desktop clients for any platform.



Fig-3: Setup screen for the WhatsApp desktop and web browser client.

The current study had the main goal of locating forensic artifacts left behind the WhatsApp desktop application and web client for Windows operating systems (OS) as well as locating deleting messages from WhatsApp databases. It combined different areas of digital forensics, such as browser forensics, mobile forensics, and instant messaging forensics, to locate artifacts of interest on OS.

A. Introduction To Android And Its Peripheral

Android is a Linux oriented operating system and is produced by Google. Android is the world’s maximum used mobile phone device operating system. Nowadays Android operating system has greater than 88 percent contribution to the world's mobile phone merchandise. Android is the most robust operating system and it provides a broad amount of applications in the mobile phone device. These apps have a higher satisfactory and modernized facility for the users.

The following chart shows the number of smartphones sold to end-users worldwide till 2020.

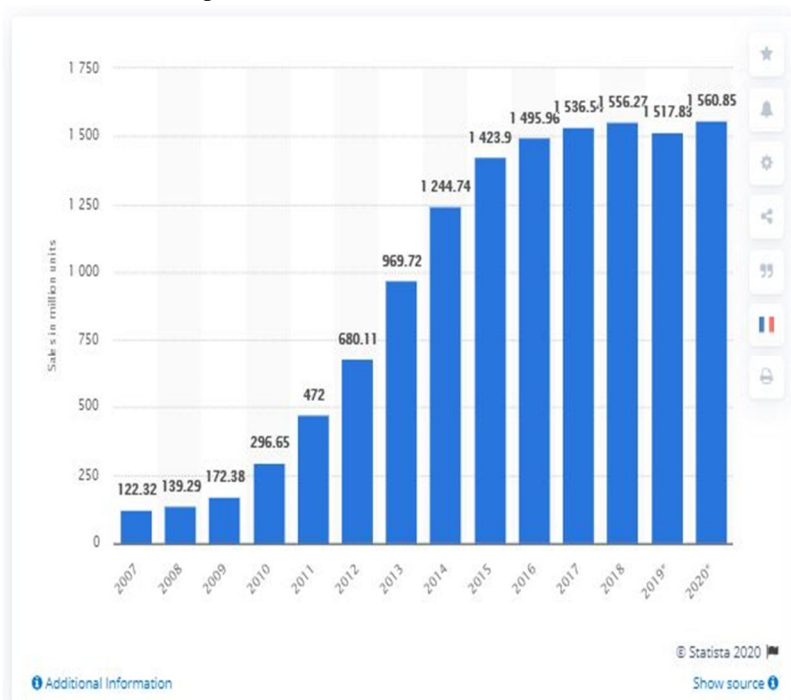


Fig-3a: Number of smartphones sold to end users worldwide from 2007 to 2020 (in million units)

B. Android Version

Table 2.1: Android Versions with Features

VERSION	INTRODUCED YEAR	FEATURES
Android 1.1	FEBRUARY 2009	Application programming Interface change, MMS attachments facility
Android 1.5 Cupcake	APRIL 2009	Bluetooth, YouTube video uploader, image uploader in Picasa
Android 1.6 Donut	SEPTEMBER 2009	Wide Video Graphics Array display supporter
Android 2.0/1 Éclair	OCTOBER 2009	HTML5 supporter
Android 2.2 Froyo	May 2010	USB Connectivity and Wi-Fi Hotspot facility
Android 2.3 Ginger bird	DECEMBER 2010	Large screen diameter supporter
Android 3.0 Honeycomb	MAY 2011	Video chat and GTalkfacility
Android 4.0/4.0.1/4.0.2/4.0.3/4.0.4 Icecream Sandwich	OCTOBER 2011	Email App facility, spelling checking facility, Face unlocking, Easy screen rotation
Android 4.1/4.1.1/4.1.2/4.2/4.2.1/4.2.2/4.3Jelly Bean	JULY 2012	Audio search, Camera Application improvement, Wireless charging facility, Security
Android 4.4/4.4.1/4.4.2/4.4.3/4.4.4 Kitkat	OCTOBER 2013	Screen record facility, Bug Fixes, Security Improvement
Android 5.0/5.0.1/5.0.2/5.1/5.1.1 Lollipop	OCTOBER 2014	Lock Protection, more than one SIM support, HD voice calls
Android 6/6.0.1 Marshmallow	OCTOBER 2015	Emojis support, Android pay facility
Android 7/7.1/7.1.1/7.1.2 Nougat	AUGUST 2016	Battery alerts, night light, new emojis
Android 8.0/8.1 Oreo	AUGUST 2017	Instant apps, system settings improvement
Android 9 Pie	AUGUST 2018	Biometric authentication, smart message notification
Android 10	SEPTEMBER 3, 2019	APIs for foldable, dark theme, gesture nav, connectivity, media, NNAPI, biometrics, high-performance codes, better biometrics, faster app starts, Vulkan 1.1, 5G,

C. Android Architecture

Android Framework consists of four layers as follows:-

- 1) Applications and features i.e, System Apps
- 2) Application framework i.e, Java API Framework
- 3) Android Runtime and native C/C++ Libraries
- 4) Linux Kernel

III. RESEARCH METHODOLOGY

Here, we will explain the methodology which is used for the research. Simultaneously we focused on the data extraction approach, different tools, and techniques that are applied in this research and all the hardware and software requirements that are needed for the observation.

A. Data Collection

For Manual data Extraction social media (i.e, WhatsApp data), used FTK, Autopsy and tool, resourceful command based tool which helps to connect to a device. Here, by using DD command we will dump a memory partition from the android seized mobile device to do the forensic investigation. From a forensic perspective, using several ADB commands we can extract data like SMS, MMS, Photos, Account Credentials, etc.

For Logical Extraction, used the AFLogical tool used to extract call logs, phone contact details, MMS messages, MMS parts, SMS messages from the target device. It is available free of cost for law enforcement personnel. Here, we have used Santoku Linux where AFLogical OSE is already installed. For Logical extraction, Physical Extraction, Capture image, and Capture Screenshot, we used Magnet Acquire, it extracts the content types like phonebook data, apps data, pictures, email data, Ringtones, Calls logs, Browsing data, Calendar, etc. To overcome the hindrance, we have used SQL DB Browser through which detection was feasible and opened for analysis.

1) Phone contents

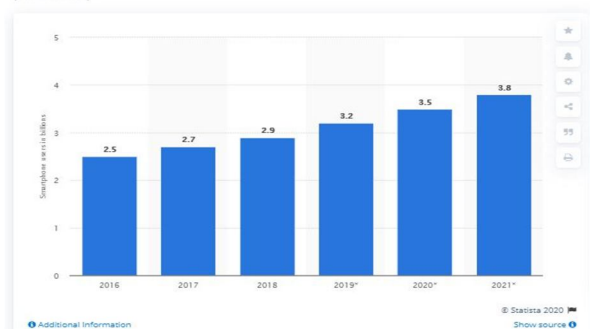
The following contents of modern Smartphone can have value as evidence:

- a) IMEI
- b) Short Dial Numbers
- c) Text Messages
- d) Settings (language, date/time, tone/volume etc)
- e) Stored Audio Recordings
- f) Stored Computer Files
- g) Logged incoming calls and dialed numbers
- h) Stored Executable Programs
- i) Stored Calendar Events

The crucial information is easily found through manufacturer software and direct analysis of the memory could potentially let out other hidden information.

The following chart shows the number of Smartphone users worldwide from 2016 to 2021.

Number of smartphone users worldwide from 2016 to 2021
(in billions)



B. Research Question for Social Media APP (i.e., Whatsapp)

The main goal of the proposed research was to answer the following question:

- 1) What artifacts can be forensically retrieved when using WhatsApp on web and Desktop Clients?
- 2) What can we access the End-to-End Encrypted data/database without rooting the mobile?
- 3) What evidence can be forensically discovered from Seize Android mobile phone and extract the data from WhatsApp .db files?

Specifically, this question was answered with the following goals:

- a) To assess if the type of operating system (i.e., Santoku Linux VM) has an impact on what can be recovered when using the adb command and AFLogical OSE.
- b) To assess if the type of web browser used (i.e., Chrome, Firefox) and OS have an impact on what can be recovered when using the WhatsApp web client and WhatsApp desktop client.
- c) To assess if the type of forensic acquisition tool used (i.e., FTK, MAGNET AXIOM/AQUIRE, Autopsy) has an impact on what can be recovered when using the WhatsApp desktop applications and web clients.
- d) To assess if the type of forensic acquisition tool used (i.e., SQLite, MAGNET AXIOM/AQUIRE, WhatsAppExtractor) has an impact on what can be recovered messages and access the encrypted to messages directly.

C. Operational Definitions

A recoverable artifact is any item of interest recovered from the forensic analysis of both the WhatsApp desktop application and the web clients on OS. Specifically, the types of recoverable artifacts, which are:

- 1) An individual chat conversation
- 2) A group chat conversation
- 3) A sent contact's information
- 4) Log of modification to the WhatsApp account's settings (i.e., display name, photo, about)
- 5) Log of viewing a status
- 6) Log of viewing a conversation's media
- 7) Log of the client being used (i.e., last access date/time, how many times)
- 8) Log of the mobile device information (e.g., device make, model, IMEI, IMSI)

D. Research Design

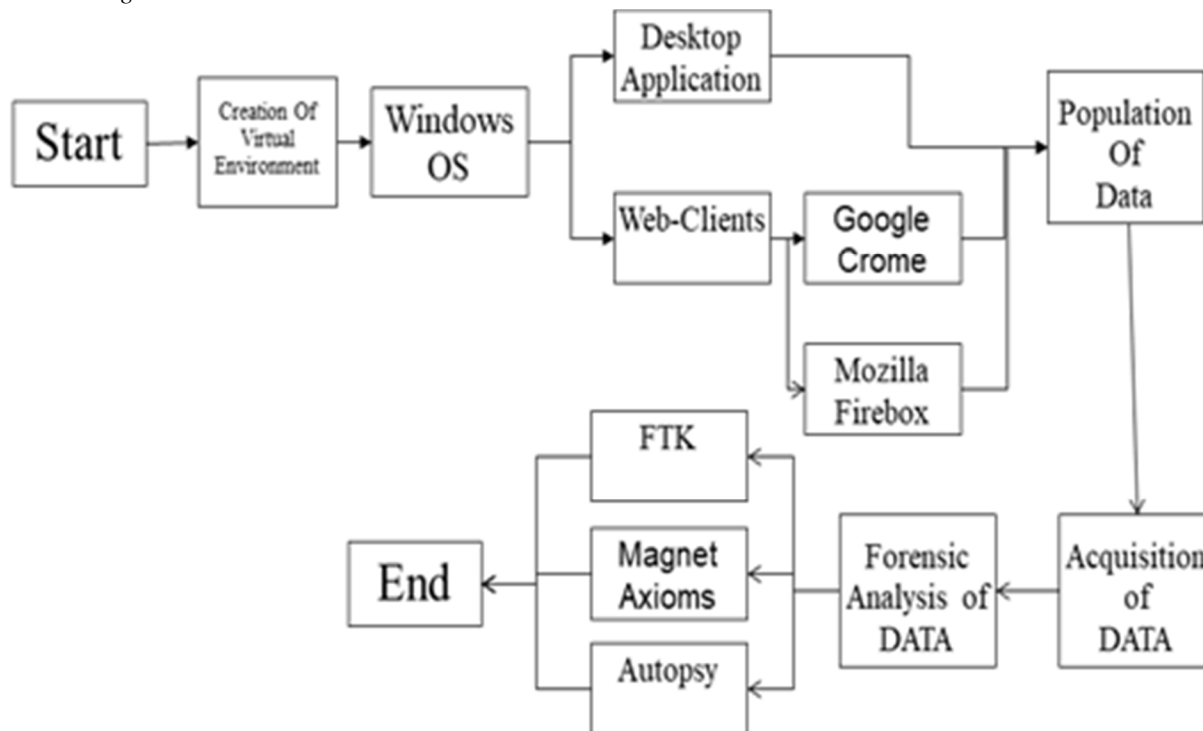


Fig-4: FlowChart for locating WhatsApp Artifacts

E. Hardware and Software Specifications

1) Windows Host Workstation

The physical host workstation for the Windows environments was a Dell Inspiron 15 3000 series with the following specifications:

- a) *CPU*: An Intel Core i3-5005U CPU @ 2.00 GHz
- b) *RAM*: 4GB RAM
- c) *Hard Drive*: 1TB HDD drive
- d) *OS*: Windows 10 Version 1903 Enterprise Build 18362.449 with NTFS

2) Software And Tools Specification/Used

- a) Magnet Acquire Tools
- b) AFLogical OSE Tools
- c) SQLite DB Browser
- d) FTK
- e) AUTOPSY

The following are the important specification in this Observation:

Table 3.1 Mobile Devices Used

Damaged Android Mobile Device	Operating System	Types Of Device
Redmi Note 3	Android 6.0.1	Rooted Condition
LeTv Max2 X821	Android 6.0.1	Unrooted Condition
Sony D5322	Android 5.1.1	Rooted Condition

Table 3.2 OS Used

Name of The Operating System
Windows OS (10 Version)
Santoku Linux

Table 3.3 Tools Used

Tool Name	Purpose
Magnet Acquire Tool	Logical and Physical Extraction
AFLogical OSE Tool	Logical Extraction
SQLite DB Browser	Extraction .db data open and access

Table 3.4 Data Cable Used

Data Cable Used
Mi Data & Charging Cable for Xiaomi Redmi Note 3 (MediaTek) Micro USB Data Cable (2.4 Amp, 1M, Black) and C-type data cable by Xiaomi Technology India Private Limited, an authorized Indian distributor of Mi products.

Table 3.5 Programming Language Used

Programming Language Used
Shell Script

IV. IMPLEMENTATIONS AND RESULTS

The data extraction using Santoku Linux with Aflogical command:

A. Evidence Intake Phase

The proposed technique was implemented using an Android mobile device that was found at a crime scene.

B. Identification Phase

It was necessary to identify whether or not the Android mobile device was associated with the crime.

C. Preparation Phase

1) *Hardware and Software Preparation:* The hardware requirements were the host machine (computer), USB Cable, USB Memory Storage, and SD Adapter and Software requirement was Santoka Linux VM, AccessData FTK imager, Autopsy, Android Studio, and other tools.

D. Isolation Phase

The Bluetooth and wireless network needed to be switched off in the mobile device. As there was no SIM card used, we did not need to perform any other steps.

E. Processing Phase

The practical steps and tools which were used in the processing and verification phases are summarized in fig-5.

There are two extra steps used in this phase:

- 1) *Step 1: Connection and Backup (Manual Acquisition)* The USB driver of mobile phone applications were installed after installing Android Studio (SDK manager) to connect the mobile device with the computer. Then, the mobile device documents need to transfer to the USB Memory Drive in the computer user manual full backup, which is called "Manual Direct Acquisition"
- 2) *Step 2: Unlock the mobile device using the Santoku Linux tool*, which is sponsored by ViaForensics, the mobile device can be unlocked to access the root of the devices file system.
 - a) The mobile device needs to be enabled for USB debugging by Settings => Developer Options, then checking (Allow mock locations), (Stay awake) and (USB debugging), as shown in fig- 6. If the Developer Options setting is not found, go to Settings => About devices => Tap on (Build Number) seven times, then Developer Options will appear.
 - b) The mobile device then connected to the computer using Santoku Linux in Virtual Machine, by going to Devices => USB Devices => Click on the mobile device name, making a checkmark next to the mobile device, as shown in figure 6. Then, we should agree on the mobile to allow debugging with the computer by choosing OK.
 - c) In the Santoku Linux Virtual Machine, Santoku => Device Forensics => AFLogical OSE command prompt, the command "adb devices" used to show the serial number of the mobile device.

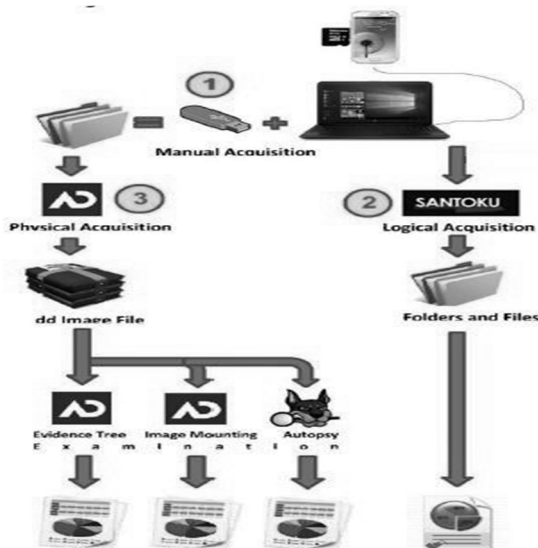


Fig-5: Diagram for Processing Phases, including Manual, Logical and Physical Acquisition; and Verification Phase.

F. Android Debug Bridge (ADB)

It is a flexible and resourceful command based tool which helps to connect to a device. It is a client-server program which consists of three segments:

- 1) One client, who is generally, runs on the forensic investigator's development machine.
- 2) One server, which is executed as a backdrop process on the forensic investigator's development machine.

One daemon, which is executed as a backdrop process on every device. It is used to execute a command on the device.

The Android OS has a choice for a developer (Developer option) whenever the analysts try to communicate and transfer data through a USB connection, the USB debugging choice must be enabled. To make it enable, first go to Phone Settings and then chose option about the phone and click on Build number seven times. Return to the settings screen you will find Developer options at the bottom. After building the Developer option, enable USB debugging and always choose the option to stay awake on.

In the Default "charge only" mode is selected, Forensic analyst has to select "Transfer files (MTP)" to allow transfer data from the seized device to the forensic workstation.

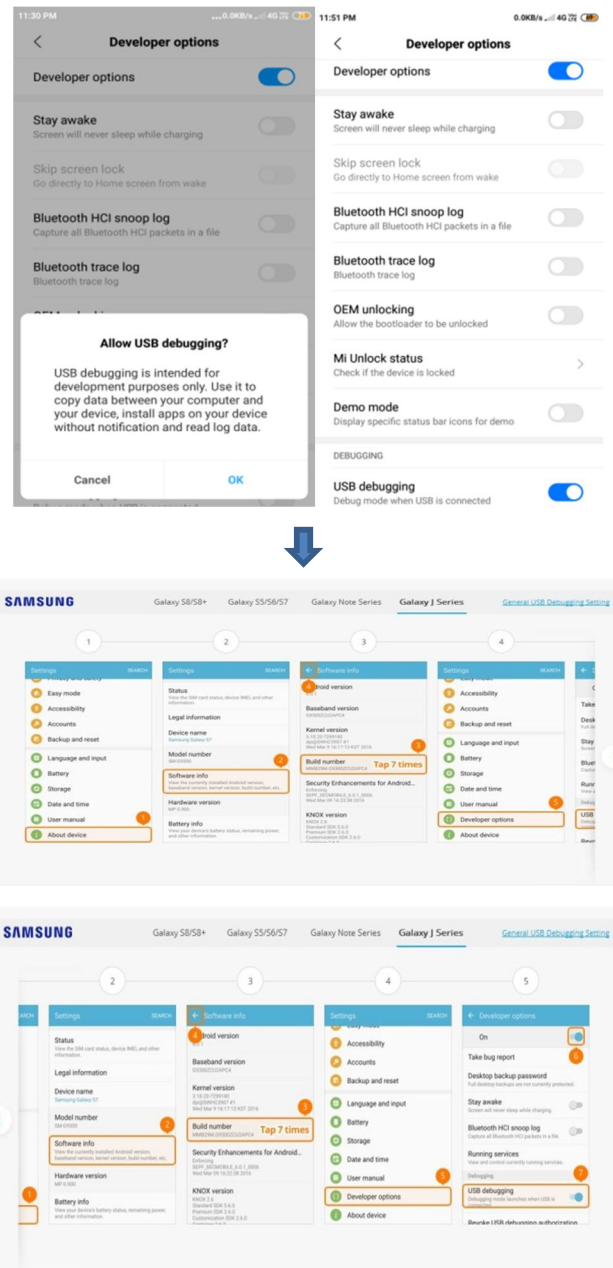


Fig 6: Enable USB Debugging

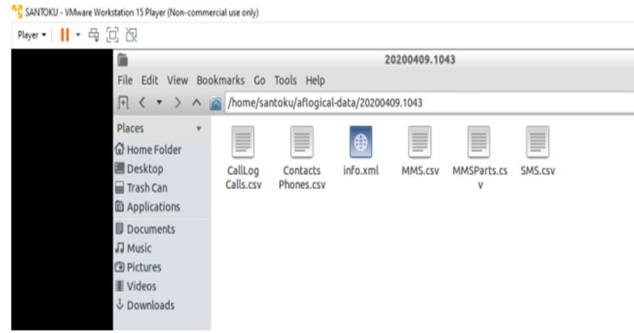


Fig-11: Extracted data or artifacts

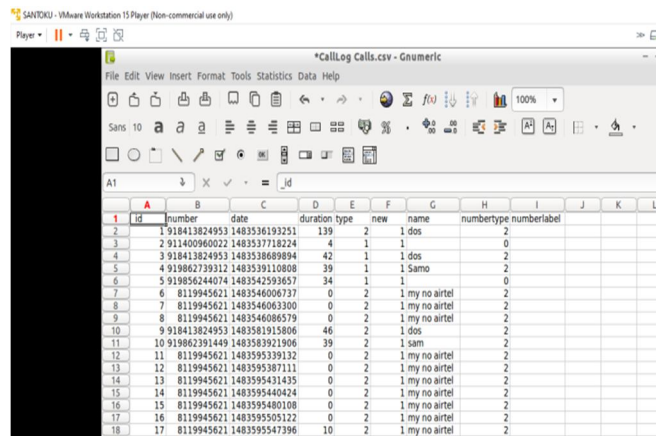


Fig-12: CallLogs History details at Santoku Machine

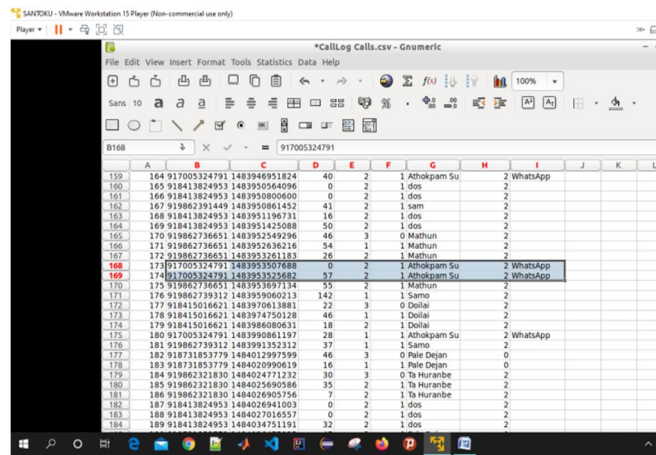


Fig-13: CallLogs History details connected with WhatsApp at Santoku Machine

H. Manual Data Extraction Using Magnet Acquire

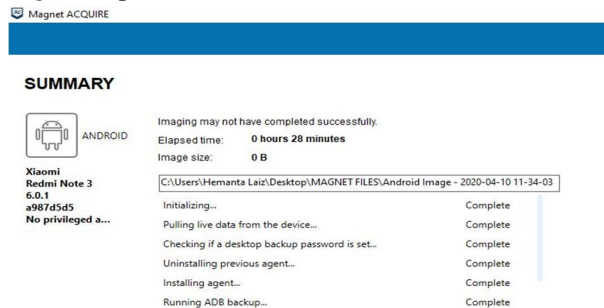
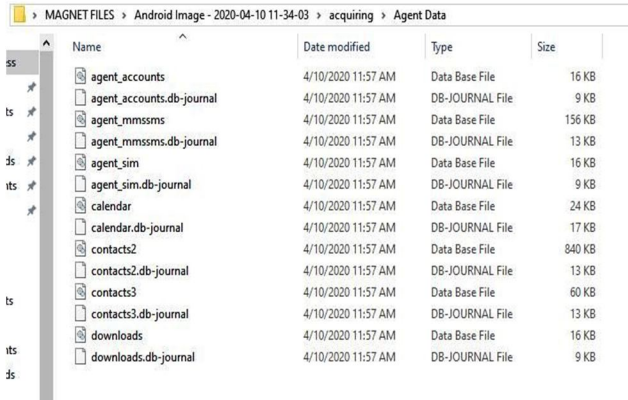
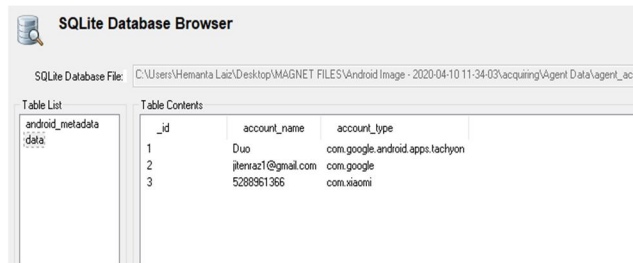


Fig-14: Extraction process for Magnet Acquire



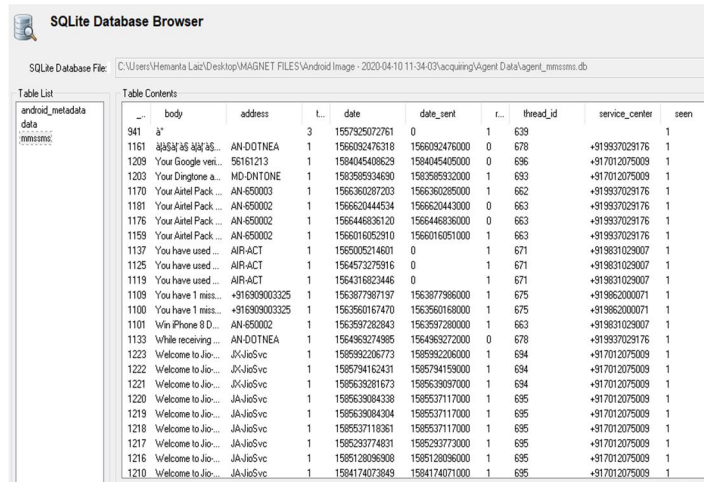
Name	Date modified	Type	Size
agent_accounts	4/10/2020 11:57 AM	Data Base File	16 KB
agent_accounts.db-journal	4/10/2020 11:57 AM	DB-JOURNAL File	9 KB
agent_mmsms	4/10/2020 11:57 AM	Data Base File	156 KB
agent_mmsms.db-journal	4/10/2020 11:57 AM	DB-JOURNAL File	13 KB
agent_sim	4/10/2020 11:57 AM	Data Base File	16 KB
agent_sim.db-journal	4/10/2020 11:57 AM	DB-JOURNAL File	9 KB
calendar	4/10/2020 11:57 AM	Data Base File	24 KB
calendar.db-journal	4/10/2020 11:57 AM	DB-JOURNAL File	17 KB
contacts2	4/10/2020 11:57 AM	Data Base File	840 KB
contacts2.db-journal	4/10/2020 11:57 AM	DB-JOURNAL File	13 KB
contacts3	4/10/2020 11:57 AM	Data Base File	60 KB
contacts3.db-journal	4/10/2020 11:57 AM	DB-JOURNAL File	13 KB
downloads	4/10/2020 11:57 AM	Data Base File	16 KB
downloads.db-journal	4/10/2020 11:57 AM	DB-JOURNAL File	9 KB

Fig-15: Extracted database from Android mobile



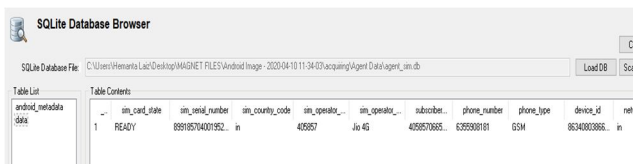
_id	account_name	account_type
1	Duo	com.google.android.apps.tachyon
2	ijeraz1@gmail.com	com.google
3	5288961366	com.xiaomi

Fig-16: Android mobile's Google account details



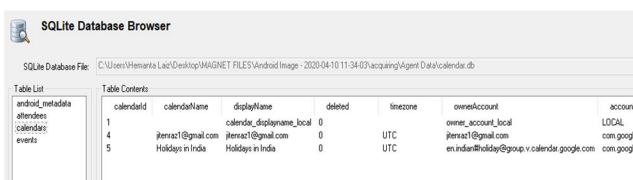
_id	body	address	l	date	date_sent	r	thread_id	service_center	seen
941	à	AN-DOTNEA	3	1557292072761	0	1	639		1
1161	اهاياك في وقتك	AN-DOTNEA	1	156092476318	1560924760000	0	678	+919937029176	1
1209	Your Google veri...	56161213	1	1584045408629	1584045405000	0	696	+917012075009	1
1203	Your Dingtone a...	MD-DNTONE	1	158395934690	1583959320000	1	693	+917012075009	1
1170	Your Airtel Pack...	AN-650003	1	1566360287203	1566360285000	1	662	+919937029176	1
1181	Your Airtel Pack...	AN-650002	1	156620444534	1566204430000	0	663	+919937029176	1
1176	Your Airtel Pack...	AN-650002	1	1566446836120	1566446836000	0	663	+919937029176	1
1159	Your Airtel Pack...	AN-650002	1	1566016052910	1566016051000	1	663	+919937029176	1
1137	You have used ...	AIR-ACT	1	1565005214801	0	1	671	+919831029007	1
1125	You have used ...	AIR-ACT	1	1564573275916	0	1	671	+919831029007	1
1119	You have used ...	AIR-ACT	1	1564318822446	0	1	671	+919831029007	1
1109	You have 1 miss...	+916300003325	1	1563877387197	1563877386000	1	675	+919862000071	1
1100	You have 1 miss...	+916300003325	1	1563560167470	1563560166000	1	675	+919862000071	1
1101	Win iPhone 8 D...	AN-650002	1	1562597282843	1562597280000	1	663	+919831029007	1
1133	While receiving...	AN-DOTNEA	1	1564969274965	1564969272000	0	678	+919937029176	1
1223	Welcome to Jio...	Jio-JioSvc	1	1595992206773	1595992206000	1	694	+917012075009	1
1222	Welcome to Jio...	Jio-JioSvc	1	1595794162431	1595794159000	1	694	+917012075009	1
1221	Welcome to Jio...	Jio-JioSvc	1	1595638281673	1595638097000	1	694	+917012075009	1
1220	Welcome to Jio...	Jio-JioSvc	1	1595639084338	1595637117000	1	695	+917012075009	1
1219	Welcome to Jio...	Jio-JioSvc	1	1595639084304	1595637117000	1	695	+917012075009	1
1218	Welcome to Jio...	Jio-JioSvc	1	1595637118361	1595637117000	1	695	+917012075009	1
1217	Welcome to Jio...	Jio-JioSvc	1	1595293774831	1595293773000	1	695	+917012075009	1
1216	Welcome to Jio...	Jio-JioSvc	1	1595128096908	1595128096000	1	695	+917012075009	1
1210	Welcome to Jio...	Jio-JioSvc	1	1584174073843	1584174071000	1	695	+917012075009	1

Fig-17: Extracted MMS-SMS data



_id	sim_card_state	sim_serial_number	sim_country_code	sim_operator	sim_operator...	subscriber...	phone_number	phone_type	device_id	network
1	READY	699165704001952	in	40957	Jio 4G	409570865...	639599181	GSM	8634080866...	in

Fig-18: Extracted Agent SIM card details



calendarid	calendarName	displayName	deleted	timezone	ownerAccount	accountType
1		calendar_display_name_local	0		owner_account_local	LOCAL
4	ijeraz1@gmail.com	ijeraz1@gmail.com	0	UTC	ijeraz1@gmail.com	com.google
5	Holidays in India	Holidays in India	0	UTC	en.india@holidaygroup.v.calendar.google.com	com.google

Fig-19: Extracted Calendar and event details

SQLite Database Browser

SQLite Database File: C:\Users\Hemanta Lait\Desktop\MAGNET FILES\Android Image - 2020-04-10 11:34:03\acquiring\Agent Data\contacts2.db

Table List	Table Contents																																																																																																																																										
android_metadata																																																																																																																																											
calls	<table border="1"> <thead> <tr> <th>id</th> <th>name</th> <th>number</th> <th>date</th> <th>type</th> <th>duration</th> </tr> </thead> <tr><td>1</td><td></td><td>07569422933</td><td>1595639136088</td><td>2</td><td>0</td></tr> <tr><td>2</td><td></td><td>+918124238160</td><td>1595128737637</td><td>1</td><td>19</td></tr> <tr><td>3</td><td></td><td>+9173630909</td><td>1595128704321</td><td>1</td><td>0</td></tr> <tr><td>4</td><td></td><td>07629008977</td><td>1594292709891</td><td>2</td><td>0</td></tr> <tr><td>5</td><td></td><td>+918073382412</td><td>1594045545792</td><td>2</td><td>1</td></tr> <tr><td>6</td><td></td><td>+918073382412</td><td>1594045533138</td><td>2</td><td>4</td></tr> <tr><td>7</td><td></td><td>+918073382412</td><td>1594045507773</td><td>2</td><td>1</td></tr> <tr><td>8</td><td></td><td>+918073382412</td><td>1594045458999</td><td>2</td><td>5</td></tr> <tr><td>9</td><td>ICHAN</td><td>08073382412</td><td>1593517313308</td><td>2</td><td>0</td></tr> <tr><td>10</td><td></td><td>08073382412</td><td>1593467425432</td><td>2</td><td>0</td></tr> <tr><td>11</td><td></td><td>7005301746</td><td>1593424047003</td><td>2</td><td>0</td></tr> <tr><td>12</td><td></td><td>9378117636</td><td>1593424007573</td><td>2</td><td>0</td></tr> <tr><td>13</td><td></td><td>07629008977</td><td>1593423985159</td><td>2</td><td>0</td></tr> <tr><td>14</td><td></td><td>+913386287602</td><td>1573473726184</td><td>2</td><td>0</td></tr> <tr><td>15</td><td></td><td>1400630127</td><td>157346936530</td><td>2</td><td>0</td></tr> <tr><td>16</td><td>ROMITA2</td><td>+917005052927</td><td>1573469791121</td><td>1</td><td>31</td></tr> <tr><td>17</td><td>ROMITA2</td><td>+917005052927</td><td>1573469763284</td><td>1</td><td>12</td></tr> <tr><td>18</td><td>ROMITA2</td><td>+917005052927</td><td>1573469369114</td><td>2</td><td>364</td></tr> <tr><td>19</td><td>roshni2</td><td>+918003886268</td><td>1573467680109</td><td>2</td><td>965</td></tr> <tr><td>20</td><td>yabba 2</td><td>+916309003325</td><td>1573446196169</td><td>3</td><td>40</td></tr> <tr><td>21</td><td>yabba 2</td><td>+916309003325</td><td>1573446119370</td><td>3</td><td>40</td></tr> <tr><td>22</td><td>chaaba mamang</td><td>+91790824587</td><td>1573445749389</td><td>3</td><td>20</td></tr> </table>	id	name	number	date	type	duration	1		07569422933	1595639136088	2	0	2		+918124238160	1595128737637	1	19	3		+9173630909	1595128704321	1	0	4		07629008977	1594292709891	2	0	5		+918073382412	1594045545792	2	1	6		+918073382412	1594045533138	2	4	7		+918073382412	1594045507773	2	1	8		+918073382412	1594045458999	2	5	9	ICHAN	08073382412	1593517313308	2	0	10		08073382412	1593467425432	2	0	11		7005301746	1593424047003	2	0	12		9378117636	1593424007573	2	0	13		07629008977	1593423985159	2	0	14		+913386287602	1573473726184	2	0	15		1400630127	157346936530	2	0	16	ROMITA2	+917005052927	1573469791121	1	31	17	ROMITA2	+917005052927	1573469763284	1	12	18	ROMITA2	+917005052927	1573469369114	2	364	19	roshni2	+918003886268	1573467680109	2	965	20	yabba 2	+916309003325	1573446196169	3	40	21	yabba 2	+916309003325	1573446119370	3	40	22	chaaba mamang	+91790824587	1573445749389	3	20
id	name	number	date	type	duration																																																																																																																																						
1		07569422933	1595639136088	2	0																																																																																																																																						
2		+918124238160	1595128737637	1	19																																																																																																																																						
3		+9173630909	1595128704321	1	0																																																																																																																																						
4		07629008977	1594292709891	2	0																																																																																																																																						
5		+918073382412	1594045545792	2	1																																																																																																																																						
6		+918073382412	1594045533138	2	4																																																																																																																																						
7		+918073382412	1594045507773	2	1																																																																																																																																						
8		+918073382412	1594045458999	2	5																																																																																																																																						
9	ICHAN	08073382412	1593517313308	2	0																																																																																																																																						
10		08073382412	1593467425432	2	0																																																																																																																																						
11		7005301746	1593424047003	2	0																																																																																																																																						
12		9378117636	1593424007573	2	0																																																																																																																																						
13		07629008977	1593423985159	2	0																																																																																																																																						
14		+913386287602	1573473726184	2	0																																																																																																																																						
15		1400630127	157346936530	2	0																																																																																																																																						
16	ROMITA2	+917005052927	1573469791121	1	31																																																																																																																																						
17	ROMITA2	+917005052927	1573469763284	1	12																																																																																																																																						
18	ROMITA2	+917005052927	1573469369114	2	364																																																																																																																																						
19	roshni2	+918003886268	1573467680109	2	965																																																																																																																																						
20	yabba 2	+916309003325	1573446196169	3	40																																																																																																																																						
21	yabba 2	+916309003325	1573446119370	3	40																																																																																																																																						
22	chaaba mamang	+91790824587	1573445749389	3	20																																																																																																																																						

Fig-20: Extracted Contact calls history details

SQLite Database Browser

SQLite Database File: C:\Users\Hemanta Lait\Desktop\MAGNET FILES\Android Image - 2020-04-10 11:34:03\acquiring\Agent Data\contacts3.db

Table List	Table Contents																																																																																																																																																																																																															
acquired_contacts																																																																																																																																																																																																																
addresses																																																																																																																																																																																																																
android_metadata																																																																																																																																																																																																																
websites																																																																																																																																																																																																																
	<table border="1"> <thead> <tr> <th>id</th> <th>ContactId</th> <th>Displayname</th> <th>PhoneNumbers</th> <th>Accounts</th> <th>Emails</th> <th>Notes</th> <th>Photo</th> <th>Ts</th> </tr> </thead> <tr><td>1</td><td>8744</td><td>Pale Nanci</td><td></td><td></td><td></td><td></td><td></td><td>0</td></tr> <tr><td>2</td><td>8745</td><td>Jugnan</td><td>Mobile +91 97 9...</td><td>com.xiaomi.528991366</td><td></td><td></td><td></td><td>0</td></tr> <tr><td>3</td><td>8746</td><td>S</td><td>Mobile 84 14 81...</td><td>com.xiaomi.528991366</td><td></td><td></td><td></td><td>0</td></tr> <tr><td>4</td><td>9002</td><td>Riano</td><td>Mobile +91 87 3...</td><td>com.xiaomi.528991366,com.google.android.apps.tachyon.Duo</td><td></td><td></td><td></td><td>0</td></tr> <tr><td>5</td><td>9003</td><td>Bojan</td><td>Mobile +91 81 3...</td><td>com.xiaomi.528991366,com.google.android.apps.tachyon.Duo</td><td></td><td></td><td></td><td>0</td></tr> <tr><td>6</td><td>9004</td><td>Geban</td><td>Mobile +91 86 1...</td><td>com.xiaomi.528991366</td><td></td><td></td><td></td><td>0</td></tr> <tr><td>7</td><td>9005</td><td>Milan</td><td>Mobile 98 56 47...</td><td>com.xiaomi.528991366</td><td></td><td></td><td></td><td>0</td></tr> <tr><td>8</td><td>9025</td><td>Chaaba New</td><td>Mobile 0721 926...</td><td>com.xiaomi.528991366,com.google.android.apps.tachyon.Duo</td><td></td><td></td><td></td><td>0</td></tr> <tr><td>9</td><td>9027</td><td>A</td><td></td><td></td><td></td><td></td><td></td><td>0</td></tr> <tr><td>10</td><td>9028</td><td>Tom</td><td>Mobile +91 94 0...</td><td>com.xiaomi.528991366</td><td></td><td></td><td>BLOB(5089)</td><td>0</td></tr> <tr><td>11</td><td>9029</td><td>Ta Kurjao</td><td>Mobile +91 87 3...</td><td>com.xiaomi.528991366</td><td></td><td></td><td></td><td>0</td></tr> <tr><td>12</td><td>9030</td><td>Ehounj</td><td></td><td></td><td></td><td></td><td></td><td>0</td></tr> <tr><td>13</td><td>9031</td><td>Enoude</td><td>Mobile +91 80 1...</td><td>com.xiaomi.528991366</td><td></td><td></td><td></td><td>0</td></tr> <tr><td>14</td><td>9032</td><td>Tanthe Etso</td><td>Mobile +91 81 1...</td><td>com.xiaomi.528991366,com.google.android.apps.tachyon.Duo</td><td></td><td></td><td></td><td>0</td></tr> <tr><td>15</td><td>9033</td><td>Maha</td><td>Mobile 96 15 27...</td><td>com.xiaomi.528991366</td><td></td><td></td><td></td><td>0</td></tr> <tr><td>16</td><td>9034</td><td>Jab Sangi</td><td></td><td></td><td></td><td></td><td></td><td>0</td></tr> <tr><td>17</td><td>9035</td><td>Da</td><td>Mobile +91 80 1...</td><td>com.xiaomi.528991366</td><td></td><td></td><td>BLOB(6007)</td><td>0</td></tr> <tr><td>18</td><td>9036</td><td>Eyden</td><td>Mobile 98 56 47...</td><td>com.xiaomi.528991366</td><td></td><td></td><td></td><td>0</td></tr> <tr><td>19</td><td>9037</td><td>Lukan</td><td>Mobile +91 8374...</td><td>com.xiaomi.528991366</td><td></td><td></td><td></td><td>0</td></tr> <tr><td>20</td><td>9038</td><td>M Hamanta</td><td></td><td></td><td></td><td></td><td></td><td>0</td></tr> <tr><td>21</td><td>9039</td><td></td><td></td><td></td><td></td><td></td><td></td><td>0</td></tr> <tr><td>22</td><td>10842</td><td>Sitanile</td><td>Mobile +91 92 8...</td><td>com.xiaomi.528991366,com.google.android.apps.tachyon.Duo</td><td></td><td></td><td></td><td>0</td></tr> </table>	id	ContactId	Displayname	PhoneNumbers	Accounts	Emails	Notes	Photo	Ts	1	8744	Pale Nanci						0	2	8745	Jugnan	Mobile +91 97 9...	com.xiaomi.528991366				0	3	8746	S	Mobile 84 14 81...	com.xiaomi.528991366				0	4	9002	Riano	Mobile +91 87 3...	com.xiaomi.528991366,com.google.android.apps.tachyon.Duo				0	5	9003	Bojan	Mobile +91 81 3...	com.xiaomi.528991366,com.google.android.apps.tachyon.Duo				0	6	9004	Geban	Mobile +91 86 1...	com.xiaomi.528991366				0	7	9005	Milan	Mobile 98 56 47...	com.xiaomi.528991366				0	8	9025	Chaaba New	Mobile 0721 926...	com.xiaomi.528991366,com.google.android.apps.tachyon.Duo				0	9	9027	A						0	10	9028	Tom	Mobile +91 94 0...	com.xiaomi.528991366			BLOB(5089)	0	11	9029	Ta Kurjao	Mobile +91 87 3...	com.xiaomi.528991366				0	12	9030	Ehounj						0	13	9031	Enoude	Mobile +91 80 1...	com.xiaomi.528991366				0	14	9032	Tanthe Etso	Mobile +91 81 1...	com.xiaomi.528991366,com.google.android.apps.tachyon.Duo				0	15	9033	Maha	Mobile 96 15 27...	com.xiaomi.528991366				0	16	9034	Jab Sangi						0	17	9035	Da	Mobile +91 80 1...	com.xiaomi.528991366			BLOB(6007)	0	18	9036	Eyden	Mobile 98 56 47...	com.xiaomi.528991366				0	19	9037	Lukan	Mobile +91 8374...	com.xiaomi.528991366				0	20	9038	M Hamanta						0	21	9039							0	22	10842	Sitanile	Mobile +91 92 8...	com.xiaomi.528991366,com.google.android.apps.tachyon.Duo				0
id	ContactId	Displayname	PhoneNumbers	Accounts	Emails	Notes	Photo	Ts																																																																																																																																																																																																								
1	8744	Pale Nanci						0																																																																																																																																																																																																								
2	8745	Jugnan	Mobile +91 97 9...	com.xiaomi.528991366				0																																																																																																																																																																																																								
3	8746	S	Mobile 84 14 81...	com.xiaomi.528991366				0																																																																																																																																																																																																								
4	9002	Riano	Mobile +91 87 3...	com.xiaomi.528991366,com.google.android.apps.tachyon.Duo				0																																																																																																																																																																																																								
5	9003	Bojan	Mobile +91 81 3...	com.xiaomi.528991366,com.google.android.apps.tachyon.Duo				0																																																																																																																																																																																																								
6	9004	Geban	Mobile +91 86 1...	com.xiaomi.528991366				0																																																																																																																																																																																																								
7	9005	Milan	Mobile 98 56 47...	com.xiaomi.528991366				0																																																																																																																																																																																																								
8	9025	Chaaba New	Mobile 0721 926...	com.xiaomi.528991366,com.google.android.apps.tachyon.Duo				0																																																																																																																																																																																																								
9	9027	A						0																																																																																																																																																																																																								
10	9028	Tom	Mobile +91 94 0...	com.xiaomi.528991366			BLOB(5089)	0																																																																																																																																																																																																								
11	9029	Ta Kurjao	Mobile +91 87 3...	com.xiaomi.528991366				0																																																																																																																																																																																																								
12	9030	Ehounj						0																																																																																																																																																																																																								
13	9031	Enoude	Mobile +91 80 1...	com.xiaomi.528991366				0																																																																																																																																																																																																								
14	9032	Tanthe Etso	Mobile +91 81 1...	com.xiaomi.528991366,com.google.android.apps.tachyon.Duo				0																																																																																																																																																																																																								
15	9033	Maha	Mobile 96 15 27...	com.xiaomi.528991366				0																																																																																																																																																																																																								
16	9034	Jab Sangi						0																																																																																																																																																																																																								
17	9035	Da	Mobile +91 80 1...	com.xiaomi.528991366			BLOB(6007)	0																																																																																																																																																																																																								
18	9036	Eyden	Mobile 98 56 47...	com.xiaomi.528991366				0																																																																																																																																																																																																								
19	9037	Lukan	Mobile +91 8374...	com.xiaomi.528991366				0																																																																																																																																																																																																								
20	9038	M Hamanta						0																																																																																																																																																																																																								
21	9039							0																																																																																																																																																																																																								
22	10842	Sitanile	Mobile +91 92 8...	com.xiaomi.528991366,com.google.android.apps.tachyon.Duo				0																																																																																																																																																																																																								

Fig-21: Extracted Contact list details

SQLite Database Browser

SQLite Database File: C:\Users\Hemanta Lait\Desktop\MAGNET FILES\Android Image - 2020-04-10 11:34:03\acquiring\Agent Data\downloads.db

Table List	Table Contents																				
android_metadata																					
downloads	<table border="1"> <thead> <tr> <th>id</th> <th>uri</th> <th>lastmod</th> <th>total_bytes</th> <th>_data</th> </tr> </thead> <tr><td>1</td><td>/storage/emulated/0/Download...</td><td>1527124427000</td><td>96</td><td>BLOB(96)</td></tr> <tr><td>2</td><td>/storage/emulated/0/Download...</td><td>1593498425000</td><td>88632363</td><td>(null)</td></tr> <tr><td>3</td><td>/storage/emulated/0/Download...</td><td>1584214185000</td><td>201318220</td><td>(null)</td></tr> </table>	id	uri	lastmod	total_bytes	_data	1	/storage/emulated/0/Download...	1527124427000	96	BLOB(96)	2	/storage/emulated/0/Download...	1593498425000	88632363	(null)	3	/storage/emulated/0/Download...	1584214185000	201318220	(null)
id	uri	lastmod	total_bytes	_data																	
1	/storage/emulated/0/Download...	1527124427000	96	BLOB(96)																	
2	/storage/emulated/0/Download...	1593498425000	88632363	(null)																	
3	/storage/emulated/0/Download...	1584214185000	201318220	(null)																	

Fig-22: Extracted Download list details

MAGNET FILES > Android Image - 2020-04-10 11:34:03 > acquiring > Live Data > Dumpsys Data

Name	Date modified	Type	Size
accessibility	4/10/2020 11:34 AM	Text Document	1 KB
account	4/10/2020 11:34 AM	Text Document	15 KB
activity	4/10/2020 11:34 AM	Text Document	172 KB
alarm	4/10/2020 11:34 AM	Text Document	48 KB
apps	4/10/2020 11:34 AM	Text Document	134 KB
appwidget	4/10/2020 11:34 AM	Text Document	10 KB
audio	4/10/2020 11:34 AM	Text Document	5 KB
backup	4/10/2020 11:34 AM	Text Document	8 KB
battery	4/10/2020 11:34 AM	Text Document	1 KB
batteryproperties	4/10/2020 11:34 AM	Text Document	1 KB
batterystats	4/10/2020 11:34 AM	Text Document	41 KB
bluetooth_manager	4/10/2020 11:34 AM	Text Document	1 KB
carrier_config	4/10/2020 11:34 AM	Text Document	1 KB
com.xiaomi.mipayservice	4/10/2020 11:34 AM	Text Document	1 KB
com.xiaomi.mtservice	4/10/2020 11:34 AM	Text Document	1 KB

Fig-23: Extracted Android Mobile artifact list details

I. Whatsapp Data Extraction And Finding Artifacts From Web Or Digital Evidence

To investigate the Social Media app i.e, WhatsApp, we have recovered the artifacts as follows:

1) **Whatsapp Log Artifacts Output:** The artifacts which are collected from Windows Environment and WhatsApp Client and WhatsApp Windows. They are in the following tables:

WhatsApp Client	WhatsApp Log File
Desktop Application	Users\{SUSPECT}\AppData\Roaming\WhatsApp\IndexedDB\file0.indexeddb.leveldb\{#####}.log
Chrome Client	Users\{SUSPECT}\AppData\Local\Google\Chrome\UserData\Default\IndexedDB\https_web.whatsapp.com_0.indexeddb.leveldb\{#####}.log
Firefox Client	Users\{SUSPECT}\AppData\Roaming\Mozilla\Firefox\Profiles\xqimcpc.default\storage\default\https+++web.whatsapp.com\idb\{##} wcaw.sqlite

Table 4.1: Recovered artifact locations for the Windows environments

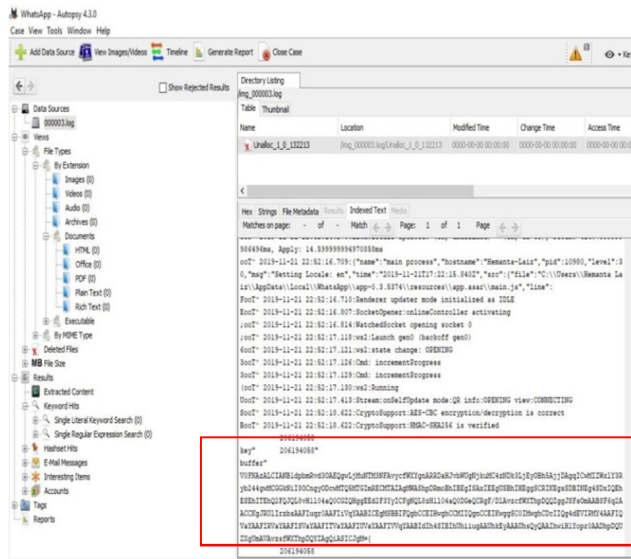
Category	Artifacts	Notes
Mobile Device Information	webcPhoneOsBuildNumber = FGXOSOP5801507066S	Mobile device OS build
Mobile Device Information	number webcPhoneOsVersion = 6.0.1	Mobile device OS version
Mobile Device Information	webcPhoneAppVersion = 2.19.1248i	Mobile device WhatsApp application version
Mobile Device Information	webcPhoneDeviceManufacturer = Google	Mobile device manufacturer
Mobile Device Information	webcPhoneCharging = false	Mobile phone charging. In this case, at the time it was not charging

Table 4.2: Recovered artifact for Mobile Device Information locations from Windows.

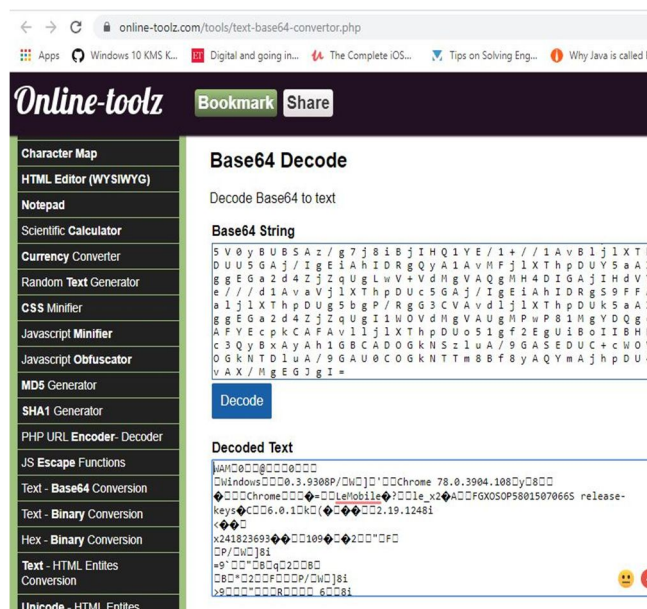
Category	Artifacts	Notes
Browser User-Agent (Mozilla)	userAgent: / Mozilla firefox/71.0/WINNT/en-US/firefox (Windows NT 10.0; Win64; x64)	Identifies the browser client and OS being used by the suspect.
Browser User-Agent (Google Chrome)	Google Chrome is up to date Version 78.0.3904.108 (Official Build) (64-bit)	Identifies the browser client and OS being used by the suspect.

Table 4.3: Browser Details and recovered artifacts extracted from the WhatsApp log file

The output for WhatsApp Client and WhatsApp data extraction with analysis details are given below:



Output-1: Locating artifacts from WhatsApp Log file using Autopsy



Output-2: Recovered the artifacts from WhatsApp Log File.

```

image_info - Notepad
File Edit Format View Help
Serial Number: a987d5d5

Additional Device Information
Boot Serial Number: a987d5d5
Bootloader: unknown
Build Date UTC: 1547470690
Build ID: MMB29M
SDK Version: 23
Security Patch: 2018-07-01
GSM Version: 6.0_r12
Device Encryption: encrypted
Encryption Type: block
Product Board: msm8952
Product Brand: Xiaomi
CPU ABI: arm64-v8a
Product Device: kenzo
  
```

Output-3: Device Information

WhatsApp Client	Artifact and Location
	Installed program ¹ : Users\{SUSPECT}\AppData\Local\WhatsApp
	Registry key ² : Users\{SUSPECT}\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Uninstall\WhatsApp
	WhatsApp prefetch file ³ : Windows\Prefetch\WHATSAPP.EXE-06A9BBC4.pf
Desktop Application	WhatsApp shortcut file ³ : Users\{SUSPECT}\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\WhatsApp\WhatsApp.lnk Users\{SUSPECT}\AppData\Desktop\WhatsApp.lnk
	Cached profile pictures ⁴ : Users\{SUSPECT}\AppData\Roaming\WhatsApp\Cache
	Chrome history file ⁵ : Users\{SUSPECT}\AppData\Local\Google\Chrome\User Data\Default\History
	Chrome prefetch file ³ : Windows\Prefetch\CHROME.EXE-CCF9F3F6.pf
Chrome Client	Chrome shortcut files ³ : ProgramData\Microsoft\Windows\Start Menu\Programs\Google Chrome.lnk Users\Public\Desktop\Google Chrome.lnk Users\{SUSPECT}\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Google Chrome.lnk
	Cached profile pictures ⁴ : Users\{SUSPECT}\AppData\Local\Google\Chrome\User Data\Default\Cache
	Firefox history file ⁵ : Users\{SUSPECT}\AppData\Roaming\Mozilla\Firefox\Profiles\xqimcpc.default\places.sqlite
	Firefox prefetch file ³ : Windows\Prefetch\FIREFOX.EXE-25FC0A66.pf
Firefox Client	Firefox shortcut files ³ : Users\{SUSPECT}\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Firefox.lnk Users\{SUSPECT}\AppData\Desktop\Firefox.lnk
	Cached profile pictures ⁴ : Users\{SUSPECT}\AppData\Local\Mozilla\Firefox\Profiles\xqimcpc.default\cache2\entries

Note. All clients described on this table refer to those located in the Windows OS.
¹: An installed program will have a unique installation location within the drive as well as an entry in the registry key of the machine.
²: The prefetch file will contain information regarding how many times the application was run along with its run date/time.
³: The shortcut files, also known as LNK file, contains information regarding the application's last accessed date/time.
⁴: Cached profile pictures recovered include the suspect, victim, and group chat.
⁵: The history file will contain information regarding the web.whatsapp.com URL such as the last visited date/time, the visit count, and the number of times the URL was typed.

Table 4.4: Additional Artifacts discovered in the Windows OS

```

image_info - Notepad
File Edit Format View Help
Imager Product: Magnet ACQUIRE
Imager Version: 2.20.0.17984

Examiner Name: Laiz
Evidence Number: 12345
Description: Mobile Forensics

Relative Activity Log Path: activity_log.txt
Original Activity Log Path: C:\Users\Hemanta Laiz\Desktop\MAGNET FILES\Android Image - 2019-12-04 01-49-19\activity_log.txt
Activity Log MD5 Hash: 260D2BB2D7F6C7EF8CD56FACA46D3B78

Output Directory: Android Image - 2019-12-04 01-49-19
Full Output Directory: C:\Users\Hemanta Laiz\Desktop\MAGNET FILES\Android Image - 2019-12-04 01-49-19

Total Segments: 1

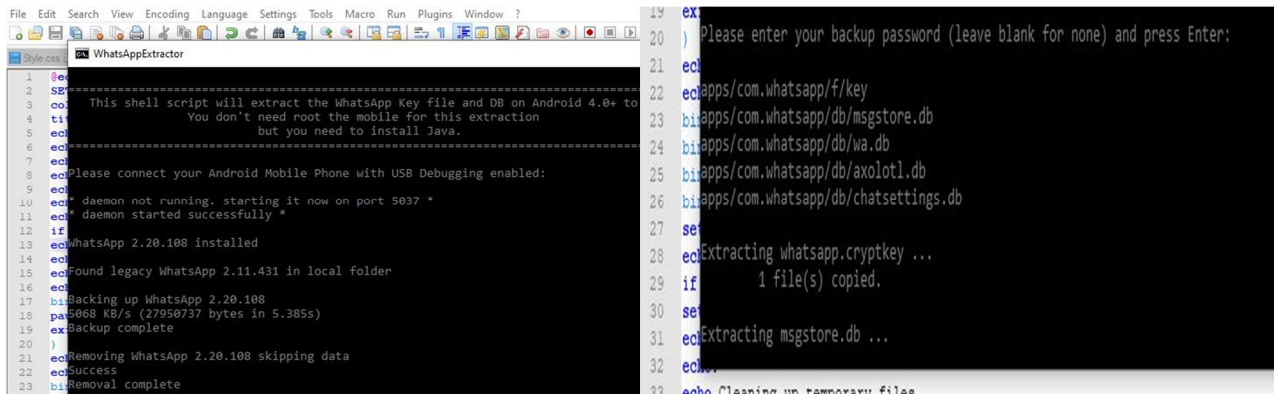
Relative Segment 1 Path: Sony D5322 Quick Image.zip
Full Segment 1 Path: C:\Users\Hemanta Laiz\Desktop\MAGNET FILES\Android Image - 2019-12-04 01-49-19\Sony D5322 Quick Image.zip
Segment 1 MD5 Hash: 5BC38E5AF82E513845228D433B124341
Segment 1 SHA1 Hash: 3158B4280FF9B6E0DFBADAFC48BB5B20D15FD3

Imaging Start UTC: 2019-12-03 20:19:47
Imaging Start UTC Ticks: 637110011873856547
Imaging End UTC: 2019-12-03 20:37:45
Imaging End UTC Ticks: 637110022657182035

Device Information
Manufacturer: Sony
Product Model: D5322
Operating System Version: 5.1.1
Unique Identifier: YT910S9M4L
Serial Number: YT910S9M4L
  
```

Output-4: Message Digest 5 (MD5) and Secure Hashing Algorithm 1 (SHA1) hashes for all files.

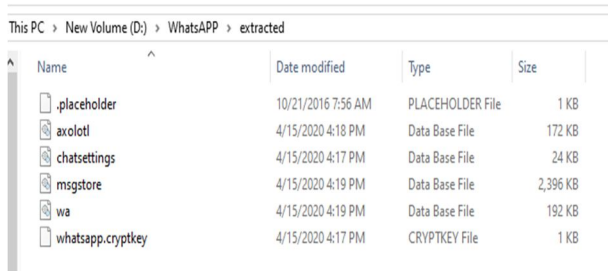
2) **WhatsApp Message/Data Extraction From WhatsApp Database .DB File:** The following framework used to identify the WhatsApp .db database extraction details from the WhatsApp end-to-end encrypted database directly without rooting the android mobile or devices.



```

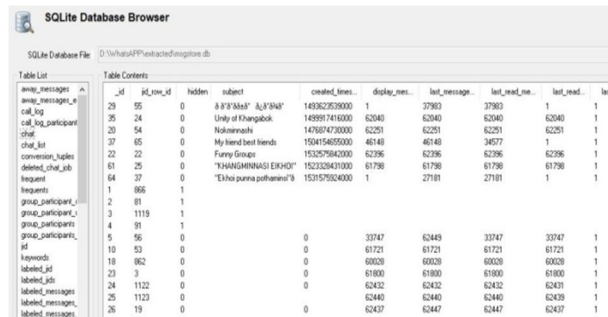
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
WhatsAppExtractor
1 #
2 #
3 =====
4 This shell script will extract the WhatsApp Key file and DB on Android 4.0+ to
5 You don't need root the mobile for this extraction
6 but you need to install Java.
7 =====
8 Please connect your Android Mobile Phone with USB Debugging enabled:
9
10 daemon not running, starting it now on port 5037 *
11 daemon started successfully *
12
13 if
14 WhatsApp 2.20.108 installed
15
16 Found legacy WhatsApp 2.11.431 in local folder
17
18 Backing up WhatsApp 2.20.108
19 5068 KB/s (27950737 bytes in 5.385s)
20 Backup complete
21
22 Removing WhatsApp 2.20.108 skipping data
23 Success
24 Removal complete
25
26 Please enter your backup password (leave blank for none) and press Enter:
27
28 apps/com.whatsapp/f/key
29
30 apps/com.whatsapp/db/msgstore.db
31
32 apps/com.whatsapp/db/wa.db
33
34 apps/com.whatsapp/db/axolotl.db
35
36 apps/com.whatsapp/db/chatsettings.db
37
38
39 Extracting whatsapp.cryptkey ...
40
41 1 file(s) copied.
42
43 Extracting msgstore.db ...
44
45 Cleaning up temporary files
  
```

Fig-24: WhatsApp .db database back-up and extraction process



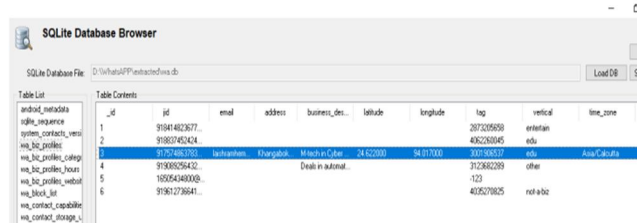
Name	Date modified	Type	Size
.placeholder	10/21/2016 7:56 AM	PLACEHOLDER File	1 KB
axolotl	4/15/2020 4:18 PM	Data Base File	172 KB
chatsettings	4/15/2020 4:17 PM	Data Base File	24 KB
msgstore	4/15/2020 4:19 PM	Data Base File	2,396 KB
wa	4/15/2020 4:19 PM	Data Base File	192 KB
whatsapp.cryptkey	4/15/2020 4:17 PM	CRYPTKEY File	1 KB

Fig-25: .db WhatsApp database Backup from Android Mobile



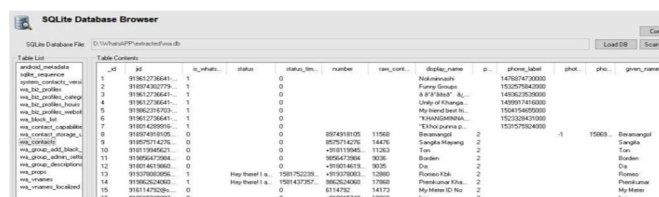
msg_id	jd_new_id	hidden	subject	created_timestamp	display_name	last_message_timestamp	last_read_timestamp	last_read
29	52	0	À 8'3'38h" ÀÙ'3'38h"	14932252000	1	3780	3780	1
35	24	0	Unly of Khargobok	14999741600	62040	62040	62040	1
20	54	0	Nakannashi	14788747000	62251	62251	62251	1
37	85	0	My Item Best Items	150415465000	61468	61468	34577	1
22	22	0	Funny Group	152297642000	62286	62286	62286	1
61	25	0	"KHANGANNASHI EKHO"	152328431000	61798	61798	61798	1
64	37	0	"Ekhoo punna pothannu"ð	153157934000	1	27181	27181	1

Fig-26: Shows the messages/chat history details from .db file



android_metadata	id	jd	email	address	business_desc	latitude	longitude	log	vertical	time_zone
1	919814023677							387209596	eretan	
2	919837462424							436263045	edu	Asia/Calcutta
3	919837462424							436263045	edu	Asia/Calcutta

Fig-27: WhatsApp Profile details for receiver contact



android_metadata	id	jd	status	status_timestamp	number	name_contact	display_name	photo	photo_timestamp	photo_name
1	919812736641		1	0	8074919105	11968	Bannaganj	14762742000		13908
2	919814023677		0	0	8076714276	14476	Sangha Mahang	2		
3	919812736641		0	0	4919119465	9026	Tan	2		
4	919812736641		0	0	8096472864	9026	Bardhan	2		
5	919812736641		0	0	4919119465	9026	Dia	2		
6	919812736641		0	0	4919119465	9026	Phonoo Kiba	2		
7	919814209956		0	0	8074919105	11968	Phonoo Kiba	2		
8	919814209956		0	0	8076714276	14476	Phonoo Kiba	2		
9	919814209956		0	0	4919119465	9026	Phonoo Kiba	2		
10	919814209956		0	0	8096472864	9026	Phonoo Kiba	2		
11	919814209956		0	0	8096472864	9026	Phonoo Kiba	2		
12	919814209956		0	0	4919119465	9026	Phonoo Kiba	2		
13	919814209956		0	0	8096472864	9026	Phonoo Kiba	2		
14	919814209956		0	0	8096472864	9026	Phonoo Kiba	2		
15	919814209956		0	0	8096472864	9026	Phonoo Kiba	2		
16	919814209956		0	0	8096472864	9026	Phonoo Kiba	2		

Fig-28: Whatsapp contact details with name, live status

V. RESULT AND DISCUSSION

This mechanism or tool was to figure out for different factors using open source & paid versions of Android forensic tools as the extraction source. This Open-Source tool gives different digital evidence as follows:

Table 4.5 Feature & Evidence Extracted

FEATURE	MAGNET ACQUIRE TOOL	AF LOGICAL
Root Needed?	Yes/No	No
Physical Extraction	Yes	No
Call log	Yes	Yes
Contacts	Yes	Yes
MMS	Yes	Yes
MMS Parts	Yes	Yes
SMS	Yes	Yes
Partition list Extraction	Yes	No
Application Data	Yes	No
Downloaded Data	Yes	No
SD Card Data	Yes	No
Hangout Messages	Yes	No
Facebook Data	Yes	No
Whatsapp Data	Yes	No
Voice Recording	Yes	No
Creating Image	Yes	No
Pictures	Yes	No
Documents	Yes	No
Video	Yes	No
Timeline Details	Yes	No

During this period of research, the authors were uncovered countless observations regarding mobile device forensic investigation. Therefore, the framework is largely beneficial and many of the agenda explained by the authors can be expected with the use of other mobile phones and handheld devices. The authors are expecting that the framework can be used for other fields also because the implementation is easy to draw out and can be applied to other handheld devices.

VI. FUTURE WORK

In future work, a study will be considered to compare the proposed tool for logical acquisition, physical acquisition, and analysis of data with other commercial and manual tools to get the best result for investigation. Also, we will use the technique of AFLogical OSE and Magnet Acquire to retrieve a handprint from an android mobile device. To obtain the data from the broken Android device, as shown in fig-34 and 35, we recommend using hardware or software tools to access this mobile.

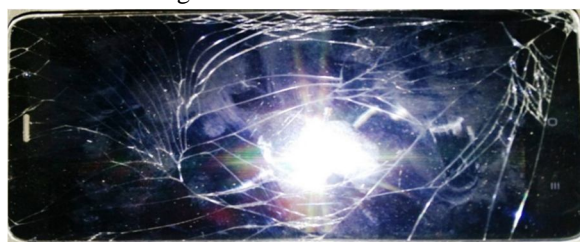


Fig-34: Broken Android Mobile: Xiaomi Note 3



Fig-25: Android Mobile-LeeCo Le Max 2

Finally, future research should address discovering how often the WhatsApp log file overwrites data, and whether any previous timestamps are purged when this takes place. It should also consider repopulating data on a few of the WhatsApp client environments that did not produce as many artifacts as the other environments (i.e., cached profile pictures, timestamps for text messages and media sent). Discovering the encrypted data from WhatsApp databases and allowing, decrypting the databases for investigation. This would be helpful as it could give investigators an estimate of how far back in time the log file has stored information and provide access to the .db files. It is recommended to develop a larger data population story where more messages and media is sent from the WhatsApp client. This will ensure more time will be spent interacting with the clients, potentially leading to the client saving more information on the log file and caching more profile pictures. Using other digital forensic tools, either open-source or commercial, should also be considered for future work to compare data found throughout the different WhatsApp clients.

VII. CONCLUSION

Doing these acquisitions and analysis technical methods by Open Source tools was challenges, so doing these tasks by the commercial tool; it will save time and will outcome accurate results. It is important to understand the Android Software Stack architecture, forensic process, and tools before data extraction and recovery of vital data and artifacts. This paper presents the design of the Android platform to choose the appropriate tools for manual, logical and physical acquisition, as well as data analysis from Android mobile and its social media apps. We used a technique to retrieve evidence from items in the file system for both damaged and undamaged android devices in crime settings. There is also a need to use commercial methods for the analysis of Android devices' data. We propose two methods by AccessData FTK Imager, namely, dd Image Evidence Tree and Image mounting, with mobile data extraction with Magnet Acquire as well as File Carving in Autopsy using a Santoku Linux Virtual Machine for analyzing data. As forensic evidence, forensic investigators can retrieve fast acquisition of data from an Android device that requires a USB cable to attach it to a computer.

It also provides the documentation and reporting of digital data evidence for investigations. Moreover, there is advice for authors that arose from this work:

- A. Best way to retrieve WhatsApp data from Android mobile phone (i.e, WhatsApp .db files).
- B. To avoid permanent data loss, use data recovery software and we will use this logic to obtain digital evidence data from a broken or normal Android mobile phone for further investigation. The research will be performed to compare the proposed tool for logical acquisition and analysis of data with other commercial and manual tools to achieve the best results in an investigation.
- C. The analysis of WhatsApp End-to-End encrypted data from WhatsApp databases provided the information by decrypting the databases (.db file) for investigation. This would be helpful as it could give investigators an estimate of how far back in time the log file has stored information and provide access to the .db files. The analysis of the WhatsApp clients revealed the presence of several artifacts of value for digital forensics investigators. The main source of artifacts is the WhatsApp log file, present throughout all WhatsApp clients. Within this log file, different data can be found, such as timestamps of user actions, mobile client device information, and browser user agent information. Moreover, an investigator can recover the WhatsApp desktop application's run date/time/count by inspecting the prefetch files. By recognizing the respective browser's history file, the web.whatsapp.com accessed URL date/time/count can also be located.



REFERENCES

- [1] <https://www.xda-developers.com/root/>
- [2] https://www.researchgate.net/publication/332093270_WEB_BROWSER_FORENSICS_Evidence_collection_And_Analysis_for_Most_Popular_Web_Browsers_usage_in_Windows_10
- [3] https://www.researchgate.net/publication/321534636_WEB_BROWSER_FORENSICS_GOOGLE_CHROME
- [4] Akbal, E., Günes, F., & Akbal, A. (2016). Digital forensic analyses of web browser records. *Journal of Software (JSW)*, 11(7), 631-637.
- [5] Developers. "Get the Google USB Driver." Internet: www.developer.android.com/425studio/run/winusb.html, 2016.
- [6] WhatsApp. (n.d.). WhatsApp legal info. Retrieved from <https://www.whatsapp.com/legal?eea=1#privacy-policy-information-we-collect>
- [7] S. Tahiri. "Android Forensic Logical Acquisition." Internet: www.resources.infosecinstitute.com/android-forensic-logical-acquisition, 2016.
- [8] WhatsApp. (2016, February). WhatsApp support for mobile devices. Retrieved from <https://blog.whatsapp.com/10000617/WhatsApp-support-for-mobile-devices>



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)