Report on

Android Device Forensic

Using

FINALMobile Forensics4 Tool

Subject: Digital Forensics (CAP921)

Date: 21/04/2020

Submitted by: Laxmi Narayan Vaishnav

Registration Number: 11706559

Email: lnvaishnavwhh@gmail.com

Submitted to: Dr Ajay Shriram Kushwaha,

Assistant Professor, LPU

Email: kushwaha.ajay22@gmail.com

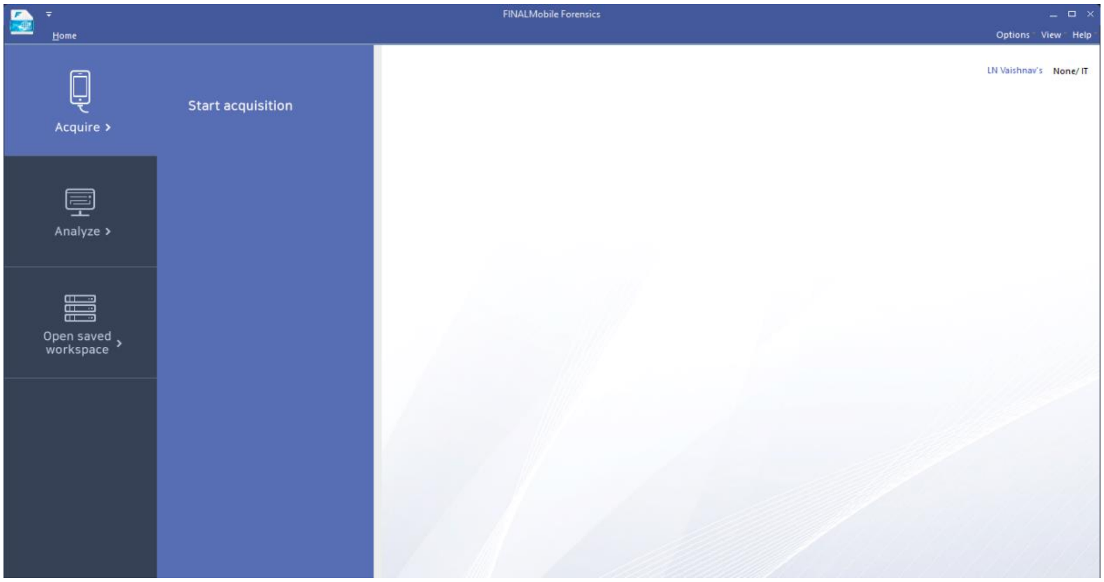
CONTENTS OF THE REPORT

Acknowledgement & Objective

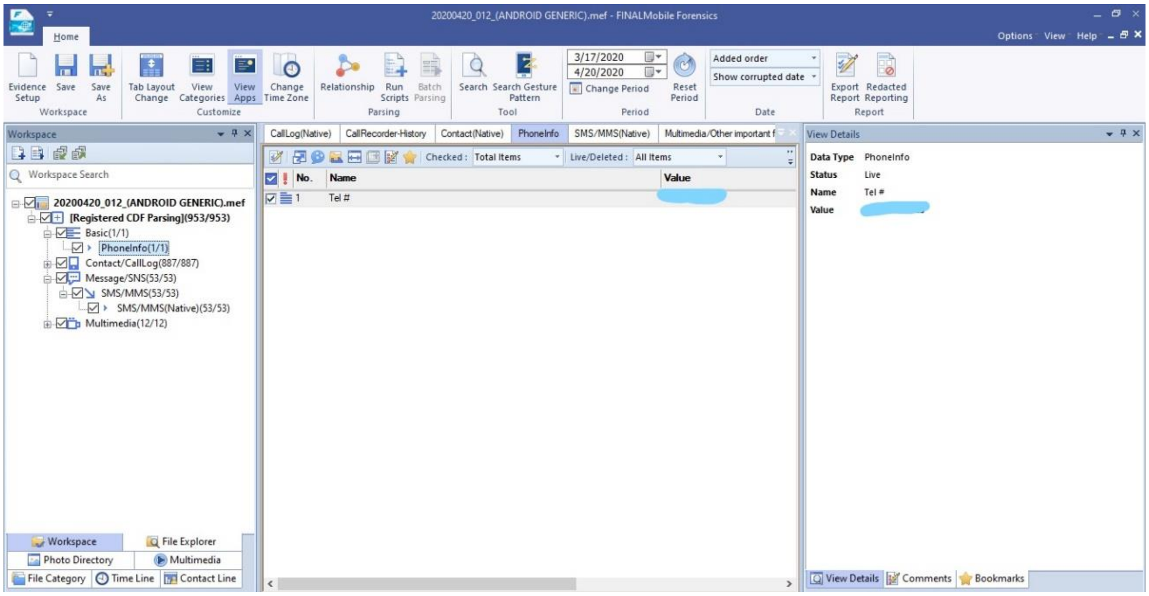
I especially want to say thanks to Ajay sir who encouraged me to learn this tool and how perfectly perform the Android forensic. This forensic operation was wonderful and I learned many things that how the mentioned tool targets the mobile device and how mobile device reacts when it loses its control over the software. I also learned many different tools which also help in various type of forensics operations.

The main objective of this forensic is to understand how the mobile device’s hidden data can be used to perform a forensic analysis. The software helps a lot in the criminal cases where forensic team catches the suspected mobile device and then performs the mobile forensic operation to know all the information of the data which is lost or currently stored in the mobile device. It also helps to know the various activities of the suspected person which may be connected with the activity of the crime.

1. OVERVIEW OF THE SOFTWARE



- This is the home windows of the **FINALMobile Forensics4** tool. Here, we’ve to choose the desire option for further process whether you want to perform initial mobile forensic or analyze the previous performed forensic data.



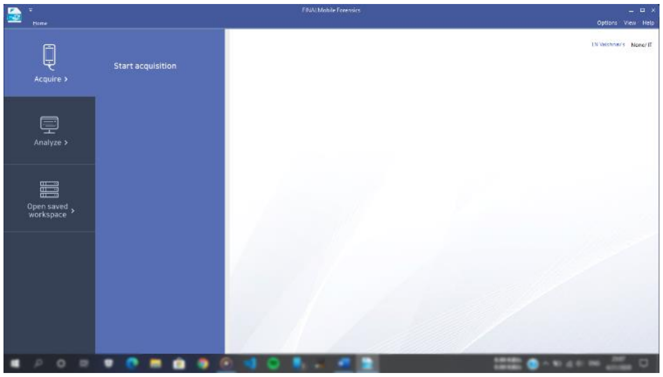
No.	Name	Value
1	Tel #	[redacted]

Data Type PhoneInfo
Status Live
Name Tel #
Value [redacted]

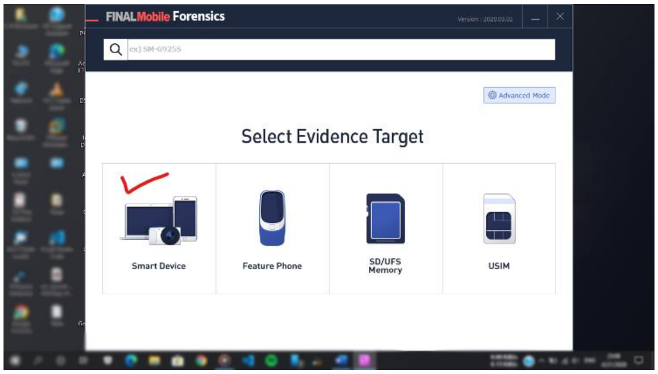
- Here, the analysis part takes the place and the examiner performs the further operations for getting results.

2. ACQUIRING THE DATA FROM THE MOBILE DEVICE

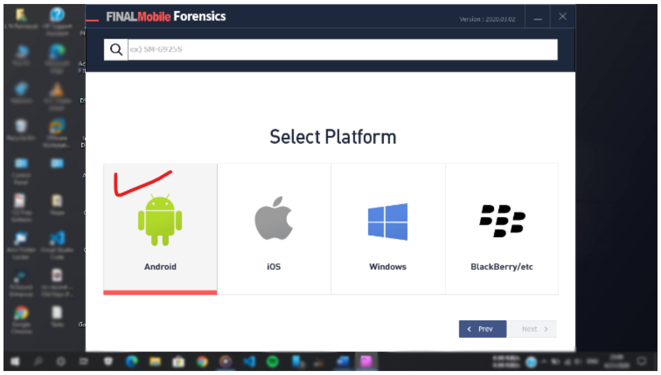
For performing this process, we need to choose to **acquire** option in this forensic tool.



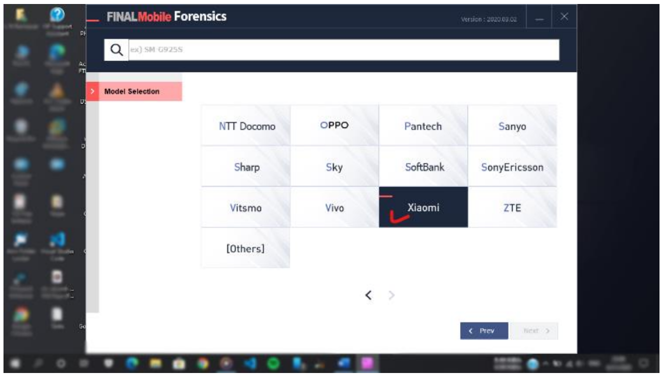
1. Now, select the type of your device.



2. Now, select the platform of your device.



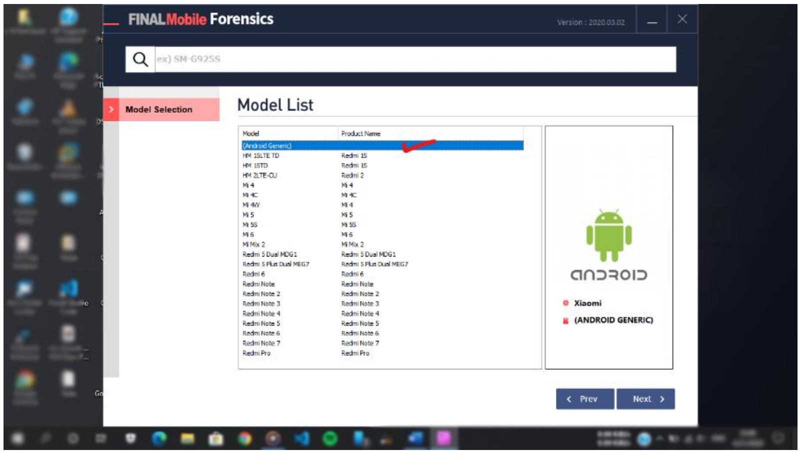
3. Now, select the company of your device.



NTT Docomo	OPPO	Pantech	Sanyo
Sharp	Sky	SoftBank	SonyEricsson
Vitsmo	Vivo	Xiaomi	ZTE
[Others]			

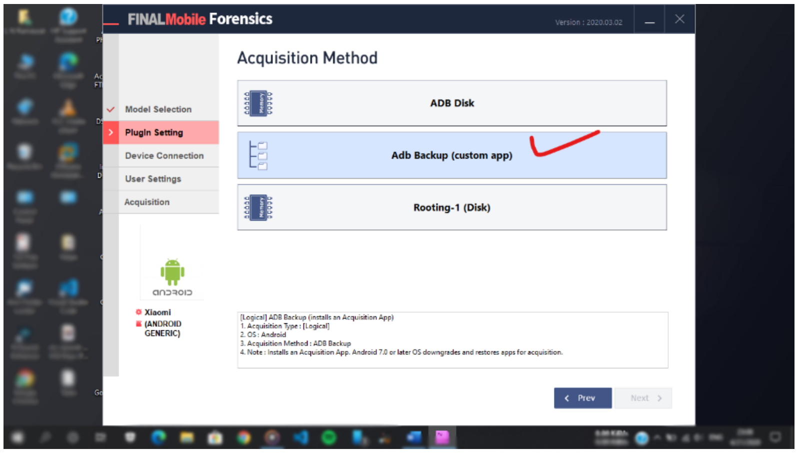
4. Now, select the model name of your device.

   NOTE: If your model is not listed then select the '**Android Generic**'.



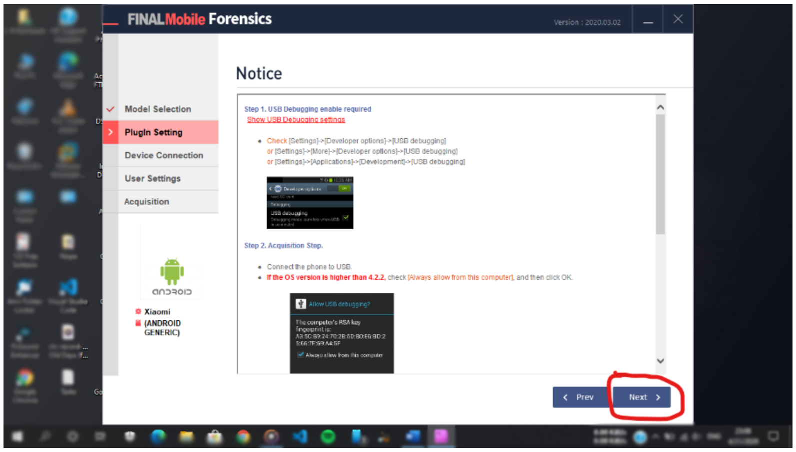
Model	Product Name
(Android Generic)	
HM 1SLTE TD	Redmi 1S
HM 1STD	Redmi 1S
HM 2LTE-CU	Redmi 2
Mi 4	Mi 4
MI 4C	MI 4C
MI 4W	Mi 4
Mi 5	Mi 5
Mi 5S	Mi 5S
MI 6	MI 6
Mi Mix 2	Mi Mix 2
Redmi 5 Dual MDG1	Redmi 5 Dual MDG1
Redmi 5 Plus Dual MEG7	Redmi 5 Plus Dual MEG7
Redmi 6	Redmi 6
Redmi Note	Redmi Note
Redmi Note 2	Redmi Note 2
Redmi Note 3	Redmi Note 3
Redmi Note 4	Redmi Note 4
Redmi Note 5	Redmi Note 5
Redmi Note 6	Redmi Note 6
Redmi Note 7	Redmi Note 7
Redmi Pro	Redmi Pro

5. Now, select the any acquisition method you wish for.
   I choose **ADB Backup (custom app)** method.



[Logical] ADB Backup (installs an Acquisition App)
1. Acquisition Type : [Logical]
2. OS : Android
3. Acquisition Method : ADB Backup
4. Note : Installs an Acquisition App. Android 7.0 or later OS downgrades and restores apps for acquisition.

6. Now, this method requires **USB debugging** enabled. If the acquisition method is,



Step 1. USB Debugging enable required
Show USB Debugging settings

- Check [Settings]->[Developer options]->[USB debugging]
  or [Settings]->[More]->[Developer options]->[USB debugging]
  or [Settings]->[Applications]->[Development]->[USB debugging]

Step 2. Acquisition Step.

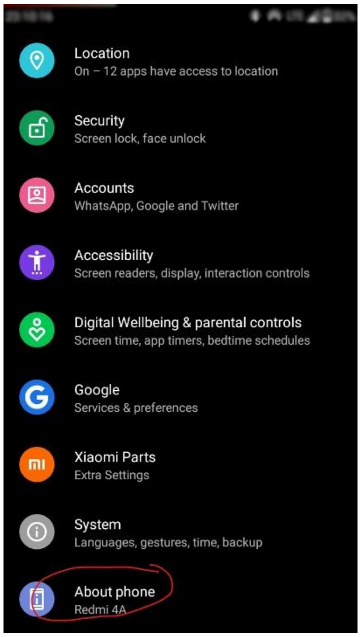
- Connect the phone to USB.
- If the OS version is higher than 4.2.2, check [Always allow from this computer], and then click OK.

The computer's RSA key fingerprint is:
A3:5C:B9:24:70:2B:5D:B0:E6:BD:2
5:66:7F:59:A4:5F

- **ADB Disk** or **ADB Backup (custom app)** then only **USB debugging** option should be enabled in the mobile.
- **Rooting-1 (Disk)** then **Root Android debugging** option must be enabled in the mobile.

2.a Steps to enable USB debugging in Android device

- ➢ Open **settings** of the device.
- ➢ Now, tap on **About Phone.**



Location
On – 12 apps have access to location

Security
Screen lock, face unlock

Accounts
WhatsApp, Google and Twitter

Accessibility
Screen readers, display, interaction controls

Digital Wellbeing & parental controls
Screen time, app timers, bedtime schedules

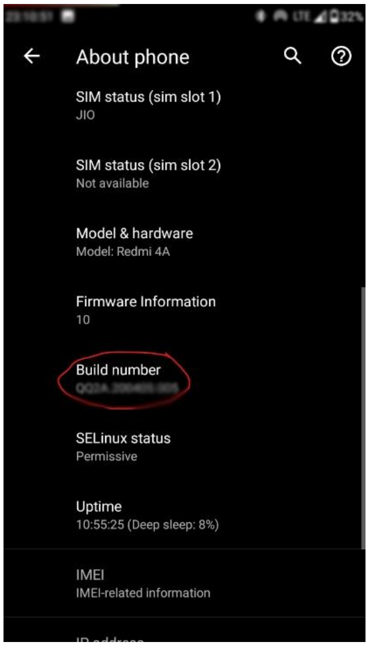
Google
Services & preferences

Xiaomi Parts
Extra Settings

System
Languages, gestures, time, backup

About phone
Redmi 4A

- ➢ Now, continuously tap until a pop-up says, '**Developer Options**' enabled



About phone

SIM status (sim slot 1)
JIO

SIM status (sim slot 2)
Not available

Model & hardware
Model: Redmi 4A

Firmware Information
10

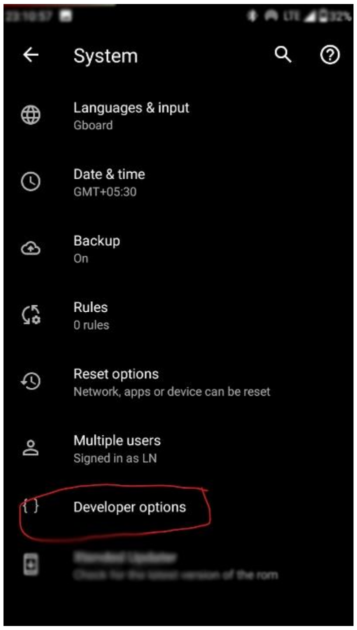
Build number
[redacted]

SELinux status
Permissive

Uptime
10:55:25 (Deep sleep: 8%)

IMEI
IMEI-related information

- ➢ Now, tap on **System**> **Developer Options**



System

Languages & input
Gboard

Date & time
GMT+05:30

Backup
On

Rules
0 rules

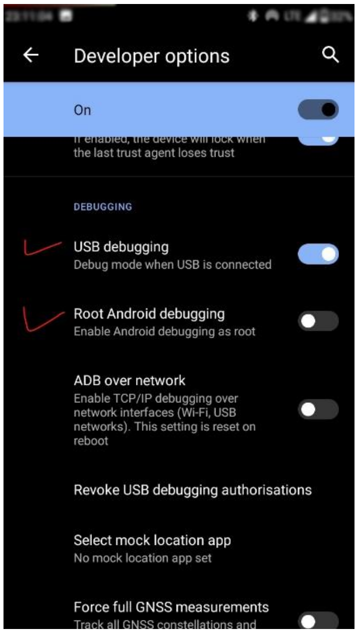
Reset options
Network, apps or device can be reset

Multiple users
Signed in as LN

Developer options

[redacted]

- ➢ Now, tap on **USB debugging**.



Developer options

On

If enabled, the device will lock when
the last trust agent loses trust

DEBUGGING

USB debugging
Debug mode when USB is connected

Root Android debugging
Enable Android debugging as root

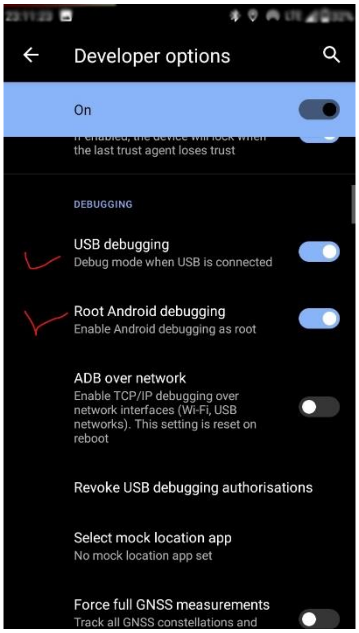
ADB over network
Enable TCP/IP debugging over network interfaces (Wi-Fi, USB networks). This setting is reset on reboot

Revoke USB debugging authorisations

Select mock location app
No mock location app set

Force full GNSS measurements
Track all GNSS constellations and

- ➢ For **Rooting-1 (Disk),** turn on **Root Android debugging**



Developer options

On

If enabled, the device will lock when
the last trust agent loses trust

DEBUGGING

USB debugging
Debug mode when USB is connected

Root Android debugging
Enable Android debugging as root

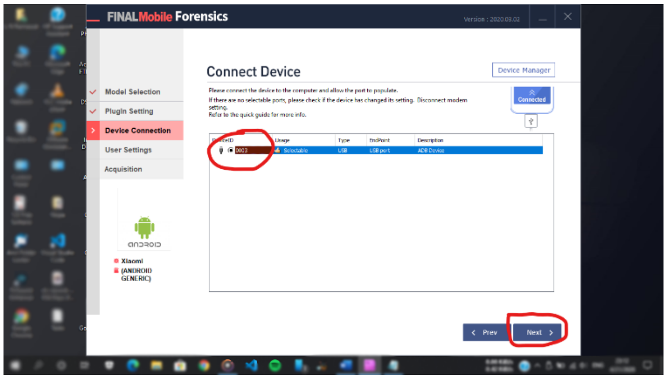
ADB over network
Enable TCP/IP debugging over network interfaces (Wi-Fi, USB networks). This setting is reset on reboot

Revoke USB debugging authorisations

Select mock location app
No mock location app set

Force full GNSS measurements
Track all GNSS constellations and

7. After enabling **USB debugging**, plug-in the USB cable which connects the device and PC/Laptop. Now, the Mobile device must be connected with the PC and listed under **Connect Device**, now click on the Next button.

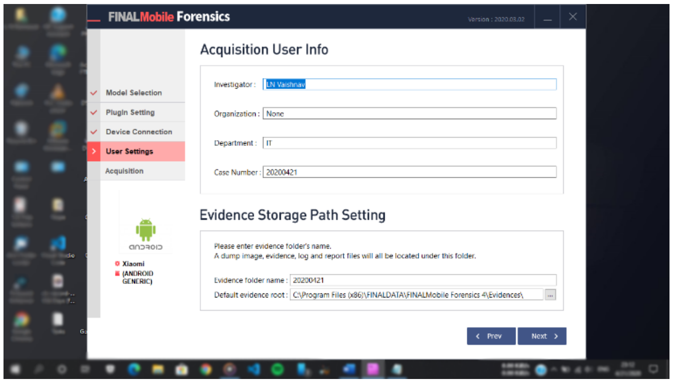


Connect Device

Please connect the device to the computer and allow the port to populate.
If there are no selectable ports, please check if the device has changed its setting. Disconnect modem setting.
Refer to the quick guide for more info.

DeviceID	Usage	Type	EndPoint	Description
[redacted]	Selectable	USB	USB port	ADB Device

8. Now, a next step will ask you to fill-up acquisition user info & path for storing the data. Fill the details and give a path or leave it on the **default** path.



Acquisition User Info

Investigator : LN Vaishnav

Organization : None

Department : IT

Case Number : 20200421

Evidence Storage Path Setting

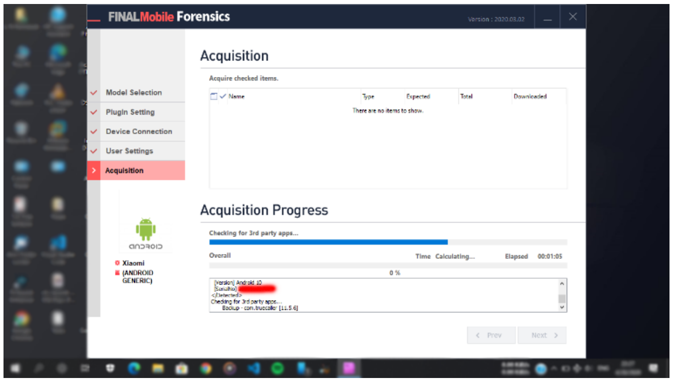
Please enter evidence folder's name.
A dump image, evidence, log and report files will all be located under this folder.

Evidence folder name : 20200421

Default evidence root : C:\Program Files (x86)\FINALDATA\FINALMobile Forensics 4\Evidences\

9. Now, the acquisition will be started.

NOTE: After sometimes, it will ask for **Mobile Desktop Password** and you've to give a password & must remember it.



Acquisition

Acquire checked items.

Name	Type	Expected	Total	Downloaded

There are no items to show.

Acquisition Progress

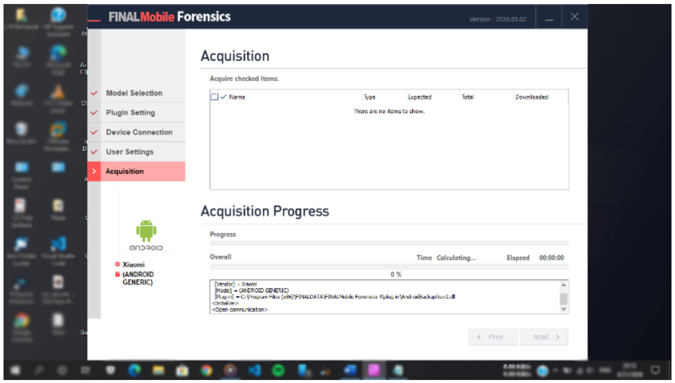
Checking for 3rd party apps...

Overall Time Calculating... Elapsed 00:01:05

0 %

```
[Version] Android 10
[SerialNo] [redacted]
</Detected>
Checking for 3rd party apps...
    Backup - com.truecaller [11.5.6]
```

NOTE: This process will take some time. 😊



Acquisition

Acquire checked items.

Name	Type	Expected	Total	Downloaded

There are no items to show.

Acquisition Progress

Progress

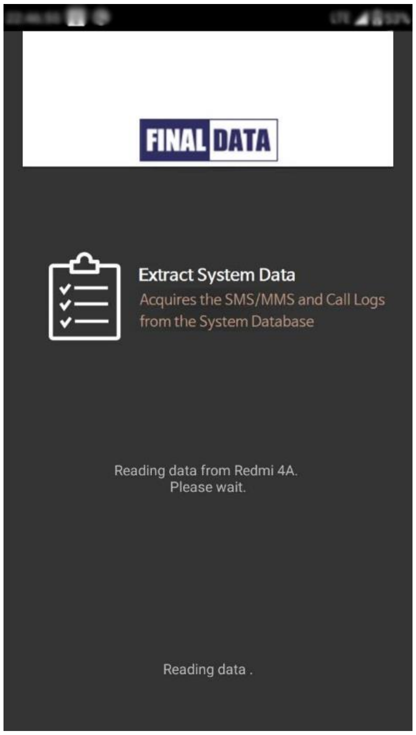
Overall Time Calculating... Elapsed 00:00:00

0 %

```
 [Vendor] = Xiaomi
 [Model] = (ANDROID GENERIC)
 [Plug-in] = C:\Program Files (x86)\FINALDATA\FINALMobile Forensics 4\plug-in\AndroidBackupRev2.dll
<Initialize>
<Open communication>
```

10. Go to your Android device and follow instructions. This tool will ask to install its APK file in the Mobile device for taking the data.

- ➢ Help the APK to be installed and give every permission which it asks.
- ➢ Now, enter the **Desktop Backup Password**.



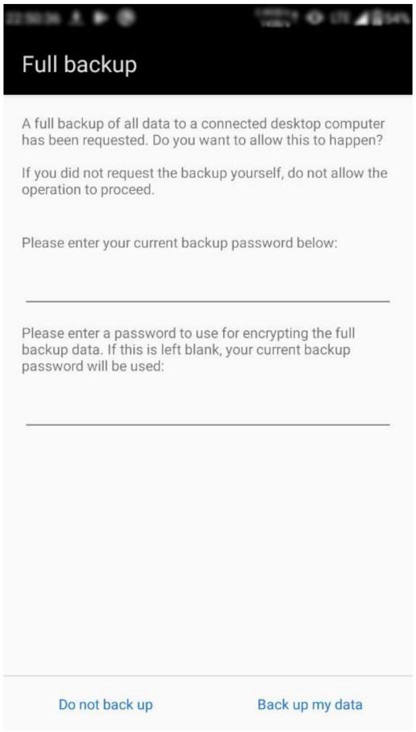
FINAL DATA

Extract System Data

Acquires the SMS/MMS and Call Logs from the System Database

Reading data from Redmi 4A.
Please wait.

Reading data .



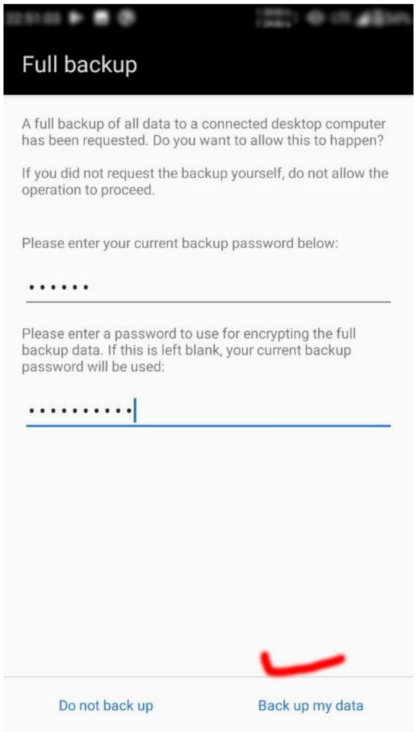
Full backup

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.

Please enter your current backup password below:

Please enter a password to use for encrypting the full backup data. If this is left blank, your current backup password will be used:



Full backup

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.

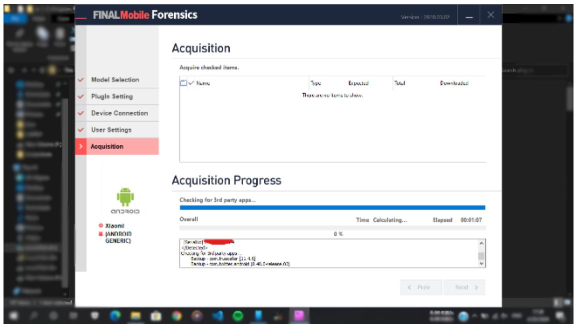
Please enter your current backup password below:

••••••

Please enter a password to use for encrypting the full backup data. If this is left blank, your current backup password will be used:

••••••••••

11. Now, the tool will check all 3rd party apps which are installed in the mobile.



Acquisition

Acquire checked items.

Name	Type	Expected	Total	Downloaded

There are no items to show.

Acquisition Progress

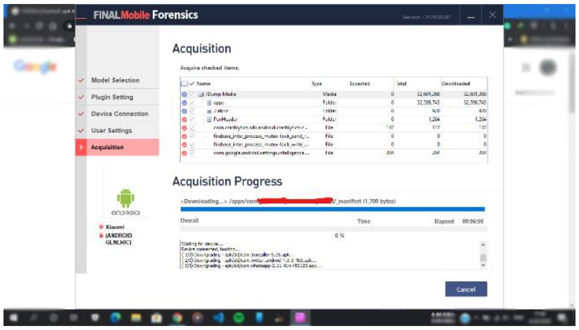
Checking for 3rd party apps...

Overall Time Calculating... Elapsed 00:01:07

0 %

```
[Serial No] [redacted]
</Detected>
Checking for 3rd party apps...
    Backup - com.truecaller [11.4.6]
    Backup - com.twitter.android [8.40.0-release.02]
```

12. Now, it will downgrade the apps.



Acquisition

Acquire checked items.

Name	Type	Expected	Total	Downloaded
/Dump Media	Media	0	32,601,268	32,601,268
apps	Folder	0	32,598,743	32,598,743
/share	Folder	0	920	920
PurHeader	Folder	0	1,264	1,264
com.crashlytics.sdk.android.crashlytics-c...	File	137	137	137
firebase_inter_process_mutex-lock_send_t...	File	0	0	0
firebase_inter_process_mutex-lock_write_...	File	0	0	0
com.google.android.settings.intelligence...	File	204	204	204

Acquisition Progress

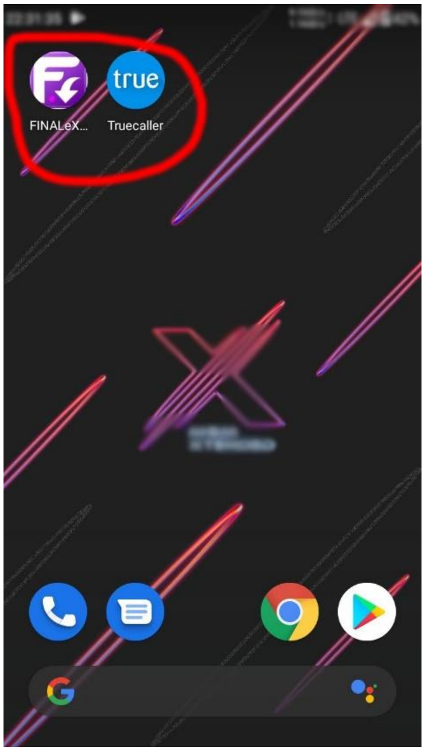
<Downloading...> /apps/com[redacted]/_manifest (1,700 bytes)

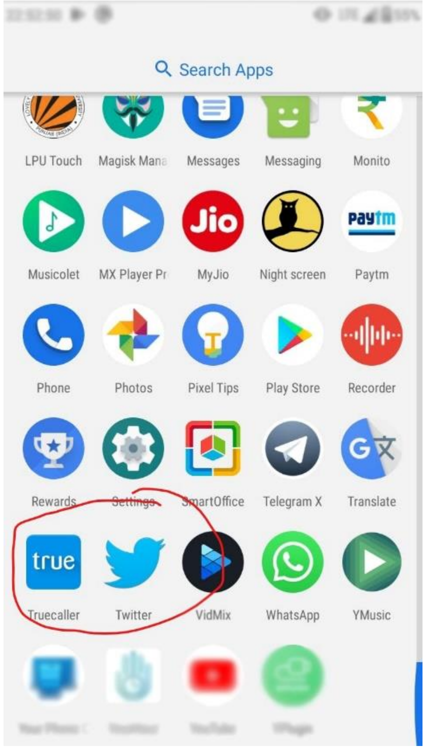
Overall Time Elapsed 00:06:50

0 %

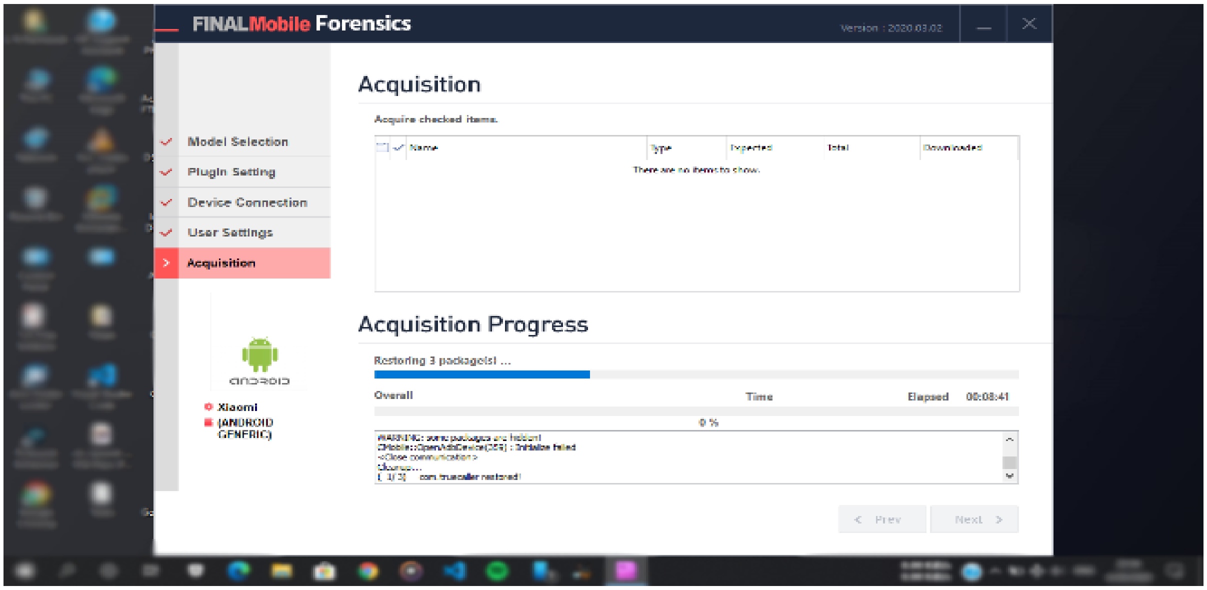
```
Waiting for device...
Device connected, booting...
(1/3) Downgrading - apk/old/com.truecaller-5.35.apk...
(2/3) Downgrading - apk/old/com.twitter.android-7.0.3-705.apk...
(3/3) Downgrading - apk/old/com.whatsapp-2.11.414-450123.apk...
```

During down-gradation & restoring, the apps go in their old versions.





13. Now, it will restore all the downgraded apps and will do normally the mobile device.



Acquisition

Acquire checked items.

There are no items to show.

Acquisition Progress

Restoring 3 package(s) ...

Overall Time Elapsed 00:08:41

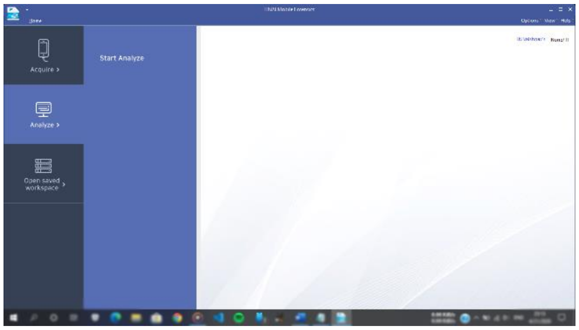
0 %

```
WARNING: some packages are hidden!
CMobile::OpenAdbDevice(355) : Initialize failed
<Close communication>
Cleanup...
[ 1/ 3]    com.truecaller restored!
```

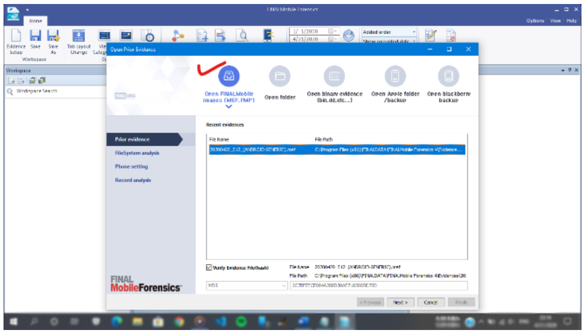
14. The process of data gathering for mobile forensic is completed.

3. ANALYZING THE ACQUIRED DATA

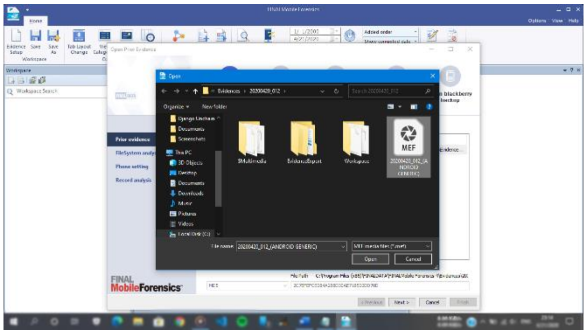
For performing the analysis part of the acquired data, we need to select the **ANALYZE** option from the mentioned forensic tool.



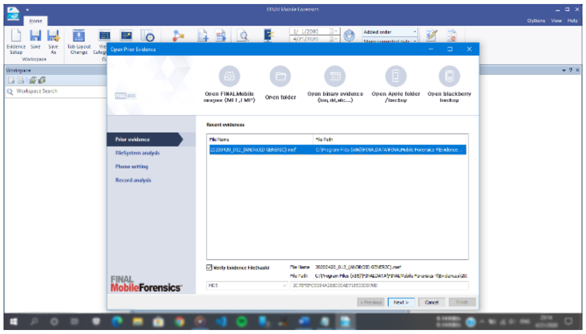
1. After selecting the Analyze option, a new window will open where we've to open previously acquired data (.MEF or .FMP format).



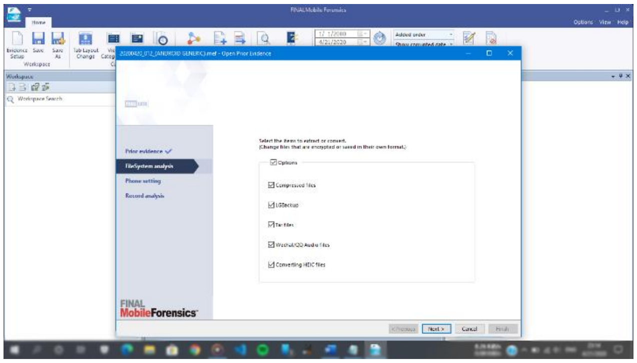
2. Now, open the source file.



3. Now, select the file and follow the next button.



4. It’s up to you that which files you’re going to analyse.



Select the items to extract or convert.
(Change files that are encrypted or saved in their own format.)

☑ Options

☑ Compressed files

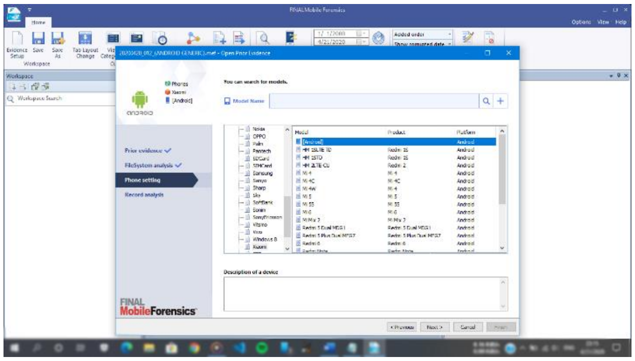
☑ LGBackup

☑ Tar files

☑ Wechat/QQ Audio files

☑ Converting HEIC files

5. Now, honestly select which model you’ve selected previously.

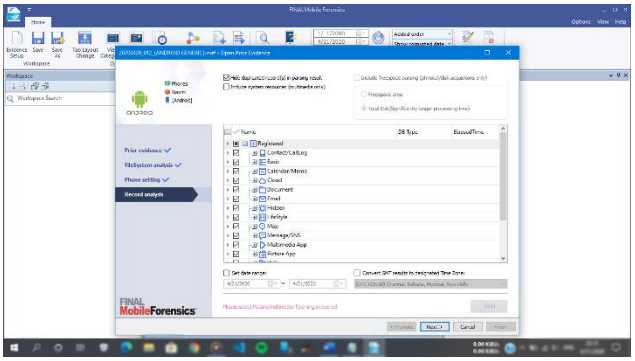


You can search for models.

Phones / Xiaomi / [Android]

Model	Product	Platform
[Android]		Android
HM 1SLTE TD	Redmi 1S	Android
HM 1STD	Redmi 1S	Android
HM 2LTE-CU	Redmi 2	Android
Mi 4	Mi 4	Android
Mi 4C	Mi 4C	Android
Mi 4W	Mi 4	Android
Mi 5	Mi 5	Android
Mi 5S	Mi 5S	Android
Mi 6	Mi 6	Android
Mi Mix 2	Mi Mix 2	Android
Redmi 5 Dual MDG1	Redmi 5 Dual MDG1	Android
Redmi 5 Plus Dual MEG7	Redmi 5 Plus Dual MEG7	Android
Redmi 6	Redmi 6	Android

6. Now, select which files you want to analyse.



☑ Hide duplicated record(s) in parsing result
☐ Include system resources (multimedia only)

☐ Include freespace parsing (physical/disk acquisitions only)
○ Freespace area
● Total Disk(Significantly longer processing time)

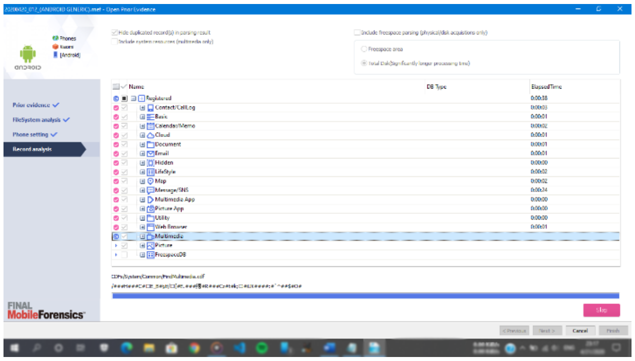
Name	DB Type	ElapsedTime
■ Registered		
☑ Contact/CallLog		
☑ Basic		
☑ Calendar/Memo		
☑ Cloud		
☑ Document		
☑ Email		
☑ Hidden		
☑ LifeStyle		
☑ Map		
☑ Message/SNS		
☑ Multimedia App		
☑ Picture App		

☐ Set date range: 4/21/2020 ~ 4/21/2020

☐ Convert GMT results to designated Time Zone: (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi

Please select Picture/multimedia if parsing is desired

7. Now, the tool will start the analysis part and wait until it finishes.



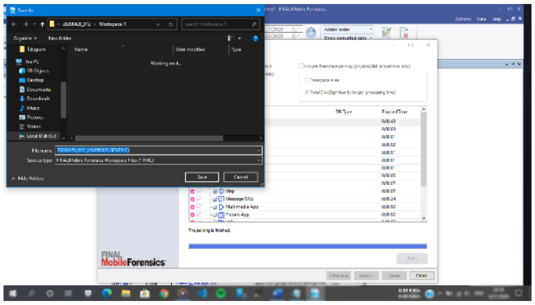
☑ Hide duplicated record(s) in parsing result
☐ Include system resources (multimedia only)

☐ Include freespace parsing (physical/disk acquisitions only)
○ Freespace area
● Total Disk(Significantly longer processing time)

Name	DB Type	ElapsedTime
Registered		0:00:38
Contact/CallLog		0:00:03
Basic		0:00:01
Calendar/Memo		0:00:02
Cloud		0:00:01
Document		0:00:01
Email		0:00:01
Hidden		0:00:00
LifeStyle		0:00:02
Map		0:00:02
Message/SNS		0:00:24
Multimedia App		0:00:00
Picture App		0:00:00
Utility		0:00:00
Web Browser		0:00:01
Multimedia		
Picture		
FreespaceDB		

CDFs/System/Common/FindMultimedia.cdf

8. You can also save this analysis part (Ctrl + S).



Save As

Workspace-1

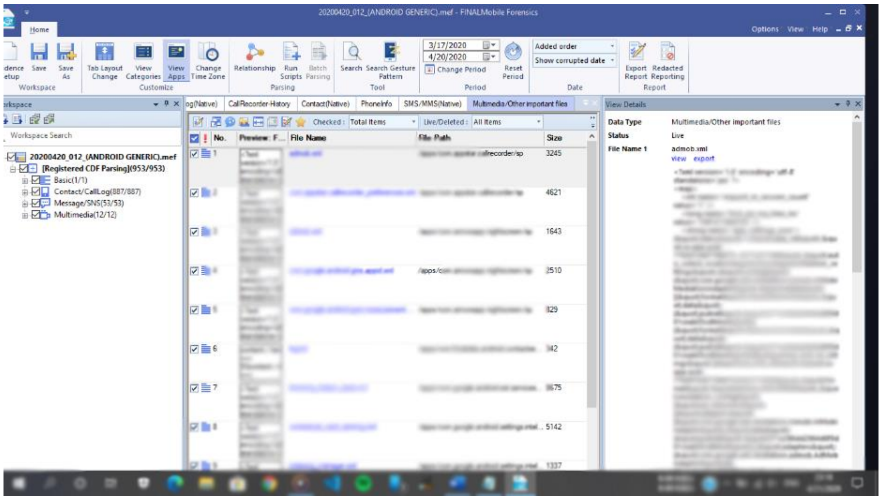
File name: 20200420_012_(ANDROID GENERIC)

Save as type: FINALMobile Forensics Workspace Files (*.FMC)

The parsing is finished.

😊 Let's analysis the Mobile Data 😊

- **Multimedia and other Android data.**



20200420_012_(ANDROID GENERIC).mef - FINALMobile Forensics

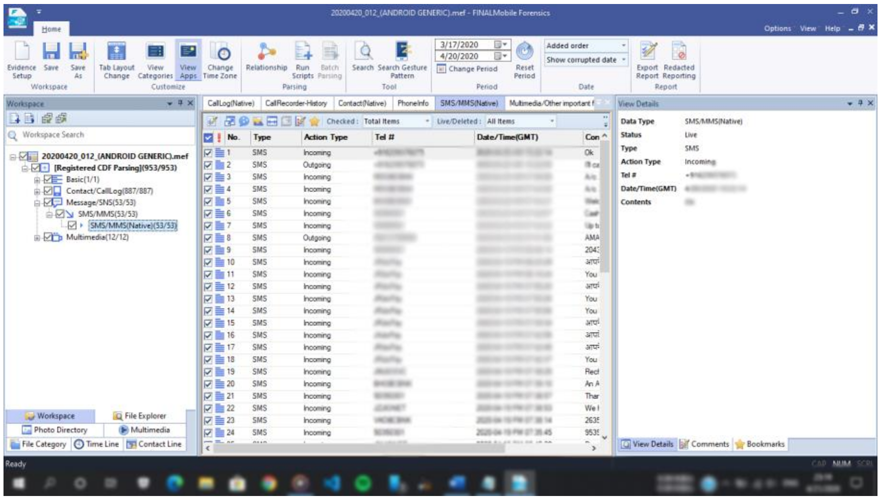
Checked: Total Items ▾ Live/Deleted: All Items ▾

☑	No.	Preview: F...	File Name	File Path	Size
☑	1	[illegible]	[illegible]	[illegible] callrecorder/sp	3245
☑	2	[illegible]	[illegible]	[illegible]	4621
☑	3	[illegible]	[illegible]	[illegible]	1643
☑	4	[illegible]	[illegible]	/apps/com [illegible]	2510
☑	5	[illegible]	[illegible]	[illegible]	329
☑	6	[illegible]	[illegible]	[illegible]	342
☑	7	[illegible]	[illegible]	[illegible]	3675
☑	8	[illegible]	[illegible]	[illegible]	5142
☑	[illegible]	[illegible]	[illegible]	[illegible]	1337

View Details

Data Type	Multimedia/Other important files
Status	Live
File Name 1	admob.xml view export

- **SMS/MMS.**



20200420_012_(ANDROID GENERIC).mef - FINALMobile Forensics

Checked: Total Items ▾ Live/Deleted: All Items ▾

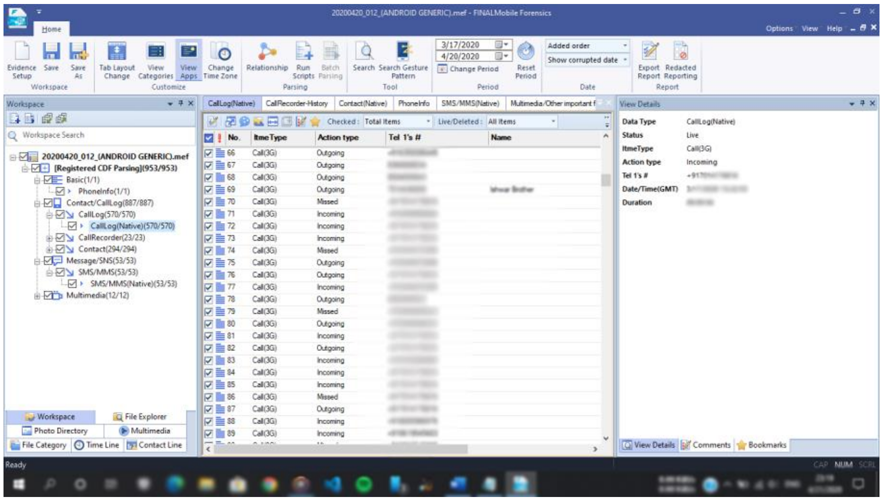
☑	No.	Type	Action Type	Tel #	Date/Time(GMT)	Con
☑	1	SMS	Incoming	[illegible]	[illegible]	Ok
☑	2	SMS	Outgoing	[illegible]	[illegible]	[illegible]
☑	3	SMS	Incoming	[illegible]	[illegible]	A/c
☑	4	SMS	Incoming	[illegible]	[illegible]	A/c
☑	5	SMS	Incoming	[illegible]	[illegible]	[illegible]
☑	6	SMS	Incoming	[illegible]	[illegible]	[illegible]
☑	7	SMS	Incoming	[illegible]	[illegible]	Up t
☑	8	SMS	Outgoing	[illegible]	[illegible]	AMA
☑	9	SMS	Incoming	[illegible]	[illegible]	2043
☑	10	SMS	Incoming	[illegible]	[illegible]	आप
☑	11	SMS	Incoming	[illegible]	[illegible]	You
☑	12	SMS	Incoming	[illegible]	[illegible]	आप
☑	13	SMS	Incoming	[illegible]	[illegible]	You
☑	14	SMS	Incoming	[illegible]	[illegible]	You
☑	15	SMS	Incoming	[illegible]	[illegible]	आप
☑	16	SMS	Incoming	[illegible]	[illegible]	आप
☑	17	SMS	Incoming	[illegible]	[illegible]	आप
☑	18	SMS	Incoming	[illegible]	[illegible]	You
☑	19	SMS	Incoming	[illegible]	[illegible]	Rec
☑	20	SMS	Incoming	[illegible]	[illegible]	An A
☑	21	SMS	Incoming	[illegible]	[illegible]	Thar
☑	22	SMS	Incoming	[illegible]	[illegible]	We
☑	23	SMS	Incoming	[illegible]	2020-04-15 PM 07:38:14	2635
☑	24	SMS	Incoming	[illegible]	2020-04-15 PM 07:35:45	9535

View Details

Data Type	SMS/MMS(Native)
Status	Live
Type	SMS
Action Type	Incoming
Tel #	[illegible]
Date/Time(GMT)	[illegible]
Contents	[illegible]

Ready

- **Call Logs.**



3/17/2020 – 4/20/2020

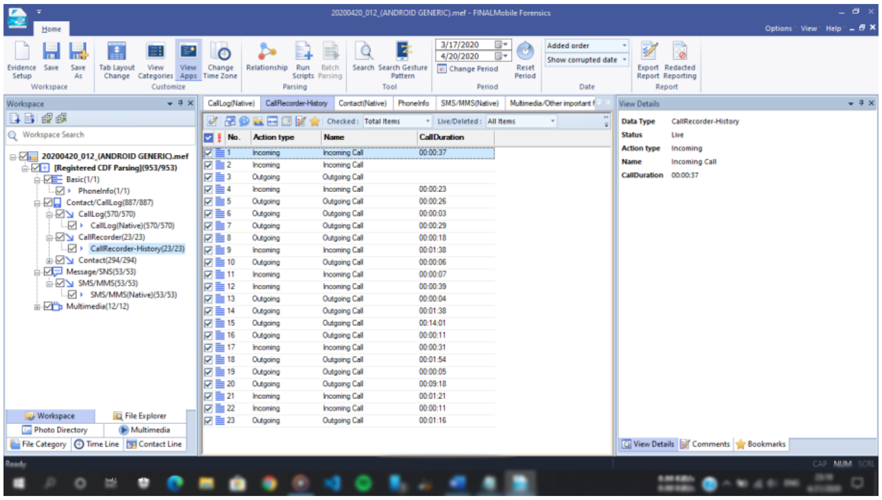
Added order · Show corrupted date

Checked : Total Items · Live/Deleted : All Items

No.	ItmeType	Action type	Tel 1's #	Name
66	Call(3G)	Outgoing	[redacted]	
67	Call(3G)	Outgoing	[redacted]	
68	Call(3G)	Outgoing	[redacted]	
69	Call(3G)	Outgoing	[redacted]	[redacted]
70	Call(3G)	Missed	[redacted]	
71	Call(3G)	Incoming	[redacted]	
72	Call(3G)	Incoming	[redacted]	
73	Call(3G)	Incoming	[redacted]	
74	Call(3G)	Missed	[redacted]	
75	Call(3G)	Outgoing	[redacted]	
76	Call(3G)	Outgoing	[redacted]	
77	Call(3G)	Incoming	[redacted]	
78	Call(3G)	Outgoing	[redacted]	
79	Call(3G)	Missed	[redacted]	
80	Call(3G)	Outgoing	[redacted]	
81	Call(3G)	Incoming	[redacted]	
82	Call(3G)	Outgoing	[redacted]	
83	Call(3G)	Incoming	[redacted]	
84	Call(3G)	Incoming	[redacted]	
85	Call(3G)	Incoming	[redacted]	
86	Call(3G)	Missed	[redacted]	
87	Call(3G)	Outgoing	[redacted]	
88	Call(3G)	Incoming	[redacted]	
89	Call(3G)	Incoming	[redacted]	

Data Type	CallLog(Native)
Status	Live
ItmeType	Call(3G)
Action type	Incoming
Tel 1's #	[redacted]
Date/Time(GMT)	[redacted]
Duration	[redacted]

- **Call-Recorder History.**



3/17/2020 – 4/20/2020

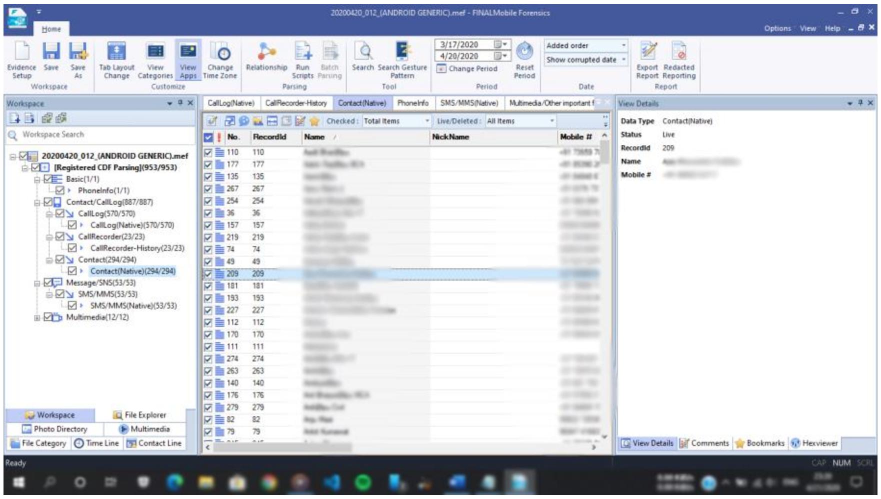
Added order · Show corrupted date

Checked : Total Items · Live/Deleted : All Items

No.	Action type	Name	CallDuration
1	Incoming	Incoming Call	00:00:37
2	Incoming	Incoming Call	
3	Outgoing	Outgoing Call	
4	Incoming	Incoming Call	00:00:23
5	Outgoing	Outgoing Call	00:00:26
6	Outgoing	Outgoing Call	00:00:03
7	Outgoing	Outgoing Call	00:00:29
8	Outgoing	Outgoing Call	00:00:18
9	Incoming	Incoming Call	00:01:38
10	Outgoing	Outgoing Call	00:00:06
11	Incoming	Incoming Call	00:00:07
12	Incoming	Incoming Call	00:00:39
13	Outgoing	Outgoing Call	00:00:04
14	Outgoing	Outgoing Call	00:01:38
15	Outgoing	Outgoing Call	00:14:01
16	Outgoing	Outgoing Call	00:00:11
17	Incoming	Incoming Call	00:00:31
18	Outgoing	Outgoing Call	00:01:54
19	Outgoing	Outgoing Call	00:00:05
20	Outgoing	Outgoing Call	00:09:18
21	Incoming	Incoming Call	00:01:21
22	Incoming	Incoming Call	00:00:11
23	Outgoing	Outgoing Call	00:01:16

Data Type	CallRecorder-History
Status	Live
Action type	Incoming
Name	Incoming Call
CallDuration	00:00:37

- **Contacts.**



3/17/2020 – 4/20/2020

Added order · Show corrupted date

Checked : Total Items · Live/Deleted : All Items

No.	RecordId	Name	NickName	Mobile #
110	110	[redacted]		[redacted]
177	177	[redacted]		[redacted]
135	135	[redacted]		[redacted]
267	267	[redacted]		[redacted]
254	254	[redacted]		[redacted]
36	36	[redacted]		[redacted]
157	157	[redacted]		[redacted]
219	219	[redacted]		[redacted]
74	74	[redacted]		[redacted]
49	49	[redacted]		[redacted]
209	209	[redacted]		[redacted]
181	181	[redacted]		[redacted]
193	193	[redacted]		[redacted]
227	227	[redacted]		[redacted]
112	112	[redacted]		[redacted]
170	170	[redacted]		[redacted]
111	111	[redacted]		
274	274	[redacted]		[redacted]
263	263	[redacted]		[redacted]
140	140	[redacted]		[redacted]
176	176	[redacted]		[redacted]
279	279	[redacted]		[redacted]
82	82	[redacted]		[redacted]
79	79	[redacted]		[redacted]

Data Type	Contact(Native)
Status	Live
RecordId	209
Name	[redacted]
Mobile #	[redacted]

4. Conclusion

This tool helps a lot to analyse the deep of the Mobile Device. It works in three different ways where the examiner has to choose the kind of acquisition.

If the acquisition is the type of,

1. **ADB Disk**, then the type of the acquisition will target the **Physical Disk**. The targeted OS will be the user selected in the earlier step. It will take the data of the physical disk of the mobile and will create an image file for further process of forensic.
2. **ADB Backup (custom app)**, then the type of the acquisition will target the 3rd party installed applications. The targeted OS will be the user selected in the earlier step. This tool will force the mobile device to install an external APK for getting the data. And later, it'll downgrade the apps and after completion of the acquisition process, the mobile device will return in its normal condition.
3. **Rooting-1 (Disk)**, then the type of the acquisition will target the **Physical Disk**. The targeted OS will be the user selected in the earlier step. This acquisition goes into the depth of the mobile and gathers the maximum data as possible. This process takes much time than other type of acquisitions. In the result, it creates an image file for further analysis of forensic.

In the analysis part, we have to select the acquisition file and go on for on for further processes. This process takes less time than acquisition part and, in the result, gives the confidential information. We can sort the resulted data in the different ways for a better understanding. There are multiple options for analysing the data in unique ways.

In the left side, it briefly shows the kind of data. In the middle side, it shows all entries of the selected kind of data (like Call logs). In the right side, it gives the full details of the selected item from the middle side.

This software is really helpful for the forensic of the mobile device to know the truth. It worthies software which helps for analysing the truth about someone and proves the right decision about something like crime etc.

Thanks, ☺