

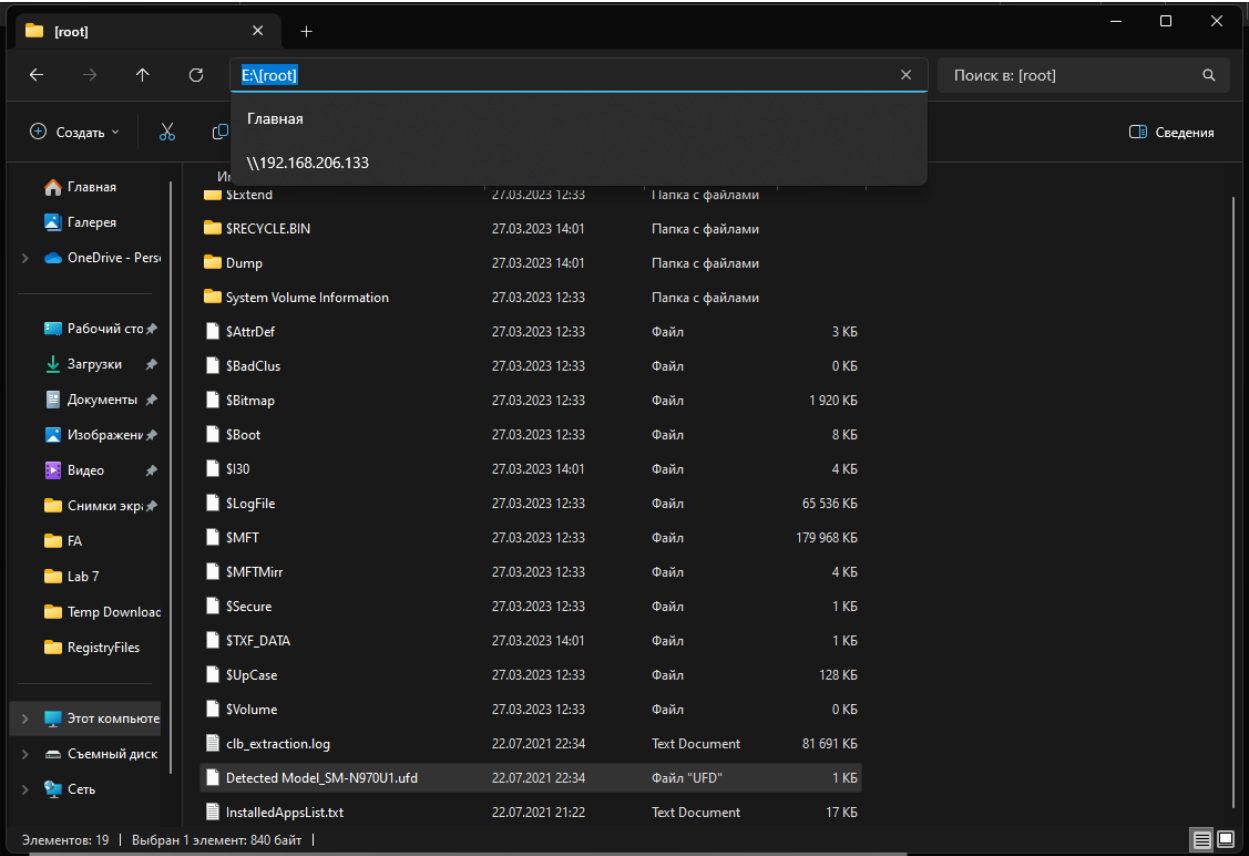
This document will include the findings that I need to do the quiz with some possible instructions upon where to find them.

These findings are important for the law case, and for my personal usage in the quiz.

## Name of the device

First, I want to know the name of the device (device model). That can be found in several ways.

Either after mounting the acquisitioned data with FTK Imager, in the root folder itself.



Or, by inspecting the image with the AutoPSY tool:

go to the path: Data Source > NameOfImage > Disk Itself > Dump/system/build.prop

The screenshot shows a forensic analysis tool interface. On the left, a file system tree is displayed under 'Data Sources' for 'ForensicsLab8.E01\_1 Host'. The 'system' folder is selected. On the right, a table lists files from '/img\_ForensicsLab8.E01/Dump/system'. The 'build.prop' file is highlighted. Below the table, the 'Strings' section shows extracted text from the selected file.

Name	S	C	O	Modified Time
[parent folder]				2023-03-27 14:01:17 CEST
apex				2023-03-27 13:59:20 CEST
app				2023-03-27 14:00:34 CEST
bin				2023-03-27 13:59:24 CEST
cameradata				2023-03-27 13:59:43 CEST
carrier				2023-03-27 13:59:24 CEST
etc				2023-03-27 14:00:11 CEST
fonts				2023-03-27 13:59:29 CEST
framework				2023-03-27 13:59:47 CEST
hidden				2023-03-27 14:00:34 CEST
lib				2023-03-27 13:59:43 CEST
lib64				2023-03-27 14:00:25 CEST
media				2023-03-27 13:59:58 CEST
priv-app				2023-03-27 14:00:57 CEST
saiv				2023-03-27 13:59:31 CEST
system_ext				2023-03-27 13:59:57 CEST
tts				2023-03-27 13:59:06 CEST
usr				2023-03-27 14:00:37 CEST
voicebargindata				2023-03-27 14:00:11 CEST
vramdiskdata				2023-03-27 14:00:34 CEST
build.prop				2008-12-31 16:00:00 CET
info.extra				2008-12-31 16:00:00 CET
recovery-from-boot.p				2008-12-31 16:00:00 CET
time_measurement_info				2008-12-31 16:00:00 CET

Strings extracted from build.prop:

```

ro.system.build.version.sdk=30
ro.product.system.brand=samsung
ro.product.system.device=d1q
ro.product.system.manufacturer=samsung
ro.product.system.model=SM-N970U1
ro.product.system.name=d1que
# end common build properties

```

The model name is **SM-N970U1** (quiz1) (Samsung) (This seems to be a Samsung Galaxy Note 10)

## Bluetooth connections

Then what I can do, is look for the Bluetooth connections to find potential other devices that the suspect might have, or connected to.

In this case, I managed to find a MAC Address of a car that the suspect connected to via Bluetooth.

It can be found in the file `bt_config` file, which is located here: `Dump/data/misc/bluedroid`

The screenshot shows a file explorer window with the file `bt_config.conf` selected. The file is located at `E:\[root]\Dump\data/misc/bluedroid`. The content of the file is displayed, showing a MAC address.

By opening that file, we can find this MAC address: **34:c7:31:f8:61:3b** (quiz2)

```
btconfig.conf
E:\> [root] > Dump > data > misc > bluetooth > [root] btconfig.conf
12 Address = f0:8a:76:c4:f8:eb
13 LE_LOCAL_KEY_IR = 35c2a8b4db3018095bc9c84761797a2b4066bc34261106e880b3b737600a33
14 LE_LOCAL_KEY_IR = b1352577a1ae118a8493d59c558619b813b57daf7a461b0a0cb9c9a0b3bad
15 LE_LOCAL_KEY_DNK = d5feaa17e279ef76feebca72e95ba470cad51768559cc5c4f2d9c4c3ad14db
16 LE_LOCAL_KEY_IR = 84bae140eac3504c26d6f0900bc0085fab7be42ab3abe01e425e0f28d274f40
17 Name = Galaxy Note10
18 ScanMode = 0
19 DiscoveryTimeout = 120
20
21 [68:a8:e1:b2:b4:f7]
22 DevType = 2
23 AddrType = 0
24 Role = 0
25 LinkType = 2
26 LinkFeature = 0
27 DevClass = 1280
28 LE_KEY_FENC = 491864e1d16f02325b6361d724dc7bae79c2e7a2473f3356c1613e5a2e1a1a44
29 LE_KEY_LCRR = 2b4e03bc5a8ca0f0d700133ba3d448d3b5a940ce892ab3f7ff035d6383264
30 LE_KEY_LTD =
31 PairingKeyAuth = 0
32 PairingKeyAuth = 0
33 Name = SPEN 01 (B4F7) JK
34 Service = 0000111e-0000-1000-8000-00005f9b34fb
35 Timestamp = 1625809528
36
37 [4c72:31:f8:01:b]
38 Manufacturer = 10
39 ImpVer = 4
40 ImpSubVer = 7298
41 Role = 1
42 LinkType = 1
43 Name = CAR MULTIMEDIA
44 DevClass = 3408904
45 DevType = 1
46 Timestamp = 1617592528
47 AddrType = 0
48 LinkKeyType = 5
49 PinLength = 0
50 LinkKey = 3a3d5035b8912913e79241f200b03691d79478174a17198770a72c133ef8ac
51 DeviceVersion = 0401
52 Service = 0000111e-0000-1000-8000-00005f9b34fb 0000110e-0000-1000-8000-00005f9b34fb 00001133-0000-1000-8000-00005f9b34fb
53 HfpVersion = 0501
54 HfpSdpFeatures = 0700
55
56 [2c:0b:7d:1d:21:a7]
57 Manufacturer = 13
```

## Internet

Apart from this, what I can do is look at possible data from the internet, as it might store the history of the user, or handles, or maybe stored passwords etc.

To take a look at that, we can use the AutoPSY, and use the Data Artifacts section, and find various information there, including web handles/accounts.

In this case, I found such information as Twitter handle, Reddit one, and probably Google email:

Twitter handle: **HeisenbergW4 (quiz3)**

Reddit handle: HeisenbergCarro

Google mail: [heisenbergcarro@gmail.com](mailto:heisenbergcarro@gmail.com) (quiz9) – this is the Google Account the user setup the device with

dev (2)

dqmdbg (4)

efs (36)

keydata (6)

linkerconfig (10)

lost+found (2)

mnt (18)

odm (2)

oem (2)

omr (4)

proc (2)

product (8)

res (3)

spu (3)

storage (3)

sys (2)

system (25)

apex (21)

app (149)

bin (229)

cameradata (10)

carrier (3)

etc (126)

fonts (325)

framework (133)

hidden (3)

lib (757)

lib64 (898)

media (25)

priv-app (230)

saiv (7)

system\_ext (10)

tts (3)

usr (8)

voicechargeindata (3)

vramdiskdata (3)

vendor (21)

System Volume Information (3)

File Views

File Types

Deleted Files

MB File Size

Data Artifacts

Communication Accounts (55)

Contacts (6)

Installed Programs (1230)

Messages (151)

Web Accounts (114)

Listing

Web Accounts

114 Results

Table Thumbnail Summary

Save Table as CSV

Source Name	S	C	O	User ID	Program Name	Pass
ForensicsLab8.E01				heisenbergcarro@gmail.com	com.google	aas_t
ForensicsLab8.E01				HeisenbergW4	com.twitter.android.auth.login	
ForensicsLab8.E01				Duo	com.google.android.apps.tachyon	
ForensicsLab8.E01				Signal	org.thoughtcrime.securesms	
ForensicsLab8.E01				TikTok	com.zhiliaoapp.musically	
ForensicsLab8.E01				Reddit for Android	com.reddit.account	
ForensicsLab8.E01				HeisenbergCarro	com.reddit.account	
ForensicsLab8.E01				WhatsApp	com.whatsapp	
ForensicsLab8.E01				heisenbergcarro@gmail.com	com.google	
ForensicsLab8.E01				HeisenbergW4	com.twitter.android.auth.login	
ForensicsLab8.E01				Duo	com.google.android.apps.tachyon	
ForensicsLab8.E01				Signal	org.thoughtcrime.securesms	
ForensicsLab8.E01				TikTok	com.zhiliaoapp.musically	
ForensicsLab8.E01				Reddit for Android	com.reddit.account	
ForensicsLab8.E01				HeisenbergCarro	com.reddit.account	
ForensicsLab8.E01				WhatsApp	com.whatsapp	
ForensicsLab8.E01				heisenbergcarro@gmail.com	com.google	eyJhI
ForensicsLab8.E01				heisenbergcarro@gmail.com	com.google	ya29
ForensicsLab8.E01				heisenbergcarro@gmail.com	com.google	ya29
ForensicsLab8.E01				heisenbergcarro@gmail.com	com.google	ya29
ForensicsLab8.E01				heisenbergcarro@gmail.com	com.google	ya29
ForensicsLab8.E01				heisenbergcarro@gmail.com	com.google	eyJhI
ForensicsLab8.E01				heisenbergcarro@gmail.com	com.google	ya29
ForensicsLab8.E01				heisenbergcarro@gmail.com	com.google	ROFV

Hex

Text

Application

Source File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Result: 1 of 5400

Result

Web Accounts

Type	Value	Source(s)
User ID	heisenbergcarro@gmail.com	Android An
Program N	com.google	Android An
Password	aas_et/AKpplNbdwOEDs7ZfQpzEfkmmycfeXufH4ZDMbq_GuZZ4U70x1KwFbSf5OnzgowVV2Zb uHRLi79LALdngA5nXPE1JmdnVmlrkY62CNH7huzn9Ah6cZzKNEBU2wzQCHK08jPsrbrj2vQcXl8 7yyPD-Yt3AMGM5Ler2lUKd0ktLWu1PqllB78lynRa-L0nl8Ct2YVWxk1bC7K_7CMw4FOz93l4=	Android An alyzer (aLE APP)
Comment	accounts ce 0	Android An

I also can see the web searches that the user have done, and in this case, the latest one was **blanton's bourbon (quiz5) (the apostrophe matters)**

### Web Search

636 Results

Source Name	S	C	O	Date Accessed	Text
ForensicsLab8.E01				2024-05-21 17:47:57 CEST	
ForensicsLab8.E01				2024-05-21 17:47:57 CEST	
ForensicsLab8.E01				2024-05-21 17:47:57 CEST	
ForensicsLab8.E01				2021-07-08 04:02:45 CEST	blanton's bourbon
ForensicsLab8.E01				2021-07-08 04:02:45 CEST	blanton's bourbon
ForensicsLab8.E01				2021-07-08 04:02:45 CEST	blanton's bourbon
ForensicsLab8.E01				2021-07-08 04:02:39 CEST	interesting car apps
ForensicsLab8.E01				2021-07-08 04:02:39 CEST	interesting car apps
ForensicsLab8.E01				2021-07-08 04:02:38 CEST	blanton's bourbon
ForensicsLab8.E01				2021-07-08 04:02:38 CEST	blanton's bourbon
ForensicsLab8.E01				2021-07-08 04:02:38 CEST	blanton's bourbon
ForensicsLab8.E01				2021-07-08 04:01:51 CEST	blanton's bourbon

Hex	Text	Application	Source File Metadata	OS Account
Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Result: 2863 of 5400				

#### Web Search

Term: blanton's bourbon  
 Time: 2021-07-08 04:02:45 CEST  
 Domain: google.com

#### Other

Comment: Chrome Search Terms

#### Source

Host: ForensicsLab8.E01\_1 Host  
 Data Source: ForensicsLab8.E01  
 File: /img\_ForensicsLab8.E01

## Messages

This Data Artifacts section also allows us to view the messages that were received on the phone.

Source Name	S	C	O	Message Type	Date/Time	Read	Direction	From Phone Number	To Phone Number	Text	Thread ID
mmssms.db	1			Android Message	2021-04-04 04:02:50 CEST	0	Incoming	29283	7603513a-d2af-4b1d-bdb6-ach40009967	<P> Your WhatsApp code: 506-924 you can also tap on...	#9402b43-0491-4d5d-a1fc-469c75c4d8c
mmssms.db	1			Android Message	2021-04-04 04:04:00 CEST	0	Incoming	86753	7603513a-d2af-4b1d-bdb6-ach40009967	<P> Heisenberg, 7357 is your Venmo phone verification...	#9402b43-0491-4d5d-a1fc-469c75c4d8c
mmssms.db	1			Android Message	2021-04-05 05:10:34 CEST	0	Incoming	32665	7603513a-d2af-4b1d-bdb6-ach40009967	286781 is your Facebook for Android confirmation code #9402b43-0491-4d5d-a1fc-469c75c4d8c	#9402b43-0491-4d5d-a1fc-469c75c4d8c
mmssms.db	1			Android Message	2021-04-07 02:32:57 CEST	0	Incoming	3340	7603513a-d2af-4b1d-bdb6-ach40009967	<P> 1988 is your T-Mobile Tuesdays code. Enter it in...	#9402b43-0491-4d5d-a1fc-469c75c4d8c
mmssms.db	1			Android Message	2021-04-12 05:14:42 CEST	1	Incoming	+15404488972	7603513a-d2af-4b1d-bdb6-ach40009967	Hey, I love this app for saving \$ on gas. My code Z3H5...	#9402b43-0491-4d5d-a1fc-469c75c4d8c
mmssms.db	1			Android Message	2021-05-06 02:31:12 CEST	0	Incoming	2297	7603513a-d2af-4b1d-bdb6-ach40009967	T-Mobile: There are safety measures you can take in a...	#9402b43-0491-4d5d-a1fc-469c75c4d8c
mmssms.db	1			Android Message	2021-05-17 18:07:08 CEST	0	Incoming	+16034301608	7603513a-d2af-4b1d-bdb6-ach40009967	<P> Snapchat Code: 842737. Happy Snapping! gany5...	#9402b43-0491-4d5d-a1fc-469c75c4d8c
mmssms.db	1			Android Message	2021-07-07 23:17:08 CEST	1	Outgoing	7603513a-d2af-4b1d-bdb6-ach40009967	+15404488972	Thought you might be interested in this CarGurus list...	#9402b43-0491-4d5d-a1fc-469c75c4d8c
mmssms.db	1			Android Message	2021-07-07 23:18:05 CEST	1	Outgoing	7603513a-d2af-4b1d-bdb6-ach40009967	+15404488972	Thought you might be interested in this CarGurus list...	#9402b43-0491-4d5d-a1fc-469c75c4d8c
mmssms.db	1			Android Message	2021-07-07 23:18:42 CEST	1	Outgoing	7603513a-d2af-4b1d-bdb6-ach40009967	+15404488972	Thought you might be interested in this CarGurus list...	#9402b43-0491-4d5d-a1fc-469c75c4d8c
mmssms.db	1			Android Message	2021-07-07 23:19:07 CEST	1	Outgoing	7603513a-d2af-4b1d-bdb6-ach40009967	+15404488972	Thought you might be interested in this CarGurus list...	#9402b43-0491-4d5d-a1fc-469c75c4d8c
mmssms.db	1			Android Message	2021-07-20 00:15:27 CEST	1	Outgoing	7603513a-d2af-4b1d-bdb6-ach40009967	+15402993169	Hey, thanks for calling. I will look up the inventory and...	#9402b43-0491-4d5d-a1fc-469c75c4d8c
mmssms.db	1			Android Message	2021-07-20 00:15:45 CEST	1	Incoming	+15402993169	7603513a-d2af-4b1d-bdb6-ach40009967	Great!	#9402b43-0491-4d5d-a1fc-469c75c4d8c

Hex	Text	Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Result: 3 of 66									

From: 29283  
 To: 7603513a-d2af-4b1d-bdb6-ach40009967  
 CC:  
 Subject:

Headers: Text HTML RTF Attachments (0) Accounts

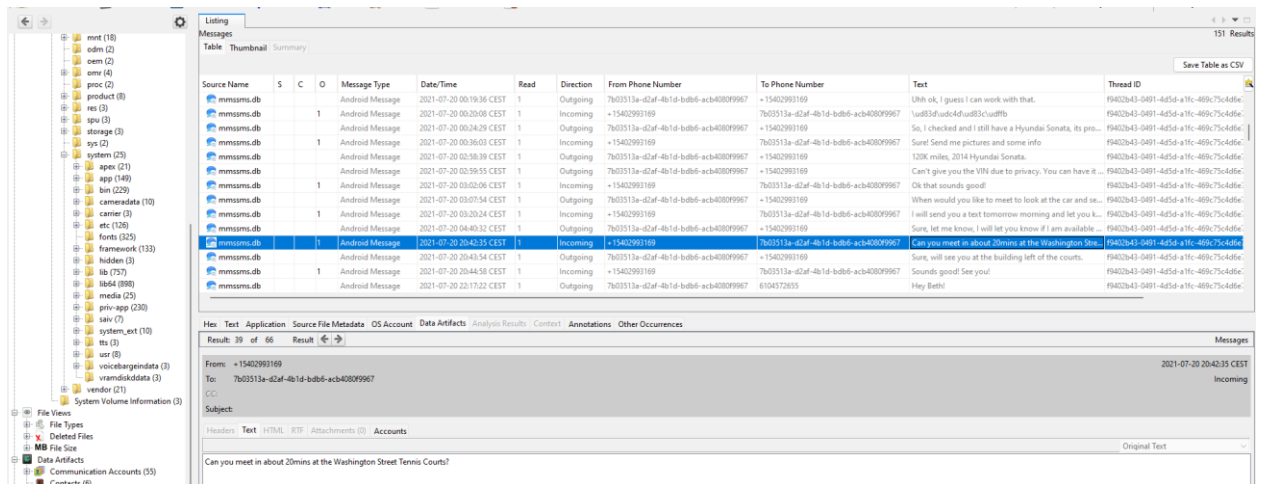
<P> Your WhatsApp code: 506-924

You can also tap on this link to verify your phone: v.whatsapp.com/506924

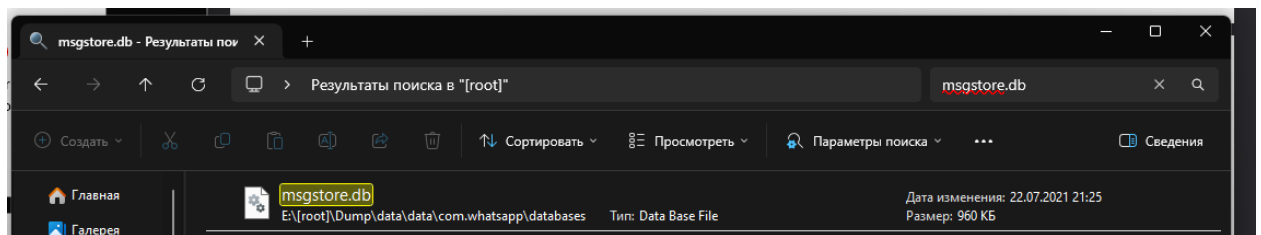
Don't share this code with others  
 4qgl-q1p5096

As seen in the screenshot, the first message was from WhatsApp, a 2FA code - **506-924 (quiz4)**

Also another thing that can be immediately noticed that the suspect also dealt a car, or is a car dealer, as he was messaging somebody else with the number +15402993169, and was going to sell a Hyundai Sonata 2014, 120k miles, VIN not shared due to privacy reasons. The suspect was found on Craigslist. The meetup was at Washington Street Tennis Courts

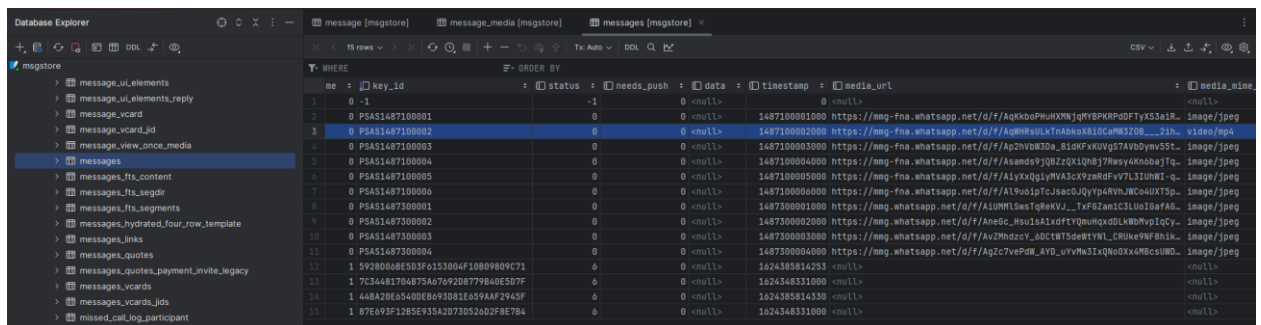


Apart from that, we can get more information regarding the user's messages in such an app as WhatsApp. To do that, I looked through some of the system files that are present in the image, and especially into the path in the screenshot:



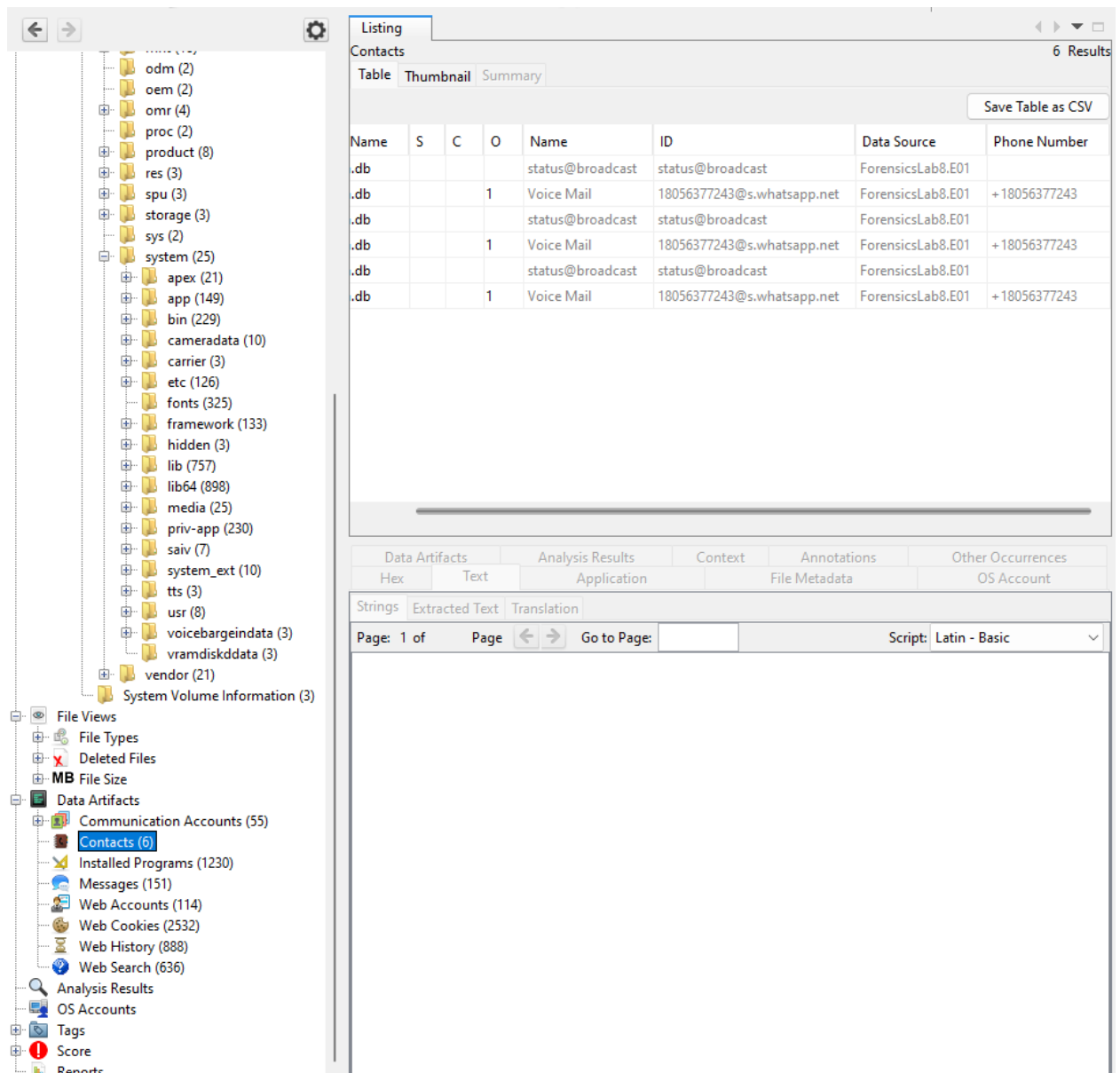
This database can be extracted via AutoPSY from the same directory, and then we can view embedded information for the messages, and their key\_id

To check the key\_id of a message where the suspect received a video, we can go to the table messages, and there we will see the key\_id: "PSAS1487100002" (quiz7)



## Contacts

Additionally, AutoPSY allows me to view the Contacts on the phone, and in this case I managed to find only one phone number: +18056377243 (quiz6)

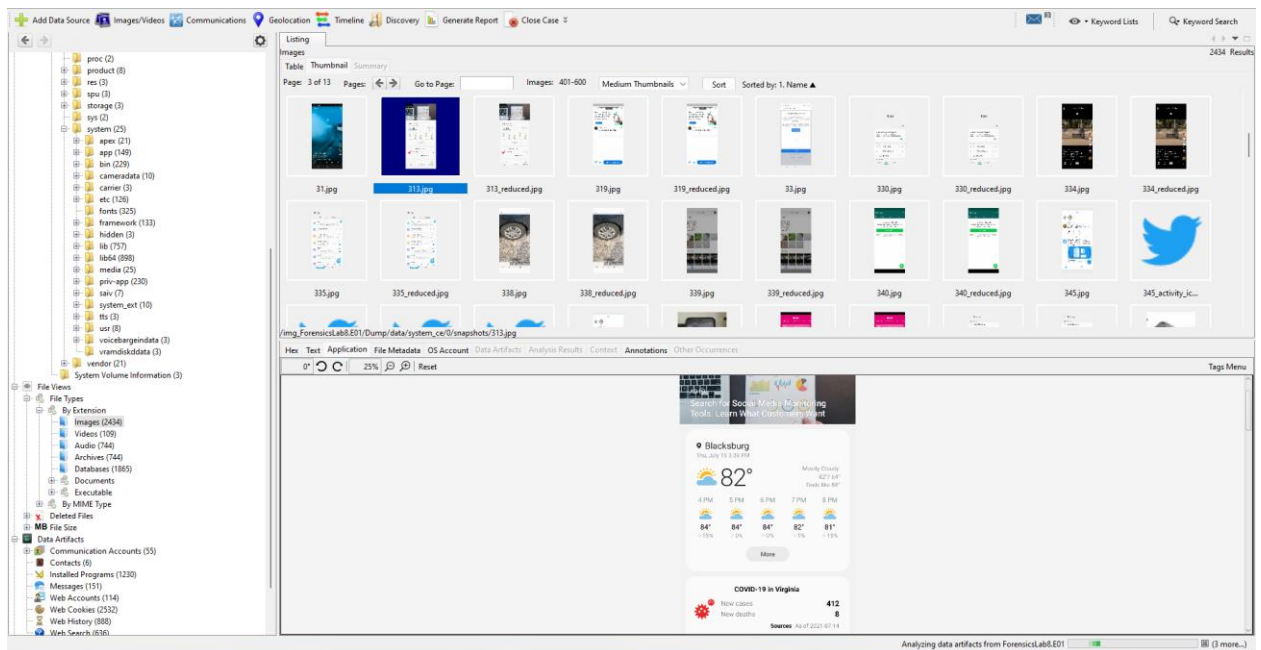


## Images

AutoPSY also allows me to view such things as images, which can be sometimes very handy

There seem to be multiple ways to also filter the images, by name, file size, and etc. In this case, I managed to find an example of a screenshot where the user was looking for weather information of a city called "Blacksburg" (quiz8)





To find it, you can look for files like 1.png, 312.jpg and etc., overall something that contains an integer only, such as that represents photos taken by the user/suspect. Then sort ascending by name, or make some other filter. In my case, I was looking personally through the photos. Also, I managed to see that the suspect had quite a few screenshots and photos with cars.

Metadata	
Name:	/img_ForensicsLab8.E01/Dump/data/system_ce/0/snapshots/313.jpg
Type:	File System

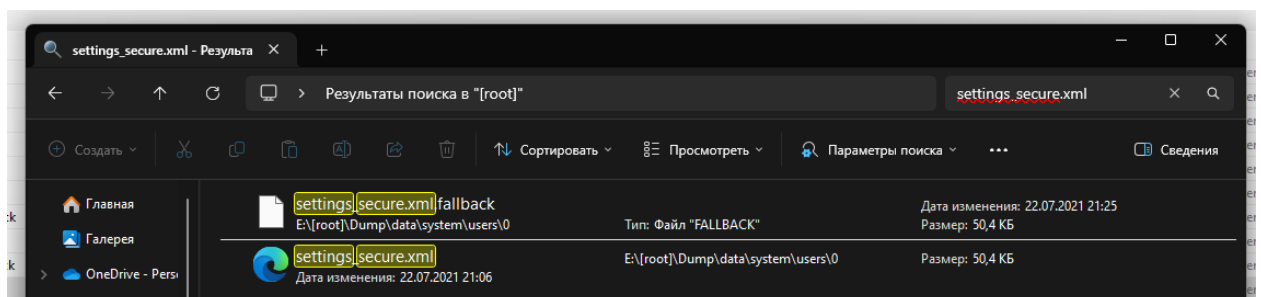
And this is where it was located in the directories of the image.

## Phone settings/System

Apart from all the above information, we can also check additional information regarding the phone settings, or phone information itself.

For example, we can look for security settings/policies that the user had enabled, or disabled. To do that, we need to look for a file called settings\_secure.xml

This file can be found in: Dump/data/system/users/0/settings\_secure.xml





Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
cocktails.xml				2021-07-02 23:18:55 CEST	2023-03-27 13:35:13 CEST	2023-03-27 13:35:13 CEST	2023-03-27 13:35:13 CEST	1108	Allocated	Allocated	unknown	/img_ForensicsLab8.E01/Dump/data/system
key_customize_info.xml				2021-07-20 20:55:41 CEST	2023-03-27 13:35:13 CEST	2023-03-27 13:35:13 CEST	2023-03-27 13:35:13 CEST	100	Allocated	Allocated	unknown	/img_ForensicsLab8.E01/Dump/data/system
package_restrictions.xml				2021-07-22 21:25:35 CEST	2023-03-27 13:35:13 CEST	2023-03-27 13:35:13 CEST	2023-03-27 13:35:13 CEST	297672	Allocated	Allocated	unknown	/img_ForensicsLab8.E01/Dump/data/system
photo.png				2021-06-03 21:21:57 CEST	2023-03-27 13:35:14 CEST	2023-03-27 13:35:14 CEST	2023-03-27 13:35:14 CEST	4311	Allocated	Allocated	unknown	/img_ForensicsLab8.E01/Dump/data/system
registered_services				2023-03-27 13:35:14 CEST	2023-03-27 13:35:14 CEST	2023-03-27 13:35:14 CEST	2023-03-27 13:35:14 CEST	360	Allocated	Allocated	unknown	/img_ForensicsLab8.E01/Dump/data/system
settings_config.xml				2021-07-21 05:31:10 CEST	2023-03-27 13:35:13 CEST	2023-03-27 13:35:13 CEST	2023-03-27 13:35:13 CEST	27884	Allocated	Allocated	unknown	/img_ForensicsLab8.E01/Dump/data/system
settings_config.xml.fallback				2021-07-22 21:25:34 CEST	2023-03-27 13:35:14 CEST	2023-03-27 13:35:14 CEST	2023-03-27 13:35:14 CEST	27884	Allocated	Allocated	unknown	/img_ForensicsLab8.E01/Dump/data/system
settings_global.xml				2021-07-22 21:17:38 CEST	2023-03-27 13:35:13 CEST	2023-03-27 13:35:13 CEST	2023-03-27 13:35:13 CEST	41109	Allocated	Allocated	unknown	/img_ForensicsLab8.E01/Dump/data/system
settings_global.xml.fallback				2021-07-22 21:25:34 CEST	2023-03-27 13:35:13 CEST	2023-03-27 13:35:13 CEST	2023-03-27 13:35:13 CEST	41109	Allocated	Allocated	unknown	/img_ForensicsLab8.E01/Dump/data/system
settings_secure.xml				2021-07-22 21:06:47 CEST	2023-03-27 13:35:13 CEST	2023-03-27 13:35:13 CEST	2023-03-27 13:35:13 CEST	51613	Allocated	Allocated	unknown	/img_ForensicsLab8.E01/Dump/data/system
settings_secure.xml.fallback				2021-07-22 21:25:34 CEST	2023-03-27 13:35:13 CEST	2023-03-27 13:35:13 CEST	2023-03-27 13:35:13 CEST	51613	Allocated	Allocated	unknown	/img_ForensicsLab8.E01/Dump/data/system
settings_usaid.xml				2021-07-02 23:18:56 CEST	2023-03-27 13:35:13 CEST	2023-03-27 13:35:13 CEST	2023-03-27 13:35:13 CEST	11769	Allocated	Allocated	unknown	/img_ForensicsLab8.E01/Dump/data/system
settings_usaid.xml.fallback				2021-07-22 21:25:34 CEST	2023-03-27 13:35:13 CEST	2023-03-27 13:35:13 CEST	2023-03-27 13:35:13 CEST	11769	Allocated	Allocated	unknown	/img_ForensicsLab8.E01/Dump/data/system
settings_system.xml				2021-07-22 21:45:06 CEST	2023-03-27 13:35:13 CEST	2023-03-27 13:35:13 CEST	2023-03-27 13:35:13 CEST	52902	Allocated	Allocated	unknown	/img_ForensicsLab8.E01/Dump/data/system

File can be opened/extracted and gathered information.

```

<?xml version="1.0" encoding="utf-8" standalone="yes" ?>
<settings version="191">
  <setting id="898" name="game_auto_temperature_control" value="0" package="com.samsung.android.game.gametools" defaultValue="0" defaultSysSet="true" preserve_in_restore="true" />
  <setting id="42" name="roam_guard_data_domestic" value="0" package="android" defaultValue="0" defaultSysSet="true" />
  <setting id="315" name="bluetooth_a2dp_uhq_support" value="0" package="com.android.bluetooth" defaultValue="0" defaultSysSet="true" preserve_in_restore="true" />
  <setting id="122" name="qspanel_media_quickcontrol_bar_available_on_top" package="com.android.systemui" />
  <setting id="237" name="masterLocationPackagePrefixBlacklist" value="com.google.android.gms.location" package="com.google.android.gms.location" preserve_in_restore="true" />
  <setting id="24" name="sleep_timeout" value="1" package="android" defaultValue="1" defaultSysSet="true" />
  <setting id="472" name="game_touchscreen_lock" value="0" package="com.samsung.android.game.gametools" defaultValue="0" defaultSysSet="true" preserve_in_restore="true" />
  <setting id="441" name="zen_setting_updated" value="1" package="android" defaultValue="1" defaultSysSet="true" />
  <setting id="1076" name="location_providers_allowed" value="gps,network" package="android" defaultValue="gps,network" defaultSysSet="true" preserve_in_restore="true" />
  <setting id="1076" name="location_providers_allowed" value="gps,network" package="android" defaultValue="gps,network" defaultSysSet="true" preserve_in_restore="true" />
  <setting id="1076" name="location_providers_allowed" value="gps,network" package="android" defaultValue="gps,network" defaultSysSet="true" preserve_in_restore="true" />
  <setting id="23" name="lock_screen_allow_private_notifications" value="1" package="android" defaultValue="1" defaultSysSet="true" />
  <setting id="52" name="roam_setting_data_lite" value="0" package="android" defaultValue="0" defaultSysSet="true" />
  <setting id="55" name="double_tap_to_wake" value="1" package="android" defaultValue="1" defaultSysSet="true" />
  <setting id="9" name="snack_password" value="1" package="android" defaultValue="1" defaultSysSet="true" />
</settings>

```

In the screenshot above, we can see that the user **enabled** (quiz10) the notifications option to be visible on the lock screen.

To view the possible backups of the applications, I had to search for backups folder, and then look for pending backups that are stored.

And in this case I managed to find that **com.google.android.apps.maps** (quiz11) is pending a backup.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[current folder]				2023-03-27 13:35:03 CEST	2023-03-27 13:35:03 CEST	2023-03-27 13:35:03 CEST	2023-03-27 13:35:03 CEST	192	Allocated	Allocated	unknown	/img_ForensicsLab8.E01/Dump/data/backup/pending
[parent folder]				2023-03-27 13:35:03 CEST	2023-03-27 13:35:03 CEST	2023-03-27 13:35:03 CEST	2023-03-27 13:35:03 CEST	56	Allocated	Allocated	unknown	/img_ForensicsLab8.E01/Dump/data/backup/pending
com.google.android.apps.maps				2021-07-22 21:06:45 CEST	2023-03-27 13:35:03 CEST	2023-03-27 13:35:03 CEST	2023-03-27 13:35:03 CEST	71	Allocated	Allocated	unknown	/img_ForensicsLab8.E01/Dump/data/backup/pending

And one last thing that I want to view, is an example of how many times the Android device powered off due to the battery being depleted (because the suspect might be roaming around neighborhoods for too long)

To find that information out, I had to go to the path: Dump/data/system/users/service/data and there, look for a file called eRR.p or something similar to it.

The screenshot shows a forensic tool interface. On the left is a file tree view showing a directory structure for a forensic dump. On the right is a log viewer displaying a list of system events. The log entries show various system events like LOGM, SHUTDOWN, LPM, and REBOOT, with reasons for power states like 'no power'.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MDS Hash
RC.p				2021-07-09 07:45:15 CEST	2023-03-27 13:35:14 CEST	2023-03-27 13:35:14 CEST	2023-03-27 13:35:14 CEST	171	Allocated	Allocated	unknown	/img_ForensicLab01/Dump/data/system/users/service/...	
[current folder]				2023-03-27 13:35:14 CEST	2023-03-27 13:35:14 CEST	2023-03-27 13:35:14 CEST	2023-03-27 13:35:14 CEST	240	Allocated	Allocated	unknown	/img_ForensicLab01/Dump/data/system/users/...	
[parent folder]				2023-03-27 13:35:14 CEST	2023-03-27 13:35:14 CEST	2023-03-27 13:35:14 CEST	2023-03-27 13:35:14 CEST	144	Allocated	Allocated	unknown	/img_ForensicLab01/Dump/data/system/users/...	
eRR.p				2021-07-09 07:45:15 CEST	2023-03-27 13:35:14 CEST	2023-03-27 13:35:14 CEST	2023-03-27 13:35:14 CEST	3371	Allocated	Allocated	unknown	/img_ForensicLab01/Dump/data/system/users/ser...	

Inside there, we can find information regarding how many times the phone's battery was completely depleted. We can count them manually, or extract the file and ask a text editor to count it for us.

The screenshot shows a text editor displaying a log file. The log entries show various system events like LOGM, SHUTDOWN, LPM, and REBOOT, with reasons for power states like 'no power'. The log entries are numbered 1 through 27.

```

1 LOGM/
2
3
4
5 2021-04-03 15:10:30-0400 | ON | RP | N970UUESEUAS / OFFSRC:(PS_HOLD,SOFT) / ONSRC:(HARDIST,PON1)
6 2021-05-01 06:04:43-0400 | SHUTDOWN | | REASON: no power
7 2021-05-04 00:55:18-0400 | NP | / /
8 2021-05-04 00:55:18-0400 | LPM |
9 2021-05-05 04:13:02-0400 | ON | NP | N970UUESEUAS / OFFSRC:(PS_HOLD,SOFT) / ONSRC:(KPD,PON1)
10 2021-05-05 04:15:14-0400 | REBOOT | | REASON: recovery
11 2021-05-05 04:22:10-0400 | ON | NP | N970UUEUFUC6 / OFFSRC:(PS_HOLD,SOFT) / ONSRC:(HARDIST,PON1)
12 2021-05-10 07:07:32-0400 | SHUTDOWN | | REASON: no power
13 2021-05-10 14:20:31-0400 | NP | / / 3771000(1%)
14 2021-05-10 14:20:31-0400 | LPM |
15 2021-05-15 20:03:42-0400 | ON | NP | N970UUEUFUC6 / OFFSRC:(PS_HOLD,SOFT) / ONSRC:(KPD,PON1)
16 2021-05-18 22:33:26-0400 | SHUTDOWN | | REASON: no power
17 2021-05-18 22:50:10-0400 | NP | / / 3775000(1%)
18 2021-05-18 22:50:10-0400 | LPM |
19 2021-05-18 22:54:19-0400 | ON | NP | N970UUEUFUC6 / OFFSRC:(PS_HOLD,SOFT) / ONSRC:(HARDIST,PON1)
20 2021-05-25 15:43:16-0400 | SHUTDOWN | | REASON: no power
21 2021-05-26 12:18:33-0400 | NP | / / 3295000(1%)
22 2021-05-26 12:18:33-0400 | LPM |
23 2021-05-26 12:27:36-0400 | ON | NP | N970UUEUFUC6 / OFFSRC:(PS_HOLD,SOFT) / ONSRC:(HARDIST,PON1)
24 2021-06-06 09:20:24-0400 | SHUTDOWN | | REASON: no power
25 2021-06-06 09:20:24-0400 | NP | / / 3751000(1%)
26 2021-06-06 09:20:24-0400 | LPM |
27 2021-06-06 16:47:27-0400 | ON | NP | N970UUEUFUC6 / OFFSRC:(PS_HOLD,SOFT) / ONSRC:(KPD,PON1)

```

The android device powered off 10 (quiz12) time