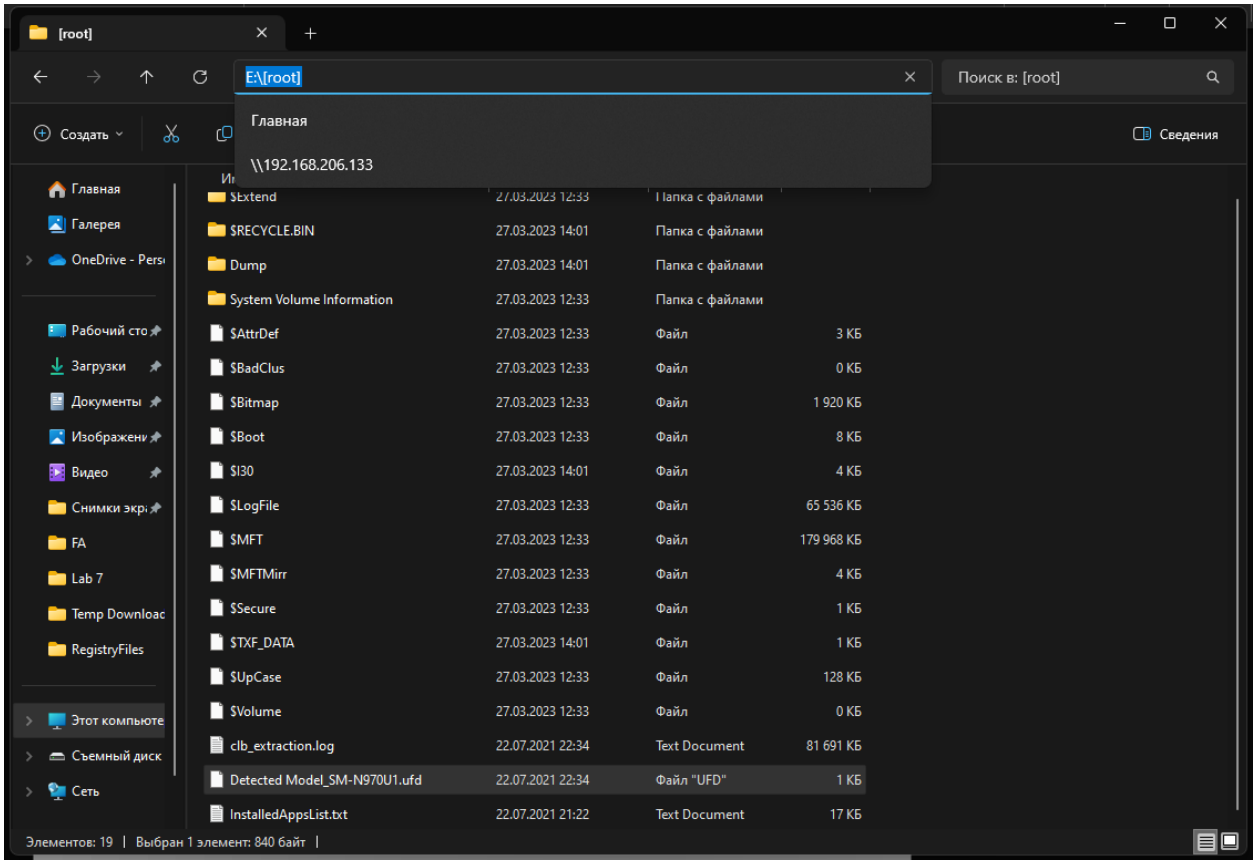
This document will include the findings that I need to do the quiz with some possible instructions upon where to find them.

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

Name of the device

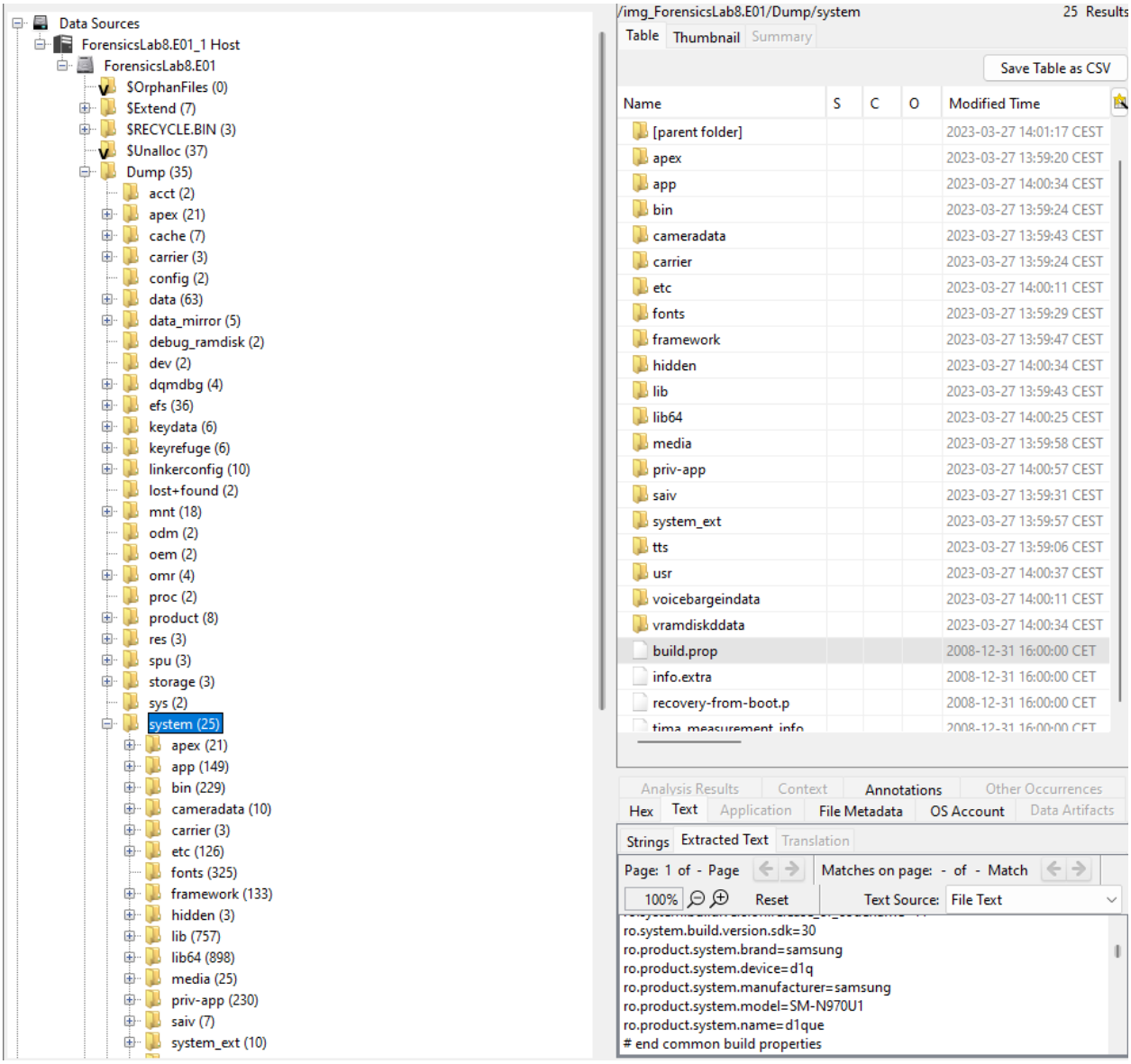
First, I want to know the name of the device (device model). That can be found in several ways.

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



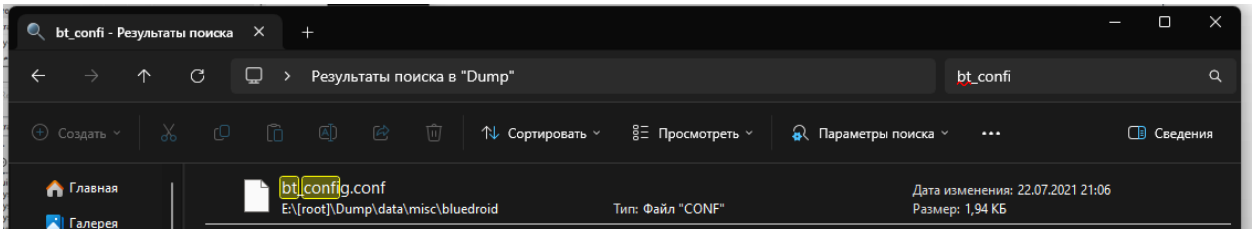
The model name is SM-N970U1 (quiz1) (Samsung) (This seems to be a Samsung Galaxy Note 10)

Bluetooth connections

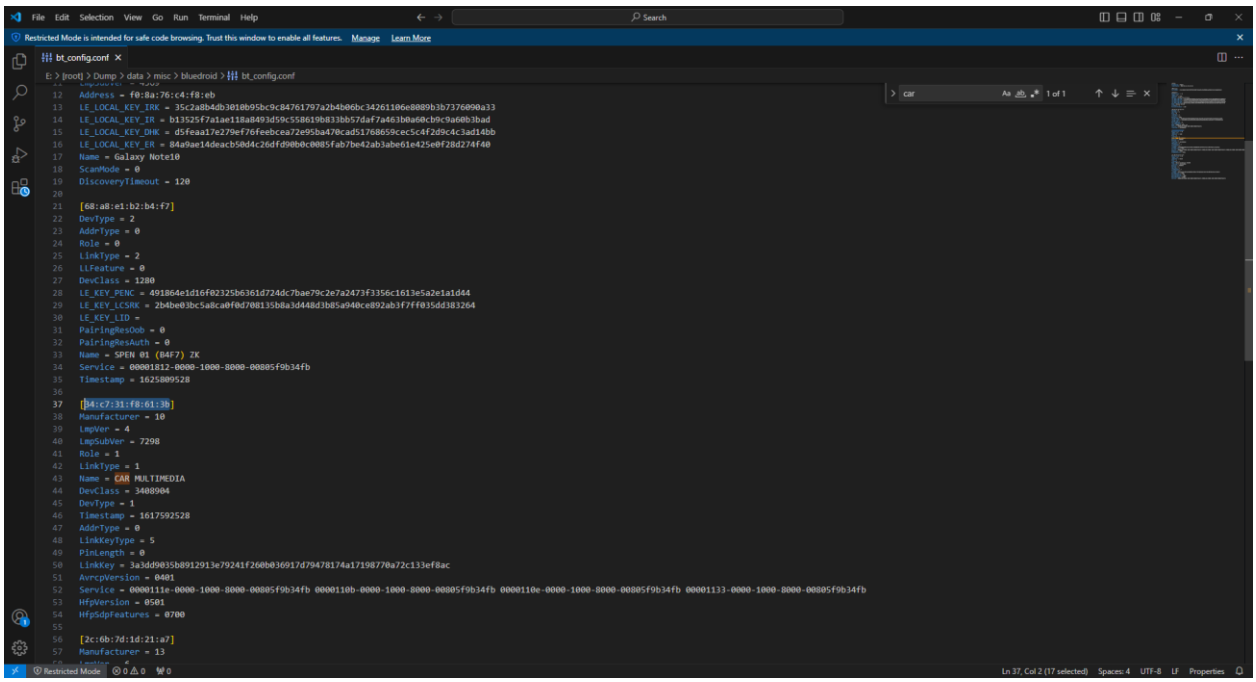
Then what I can do, is look for the Bluetooth connections to find potential other devices that the suspect might have, or connected to.

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



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



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.

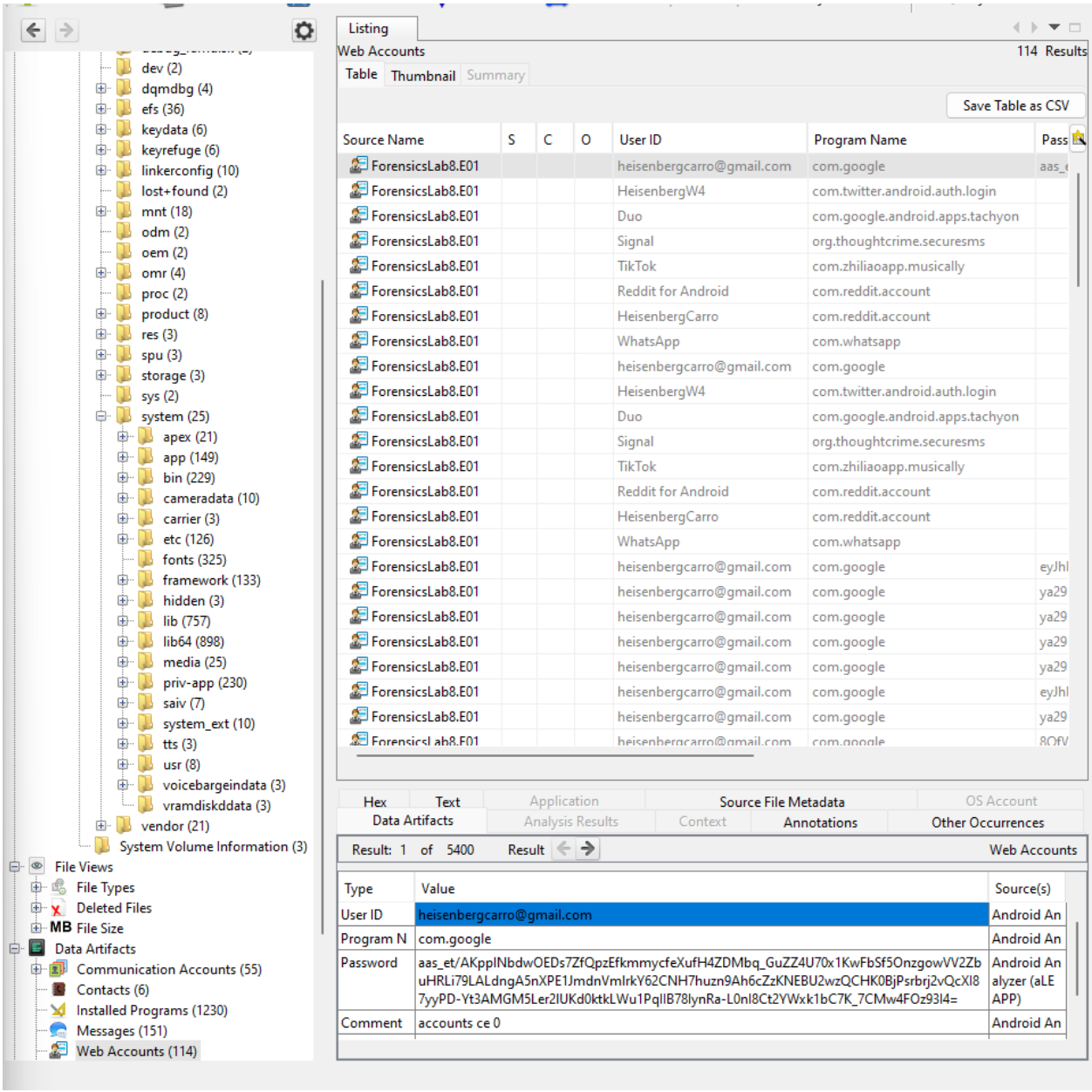
To take a look at that, we can use the AutoPSY, and use the Data Artifacts section, and find various information there, including web handles/accounts.

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

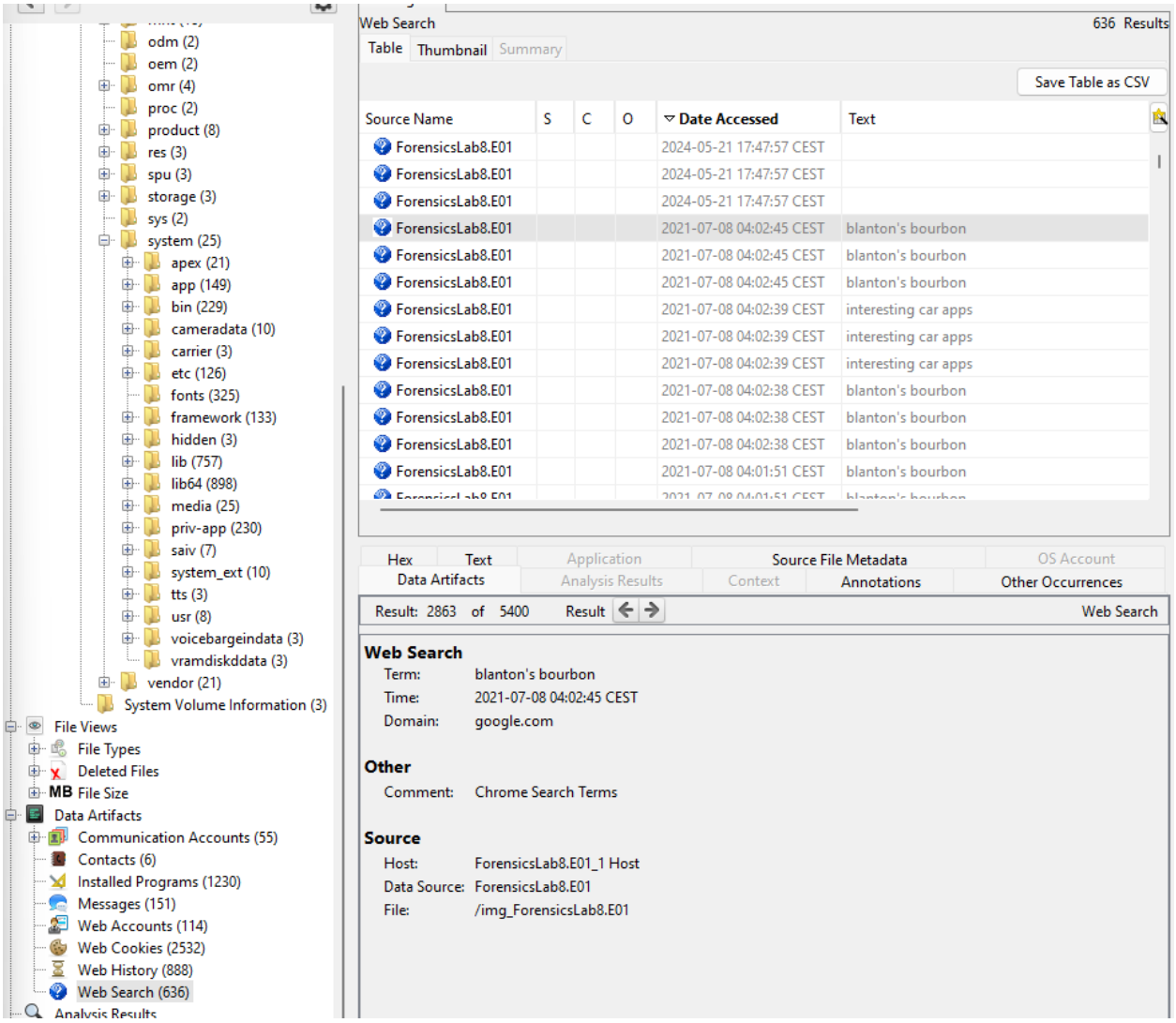
Twitter handle: HeisenbergW4 (quiz3)

Reddit handle: HeisenbergCarro

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

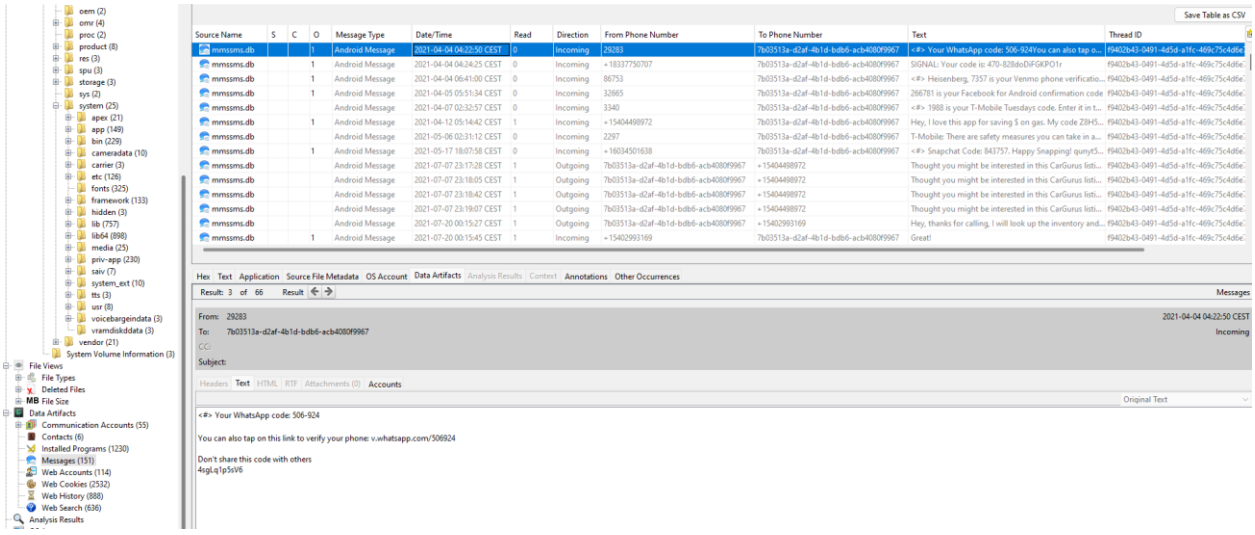


I also can see the web searches that the user have done, and in this case, the latest one was blanton's bourbon (quiz5) (the apostrophe matters)



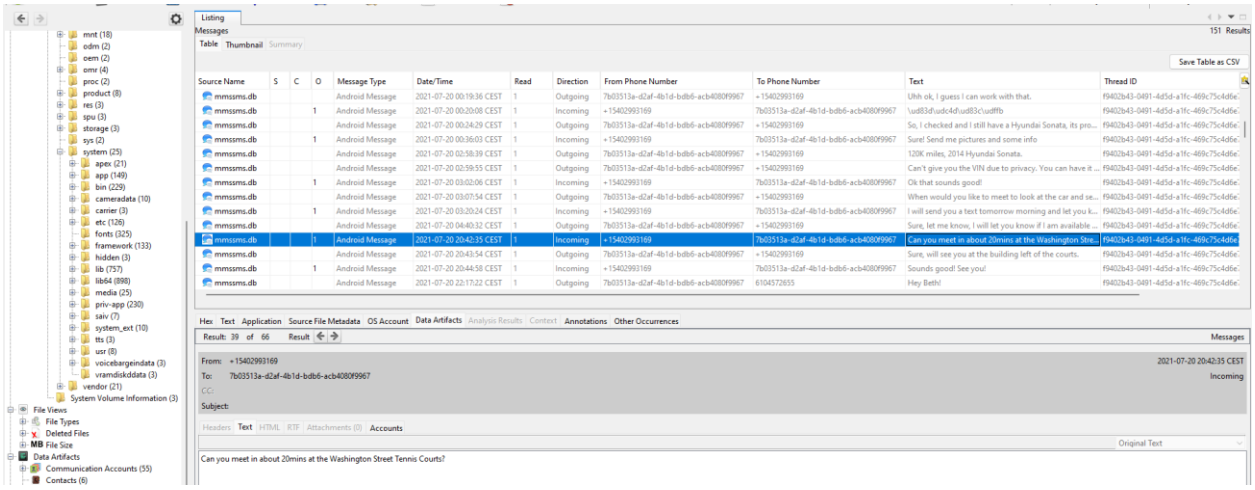
Messages

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

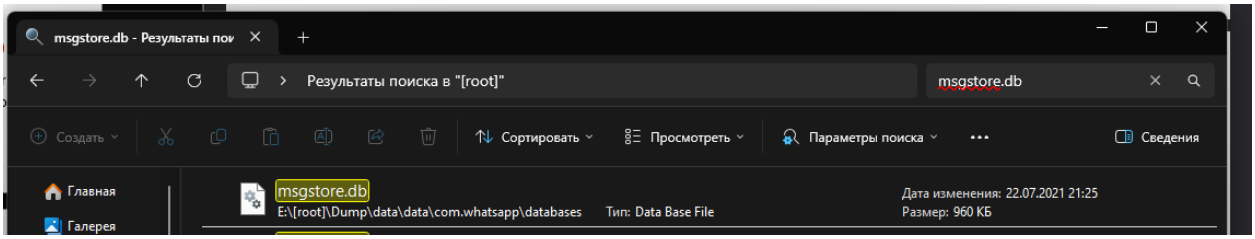


As seen in the screenshot, the first message was from WhatsApp, a 2FA code - 506-924 (quiz4)

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 Craiglist. The meetup was at Washington Street Tennis Courts

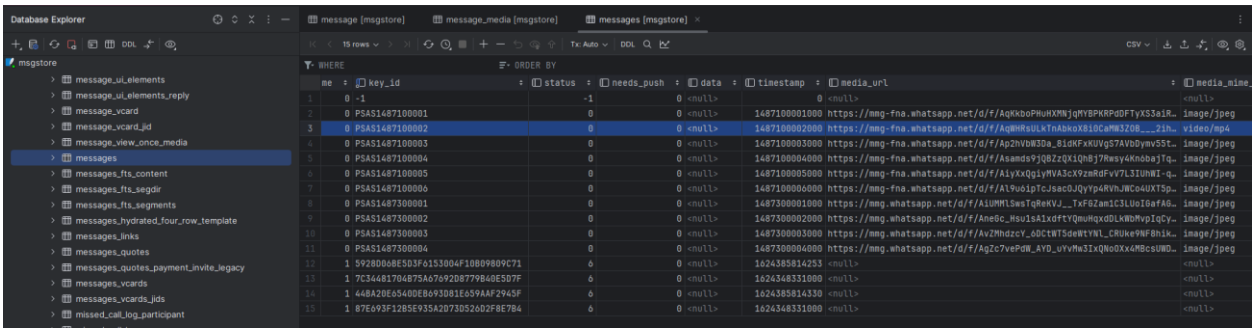


Apart from that, we can get more information regarding the user's messages in such an app as WhatsApp. To do that, I looked through some of the system files that are present in the image, and especially into the path in the screenshot:



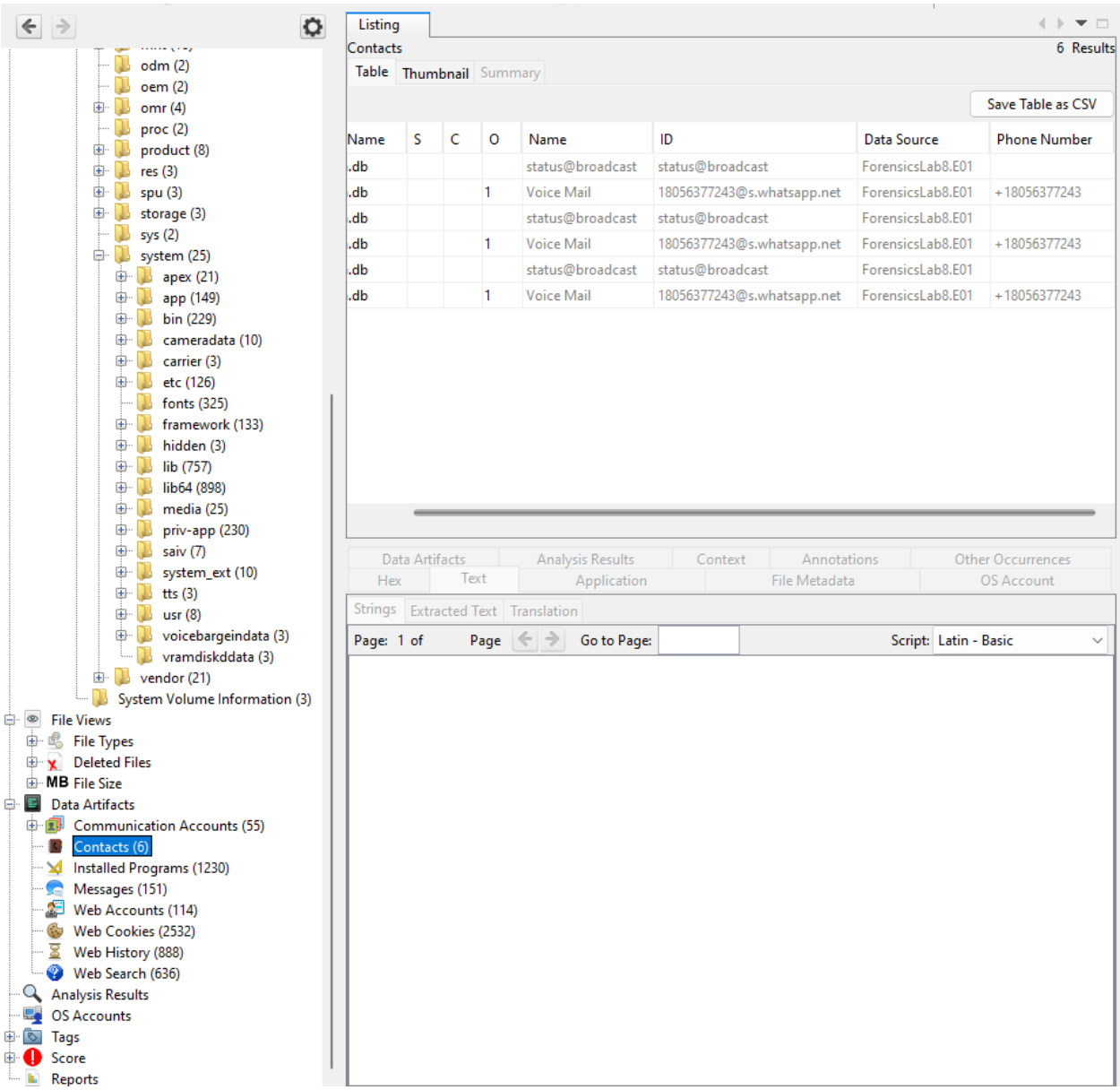
This database can be extracted via AutoPSY from the same directory, and then we can view embedded information for the messages, and their key_id

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

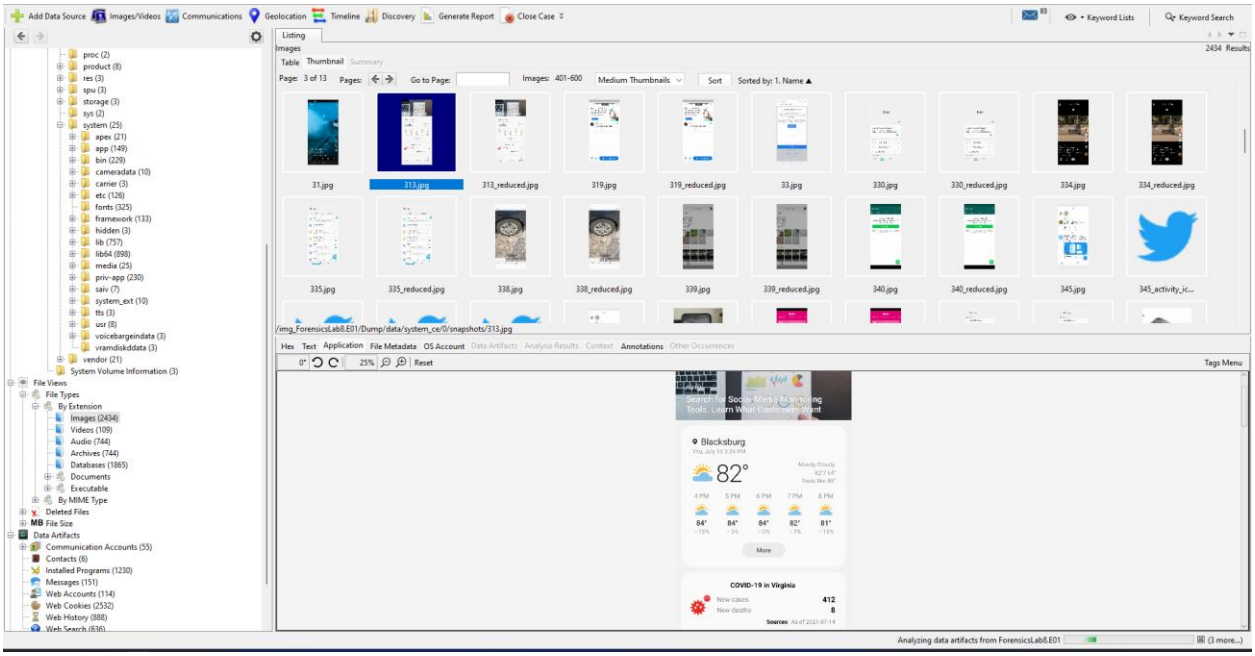
Additionally, AutoPSY allows me to view the Contacts on the phone, and in this case I managed to find only one phone number: +18056377243 (quiz6)



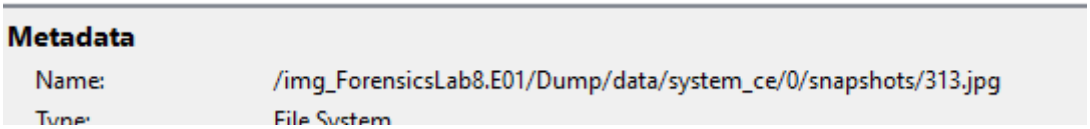
Images

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.



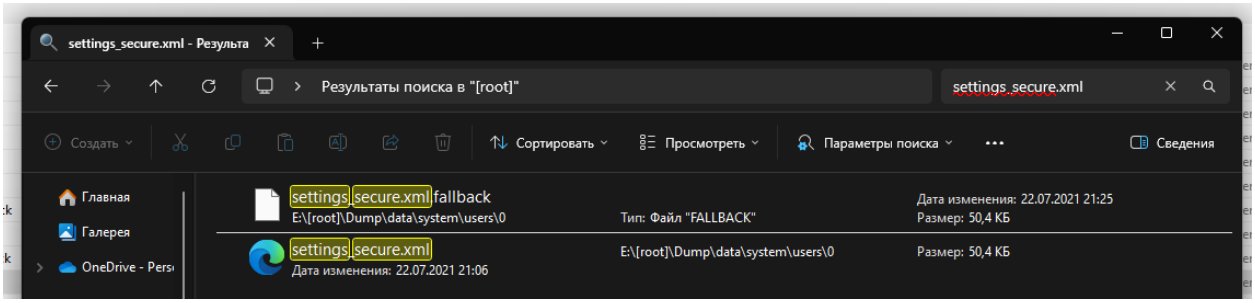
And this is where is was located in the directories of the image.

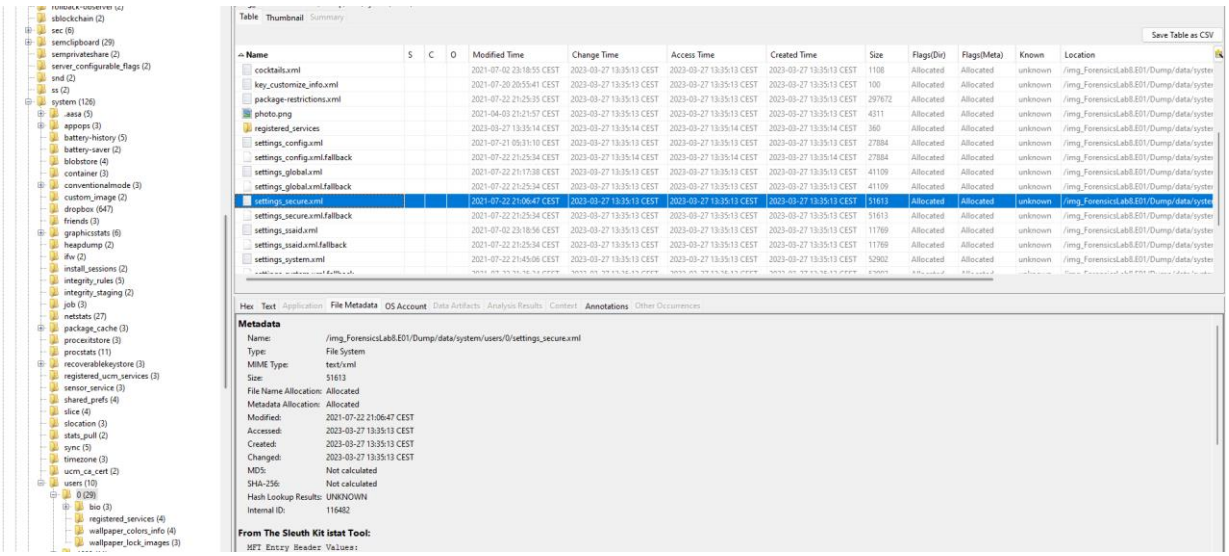
Phone settings/System

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

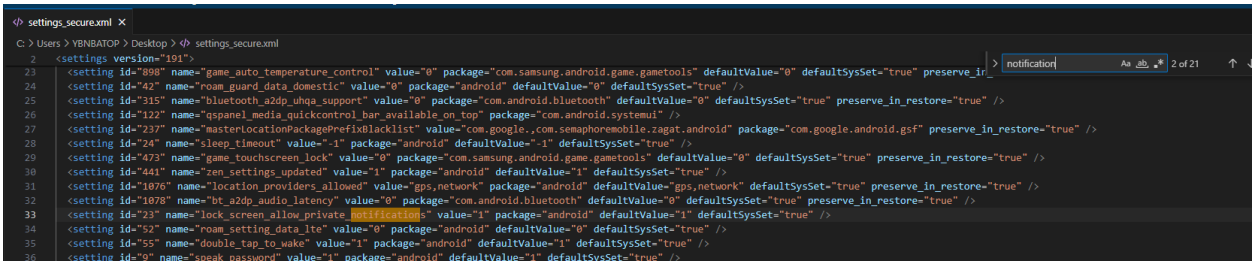
For example, we can look for security settings/policies that the user had enabled, or disabled. To do that, we need to look for a file called settings_secure.xml

This file can be found in: Dump/data/system/users/0/settings_secure.xml





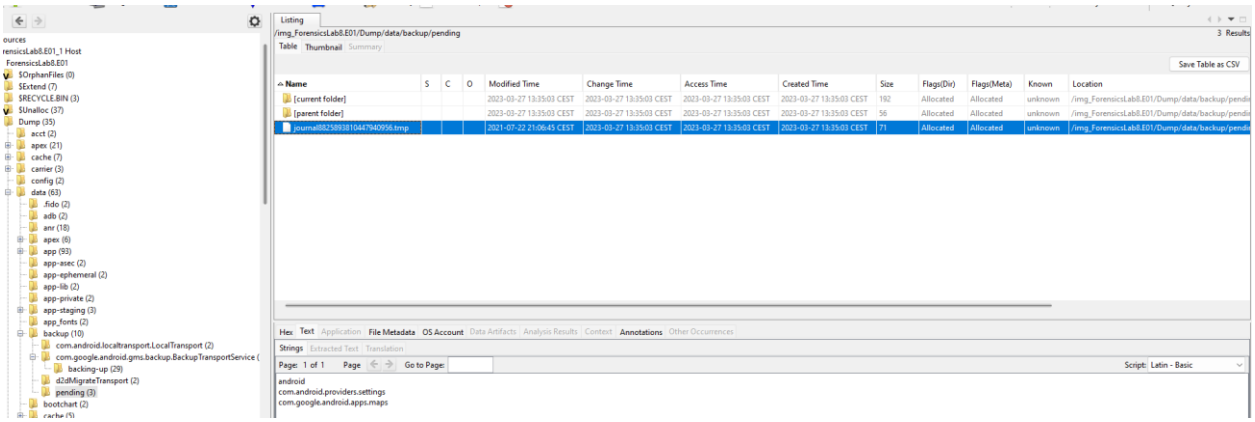
File can be opened/extracted and gathered information.



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.

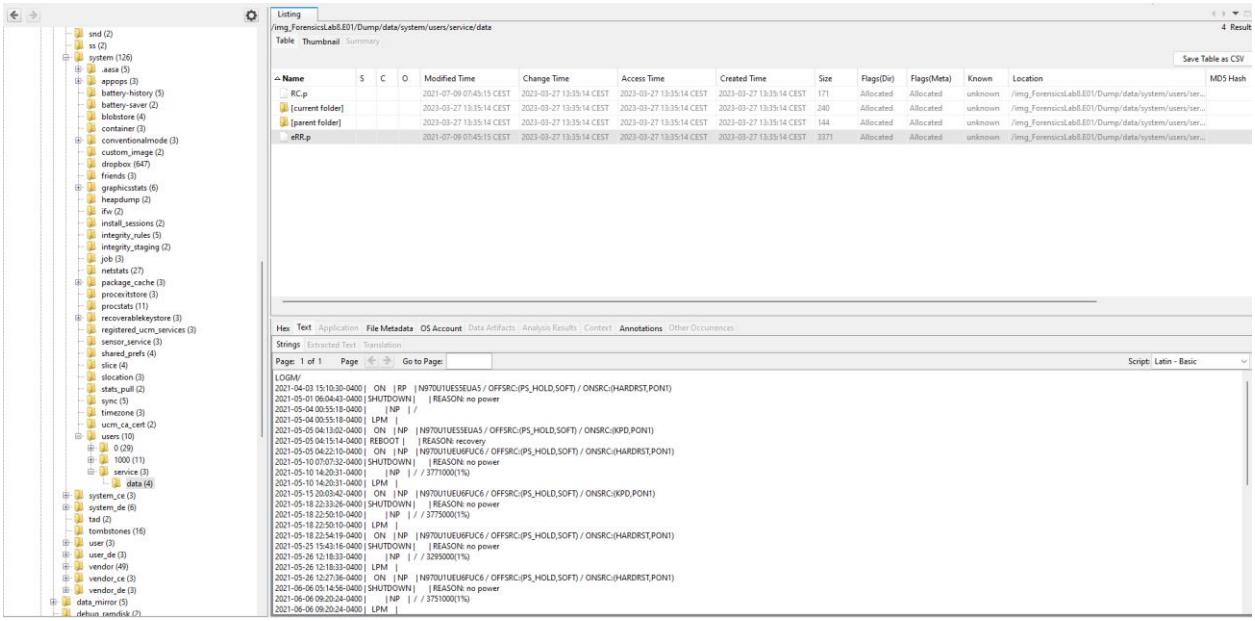
And in this case I managed to find that com.google.android.apps.maps (quiz11) is pending a backup.



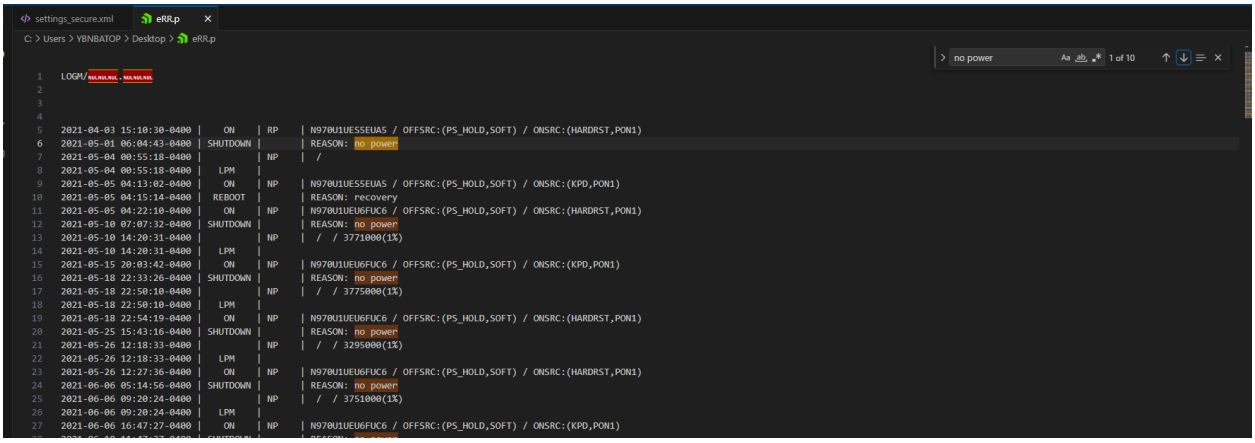
And one last thing that I want to view, is an example of how many times the Android device powered off due to the battery being depleted (because the suspect might be roaming around neighborhoods for too long)

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.



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 android device powered off 10 (quiz12) time