Assignment 3: Smartphones
Digital Forensics

Elisa Pioldi
ID 12305812

December 20, 2023

1 Factual part

1.1 Background

This analysis is regarding the smartphone of a man called Heisenberg, who was arrested for allegedly dealing with stolen cars.

1.2 Software and hardware specifications

For this analysis, I utilized the following software:

- **Cellebrite Reader** [1] – version 7.59.0.36; used to analyze the report already produced by the same software.
- **ALEAPP** [2] – version 2.7.0; used to extract data from the image of the smartphone.

Figure 1: Cellebrite logo.

1.3 Workflow

For this anaylis I got advantage of various tool of Cellebrite Reader, such as the search bar and the timeline.

To preserve the integrity of the evidence, I reported the MD5 hash of the files I found. You can find the MD5 hashes in the table 1.

Content	MD5
Video of the arrest	1fb629ceb7e03948032448b6af978c94
1st photo of the car	626e1bf6821aa7d3212727ee3bf9c63d
2nd photo of the car	13c3ebfb60c5ec08893c233ce42a3643
3rd photo of the car	dd27d1cf0fbcbd654c27c65aeb7f0efa
Hidden image	066858f4b1971b0501b9a06296936a34

Table 1: Checksums of important files.

1.4 Hash values

1.5 Findings

There are numerous files and applications concerning automobiles, as well as pictures of cars.

Between the installed apps, I report the following:

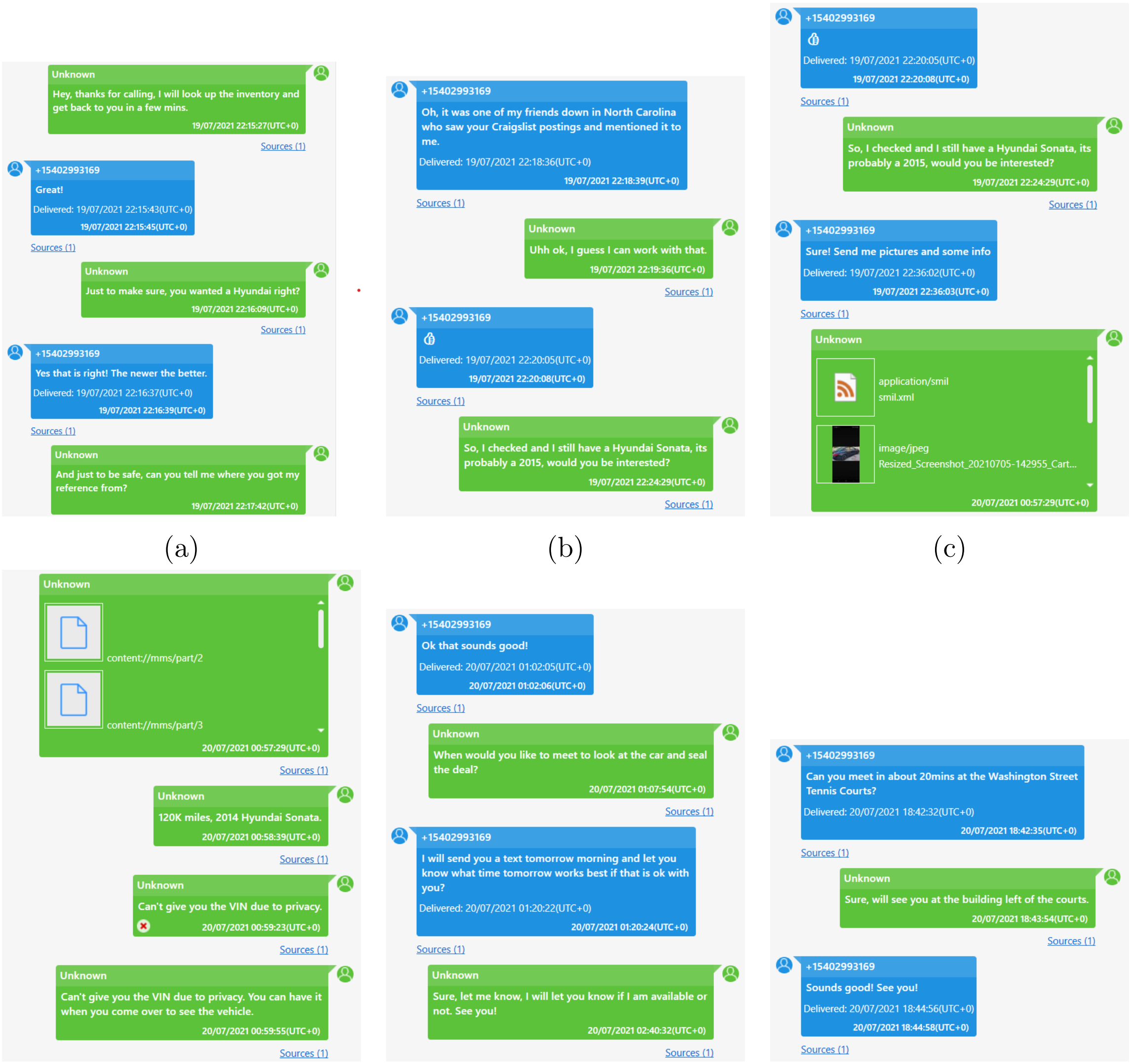
- **Venmo** [3]
- **Twitter**
- **HideX: Calculator Lock, App Hider and Photo Vault** [4]
- **BlueDriver OBD2 Scan Tool** [5]
- **Signal** [6]
- **CarGurus**
- **Autotrader**
- **Cartomizer**

I found some messages exchanged with a contact called `+15402993169` (see Figure 2).

You can see the pictures of the car he sent during the conversation with `+15402993169` in Figure 3. The paths of the pictures are the following:

- `Dump/data/user_de/0/com.android.providers.telephony/app_parts/PART_1626742644543_Resized_Screenshot_20210705-142955_Cartomizer.jpeg`
- `Dump/data/user_de/0/com.android.providers.telephony/app_parts/PART_1626742644555_Resized_20210703_192751.jpeg`
- `Dump/data/user_de/0/com.android.providers.telephony/app_parts/PART_1626742644568_Resized_20210703_192806.jpeg`

Moreover, I found some other messages with a contact called Beth Dutton in Instagram. You can see the messages in Figure 4.



Unknown
Hey, thanks for calling, I will look up the inventory and get back to you in a few mins.
19/07/2021 22:15:27(UTC+0)
Sources (1)

+15402993169
Great!
Delivered: 19/07/2021 22:15:43(UTC+0)
19/07/2021 22:15:45(UTC+0)
Sources (1)

Unknown
Just to make sure, you wanted a Hyundai right?
19/07/2021 22:16:09(UTC+0)
Sources (1)

+15402993169
Yes that is right! The newer the better.
Delivered: 19/07/2021 22:16:37(UTC+0)
19/07/2021 22:16:39(UTC+0)
Sources (1)

Unknown
And just to be safe, can you tell me where you got my reference from?
19/07/2021 22:17:42(UTC+0)

(a)

+15402993169
Oh, it was one of my friends down in North Carolina who saw your Craigslist postings and mentioned it to me.
Delivered: 19/07/2021 22:18:36(UTC+0)
19/07/2021 22:18:39(UTC+0)
Sources (1)

Unknown
Uhh ok, I guess I can work with that.
19/07/2021 22:19:36(UTC+0)
Sources (1)

+15402993169
👍
Delivered: 19/07/2021 22:20:05(UTC+0)
19/07/2021 22:20:08(UTC+0)
Sources (1)

Unknown
So, I checked and I still have a Hyundai Sonata, its probably a 2015, would you be interested?
19/07/2021 22:24:29(UTC+0)
Sources (1)

(b)

+15402993169
👍
Delivered: 19/07/2021 22:20:05(UTC+0)
19/07/2021 22:20:08(UTC+0)
Sources (1)

Unknown
So, I checked and I still have a Hyundai Sonata, its probably a 2015, would you be interested?
19/07/2021 22:24:29(UTC+0)
Sources (1)

+15402993169
Sure! Send me pictures and some info
Delivered: 19/07/2021 22:36:02(UTC+0)
19/07/2021 22:36:03(UTC+0)
Sources (1)

Unknown
application/smil
smil.xml
image/jpeg
Resized_Screenshot_20210705-142955_Cart...
20/07/2021 00:57:29(UTC+0)

(c)

Unknown
content://mms/part/2
content://mms/part/3
20/07/2021 00:57:29(UTC+0)
Sources (1)

Unknown
120K miles, 2014 Hyundai Sonata.
20/07/2021 00:58:39(UTC+0)
Sources (1)

Unknown
Can't give you the VIN due to privacy.
20/07/2021 00:59:23(UTC+0)
Sources (1)

Unknown
Can't give you the VIN due to privacy. You can have it when you come over to see the vehicle.
20/07/2021 00:59:55(UTC+0)
Sources (1)

(d)

+15402993169
Ok that sounds good!
Delivered: 20/07/2021 01:02:05(UTC+0)
20/07/2021 01:02:06(UTC+0)
Sources (1)

Unknown
When would you like to meet to look at the car and seal the deal?
20/07/2021 01:07:54(UTC+0)
Sources (1)

+15402993169
I will send you a text tomorrow morning and let you know what time tomorrow works best if that is ok with you?
Delivered: 20/07/2021 01:20:22(UTC+0)
20/07/2021 01:20:24(UTC+0)
Sources (1)

Unknown
Sure, let me know, I will let you know if I am available or not. See you!
20/07/2021 02:40:32(UTC+0)
Sources (1)

(e)

+15402993169
Can you meet in about 20mins at the Washington Street Tennis Courts?
Delivered: 20/07/2021 18:42:32(UTC+0)
20/07/2021 18:42:35(UTC+0)
Sources (1)

Unknown
Sure, will see you at the building left of the courts.
20/07/2021 18:43:54(UTC+0)
Sources (1)

+15402993169
Sounds good! See you!
Delivered: 20/07/2021 18:44:56(UTC+0)
20/07/2021 18:44:58(UTC+0)
Sources (1)

(f)

Figure 2: Screenshots of the messages exchanged with `+15402993169`.

2 Analysis

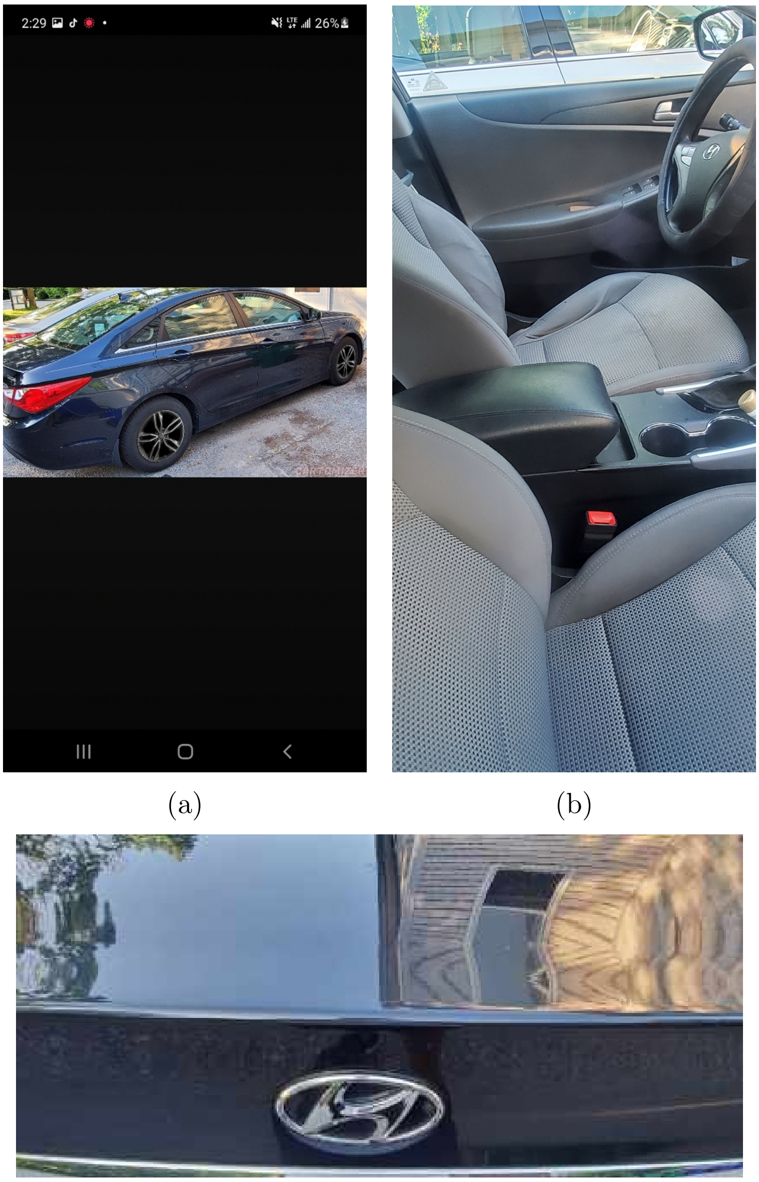
2.1 Evidence of deals with stolen cars

The major evidence comes from messages exchanged with the contact `+15402993169` (see Figure 2). The conversation starts with Heisenberg looking at his inventory to find a Hyundai for the contact. He asks him how he obtained his name, probably to be sure he is not a police officer. Heisenberg finds him a Hyundai Sonata and they plan to meet at the Washington Street Tennis Court in 20 minutes.

Moreover, as I already mentioned, I found some suspicious messages with a contact called Beth Dutton, where there are death menaces from her. This indicates that Heisenberg was conducting sketchy business.

I found numerous pictures of cars in the gallery, which are probably the cars that Heisenberg was selling.

Since I didn't find any other message with other contacts, I suppose he was conducting his main business in the app Signal [6], which is an end-to-end encrypted messaging app.



(a)

(b)

(c)

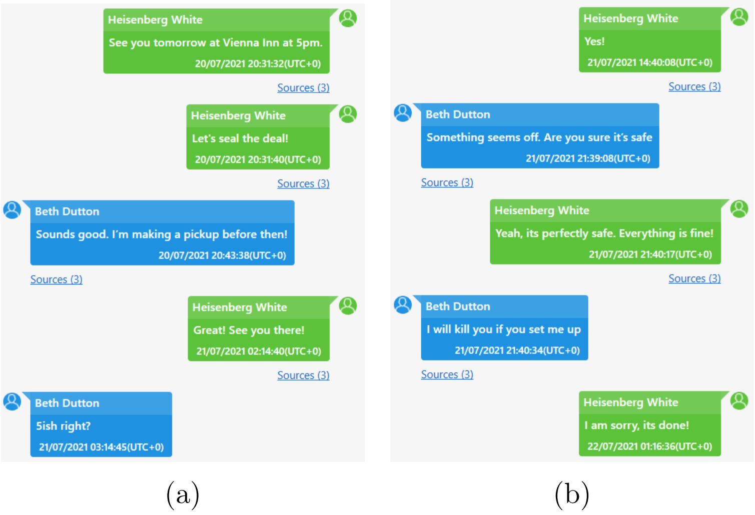
Figure 3: Pictures of the car that Heisenberg was selling.

I found numerous activities related to this app in the timeline.

2.2 Recordings of the arrest

I found a video of the arrest, which was recorded by Heisenberg, filtering the videos by date. It was created on 20/07/2021 at 14:03:34 (UTC+0) The MD5 hash of the video is `1fb629ceb7e03948032448b6af978c94` and the path is:
`Dump/data/media/0/DCIM/Camera/20210720_150222.mp4`.

The video shows Heisenberg showing a car to a possible buyer, who is actually an undercover police officer. At the end of the video, the police officer after saying that the car is stolen, arrests Heisenberg.



(a)

Heisenberg White
See you tomorrow at Vienna Inn at 5pm.
20/07/2021 20:31:32(UTC+0)
Sources (3)

Heisenberg White
Let's seal the deal!
20/07/2021 20:31:40(UTC+0)
Sources (3)

Beth Dutton
Sounds good. I'm making a pickup before then!
20/07/2021 20:43:38(UTC+0)
Sources (3)

Heisenberg White
Great! See you there!
21/07/2021 02:14:40(UTC+0)
Sources (3)

Beth Dutton
5ish right?
21/07/2021 03:14:45(UTC+0)

(b)

Heisenberg White
Yes!
21/07/2021 14:40:08(UTC+0)
Sources (3)

Beth Dutton
Something seems off. Are you sure it's safe
21/07/2021 21:39:08(UTC+0)
Sources (3)

Heisenberg White
Yeah, its perfectly safe. Everything is fine!
21/07/2021 21:40:17(UTC+0)
Sources (3)

Beth Dutton
I will kill you if you set me up
21/07/2021 21:40:34(UTC+0)
Sources (3)

Heisenberg White
I am sorry, its done!
22/07/2021 01:16:36(UTC+0)

Figure 4: Screenshots of the messages exchanged with Beth Dutton.

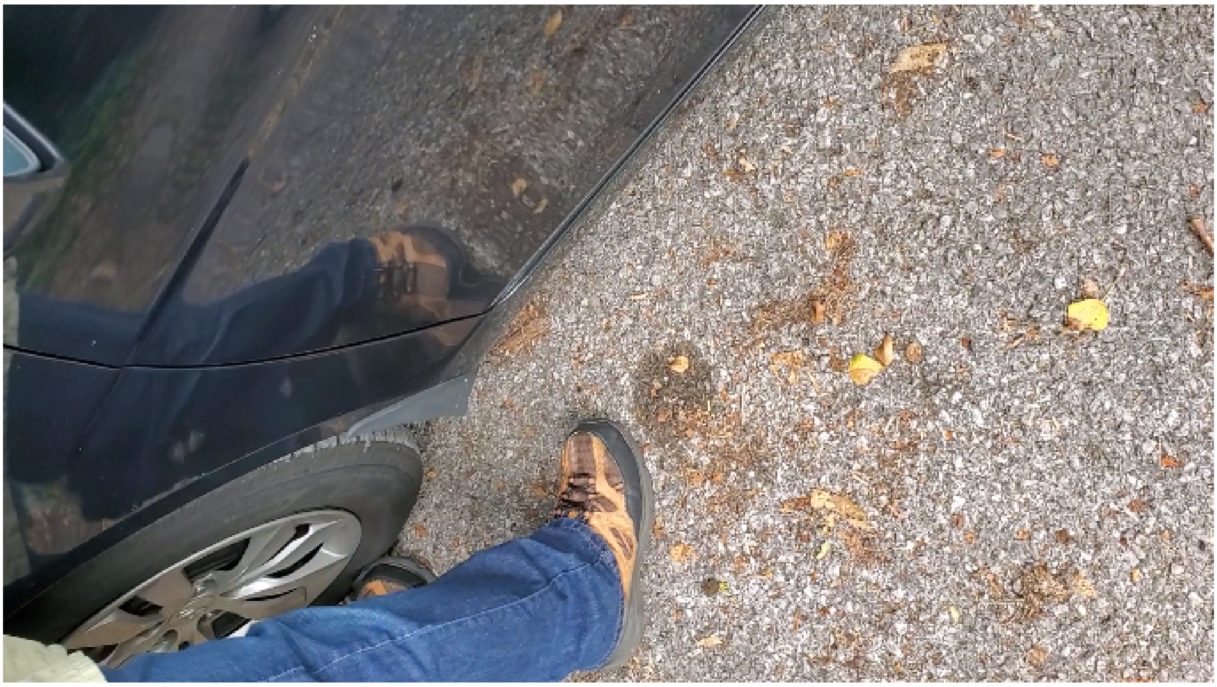
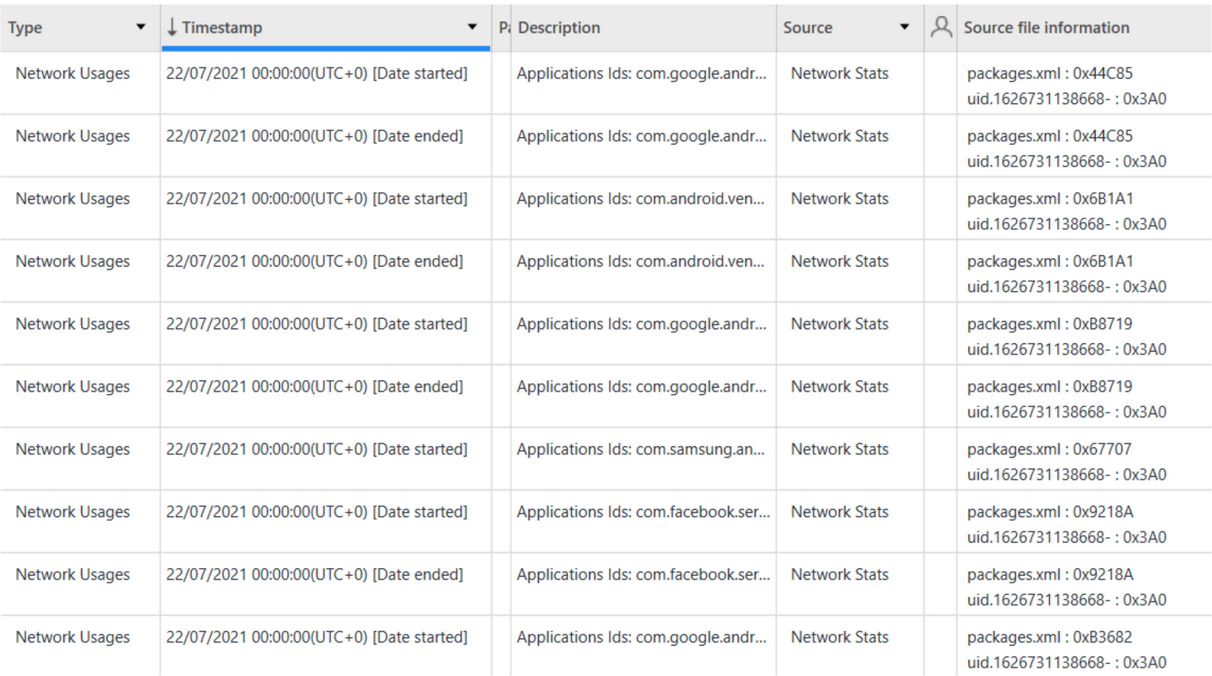


Figure 5: Frame of the video showing the arrest.

2.3 Police best practices

To find out if the police followed best practices, I got advantage of the timeline tool: I looked for activities on the smartphone after the arrest and I found that there are network activities in the smartphone after it. This means that the police did not follow best practices, because they should have disconnected it from the network as soon as possible and don't use it anymore. This is because the smartphone could be remotely wiped, so it is important to disconnect it from the network.

You can see for example some of the network activities during 22/07/2021 which is two days after the arrest in Figure 6.



Type	Timestamp	P	Description	Source		Source file information
Network Usages	22/07/2021 00:00:00(UTC+0) [Date started]		Applications Ids: com.google.andr...	Network Stats		packages.xml : 0x44C85 uid.1626731138668- : 0x3A0
Network Usages	22/07/2021 00:00:00(UTC+0) [Date ended]		Applications Ids: com.google.andr...	Network Stats		packages.xml : 0x44C85 uid.1626731138668- : 0x3A0
Network Usages	22/07/2021 00:00:00(UTC+0) [Date started]		Applications Ids: com.android.ven...	Network Stats		packages.xml : 0x6B1A1 uid.1626731138668- : 0x3A0
Network Usages	22/07/2021 00:00:00(UTC+0) [Date ended]		Applications Ids: com.android.ven...	Network Stats		packages.xml : 0x6B1A1 uid.1626731138668- : 0x3A0
Network Usages	22/07/2021 00:00:00(UTC+0) [Date started]		Applications Ids: com.google.andr...	Network Stats		packages.xml : 0xB8719 uid.1626731138668- : 0x3A0
Network Usages	22/07/2021 00:00:00(UTC+0) [Date ended]		Applications Ids: com.google.andr...	Network Stats		packages.xml : 0xB8719 uid.1626731138668- : 0x3A0
Network Usages	22/07/2021 00:00:00(UTC+0) [Date started]		Applications Ids: com.samsung.an...	Network Stats		packages.xml : 0x67707 uid.1626731138668- : 0x3A0
Network Usages	22/07/2021 00:00:00(UTC+0) [Date started]		Applications Ids: com.facebook.ser...	Network Stats		packages.xml : 0x9218A uid.1626731138668- : 0x3A0
Network Usages	22/07/2021 00:00:00(UTC+0) [Date ended]		Applications Ids: com.facebook.ser...	Network Stats		packages.xml : 0x9218A uid.1626731138668- : 0x3A0
Network Usages	22/07/2021 00:00:00(UTC+0) [Date started]		Applications Ids: com.google.andr...	Network Stats		packages.xml : 0xB3682 uid.1626731138668- : 0x3A0

Figure 6: network activities of the smartphone after the arrest.

2.4 Interest in cryptocurrency

I noticed the presence of the app *Venmo* (see Figure 7), which is an app used to manage crypto wallets. I checked the timeline to see if there are any activities related to this app and I found numerous network activities related to it. You can see part of the timeline in Figure 8.

Figure 7: Icon of the app *Venmo*.

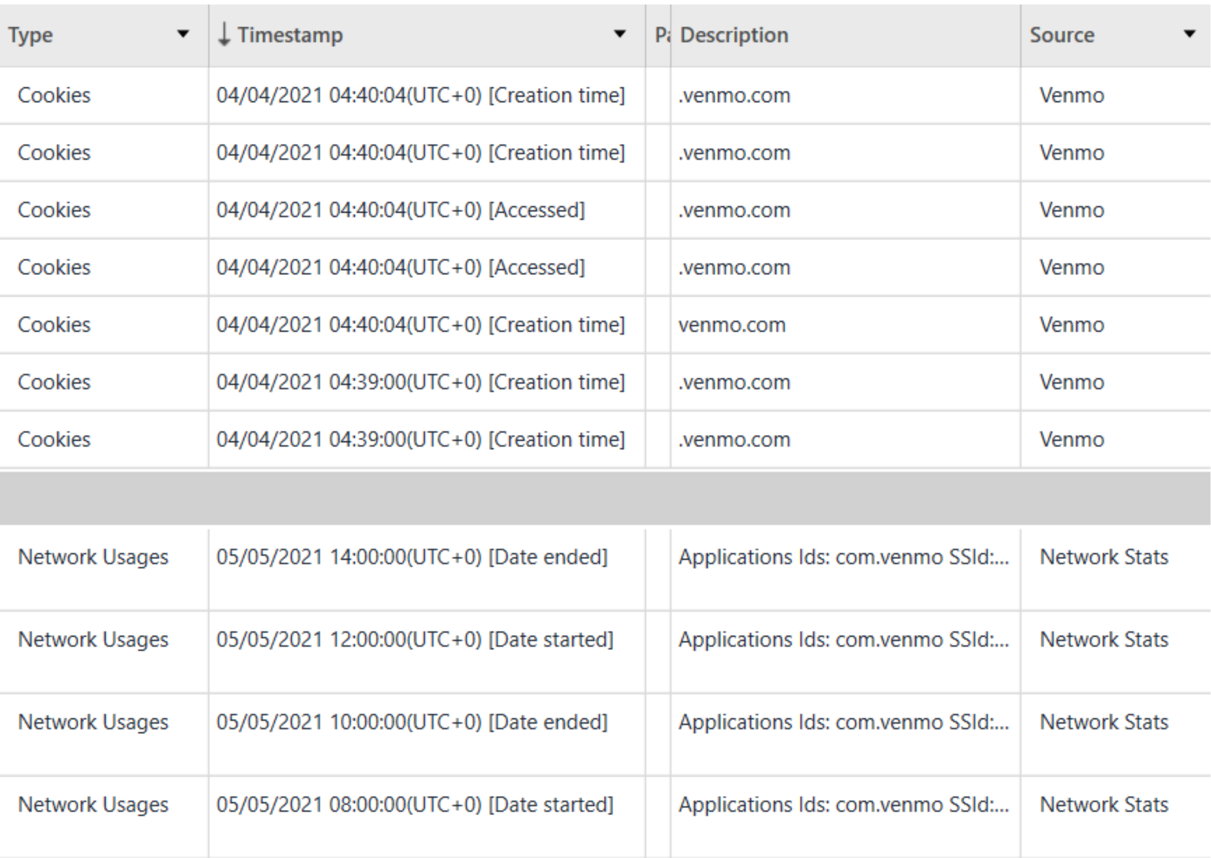
Moreover, checking Twitter notifications in Gmail, I found numerous news about cryptocurrency: he follows accounts as *Bitcoin News* and *Bitcoin*. See Figure 9 for some of the notifications.

2.5 File hiding or encryption

I found the app *Calculator* [4] which is used to hide files.

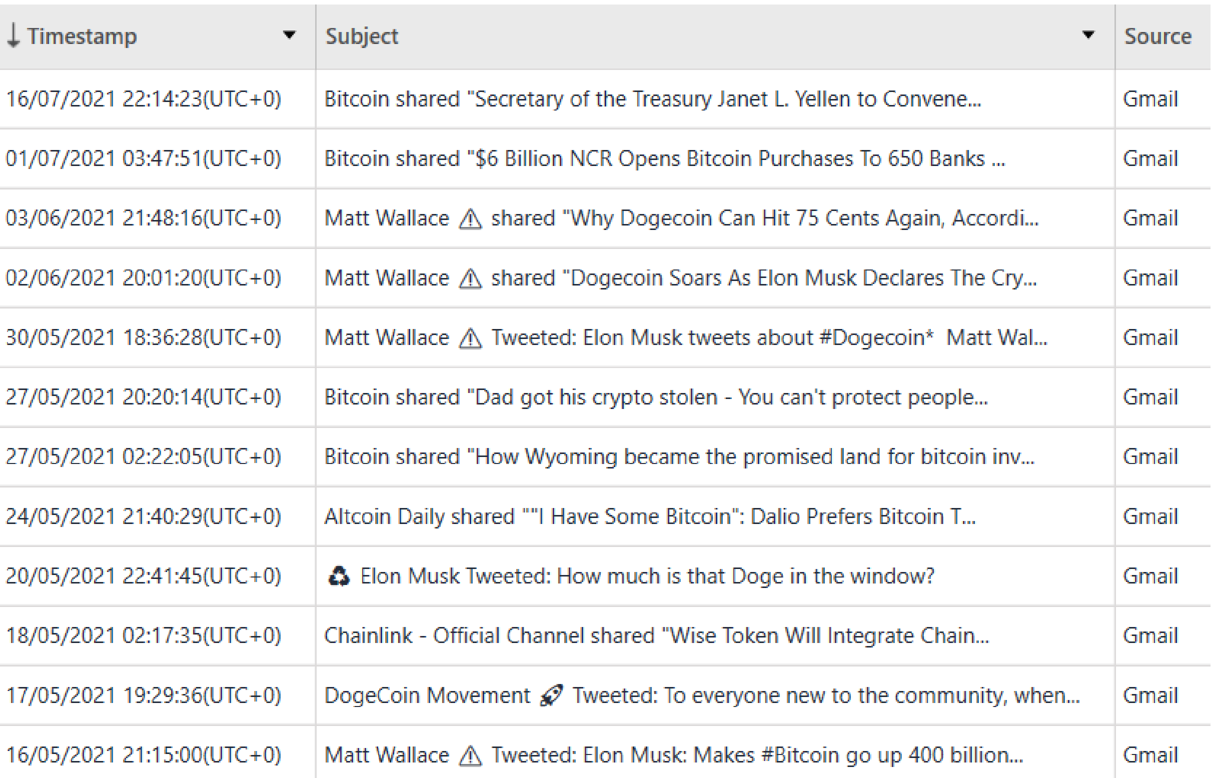
The app code is `com.flatfish.calculator` and the path is the following: `Dump/data/app/com.flatfish.calculator`.

The app presents itself as a calculator, but it is actually used to hide files. You can see the app icon in Figure 10.



Type	↓ Timestamp	P	Description	Source
Cookies	04/04/2021 04:40:04(UTC+0) [Creation time]		.venmo.com	Venmo
Cookies	04/04/2021 04:40:04(UTC+0) [Creation time]		.venmo.com	Venmo
Cookies	04/04/2021 04:40:04(UTC+0) [Accessed]		.venmo.com	Venmo
Cookies	04/04/2021 04:40:04(UTC+0) [Accessed]		.venmo.com	Venmo
Cookies	04/04/2021 04:40:04(UTC+0) [Creation time]		venmo.com	Venmo
Cookies	04/04/2021 04:39:00(UTC+0) [Creation time]		.venmo.com	Venmo
Cookies	04/04/2021 04:39:00(UTC+0) [Creation time]		.venmo.com	Venmo
Network Usages	05/05/2021 14:00:00(UTC+0) [Date ended]		Applications Ids: com.venmo SSId:...	Network Stats
Network Usages	05/05/2021 12:00:00(UTC+0) [Date started]		Applications Ids: com.venmo SSId:...	Network Stats
Network Usages	05/05/2021 10:00:00(UTC+0) [Date ended]		Applications Ids: com.venmo SSId:...	Network Stats
Network Usages	05/05/2021 08:00:00(UTC+0) [Date started]		Applications Ids: com.venmo SSId:...	Network Stats

Figure 8: Some activities of the smartphone related to the app *Venmo*.



↓ Timestamp	Subject	Source
16/07/2021 22:14:23(UTC+0)	Bitcoin shared "Secretary of the Treasury Janet L. Yellen to Convene...	Gmail
01/07/2021 03:47:51(UTC+0)	Bitcoin shared "$6 Billion NCR Opens Bitcoin Purchases To 650 Banks ...	Gmail
03/06/2021 21:48:16(UTC+0)	Matt Wallace ⚠ shared "Why Dogecoin Can Hit 75 Cents Again, Accordi...	Gmail
02/06/2021 20:01:20(UTC+0)	Matt Wallace ⚠ shared "Dogecoin Soars As Elon Musk Declares The Cry...	Gmail
30/05/2021 18:36:28(UTC+0)	Matt Wallace ⚠ Tweeted: Elon Musk tweets about #Dogecoin* Matt Wal...	Gmail
27/05/2021 20:20:14(UTC+0)	Bitcoin shared "Dad got his crypto stolen - You can't protect people...	Gmail
27/05/2021 02:22:05(UTC+0)	Bitcoin shared "How Wyoming became the promised land for bitcoin inv...	Gmail
24/05/2021 21:40:29(UTC+0)	Altcoin Daily shared ""I Have Some Bitcoin": Dalio Prefers Bitcoin T...	Gmail
20/05/2021 22:41:45(UTC+0)	♻ Elon Musk Tweeted: How much is that Doge in the window?	Gmail
18/05/2021 02:17:35(UTC+0)	Chainlink - Official Channel shared "Wise Token Will Integrate Chain...	Gmail
17/05/2021 19:29:36(UTC+0)	DogeCoin Movement 🚀 Tweeted: To everyone new to the community, when...	Gmail
16/05/2021 21:15:00(UTC+0)	Matt Wallace ⚠ Tweeted: Elon Musk: Makes #Bitcoin go up 400 billion...	Gmail

Figure 9: Some Twitter notifications about cryptocurrency.

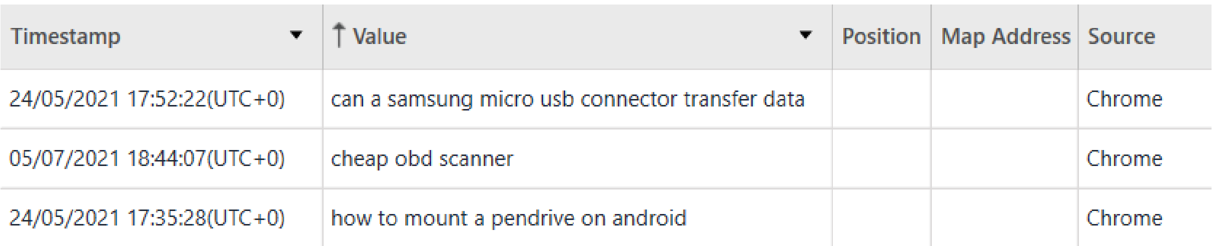
Figure 10: Icon of the app *Calculator*.

2.6 External drives

I found the some pictures related to *Android USB OTG*, which is a standard that allows mobile devices to connect to external drives.

In addition, I found that Heisenberg installed the apps *ANT Radio Service* and *ANT+ Plugins Service*, which are used to connect to external devices.

Looking at his web searches, I noticed that he looked for *can a samsung micro usb connector transfer data*, *how to mount a pendrive on android* and *cheap obd scanner* (see Figure 11).



Timestamp ▼	↑ Value ▼	Position	Map Address	Source
24/05/2021 17:52:22(UTC+0)	can a samsung micro usb connector transfer data			Chrome
05/07/2021 18:44:07(UTC+0)	cheap obd scanner			Chrome
24/05/2021 17:35:28(UTC+0)	how to mount a pendrive on android			Chrome

Figure 11: Web searches concerning external drives.

Finally, I found the app *BlueDriver OBD2 Scan Tool*, which is used to scan a vehicle. BlueDriver is a dongle that connects to the OBD2 port of a vehicle and sends data to a smartphone via Bluetooth. You can see the device in Figure 12.

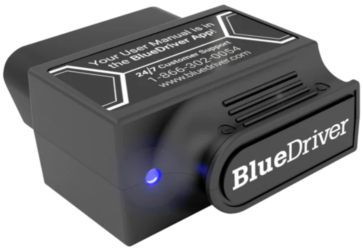


Figure 12: Device *BlueDriver*.

2.7 Hidden image

Thanks to the search bar, I found the image with the following MD5 hash: `066858f4b1971b0501b9a06296936a34`.

The path is `Dump/data/data/com.flatfish.cal.privacy/cache/image_manager_disk_cache/7ae6e97ba4ad0d693413273d6e270a412af3331a9c96c7a9049e3ae9b6047c9d.0`.

We can see that the picture was hidden with the app *HideX: Calculator Lock, App Hider and Photo Vault* (see Section 2.5): I luckily found it in the cache of the app (see Figure 13).

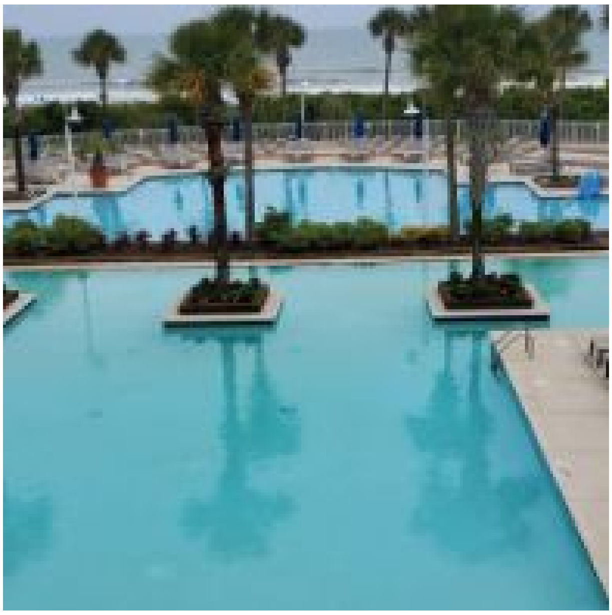


Figure 13: Hidden image.

2.8 Meeting with +15402993169

I found the messages exchanged with `+15402993169`: you can see part of the messages in Figure 2f, where the meeting is arranged. They planned to meet on 20/07/2021 at 19:00 at the Washington Street Tennis Court.

2.9 Signal app usage

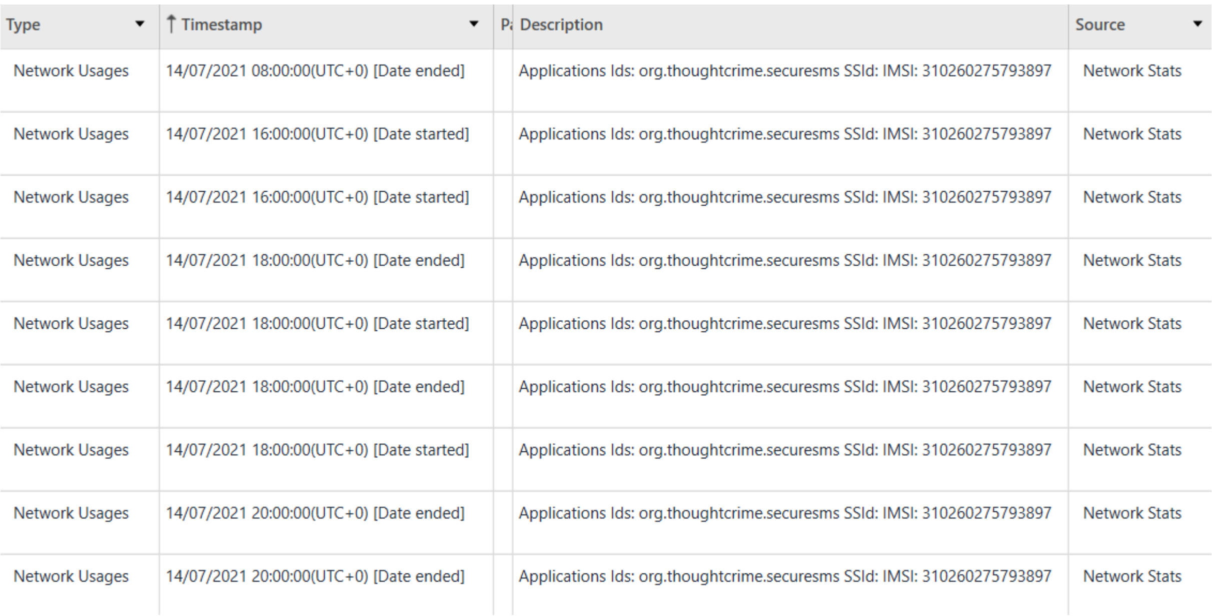
To check the last usages of the app Signal [6] on 14/07/2021, I used the timeline tool, given that the app code is `org.thoughtcrime.securesms`. You can see part of the timeline in Figure 14.

References

[1] Cellebrite. *Cellebrity Reader*. URL: https://www.cellebrite.com/en/reader/ (visited on 10/2023).

[2] Alexis Brignoni. *ALEAPP*. URL: https://github.com/abrignoni/ALEAPP (visited on 10/2023).

[3] *Venmo*. URL: https://venmo.com (visited on 10/2023).



Type	Timestamp	Pa	Description	Source
Network Usages	14/07/2021 08:00:00(UTC+0) [Date ended]		Applications Ids: org.thoughtcrime.securesms SSId: IMSI: 310260275793897	Network Stats
Network Usages	14/07/2021 16:00:00(UTC+0) [Date started]		Applications Ids: org.thoughtcrime.securesms SSId: IMSI: 310260275793897	Network Stats
Network Usages	14/07/2021 16:00:00(UTC+0) [Date started]		Applications Ids: org.thoughtcrime.securesms SSId: IMSI: 310260275793897	Network Stats
Network Usages	14/07/2021 18:00:00(UTC+0) [Date ended]		Applications Ids: org.thoughtcrime.securesms SSId: IMSI: 310260275793897	Network Stats
Network Usages	14/07/2021 18:00:00(UTC+0) [Date started]		Applications Ids: org.thoughtcrime.securesms SSId: IMSI: 310260275793897	Network Stats
Network Usages	14/07/2021 18:00:00(UTC+0) [Date ended]		Applications Ids: org.thoughtcrime.securesms SSId: IMSI: 310260275793897	Network Stats
Network Usages	14/07/2021 18:00:00(UTC+0) [Date started]		Applications Ids: org.thoughtcrime.securesms SSId: IMSI: 310260275793897	Network Stats
Network Usages	14/07/2021 20:00:00(UTC+0) [Date ended]		Applications Ids: org.thoughtcrime.securesms SSId: IMSI: 310260275793897	Network Stats
Network Usages	14/07/2021 20:00:00(UTC+0) [Date ended]		Applications Ids: org.thoughtcrime.securesms SSId: IMSI: 310260275793897	Network Stats

Figure 14: Activities of the smartphone related to the app *Signal*.

[4] *Calculator*. URL: `https://fr.apkshub.com/app/com.flatfish.cal.privacy` (visited on 10/2023).

[5] *BlueDriver OBD2 Scan Tool*. URL: `https://play.google.com/store/apps/details?id=com.lemurmonitors.bluedriver&hl=en` (visited on 10/2023).

[6] *Signal*. URL: `https://signal.org` (visited on 10/2023).