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 3.1.9; 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.

Content	MD5
Video of the arrest	1fb629ceb7e03948032448b6af978c94
Hidden image	066858f4b1971b0501b9a06296936a34
1st photo of the car	626e1bf6821aa7d3212727ee3bf9c63d
2nd photo of the car	13c3ebfb60c5ec08893c233ce42a3643
3rd photo of the car	dd27d1cf0fbcbd654c27c65aeb7f0efa
Native messages DB	af39b6fbe58e2ef549ea2089f164763c
Instagram messages DB	ccc30adbe925068c642f96c8eb2b9b80
Chrome cache picture	505fe0c5db1342818ed42089e2ba1edb
System packages	cd3b0e339b44cf03945a2926bddd15a1

Table 1: Checksums of important files.

Content	MD5
20210703_192737.jpg	038744fe39f45d0244dc608fca2fab56
20210703_192751.jpg	af34c57432d5b3f618b7d82361e9b556
20210703_192759.jpg	6baa8d4847e75a506a1e672b7242d663
20210703_192806.jpg	37c5342fd43d988b26c78c918b267751
20210703_192822.jpg	5bba7e07e07899a7b6b76b947add96b5
20210703_192830.jpg	0819ea4063e283481794b5cc60cb9810
20210703_192836.jpg	670129451ce9faeab6732a6d4e9222df
20210703_192839.jpg	7a33ec7e929bfaa2f9f35b5e88c2c38d
20210703_192901.jpg	e2f0e4d078508b20d03d5ce94557f1de
20210703_192907.jpg	26ef1f2bab90414dd29c770c23cb5b68

Table 2: Checksums of the photos of the cars.

1.4 Hash values

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 tables 1 and 2.

1.5 Findings

There are numerous files and applications concerning automobiles, as well as pictures of cars. The majority of these photos are simply related to the apps installed on the smartphone.

Between the installed apps, I report the following:

- **Venmo** [3]
- **Twitter**
- **HideX: Calculator Lock, App Hider and Photo Vault** [4]
- **Signal** [5]
- **CarGurus**
- **Autotrader**

- **Cartomizer**

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 was conducted in the native messages app of the smartphone (you can see the hash of the DB containing the messages in the table 1).

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.

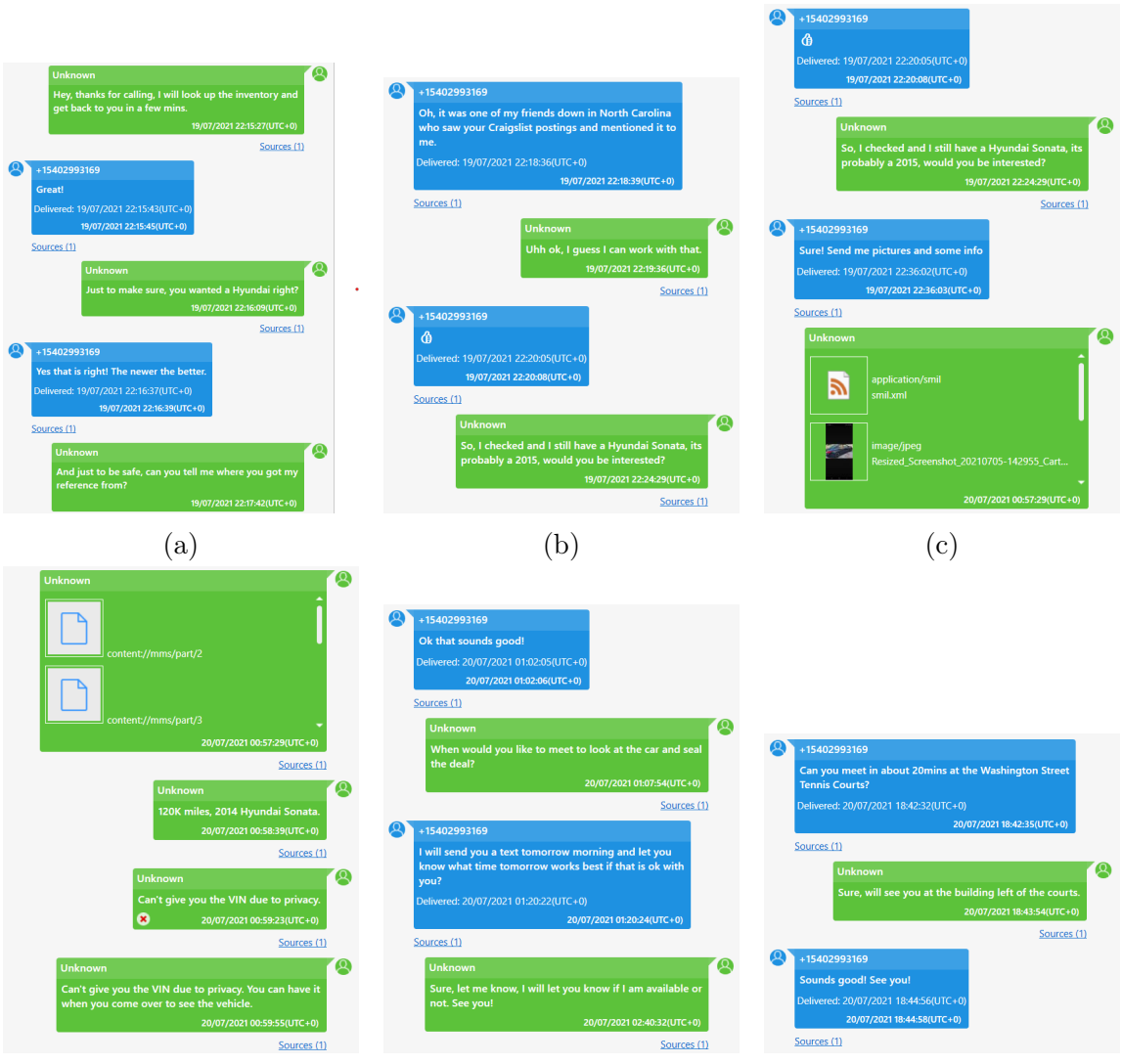
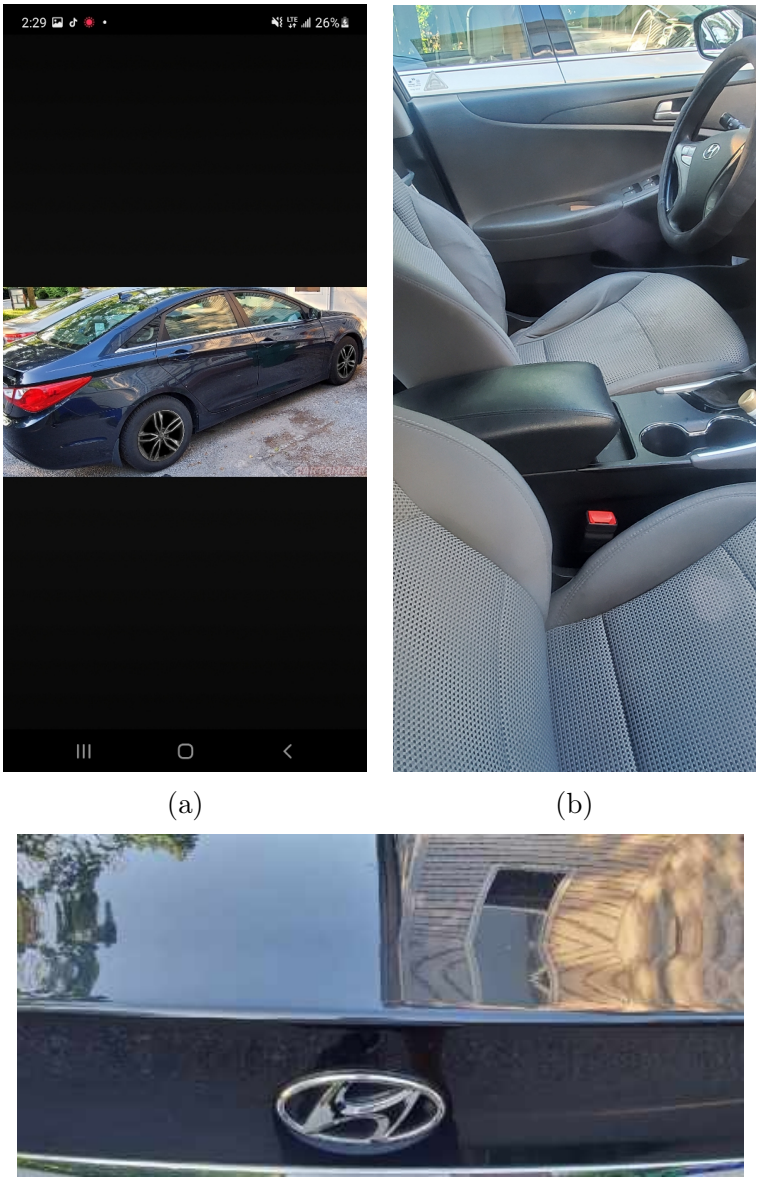


Figure 2: Screenshots of the messages exchanged with `+15402993169`.

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`



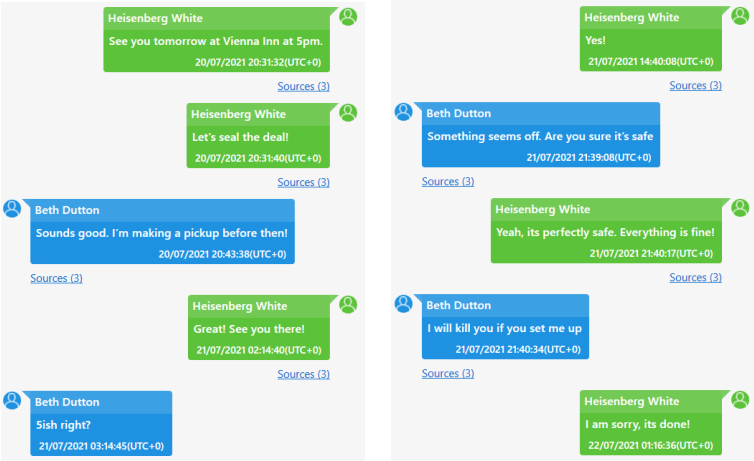
(a) (b)

(c)

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

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

You can see the messages in Figure 4 and the hash of the DB containing Instagram direct messages in the table 1.



(a) (b)

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

As I already mentioned, there are many pictures of cars in his smartphone, but they are related to the apps installed on the smartphone. So I looked for pictures with capture time in the DCMI folder: in this way we can suppose that the pictures were taken by Heisenberg. I found 10 pictures of cars in this way, which are shown in Figure 5. All the pictures are in the folder `Dump/data/media/0/DCIM` and you can check their names and hashes in the table 2.

Since I didn't find any other message with other contacts, I suppose he was conducting his main business in the app Signal [5], which is an end-to-end encrypted messaging app. I found numerous activities related to this app in the timeline.

Finally, the presence of numerous apps related to buying and selling cars, such as *CarGurus* and *Autotrader*, could be evidence of him selling cars on these apps.

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.

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 7.

(a) (b) (c) (d) (e) (f) (g) (h) (i) (j)

Figure 5: Pictures of cars with capture time.

I retrieved the network activities in the file at the path: `Dump/data/system/packages.xml`.

You can see the hash of the file in the table 1.

2.4 Interest in cryptocurrency

I noticed the presence of the app *Venmo* (see Figure 8), which is an app used to manage crypto wallets. I checked the timeline to see if there are any activities related to this app

Figure 6: Frame of the video showing the arrest.

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 7: Network activities of the smartphone after the arrest.

and I found numerous network activities related to it. You can see part of the timeline in Figure 9.

Moreover, checking Twitter notifications in Gmail, I found numerous news about cryptocurrency: he follows accounts as *Bitcoin News* and *Bitcoin*. See Figure 10 for some of the notifications.

Figure 8: Icon of the app *Venmo*.

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

2.5 File hiding or encryption

Looking at Heisenberg's web searches I found different searches related to file hiding and encryption, such as *hidden photos app*.

I found the app *HideX: Calculator Lock, App Hider and Photo Vault* [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 11.

2.6 External drives

I found a picture in the Chrome cache related to *Android USB OTG* (see Figure 13), which is a standard that allows mobile devices to connect to external drives. You can see

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 10: Some Twitter notifications about cryptocurrency.

Figure 11: Icon of the app *HideX: Calculator Lock, App Hider and Photo Vault*.

the hash of the picture in the table 1 and the path is the following: `Dump/data/data/com.android.chrome/cache/Cache/ff922abbaff591ef_0/android-usb-otg.jpg`.

Looking indeed at his web searches, I noticed that he searched for *can a samsung micro usb connector transfer data* and *how to mount a pendrive on android* (see Figure 12).

Given these information, I suppose that he wanted to connect a pendrive to his smartphone to transfer data.

Timestamp	Value	Position	Map Address	Source
24/05/2021 17:55:11(UTC+0)	can a samsung micro usb connector transfer data			Chrome
24/05/2021 17:36:59(UTC+0)	how to mount a pendrive on android			Chrome

Figure 12: Web searches concerning external drives.

Figure 13: Picture found in the cache of Chrome.

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 found it in the cache of the app (see Figure 14).

Figure 14: 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 [5] 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 15.

The last usage of the app on 14/07/2021 was at 20:00:00 (UTC+0).

Type	Timestamp	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 15: Activities of the smartphone related to the app *Signal*.

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).

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

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