

Technische Universität Wien

188.922 Digital Forensics

Lecturers: Dipl.Inf. (FH) Karsten Theiner and DI Dr. Martin Schmiedecker

Teaching Assistant: Christoph Kraus

Assignment 3: Smartphones

Bruno André Moreira Rosendo

e12302727

Due Date: December 20, 2023

Submitted: December 18, 2023

Contents

1	Purpose	1
2	Procedure	2
3	Analysis	3
3.1	Are there clues or evidence for Heisenberg dealing with (stolen) cars?	3
3.2	Heisenberg used his cellphone during the arrest. Did he create any recordings of the arrest?	8
3.3	Are there any hints that the police did not quite follow best practices in handling the cellphone during/after the arrest? If so, what did they do wrong?	8
3.4	Are there any clues for Heisenberg taking an interest in cryptocurrency?	11
3.5	Did Heisenberg use any apps for file hiding or encryption?	11
3.6	Are there any clues for Heisenberg connecting or planning to connect external drives to his Cellphone?	13
3.7	Was the image with the MD5 hash “066858f4b1971b0501b9a06296936a34” hidden by Heisenberg? If yes, what app was used?	13
3.8	Where did Heisenberg plan to meet with the owner of the telephone number “+15402993169”?	16
3.9	At which time(s) did Heisenberg actively use the Signal app on 2021-07-14?	19

1 Purpose

This assignment was designed to support the investigation into someone known as Heisenberg, who was arrested for allegedly dealing with stolen cars. The focus of the task was to analyze Heisenberg's smartphone as part of this process. This assignment was undertaken as part of a Digital Forensics course, wherein students were assigned the role of forensic analysts responsible for conducting this fictional investigation.

To kickstart the process, the students were given an image containing the file system of Heisenberg's Android phone. The goal is to use this image to answer a few questions that are proposed about the case, which are detailed in section 3.

This project's primary challenge is acquiring proficiency in the techniques for retrieving, analyzing, and documenting information from a smartphone file system. The Cellebrite Reader and ALEAPP software tools were suggested for the analysis, providing hands-on experience in digital forensics for the participating students.

2 Procedure

After downloading and extracting the smartphone's image, and prior to anything else, it is important to hash the image to guarantee that any modifications made to it do not alter its content in any manner. To ensure the ability to return to the initial state, one option could be to redownload it; however, a safer approach is to duplicate its contents into a new file. The hashes of both files were stored and compared throughout the investigation:

```
md5sum smartphone-image.zip > hash.txt  
md5sum smartphone-image-copy.zip > hash-copy.txt  
cat hash.txt  
XX  smartphone-image.zip  
cat hash-copy.txt  
XX smartphone-image-copy.zip
```

After hashing the image, the first actions involved using the Cellebrite Reader (v7.59.0.36) and ALEAPP (v3.1.9) tools to scrutinize the smartphone. The generated reports from these tools were subsequently utilized in the investigation to address the questions outlined in the assignment.

3 Analysis

The subsequent section responds to all the assignment's specific questions and assesses the results of the investigation according to the reports generated in section 2.

3.1 Are there clues or evidence for Heisenberg dealing with (stolen) cars?

There are numerous compelling indicators strongly suggesting Heisenberg's involvement with cars, and there is specific evidence hinting at the potential theft of these cars. Utilizing ALEAPP to inspect the applications installed on his phone (Figure 1), we can discern the presence of the following suspicious apps by searching the app ID in Google Play:

- **Cartomizer - Wheels Visualizer:** Enables the visualization of wheels on personal vehicles, implying a connection to the trade of cars.
- **Autotrader, CARFAX, CarGurus:** Apps designed for buying and selling used cars. The simultaneous use of multiple apps suggests Heisenberg's involvement in the car trade.
- **Car info - Car Data, Cars Specs:** A comprehensive database providing information about various car models.
- **Instant Checkmate Search:** One among several apps installed for conducting background checks on individuals, potentially used to vet potential car buyers.
- **BlueDriver OBD2 Scan Tool:** An app offering detailed information about car models, including specific mechanical details.
- **ORTO:** An app allowing the scanning of car plates for information on car history and ownership.

ALEAPP 3.1.9		Installed Apps report					
GOOGLE MAPS TEMP VOICE GUIDANCE							
Google Maps Temp Voice Guidance							
GOOGLE MAPS VOICE GUIDANCE							
Google Maps Voice Guidance							
GOOGLE NOW & QUICKSEARCH							
Recent Searches & Google Now							
Searches & Personal assistant							
GOOGLE PHOTOS							
Google Photos (gphotos-1) - Local Media							
Google Photos (gphotos0) - Cache							
Google Photos (gphotos0) - Local Media							
GOOGLE PLAY							
Google Play Searches							
GROUPME							
HideX - Locked Apps							
IMAGE MANAGER CACHE							
Image Manager Cache							
INSTALLED APPS							
App Updates (Frosting.db)							
Google Play Links for Apps							
Installed Apps (GMS)							
Installed Apps (GMS).0							
		Show: 15 entries	Search:				
Bundle ID	Version Code	SHA-256 Hash					
android.autoinstalls.config.samsung	1008	3d7db7b8e266555068ea1f4ab0e4db44503a62296cf68a0ba8351eb87e781d6d					
app.cartomizer	241020104	e0686c3c372753da203fb494fd5c91e1410c45988fbba3fb266b1552467f9c5					
app.greyshirts.ssiscapture	30	f50065c868619929e6a7848ade1cc8bf61935e4dd252885de59686a578a901d					
catching.cheatingspouseapp.app	9	8afa8d6361222fd1e56958edbf1558138e22ba14123e392aa184fc78e334663					
com.android.chrome	410410683	c560ad53c55f6a7e62d1ca0153319c90432fa1615cbffff894de8080ec29208df					
com.android.chrome	438910534	fba4237dbafe5423675e93a7a59fddeb734bfed9e4319a5b6731c77698e7e4b					
com.android.chrome	443009134	5ea68587b1fc9592fe9d433a8d4abfcfa5772fbfaa1544d4f286a3c9c1eb2f					
com.android.chrome	443021034	f3d6d480aaafac41369fc25cb5a91725d28044fc6bc98768921d4d2a6274de8					
com.android.chrome	447208834	f4968a4c4a2b8b5526e2aa54c93479b9deb1d7cb8b04452f1024f150ba7d25e1ec					
com.android.chrome	447210134	ec05ed476ff195887df0cb006c776aa71707e7f6764984827e2205730f38					
com.android.vending	82211810	f09146592e0cd29300bf2e7da772587162bd56e3539bdfde282f5938360e8d					
com.android.vending	82242510	558f3c6865bf2fd6b731a3ba2deec0ce6b242429b8127831aa119baa73eb5					
com.android.vending	82463110	c26ea36139c54a894dc75a8dbf99ac8e87221838797b20192700026578aa4c3					
com.android.vending	82472010	0ec8f116d9116d934b13a9bcd9c8e6cea7da36d79cdaf2b0e1600393bd8ae5					
com.android.vending	82472810	acf8fef821589fc348ca54b3e026ccf017d0080ede04f0ce09c227d499129					
Bundle ID	Version Code	SHA-256 Hash					

Figure 1: ALEAPP’s report showing the apps installed on the smartphone

Additionally, examining his text messages with potential buyers further confirms his involvement in dealing cars, as illustrated in Figure 3.

Furthermore, insights into Heisenberg’s financial challenges emerge, providing a potential explanation for his engagement with stolen cars. Notably, he had installed money-saving apps such as **T-Mobile Tuesdays** and **Upside: Fuel Rewards Cash Back**. Accessing his email history (Figure 4) reveals his exploration of new avenues to generate income. He was also searching the web for cheap OBD scanners, revealing his interest in car trading and low amount of cash (Figure 5).

Finally, it is noteworthy that he had installed an app named **Cheating Spouse Catching**, suggesting potential issues in his personal life and raising concerns about his mental health.

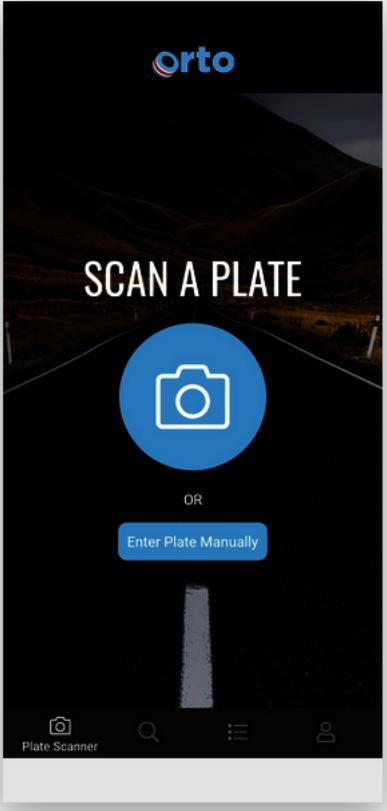
Snapshot_Image	Recent_Image
 A screenshot of the ORTO mobile application. The screen is predominantly black. At the top center, the word "orto" is written in a blue, lowercase, sans-serif font. Below it, the text "SCAN A PLATE" is displayed in large, white, uppercase letters. In the center is a large blue circular button containing a white camera icon. Below this button, the word "OR" is centered in small white capital letters. Underneath "OR" is a blue rectangular button with the white text "Enter Plate Manually". At the bottom of the screen, there is a navigation bar with four icons: a camera icon labeled "Plate Scanner", a magnifying glass icon, a three-dot menu icon, and a person icon.	No Image

Figure 2: A snapshot of the app ORTO, used by Heisenberg

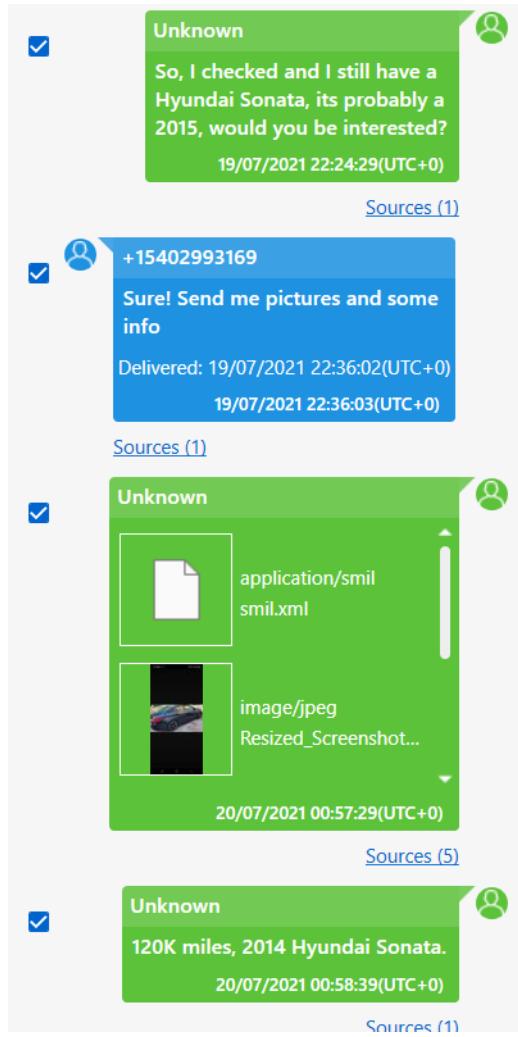


Figure 3: An SMS conversation with a potential car buyer, exported from Cellebrite Reader

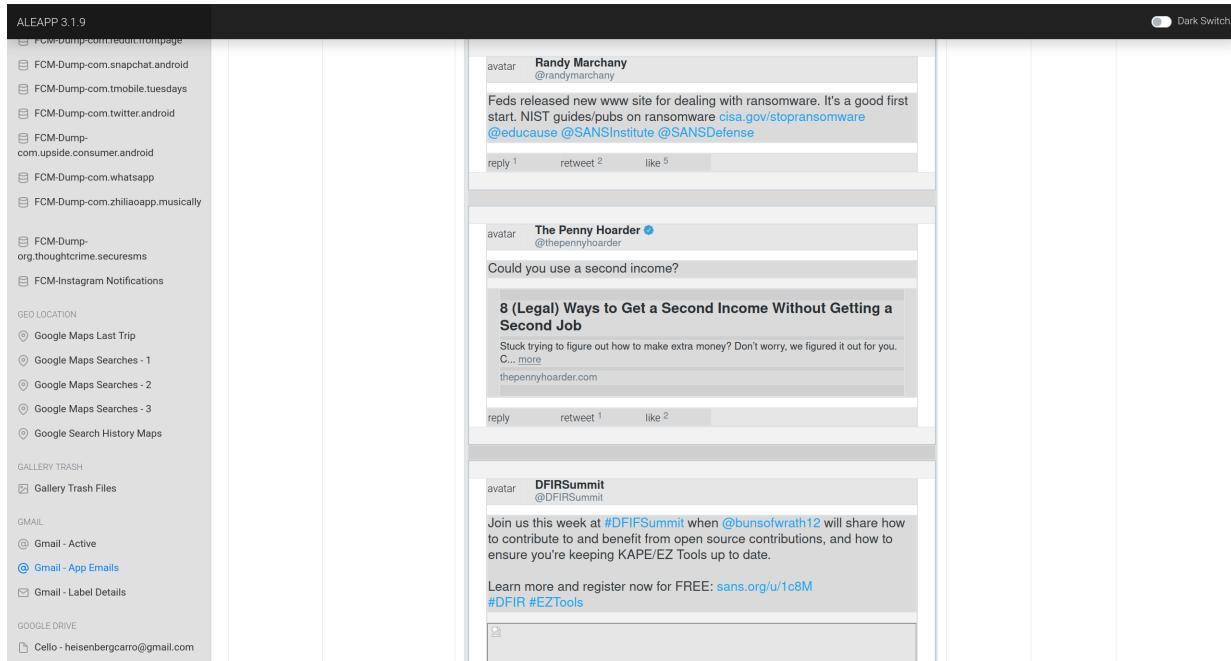


Figure 4: ALEAPP's email report showing activity on a Tweet related to extra income

ALEAPP 3.1.9		
⊕ FCM-Dump.com.readthispage		Dark Switch
└ FCM-Dump.com.snapchat.android		
└ FCM-Dump.com.tmobile.tuesday		
└ FCM-Dump.com.twitter.android		
└ FCM-Dump.com.uside.consumer.android		
└ FCM-Dump.com.whatsapp		
└ FCM-Dump.com.zhiliaoapp.musically		
└ FCM-Dump.org.thoughtcrime.securesms		
└ FCM-Instagram Notifications		
GEO LOCATION		
└ Google Maps Last Trip		
└ Google Maps Searches - 1		
└ Google Maps Searches - 2		
└ Google Maps Searches - 3		
└ Google Search History Maps		
GALLERY TRASH		
└ Gallery Trash Files		
GMAIL		
└ Gmail - Active		
└ Gmail - App Emails		
└ Gmail - Label Details		
GOOGLE DRIVE		
└ Cello - heisenbergcarro@gmail.com		

ALEAPP 3.1.9		
⊕ Browser - Web Visits-01		Dark Switch
└ Browser - Web Visits-02		
└ Browser - Web Visits		
└ Chrome - Autofill - Entries-01		
└ Chrome - Autofill - Entries-02		
└ Chrome - Autofill - Entries		
└ Chrome - Keyword Search Terms-01		
└ Chrome - Keyword Search Terms-02		
└ Chrome - Keyword Search Terms		
└ Chrome - Offline Pages-01		
└ Chrome - Offline Pages-02		
└ Chrome - Offline Pages		
└ Chrome - Search Terms-01		
└ Chrome - Search Terms-02		
└ Chrome - Search Terms		
└ Chrome - Web History-01		
└ Chrome - Web History-02		
└ Chrome - Web History		
└ Chrome - Web Visits-01		
└ Chrome - Web Visits-02		
└ Chrome - Web Visits		
└ CLIPBOARD		
└ Clipboard Data		
└ DEVICE HEALTH SERVICES		
└ Turbo - Application Usage		

Figure 5: Web search revealing interest to buy a cheap OBD scanner

3.2 Heisenberg used his cellphone during the arrest. Did he create any recordings of the arrest?

Yes, by searching for videos recorded on the day of the arrest (20-07-2021) using Cellebrite Reader, a recording made during the arrest can be easily located. In this video, Heisenberg mistakenly believed that the police woman was a potential buyer for the car he possessed. When confronted, he attempted to deny his involvement with the stolen car, attributing the blame to someone named Beth. The recording is stored on his phone in the directory `"/Dump/data/media/0/DCIM/Camera/20210720_150222.mp4"`. A screenshot of the video is provided in Figure 6. The hash of the video is `"1fb629ceb7e03948032448b6af978c94"`. Note that it is also possible to find texts between Heisenberg and Beth, so the investigation should analyze her in the future as well.

3.3 Are there any hints that the police did not quite follow best practices in handling the cellphone during/after the arrest? If so, what did they do wrong?

Following the arrest and the seizure of the smartphone, standard protocols dictate isolating the phone to minimize external interactions. This typically involves implementing measures such as enabling airplane mode, removing the SIM card, and restricting access to various functionalities like Wi-Fi, mobile data, GPS, and Bluetooth. Additionally, shielding the device from external communications, for example, by using a Faraday bag, is a possible practice. If the device remains unused and lacks password protection, it is also advisable to turn it off.

However, it appears that these standard practices were not followed by the police, as there is significant phone activity observed after the arrest. Notably, activities such as Google Maps usage and geolocation information indicate that GPS and Wi-Fi connectivity



Figure 6: Screenshot of the video recorded during the arrest

were not prevented (Figure 7). Moreover, there is evidence of pictures being taken and USB devices connected (figures 8 and 9), as evident from the system logs, even after the phone was taken into custody for investigation. This oversight could potentially compromise the integrity of the evidence stored on the smartphone.

The screenshot shows the ALEAPP 3.1.9 interface. On the left is a sidebar with sections for FCM-Dump, GEO LOCATION, GALLERY TRASH, GMAIL, GOOGLE DRIVE, and GOOGLE DUO. The main panel is titled "Google Maps Last Trip report". It displays a table with the following data:

Timestamp	Directionality	Place	Latitude	Longitude	Data	
2021-07-22 04:17:27.026000+00.00	Start	Your location	37.2349758	-80.4365012	/dir/37.2349758,-80.4365012/Blacksburg,+VA /data=4m134m121m14e11m51m11s0x884d950adc06dcc3.0x86ceb8ea4842da2d2m21d-80.41393932d37.2295733m2f6e0f7e23e0	
2021-07-22 04:17:27.026000+00.00	Start	Your location	37.2349758	-80.4365012	/dir/37.2349758,-80.4365012/Blacksburg,+VA /data=4m134m121m14e11m51m11s0x884d950adc06dcc3.0x86ceb8ea4842da2d2m21d-80.41393932d37.2295733m2f6e0f7e23e0	
2021-07-22 04:17:27.026000+00.00	Start	Your location	37.2349758	-80.4365012	/dir/37.2349758,-80.4365012/Blacksburg,+VA /data=4m134m121m14e11m51m11s0x884d950adc06dcc3.0x86ceb8ea4842da2d2m21d-80.41393932d37.2295733m2f6e0f7e23e0	
2021-07-22 05:25:34.603000+00.00	End	Blacksburg, Virginia	37.2295733	-80.4139393		
2021-07-22 05:25:34.603000+00.00	End	Blacksburg, Virginia	37.2295733	-80.4139393		
	Timestamp	Directionality	Place	Latitude	Longitude	Data

Showing 1 to 6 of 6 entries

Figure 7: Evidence showing Google Maps information being tracked after the arrest

2021-07-22 19:07:06	event-log		0					com.samsung.android.MtpApplication	ACTIVITY_RI
2021-07-22 19:07:08	event-log		0					com.android.systemui	NOTIFICATION
2021-07-22 19:07:08	event-log		0					com.samsung.android.MtpApplication	ACTIVITY_P
2021-07-22 19:07:09	event-log		0					com.sec.android.app.launcher	ACTIVITY_R
2021-07-22 19:07:09	event-log		0					com.samsung.android.MtpApplication	ACTIVITY_S

Figure 8: System logs showing USB media activity after the arrest

com.samsung.android.MtpApplication	ACTIVITY_RESUMED	com.samsung.android.MtpApplication.USBConnection
com.android.systemui	NOTIFICATION INTERRUPTION	
com.samsung.android.MtpApplication	ACTIVITY_PAUSED	com.samsung.android.MtpApplication.USBConnection
com.sec.android.app.launcher	ACTIVITY_RESUMED	com.android.launcher3.uioverrides.QuickstepLauncher
com.samsung.android.MtpApplication	ACTIVITY_STOPPED	com.samsung.android.MtpApplication.USBConnection

Figure 9: System logs showing USB media activity after the arrest

3.4 Are there any clues for Heisenberg taking an interest in cryptocurrency?

Yes, we can find emails and Twitter activity related to cryptocurrencies, such as Bitcoin, Dogecoin and NFTs, as shown in figures 10 and 11.

3.5 Did Heisenberg use any apps for file hiding or encryption?

Indeed, a manual inspection of the apps installed on Heisenberg’s smartphone uncovered an application that disguises as a calculator. Contrary to its appearance, the primary function of this app is to hide other apps, files, and web history by securing them behind a secret code within the calculator interface. The app in question can be identified by its ID among the installed apps: *“com.flatfish.cal.privacy”*.

Another suspicious app associated with encryption is named *“Packet Capture”*, which aims to capture encrypted SSL packets through a man-in-the-middle attack. While this doesn’t involve file hiding, it does raise concerns about potential nefarious activities on Heisenberg’s part.

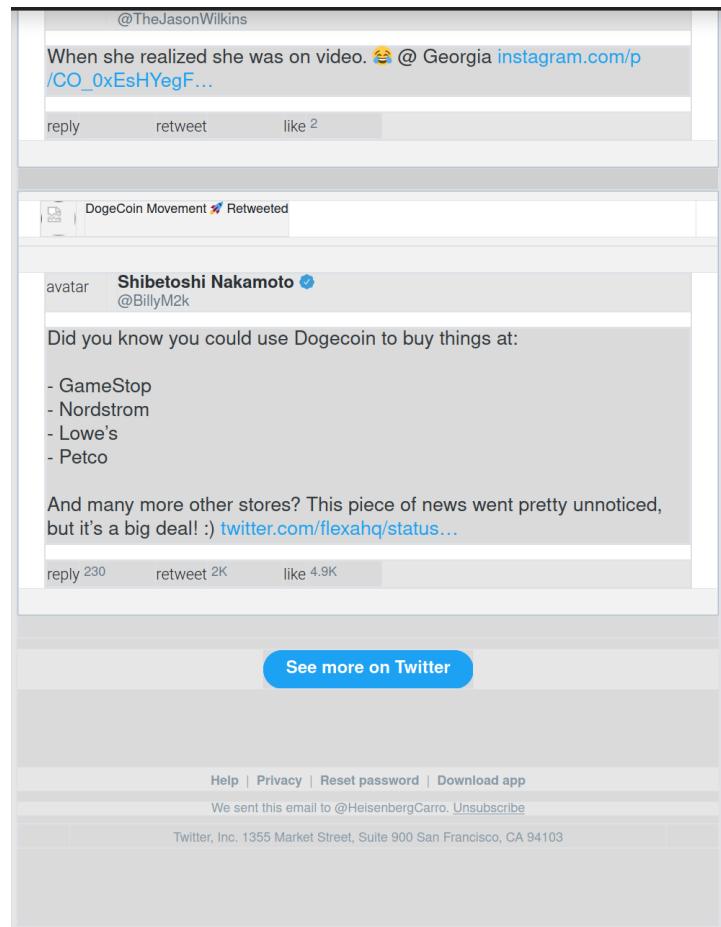


Figure 10: Twitter activity on Dogecoin

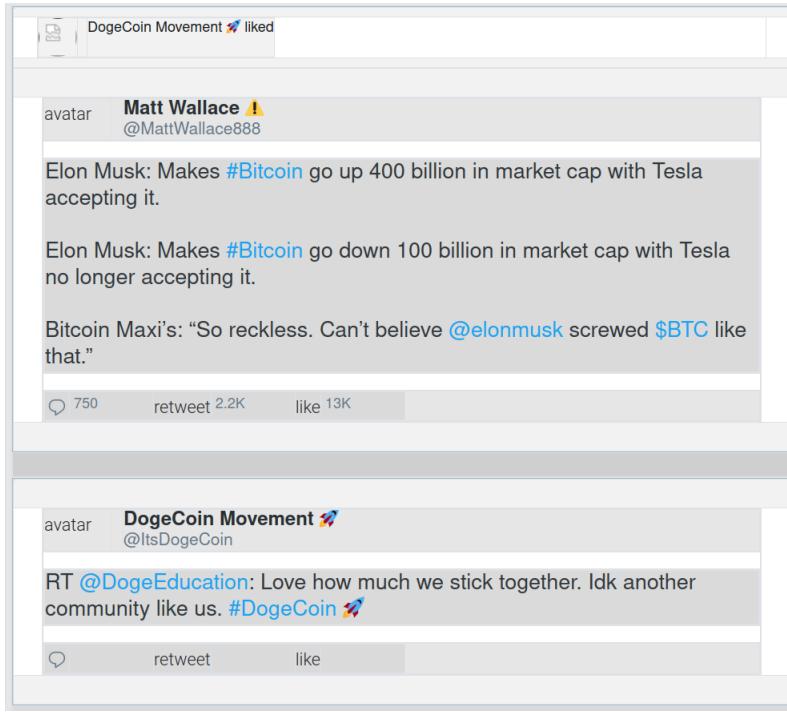


Figure 11: Twitter activity on Bitcoin and Dogecoin

3.6 Are there any clues for Heisenberg connecting or planning to connect external drives to his Cellphone?

Indeed, there is evidence of web searches indicating Heisenberg's interest in connecting a USB storage device to his smartphone, as depicted in Figure 12. Additionally, his search history includes queries for a micro USB adapter, suggesting a potential intention to facilitate the connection of the USB device, as illustrated in Figures 13 and 14.

3.7 Was the image with the MD5 hash “066858f4b1971b0501b9a06296936a34” hidden by Heisenberg? If yes, what app was used?

In Cellebrite Reader, searching for the file hash yields a result associated with the HideX application's cache directory, indicating that Heisenberg hid the file. The file is located at

Web History		Go to ▾
Title:	How to Connect USB Storage Devices to Your Android Phone Tom's Guide	
Last Visited:	24/05/2021 17:35:58(UTC+0)	
URL:	https://www.google.com/amp/s/www.tomsguide.com/amp/us/connect-usb-drive-to-android.news-21213.html	
Visits:		
Account:		
Artifact Family:		
Source Repository Path:		
Source:	Chrome	
Extraction:	Legacy	
Source file:	Heisenberg Samsung Full File System_22.zip/Dump/data/data/com.android.chrome/app_chrome/Default/History : 0x291FD (Table: visits, urls; Size: 393216 bytes)	

Figure 12: Web search for how to connect a USB storage device to an Android phone

Web History		Go to ▾
Title:	Samsung (GH96-09772A) OTG Adapter for Micro USB Devices - White – Simple Cell Shop	
Last Visited:	24/05/2021 17:54:56(UTC+0)	
URL:	https://www.googleadservices.com/pagead/aclk?sa=L&ai=DChcSEwiVw8yS8eLwAhUx8uMHHSYfAKEYABAEGgJ5bQ&ae=2&ohost=www.google.com&cid=C_AASEuRo3dwBZ14F6aUUTW38gtjYUw&sig=AOD64_1dAZIIQknYJ9dvHBY6MLYnTZd7DQ&ctype=5&q=&ved=2ahUKEwh28GS8eLwAhWGVTABHauJDAwQ8w56BAgBECo&dct=1&adurl=	
Visits:		
Account:		
Artifact Family:		
Source Repository Path:		
Source:	Chrome	
Extraction:	Legacy	
Source file:	Heisenberg Samsung Full File System_22.zip/Dump/data/data/com.android.chrome/app_chrome/Default/History : 0x2ADEC (Table: visits, urls; Size: 393216 bytes)	

Figure 13: Web search for a potential micro USB adapter

Searched Item		Go to ▾
Timestamp:	24/05/2021 17:55:11(UTC+0)	
Source:	Chrome	
Value:	can a samsung micro usb connector transfer data	
Search Results:		
Searched In:		
Origin:		
Account:		
Extraction:	Legacy	
Source file:		
Heisenberg Samsung Full File System_22.zip/Dump/data/data/ com.android.chrome/app_chrome/ Default/History : 0x2ACE4 (Table: visits, keyword_search_terms; Size: 393216 bytes)		

Figure 14: Web search to check if a micro USB connector can transfer data

"/Dump/data/data/com.flatfish.cal.privacy/cache/image_manager_disk_cache/
7ae6e97ba4ad0d693413273d6e270a412af3331a9c96c7a9049e3ae9b6047c9d.0". It is an image depicted in Figure 15.

3.8 Where did Heisenberg plan to meet with the owner of the telephone number “+15402993169”?

The planned meeting location can be ascertained by examining SMS messages between Heisenberg and the owner of the phone number. In one of the texts, detailed in Figure 16, it is revealed that they intended to meet at the Washington Street Tennis Courts. Additionally, it is noteworthy that the owner of this number is the same police officer who arrested him on the 20th of July.



Figure 15: The image hidden by Heisenberg using the HideX calculator

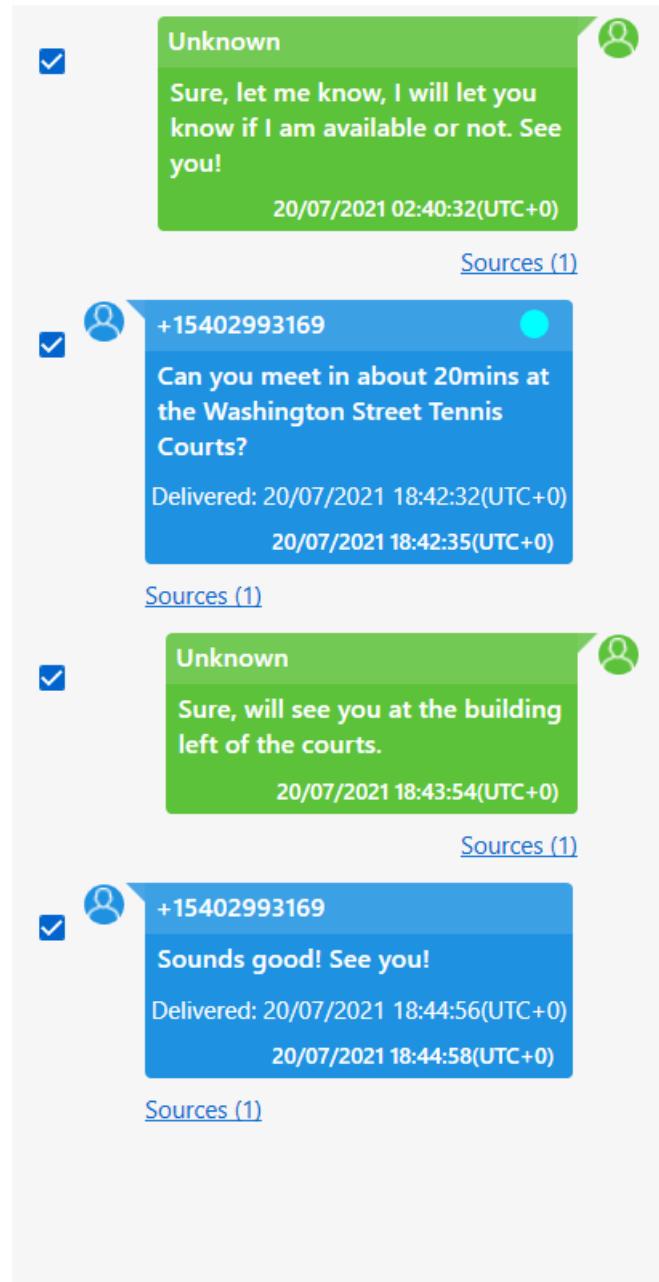


Figure 16: SMS messages revealing the meeting place between Heisenber and the cop

3.9 At which time(s) did Heisenberg actively use the Signal app on 2021-07-14?

To begin, it is essential to note that Signal's app ID is "*org.thoughtcrime.securesms*." Leveraging this information, ALEAPP was utilized to investigate app activity, revealing a substantial amount of activity between 18:38 and 18:40. This timeframe strongly indicates an exchange of messages. The corresponding evidence is presented in Figure 17.

ALEAPP 3.1.9			
□ Strings - SQLite Journal & WAL	2021-07-14 18:38:18.07	com.sec.android.app.launcher	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data_mirror/data_ce/null/0 /com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
SAMSUNG WEATHER CLOCK	2021-07-14 18:38:18.067	org.thoughtcrime.securesms	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data/data /com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
⌚ Samsung Weather Clock - Daily			
⌚ Samsung Weather Clock - Hourly	2021-07-14 18:38:18.067	org.thoughtcrime.securesms	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data/user /0/com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
⌚ Samsung Weather Clock - Info			
SAMSUNG_CMH	2021-07-14 18:38:18.067	org.thoughtcrime.securesms	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data_mirror/data_ce/null/0 /com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
⊕ Geodata	2021-07-14 18:38:24.899	org.thoughtcrime.securesms	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data/data /com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
SNAPCHAT	2021-07-14 18:38:24.899	org.thoughtcrime.securesms	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data/user /0/com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
⌚ Snapchat - Feeds			
⌚ Snapchat - Friends	2021-07-14 18:38:24.899	org.thoughtcrime.securesms	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data_mirror/data_ce/null/0 /com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
⌚ Snapchat - Identity Persistent			
⌚ Snapchat - Login Signup	2021-07-14 18:38:33.717	org.thoughtcrime.securesms	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data/data /com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
⌚ Snapchat - User Session Shared			
USAGE STATS	2021-07-14 18:38:33.717	org.thoughtcrime.securesms	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data/user /0/com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
↳ OS Version	2021-07-14 18:38:33.717	org.thoughtcrime.securesms	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data_mirror/data_ce/null/0 /com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
↳ UsageStats_0	2021-07-14 18:39:03.827	org.thoughtcrime.securesms	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data/data /com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
WHATSAPP	2021-07-14 18:39:03.827	org.thoughtcrime.securesms	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data/user /0/com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
⌚ WhatsApp - Contacts			
⌚ WhatsApp - Messages	2021-07-14 18:39:03.827	org.thoughtcrime.securesms	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data_mirror/data_ce/null/0 /com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
⌚ WhatsApp - User Profile			
WIFI PROFILES	2021-07-14 18:39:42.12	org.thoughtcrime.securesms	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data/data /com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
⌚ Wi-Fi Hotspot			
⌚ Wi-Fi Profiles	2021-07-14 18:39:42.12	org.thoughtcrime.securesms	/home/brosendo/Documents/Digital Forensics/A3/ALEAPP_Reports_2023-12-02_Saturday_141250/temp/Dump/data/user /0/com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml
WIPE & SETUP			

Figure 17: ALEAPP's report showing Signal's activity