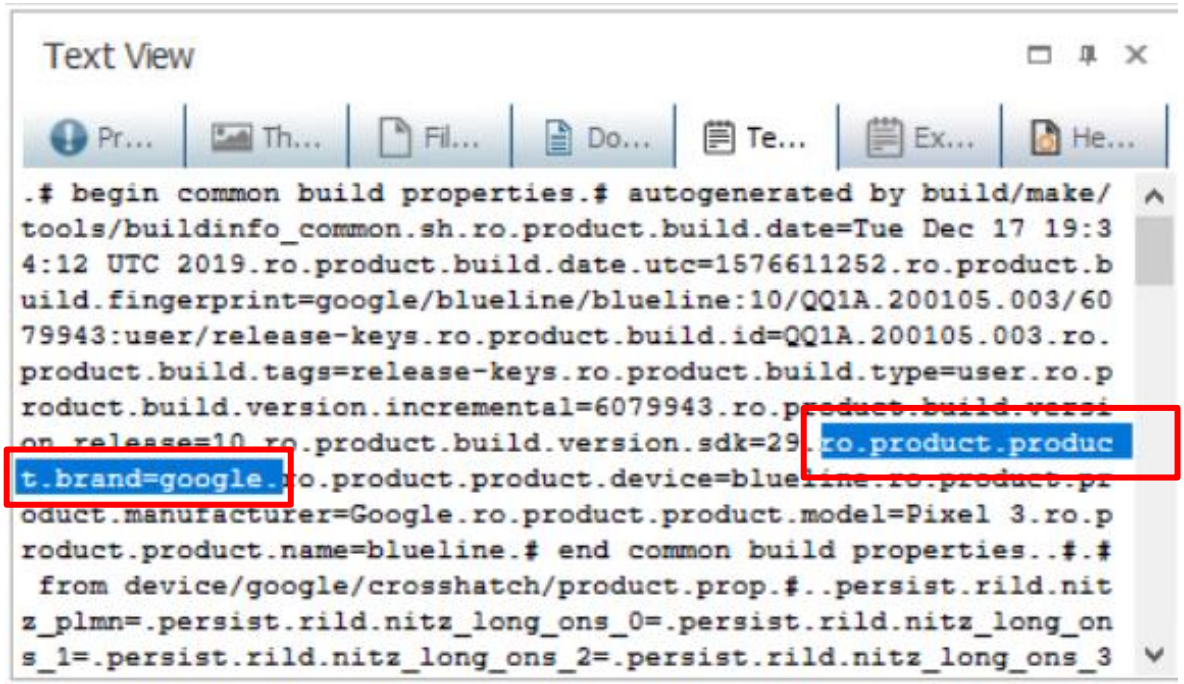
Question 1. What is the make, model, serial number of the device?

Answer: The files ***product/build.prop*** and ***system/build.prop*** store a wealth of information about the device, including its model, manufacturer, Android version, build number, kernel version, and various other system properties. This information is crucial for understanding the device's capabilities, potential vulnerabilities, and compatibility with forensic tools.

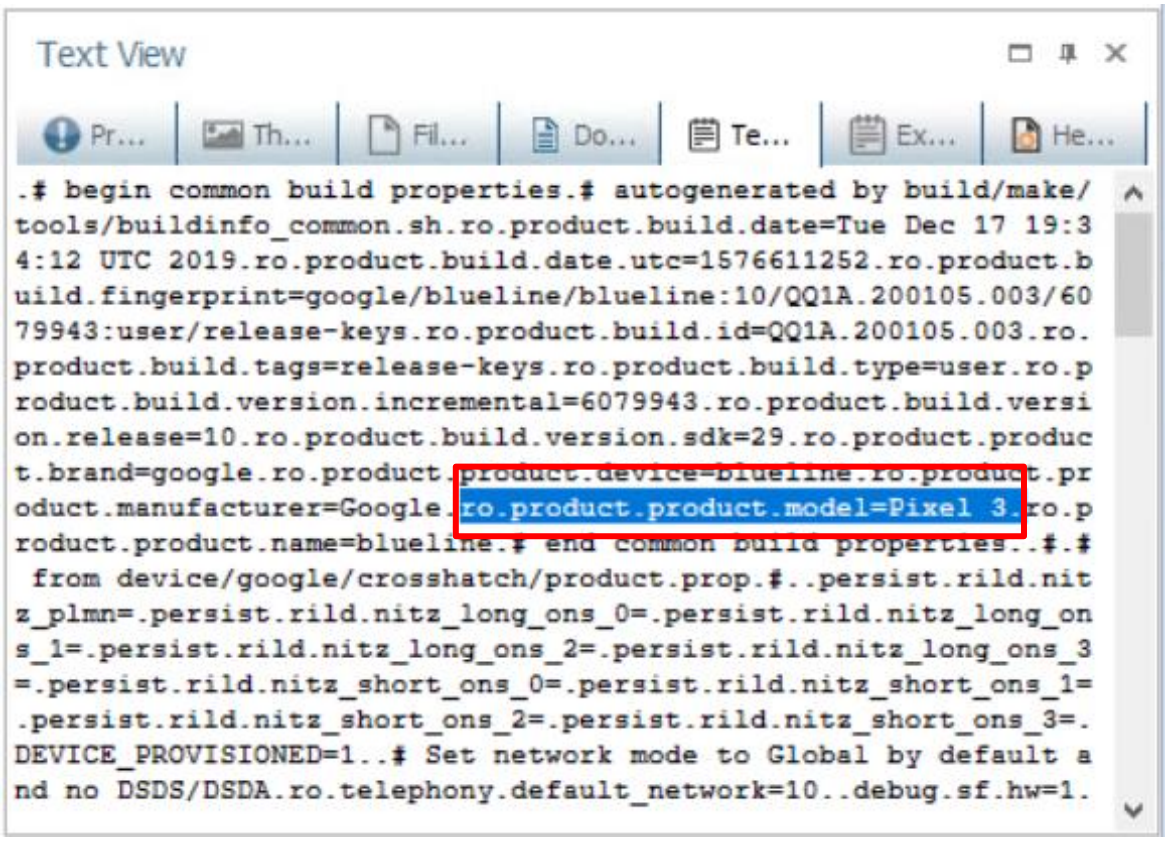
❖ **Why build.prop file:**

- The **build.prop** file is a system file in Android devices that contains a list of properties and settings used by the Android system. It's essentially a text file with key-value pairs that define various aspects of the device and its behavior.

1. **Device make:**
   - The device make or manufacturer is "**Google**". This is explicitly stated in the properties: **ro.product.product.brand=google** and **ro.product.product.manufacturer=Google.**
   - **Path:** e3://quiz2/Pixel 3/ArchiveRoot/Pixel 3/product?item=build.prop
   - **Evidence:**



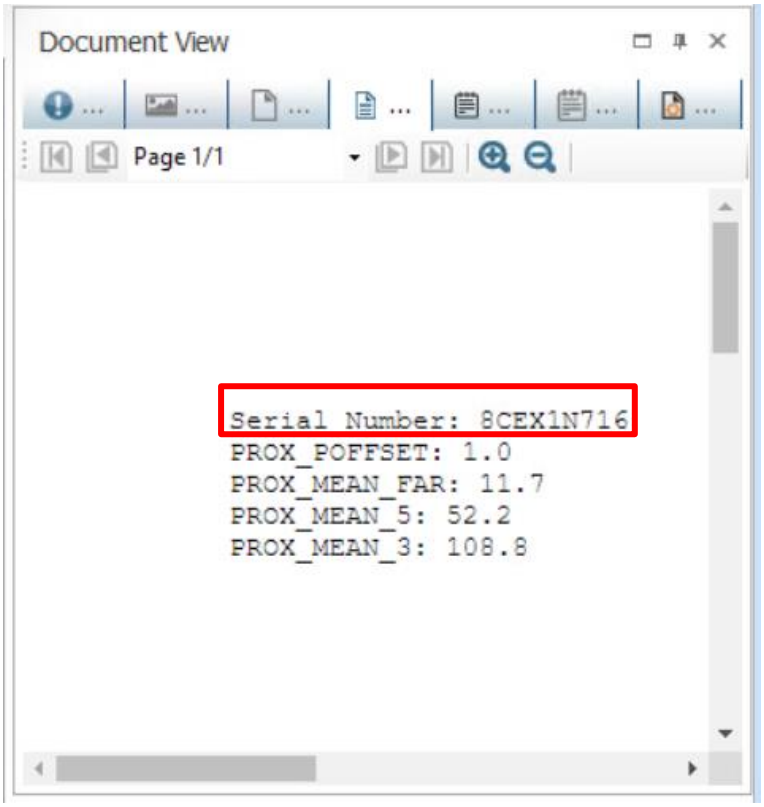
2. **Device model:**
   - The model of this device is "**Pixel 3**". This can be identified from **ro.product.product.model=Pixel 3**.
   - **Path:** e3://quiz2/Pixel 3/ArchiveRoot/Pixel 3/product?item=build.prop
   - **Evidence:**



3. **Device Serial Number:**
   - The serial number of device is **8CEX1N716**. The serial number was found in the **tmd2725_als_factory.txt** because this file contains hardware-specific configuration and calibration data for the device's ambient light sensor (ALS). The "**tmd2725**" refers to the model number of the sensor. Manufacturers often include the device's serial number in such files to uniquely identify the device and associate it with specific hardware components.

   - **Path:** e3://quiz2/Pixel 3/ArchiveRoot/Pixel 3/mnt/vendor/persist/sensors?item=tmd2725_als_factory.txt

- **Evidence:** The serial number information is likely stored in the persist partition. This partition holds persistent data that survives factory resets, including device-specific information like serial numbers, IMEI, and MAC addresses. It's a common location for manufacturers to store unique identifiers.



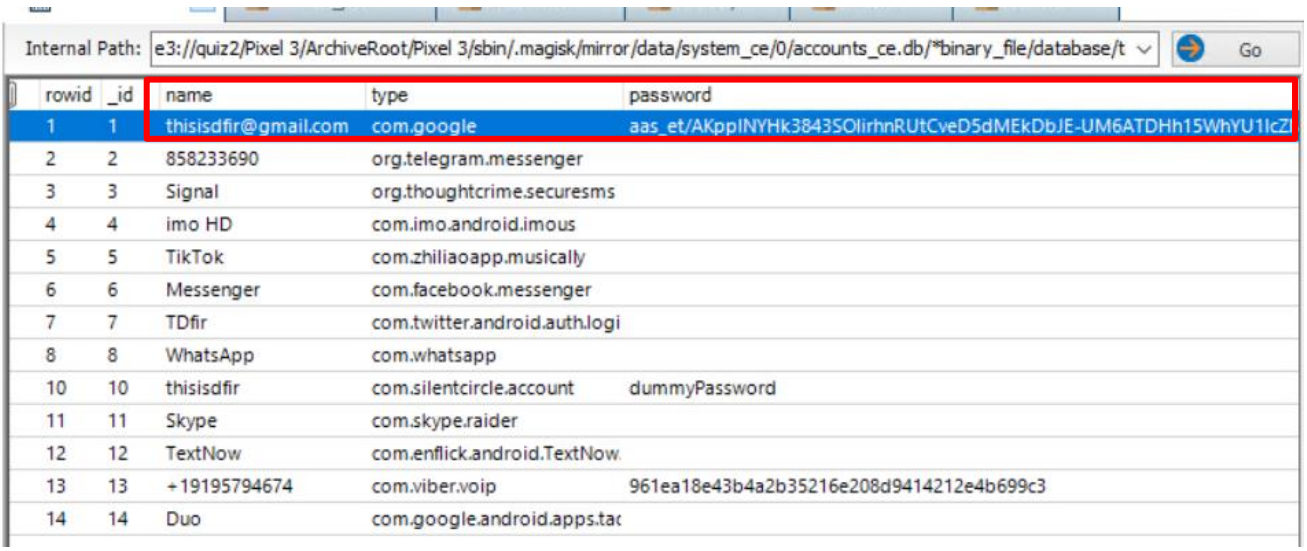
- **Verification:** To verify the acquired serial number, I have used an online tool to look up and verify the identity of the serial number.

Pixel-3 Analysis

Question 2. What is the Google account email and password of the device? (Encrypted password)

Answer: There is 1 google account associated with the device. The credentials of that account are:

- **Email**: thisisdfir@gmail.com
- **Name**: thisisdfir
- **Password(encrypted):**
  aas_et/AKppINYHk3843SOlirhnRUtCveD5dMEkDbJE-UM6ATDHh15WhYU1lcZNba5nhbrKUmsSReDEDBsCeGL7JPU4q-Yg4xnvw0l3EIJFTafNRpTQp9VWTc60f96ZOmBpTtd9rcFCO31RD2qnXx2XDpWJ7u0jnSIu78gwiCGPaUpaegazIAQxH1Pa-1h0VwGXElenMabM5yUWpAIhzpatx3xMFoA=

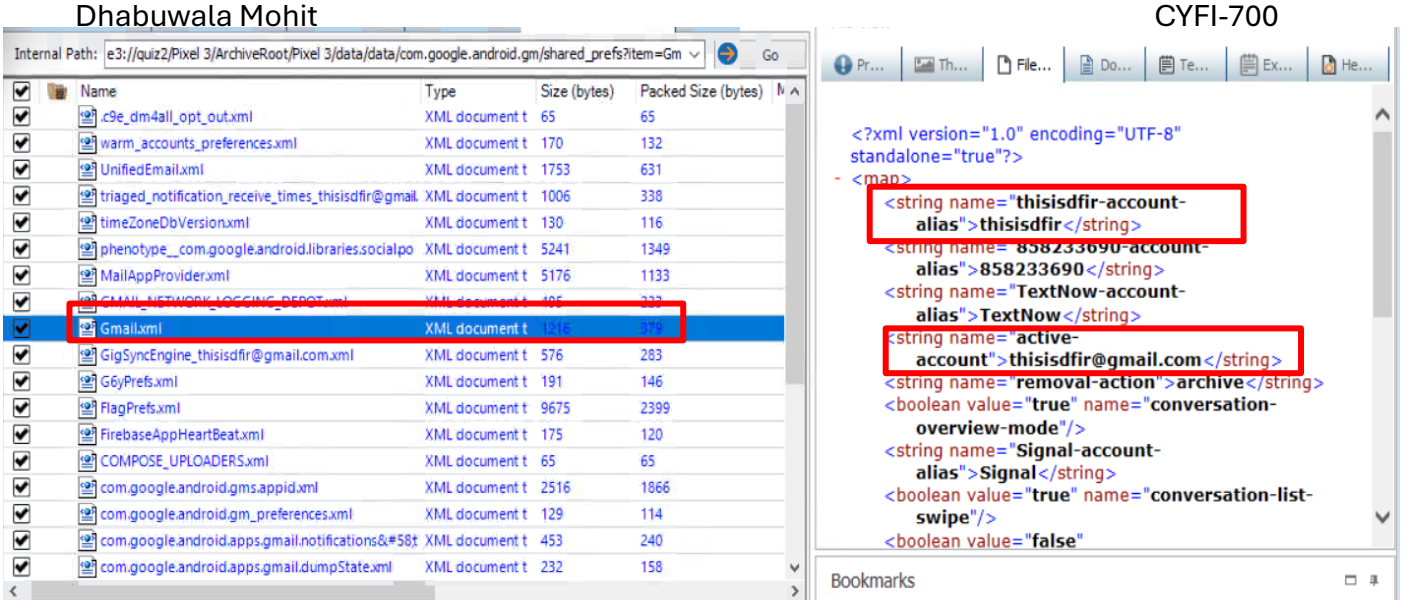


rowid	_id	name	type	password
1	1	thisisdfir@gmail.com	com.google	aas_et/AKppINYHk3843SOlirhnRUtCveD5dMEkDbJE-UM6ATDHh15WhYU1lcZ
2	2	858233690	org.telegram.messenger	
3	3	Signal	org.thoughtcrime.securesms	
4	4	imo HD	com.imo.android.imous	
5	5	TikTok	com.zhiliaoapp.musically	
6	6	Messenger	com.facebook.messenger	
7	7	TDfir	com.twitter.android.auth.logi	
8	8	WhatsApp	com.whatsapp	
10	10	thisisdfir	com.silentcircle.account	dummyPassword
11	11	Skype	com.skype.raider	
12	12	TextNow	com.enflick.android.TextNow	
13	13	+19195794674	com.viber.voip	961ea18e43b4a2b35216e208d9414212e4b699c3
14	14	Duo	com.google.android.apps.tac	

- **Path:** e3://quiz2/Pixel 3/ArchiveRoot/Pixel 3/sbin/.magisk/mirror/data/system_ce/0/accounts_ce.db/*binary_file/database/tables/accounts/1-15?item=row_1

❖ **Verification:** This account's email address and name can be found as a primary account in the **Gmail.xml** file.

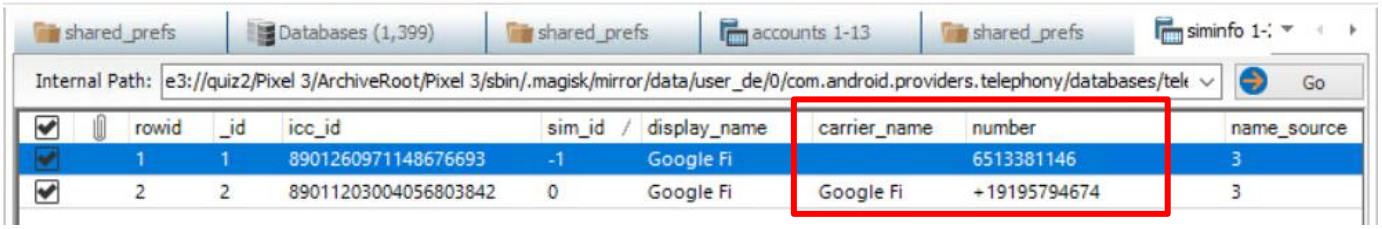
- The Gmail.xml file in an Android device holds a wealth of information related to the user's Gmail account and activities. It's a crucial artifact in providing insights into the user's communications, contacts, and online behavior.



Question 3. What is the telephone number of the device?

Answer The device has two phone numbers associated with it. Though, both the sim cards are different as one is an "**eSIM**" and other is a "**Physical SIM**".

1. **eSIM:** 6513381146
2. **Physical SIM:** +19195794674 - This number appears twice, associated with the keys carrier_number_8901260971148676693F and carrier_number_89011203004056803842. This seems to be the actual phone number assigned to the device, potentially associated with both the eSIM and the physical SIM.



Both SIM cards are provided by the same carrier, "Google Fi." This information is clearly shown in the "number" column of the provided data, corresponding to each **sim_id.**

- **Path:** e3://quiz2/Pixel 3/ArchiveRoot/Pixel 3/data/user_de/0/com.android.providers.telephony/databases/telephony.db/*binary_file/database/tables/siminfo/1-3?item=row_1

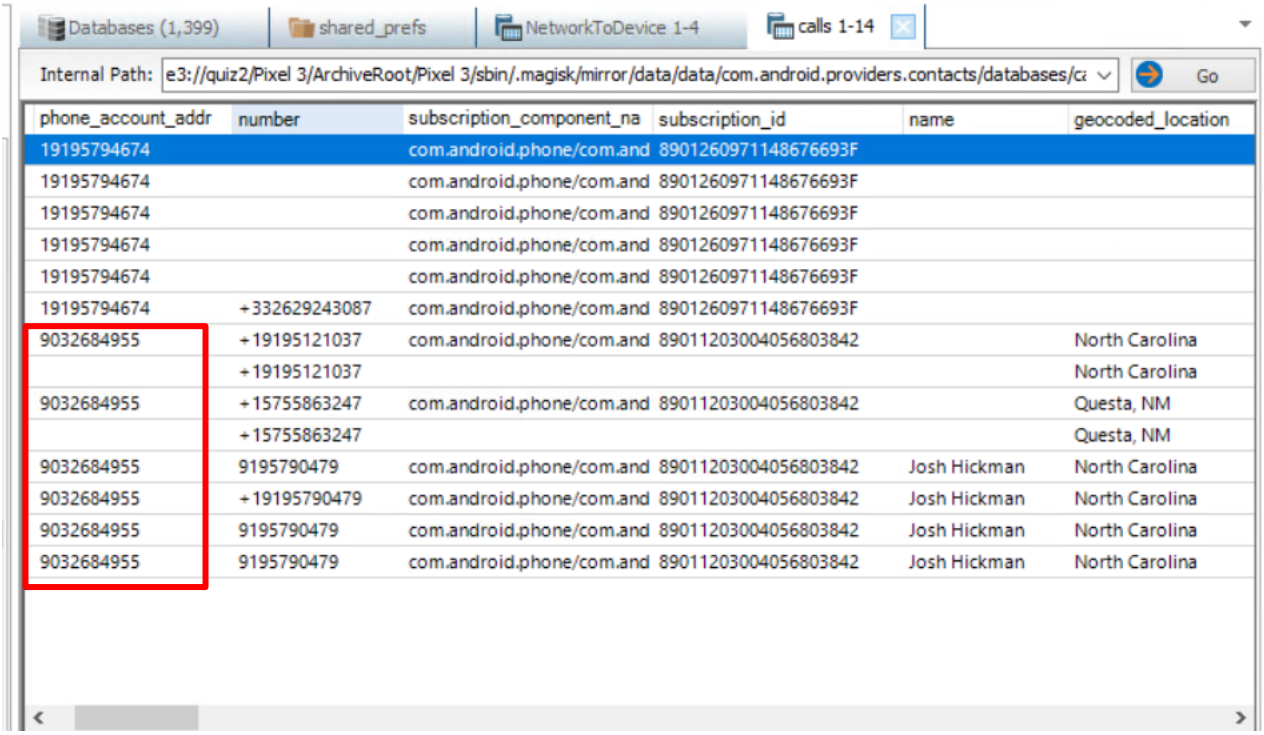
- The **telephony.db** serves as a centralized repository for various SIM-related information on Android devices. It stores details about the SIM cards present in the device, network settings, carrier information, and more. It provides a comprehensive view of the SIM card data, including **ICCID, SIM ID, Phone numbers, Carrier information** and **Network status.**

❖ **Meaning of sim_id:**

- **sim_id = -1:** This typically indicates an **eSIM**. An eSIM is an embedded SIM that's built into the device and functions like a traditional SIM card but is not physically removable.
- **sim_id = 0:** This usually refers to the **first physical SIM card slot** in a device that has multiple SIM card slots.

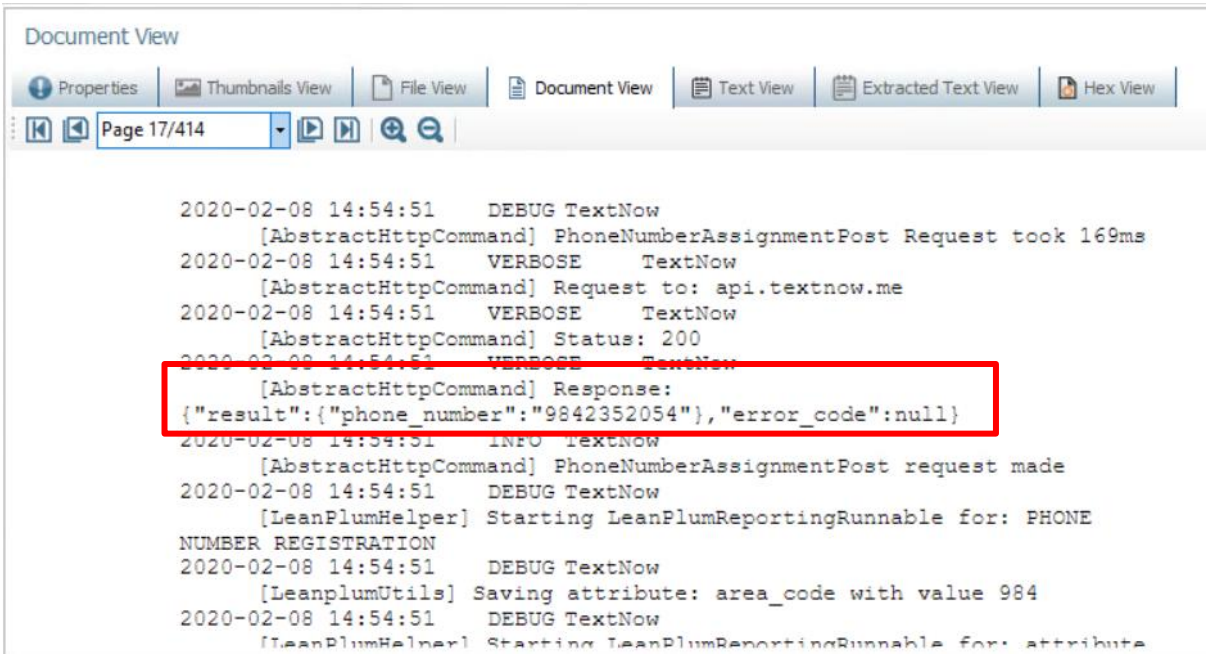
❖ **Number used by user on the device:** Apart from the number registered on the device, there are other 2 numbers which were found from other apps like from call logs, twitter, snapchat, voicemail and other apps etc. They are:

3. **Previous Number**: (903)268-4955 (Acquired from Call log)
   - **Path**: e3://quiz2/Pixel 3/ArchiveRoot/Pixel 3/sbin/.magisk/mirror/data/data/com.android.providers.contacts/databases/calllog.db/*binary_file/database/tables/calls/1-15



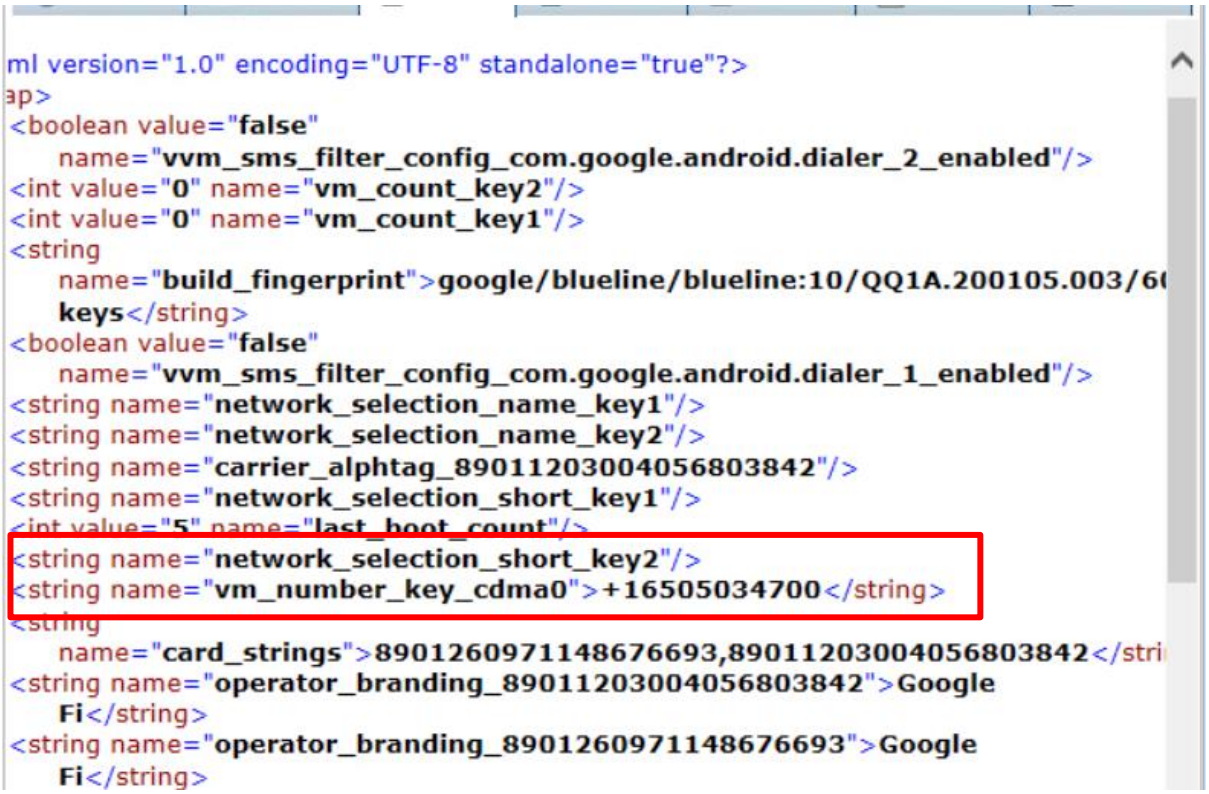
phone_account_addr	number	subscription_component_na	subscription_id	name	geocoded_location
19195794674		com.android.phone/com.and	8901260971148676693F		
19195794674		com.android.phone/com.and	8901260971148676693F		
19195794674		com.android.phone/com.and	8901260971148676693F		
19195794674		com.android.phone/com.and	8901260971148676693F		
19195794674		com.android.phone/com.and	8901260971148676693F		
19195794674	+332629243087	com.android.phone/com.and	8901260971148676693F		
9032684955	+19195121037	com.android.phone/com.and	89011203004056803842		North Carolina
	+19195121037				North Carolina
9032684955	+15755863247	com.android.phone/com.and	89011203004056803842		Questa, NM
	+15755863247				Questa, NM
9032684955	9195790479	com.android.phone/com.and	89011203004056803842	Josh Hickman	North Carolina
9032684955	+19195790479	com.android.phone/com.and	89011203004056803842	Josh Hickman	North Carolina
9032684955	9195790479	com.android.phone/com.and	89011203004056803842	Josh Hickman	North Carolina
9032684955	9195790479	com.android.phone/com.and	89011203004056803842	Josh Hickman	North Carolina

4. **Virtual Number**: (984)235-2054 (Used in Textview Application)
    - This number id used to login and created an account in the textview Application by the user having email ID: thisisdfir@gmail.com and username: thidfir
    - **Path:** e3://quiz2/Pixel 3/ArchiveRoot/Pixel 3/data/media/0/Android/data/com.enflick.android.TextNow/cache?item=logcat_0_2020-02-08_19-52-34.log



5. **Voicemail number**: +16505034700
    - **+16505034700:** This number appears twice in the file, associated with the keys **vm_number_key_cdma0** and **vm_number_key0**. This likely indicates a voicemail number.
    - **Path:** e3://quiz2/Pixel 3/ArchiveRoot/Pixel 3/data/user_de/0/com.android.phone/shared_prefs?item=com.android.phone_preferences.xml

- **Evidence**:



6. **Virtual Number**: (919)758-0276 (Twitter)

- The phone number is associated with login credentials of twitter and many other social media applications. This evidence can be found in the **password_index** sqlite table of **chromesync.data_store** database

- **chromesync.data_store** is a file that stores the data synced by the Chrome browser using the Chrome Sync feature. This feature allows users to synchronize their browsing data, such as bookmarks, history, passwords,

and settings, across multiple devices signed in with the same Google account. This file is essentially a LevelDB database that contains various types of synced data, including **Bookmarks, History, Passwords, Autofill data, Extensions, Settings, Other synced data.**

Question 4. How many non-stock apps were installed on the device? Indicate five non-stock Android apps.

- Answer: Given that the Pixel 3 device is likely rooted (as indicated by the presence of the Magisk rooting tool in the packages.txt file) there are **approximately 53 non-stock** apps installed on this device. This data can be acquired from **packages.xml** file, a file which contains all the app present on the device. This includes apps like:

Serial Number	App Name	Application Package Name
1	MeWe	com.mewe
2	Cyber Dust	com.radicalapps.cyberdust
3	TikTok	com.zhiliaoapp.musically
4	Kik Messenger	kik.android
5	Instagram Threads	com.instagram.threadsapp
6	imo video and chat	com.imo.android.imous
7	Instagram	com.instagram.android
8	LinkedIn	com.linkedin.android
9	Slack	com.Slack
10	Google Chrome	com.android.chrome
11	MyFitnessPal	com.myfitnesspal.android
12	Spotify	com.spotify.music
13	Viber	com.viber.voip
14	Trello	com.trello
15	Uber	com.ubercab
16	Duolingo	com.duolingo
17	Google Keep	com.google.android.keep
18	Strava	com.strava
19	Tor Browser	org.torproject.torbrowser
20	Google Fi	com.google.android.apps.tychod
21	Wickr Me	com.mywickr.wickr2
22	Discord	com.discord
23	Twitch	tv.twitch.android.app
24	SoundCloud	com.soundcloud.android
25	Magisk Root	com.topjohnwu.magisk
26	Musical.ly	com.zhiliaoapp.musically (now TikTok)
27	Facebook Messenger	com.facebook.orca
28	Skout	com.skout.android
29	Tumblr	com.tumblr

30	LINE Messenger	jp.naver.line.android
31	Fitbit	com.fitbit.FitbitMobile
32	Amazon Kindle	com.amazon.kindle
33	Skype	com.skype.raider
34	Gallery Vault	com.thinkyeah.galleryvault
35	Signal Private Messenger	org.thoughtcrime.securesms
36	Wire	com.wire
37	Reddit	com.reddit.frontpage
38	WhatsApp	com.whatsapp
39	TextNow	com.enflick.android.TextNow
40	Venmo	com.venmo
41	Silent Phone	com.silentcircle.silentphone
42	Snapchat	com.snapchat.android
43	Pinterest	com.pinterest
44	Dropbox	com.dropbox.android
45	Twitter	com.twitter.android
46	Telegram Messenger	org.telegram.messenger
47	Truecaller	com.truecaller
48	Imgur	com.imgur.mobile
49	My Verizon	(This might vary depending on the specific Verizon app)
50	Netflix	com.netflix.mediaclient
51	GitHub	com.github.android
52	FODA	com.ponciano.foda
53	Google Docs	com.google.android.apps.docs.editors.docs

- **Path**: e3://quiz2/Pixel 3/ArchiveRoot/Pixel 3/data/data
- "**non-stock apps**" are the applications that are not included with the device's original factory image or OS distribution. These are broadly any apps that the user installs themselves or that come pre-installed by the device manufacturer or carrier as additions to the core Android experience.

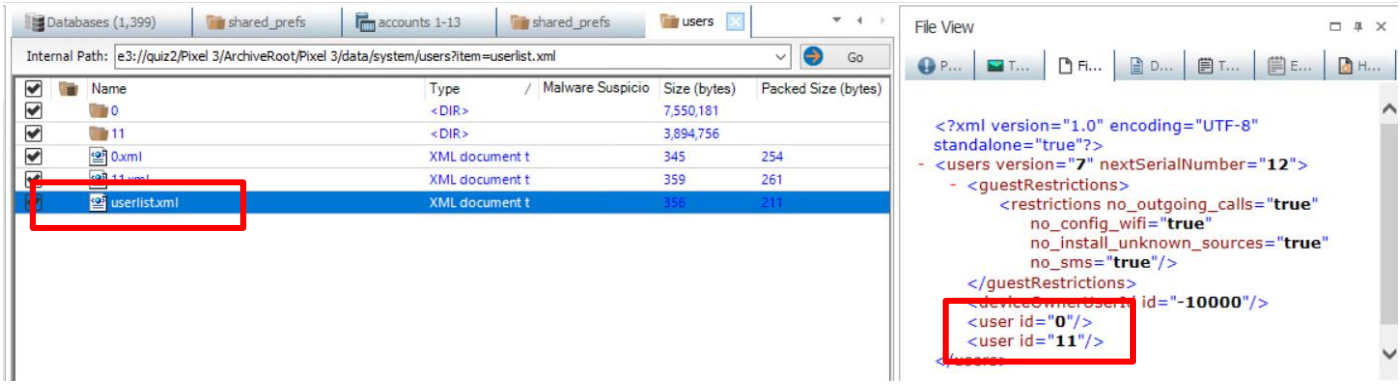
❖ **Types of Non-Stock Apps:**

1. **User-Installed Apps**: These are apps that users explicitly download and install from sources like the Google Play Store, Amazon Appstore, or even directly from APK files. Examples include social media apps (Facebook, Twitter), productivity tools (Microsoft Office, Evernote), and countless others.
2. **Manufacturer/Carrier-Installed Apps**: Device manufacturers or mobile carriers often include their own apps on top of the stock Android operating system. These can include custom user interfaces, utilities, or even bloatware (unwanted pre-installed apps). Examples might be Samsung's "Galaxy Store," HTC's "Sense Home," or carrier-specific apps for managing accounts or services.

Question 5. What is the 2nd user profile that was added to this device?

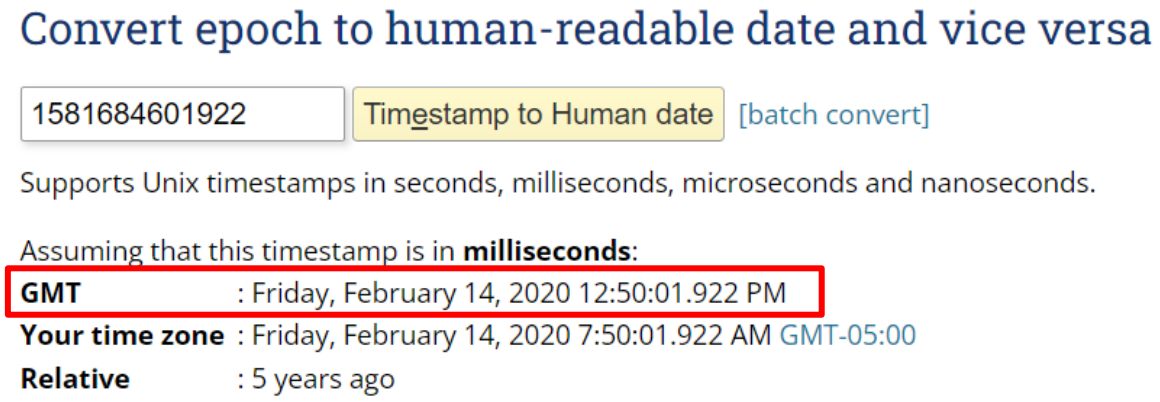
Answer: The name of the second user profile added to this device is "**user 2**". This evidence can be found from the **userlist.xml** file. This file maintains a list of all users on the system, including their user IDs and other relevant attributes. As per this file there are 2 users registered on the device.

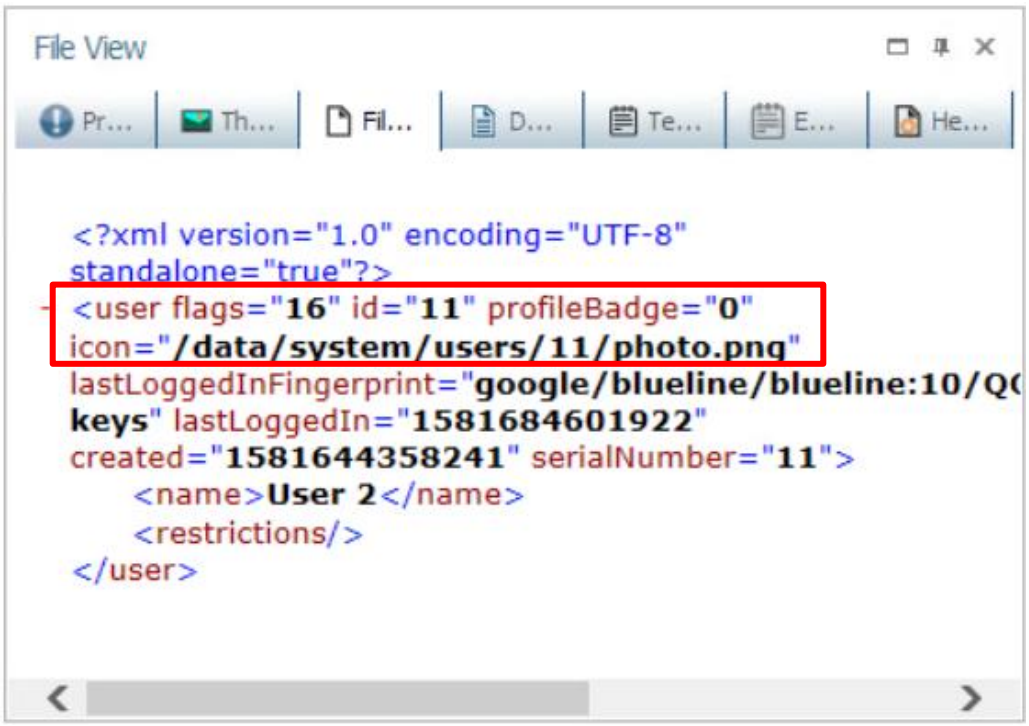
- **Path:** e3://quiz2/Pixel 3/ArchiveRoot/Pixel 3/data/system/users?item=userlist.xml
- <user id="0" /> and <user id="11" />: These lines confirm the presence of two user accounts with user IDs 0 and 11.



- **Evidence of User-2:** The name of the user is "user-2" and the user last logged in on **Friday, February 14, 2020, 12:50:01.922 PM GMT** and the account was created on **Friday, February 14, 2020, 1:39:18.241 AM GMT.**

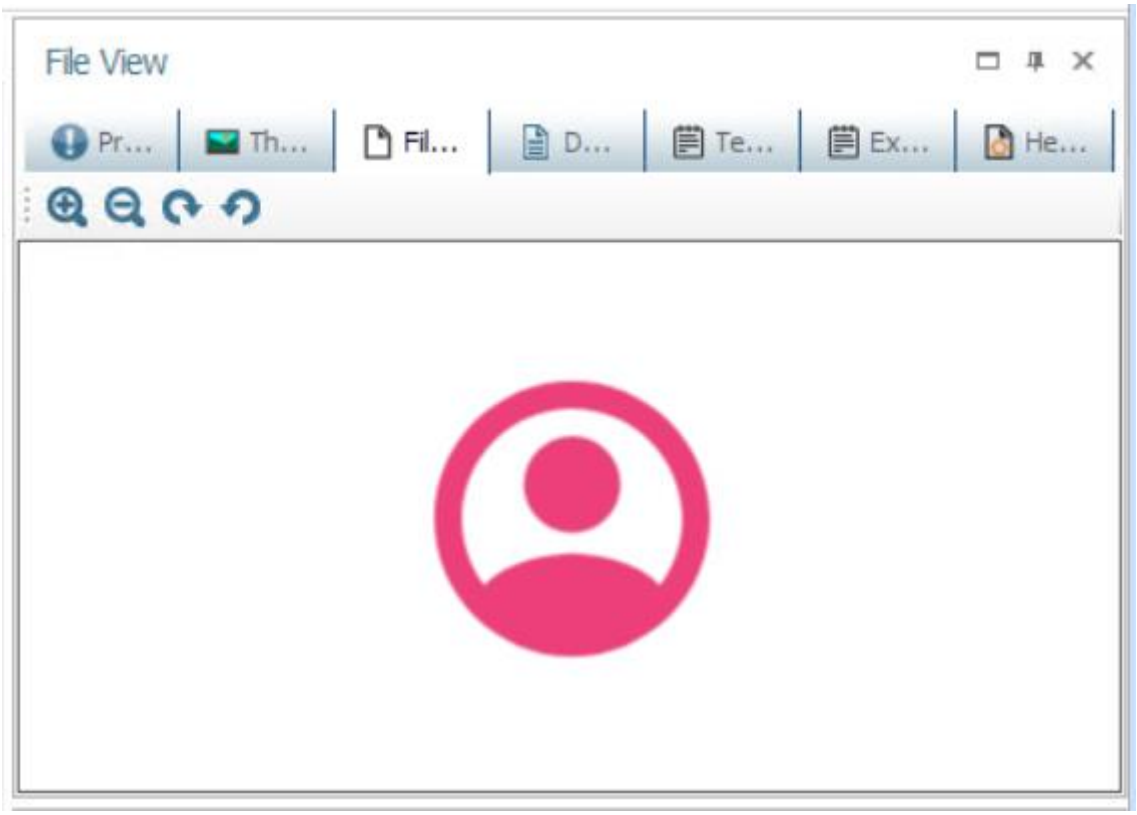
  - **Path:** e3://quiz2/Pixel 3/ArchiveRoot/Pixel 3/data/system/users?item=11.xml





- The **11.xml** file also gives information about the last login time, profile picture and username.

- **Profile photo:** e3://quiz2/Pixel 3/ArchiveRoot/Pixel 3/data/system/users/11?item=photo.png



Question 6. Facebook Messenger was one of the apps used by the suspect in this case. Identify the version number, install date, username and password, and at least one of the messages from FB messenger with its date.

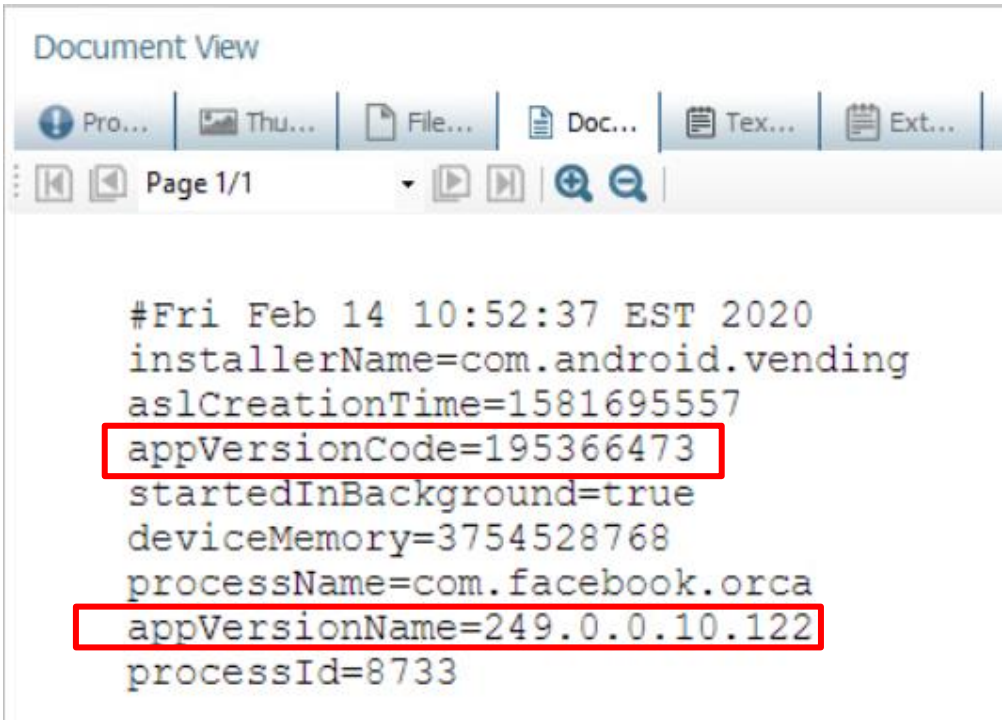
Answer: Facebook Messenger is one of the prime applications which the suspect has used. There is evidence of using the app for chatting with a user named "**Josh Hickman**"**.** The following are the key information acquired from the app.

❖ **App Version Number:**

- The app version is **"249.0.0.10.122 (internal version code 195366473)".** This information can be obtained from a log file named **"com.facebook.orca_27959206-78b7-1464-b9f8-83045eb6fe54.v4.txt_static**". This file is related to app's state logs. These logs store information about the state and activity of the Messenger app on the device.

- **Path:** e3://quiz2/Pixel 3/ArchiveRoot/Pixel 3/data/data/com.facebook.orca/app_state_logs?item=com.facebook.orca_27959206-78b7-1464-b9f8-83045eb6fe54.v4.txt_static

- **Evidence:** The variables "**appVersionCode=195366473 and appVersionName=249.0.0.10.122"** suggests this required information.
  - **appVersionCode** is an integer used internally by the app for versioning and **appVersionName** is the human-readable version number shown to users (e.g., in the Play Store).

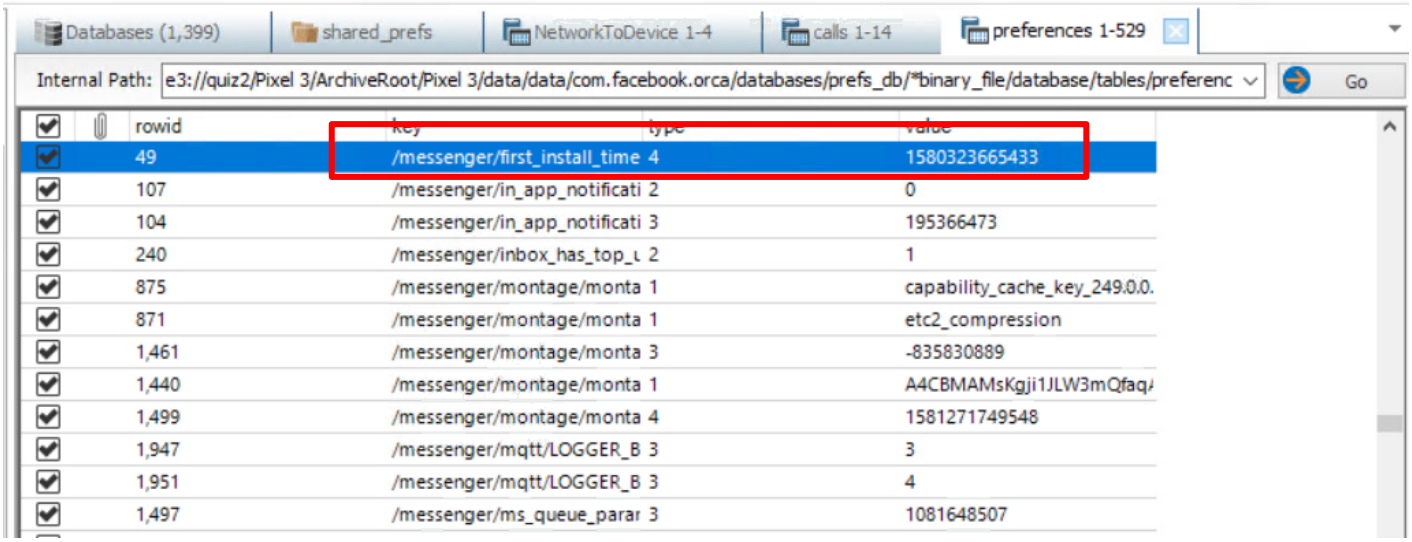


❖ **App Install Date:**

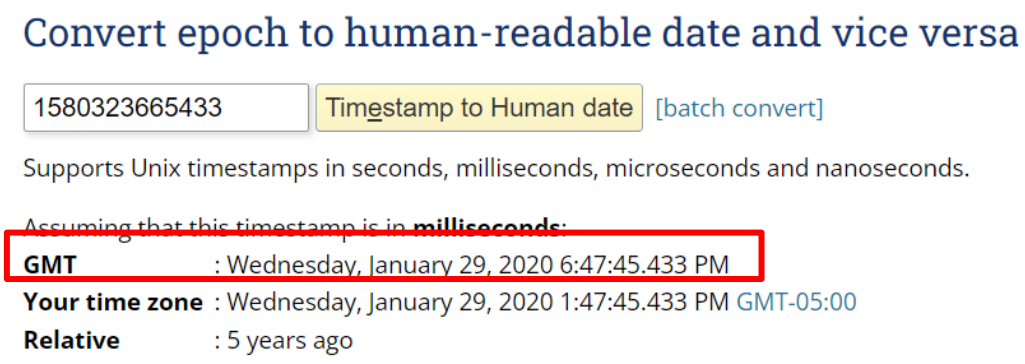
- The app was installed on or before "**January 29, 2020, 6:47:45 PM".** This information can be obtained from the database file "**prefs.db**." This database stores the preferences and settings of the Facebook Messenger app. These settings can reveal user choices, configurations, and features that were enabled or disabled.

- **Path:** e3://quiz2/Pixel 3/ArchiveRoot/Pixel 3/data/data/com.facebook.orca/databases/prefs_db/*binary_file/database/tables/preferences/1-1992?item=row_49

- **Evidence:** The Unix timestamp **(1580323665433)** indicates that when the application was installed for the first time. The **row_49** in the preferences table contains the key ***/messenger/first_install_time*** and a corresponding value. This indicates the timestamp of when the Facebook Messenger app was first installed on the device was **January 29, 2020, 6:47:45 PM**.

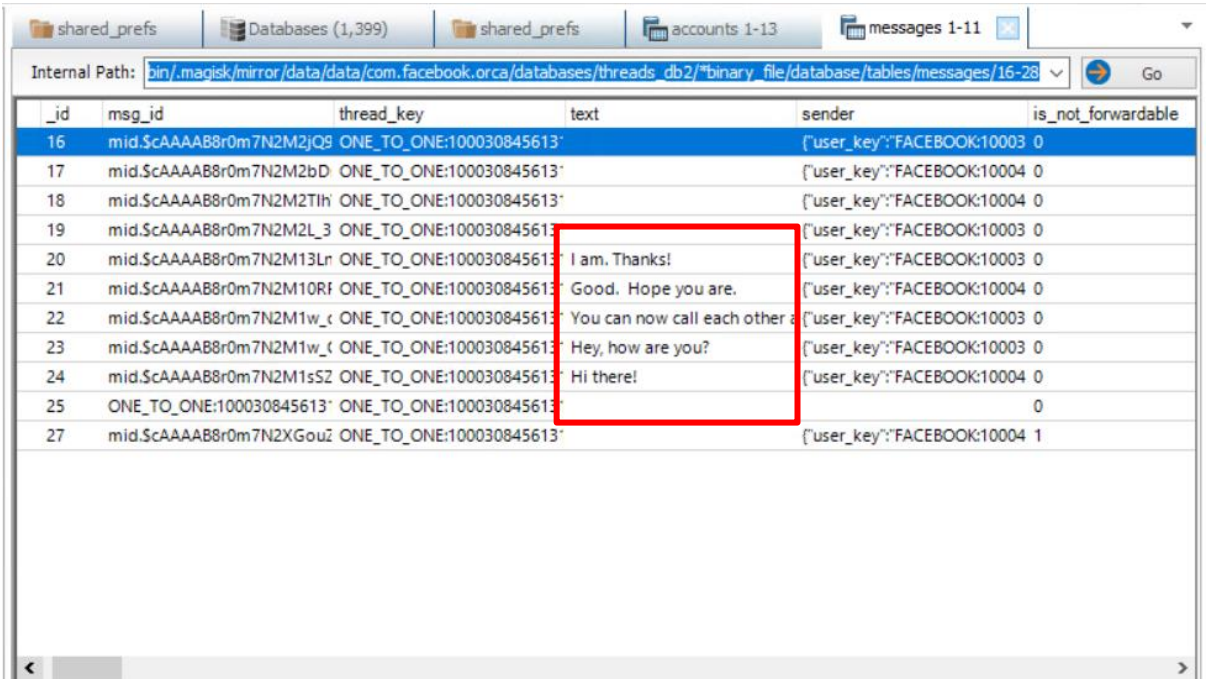


➢ **UNIX time converted to human readable timestamp**



❖ **Messages**:

- The "**messages**" table from the **threads_db2** database within Facebook Messenger on an Android device contains records of messages exchanged between users.
- One conversation thread highlighted in the evidence involves two users with Facebook IDs 100030845613 and 1000410004. The conversation starts on 2020-02-01 18:49:07. with a simple "Hi there!" and includes brief exchanges like "Hey, how are you?" and "Good. Hope you are." It also shows a notification that the users can now call each other.



❖ **App user details:**

- The username acquired from the device for the Facebook Messenger app is "**ThisIs Dfir**" but instead of password, an authentication token was found during the analysis.
- **Username**: ThisIs Dfir
- **Password**: (Access Token): EAADo1TDZCuu8BAPKhV3mbFskutluBZCiIKWwhZAPwzvor1PUXQvp2jjSuT8ZAT3SVHE3kRvMgLbzxmBroZCiBQSt5nni2goZC2HwYZCSVlGLZBmF5D8asPT3Vu1tMUuxwtmsVmaGhZADZBb2Y61M8Jl8jqR8GbRrtonUj4mhds8z8OzWWAy8u3iT5XUUzrKRy34ZC8ZD

- **Path:** e3://quiz2/Pixel 3/ArchiveRoot/Pixel 3/data/data/com.facebook.orca/shared_prefs?item=crash_loop_critical_data.xml

❖ **Why auth token is as good as password:**

- Authentication tokens are used by apps and services to verify user identity *without* requiring the password every time. This token grants access to the user's Facebook account, like how a password would.
- Even if the password is hashed or encrypted, the auth token allows investigators to bypass the need to crack the password and still gain access to potentially valuable data within the Facebook account.

Question 7. Identify the app that generated a payment of $5.

Answer: Out of all the installed applications, there is only one app which supports payment services. The app name is **Venmo.**

- **Venmo** is a mobile payment service owned by PayPal. It allows users to quickly send and receive money to and from friends, family, and approved businesses. It's particularly popular in the United States and is often used to split bills, pay rent, or reimburse friends for shared expenses.

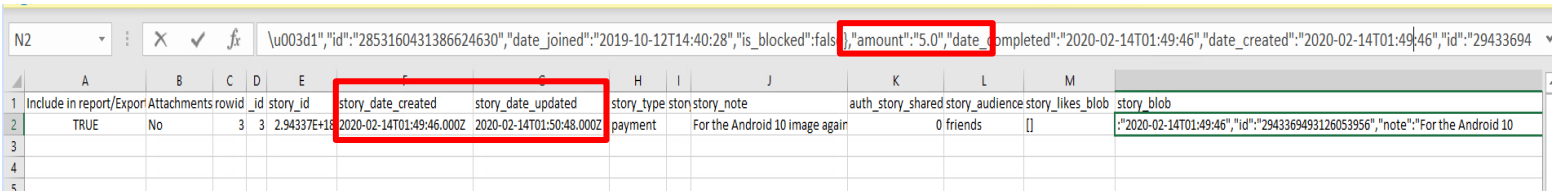
- **Path:** e3://quiz2/Pixel 3/ArchiveRoot/Pixel 3/data/data/com.venmo/databases/venmo.sqlite/*binary_file/database/tables/marvin_stories/1-4?item=row_3

- **Evidence**: This evidence comes from a partial dump of data from a SQLite database file named "**venmo.sqlite".** The data provides insights into Venmo transactions, user details, and comments.

    - In the **marvin_stories** table, the third row (with _id = 3) shows a transaction with an amount of "5.0". Here's the relevant part of the data:

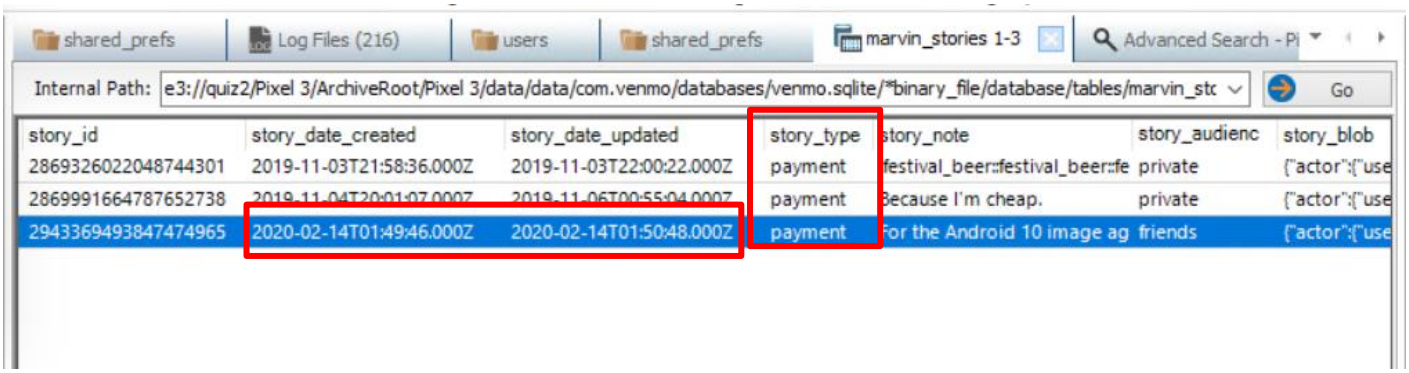
** 3 2943369493847474965 2020-02-14T01:49:46.000Z 2020-02-14T01:50:48.000Z payment For the Android 10 image again. 0 friends [] {"actor":{"username":"Josh-Hickman-19","first_name":"Joshua","last_name":"Hickman","display_name":"Joshua Hickman","friend_status":"friend","friends_count":0,"mutual_friends_count":0,"profile_picture_url":"https://pics.venmo.com/bc1acbdc-8c5c-44b7-af3c-86b9fefc0c52?width\u003d460\u0026height\u003d460\u0026photoVersion\u003d1","id":"2853160431386624630","date_joined":"2019-10-12T14:40:28","is_blocked":false},"**amount":"5.0**","date_completed":"2020-02-14T01:49:46","date_created":"2020-02-14T01:49:46","id":"2943369493126053956","**note":"For the Android 10 image again.","status":"settled**","target":{"type":"user","user":{"username":"ThisIs-DFIR","first_name":"Joshua","last_name":"Hickman","display_name":"Joshua Hickman","friend_status":"not_friend","friends_count":0,"mutual_friends_count":0,"profile_picture_url":"https://pics.venmo.com/8db48124-5c0d-45af-8ed4-e2e48b010e54?width\u003d460\u0026height\u003d460\u0026photoVersion\

u003d1","id":"2864291317284864770","date_joined":"2019-10-27T23:15:33","is_blocked":false}},"action":"pay"} **



Include in report/Export	Attachments	rowid	_id	story_id	story_date_created	story_date_updated	story_type	ston	story_note	auth_story_shared	story_audience	story_likes_blob	story_blob
TRUE	No	3	3	2.94337E+18	2020-02-14T01:49:46.000Z	2020-02-14T01:50:48.000Z	payment		For the Android 10 image again	0	friends	[]	:"2020-02-14T01:49:46","id":"2943369493126053956","note":"For the Android 10

- This indicates a `$5' payment made by "Josh-Hickman-19" to "ThisIs-DFIR" on February 14, 2020, with the note "For the Android 10 image again." Therefore, the Venmo app itself generated this $5 payment.



Internal Path: e3://quiz2/Pixel 3/ArchiveRoot/Pixel 3/data/data/com.venmo/databases/venmo.sqlite/*binary_file/database/tables/marvin_stc

story_id	story_date_created	story_date_updated	story_type	story_note	story_audienc	story_blob
2869326022048744301	2019-11-03T21:58:36.000Z	2019-11-03T22:00:22.000Z	payment	festival_beer::festival_beer::fe	private	{"actor":{"use
2869991664787652738	2019-11-04T20:01:07.000Z	2019-11-06T00:55:04.000Z	payment	Because I'm cheap.	private	{"actor":{"use
2943369493847474965	2020-02-14T01:49:46.000Z	2020-02-14T01:50:48.000Z	payment	For the Android 10 image ag	friends	{"actor":{"use

- ❖ **Why Mervin_stories**: This table store information about Venmo stories, which are posts about transactions that users can share with their network. The data includes details like:
  - I. **story_id**: Unique identifier for the story.
  - II. **story_date_created** and **story_date_updated**: Timestamps of creation and updates.
  - III. **story_type**: Type of story (e.g., "payment").
  - IV. **story_note**: A note or description associated with the story.
  - V. **story_audience**: Who can view the story (e.g., "private").
  - VI. **story_blob**: A JSON object containing detailed information about the transaction, including the sender ("actor"), recipient ("target"), amount, date, and action (pay or charge).

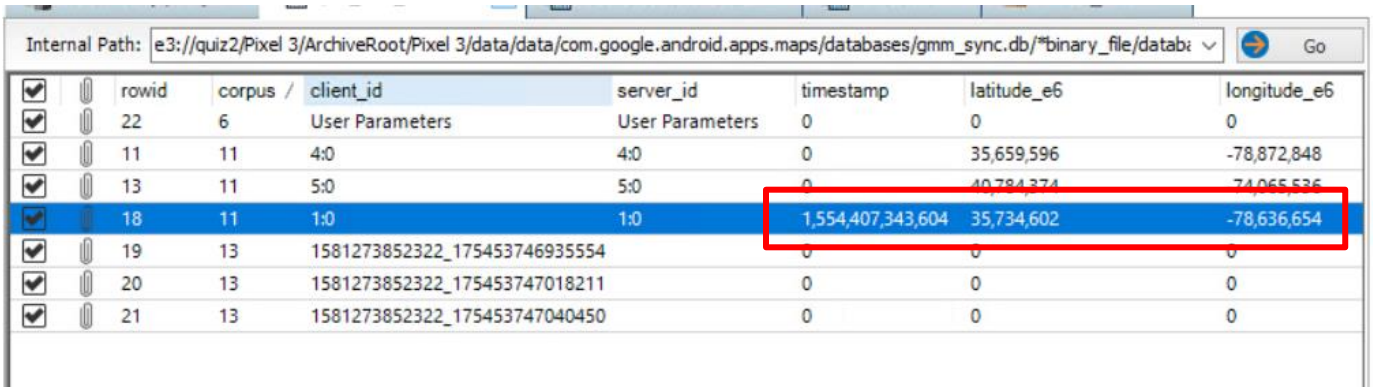
Question 8. You encounter a stock/default Android app that doubles as a directions finder. Indicate the name of this app, where the suspect was headed as well as the date and time if available.

Answer: The stock/default Android app that functions as a directions finder is **Google Maps**. According to the data, the suspect appears to have been headed to the **121 E Tryon Rd, Raleigh, NC 27603.** The date and time of the location request were **Thursday, April 4th, 2019, at 7:49:03 PM GMT.**

- **Path:** e3://quiz2/Pixel 3/ArchiveRoot/Pixel 3/data/data/com.google.android.apps.maps/databases/gmm_sync.db/*binary_file/database/tables/sync_item_data/11-23?item=row_18

- **Evidence:** The image shows a portion of the **gmm_sync.db** database, which stores synchronized data for Google Maps. This database can contain a history of locations accessed or searched for within the app.

    - The **gmm_sync.db** database stores synchronized data for Google Maps, including search history, saved locations, and navigation requests. The timestamp, latitude_e6, and longitude_e6 fields provide the necessary information to determine the time and location of the navigation request.

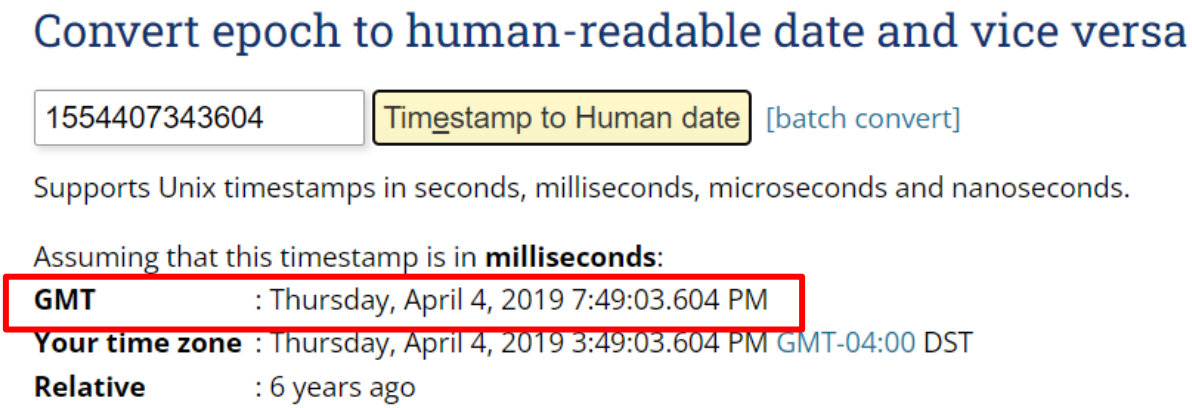


rowid	corpus	client_id	server_id	timestamp	latitude_e6	longitude_e6
22	6	User Parameters	User Parameters	0	0	0
11	11	4:0	4:0	0	35,659,596	-78,872,848
13	11	5:0	5:0	0	40,784,374	-74,065,636
18	11	1:0	1:0	1,554,407,343,604	35,734,602	-78,636,654
19	13	1581273852322_175453746935554		0	0	0
20	13	1581273852322_175453747018211		0	0	0
21	13	1581273852322_175453747040450		0	0	0

The "Hotspot BSSID" is a more specific term used to refer to the BSSID of a Wi-Fi hotspot, while "BSSID" is a general term that applies to any access point. In this case, they are same, as the devices are connected to the same access point creating the hotspot.

The image reveals three distinct sets of coordinates with associated timestamps:

1. **35,659,596, -78,872,848 at timestamp 0**: 152 Sweet Vista Ln, Holly Springs, NC 27540. It's important to note that the Unix epoch is a specific point in time, and the timestamp "0" does not necessarily mean that the location was recorded at that exact moment. It could simply mean that the data was collected and stored in a system that uses the Unix epoch as a reference point.
2. **40,784,374, -74,065,536 at timestamp 0:** 30 Enterprise Ave N, Secaucus, NJ 07094. It's important to note that the Unix epoch is a specific point in time, and the timestamp "0" does not necessarily mean that the location was recorded at that exact moment. It could simply mean that the data was collected and stored in a system that uses the Unix epoch as a reference point.
3. **35,734,602, -78,636,654 at timestamp 1554407343604**: This coordinate, with a specific timestamp of April 4th, 2019, is still the most likely candidate for the suspect's intended destination **121 E Tryon Rd, Raleigh, NC 27603**. It represents a deliberate navigation request made by the user at that specific time.



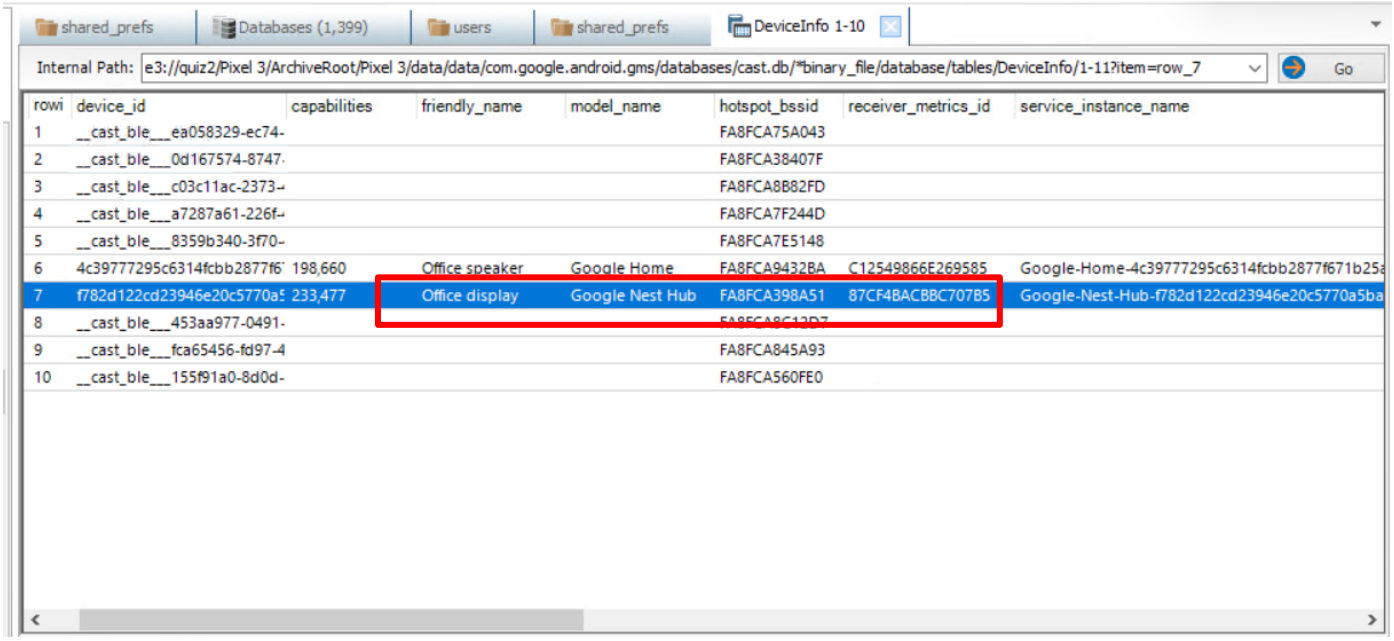
Question 9. Indicate one Google device that data was casted to: name of device, MAC address, BSSID, Hotspot BSSID and SSDP_UDN. (casted means connected or hooked up).

Answer: Based on the data found, one Google device that data was casted to is:

- **Name of device:** Office display
- **MAC address:** F8:BB:BF:1E:FA:E8
- **BSSID:** FA8FCA398A51
- **Hotspot BSSID:** FA8FCA398A51
- **SSDP_UDN:** 87CF4BACBBC707B5

➢ **Path:** e3://quiz2/Pixel 3/ArchiveRoot/Pixel 3/data/data/com.google.android.gms/databases/cast.db/*binary_file/database/tables/DeviceInfo/1-11

➢ **Evidence:** The image shows a portion of a database, extracted from the Chromecast app on the Pixel 3 device. The database contains information about devices that have been connected to or "casted to" using the Chromecast app.



rowi	device_id	capabilities	friendly_name	model_name	hotspot_bssid	receiver_metrics_id	service_instance_name
1	__cast_ble___ea058329-ec74-				FA8FCA75A043		
2	__cast_ble___0d167574-8747-				FA8FCA38407F		
3	__cast_ble___c03c11ac-2373-4				FA8FCA8B82FD		
4	__cast_ble___a7287a61-226f-4				FA8FCA7F244D		
5	__cast_ble___8359b340-3f70-				FA8FCA7E5148		
6	4c39777295c6314fcbb2877f6	198,660	Office speaker	Google Home	FA8FCA9432BA	C12549866E269585	Google-Home-4c39777295c6314fcbb2877f671b25a
7	f782d122cd23946e20c5770a5	233,477	Office display	Google Nest Hub	FA8FCA398A51	87CF4BACBBC707B5	Google-Nest-Hub-f782d122cd23946e20c5770a5ba
8	__cast_ble___453aa977-0491-				[illegible]		
9	__cast_ble___fca65456-fd97-4				FA8FCA845A93		
10	__cast_ble___155f91a0-8d0d-				FA8FCA560FE0		

❖ **Why this file?**

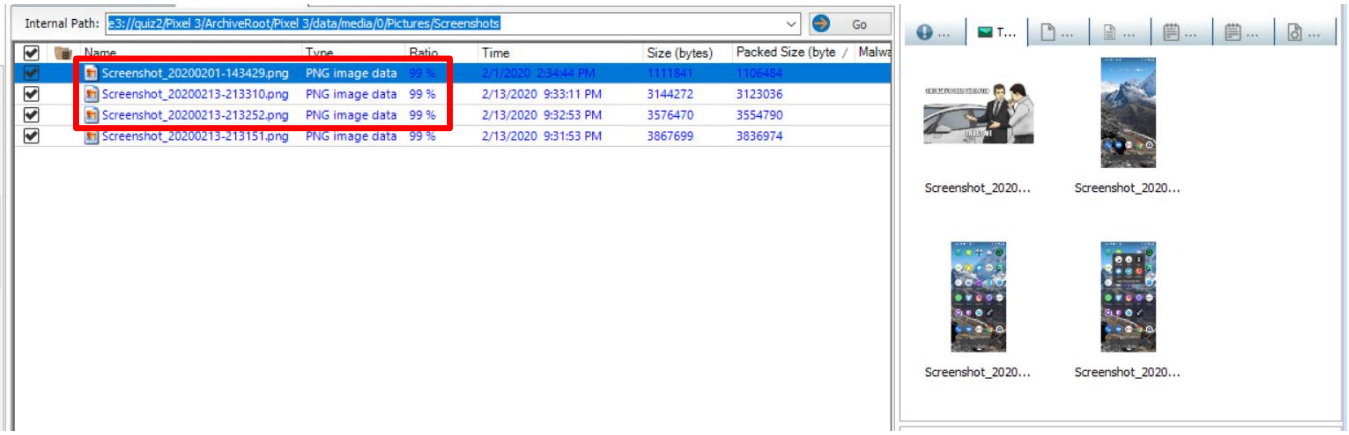
- The **cast.db** file is a database file associated with the Google Chromecast app on Android devices. It stores information about devices that have been connected to or "casted to" by the Chromecast.
- The database also contains network-related information, such as IP addresses and BSSIDs, which can provide insights into the network environment and connected devices.

Question 10. Provide screen shots of user 1 home screen.

Answer: There are “3” screenshots available in the device for the home screen layout of user 1. The name of all the 3 screenshots is **Screenshot_20200213-213252.png, Screenshot_20200213-213151.png and Screenshot_20200213-213310.png**.

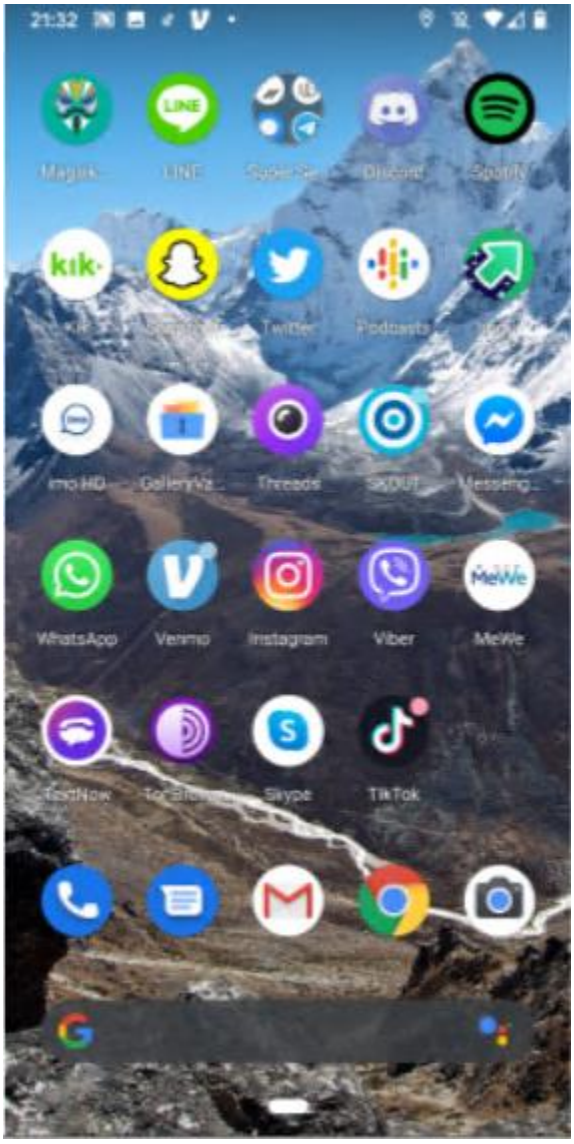
- **Path**: e3://quiz2/Pixel 3/ArchiveRoot/Pixel 3/data/media/0/Pictures/Screenshots

- **Evidence**: The ***/data/media/0/Pictures/Screenshots*** directory is the standard location where Android devices store screenshots taken by the user. Therefore, it's the logical place to look for images capturing the user's home screen layout.



- Given that the Pixel 3 device is likely rooted (as indicated by the presence of the Magisk rooting tool in the packages.txt file), a plausible thesis about the user taking these screenshots is that they wanted to **document their home screen layout and app configuration before proceeding with the rooting process.**

Home Screen - 1



Home Screen - 2

Home Screen - 3