Digital Forensics Research Paper

By Christo-odysseus Keramitzis

Christo-
Odysseus
Keramitzis

Digitally signed by Christo-Odysseus
Keramitzis
DN: cn=Christo-Odysseus
Keramitzis, c=AU,
email=CKbusinessemail@proton.me
Date: 2024.11.22 22:39:14 +11'00'

Executive summary

This report explores the functional and technical qualities of mobile forensics in artefacts extraction. Due to the interconnectivity and complexity of mobile devices, findings can be difficult to keep in scope as applications share and collect data. therefore risking breaching warrants and case boundaries.

This report will outline the importance of phone attribution in triage through the analysis of communication mediums individuals use. The stock communication dialer and messenger analysed provided key insights into user activity over a period of 7 months. Through sql

viewers and artefact organisation, affiliations messages and a record of call logs allowed the mapping of the communication network by date and times. The purpose is to acquire identifiable information that ties the user to the device.

Furthermore, Applications such as browsers and social media house a great deal of user information that enables accurate journey mapping. Google chrome subsequently allowed for timeline plotting of the various websites and data surfed through cache and chrome databases. Through the use of database browsers such as SQlite for db, cache, history and autofill data was able to be extracted. These searches can be compared to the recent activities of other applications such as snapchat; therefore ascertaining the motive, thought process and relations with other individuals leading up to the crime. This is achieved through media sent and downloaded, friends lists and communications. Snapchat required other tools such as XML and hex viewers for session and login acquisition.

What was found was a complex web of communications that revealed geolocation activities, financial interests and the thoughts of the individual through social interactions. There was no evidence of illegal activity found; rather a showcase of how possible artefacts fit into the digital forensics structure and what type of evidence can be extrapolated was achieved.

Introduction

Digital forensics and its presence within criminal cases has become more apparent with the rise of globalisation and reduction in cost of technology. This has empowered individuals to access services and tools that enhance their work, daily lives and communication. Simultaneously, this places technology in the hands of criminals, thus requiring a form of device analysis in most criminal cases. Due to the software support the android operating system exhibits, individuals can freely create applications that collect a great deal of data or actively avoid it. To the consumer, this is a blessing and a curse with the rise of privacy concerns and the constant need for better software and features. In regards to forensics, this creates a nightmare for data acquisition during cases with strict triage guidelines; as the overlapping of data creates more entries that must be organised into artefacts and non-artefacts. There is also a concern for a lack of artefacts that inhibit device attribution such as apps similar to signal, secure folder and telegram. This constant evolving software and hardware landscape requires a need for continuous improvement in forensic tools and techniques. The purpose of this report is to depict the process of artefact acquisition using various tools and methods.

Forensics analysis

General discussion

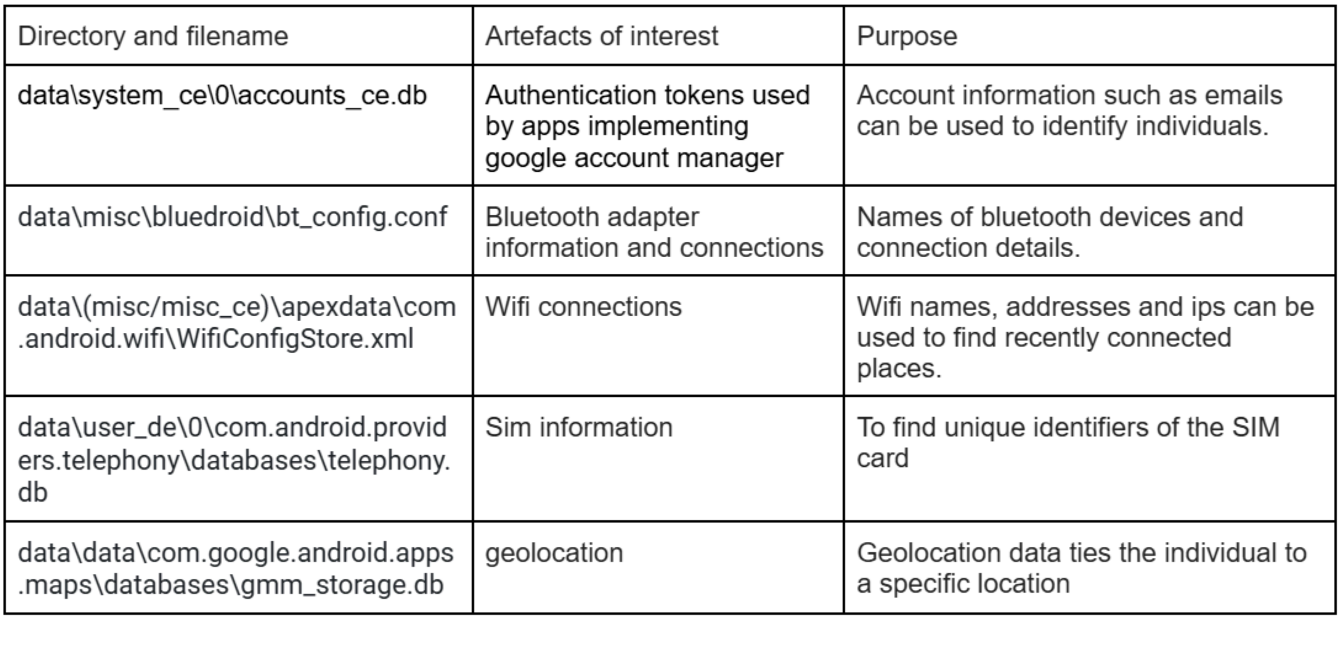
Mobile forensics is a complex and delicate process that is becoming increasingly more important as mobile devices become more present. Mobile devices have become more prevalent within forensics triage as these devices have become the primary form of communication. Over 90% of all individuals who use the internet do so through mobile devices(Oberlo. (n.d.)); therefore, there is a higher chance that Forensic specialists are “more likely to run into a cellular device as opposed to a PC”(Colvin, D. (2022, June 10)).

The android operating system is open source and supported by companies such as google samsung and hardware manufacturers. This strong software support enables individuals to create applications. Due to this consumer choice and differences in international data laws, what data and how it is stored, transformed and transferred changes between states and countries. Since mobile phones contain a variety of personal identifiable and confidential information, a warrant or a subpoena is needed for seizure and the right to conduct a forensics investigation. Therefore, a strong understanding of mobile forensic laws are needed with clear guidelines for the triage process.

Mobile security is constantly developing new methods of intrusion detection and prevention, data security and system hardening; Android 6.0 is a strong example of this security shift that implemented many new technologies that prevented Forensics triage. These included SELinux enforcement that isolated apps between each other and the system, verified boot that prevented various tools from acquiring a system image and direct boot that launched apps before user login. Therefore the methods of acquiring data have changed; the two most common data acquisition methods are either a system image or a file system dump. Due to the hardware complexity of a mobile device, the main focus of this report will exclude memory analysis and focus on the file system structure.

(10 marks) Phone attribute method

Phone attribution is the process of identifying a user to their mobile device through various means such as UID, SSID, applists, numbers and accounts. Android, similarly to windows, spreads device specific information throughout various files. These can range from app package databases to simple xml files that include wifi and bluetooth connections.



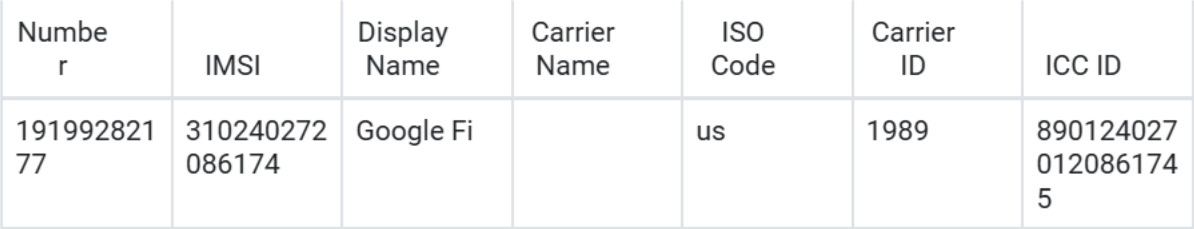
Directory and filename	Artefacts of interest	Purpose
data\system_ce\0\accounts_ce.db	Authentication tokens used by apps implementing google account manager	Account information such as emails can be used to identify individuals.
data\misc\bluedroid\bt_config.conf	Bluetooth adapter information and connections	Names of bluetooth devices and connection details.
data\(misc/misc_ce)\apexdata\com.android.wifi\WifiConfigStore.xml	Wifi connections	Wifi names, addresses and ips can be used to find recently connected places.
data\user_de\0\com.android.providers.telephony\databases\telephony.db	Sim information	To find unique identifiers of the SIM card
data\data\com.google.android.apps.maps\databases\gmm_storage.db	geolocation	Geolocation data ties the individual to a specific location

System files

During mobile setup, individuals customise their device name and setting that may include identifiable information. Additionally, some aspects of device hardware inherently come with unique identifiers for that device such as SIM cards and mobile hotspot.

SIM identifier

SIM card logs and information are a reliable tool for identifying the attributing the individual to the mobile device. Similarly to credit cards SIM cards have a unique ICCID and IMSI that follows a strict structure. They are used to identify the individual and the SIM connected to the device



Number	IMSI	Display Name	Carrier Name	ISO Code	Carrier ID	ICC ID
19199282177	310240272086174	Google Fi		us	1989	8901240270120861745

Table 1 sim information

Table 1 shows these two identifiers along with the country code US. The integrated circuit card number can provide a significant amount of attribution data due to its structure:

1. 89 represents the telecommunications industry.
2. 01 is the country code of the USA
3. 240 is the carrier, in this case they are T-mobile.
4. The individual account identifier
5. Luhn check digit 5 which acts as a checksum

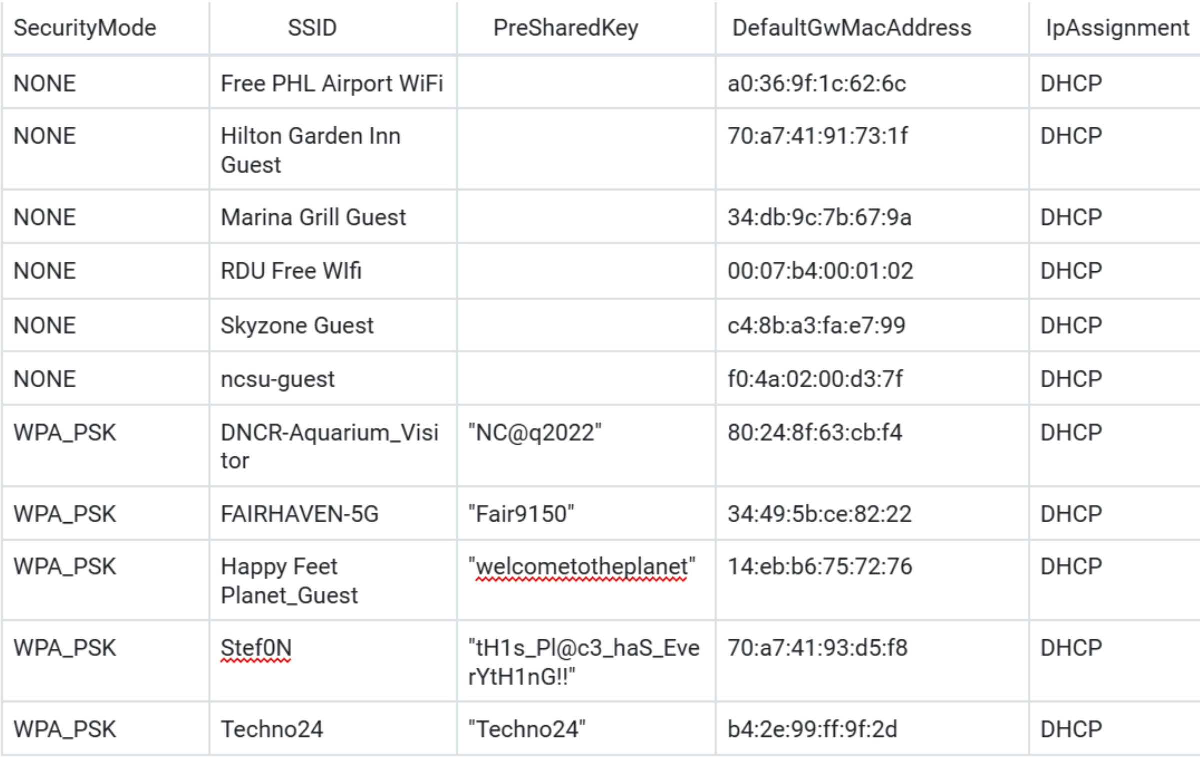
IMSI acts in a similar manner, they are unique to the profile and not the device:

1. First 3 number 310 is the country USA
2. Mobile network code T-mobile 240
3. The remaining are the mobile subscriber identification number

The main difference between these is the ICCID identifies the sim card while the IMSI identifies the user. These identifiers can be used to query the respective provider thus attributing the individual to the device

Wifi

Most individuals who use their devices will, over time, connect to an array of wifi connections/modems that the device will log. These can include both public and private networks each with unique identifiers that can provide approximate location. Table 2 depicts the WifiConfigStore.xml that logs all connections. Several SSIDs stand out such as the Free PHL Airport Wifi connection, DNCR Aquarium_Visitor and Hilton Garden Inn Guest.



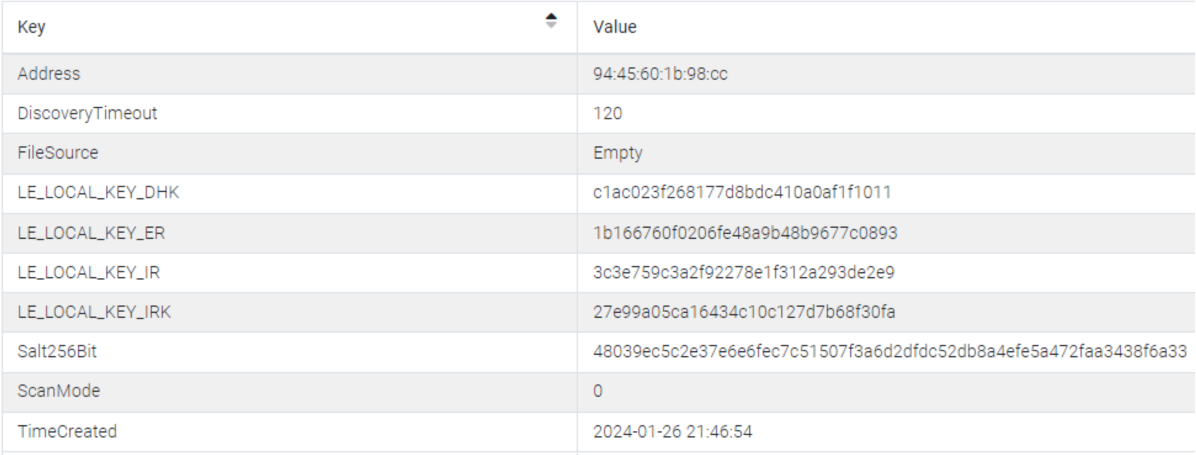
SecurityMode	SSID	PreSharedKey	DefaultGwMacAddress	IpAssignment
NONE	Free PHL Airport WiFi		a0:36:9f:1c:62:6c	DHCP
NONE	Hilton Garden Inn Guest		70:a7:41:91:73:1f	DHCP
NONE	Marina Grill Guest		34:db:9c:7b:67:9a	DHCP
NONE	RDU Free WIfi		00:07:b4:00:01:02	DHCP
NONE	Skyzone Guest		c4:8b:a3:fa:e7:99	DHCP
NONE	ncsu-guest		f0:4a:02:00:d3:7f	DHCP
WPA_PSK	DNCR-Aquarium_Visitor	"NC@q2022"	80:24:8f:63:cb:f4	DHCP
WPA_PSK	FAIRHAVEN-5G	"Fair9150"	34:49:5b:ce:82:22	DHCP
WPA_PSK	Happy Feet Planet_Guest	"welcometotheplanet"	14:eb:b6:75:72:76	DHCP
WPA_PSK	Stef0N	"tH1s_Pl@c3_haS_EverYtH1nG!!"	70:a7:41:93:d5:f8	DHCP
WPA_PSK	Techno24	"Techno24"	b4:2e:99:ff:9f:2d	DHCP

Table 2 wifi connections

This geolocation map located in the references is a complete map of its geolocation activities from wifi and communication locations. This depicts that the owner of this device is an avid traveller over the lifespan of this phone (february till september). Cross examining the information gained from his wifi connections with other application data, it is fairly simple to map all of his activities including the place of residency.

Bluetooth

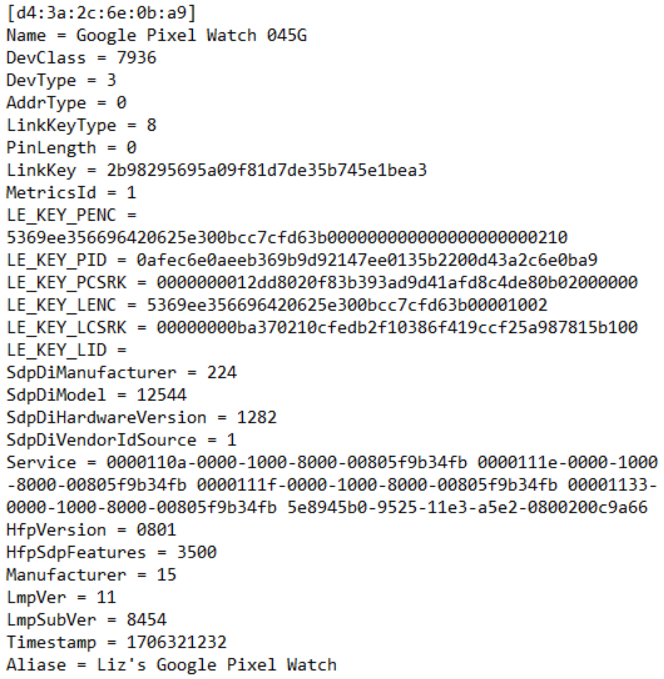
Bluetooth names and connections can reveal names and unique identifiers of those devices. The figure below depicts some bluetooth connectivity data; the most notable artefact is the address. All bluetooth devices are manufactured with a registered public bluetooth mac address that can uniquely identify the device. The various keys below are used for encryption purposes that secure the connection via the salt and an algorithm.



Key	Value
Address	94:45:60:1b:98:cc
DiscoveryTimeout	120
FileSource	Empty
LE_LOCAL_KEY_DHK	c1ac023f268177d8bdc410a0af1f1011
LE_LOCAL_KEY_ER	1b166760f0206fe48a9b48b9677c0893
LE_LOCAL_KEY_IR	3c3e759c3a2f92278e1f312a293de2e9
LE_LOCAL_KEY_IRK	27e99a05ca16434c10c127d7b68f30fa
Salt256Bit	48039ec5c2e37e6e6fec7c51507f3a6d2dfdc52db8a4efe5a472faa3438f6a33
ScanMode	0
TimeCreated	2024-01-26 21:46:54

Figure 1 bluetooth adaptor

By identifying the mac addresses of the bluetooth device within the phone, law enforcement can then retrace the device's journey to the individual who purchased it. Additional attribution can be acquired through connected devices and their details. When a Bluetooth device makes a connection, device information is saved for future reconnections. Figure 2 depicts connection information that was logged when the mobile connected with Liz’s pixel watch. Without additional information, we cannot assume that the owner goes by this name, but it does prove that someone that they contact goes by that alias..

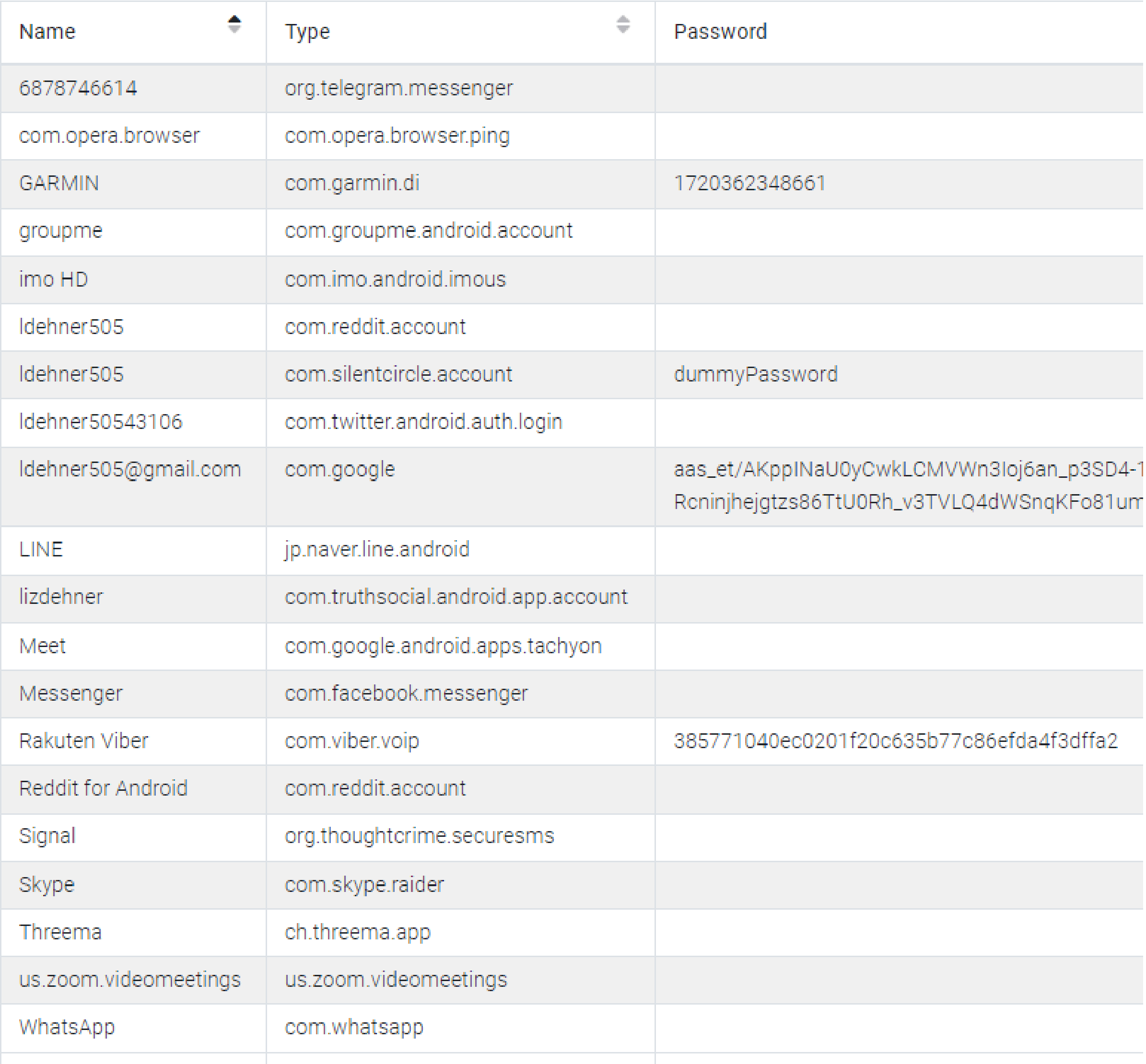


```
[d4:3a:2c:6e:0b:a9]
Name = Google Pixel Watch 045G
DevClass = 7936
DevType = 3
AddrType = 0
LinkKeyType = 8
PinLength = 0
LinkKey = 2b98295695a09f81d7de35b745e1bea3
MetricsId = 1
LE_KEY_PENC =
5369ee356696420625e300bcc7cfd63b000000000000000000000210
LE_KEY_PID = 0afec6e0aeeb369b9d92147ee0135b2200d43a2c6e0ba9
LE_KEY_PCSRK = 0000000012dd8020f83b393ad9d41afd8c4de80b02000000
LE_KEY_LENC = 5369ee356696420625e300bcc7cfd63b00001002
LE_KEY_LCSRK = 00000000ba370210cfedb2f10386f419ccf25a987815b100
LE_KEY_LID =
SdpDiManufacturer = 224
SdpDiModel = 12544
SdpDiHardwareVersion = 1282
SdpDiVendorIdSource = 1
Service = 0000110a-0000-1000-8000-00805f9b34fb 0000111e-0000-1000
-8000-00805f9b34fb 0000111f-0000-1000-8000-00805f9b34fb 00001133-
0000-1000-8000-00805f9b34fb 5e8945b0-9525-11e3-a5e2-0800200c9a66
HfpVersion = 0801
HfpSdpFeatures = 3500
Manufacturer = 15
LmpVer = 11
LmpSubVer = 8454
Timestamp = 1706321232
Aliase = Liz's Google Pixel Watch
```

Figure 2 google pixel watch connection

Accounts and Applications

A user can be attributed to the device they own through their various account logins that may identify them. These can come in the form of social media names, email addresses and website logins. Android devices log the various accounts individuals login through applications. The owner of this device had approximately 20 recorded logins.

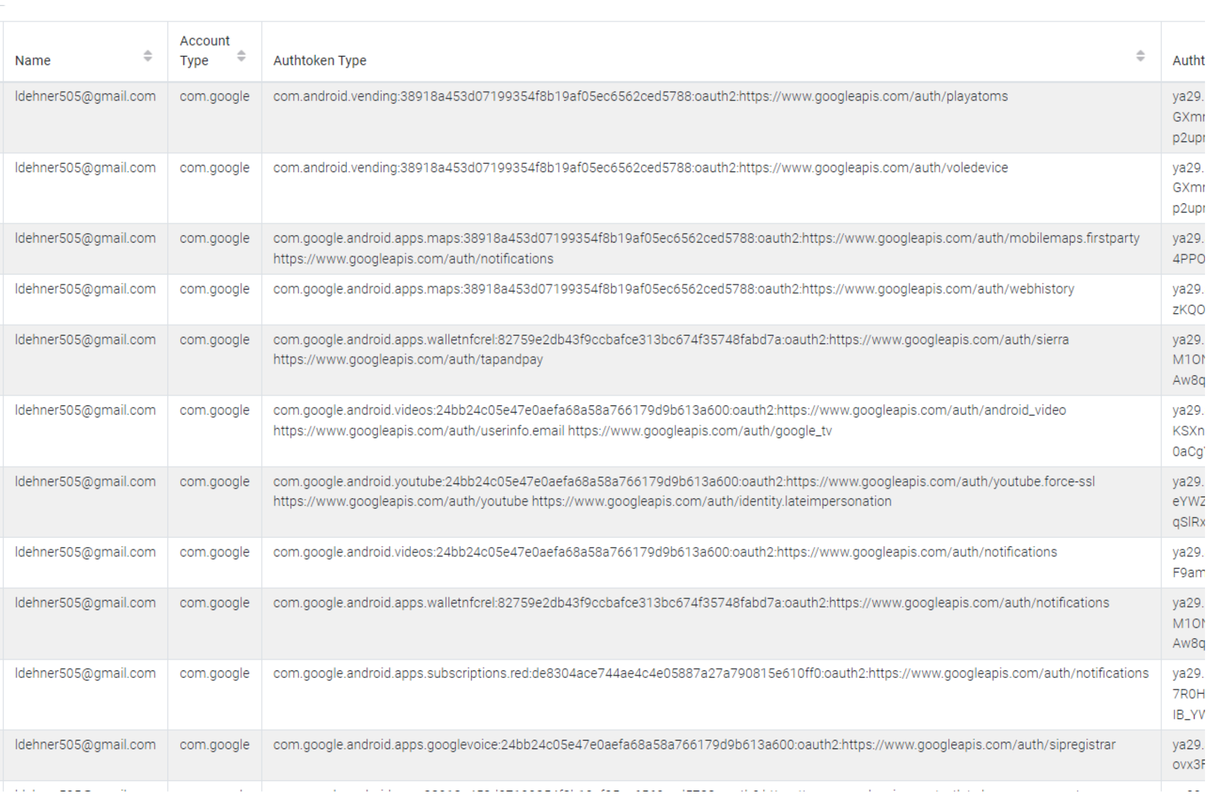


Name	Type	Password
6878746614	org.telegram.messenger	
com.opera.browser	com.opera.browser.ping	
GARMIN	com.garmin.di	1720362348661
groupme	com.groupme.android.account	
imo HD	com.imo.android.imous	
ldehner505	com.reddit.account	
ldehner505	com.silentcircle.account	dummyPassword
ldehner50543106	com.twitter.android.auth.login	
ldehner505@gmail.com	com.google	aas_et/AKppINaU0yCwkLCMVWn3loj6an_p3SD4-1 Rcninjhejgtzs86TtU0Rh_v3TVLQ4dWSnqKFo81um
LINE	jp.naver.line.android	
lizdehner	com.truthsocial.android.app.account	
Meet	com.google.android.apps.tachyon	
Messenger	com.facebook.messenger	
Rakuten Viber	com.viber.voip	385771040ec0201f20c635b77c86efda4f3dffa2
Reddit for Android	com.reddit.account	
Signal	org.thoughtcrime.securesms	
Skype	com.skype.raider	
Threema	ch.threema.app	
us.zoom.videomeetings	us.zoom.videomeetings	
WhatsApp	com.whatsapp	

Figure 3 depicts the accounts

Several accounts should be noted such as the telegram number, social media, communication apps and the plaintext passwords. Most importantly, there is a google email most signed in to the device with the credential ldehner (lizdehner). This reveals an identifiable name that could belong to the user thus successfully attributing the device to a possible user. Further forensic analysis also reveals a possible account that can be used to ascertain further artefacts; it is important to keep in mind the scope case when accessing accounts externally.

Exploring the accounts.ce database further reveals a total of 162 authentication tokens that frequently link to the ldehner505 email for various android applications such as youtube and chrome.



Name	Account Type	Authtoken Type	Autht
ldehner505@gmail.com	com.google	com.android.vending:38918a453d07199354f8b19af05ec6562ced5788:oauth2:https://www.googleapis.com/auth/playatoms	ya29. GXmr p2upr
ldehner505@gmail.com	com.google	com.android.vending:38918a453d07199354f8b19af05ec6562ced5788:oauth2:https://www.googleapis.com/auth/voledevice	ya29. GXmr p2upr
ldehner505@gmail.com	com.google	com.google.android.apps.maps:38918a453d07199354f8b19af05ec6562ced5788:oauth2:https://www.googleapis.com/auth/mobilemaps.firstparty https://www.googleapis.com/auth/notifications	ya29. 4PPO
ldehner505@gmail.com	com.google	com.google.android.apps.maps:38918a453d07199354f8b19af05ec6562ced5788:oauth2:https://www.googleapis.com/auth/webhistory	ya29. zKQO
ldehner505@gmail.com	com.google	com.google.android.apps.walletnfcrel:82759e2db43f9ccbafce313bc674f35748fabd7a:oauth2:https://www.googleapis.com/auth/sierra https://www.googleapis.com/auth/tapandpay	ya29. M1ON Aw8q
ldehner505@gmail.com	com.google	com.google.android.videos:24bb24c05e47e0aefa68a58a766179d9b613a600:oauth2:https://www.googleapis.com/auth/android_video https://www.googleapis.com/auth/userinfo.email https://www.googleapis.com/auth/google_tv	ya29. KSXn 0aCg
ldehner505@gmail.com	com.google	com.google.android.youtube:24bb24c05e47e0aefa68a58a766179d9b613a600:oauth2:https://www.googleapis.com/auth/youtube.force-ssl https://www.googleapis.com/auth/youtube https://www.googleapis.com/auth/identity.lateimpersonation	ya29. eYWZ qSlRx
ldehner505@gmail.com	com.google	com.google.android.videos:24bb24c05e47e0aefa68a58a766179d9b613a600:oauth2:https://www.googleapis.com/auth/notifications	ya29. F9am
ldehner505@gmail.com	com.google	com.google.android.apps.walletnfcrel:82759e2db43f9ccbafce313bc674f35748fabd7a:oauth2:https://www.googleapis.com/auth/notifications	ya29. M1ON Aw8q
ldehner505@gmail.com	com.google	com.google.android.apps.subscriptions.red:de8304ace744ae4c4e05887a27a790815e610ff0:oauth2:https://www.googleapis.com/auth/notifications	ya29. 7R0H IB_YV
ldehner505@gmail.com	com.google	com.google.android.apps.googlevoice:24bb24c05e47e0aefa68a58a766179d9b613a600:oauth2:https://www.googleapis.com/auth/sipregistrar	ya29. ovx3F

Figure 4 Authentication tokens.

The authentication token for this email is used to sign into all google services on the device.

(10 marks) Analysis of phone communications

It is important to recognise that modern communication is spread over many applications and mediums such as email, SMS and other social platforms; each of these applications differ in encryption standards, features provided and data storage. Mobile devices carry a significant amount of forensics artefact surrounding communications; it is simple for an ordinary user to decentralise their communications due to consumer app choice. Out of the total 155 installed app entries found (data\data\com.android.vending\databases\localappstate.db), 13 of them focus entirely on communications. These include applications such as whatsapp, telegram, discord, messenger, viber and the stock communication apps.

Due to the forensic value that can be obtained from these types of artefacts such as identity of parties, message content and time of exchange. These artefacts provide not only contextual understanding but also insight into whether the device has been involved in any illegal activity. The goal is to provide relevant artefacts that can aid the case. To better visualise communications; the figure below depicts all sms and mms communications.

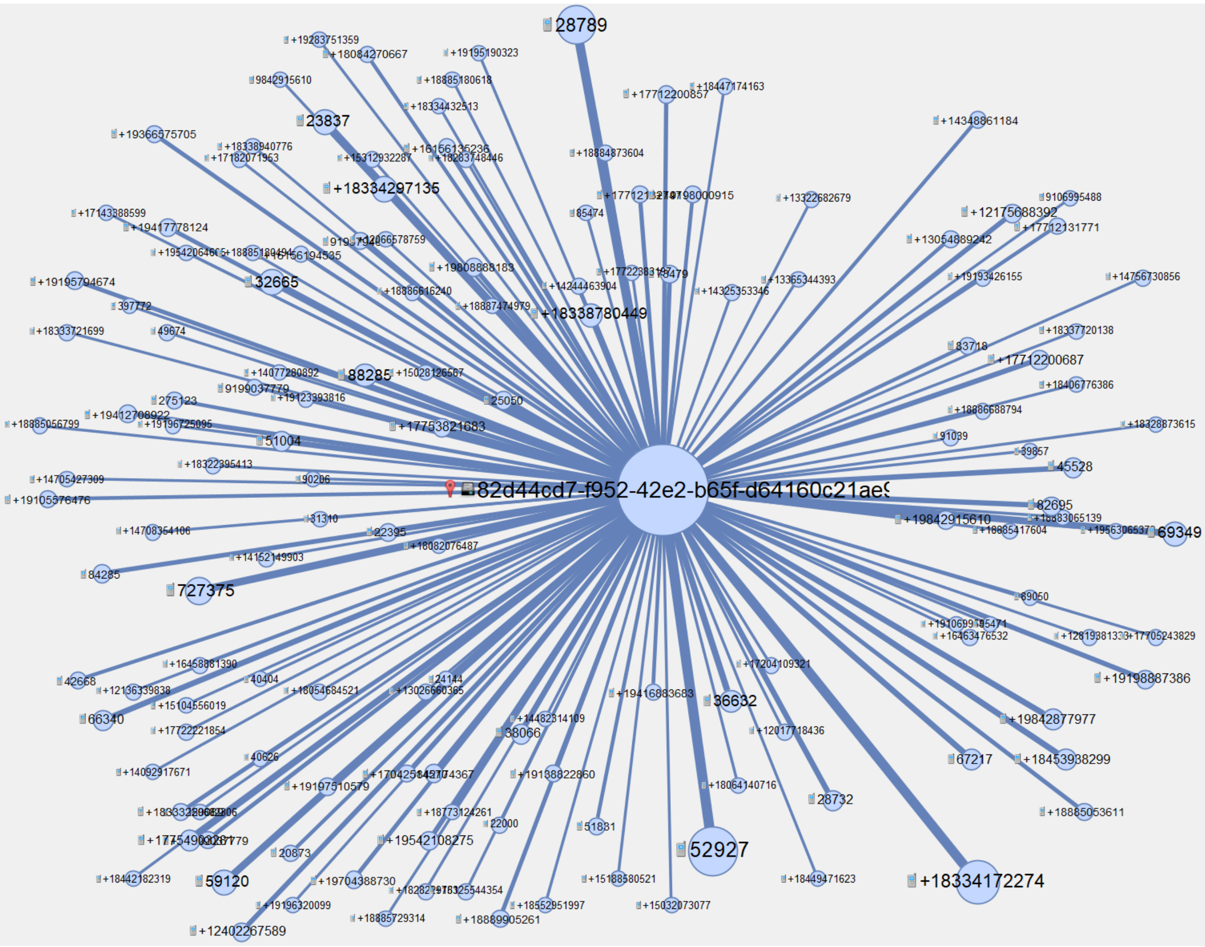


Figure 5 MMSSMS communications visualisation

The larger the labelled bubble is, the higher amount of cumulative traffic that contact received and sent. Addresses of interest such as 52927, will be explored in the following section. To simplify the analysis process, showcased communication artefacts will be limited to the stock telephone communication applications.

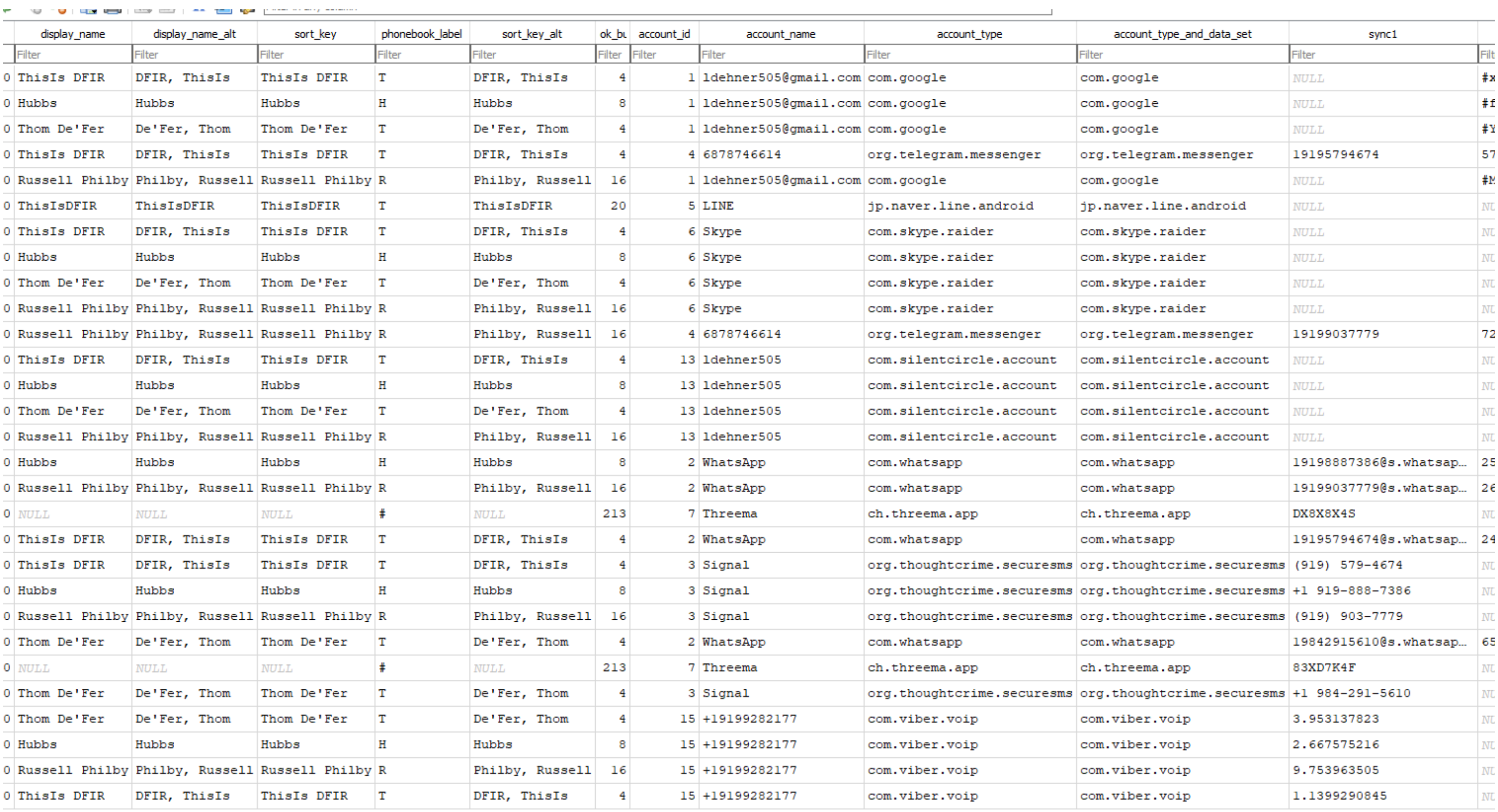
Directory and filename	Artefacts of interest	Purpose
data\data\com.android.providers.contacts\databases\contacts2.db	Contact list	Provides a list of affiliates who the user communicated with, may reveal important thoughts and information leading up to the investigation
data\data\com.android.providers.telephony\databases\mmssms.db	Sms and mms	To gather whether the user did commit the crime and what their motive was based on communication with affiliates,
data\data\com.android.providers.contacts\databases\calllog.db	Call log history	Can “fill in the blanks” when there is missing mms information.

Stock communication apps

The default sms and Dialer application store the users data over various databases; the primary ones that will be studied is the mmssms.db (which stores the various messages and multimedia messages), the calllog.db that provides the users voicemail and call log history; and contacts2.db that contains registered contacts.

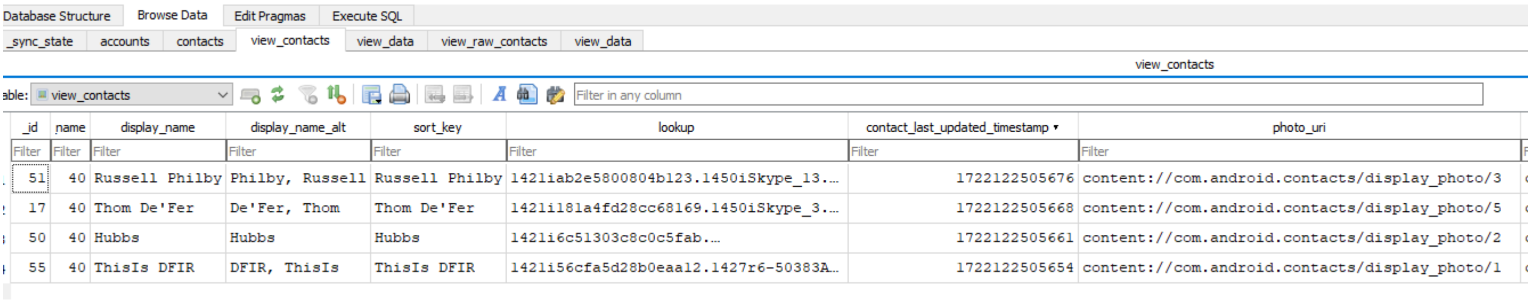
Contacts

By first viewing the contacts2.db in SQLite, registered contacts that the user manually wrote can be seen. These numbers can then be searched for within mmssms.db to find further sms artefacts. This helps in accelerate the forensics process by narrowing communications down to individuals.



	display_name	display_name_alt	sort_key	phonebook_label	sort_key_alt	ok_bu	account_id	account_name	account_type	account_type_and_data_set	sync1	Filt
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filt
0	ThisIs DFIR	DFIR, ThisIs	ThisIs DFIR	T	DFIR, ThisIs	4	1	ldehner505@gmail.com	com.google	com.google	NULL	#x
0	Hubbs	Hubbs	Hubbs	H	Hubbs	8	1	ldehner505@gmail.com	com.google	com.google	NULL	#f
0	Thom De'Fer	De'Fer, Thom	Thom De'Fer	T	De'Fer, Thom	4	1	ldehner505@gmail.com	com.google	com.google	NULL	#Y
0	ThisIs DFIR	DFIR, ThisIs	ThisIs DFIR	T	DFIR, ThisIs	4	4	6878746614	org.telegram.messenger	org.telegram.messenger	19195794674	57
0	Russell Philby	Philby, Russell	Russell Philby	R	Philby, Russell	16	1	ldehner505@gmail.com	com.google	com.google	NULL	#M
0	ThisIsDFIR	ThisIsDFIR	ThisIsDFIR	T	ThisIsDFIR	20	5	LINE	jp.naver.line.android	jp.naver.line.android	NULL	NU
0	ThisIs DFIR	DFIR, ThisIs	ThisIs DFIR	T	DFIR, ThisIs	4	6	Skype	com.skype.raider	com.skype.raider	NULL	NU
0	Hubbs	Hubbs	Hubbs	H	Hubbs	8	6	Skype	com.skype.raider	com.skype.raider	NULL	NU
0	Thom De'Fer	De'Fer, Thom	Thom De'Fer	T	De'Fer, Thom	4	6	Skype	com.skype.raider	com.skype.raider	NULL	NU
0	Russell Philby	Philby, Russell	Russell Philby	R	Philby, Russell	16	6	Skype	com.skype.raider	com.skype.raider	NULL	NU
0	Russell Philby	Philby, Russell	Russell Philby	R	Philby, Russell	16	4	6878746614	org.telegram.messenger	org.telegram.messenger	19199037779	72
0	ThisIs DFIR	DFIR, ThisIs	ThisIs DFIR	T	DFIR, ThisIs	4	13	ldehner505	com.silentcircle.account	com.silentcircle.account	NULL	NU
0	Hubbs	Hubbs	Hubbs	H	Hubbs	8	13	ldehner505	com.silentcircle.account	com.silentcircle.account	NULL	NU
0	Thom De'Fer	De'Fer, Thom	Thom De'Fer	T	De'Fer, Thom	4	13	ldehner505	com.silentcircle.account	com.silentcircle.account	NULL	NU
0	Russell Philby	Philby, Russell	Russell Philby	R	Philby, Russell	16	13	ldehner505	com.silentcircle.account	com.silentcircle.account	NULL	NU
0	Hubbs	Hubbs	Hubbs	H	Hubbs	8	2	WhatsApp	com.whatsapp	com.whatsapp	19198887386@s.whatsap...	25
0	Russell Philby	Philby, Russell	Russell Philby	R	Philby, Russell	16	2	WhatsApp	com.whatsapp	com.whatsapp	19199037779@s.whatsap...	26
0	NULL	NULL	NULL	#	NULL	213	7	Threema	ch.threema.app	ch.threema.app	DX8X8X4S	NU
0	ThisIs DFIR	DFIR, ThisIs	ThisIs DFIR	T	DFIR, ThisIs	4	2	WhatsApp	com.whatsapp	com.whatsapp	19195794674@s.whatsap...	24
0	ThisIs DFIR	DFIR, ThisIs	ThisIs DFIR	T	DFIR, ThisIs	4	3	Signal	org.thoughtcrime.securesms	org.thoughtcrime.securesms	(919) 579-4674	NU
0	Hubbs	Hubbs	Hubbs	H	Hubbs	8	3	Signal	org.thoughtcrime.securesms	org.thoughtcrime.securesms	+1 919-888-7386	NU
0	Russell Philby	Philby, Russell	Russell Philby	R	Philby, Russell	16	3	Signal	org.thoughtcrime.securesms	org.thoughtcrime.securesms	(919) 903-7779	NU
0	Thom De'Fer	De'Fer, Thom	Thom De'Fer	T	De'Fer, Thom	4	2	WhatsApp	com.whatsapp	com.whatsapp	19842915610@s.whatsap...	65
0	NULL	NULL	NULL	#	NULL	213	7	Threema	ch.threema.app	ch.threema.app	83XD7K4F	NU
0	Thom De'Fer	De'Fer, Thom	Thom De'Fer	T	De'Fer, Thom	4	3	Signal	org.thoughtcrime.securesms	org.thoughtcrime.securesms	+1 984-291-5610	NU
0	Thom De'Fer	De'Fer, Thom	Thom De'Fer	T	De'Fer, Thom	4	15	+19199282177	com.viber.voip	com.viber.voip	3.953137823	NU
0	Hubbs	Hubbs	Hubbs	H	Hubbs	8	15	+19199282177	com.viber.voip	com.viber.voip	2.667575216	NU
0	Russell Philby	Philby, Russell	Russell Philby	R	Philby, Russell	16	15	+19199282177	com.viber.voip	com.viber.voip	9.753963505	NU
0	ThisIs DFIR	DFIR, ThisIs	ThisIs DFIR	T	DFIR, ThisIs	4	15	+19199282177	com.viber.voip	com.viber.voip	1.1399290845	NU

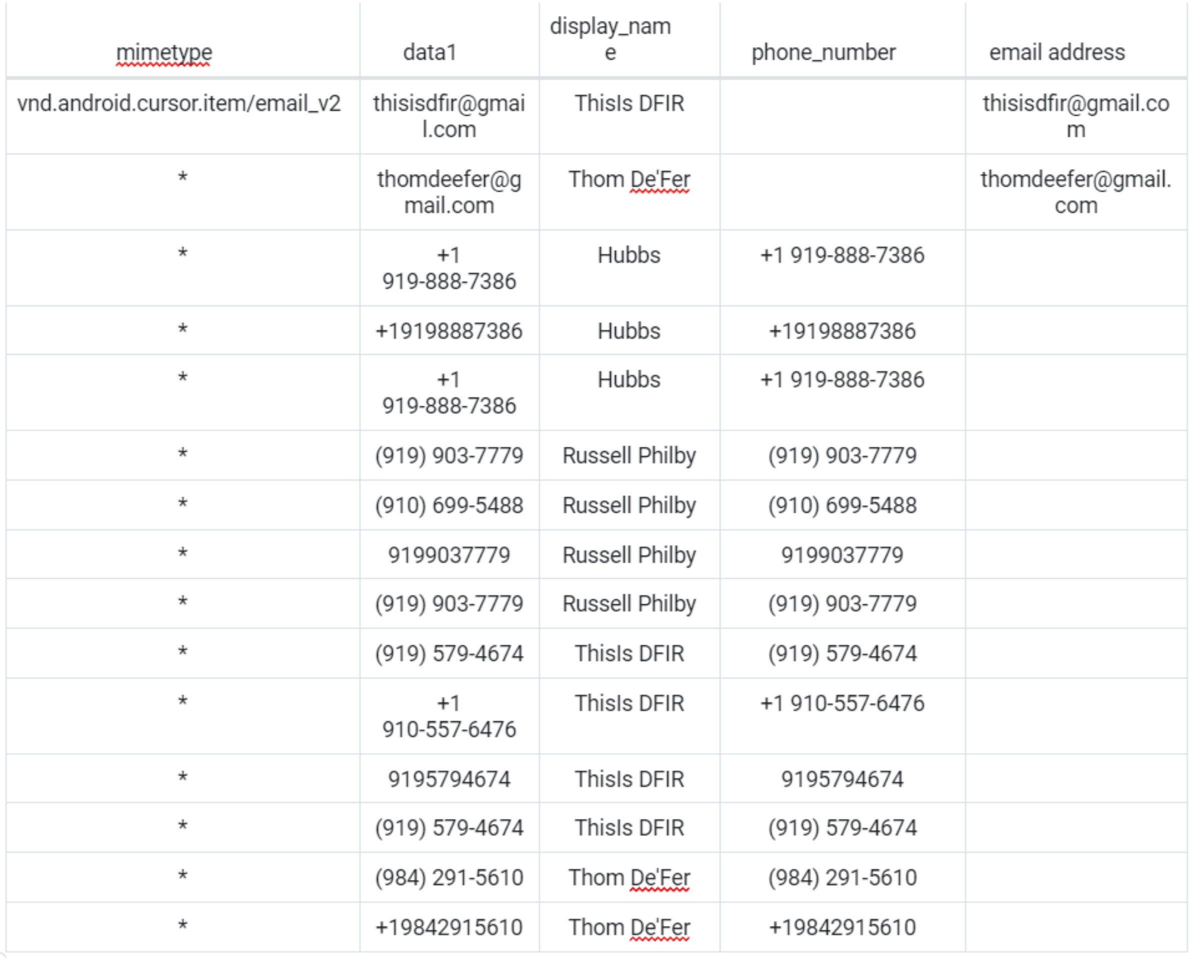
Figure 6 raw contacts view



_id	name	display_name	display_name_alt	sort_key	lookup	contact_last_updated_timestamp	photo_uri
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
51	40	Russell Philby	Philby, Russell	Russell Philby	1421iab2e5800804b123.1450iSkype_13...	1722122505676	content://com.android.contacts/display_photo/3
17	40	Thom De'Fer	De'Fer, Thom	Thom De'Fer	1421i181a4fd28cc68169.1450iSkype_3...	1722122505668	content://com.android.contacts/display_photo/5
50	40	Hubbs	Hubbs	Hubbs	1421i6c51303c8c0c5fab....	1722122505661	content://com.android.contacts/display_photo/2
55	40	ThisIs DFIR	DFIR, ThisIs	ThisIs DFIR	1421i56cfa5d28b0eaa12.1427r6-50383A...	1722122505654	content://com.android.contacts/display_photo/1

Figure 7 contacts view

The contacts tables reveal a great deal of information about the contacted users including names, phone numbers, addresses, account type, date last contacted and where the icon is stored. This data forms an information base that can be used to begin further communication forensics

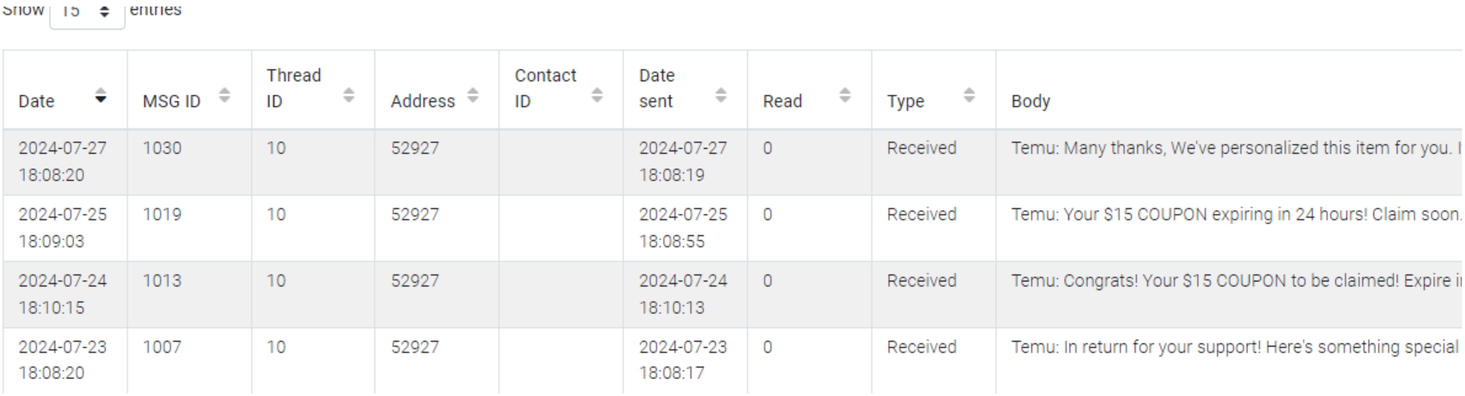


mimetype	data1	display_name	phone_number	email address
vnd.android.cursor.item/email_v2	thisisdfir@gmail.com	ThisIs DFIR		thisisdfir@gmail.com
*	thomdeefer@gmail.com	Thom De'Fer		thomdeefer@gmail.com
*	+1 919-888-7386	Hubbs	+1 919-888-7386	
*	+19198887386	Hubbs	+19198887386	
*	+1 919-888-7386	Hubbs	+1 919-888-7386	
*	(919) 903-7779	Russell Philby	(919) 903-7779	
*	(910) 699-5488	Russell Philby	(910) 699-5488	
*	9199037779	Russell Philby	9199037779	
*	(919) 903-7779	Russell Philby	(919) 903-7779	
*	(919) 579-4674	ThisIs DFIR	(919) 579-4674	
*	+1 910-557-6476	ThisIs DFIR	+1 910-557-6476	
*	9195794674	ThisIs DFIR	9195794674	
*	(919) 579-4674	ThisIs DFIR	(919) 579-4674	
*	(984) 291-5610	Thom De'Fer	(984) 291-5610	
*	+19842915610	Thom De'Fer	+19842915610	

Figure 8 summary of contacts

SMS and MMS database

ALEAPP will be used as a frontend for the sms databases; ALEAP analyses the tables and sorts them into important data for faster artefact selection. As shown in figure 5 some notable contacts that received a large portion of traffic include 52927 and 18334172274.



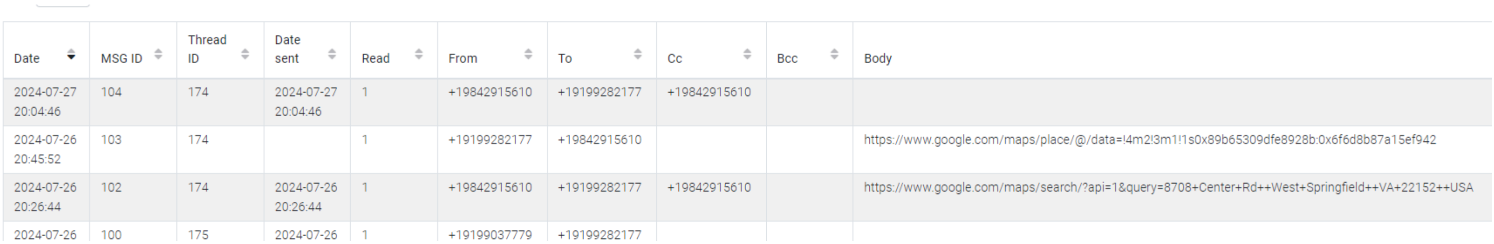
Show 15 entries

Date	MSG ID	Thread ID	Address	Contact ID	Date sent	Read	Type	Body
2024-07-27 18:08:20	1030	10	52927		2024-07-27 18:08:19	0	Received	Temu: Many thanks, We've personalized this item for you. I
2024-07-25 18:09:03	1019	10	52927		2024-07-25 18:08:55	0	Received	Temu: Your $15 COUPON expiring in 24 hours! Claim soon.
2024-07-24 18:10:15	1013	10	52927		2024-07-24 18:10:13	0	Received	Temu: Congrats! Your $15 COUPON to be claimed! Expire i
2024-07-23 18:08:20	1007	10	52927		2024-07-23 18:08:17	0	Received	Temu: In return for your support! Here's something special

Figure 9 depicts 52927 sms

The number with the highest traffic shows the user is an avid Temu user(245 entries). Looking through these messages, key words such as knives, delivery addresses or electronics can be used to garner purchased items; for criminal court cases, this may reveal weapons or items potentially relevant to the case. 18334172274 reveals the financial app (Cash app) that was likely used to purchase these items (173 recorded entries).

ALEAP conveniently categorises all MMS and SMS database entries that can be viewed separately. Since there were little sms threads on the registered contacts, viewing all mms messages we can see several exchanges between Thom De'Fer. These include sending location of a fireworks store and meeting locations.



Date	MSG ID	Thread ID	Date sent	Read	From	To	Cc	Bcc	Body
2024-07-27 20:04:46	104	174	2024-07-27 20:04:46	1	+19842915610	+19199282177	+19842915610		
2024-07-26 20:45:52	103	174		1	+19199282177	+19842915610			https://www.google.com/maps/place/@/data=!4m2!3m1!1s0x89b65309dfe8928b:0x6f6d8b87a15ef942
2024-07-26 20:26:44	102	174	2024-07-26 20:26:44	1	+19842915610	+19199282177	+19842915610		https://www.google.com/maps/search/?api=1&query=8708+Center+Rd++West+Springfield++VA+22152++USA
2024-07-26	100	175	2024-07-26	1	+19199037779	+19199282177			

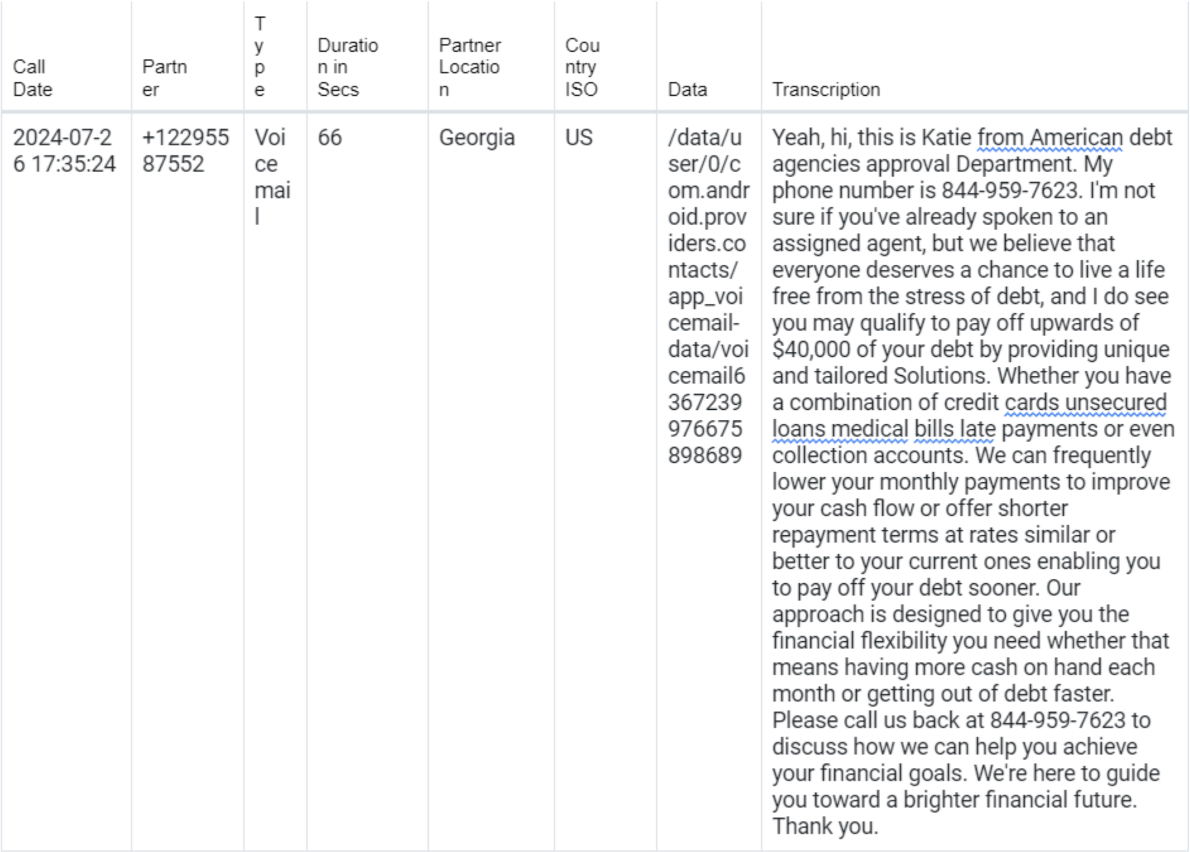
Figure 10 MMS artefact

- 8708 Center Rd, West Springfield, VA 22152, USA
- “Gorilla fireworks” 9598 Old Keene Mill Rd, Burke, VA 22015, United States

Within these messages, additional contacts can be found such as the number of the users immediately family circle and other affiliates.

Dialer call logs Database

SMS and MMS only provide information based on direct messaging, this creates blank timeline entries which may be fixed by analysing call log history. Call log history can be spread over many applications. The stock dialer app for android stores all call history via the calllog.db.



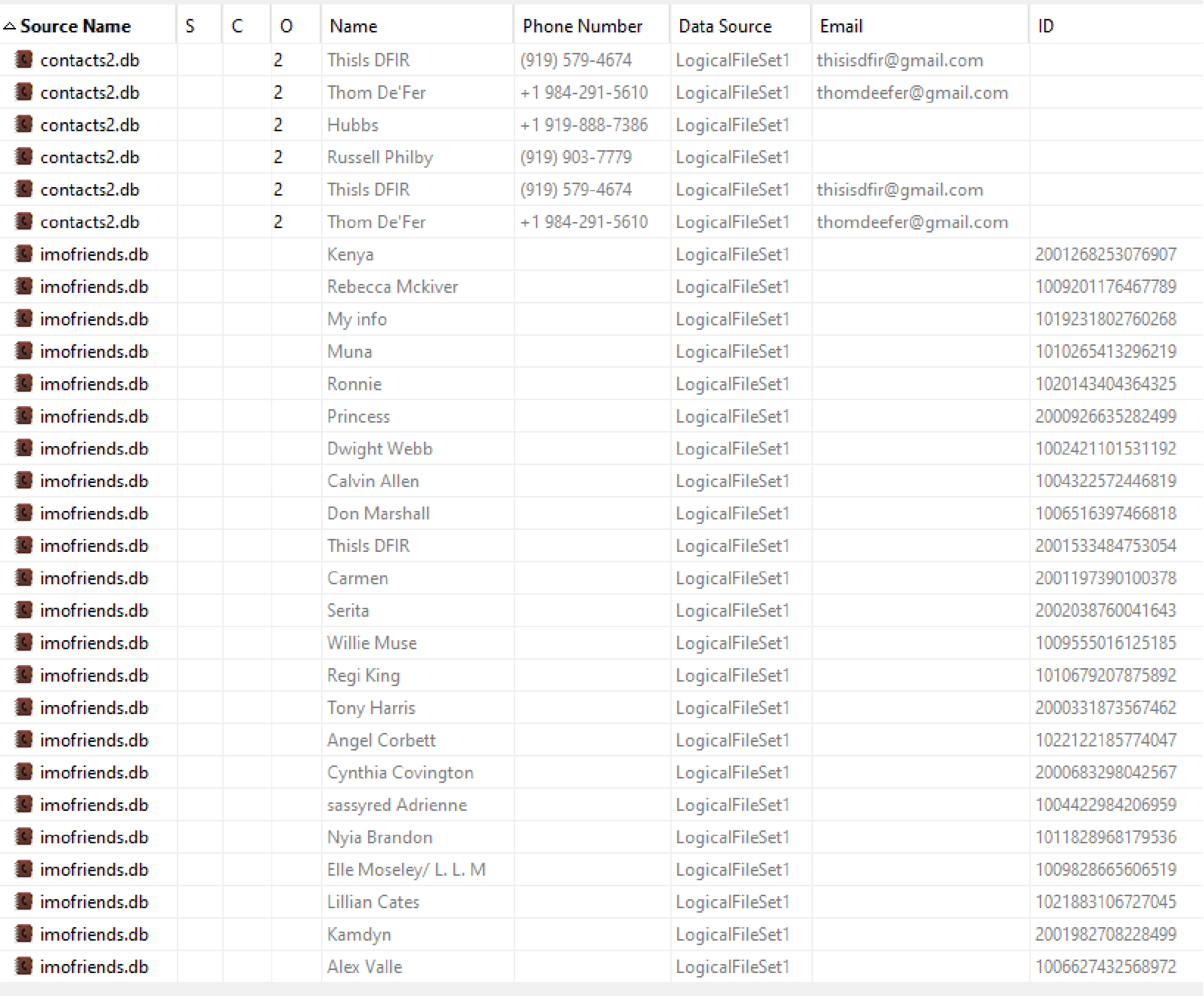
Call Date	Partner	Type	Duration in Secs	Partner Location	Country ISO	Data	Transcription
2024-07-26 17:35:24	+12295587552	Voicemail	66	Georgia	US	/data/user/0/com.android.providers.contacts/app_voicemail-data/voicemail6367239976675898689	Yeah, hi, this is Katie from American debt agencies approval Department. My phone number is 844-959-7623. I'm not sure if you've already spoken to an assigned agent, but we believe that everyone deserves a chance to live a life free from the stress of debt, and I do see you may qualify to pay off upwards of $40,000 of your debt by providing unique and tailored Solutions. Whether you have a combination of credit cards unsecured loans medical bills late payments or even collection accounts. We can frequently lower your monthly payments to improve your cash flow or offer shorter repayment terms at rates similar or better to your current ones enabling you to pay off your debt sooner. Our approach is designed to give you the financial flexibility you need whether that means having more cash on hand each month or getting out of debt faster. Please call us back at 844-959-7623 to discuss how we can help you achieve your financial goals. We're here to guide you toward a brighter financial future. Thank you.

Figure 11 call log artefact

Figure 11 depicts the contents of a business voicemail that contacted the user. The call log database provides critical insight into which individual was contacted, duration, country of origin and if possible a transcript of a voicemail. This enables digital forensics specialists to build a timeline of communication that can map the artefacts over the suspected crime period; thus visualising who was contacted during this time.

Other communication apps

In total Autopsy found 405 total contacts across the communication apps; many of these included accounts by the same individual such as Thom having both whatsapp, viber and a stock dialer entry.



Source Name	S	C	O	Name	Phone Number	Data Source	Email	ID
contacts2.db			2	ThisIs DFIR	(919) 579-4674	LogicalFileSet1	thisisdfir@gmail.com	
contacts2.db			2	Thom De'Fer	+1 984-291-5610	LogicalFileSet1	thomdeefer@gmail.com	
contacts2.db			2	Hubbs	+1 919-888-7386	LogicalFileSet1		
contacts2.db			2	Russell Philby	(919) 903-7779	LogicalFileSet1		
contacts2.db			2	ThisIs DFIR	(919) 579-4674	LogicalFileSet1	thisisdfir@gmail.com	
contacts2.db			2	Thom De'Fer	+1 984-291-5610	LogicalFileSet1	thomdeefer@gmail.com	
imofriends.db				Kenya		LogicalFileSet1		2001268253076907
imofriends.db				Rebecca Mckiver		LogicalFileSet1		1009201176467789
imofriends.db				My info		LogicalFileSet1		1019231802760268
imofriends.db				Muna		LogicalFileSet1		1010265413296219
imofriends.db				Ronnie		LogicalFileSet1		1020143404364325
imofriends.db				Princess		LogicalFileSet1		2000926635282499
imofriends.db				Dwight Webb		LogicalFileSet1		1002421101531192
imofriends.db				Calvin Allen		LogicalFileSet1		1004322572446819
imofriends.db				Don Marshall		LogicalFileSet1		1006516397466818
imofriends.db				ThisIs DFIR		LogicalFileSet1		2001533484753054
imofriends.db				Carmen		LogicalFileSet1		2001197390100378
imofriends.db				Serita		LogicalFileSet1		2002038760041643
imofriends.db				Willie Muse		LogicalFileSet1		1009555016125185
imofriends.db				Regi King		LogicalFileSet1		1010679207875892
imofriends.db				Tony Harris		LogicalFileSet1		2000331873567462
imofriends.db				Angel Corbett		LogicalFileSet1		1022122185774047
imofriends.db				Cynthia Covington		LogicalFileSet1		2000683298042567
imofriends.db				sassyred Adrienne		LogicalFileSet1		1004422984206959
imofriends.db				Nyia Brandon		LogicalFileSet1		1011828968179536
imofriends.db				Elle Moseley/ L. L. M		LogicalFileSet1		1009828665606519
imofriends.db				Lillian Cates		LogicalFileSet1		1021883106727045
imofriends.db				Kamdyn		LogicalFileSet1		2001982708228499
imofriends.db				Alex Valle		LogicalFileSet1		1006627432568972

Figure 12 excerpt from Autopsy contact list

Although not all apps will be studied within this report, it is important to convey how decentralised communication between individuals are. These lines of communication often cross devices and apps; and with the increase in consumer choice, forensics specialists will need to consider where important artefacts will be found.

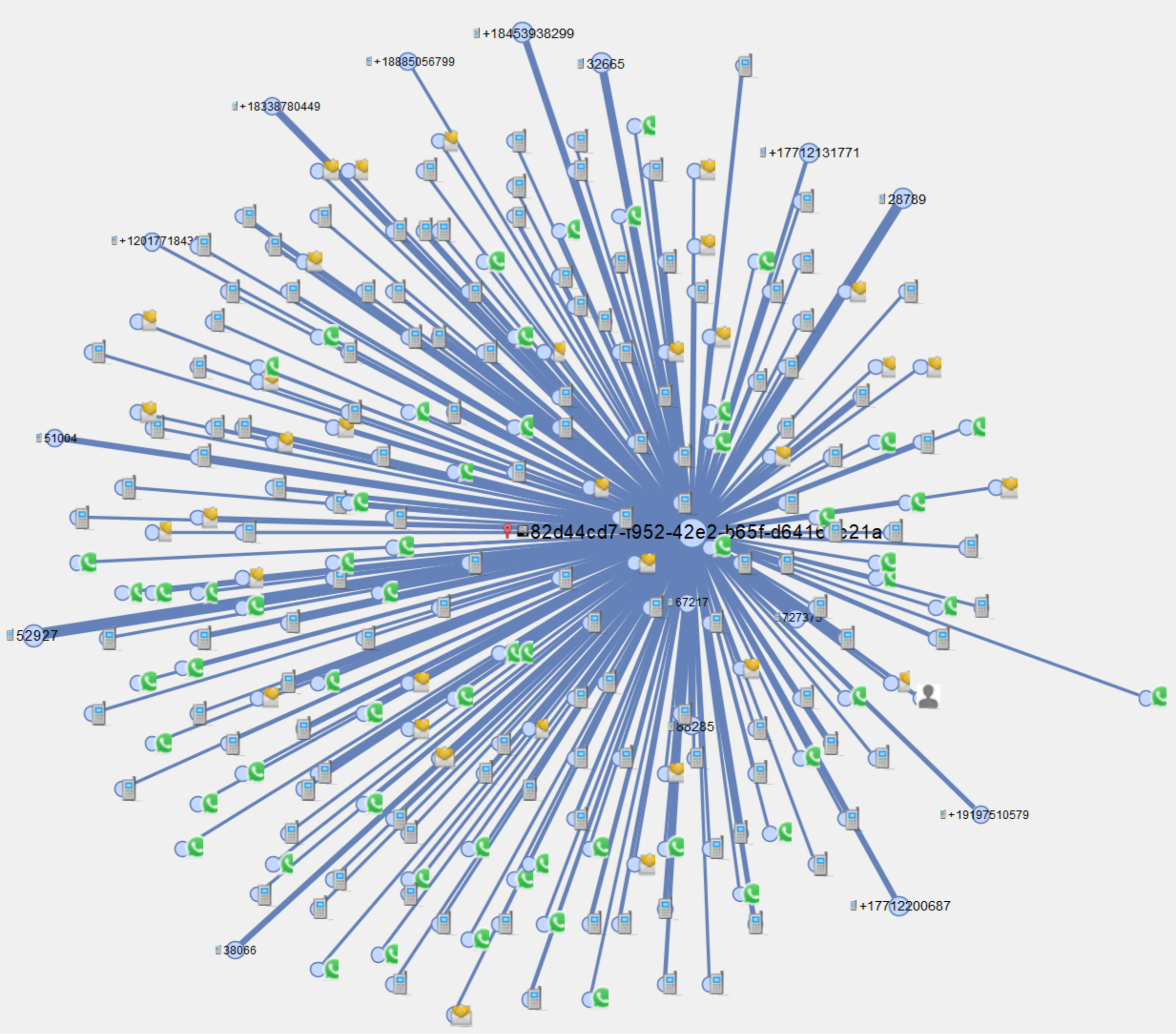


Figure 13 depicts all communications across 5 device communication apps

(20 marks) Analysis of two applications

Chrome Browser

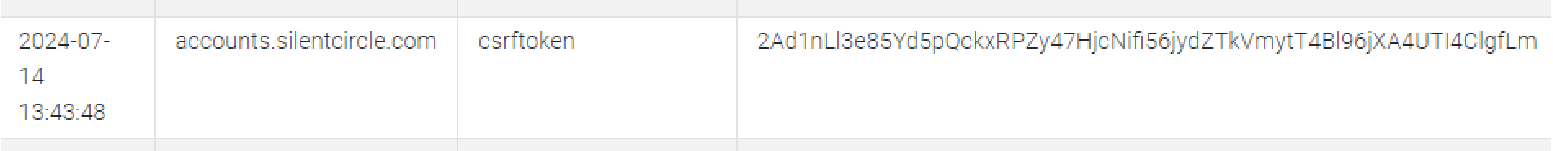
Browsers are arguably one of the most important portals to access the internet with over 3.25 Billion users. Google chrome browser will naturally contain a great deal of forensics artefacts that should be analysed and explored. Browsers provide a journey of users' online activity, thus they play a vital role in Incident response and forensics. The following tables contain the databases and files that will be explored through hex and sqlite viewers; artefacts of forensics interest can then be extracted to be reported. To depict how journey mapping is conducted through mobile forensics, the “silent circle” website will be depicted through showcased artefacts.

Directory and File Name	Data stored	Purpose
\data\data\com.android.chrome\app_chrome\Default\Cookies	Cookies	Contains text that websites generate for various reasons such as login auth tokens, data from forms and location. The purpose is better functionality with websites a user visits often.
\data\data\com.android.chrome\app_chrome\Default\History	History	Keyword searches, web visits and history are all stored in this file
\data\data\com.android.chrome\cache	Chrome browser cache	Cache is used to store various site data such as images, javascript, html pages for a faster viewing experience.
\data\data\com.android.chrome\app_chrome\Default\Web Data	Autofill	Search terms, bank details, addresses etc. chrome provides this feature for user convenience

Cookies

Although they enhance users' internet surfing experience, they also pose a privacy and security risk as important details filled out on websites such as geolocation are held for tracking purposes. For Forensics purposes, it provides a great deal of user information such as address information from online commerce, shopping cart history, account logins and forms filled. Additionally, it is important to take note of the creation date as similarly to history, it provides a timeline marker of when the account was signed into; thus aiding in building the digital persona of the individual.

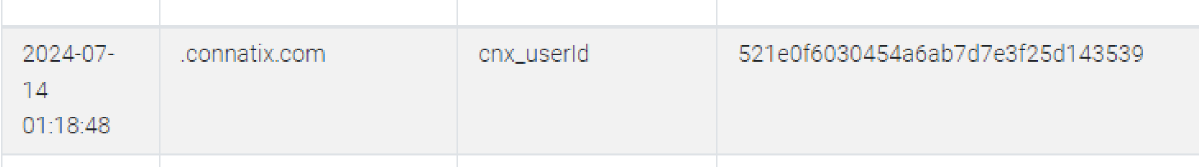
There are a total of 703 cookies entries that range from account uids to consent forms, the following figures depict interesting artefacts that may be of forensic use.



2024-07-14 13:43:48	accounts.silentcircle.com	csrftoken	2Ad1nLl3e85Yd5pQckxRPZy47HjcNifi56jydZTkVmytT4Bl96jXA4UTI4ClgfLm

Figure 14 depicts a csrftoken

In the above figure is a possible cookie of a CSRF token. To circumvent the security flaws of cookies, many websites protect account cookies from cross site request forgery through these synchronising tokens that authenticate requests.



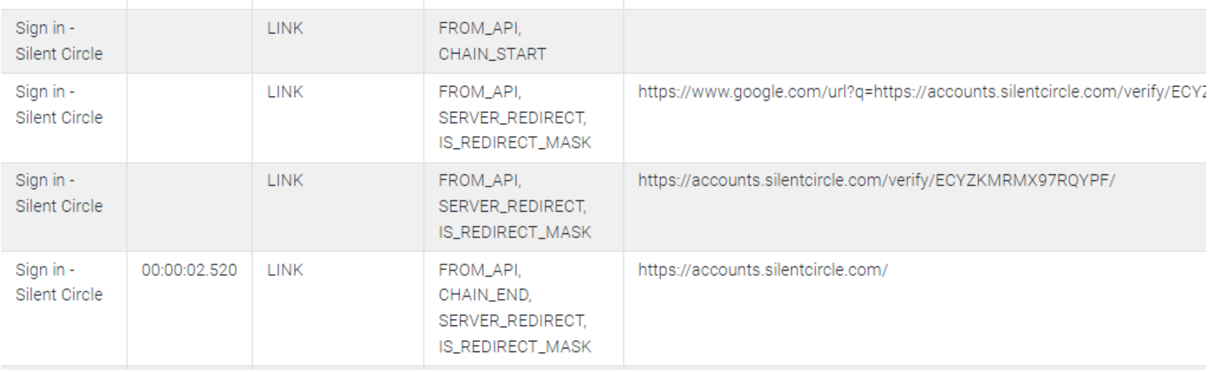
2024-07-14 01:18:48	.connatix.com	cnx_userId	521e0f6030454a6ab7d7e3f25d143539

Figure 15 userid of a website

Cookies that contain usernames and passwords provide insight into the accounts the device owner has. By acquiring user account information, law enforcement can ask the company for further data such as purchase history, user activity and forum interactions; if the warrant/case allows it. This type of cookie is known as *persistent* as it comes with an expiry date (2024-08-13 01:14:54). Other cookies such as session, encrypted and third party can also be found.

History

History is the primary method of journey mapping as it provides detailed description of the site visited, when it was visited and how the user interacted with the site (APIs, requests etc).

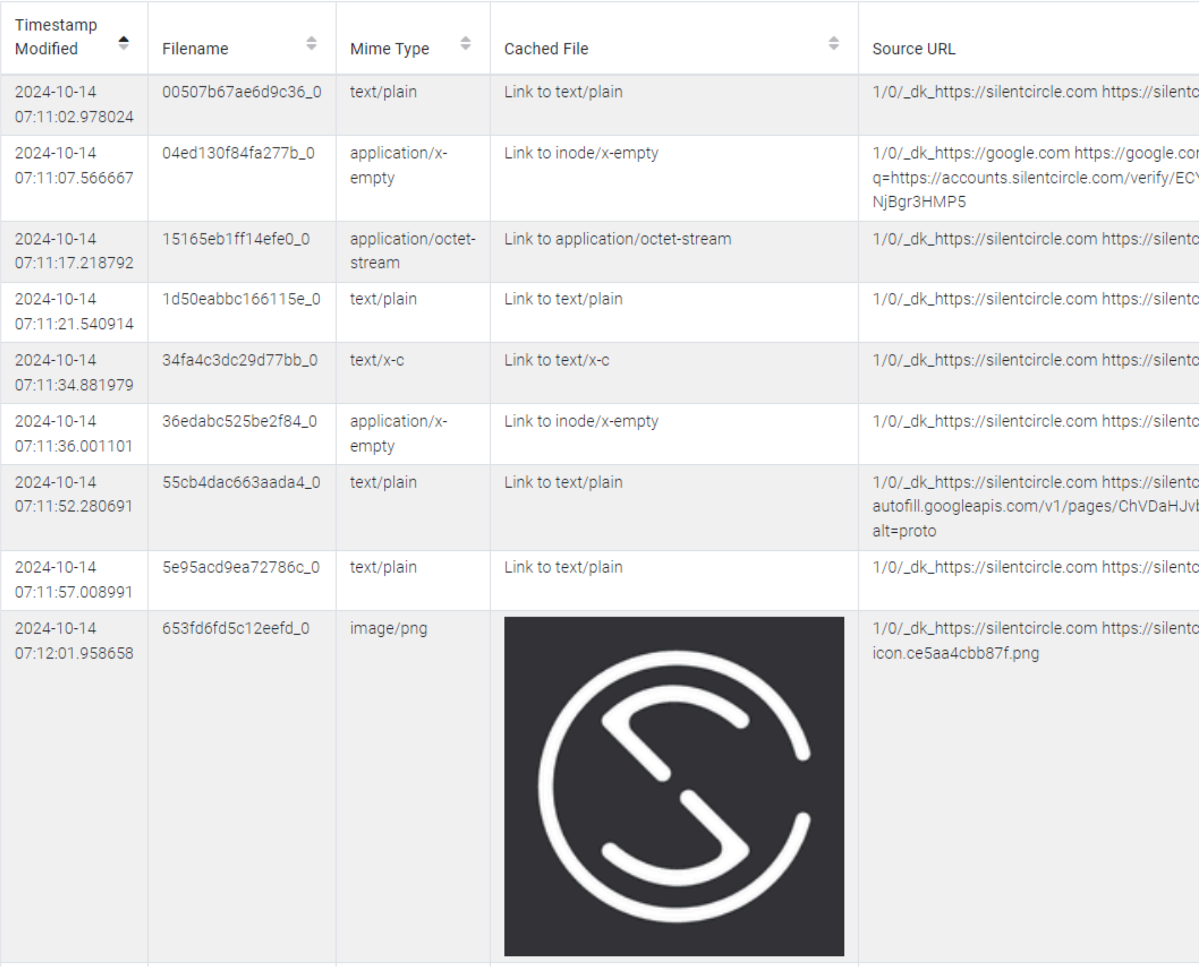


Sign in - Silent Circle		LINK	FROM_API, CHAIN_START	
Sign in - Silent Circle		LINK	FROM_API, SERVER_REDIRECT, IS_REDIRECT_MASK	https://www.google.com/url?q=https://accounts.silentcircle.com/verify/ECYZ
Sign in - Silent Circle		LINK	FROM_API, SERVER_REDIRECT, IS_REDIRECT_MASK	https://accounts.silentcircle.com/verify/ECYZKMRMX97RQYPF/
Sign in - Silent Circle	00:00:02.520	LINK	FROM_API, CHAIN_END, SERVER_REDIRECT, IS_REDIRECT_MASK	https://accounts.silentcircle.com/

Figure 16 excerpt of chrome history file

Cache

The primary way cache differs to history and cookies is the ability to see the contents of the webpages that have been visited. This uniquely provides insight into users' habits they exhibit when browsing the internet. Cache downloads pages with the primary purpose of enhancing user experience through loading times. This enables forensic specialists to view whether any pages they visited have incriminating evidence such as images shown in the figure below; or content the user interacted with such as forms, javascript and various other artefacts. When analysing cache, it is important to identify dates, file names and types of files and the url related to the cached item.

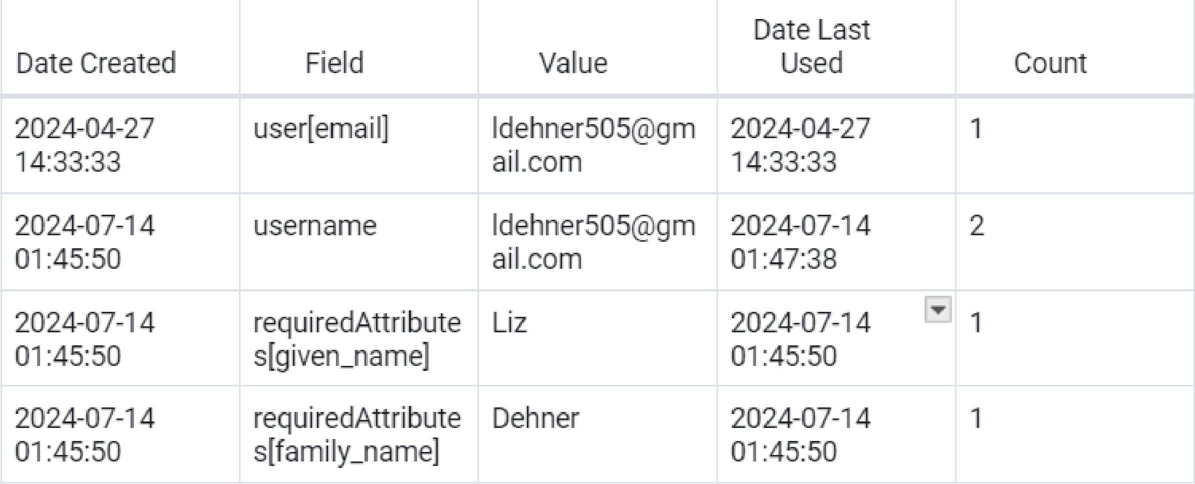


Timestamp Modified	Filename	Mime Type	Cached File	Source URL
2024-10-14 07:11:02.978024	00507b67ae6d9c36_0	text/plain	Link to text/plain	1/0/_dk_https://silentcircle.com https://silentc
2024-10-14 07:11:07.566667	04ed130f84fa277b_0	application/x-empty	Link to inode/x-empty	1/0/_dk_https://google.com https://google.cor q=https://accounts.silentcircle.com/verify/ECY NjBgr3HMP5
2024-10-14 07:11:17.218792	15165eb1ff14efe0_0	application/octet-stream	Link to application/octet-stream	1/0/_dk_https://silentcircle.com https://silentc
2024-10-14 07:11:21.540914	1d50eabbc166115e_0	text/plain	Link to text/plain	1/0/_dk_https://silentcircle.com https://silentc
2024-10-14 07:11:34.881979	34fa4c3dc29d77bb_0	text/x-c	Link to text/x-c	1/0/_dk_https://silentcircle.com https://silentc
2024-10-14 07:11:36.001101	36edabc525be2f84_0	application/x-empty	Link to inode/x-empty	1/0/_dk_https://silentcircle.com https://silentc
2024-10-14 07:11:52.280691	55cb4dac663aada4_0	text/plain	Link to text/plain	1/0/_dk_https://silentcircle.com https://silentc autofill.googleapis.com/v1/pages/ChVDaHJvb alt=proto
2024-10-14 07:11:57.008991	5e95acd9ea72786c_0	text/plain	Link to text/plain	1/0/_dk_https://silentcircle.com https://silentc
2024-10-14 07:12:01.958658	653fd6fd5c12eefd_0	image/png		1/0/_dk_https://silentcircle.com https://silentc icon.ce5aa4cbb87f.png

Figure 17 cache artefact

Autofill

Autofill data, similarly to cookies, provide another source of identity information. When the individual is not known it is important to note any form of account information tied to the device. Autofill is a subtle method of acquiring valuable phone attribution artefacts such as emails, names, mobile numbers and addresses.

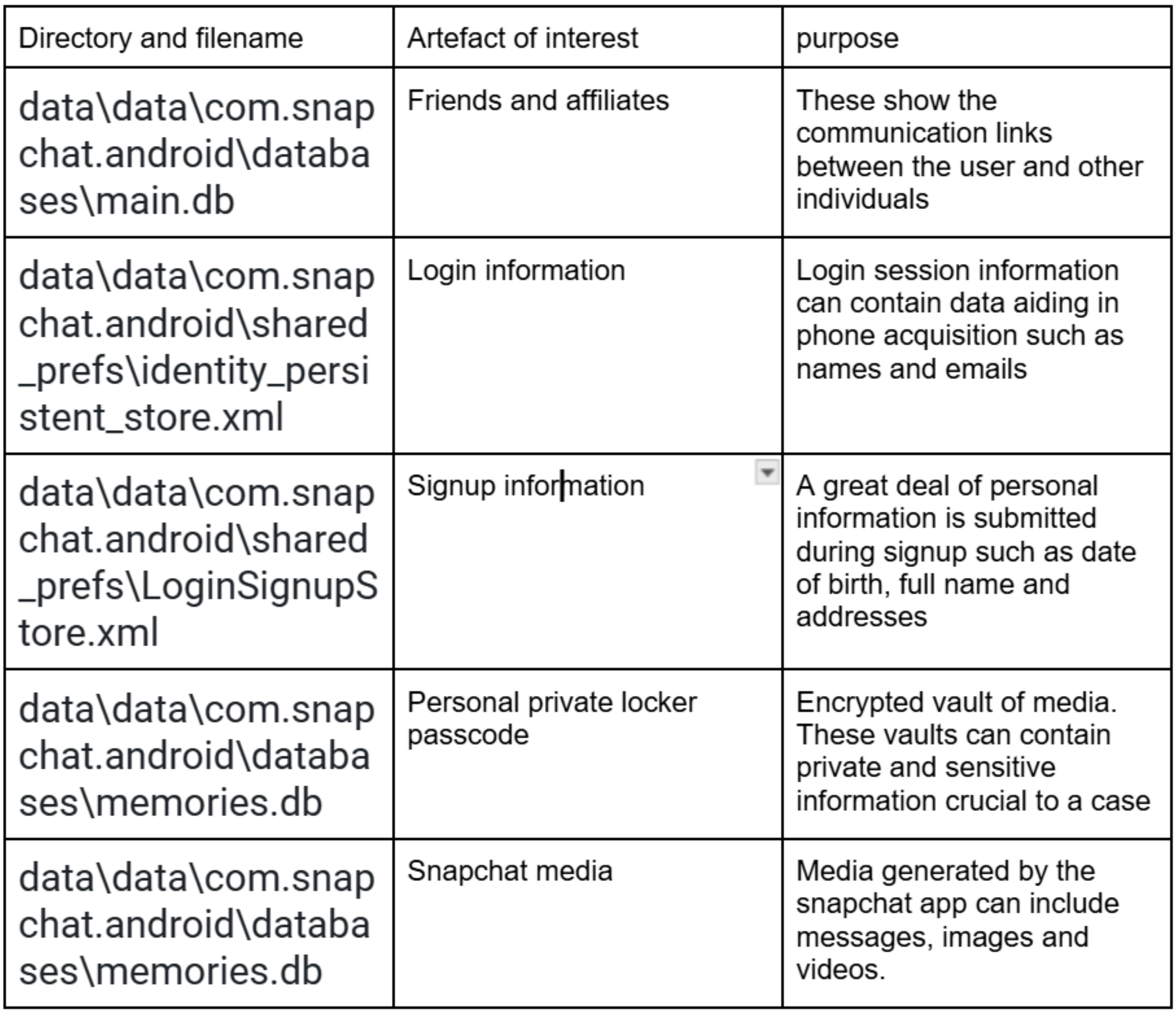


Date Created	Field	Value	Date Last Used	Count
2024-04-27 14:33:33	user[email]	ldehner505@gmail.com	2024-04-27 14:33:33	1
2024-07-14 01:45:50	username	ldehner505@gmail.com	2024-07-14 01:47:38	2
2024-07-14 01:45:50	requiredAttributes[given_name]	Liz	2024-07-14 01:45:50	1
2024-07-14 01:45:50	requiredAttributes[family_name]	Dehner	2024-07-14 01:45:50	1

Figure 18 autofill data

Snapchat

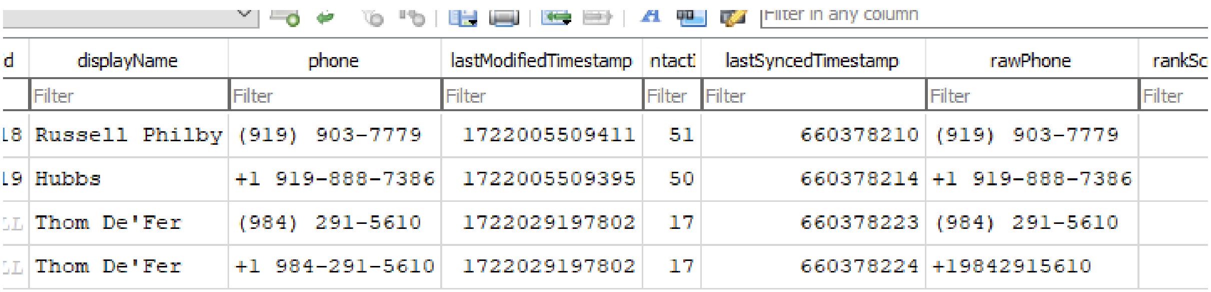
Social media applications can provide unique insight into the users/actors activity. We frequently post our private lives on social media; due to its interconnectivity online, unique artefacts pertaining to our immediate social circle, interests and behaviour can be discovered. This goldmine of forensic information can clearly depict the individuals the user messaged and shared media with; therefore providing user identification artefacts crucial to a criminal case. The following table depicts the databases/files accessed and their directory:



Directory and filename	Artefact of interest	purpose
data\data\com.snapchat.android\databases\main.db	Friends and affiliates	These show the communication links between the user and other individuals
data\data\com.snapchat.android\shared_prefs\identity_persistent_store.xml	Login information	Login session information can contain data aiding in phone acquisition such as names and emails
data\data\com.snapchat.android\shared_prefs\LoginSignupStore.xml	Signup information	A great deal of personal information is submitted during signup such as date of birth, full name and addresses
data\data\com.snapchat.android\databases\memories.db	Personal private locker passcode	Encrypted vault of media. These vaults can contain private and sensitive information crucial to a case
data\data\com.snapchat.android\databases\memories.db	Snapchat media	Media generated by the snapchat app can include messages, images and videos.

Affiliations

Considering snapchat was marketed as a more private solution to social media, the app goes to a great length in order to search for affiliates by analysing user contacts within the contacts2.db. Searching through the main.db, we can find identical contact entries depicted in the below figure:



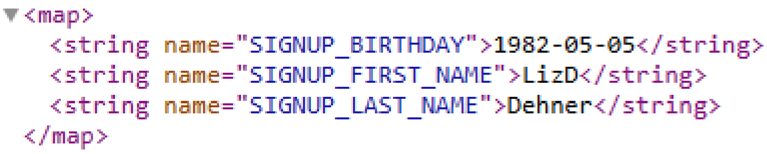
d	displayName	phone	lastModifiedTimestamp	ntact	lastSyncedTimestamp	rawPhone	rankSc
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
18	Russell Philby	(919) 903-7779	1722005509411	51	660378210	(919) 903-7779	
19	Hubbs	+1 919-888-7386	1722005509395	50	660378214	+1 919-888-7386	
LL	Thom De'Fer	(984) 291-5610	1722029197802	17	660378223	(984) 291-5610	
LL	Thom De'Fer	+1 984-291-5610	1722029197802	17	660378224	+19842915610	

Figure 19 snapchat contact taken from contact2.db

Snapchat stores locally a history of all users the device owner interacted with. An artefact of “FriendsWithUsernames” table will not be depicted as snapchat records all users and not just ones manually added, therefore posing a privacy risk.

Login and Signup information

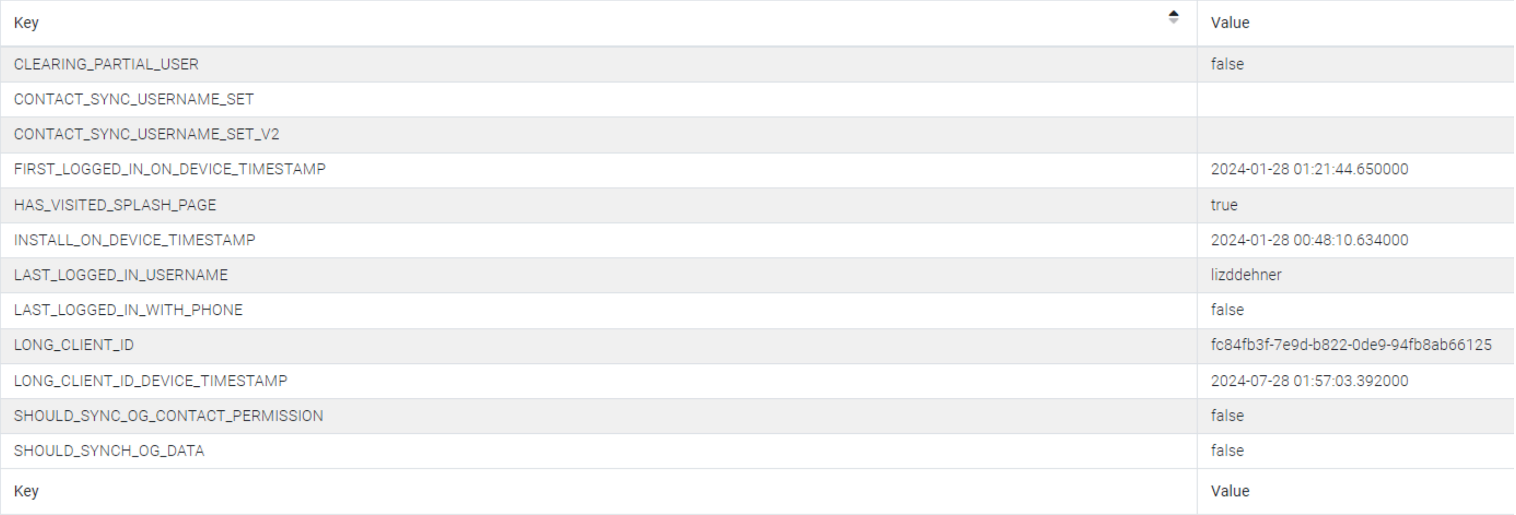
Constructing a timeline of artefacts clearly defines the device owners digital path that may reveal the moments leading up to the crime. The following artefacts depict in an xml identifiable information such as the users date and name.



```
▼<map>
   <string name="SIGNUP_BIRTHDAY">1982-05-05</string>
   <string name="SIGNUP_FIRST_NAME">LizD</string>
   <string name="SIGNUP_LAST_NAME">Dehner</string>
 </map>
```

Figure 20 xml signup

Additional artefacts can be found through the persistent login details that records the most recent login.

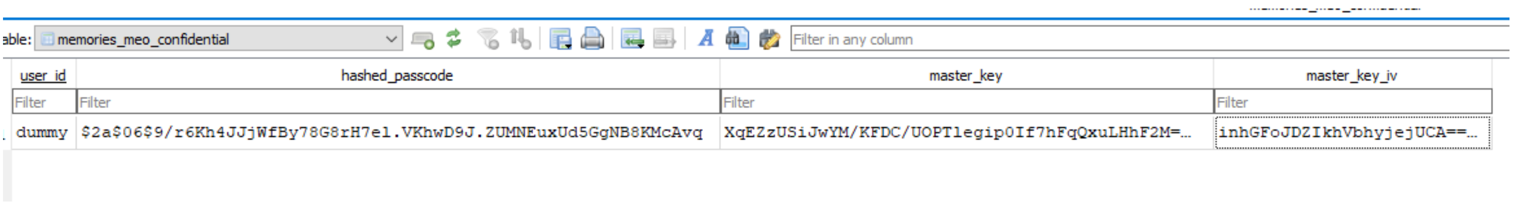


Key	Value
CLEARING_PARTIAL_USER	false
CONTACT_SYNC_USERNAME_SET	
CONTACT_SYNC_USERNAME_SET_V2	
FIRST_LOGGED_IN_ON_DEVICE_TIMESTAMP	2024-01-28 01:21:44.650000
HAS_VISITED_SPLASH_PAGE	true
INSTALL_ON_DEVICE_TIMESTAMP	2024-01-28 00:48:10.634000
LAST_LOGGED_IN_USERNAME	lizddehner
LAST_LOGGED_IN_WITH_PHONE	false
LONG_CLIENT_ID	fc84fb3f-7e9d-b822-0de9-94fb8ab66125
LONG_CLIENT_ID_DEVICE_TIMESTAMP	2024-07-28 01:57:03.392000
SHOULD_SYNC_OG_CONTACT_PERMISSION	false
SHOULD_SYNCH_OG_DATA	false
Key	Value

Figure 21 persistent login details

Personal private locker passcode

The popularisation of encrypted vaults have added an extra challenge for forensic specialists; these vaults can hide very personal and incriminating artefacts that could be vital to a case. During triage, it is important to assess the hashed passwords for their importance and time to cracking. For example, snapchat's My Eyes Only vault uses a four length pin number and an easily identifiable hash:



able: memories_meo_confidential

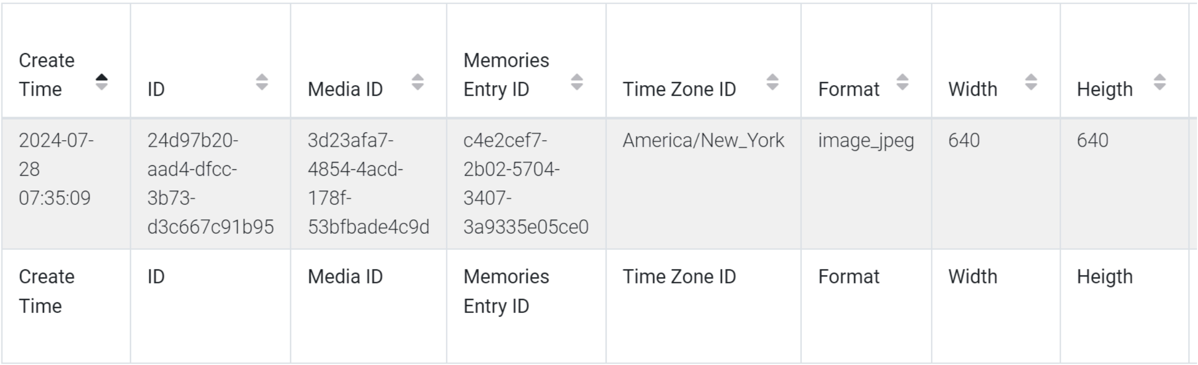
user_id	hashed_passcode	master_key	master_key_iv
Filter	Filter	Filter	Filter
dummy	$2a$06$9/r6Kh4JJjWfBy78G8rH7el.VKhwD9J.ZUMNEuxUd5GgNB8KMcAvq	XqEZzUSiJwYM/KFDC/UOPTlegip0If7hFqQxuLHhF2M=...	inhGFoJDZIkhVbhyjejUCA==...

Figure 22 snapchat MEO hashes

Turns out, using tools like john the ripper or hashcat, the passcode could easily be cracked as there are only 10,000 possible outcomes (pass:1149)! To make this more difficult, snapchat should have included a stronger salt. Before attempting password cracking, it is important to identify the possible length of the password used, the type (numerical or string) and complexity. Many applications require passwords to have a minimum "standard" such as capital letters and special characters, thus increasing time.

Snapchat media

Media uniquely generated can be difficult to pinpoint, especially messages and unsaved photos as within 24 hours they are removed from both the servers and locally. Within memories.db, media such as camera roll, downloaded images and icons can be located. Snapchat stores these images within their file structure and globally accessed storage folders such as DCIM.



Create Time	ID	Media ID	Memories Entry ID	Time Zone ID	Format	Width	Heigth
2024-07-28 07:35:09	24d97b20-aad4-dfcc-3b73-d3c667c91b95	3d23afa7-4854-4acd-178f-53bfbade4c9d	c4e2cef7-2b02-5704-3407-3a9335e05ce0	America/New_York	image_jpeg	640	640
Create Time	ID	Media ID	Memories Entry ID	Time Zone ID	Format	Width	Heigth

Figure 23 snapchat media jpeg

How this project was run

This project was conducted under several limitations and strictly organised into workflows that will streamline the forensic process. These include excluding a large portion of applications, instead analysing a few applications that serve a specific purpose such as communication and internet surfing. This enabled a greater analysis of user activity while showcasing methods used to categorise and extract important artefacts. Initially there was going to be an analysis of another communication application; due to the volume of data it was swapped with a brief explanation and visualisation of communication through some applications for clarity.

The rigid structure was designed to standardise the reporting and retrieval process. This included requiring to place all directories of files used in a table, outlining the purpose of the artefact with a brief description and researching artefacts to speed up acquisition. Additionally, the information collected must be unique and specific either acquired through direct exploration of databases and files or the forensic tools such as Autopsy. For a better artefact visualisation, ALEAPP module within Autopsy was used to gather a summary of detected artefacts. Due to the changing nature of mobile devices, the most popular and current Android version (android 14) is used. In order for all tools that directly interact with the android file system to work; they will be no older than 1 year old.

Challenges encountered and overcome

Mobile forensics is a complex and intricate subject that involves a limitless supply of artefacts. Narrowing down the most important artefacts and file system targets that still portrays the complexity of mobile forensics was a notable challenge. I remedied this through extensive research of android artefacts and selecting general sources of information such as System and App cache, System files for device information and identifiable information such as accounts and app data for phone attribution.

Initial steps were taken to outline the scope and purpose of this report before conducting the forensics analysis. These included researching the various forensic triage tools and various targets within the android file system structure that would be used to acquire artefacts for the investigation.Extensive research was required to utilise current forensic tools and understand how the android file structure was organised. I found a limited supply of forensic tools catered to mobile forensics, the sleuth kits Autopsy was eventually decided as it implements a number of modules that can process logical datasets of the android system.

Image acquisition was the main roadblock due to the security of modern devices and systems; it is difficult to rip a complete file system or generate an image for forensic use without expensive tools such as celebrite. Therefore I had to use an external image generated by a specialist that included data from daily use.

Reflection

The research report was not only challenging but an interesting journey in discovering the complexities of mobile forensics. It required me to think critically about the strategies I would use in ascertaining the right artefacts to showcase. Certain methods I used to speed up data acquisition and narrow things down to the correct artefacts; was to do extensive research into the artefacts i wanted to depict by either reading academic studies or exploring the file structure myself. This simultaneously allowed for a greater understanding of the android subsystem which I initially explored using my phone with adb through android studio.

The phone model used within this report was a google pixel. Research into samsung phone forensics showed a higher level of filesystem isolation making it harder to administrator access to samsung version of android. This represents how different competitors treat their users; whether they prevent access to certain features and administrator abilities or provide more freedom to how a user can interact with their phone's system.

When undertaking app analysis of snapchat, i had to be extraordinarily careful when it came to user privacy. Unlike other apps that limit contacts and friends list to manually added users. Snapchat databases included an extensive number of users which made me believe that most of these were real individuals that had interacted directly with stories. This made me reevaluate how I use my applications and subsequently, led me down a rabbit hole of private alternatives that managed my data better.

Conclusion

Mobile forensics continues to prove the value data has within identifying and mapping individuals to their devices. Phones act as the primary communication tool, therefore it provides critical insights into user activity, temperament and motives through their interactions. Through the various sensors and the applications that utilise them, phone attribution can be achieved by studying the various databases, log and configuration files left behind. Identification is achieved through determining the uuids of hardware and accounts signed in by the user. Thus accurate geolocation and relational data can be mapped, depicting the places the individual visited leading up to the crime. It is important to continuously recognise the role application data has within triage. Internet portals such as google chrome and social media platforms such as snapchat; enable forensic specialists to journey map. A digital timeline can be created of users activity within the web, exposing activities through app data exploration that may be crucial to the case. Through a combination of tools such as Autopsy and methods of artefact determination, a holistic understanding of the mobile forensics triage process can be ascertained.

References

- Oberlo. (n.d.). Most Popular Electronics Worldwide [July 2022 Update]. Www.oberlo.com. https://www.oberlo.com/statistics/most-popular-electronics
    - User statistics, providing
- Colvin, D. (2022, June 10). What is Forensic Triage for Smartphones? Adfsolutions.com; ADF Solutions, Inc. https://www.adfsolutions.com/news/what-is-forensic-triage-for-smartphones?srsltid=AfmBOoop9gkAzbjLJFJLQwo8G-x7nblQcwSOt9Mvec9dUdulKcLwl9vD

  - Stresses the importance of mobile forensic in modern forensic triage. It proves that cases are requiring more experts in managing the legal and technical risks of phones during examination.

Android Image Reference

I would like to thank the Digital forensic practitioner Mr Joshua Hickman, it is through his Android 14 images that this research paper can be completed.

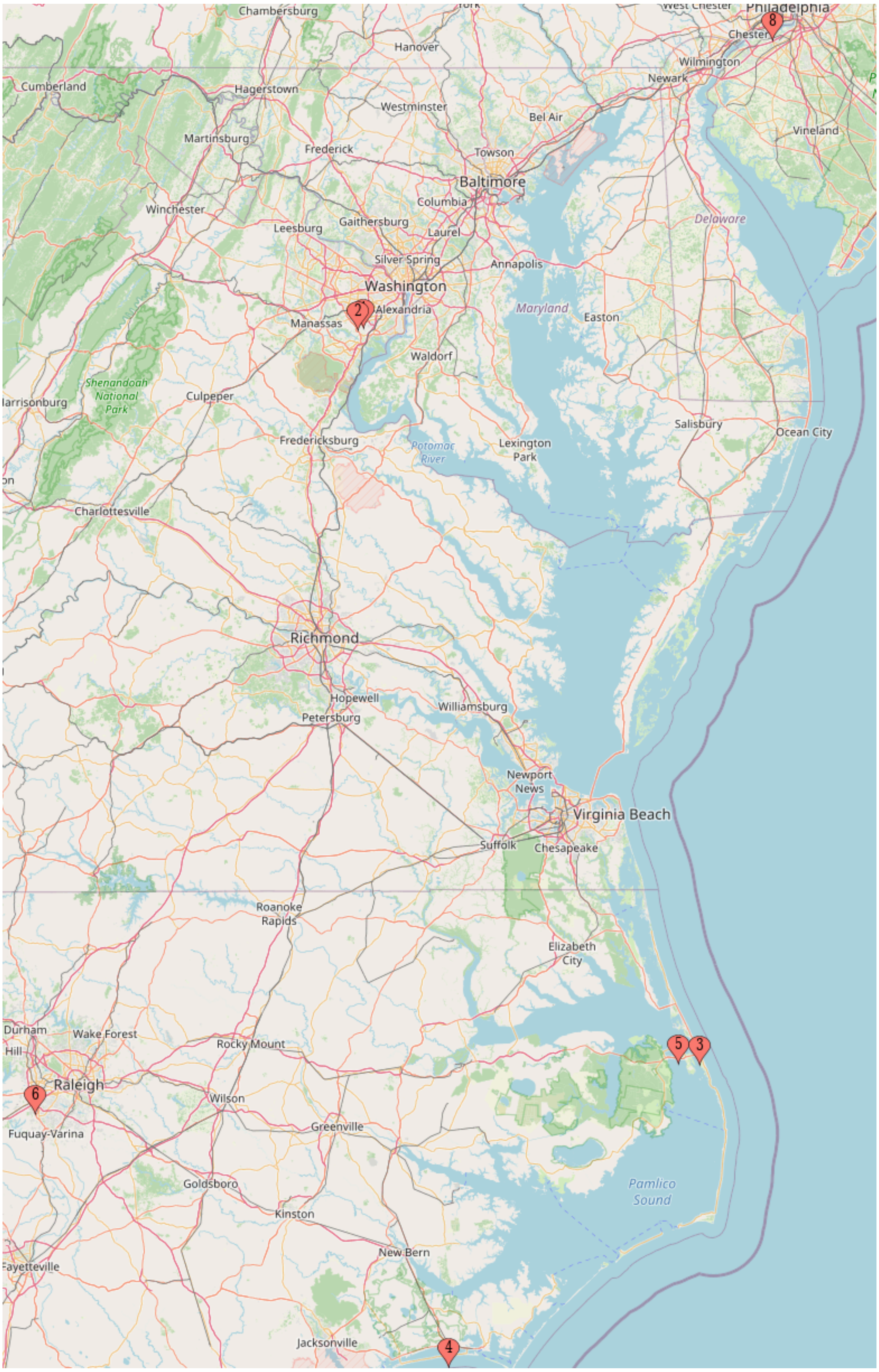
- https://thebinaryhick.blog/public_images/
- https://x.com/josh_hickman1
- https://infosec.exchange/@joshua_hickman1

These images are hosted by Digital corpora, a digital forensic research website.

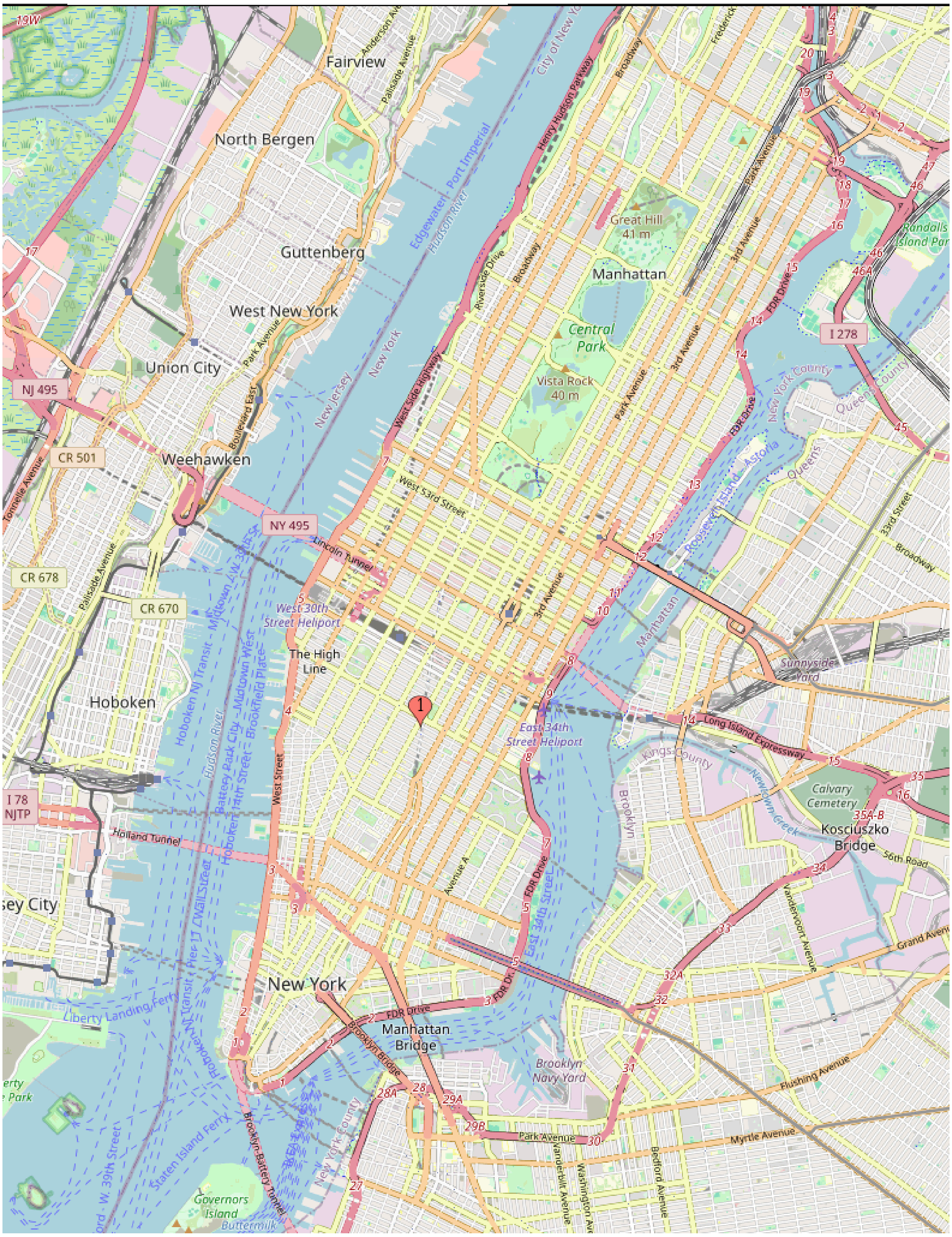
- https://digitalcorpora.org/

Additional visuals

Map of user location activities.



Fitbit geolocation data:



Peer participation

Group Member	%	Reason
Christo-Odysseus Keramitzis	100	Assessment was conducted individually
Total	100%	

Name (PRINTED) : Christo-Odysseus Keramitzis

Student ID: 24488761

SIGNATURE: C.Keramitzis