



Seidenberg School of Computer Science &  
Information Systems

IT 670

---

Mobile Forensics Investigation

---

Jagdeep Kainth

#U01840609

Investigative report(autopsy)

**Lesson 4**

Date – 10/7/2024

Subject – Digital forensics investigation of Cingular\_Sim.ad1 and LG\_LG-VX9100.ad1

**Cingular\_Sim.ad1**

After opening Cingular\_Sim.ad1, we got Unknown\_SIM\_0 which has two files, first one is file system and second is user data. We investigated every single file inside these two files. While searching file system,

**File System**

We found out **AccessControlClass-Bytes : 0001** means that the mobile device so successfully connected to network in the given time frame. **Accumulated count of units 1 : 0** refers to zero

usage of service during a certain time frame. **Maximum value of the Accumulated Call Meter (ACM) : 0** tells that no calls made or received during a certain time frame. **MS\_Operation\_Mode : 00 Additional\_Information : 0000** says that device was actively engaged in mobile service and able to receive calls and messages. Broadcast control channels **Octet 1 : 0x9F, Octet 2 : 0x32, Octet 3 : 0xBF, Octet 4 : 0xEF, Octet 5 : 0xBE** showing the given octets represent different system and network parameters in BCCH messages. System flags are indicated by octet 1, channel allocation is covered by octet 2, power control features are covered by octet 3, additional control flags are covered by octet 4, and network identification, including Mobile Country Code and Mobile Network Code, is indicated by octet 5. **CB\_Message\_Identifier 1 : FFFF** there are 10 different messages which represents FFFF indicates they were failed to send to their destination due number of reasons for example wrong destination address, different geographical location, connectivity issues. **SIM group identifier(s) : FFFF** this says sim is not a part of special service or any corporate service. Higher Priority PLMN search period : **time interval between two searches :255** tells that the device was actively looking for higher priority Public land mobile network which apparently happens due to roaming. This indicates that the person was travelling a lot.

**IMSI : 310170511316860**

We found out the device IMSI number, **310170511316860** that says the mobile sim was registered in united states (MCC – 310) and it is metro PCS prepaid carrier service(MNC-170) with MSIN 511316860 that will identity the subscriber. **Ciphering key KcGPRS : FFFFFFFFFFFFFFFF, Ciphering key sequence number n for GPRS : 07** the multi FFF indicates ciphering was disabled also in GPRS data.

**P-TMSI : FFFFFFFF**  
**P-TMSI-SignatureValue : FFFFFFFF**  
**RAI : FFFFFFFFE00**  
**RoutingAreaUpdateStatus : 02**

**LanguageCode : 01** means device communication with network is default to Spanish. **Phase identification : 0x03** refers that mobile device was operating under GSM Phase2/2+ which gives SMS, GPRS and supplementary services.

**ICCID : 89310170105113168601** **Integrated circuit card identifier(ICCID)** is a identifier for sim card. The first two letter **89** is the industry identifier for telecommunications.

Abbreviated Dialling numbers means saved contacts or numbers that are simplified in calling process reducing the number of digits the user needs to type or enter.

**AlphaIdentifier : BRYAN PRUITT**  
**Length of BCD number/SSC contents : 06**  
**TON and NPI : 81**  
**Dialling Number/SSC String : 8703916823**  
**Capability/Configuration Identifier : FF**  
**Extension1 Record Identifier : FF**

We found 23 saved contacts in this SIM device like the one given above **BRYAN PRUITT- 8703916823, ALLEN FORNEY – 8704372304, ALLEN FORNEY – 8704375109, MORGAN KEENER – 7159421, FRANKIE YOUNGBLOOD – 8707049266, FRANKIE YOUNGBLOOD – 8705532206, FRANKIE YOUNGBLOOD – 8707435555, GRANNY – 8705453450, MORGAN DARBY – 8704806026, TREY – 8704809229, HOLLY BRYANT – 8707049302, BRYAN PRUITT –**

8707417182, GREG GALLANT – 8704802044, LANDON LOGAN – 4792000410, JUSTIN DILLON – 8703911585, MATT LOCKARD – 4799031790 , DAD – 8705453257, BILLY JACK BURNS – 8707418228, BILLY JACK BURNS – 8707049330, DUSTIN DEWEY – 8707049028, SARA SMITH – 8703916878, CASEY HAMMOND – 4799656652, LANCE LOGAN – 4795306957

Last number dialed –

Length of BCD number/SSC contents : 07  
TON and NPI : 81  
Dialling Number/SSC String : 19494128388  
Capability/Configuration Identifier : FF  
Extension1 Record Identifier : FF

## Short messages

ShortMessage : Cool. Gimme a call sometime after nine pm... Later  
Date : 08/22/04 08:07:39  
Status : Used space; Message received by MS from network; Message read  
Number-Type : Unknown  
Number-Plan : ISDN/telephone numbering plan  
Service Center Number : 0  
TP Message Type Indicator : SMS-DELIVER  
TP Reply Path : False. Is not set  
Number-Type : Unknown  
Number-Plan : ISDN/telephone numbering plan  
Service Center Number : 17144037320  
TP Protocol Identifier : 0x00  
TP Data Coding Scheme : 0x00  
SMS Data Coding Group : General Data Coding  
Compressed text indicator : False  
GSM 7 bit default alphabet : 7-bit  
Message Class : No message class defined  
TP User Data Length : 44

The short message is: "Cool. Gimme a call sometime after nine pm... Later," received on 08/22/04 at 08:07:39. The number type is unknown, and the associated number is 17144037320. The short message is: "Y not," received on 08/24/04 at 20:02:22. The number type is an international number, and the associated number is 16023093848. The short message is: "You ain't gotta lie about your booty call...." received on 06/19/04 at 16:59:02. The number type is an international number, and the associated number is 14802316430. The short message is: "Call me on my cell if you call.Â" received on 08/21/04 at 14:56:32. The number type is an international number, and the associated number is 16234513145. The short message is: "Lets go to star bucks." received on 06/30/04 at 06:31:02. The number type is an international number, and the associated number is 14808624170. The short message is: "Thanx 4 the call u brat i was waitin 4 u to call mayb nxt time huh! :-P" received on 07/02/04 at 17:12:09. The number type is an international number, and the associated number is 16024751306. The short message is: "Do" received on 08/25/04 at 17:37:50. The number type is an international number, and the associated number is 16234513145. The short message is: "Page: '7205879978'" received on 06/14/04 at 12:55:43. The number type is unknown, and the associated number is 129. The short message is: "Pick up your phone!" received on 05/01/04 at 20:57:04. The number type is an international number, and the associated number is 16025108674. The short message is: "Was good to see you... Miss you..." received on 08/26/04 at 07:18:42. The number type is an international number, and the associated number is 17144037320. The short message is: "You okay?" received on 08/25/04 at 18:34:57. The number type is an international number, and the associated number is 17144037320. The short message is: "Its me Shawna... My new number.Â" received on 08/15/04 at 10:22:51. The number type is an international number, and the associated number is 17144037320. The short message is: "You have a girl frien" received on 06/10/04 at 07:26:56. The number type is an international number, and the associated

number is 14802316430. The short message is: "Hmmm...Â" received on 06/10/04 at 07:49:02. The number type is an international number, and the associated number is 14802316430. The short message is: "What up? we at dos gringos in scottsdale" received on 06/25/04 at 16:13:10. The number type is an international number, and the associated number is 14802316430.

Findings - From the data above, we conclude that the number **1714403720** first message came on 08/15/04 saying its me shawna, sender name is shawna to be noted. Second message comes on 08/22/04 in the morning. Sender asking a call back after 9 Pm at night. Third message was on 08/25/04 sender messaged are you okay. On 08/26/04 sender messaged , ' was good to see you, miss you' means there is a possibility sender meet the user of the device in person between 08/25/04 - 08/26/04

**14802316430** talking about this number, there were 4 messages from this number, the sender first message came on 06/10/04 at 7:26 am in morning, sender asking user that did he have a girlfriend which can indicate, that user is a male person, second message on same day at 7:49 am with a reply 'hm'. Third message on 06/19/04 sender saying that the user was being dishonest for something that is related to the relationship between the sender and the user. Fourth message comes on 06/25/04, sender invites the user to a bar called dos gringos in 4209 N Craftsman Ct, Scottsdale, Arizona, 85251, USA

## User data

### Contacts

Name	Size	Type	Date Modified
BRYAN PRUITT		Directory	
BRYAN PRUITT		Directory	
DAD		Directory	
BILLY JACK BURNS		Directory	
BILLY JACK BURNS		Directory	
DUSTIN DEWEY		Directory	
SARA SMITH		Directory	
CASEY HAMMOND		Directory	
LANCE LOGAN		Directory	
ALLEN FORNEY		Directory	
ALLEN FORNEY		Directory	
MORGAN KEENER		Directory	
FRANKIE YOUNGBLOOD		Directory	
FRANKIE YOUNGBLOOD		Directory	
FRANKIE YOUNGBLOOD		Directory	
GRANNY		Directory	
MORGAN DARBY		Directory	
TREY		Directory	
HOLLY BRYANT		Directory	
GREG GALLANT		Directory	
LONDON LOGAN		Directory	
JUSTIN DILLON		Directory	
MATT LOCKARD		Directory	

### Text messages

Name	Size	Type	Date Modified
Cool. Gimme a call s		MPE Data Item	
Page: "7205879978"		MPE Data Item	
Pick up your phone!		MPE Data Item	
Was good to see you.		MPE Data Item	
You okay?		MPE Data Item	
Its me Shawna... My		MPE Data Item	
You have a girl frie		MPE Data Item	
Hmmm...;		MPE Data Item	
What up? we at dos g		MPE Data Item	
Y not		MPE Data Item	
You ain't gotta lie		MPE Data Item	
Call me on my cell i		MPE Data Item	
Lets go to star buck		MPE Data Item	
Thanx 4 the call u b		MPE Data Item	
Do		MPE Data Item	

## LG\_LG-VX9100.ad1

After opening LG\_LG-VX9100.ad1 we did explored File system and user data simultaneously.

### Calender

Name	Size	Type	Date Modified
i am happy		MPE Data Item	

**Media** contains audio and vishual

### Audio

Beethovens_fifth.mid.html	MPE Data Item
Dreamsequence.mid.html	MPE Data Item
Ode_to_joy.mid.html	MPE Data Item
Rainforest.mid.html	MPE Data Item
Train.mid.html	MPE Data Item

Beethovens\_fifth.mid.html

It's a audio mobile ringtone of a piano playing. Very common in old phones.

[Click Here To Open ../../File System/brew/mod/18067/Beethovens\\_fifth.mid](#)

Dreamsequence.mid.html

It's a mobile ringtone sounds like a parade.

[Click Here To Open ../../File System/brew/mod/18067/Dreamsequence.mid](#)

Ode\_to\_joy.mid.html

It's a fast pace piano with a very unique theme mobile ringtone

[Click Here To Open ../../File System/brew/mod/18067/Ode\\_to\\_joy.mid](#)

Rainforest.mid.html

Mobile ringtone sounds like rain and birds voices












[Click Here To Open ../../File System/brew/mod/18067/Rainforest.mid](#)

Train.mid.html

Mobile ringtone with train horn blowing and a musical instrument similar to sound plates drum.

[Click Here To Open ../../File System/brew/mod/18067/Train.mid](#)

## Visual

 Congratulations.jpg.html	MPE Data Item
 Happy Birthday.jpg.html	MPE Data Item
 Hearts.jpg.html	MPE Data Item
 Smile.jpg.html	MPE Data Item
 Thinking of you.jpg.html	MPE Data Item
 0817001018.jpg.html	MPE Data Item
 0824001058.jpg.html	MPE Data Item
 0824001059.jpg.html	MPE Data Item
 0824001100.jpg.html	MPE Data Item
 0712001209.3g2.html	MPE Data Item
 0824001100.3g2.html	MPE Data Item

Congratulations.jpg.html

[Click Here To Open ../../File System/brew/mod/10888/Congratulations.jpg](#)



Happy Birthday.jpg.html

[Click Here To Open ../../File System/brew/mod/10888/Happy Birthday.jpg](#)



Hearts.jpg.html

[Click Here To Open ../../File System/brew/mod/10888/Hearts.jpg](#)



Smile.jpg.html

[Click Here To Open ../../File System/brew/mod/10888/Smile.jpg](#)



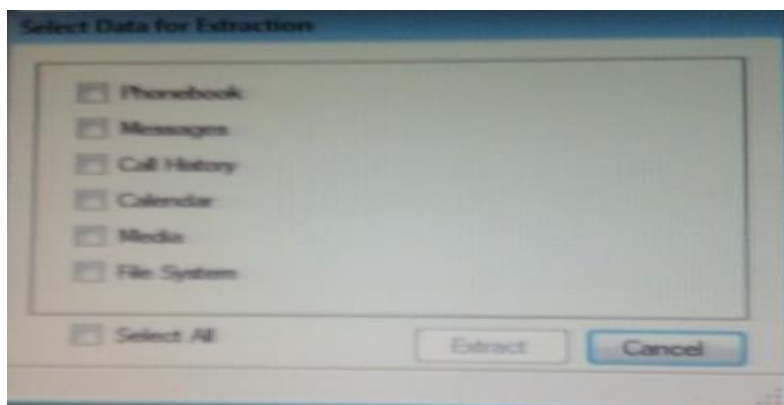
Thinking of you.jpg.html

[Click Here To Open ../../File System/brew/mod/10888/Thinking of you.jpg](#)



0817001018.jpg.html

[Click Here To Open ../../File System/brew/mod/10888/0817001018.jpg](#)

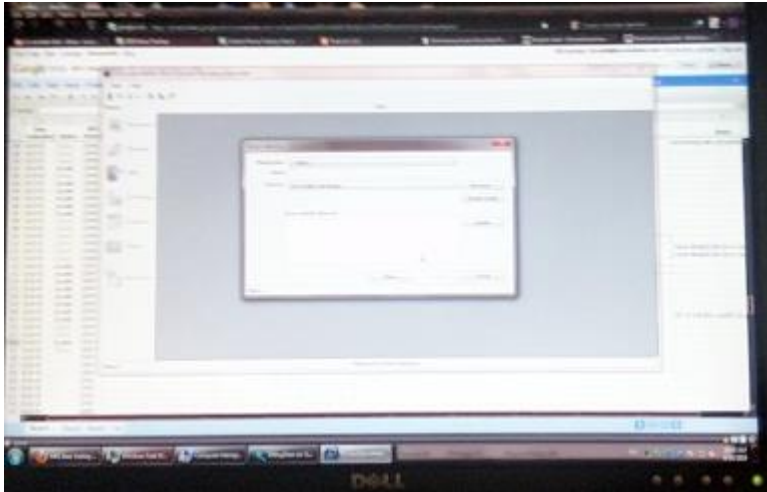


User is extracting data from Phonebook, messages, call history, calender, media, file system.

0824001058.jpg.html

[Click Here To Open ../../File System/brew/mod/10888/0824001058.jpg](#)





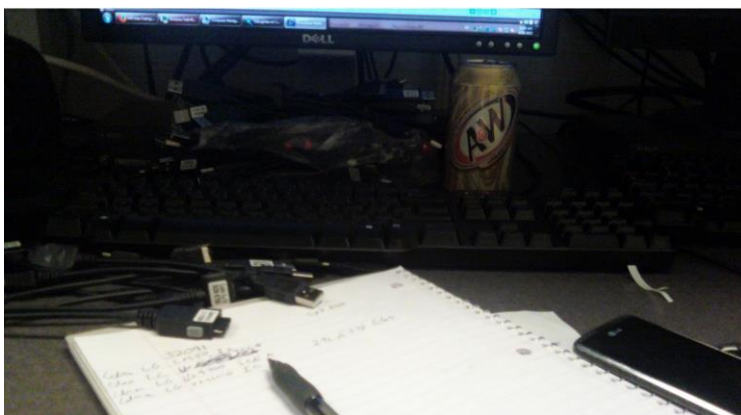
0824001059.jpg.html

[Click Here To Open ../../File System/brew/mod/10888/0824001059.jpg](#)



0824001100.jpg.html

[Click Here To Open ../../File System/brew/mod/10888/0824001100.jpg](#)

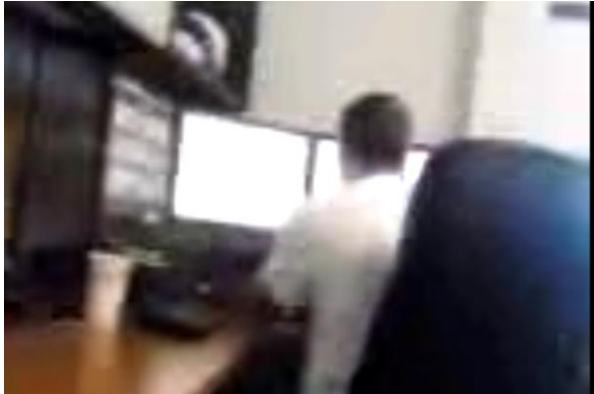


Desktop looks like microsoft windows 7 on Dell monitor , person drinking A and W cold drink, the whole room looks like a high tech computer lab. There are too many wires on table, HDMI wire, USB wire. An android smart with a notebook and a pen.



0712001209.3g2.html

[Click Here To Open ../../File System/brew/mod/10890/0712001209.3g2](#)



It's a video, the recording resembles a office which looks like a advanced tech room or lab with a person recording and other person working on Computer, in the end the england sticker could be a possibly this video is from UK(united Kingdom)

0824001100.3g2.html

[Click Here To Open ../../File System/brew/mod/10890/0824001100.3g2](#)



















In this video, two persons talking in english with american accent, due to poor audio quality, I didn't understand fully but person 1 asks, person 2 with a name then says something sounds like '3 times with that'.

Phonebook

 #BAL	Directory
 #MIN	Directory
 #PMT	Directory
 Zack	Directory
 Jay	Directory
 Hfiuuufy	Directory

#BAL, #MIN, and #PMT: Most likely, these folders include classified contacts. The prefix "#" may suggest that these are unique categories, sometimes associated with certain groups; for example, "BAL" stands for contacts pertaining to balances, "MIN" for minimal or emergency interactions, and "PMT" for contacts pertaining to payments. Jay, Hfiuuufy, Zack: These seem to be the names of certain contacts. The name "Hfiuuufy" seems strange; it may be a nickname or a misspelling.

Text Messages

 What's up?	MPE Data Item
 Wanna meet up?	MPE Data Item
 Check this out!	MPE Data Item
 Whacha doing?	MPE Data Item
 On my way	MPE Data Item
 What do you think?	MPE Data Item
 You're the best!	MPE Data Item
 Call me	MPE Data Item
 I love you!	MPE Data Item
 Miss you!	MPE Data Item
 Where are you?	MPE Data Item
 Good morning!	MPE Data Item
 Good night	MPE Data Item
 How are you?	MPE Data Item
 Thanks	MPE Data Item
 hello!	MPE Data Item

eri\_sound folder has 4 files

 verizonwireless.qcp	3 Regular File
 roaming.qcp	2 Regular File
 lossofservice.qcp	3 Regular File
 extendednetwork.qcp	3 Regular File

The carrier of the mobile network may be verizon wireless.

# Investigative report (Practical) Cellebrite

## Lesson 5

Date – 10/26/2024

Subject – Digital forensics investigation of Apple iOS Full File system\_2021-10-01\_Report.ufdr

### Device type

IOS Device

APPLE iPhone 8 and Phone Number is 6466535699

Detected Phone Model

iPhone 8

Your Google Voice number (646) 653-5699 will expire in 30 days

### Owner of the device

Berg

Device Name

Berg's iPhone

### Suspect home location

51-16 Van Loon Street, New York, 11373, United States

This address is the most repeated address in the location logs in cache SQLite ZRTCLLOCATIONMO.

Z_PK ▾	Z_ENT ▾	Z_OPT ▾	ZSOURCE ▾	ZDATE ▾	ZLATITUDE ▾	ZLONGITUDE ▾
84	8	1	4	653816289.554423	40.7375045640555	-73.8792423548141
83	8	1	4	653807678.101806	40.7376889725789	-73.8793445272471
82	8	1	4	653806532.10926	40.7377954508835	-73.8793239244111
81	8	1	4	653804926.896405	40.7376969788432	-73.8793425680426
80	8	1	4	653791924.853608	40.7375642082131	-73.8793182481629
79	8	1	4	653788636.357815	40.7378616292898	-73.8793071492731
78	8	1	4	653782544.006978	40.7377446352992	-73.8793127368778
77	8	1	4	653780931.911803	40.7377582463255	-73.8793392462231
76	8	1	4	653771725.830146	40.7377618273235	-73.8793462431298
75	8	1	4	653752262.893568	40.7377450671425	-73.8793338580599
74	8	1	4	653741441.573538	40.7377547115417	-73.8793224800603
73	8	1	4	653740054.826645	40.7376986576405	-73.8793599005816
72	8	1	3	653701962.821057	40.7379734162915	-73.8793201615526
67	8	1	3	653699019.882771	40.7379128246806	-73.8793169465521
66	8	1	4	653670768.124986	40.7377201093375	-73.8793495200518
65	8	1	4	653660513.744468	40.7377802580778	-73.8793111498179
64	8	1	4	653655739.266899	40.7377746464273	-73.8793246153185
63	8	1	4	653654567.488539	40.7377885800358	-73.8793271028039
62	8	1	4	653647035.212698	40.7377676134998	-73.8793349753068
61	8	1	4	653644297.058808	40.737776603039	-73.8793292319705
60	8	1	4	653636984.047855	40.7377879547843	-73.8793338318313
59	8	1	4	653635362.835439	40.7377624127234	-73.8793534468918
58	8	1	4	653624576.439696	40.7374417113588	-73.8792990112956
57	8	1	4	653623565.020759	40.7377075901857	-73.8793261003109
56	8	1	4	653621355.168381	40.737802413066	-73.8793241207543
55	8	1	4	653615753.848781	40.7377539962546	-73.8793053201448
54	8	1	4	653609313.553908	40.7375640276201	-73.8793175928985
53	8	1	4	653583033.901523	40.737825527016	-73.8792835072962
52	8	1	4	653538006.062956	40.7378470037022	-73.8793201764197
51	8	1	4	653530237.573269	40.7377187177925	-73.8793731174846
50	8	1	4	653523223.766089	40.7377832955139	-73.8793448925625
49	8	1	4	653520514.93646	40.73784732213	-73.8793155543088
48	8	1	4	653502900.63607	40.7375345329241	-73.8793433243779
47	8	1	4	653491822.940665	40.7377985460214	-73.8792756522627
46	8	1	4	653487988.204883	40.7377881820053	-73.8793421577509
45	8	1	4	653486981.850519	40.7377542273887	-73.8793330816122
44	8	1	4	653446821.105646	40.7375870863157	-73.8793182445744
43	8	1	4	653444410.587791	40.7375870409803	-73.8793182237038

Time Zone

(UTC-05:00) New\_York (America)

Address

51-16 Van Loon Street, New York, NY 11373, U

Get GPS Coordinates

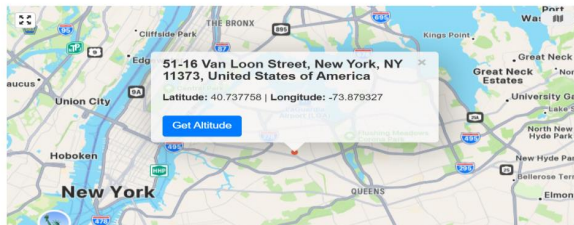
DD (decimal degrees)\*

Latitude 40.737757740844

Longitude -73.879327112342

Get Address

Lat,Long 40.737757740844,-73.879327112342



## Suspect travelling to these locations more frequently

After investigating in 271b2d62e4ab929f60e2ded6cfdb6e097f0f92d1\_files\_full.zip/private/var/mobile/Library/Caches/com.apple.routined/Cache.sqlite, ZRTCLLOCATIONMO, we found out that the suspect was more often travelling from Queens to downtown Manhattan. So we are assuming that the suspect was working in Manhattan, that's why there is a pattern of daily commute to these places.

Extraction Summary (1)

Device Locations (5790)

Cache.sqlite

Database View

File Info

Hide

Z\_METADATA (1)

Z\_MODEL\_CACHE (1)

Z\_PRIMARYKEY (22)

ZRTADDRESSMO (0)

ZRTCLLOCATIONMO (3359)

ZRTDEVICEMO (0)

ZRTIDENTITYDELETIONREQUESTMO (0)

ZRTLOCATIONIDENTIFIERMO (0)

ZRTMODELUSERINTERACTIONMO (0)

ZRTFINGERPRINTMO (101)

ZRTHINTMO (149)

ZRTLEARNEDLOCATIONOFINTERESTS... (0)

ZRTLEARNEDLOCATIONOFINTERESTS... (0)

ZRTLEARNEDPLACEMO (0)

ZRTLEARNEDTRANSITIONMO (0)

ZRTLEARNEDVISITMO (0)

ZRTCLLOCATIONMO (3359)

PK	Z_ENT	Z_OPT	ZALTITUDE	ZCOURSE	ZHORIZONTALACCURACY	ZLATITUDE	ZLONGITUDE
22	2	1	7.46498775482178	-1	65	40.737757740844	-73.879327112342
21	2	1	7.46505069732666	-1	65	40.737755875321	-73.8793285121364
20	2	1	7.4467134475708	-1	65	40.7377243059888	-73.8793563877052
19	2	1	7.46474266052246	-1	65	40.7377321267934	-73.8793374142343
18	2	1	7.45730018615723	-1	65	40.7377777715574	-73.8793249802456
17	2	1	7.46513175964355	-1	65	40.7377528853433	-73.8793255641592
16	2	1	7.46498012542725	-1	65	40.7377527605037	-73.8793327092651
15	2	1	9.73426347716246	-1	20	40.7379168463226	-73.8793184316262
14	2	1	7.46095848083496	-1	65	40.7377080582109	-73.8793541372281
13	2	1	9.80269566570157	-1	25.8586887335447	40.7379577042256	-73.879328204268
12	2	1	9.03080226849787	-1	23.3335670943042	40.7379535476376	-73.8793371774775
11	2	1	9	-1	20.4349633160867	40.7377078792934	-73.8793798892814
10	2	1	10	-1	25.3328378803537	40.7382492193207	-73.8792793467737
09	2	1	10	-1	31.3695971638281	40.7382719833388	-73.8790916324536
08	2	1	8.39615345001221	-1	65	40.7382004100822	-73.8792616765068

Text

-73.879327112342

## (1) First location

Address  
51-16 Van Loon Street, New York, NY 11373, U  
Get GPS Coordinates

DD (decimal degrees)\*  
Latitude 40.737757740844  
Longitude -73.879327112342  
Get Address  
Lat,Long 40.737757740844,-73.879327112342

ZDATE	ZLATITUDE	ZLONGITUDE
654658341.637677	40.7377321267934	-73.8793374142343

## Date

654658341.637677
Convert Core Data timestamp to human date

Converting timestamp (654658341) in seconds:

**GMT:** Thursday, September 30, 2021 1:32:21 AM

**Your time zone:** Wednesday, September 29, 2021 9:32:21 PM GMT-04:00

Suspect was at 51-16 Van Loon Street, New York, 11373, United States on September 29, 2021, at this time 9:32 pm eastern standard time (new York)

## (2) Second location

At 82-23 Broadway, New York, NY 11373, United States of America

ZLATITUDE	ZLONGITUDE
40.7427070624039	-73.8824295041327



82-23 Broadway, New York, NY 11373, United States

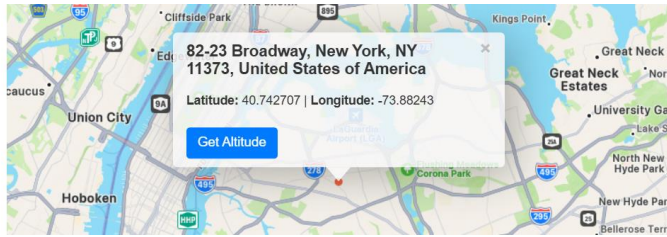
[Get GPS Coordinates](#)

DD (decimal degrees)\*

Latitude 40.7427070624039

Longitude -73.8824295041327

[Get Address](#)



### (3) Third Location

15 Beekman Street, New York, NY, 10038, United States of America

40.7108344000806 -74.0064620120035 -

Address

15 Beekman, 15 Beekman Street, New York, N

[Get GPS Coordinates](#)

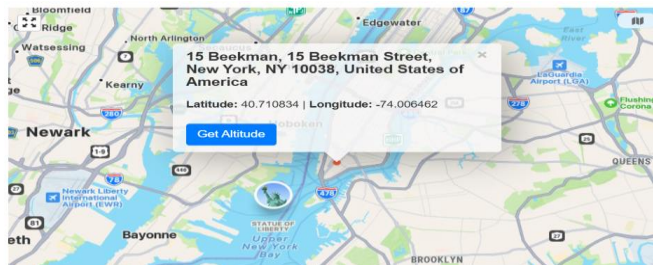
DD (decimal degrees)\*

Latitude 40.7108344000806

Longitude -74.0064620120035

[Get Address](#)

Lat,Long 40.7108344000806,-74.006462012



(4) 40.7101209365254 -74.0063131986383 -

161 Williams Street, New York, NY, 10038, United States

Address

161 William Street, New York, NY 10038, United

[Get GPS Coordinates](#)

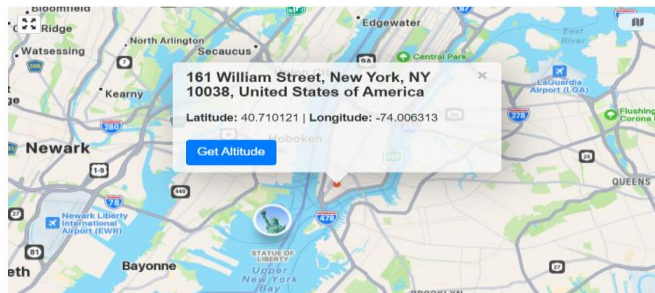
DD (decimal degrees)\*

Latitude 40.7101209365254

Longitude -74.0063131986383

[Get Address](#)

Lat,Long 40.7101209365254,-74.006313198



(5) 40.7114410131095 -74.0098367044791

St Paul's Churchyard, Broadway, New York, NY, 10279, United States

Address

St. Paul's Churchyard, Broadway, New York, NY

[Get GPS Coordinates](#)

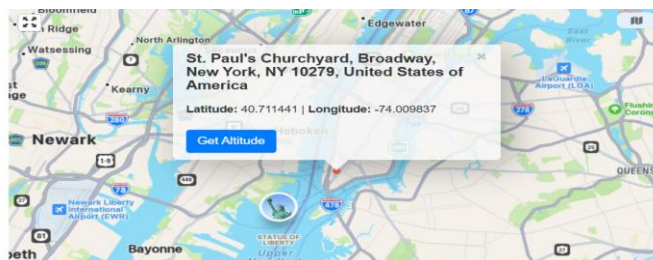
DD (decimal degrees)\*

Latitude 40.7114410131095

Longitude -74.0098367044791

[Get Address](#)

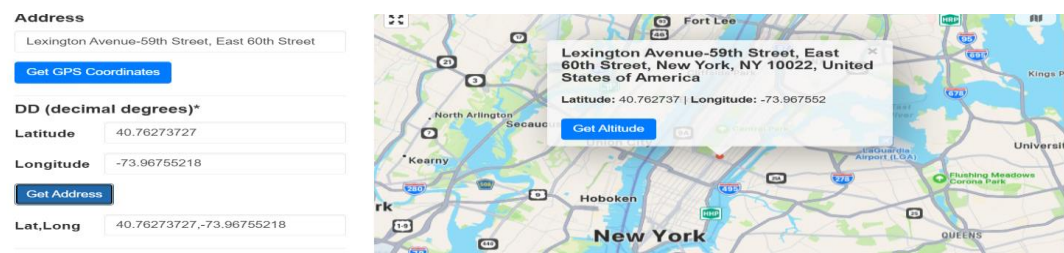
Lat,Long 40.7114410131095,-74.009836704



(6) 

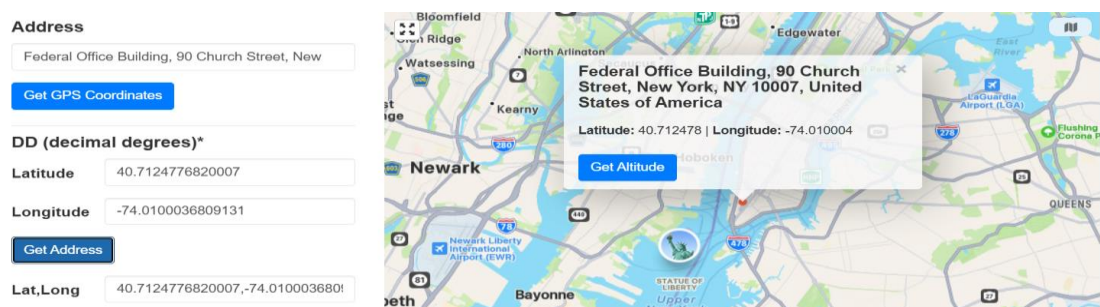
ZLATITUDE ▾	ZLONGITUDE ▾
40.76273727	-73.96755218

Lexington Avenue-59<sup>th</sup> Street, East 60<sup>th</sup> Street, New York, NY, 10022, United States



Almost all the timestamps are of September 2021

Suspects entered to the Federal Office Building, 90 Church Street, New York, NY, 10007, United States.



ZENTRYDATE ▾	ZLOCATIONLATITUDE ▾	ZLOCATIONLONGITUDE ▾	ZEXITDATE ▾
654657866.115645	40.7382004100822	-73.8792616765068	
654657866.115645	40.7386331403187	-73.8776564759629	
654657446.848404	40.7466722241441	-73.8913344306159	654657586.716106
654657446.848404	40.7466722701553	-73.8913328539823	
654657011.297403	40.7488670384397	-73.9378936785856	654657028.874855
654657011.297403	40.7488677407262	-73.9378936787705	
654655098.113843	40.7124776820007	-74.0100036809131	654655502.632073

Suspect entered the building at 8:38 Pm on September 29, 2021

654655098.113843	Convert Core Data timestamp to human date
------------------	---

Converting timestamp (654655098) in seconds:  
**GMT:** Thursday, September 30, 2021 12:38:18 AM  
**Your time zone:** Wednesday, September 29, 2021 8:38:18 PM GMT-04:00

Suspect left the building at 8:45 Pm on September 29, 2021



65465502.632073

Convert Core Data timestamp to human date

Converting timestamp (65465502) in seconds:

**GMT:** Thursday, September 30, 2021 12:45:02 AM

**Your time zone:** Wednesday, September 29, 2021 8:45:02 PM GMT-04:00

## Applications used by the suspect

As we can see in the

271b2d62e4ab929f60e2ded6cfdb6e097f0f92d1\_files\_full.zip/private/var/mobile/Library/AggregateDictionary/ADDDataStore.sqlited

Suspect was using camera, weather, maps, music, and app called MenoLife - (Menopause Tracker) which are more often used by Women. This can conclude that suspect can be a woman.

Suspect also used calculator

Filters														
Actions														
Search														
			#			↑ Name	Identifier	Alias Names	Action Identifier	Launches	Activations	Active Time	Background Time	Details
		<input checked="" type="checkbox"/>	1				com.apple.camera			1	1	00:00:01		
		<input checked="" type="checkbox"/>	2				com.apple.Spotlight			1	1	00:00:15	00:00:31	
		<input checked="" type="checkbox"/>	3				com.apple.Preferences			1	1	00:00:25		
		<input checked="" type="checkbox"/>	4				com.apple.CryptoTokenKit.se...						00:00:33	
		<input checked="" type="checkbox"/>	5				com.apple.Translate.CacheD...						00:00:01	
		<input checked="" type="checkbox"/>	6				com.apple.weather.widget						00:00:03	
		<input checked="" type="checkbox"/>	7				com.apple.springboard			1	1			
		<input checked="" type="checkbox"/>	8				com.apple.ScreenTimeWidg...						00:00:01	
		<input checked="" type="checkbox"/>	9				com.apple.stocks.widget						00:00:19	
		<input checked="" type="checkbox"/>	10				com.apple.news.widget						00:00:25	
		<input checked="" type="checkbox"/>	11				com.apple.Maps.GeneralMa...						00:00:33	
		<input checked="" type="checkbox"/>	12				com.apple.FileProvider.Local...						00:00:14	
		<input checked="" type="checkbox"/>	13				com.apple.AppTrackingTrans...						00:00:01	
		<input checked="" type="checkbox"/>	14				com.apple.WebKit.WebCont...						00:01:26	
		<input checked="" type="checkbox"/>	15				com.apple.WebKit.Networking						00:01:26	
		<input checked="" type="checkbox"/>	16				com.apple.Music						00:02:28	
		<input checked="" type="checkbox"/>	17			MenoLife - Menopause Trac...	com.menolabs.menolife			1	2	00:01:25	00:00:04	
		<input checked="" type="checkbox"/>	18			My Luna	bts.lunanueva						00:00:10	

					Identifier	Start time	End time	Sub Module	Additional info	A
		1			com.apple.MobileAddressBo...	12-09-2021 03:48:00(UTC+0)	12-09-2021 03:48:26(UTC+0)		App installation	
		2			com.apple.calculator	12-09-2021 03:48:00(UTC+0)	12-09-2021 03:48:26(UTC+0)		App installation	
		3			com.apple.DocumentsApp	12-09-2021 03:48:00(UTC+0)	12-09-2021 03:48:26(UTC+0)		App installation	
		4			com.apple.weather	12-09-2021 03:48:00(UTC+0)	12-09-2021 03:48:27(UTC+0)		App installation	
		5			com.apple.VoiceMemos	12-09-2021 03:48:00(UTC+0)	12-09-2021 03:48:28(UTC+0)		App installation	
		6			com.apple.tips	12-09-2021 03:48:00(UTC+0)	12-09-2021 03:48:28(UTC+0)		App installation	
		7			com.apple.mobilecal	12-09-2021 03:48:00(UTC+0)	12-09-2021 03:48:32(UTC+0)		App installation	
		8			com.apple.Maps	12-09-2021 03:48:00(UTC+0)	12-09-2021 03:48:32(UTC+0)		App installation	
		9			com.apple.podcasts	12-09-2021 03:48:00(UTC+0)	12-09-2021 03:48:32(UTC+0)		App installation	
		10			com.apple.Translate	12-09-2021 03:48:00(UTC+0)	12-09-2021 03:48:32(UTC+0)		App installation	
		11			com.apple.Bridge	12-09-2021 03:48:00(UTC+0)	12-09-2021 03:48:36(UTC+0)		App installation	
		12			com.apple.MobileStore	12-09-2021 03:48:00(UTC+0)	12-09-2021 03:48:40(UTC+0)		App installation	
		13			com.apple.iBooks	12-09-2021 03:48:00(UTC+0)	12-09-2021 03:48:40(UTC+0)		App installation	
		14			com.apple.Music	12-09-2021 03:48:00(UTC+0)	12-09-2021 03:48:41(UTC+0)		App installation	
		15			com.apple.facetime	12-09-2021 03:48:00(UTC+0)	12-09-2021 03:48:41(UTC+0)		App installation	
		16			com.apple.Home	12-09-2021 03:48:00(UTC+0)	12-09-2021 03:48:42(UTC+0)		App installation	
		17			com.apple.measure	12-09-2021 03:48:00(UTC+0)	12-09-2021 03:48:42(UTC+0)		App installation	
		18			com.apple.reminders	12-09-2021 03:48:00(UTC+0)	12-09-2021 03:48:45(UTC+0)		App installation	

		96			com.apple.mobilemail	19-09-2021 04:24:20(UTC+0)	19-09-2021 04:24:22(UTC+0)	Activity Type: com.apple.mai...		
		97			com.apple.HealthENBuddy	21-09-2021 21:46:58(UTC+0)	21-09-2021 21:48:31(UTC+0)			
		98			com.apple.HealthENBuddy	21-09-2021 21:48:31(UTC+0)	21-09-2021 21:48:41(UTC+0)		Launch reason: com.apple.S...	
		99			com.apple.carkit.DNDBuddy	22-09-2021 20:35:04(UTC+0)	22-09-2021 20:35:08(UTC+0)			

These are some email addresses that the suspect was interacting to more often

From: groupupdates@facebookmail.com Facebook	From: contact@protonvpn.com ProtonVPN
From: security@facebookmail.com Facebook	From: contact@menolabs.com
alexongkowijoyo91@gmail.com	From: contact@myluna.care
From: contact@womaneze.com	From: groupupdates@facebookmail.com Facebook
From: noreply@owhealth.com Flo	From: notify@wayforpay.com.ua WayForPay

12-09-2021 00:02:27(UTC-4)	Find My has been disabled on Berg's iPhone.	Emails
4)	Bergcybersec, finish setting up your Galaxy S10e with Google	Emails
08-05-2021 23:34:48(UTC-4)	Notice of unsuccessful payment	
17-09-2021 16:16:20(UTC-4)	Verify Your Email - My Luna APP.	

From the evidence above, this is proved that suspect was a regular user of fakebook (social media platform). Suspect was interacting with Meno labs, Womeneze, my Luna Care through emails, these are companies that makes products includes supplements, probiotics, and mobile applications to help women track symptoms related to Menopause. Suspect got emails from a

VPN company called proton VPN . suspect also disabled the find my device option on the iPhone on December 8<sup>TH</sup> 2021 at 11:02pm(EST) . There was a google account login on suspect account on a different mobile device(Samsung Galaxy S10e)

## List of devices the suspect's iPhone got connected to through Bluetooth.

(1) RANDOM C6:A0:4D:62:5F:FD

(2) RANDOM F7:16:3C:3B:68:DE

(3) RANDOM CD:1A:AD:92:C1:88

(4)RANDOM FC:10:90:CB:2E:D7

All these mac address are useless because these are randomized address and can't be traced. Hence we don't have any vendor information for these devices.

Device Connectivity	Go to	Device Connectivity	Go to
Device Name:		Device Name:	
Device type:		Device type:	
Timestamp:		Timestamp:	
Connectivity method:	Bluetooth	Connectivity method:	Bluetooth
Connectivity nature:	Detected	Connectivity nature:	Detected
Artifact Family:		Artifact Family:	
Source Repository Path:		Source Repository Path:	
Source:		Source:	
Source file:	271b2d62e4ab929f60e2ded6cfdb6e097f0f92d1_files_full.zip/private/var/containers/Shared/SystemGroup/ACD57B49-6C8D-40AD-AD2A-6B21DB7EBD14/Library/Database/com.apple.MobileBluetooth.ledevices.other.db-wal : 0x8DB56 (Table: OtherDevices, Size: 1013552 bytes)	Source file:	271b2d62e4ab929f60e2ded6cfdb6e097f0f92d1_files_full.zip/private/var/containers/Shared/SystemGroup/ACD57B49-6C8D-40AD-AD2A-6B21DB7EBD14/Library/Database/com.apple.MobileBluetooth.ledevices.other.db-wal : 0xF7715 (Table: OtherDevices, Size: 1013552 bytes)
Device Identifiers		Device Identifiers	
Address	Random C6:A0:4D:62:5F:FD	Address	Random F7:16:3C:3B:68:DE

» Device Connectivity <span>Go to ▾</span>	» Device Connectivity <span>Go to ▾</span>
<p>Device Name:</p> <p>Device type:</p> <p>Timestamp:</p> <p>Connectivity method: Bluetooth</p> <p>Connectivity nature: Detected</p> <p>Artifact Family:</p> <p>Source Repository Path:</p> <p>Source:</p> <p>Source file: 271b2d62e4ab929f60e2ded6cfdb6e097f0f92d1_files_full.zip/private/var/containers/Shared/SystemGroup/ACD57B49-6C8D-40AD-AD2A-6B21DB7EBD14/Library/Database/com.apple.MobileBluetooth.ledevices.other.db-wal : 0x4D661 (Table: OtherDevices, Size: 1013552 bytes)</p> <div data-bbox="221 763 724 813">Device Identifiers</div> <p>Address Random CD:1A:AD:92:C1:88</p>	<p>Device Name:</p> <p>Device type:</p> <p>Timestamp:</p> <p>Connectivity method: Bluetooth</p> <p>Connectivity nature: Detected</p> <p>Artifact Family:</p> <p>Source Repository Path:</p> <p>Source:</p> <p>Source file: 271b2d62e4ab929f60e2ded6cfdb6e097f0f92d1_files_full.zip/private/var/containers/Shared/SystemGroup/ACD57B49-6C8D-40AD-AD2A-6B21DB7EBD14/Library/Database/com.apple.MobileBluetooth.ledevices.other.db-wal : 0x4D20B (Table: OtherDevices, Size: 1013552 bytes)</p> <div data-bbox="780 763 1291 813">Device Identifiers</div> <p>Address Random FC:10:90:CB:2E:D7</p>

## List of devices suspects iPhone got connected to through Wi-Fi

- (1) 28:56:5a:df:65:cc, It's a router of the company Hon Hai Precision, the suspect got connected to this router at Queens Boulevard, New York, NY, 11373, United States on January 10,2021 at 1:32 am.
- (2) 18:1b:eb:c7:a6:83 belongs to Actiontec Electronics router
- (3) 5c:5a:c7:dd:4d:e1 belongs to cisco systems
- (4) 00:cb:51:4d:35:1e belongs to Sagemcom Broadband SAS

## >> Wireless Network

Go to ▾

BSSID: 28:56:5A:DF:65:CC  
SSID:  
Security Mode:  
Password:  
Last Connected:  
Last Auto Connected:  
Timestamp: 01-10-2021 02:32:58(UTC-4)  
End time:  
Package:  
Connection Type:  
Artifact Family:  
Source Repository Path:  
Source:  
Extraction: Legacy  
Manually decoded: False  
Source file: 271b2d62e4ab929f60e2ded6cfdb6e097f0f92d1\_files\_full.zip/private/var/root/Library/Caches/locationd/cache\_encryptedB.db : 0x508649 (Table: WifiLocation, Size: 44048384 bytes)

### Map

Position: (40.737583, -73.880951)  
Map Address:

Source

### Location

Go to ▾

Name: Wireless Networks Location - BSSID: 28:56:5A:DF:65:CC  
Description:  
Type: Harvested  
Origin:  
Timestamp: 01-10-2021 02:32:58(UTC-4)  
End time:  
Position: (40.737583, -73.880951)  
Aggregated locations:  
Map Address:

## >> Wireless Network

Go to ▾

BSSID: 18:1B:EB:C7:A6:83  
SSID:  
Security Mode:  
Password:  
Last Connected:  
Last Auto Connected:  
Timestamp: 01-10-2021 02:32:58(UTC-4)  
End time:  
Package:  
Connection Type:  
Artifact Family:  
Source Repository Path:  
Source:  
Extraction: Legacy  
Manually decoded: False  
Source file: 271b2d62e4ab929f60e2ded6cfdb6e097f0f92d1\_files\_full.zip/private/var/root/Library/Caches/locationd/cache\_encryptedB.db : 0x508939 (Table: WifiLocation, Size: 44048384 bytes)

### Map

Position: (40.737533, -73.880784)  
Map Address:

Source

### Location

Go to ▾

Name: Wireless Networks Location - BSSID: 18:1B:EB:C7:A6:83  
Description:  
Type: Harvested  
Origin:  
Timestamp: 01-10-2021 02:32:58(UTC-4)  
End time:  
Position: (40.737533, -73.880784)  
Aggregated locations:  
Map Address:



# Mobile Forensics Practical

## Lesson 8

This practical exercise will focus on a file image of a Google Pixel 3, running Android 10. we will examine this image using Autopsy.

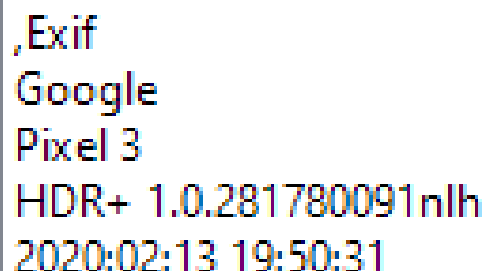
### Questions

1. Can a photo's metadata tell an investigator what make/model of camera took a photo?

a. Yes

b. No

it is correct that the phone metadata related to an image tells the camera model by which that photo was taken. I choose this path to find the images /LogicalFileSet1/Pixel 3/data/media/0/DCIM/Camera/. I opened the image in content viewer and click on text option where there was information given about camera make and model.



Exif  
Google  
Pixel 3  
HDR+ 1.0.281780091nlh  
2020:02:13 19:50:31

Name	IMG_20200209_132353.jpg
Analyzed	true
Category	
Tags	
Path	/LogicalFileSet1/Pixel 3/data/media/0/DCIM/Camera/
Created Time	0000-00-00 00:00:00
Modified Time	0000-00-00 00:00:00
MDS Hash	88b824dcf1af590ce769f9b0c549883
Hashset	
Camera Make	Google
Camera Model	Pixel 3

2. After reviewing the Snapchat databases, how many Snap memories were successfully uploaded?

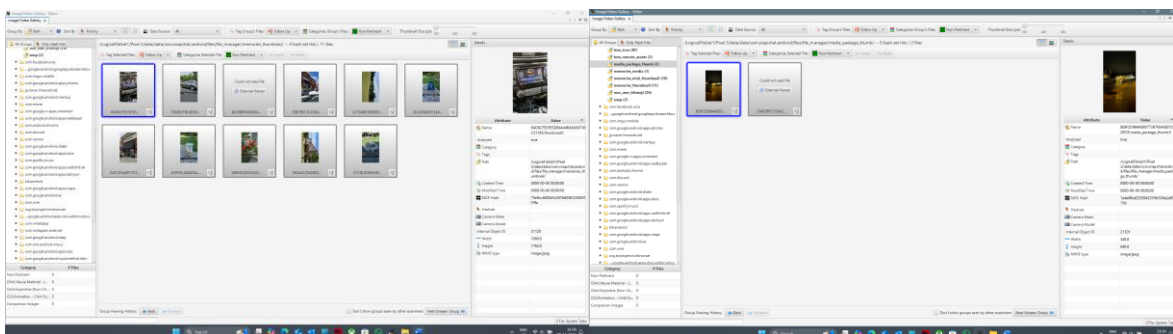
a. 10

b. 11

c. 1

d. 4

After reviewing the snapchat database, I found 11 snaps that was successfully uploaded. I choose this path /LogicalFileSet1/Pixel 3/data/data/com.snapchat.android/files/file\_manager/media\_package\_thumb/



3. What is the phone number that is associated with the user's "Viber" account?



- a. 919-765-3489
- b. 919-579-4674
- c. 215-641-2628
- d. 800-000-5000

Type	Value	Source(...
Account	VIBER	Viber Par
ID	+19195794674	Viber Par
Source File Path	/LogicalFileSet1/Pixel 3/data/data/com.viber.voip/databases/viber_messages	
Artifact I	-9223372036854775500	

4. How many photos contain geolocation data?
- a. 3
  - b. 14
  - c. 24
  - d. 6

When I was looking for images related to geolocation data, I tried looking pictures in snapchat and Instagram related data folders and I couldn't find geolocation data in those pictures, I think social media application alter Exif metadata related to photo geolocation. So looked images that was not in social media database, which is camera images. And I got the geolocation of the images of camera and there were 3 images in camera.



/LogicalFileSet1/Pixel 3/data/media/0/DCIM/Camera/

/LogicalFileSet1/Pixel 3/data/media/0/DCIM/Restored/

By opening these images in content viewer and clicking on analysis results

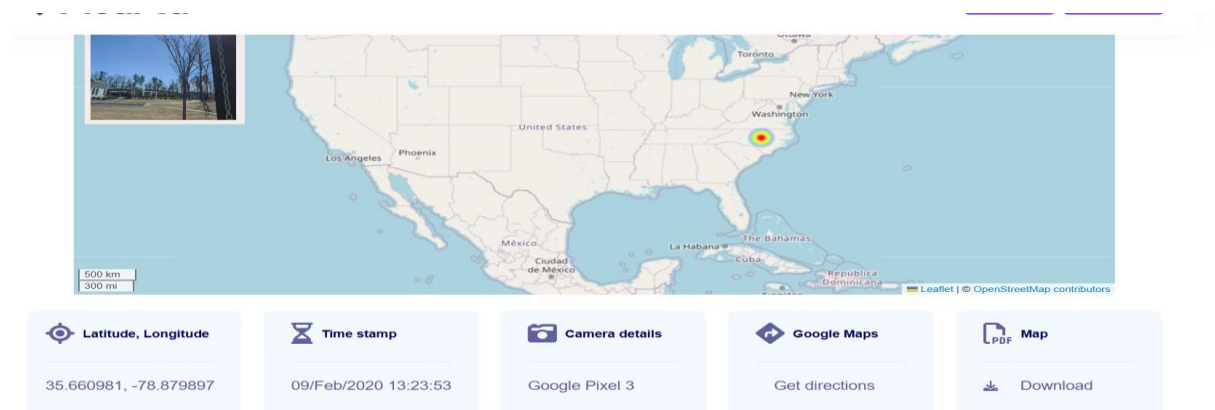
Item: IMG\_20200209\_132353.jpg  
Aggregate Score: Not Notable

**Analysis Result 1**

Score:	Not Notable
Type:	EXIF Metadata
Configuration:	
Conclusion:	
Altitude:	76.24
Date Created:	2020-02-09 08:23:53 GMT-05:00
Device Make:	Google
Device Model:	Pixel 3
Latitude:	35.660980555555554
Longitude:	-78.87989722222221

5. What state is associated with the geolocation coordinates?
- Virginia
  - North Carolina
  - New York
  - California

I download the image from autopsy and uploaded in a tool to get the geolocation of the image.



6. What was the last application that was downloaded from Google Chrome?
- MagiskManager
  - Whatsapp
  - Github
  - Google

/LogicalFileSet1/Pixel 3/data/data/com.android.chrome/app\_chrome/Default/History

I opened the text option in content viewer, and I found magisk manager.

Listing

LogicalFileSet1/Pixel 3/data/data/com.android.chrome/app\_chrome/Default

54 Results

Table	Thumbnail	Summary							
Save Table as CSV									
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	
UsageReportsBuffer				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	
UsageStats				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	
000035.ldb			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	997	
000038.ldb			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	157	
000317.log			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3482	
Affiliation Database			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	32768	
Bookmarks			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2660	
Cookies			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	40960	
CURRENT			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	16	

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Strings

Extracted Text

Translation

Page: 1 of 1 Page

Matches on page: - of - Match

100%

Reset

Text Source: File Text

```

SignedHeaders=host&actor_id=0&response-content-disposition=attachment%3B%20filename%3Dmagiskmanager-v7.5.1.apk&response-content-type=application%2Fvnd.android.package-archive
2 0 https://magiskmanager.com/downloading-magisk-manager
2 1 https://github.com/topjohnwu/Magisk/releases/download/manager-v7.5.1/MagiskManager-v7.5.1.apk
2 2 https://github-production-release-asset-2e65be.s3.amazonaws.com/67702184/5718de00-334c-11ea-9996-339eab534af0?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20200214%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20200214T215720Z&X-Amz-Expires=300&X-Amz-Signature=884719b02e3b28be455c7457ed91920978b0e28dd2f57bde9ab5dbe73564cc0e8&X-Amz-SignedHeaders=host&actor_id=0&response-content-disposition=attachment%3B%20filename%3Dmagiskmanager-v7.5.1.apk&response-content-type=application%2Fvnd.android.package-archive

downloads_slices

    download_id offset received_bytes finished

segments

    id name url_id

segment_usage

    id segment_id time_slot visit_count

typed_url_sync_metadata

    storage_key value

keyword_search_terms

    keyword_id url_id term normalized_term
2 2 magisk magisk

```

-----METADATA-----

7. What is the TikTok username that was assigned to the user?
- a. JoshuaHickman
  - b. ThisIsDFIR
  - c. User2812914319221
  - d. Unamed

/LogicalFileSet1/Pixel 3/data/data/com.zhiliaobaoapp.musically/databases/db\_im\_xx

Device	Register	Monitor	Id		U	UUUU-UUU-UUU UUUUUUU	UUUU-UUU-UUU UUUUUUU	UUUU-UUU-UUU UUUUUUU	UUUU-UUU-UUU UUUUUUU	z8r/z	Allocated	Allocated	unknown	/LogicalHwReset/1pxei s/d
Device	Register	Monitor	Id		+	UUUU UU UU UUUUUUU	UUUU UU UU UUUUUUU	UUUU UU UU UUUUUUU	UUUU UU UU UUUUUUU	76E64	Allocated	Allocated	unknown	HwSelfResetWd32/3rd

Hex    Text    Application    File Metadata    OS Account    Data Artifacts    Analysis Results    Context    Annotations    Other Occurrences

Strings    Extracted Text    Translation

Page: 1 of 1 Page    Matches on page: - of - Match    100%    Reset    Text Source: File Text

```

UID_SEC_UID_NICK_NAME_SIGNATURE_AVATAR_THUMB_FOLLOW_STATUS_UNIQUE_ID_WBINFO_VERIFY_CUSTOM_VERIFY_ENTERPRISE_VERIFY_REASON_VERIFICATION_TYPE_REMARK_NAME_SORT_WEIGHT_INITIAL_LETTER
SHORT_ID_REMARK_PINVIN_REMARK_INITIAL_NICK_NAME_PIVIN_NICK_NAME_UNIQUE_COMMERCE_UID_LEVEL_COLUMN_CONTACT_NAME_COLUMN_CONTACT_NAME_PIVIN_COLUMN_CONTACT_NAME_INITIAL
COLUMN_USER_SHARE_STATUS
6787436503258760198 M$4wLJABAAAAALWB6ftqZkQ5O2zic- ekBvTAe2nRmMPYmpdnMm_wKlhatcIQubQyA1TdHFUNP user2812914319221 {"height":0,"data_size":0,"url":"","url_list":["http://p16.muscdn.com/obj/musically-maliva-obj/1657089185431558"],"width":0} 2 user2812914319221 0 214531445763565764656958 U 46937952944 0 1
6791183665130374150 M$4wLJABAAAAMb-vYKR6tEbCfFYGOm4mNrItmDucG059g5S8PEEZabGWisiQQDPQZpX1Y91m user828007582568 {"height":0,"data_size":0,"url":"","url_list":["http://p16.muscdn.com/obj/musically-maliva-obj/1658004050243590"],"width":0} 2 user828007582568 0 21453144636576355556260 U 0 1
USER_EXTRA

UID_IS_DISABLE_SHOW_FOLLOW_BAR_IS_SAY_HELLO_LOGGER
.....METADATA.....
    
```

8. What was the TikTok verification code that was sent to the phone via messages?
- a. 2981
  - b. 9073
  - c. 352-593

d. **6327**

I opened the messages option in the phone database and found this.



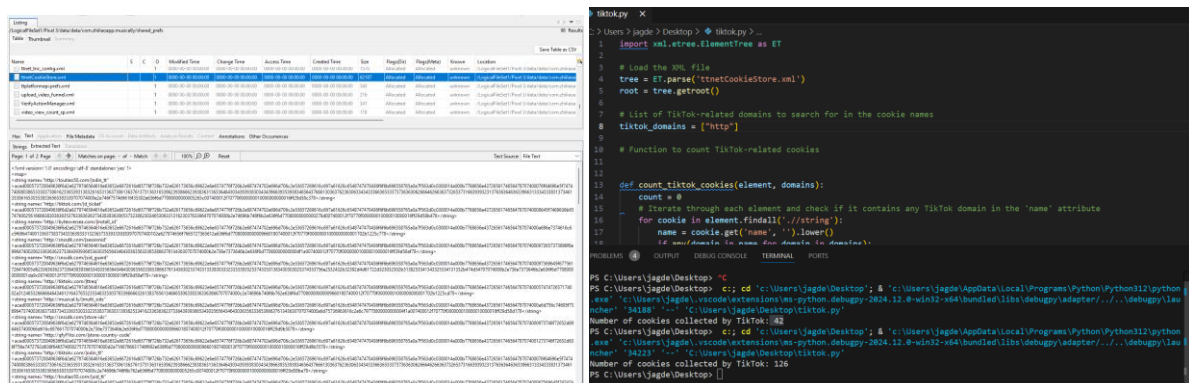
9. How many cookies did TikTok collect?

- a. 181
- b. **138**
- c. 57
- d. 23

/LogicalFileSet1/Pixel

3/data/data/com.zhiliaoapp.musically/shared\_prefs/ttnetCookieStore.xml

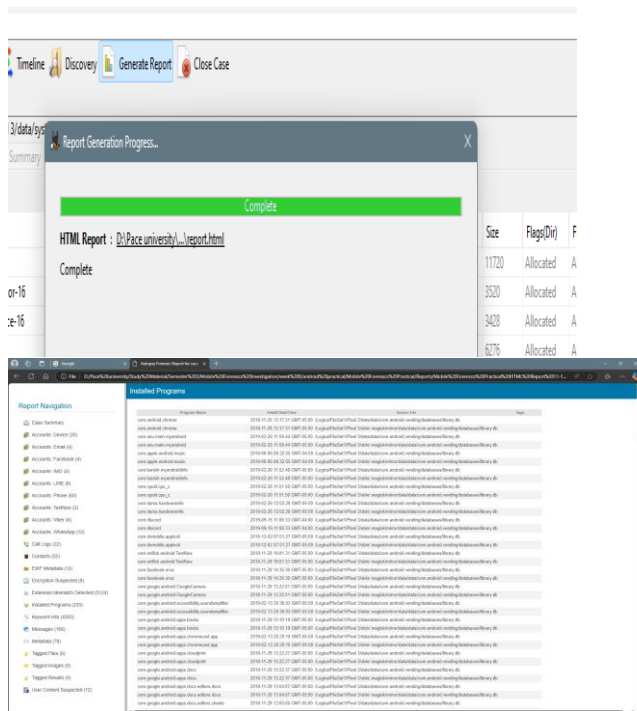
I found a file(ttnetCookieStore.xml) which contains list of cookies related to TikTok database, I made a python program to count the cookies and I got a number 126.



10. How many programs were installed on the device?

- a. 237
- b. 70
- c. 47
- d. **116**

I used the generate report option to get a report which gave me a list of the installed programs. I counted them manually they were 116 .



11. What is the Discord username for the phone's user?

- ThisIsDFIR#6767**
- 9197580276
- Thisisdfr100
- Thisisdfr#9980

/LogicalFileSet1/Pixel 3/sbin/.magisk/mirror/data/data/com.discord/files

```
ThisIsDFI
2020-01-29T20:20:59.769000+00:0
ThisIsDFI
Well hello there
2020-02-01T01:39:39.931000+00:0
```

12. What is the username of the only friend the user had on Venmo?

- Josh-Hickman-19**
- Thisisdffir100
- Hickman26
- ThisIsDFIR

/LogicalFileSet1/Pixel 3/sbin/.magisk/mirror/data/data/com.venmo/databases/venmo.sqlite

```
name lastname user_id external_id username picture_url last_accessed_timestamp registration_status phones_list emails_list is_returned_from_search friend_status is_top_friend address_book_id blocked
hua Hickman 2853160431386624630 Josh-Hickman-19 https://pics.venmo.com/bc1acbd-c8c5c-44b7-af3c-86b9f9efc0c52?width=460&height=460&photoVersion=1 0 is_user 0 friend 1 0
_ on_venmo 9195790479 0 not_friend 0 9 0
```

13. The user had a conversation on TextNow with a non-contact, what was their number?

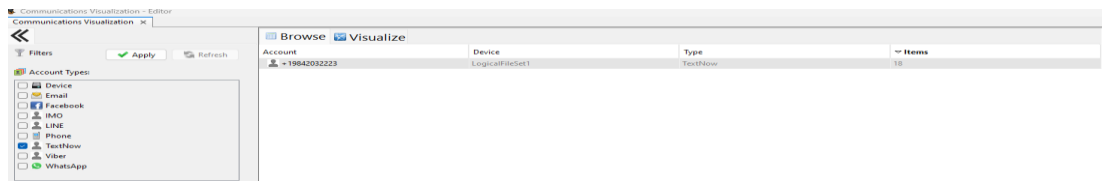
a. 212-367-1200

b. 919-574-4674

c. 984-203-2223

d. 984-235-2054 I open the communication option in autopsy to get the answer.

And I unchecked all options except TextNow



14. Can Autopsy crack passwords or decrypt files?

a. True

b. False

# Android App Practical

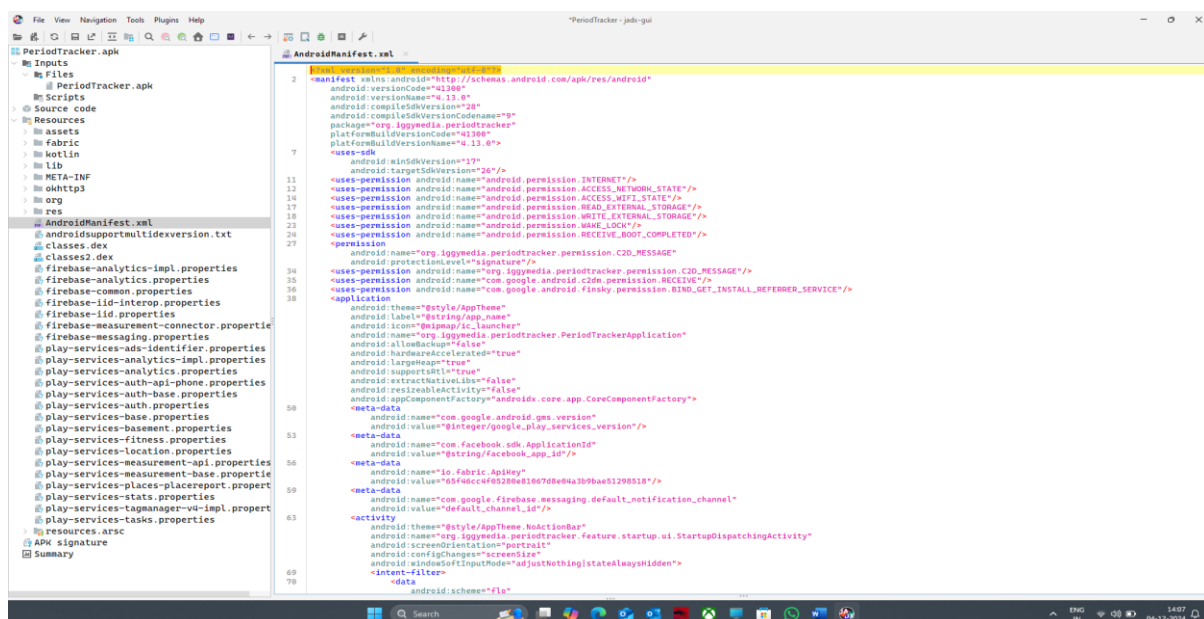
## Lesson 11

12/5/24

Subject - Doing Static and Dynamic Analysis of Period Tracker

### Static Analysis

At first, to perform the static analysis of period tracker, I used the JADX graphical user interface 1.5.1.exe and open the period tracker APK file in this tool. Then I decompiled the APK file to further analyse its different components. Then I looked up for AndroidManifest.xml file which is present in resources section.



After looking at the Android Manifest, we can see the user permissions given, and from that we can conclude risk level based on that which are as follows:-

android.permission.INTERNET - is required for connecting to external services, syncing data or downloading resources. The risk level **low**.

android.permission.ACCESS\_NETWORK\_STATE – is required for checking network connectivity(Wi-Fi, mobile data). The risk level is **low**.

android.permission.ACCESS\_WIFI\_STATE – is required monitoring Wi-Fi status and connectivity changes. The risk level is **low**.



android.permission.READ\_EXTERNAL\_STORAGE – is required to allow the app to read files on external storage such as logs, backups or media. The risk level for this is **moderate**.

android.permission.WRITE\_EXTERNAL\_STORAGE – is required to permit writing files to external storage. Risks include creating unencrypted backups. The risk level is **high**.

android.permission.WAKE\_LOCK – is required to prevent the device from sleeping during specific tasks such as background tasks and syncing. The risk level is **low**.

Android.permission.RECEIVE\_BOOT\_COMPLETED – is required for allowing the app to start background processes after device boots. The risk factor is **moderate**.

org.iggymedia.periodtracker.permission.C2D\_MESSAGE – is required for internal permission for handling messages specific to this app. The Risk factor is **low**.

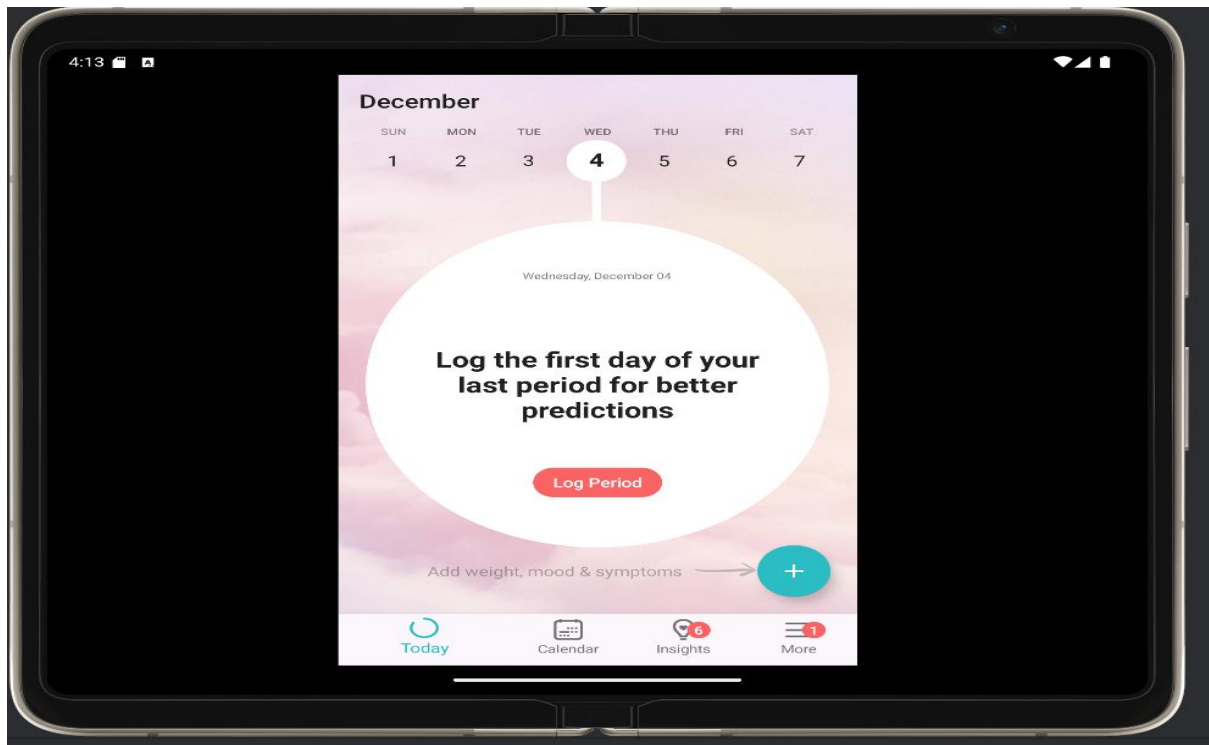
com.google.android.c2dm.permission.RECEIVE- is required for receiving push notifications via firebase cloud messaging. The risk level is **low**.

com.google.android.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE – is required for allowing app to track installations via the google play store. The risk is **low**.

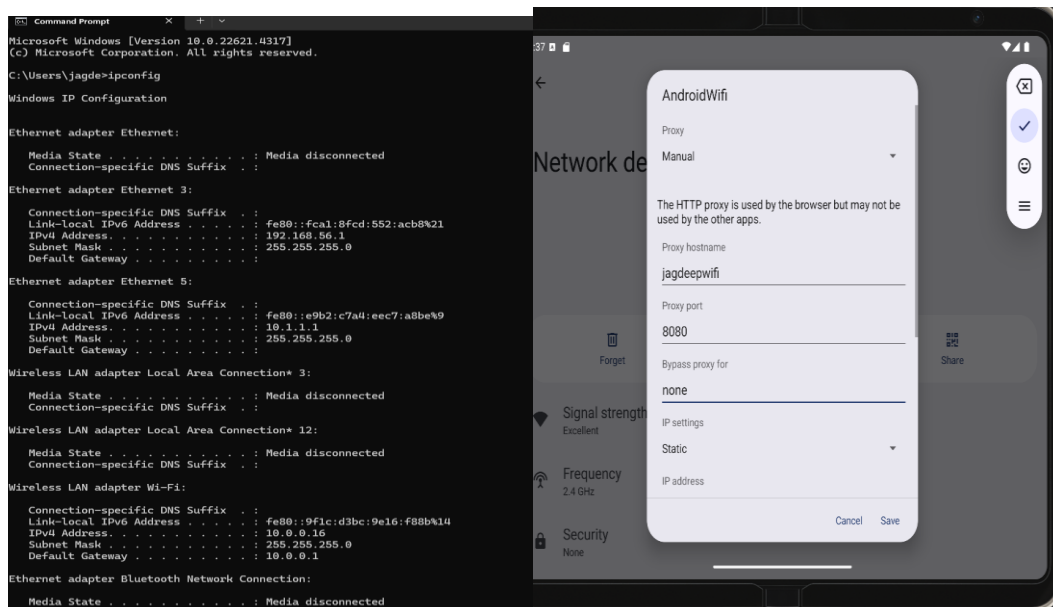
## Dynamic analysis

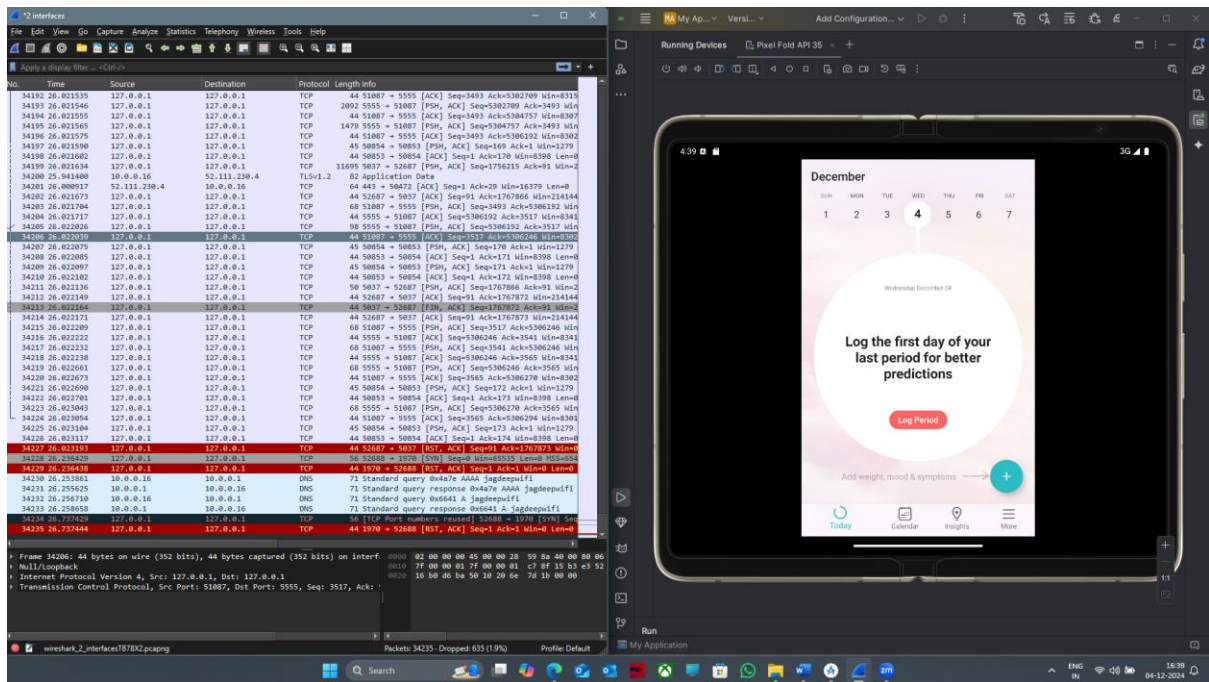
For performing the dynamic analysis of the app. I did used android studio emulator on my windows 11 PC and then installed the provided application period tracker using drag and dropping the APK file over the graphical interface of the Android emulator. I am using pixel fold API 35, android version 15 vanilla ice cream.





I Successfully turned the application on and start doing activities on it. To do the dynamic analysis, I am using Wireshark tool which will intercept the network activity while I am using the app. To perform this I have to manually set up proxy settings in android emulator Wi-Fi settings according to my PC host configurations.





As we can clearly see the packet capturing while using the app,