



COMP2320

Assignment-2



JUNE 6, 2021

SUJITH BELLAM
45664455

Abstract

This report contains the forensic analysis of two different network traffic captures. One network traffic capture is from my friend, and the other is from Google. My friend captured the network traffic of his neighbour a week ago, and I'm an employee at Google and was asked to perform analysis on the MobInCube app.

Table of Contents

Abstract.....	1
Acquisition	3
Network Forensics	3
Q1. What is the neighbour's name?	3
Answer:	3
Analysis:	3
Evidence Analysed:	3
Steps Taken:.....	3
Q2. What is the neighbour's email address?	4
Answer:	4
Analysis:	4
Evidence:.....	4
Steps Taken:.....	5
Q3. What is the neighbour's email password?	5
Answer:	5
Analysis:	5
Evidence:.....	5
Steps Taken:.....	6
Q4. What are the email addresses (at least two) of the neighbour's correspondents? What is the email of the correspondent the neighbour is most likely have gone to visit?	7
Answer:	7
Analysis:	7
Evidence:.....	8
Steps Taken:.....	9
Q5. What is the name of the file containing the meeting location?	11
Answer:	11
Analysis:	11
Evidence:.....	12

Steps Taken:	12
Q6. Where are they meeting, and what is the correspondent bringing?	13
Answer:	13
Analysis:	13
Evidence:	14
Steps Taken:	14
App Forensics	19
Q7. What is the Phone Model and network carrier name (carrierName) on which MobInCube was run?	19
Answer:	19
Analysis:	19
Evidence:	20
Steps Taken:	20
Q8. What is the location (latitude and longitude) value shared with https://stats.mobincube.com ?	24
Answer:	24
Analysis:	24
Evidence:	25
Steps Taken:	25
Q9. Visit the privacy policy of MobInCube (http://myapptterms.com/reader.php?lang=en), and report whether or not the app is transparent about the information they collect?	25
Answer:	25
Analysis:	25
Evidence:	26
Q10. What are your recommendations on the security and privacy options of the app? Would you recommend this app to a user? Why or why not?	26
Answer:	26
Conclusion	27
Glossary	27
Appendix	28
References	28

Acquisition

I was given two network traffic captures to be analysed, one by my friend and another by Google. The first network traffic capture contains my friend's neighbour's traffic, whom my friend suspects to be in the wrong place. The second network capture has the traffic that was sent and received by the MobInCube app. MobInCube is a tool to create apps for free without the need for coding [1]. I used Wireshark 3.4.4, NetworkMiner 2.6, and mitmproxy 6.0.2 to conduct the forensic analysis with Windows 10 Pro operating system. I used lightshot software to capture snapshots and Microsoft Word to generate this report.

Network Forensics

Q1. What is the neighbour's name?

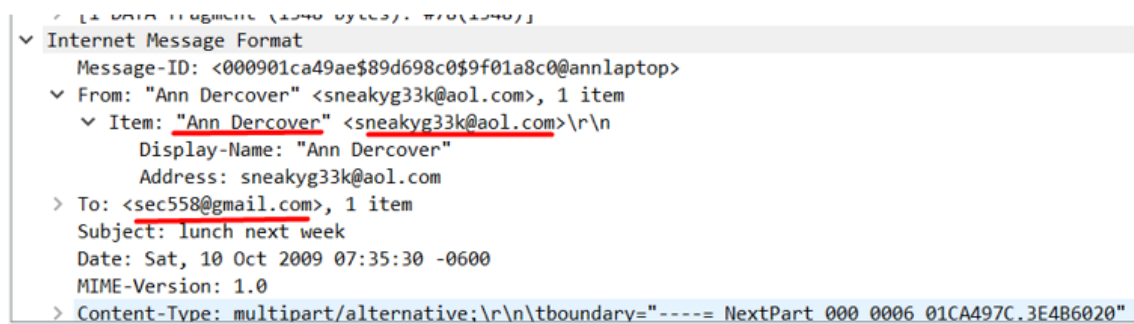
Answer:

The name of my friend's neighbour is Ann Decover.

Analysis:

After analysing packets with SMTP (Simple Mail Transfer Protocol) protocol, I found a mail from Ann Decover to sec558@gmail.com. The mail also states that Ann cannot go to lunch with the recipient next week as Ann is going out of town.

Evidence Analysed:



```
Internet Message Format
Message-ID: <000901ca49ae$89d698c0$9f01a8c0@annlaptop>
From: "Ann Decover" <sneakyg33k@aol.com>, 1 item
  Item: "Ann Decover" <sneakyg33k@aol.com>\r\n
    Display-Name: "Ann Decover"
    Address: sneakyg33k@aol.com
To: <sec558@gmail.com>, 1 item
Subject: lunch next week
Date: Sat, 10 Oct 2009 07:35:30 -0600
MIME-Version: 1.0
Content-Type: multipart/alternative;\r\n\tboundary="----- NextPart 000 0006 01CA497C.3E486020"
```

Snapshot 1 - Email from Ann (neighbour) to sec558@gmail.com

From Snapshot-1, we know the name of the neighbour as Ann Decover.

Steps Taken:

1. Open Wireshark
2. Load the network capture file (pcap file) into Wireshark
3. Scroll down till you find SMTP

52	82.678216	10.1.1.20	192.168.1.159	DNS	299 Standard query response 0xecac9 A smtp.aol.com OWWE smtp.cs.com A 64.12.102.142 A 64.12.194.119 A 205.188.159.148 A 205.188.24...
53	82.707578	192.168.1.159	64.12.102.142	TCP	62 1856 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
54	82.812857	64.12.102.142	192.168.1.159	TCP	58 587 → 1856 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
55	82.822388	192.168.1.159	64.12.102.142	TCP	54 1856 → 587 [ACK] Seq=1 Ack=1 Win=64240 Len=0
56	82.908997	64.12.102.142	192.168.1.159	SMTP	134 S: 220 cia-mc06.mx.aol.com ESMTP mail.cia-mc06.1; Sat, 10 Oct 2009 15:35:16 -0400
57	82.908439	192.168.1.159	64.12.102.142	SMTP	70 C: 1850 annlaptop
58	82.998926	64.12.102.142	192.168.1.159	TCP	54 587 → 1036 [ACK] Seq=81 Ack=17 Win=64240 Len=0
59	83.107523	64.12.102.142	192.168.1.159	SMTP	305 S: 250-cia-mc06.mx.aol.com host-69-148-19-190.static.comcast.net AUTH=LOGIN PLAIN XOOL-UAS-#B AUTH LOGIN PLAIN XOOL-UAS-#L
60	83.109678	192.168.1.159	64.12.102.142	SMTP	66 C: AUTH LOGIN
61	83.118259	64.12.102.142	192.168.1.159	TCP	54 587 → 1036 [ACK] Seq=332 Ack=29 Win=64240 Len=0
62	83.228262	64.12.102.142	192.168.1.159	SMTP	72 S: 314 XOOL-cia-mc06

Snapshot 2 - SMTP Packets

4. Find the packet where a mail was sent from the neighbour

79	83.811530	64.12.102.142	192.168.1.159	TCP	54 587 → 1036 [ACK] Seq=471 Ack=1485 Win=64240 Len=0
80	83.811862	192.168.1.159	64.12.102.142	SMTP/IMF	59 From: "Ann Dercover" <sneakyg33k@aol.com>, subject: lunch next week, (text/plain) (text/html)
81	83.812250	64.12.102.142	192.168.1.159	TCP	54 587 → 1036 [ACK] Seq=471 Ack=1490 Win=64240 Len=0

Snapshot 3 - Mail from Ann Dercover

5. Double click on the packet to see its information

Snapshot 4 - More information on SMTP/IMF packet

Q2. What is the neighbour's email address?

Answer:

Ann Dercover's email address is sneakyg33k@aol.com

Analysis:

Similar to Q1, analysing SMTP packets will give us information regarding Ann's email address

Evidence:

From snapshot-1, we know that Ann Dercover's email address is sneakyg33k@aol.com

Steps Taken:

- Same as Q1

Q3. What is the neighbour's email password?

Answer:

The password of Ann Dercovers email address is 558r00lz. As the username and password are encrypted, I decrypted the hashed password NTU4cjAwbHo= with base64.

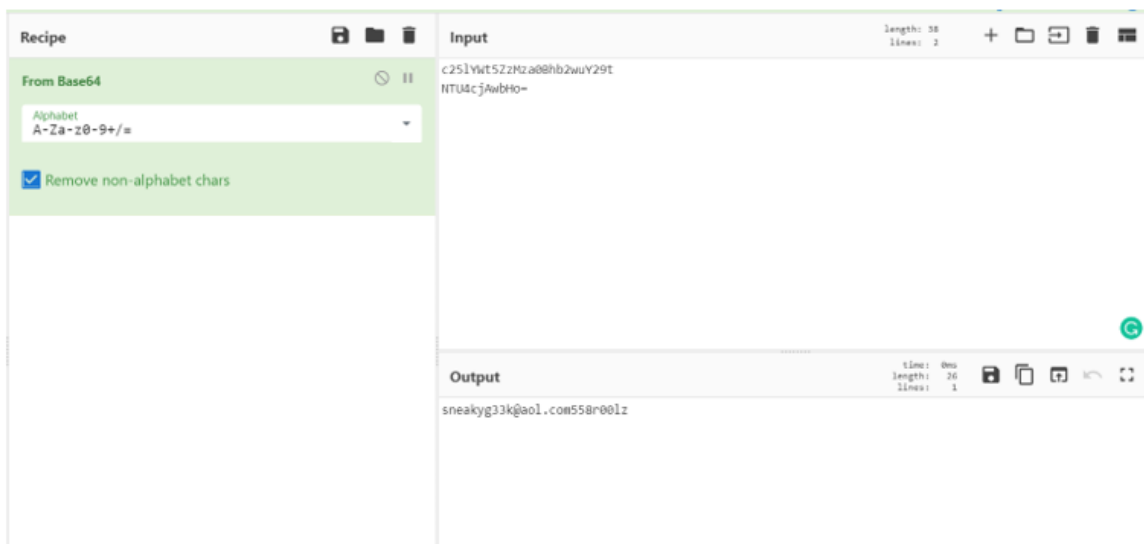
Analysis:

By going through SMTP packets, we can find the username and password used by Ann Dercover. However, the username and the password are encrypted and can be decrypted using base64. I used the online tool icyberchef to decrypt the username and password.

Evidence:

61	83.110259	64.12.102.142	192.168.1.159	TCP	54 587 → 1036 [ACK] Seq=332 Ack=29 Win=64240 Len=0
62	83.220242	64.12.102.142	192.168.1.159	SMTP	72 S: 334 VXN1cm5hbWU6
63	83.221008	192.168.1.159	64.12.102.142	SMTP	80 C: User: c251Ymt5ZzZMza08hb2wuY29t
64	83.221698	64.12.102.142	192.168.1.159	TCP	54 587 → 1036 [ACK] Seq=350 Ack=55 Win=64240 Len=0
65	83.331342	64.12.102.142	192.168.1.159	SMTP	72 S: 334 UGFzc3dvcmQ6
66	83.331953	192.168.1.159	64.12.102.142	SMTP	68 C: Pass: NTU4cjAwbHo=
67	83.332382	64.12.102.142	192.168.1.159	TCP	54 587 → 1036 [ACK] Seq=368 Ack=69 Win=64240 Len=0
68	83.462637	64.12.102.142	192.168.1.159	SMTP	85 S: 235 AUTHENTICATION SUCCESSFUL
69	83.465436	192.168.1.159	64.12.102.142	SMTP	87 C: MAIL FROM: <sneakyg33k@aol.com>
70	83.466089	64.12.102.142	192.168.1.159	TCP	54 587 → 1036 [ACK] Seq=399 Ack=102 Win=64240 Len=0

Snapshot 5 - Wireshark analysis of username and password of Ann Decovers email address



Snapshot 6 - Decrypted Ann Dercovers email address username and password

From Snapshot-1, Snapshot-5 and Snapshot-6, we know that the email address of Ann Dercover is sneakyg33k@gmail.com, and the password is 558r00lz.

Steps Taken:

1. Follow the steps 1-3 from Q1
2. Find the packet that contains the hashed username

62	83.220242	64.12.102.142	192.168.1.159	SMTP	72 S: 334 VX01cm5hbU06
63	83.221008	192.168.1.159	64.12.102.142	SMTP	80 C: User: c25lYwt5ZzZmZa0Bhb2wuY29t
64	83.221698	64.12.102.142	192.168.1.159	TCP	54 587 → 1036 [ACK] Seq=350 Ack=55 Win=64240 Len=0

Snapshot 7 - Hashed username of Ann Dercover Email address

3. Find the packet that contains the hashed password

65	83.331342	64.12.102.142	192.168.1.159	SMTP	72 S: 334 UGFzc3dvcnQ6
66	83.331953	192.168.1.159	64.12.102.142	SMTP	68 C: Pass: NTU4cjAwbHo=
67	83.332382	64.12.102.142	192.168.1.159	TCP	54 587 → 1036 [ACK] Seq=368 Ack=69 Win=64240 Len=0

Snapshot 8 - Hashed password of Ann Dercover's Email address

4. Copy the hashes and paste them on the Input box of the icyberchef.com website

Input length: 38
lines: 2 + 📁 ↻ 🗑️ 🖨️

```
c25lYwt5ZzZmZa0Bhb2wuY29t
NTU4cjAwbHo=
```

Snapshot 9 - iCyberChef Input

5. Select the recipe as From Base64 (decrypt from base64)

Operations

Search...

Favourites ★

- To Base64
- From Base64**
- To Hex

Recipe 📁 🗑️

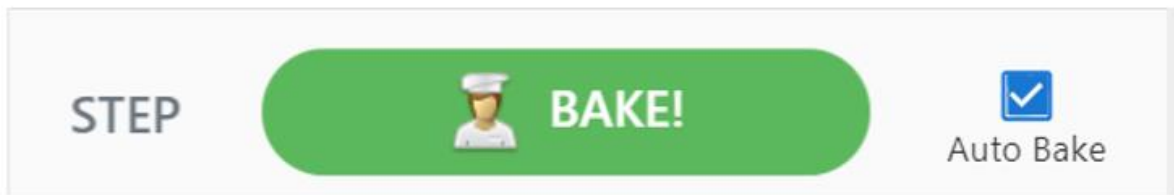
From Base64 🔇 ||

Alphabet
A-Za-z0-9+/=

Remove non-alphabet chars

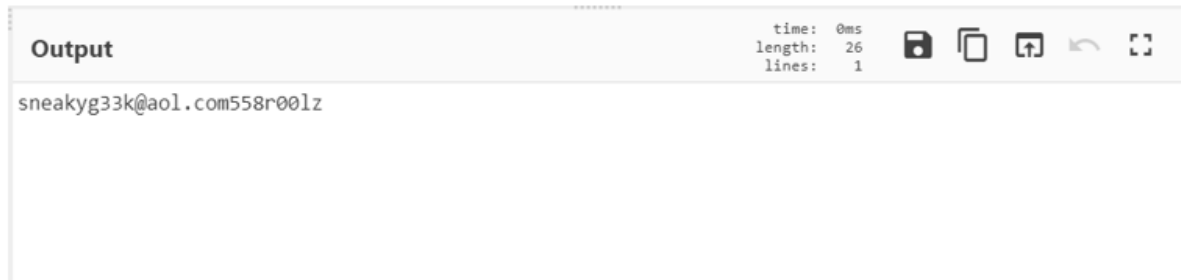
Snapshot 10 - iCyberChef recipe

6. Click on the Bake button if auto bake is not selected



Snapshot 11 - iCyberChef bake

7. Get the decrypted username and password from the Output box



Snapshot 12 - iCyberChef Output

Q4. What are the email addresses (at least two) of the neighbour's correspondents?
What is the email of the correspondent the neighbour is most likely have gone to visit?

Answer:

Ann Dercover sent an email to:

1. sec558@gmail.com
2. mistersecretx@aol.com

Ann Dercover is most likely to visit the owner of the mistersecretx@aol.com email address.

Analysis:

By analysing the SMTP packets from the network capture, we can find two emails sent by Ann Dercover. One email was sent to sec588@gmail.com with the subject lunch next week, and the other email was sent to mistersecretx@aol.com with the subject rendezvous. In the email to sec588@gmail.com, Ann Dercover says that he/she/they will not be available for lunch next week as Ann is going out of town. Whereas in the email to mistersecretx@aol.com, Ann Dercover asks the recipient to bring a fake passport and a bathing suit and that the address is attached to the email. It looks like Ann Dercover is going out on vacation with mistersecretx@aol.com.

Evidence:

Message-ID: <000901ca49ae\$89d698c0\$9f01a8c0@annlaptop>\r\n
From: "Ann Dercover" <sneakyg33k@aol.com>\r\n
To: <sec558@gmail.com>\r\n
Subject: lunch next week\r\n
Date: Sat, 10 Oct 2009 07:35:30 -0600\r\n
MIME-Version: 1.0\r\n
Content-Type: multipart/alternative;\r\n
\tboundary="-----_NextPart_000_0006_01CA497C.3E4B6020"\r\n
X-Priority: 3\r\n
X-MSMail-Priority: Normal\r\n
X-Mailer: Microsoft Outlook Express 6.00.2900.2180\r\n
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180\r\n
\r\n
This is a multi-part message in MIME format.\r\n
\r\n
-----_NextPart_000_0006_01CA497C.3E4B6020\r\n
Content-Type: text/plain;\r\n
\tcharset="iso-8859-1"\r\n
Content-Transfer-Encoding: quoted-printable\r\n
\r\n
Sorry-- I can't do lunch next week after all. Heading out of town. =\r\n
Another time! -Ann\r\n
-----_NextPart_000_0006_01CA497C.3E4B6020\r\n
Content-Type: text/html;\r\n

Snapshot 13 - Ann's email to sec558@gmail.com

Message-ID: <001101ca49ae\$e93e45b0\$9f01a8c0@annlaptop>\r\n
From: "Ann Dercover" <sneakyg33k@aol.com>\r\n
To: <mistersecretx@aol.com>\r\n
Subject: rendezvous\r\n
Date: Sat, 10 Oct 2009 07:38:10 -0600\r\n
MIME-Version: 1.0\r\n
Content-Type: multipart/mixed;\r\n
\tboundary="-----_NextPart_000_000D_01CA497C.9DEC1E70"\r\n
X-Priority: 3\r\n
X-MSMail-Priority: Normal\r\n
X-Mailer: Microsoft Outlook Express 6.00.2900.2180\r\n
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180\r\n
\r\n
This is a multi-part message in MIME format.\r\n
\r\n
-----_NextPart_000_000D_01CA497C.9DEC1E70\r\n
Content-Type: multipart/alternative;\r\n
\tboundary="-----_NextPart_001_000E_01CA497C.9DEC1E70"\r\n
\r\n
\r\n
-----_NextPart_001_000E_01CA497C.9DEC1E70\r\n
Content-Type: text/plain;\r\n
\tcharset="iso-8859-1"\r\n
Content-Transfer-Encoding: quoted-printable\r\n
\r\n
Hi sweetheart! Bring your fake passport and a bathing suit. Address =\r\n
attached. love, Ann\r\n
-----_NextPart_001_000E_01CA497C.9DEC1E70\r\n

Snapshot 14 - Ann's email to mistersecretx@aol.com

From Snapshot-13 and Snapshot-14, we can understand that Ann Dercover is mostly to visit mistersecretx@aol.com.

Steps Taken:

1. Follow steps one and two from Q1.
2. Enter smtp into filter bar and press enter

No.	Time	Source	Destination	Protocol	Length	Info
56	82.708997	64.12.102.142	192.168.1.159	SMTP	1345	220 cia-mc06.sx.aol.com [SMTP mail_cia-mc06.1; Sat, 10 Oct 2009 15:35:10 -0400
57	82.908439	192.168.1.159	64.12.102.142	SMTP	70	C: EML0 annlaptop
59	83.107523	64.12.102.142	192.168.1.159	SMTP	305	S: 250-cia-mc06.sx.aol.com host=69-140-19-190.static.comcast.net AUTH:LOGIN PLAIN XAOL-UAS-MB AUTH:LOGIN PLAIN XAOL-UAS-MB
60	83.109678	192.168.1.159	64.12.102.142	SMTP	66	C: AUTH LOGIN
62	83.228242	64.12.102.142	192.168.1.159	SMTP	72	S: 334 VOICE05H0M6
63	83.221088	192.168.1.159	64.12.102.142	SMTP	80	C: User: c251Pnt5ZtZa0thb2auV20t
65	83.331342	64.12.102.142	192.168.1.159	SMTP	72	S: 334 V0Fzc3b0v0Q0
66	83.331953	192.168.1.159	64.12.102.142	SMTP	60	C: Pass: NTLM:3Aub0o:
68	83.462637	64.12.102.142	192.168.1.159	SMTP	85	S: 235 AUTHENTICATION SUCCESSFUL
69	83.465436	192.168.1.159	64.12.102.142	SMTP	87	C: MAIL FROM: <sneaky33k@aol.com>
71	83.578844	64.12.102.142	192.168.1.159	SMTP	62	S: 250 OK
72	83.579698	192.168.1.159	64.12.102.142	SMTP	83	C: RCPT TO: <sec558@gmail.com>
78	83.697313	64.12.102.142	192.168.1.159	SMTP	62	S: 250 OK
75	83.698397	192.168.1.159	64.12.102.142	SMTP	60	C: DATA
77	83.808024	64.12.102.142	192.168.1.159	SMTP	110	S: 354 START MAIL INPUT, END WITH "." ON A LINE BY ITSELF
78	83.810602	192.168.1.159	64.12.102.142	SMTP	1402	C: DATA fragment, 1348 bytes
80	83.811862	192.168.1.159	64.12.102.142	SMTP	59	C: DATA fragment, 1348 bytes
83	84.149429	192.168.1.159	64.12.102.142	SMTP	60	C: QUIT
85	84.299730	64.12.102.142	192.168.1.159	SMTP	81	S: 221 SERVICE CLOSING CHANNEL

Snapshot 15 - SMTP filter on Wireshark

This will only show the packets that use the SMTP protocol.

- Find the packet that contains the data of the email sent to sec558@gmail.com

77	83.808024	64.12.102.142	192.168.1.159	SMTP	110	S: 354 START MAIL INPUT, END WITH "." ON A LINE BY ITSELF
78	83.810602	192.168.1.159	64.12.102.142	SMTP	1402	C: DATA fragment, 1348 bytes
80	83.811862	192.168.1.159	64.12.102.142	SMTP	59	C: DATA fragment, 1348 bytes

Snapshot 16 - Data packet sent to email address sec558@gmail.com

- Double click on the packet to see the email content

Wireshark - Packet 78 - forensics.pcap

```

> Frame 78: 1402 bytes on wire (11216 bits), 1402 bytes captured (11216 bits)
> Ethernet II, Src: Dell14d:4f:ae (00:21:70:Ad:4f:ae), Dst: VMware_9b:ee:14 (00:0c:29:9b:ee:14)
> Internet Protocol Version 4, Src: 192.168.1.159, Dst: 64.12.102.142
> Transmission Control Protocol, Src Port: 1036, Dst Port: 587, Seq: 137, Ack: 471, Len: 1348
Simple Mail Transfer Protocol
  Line-based text data (40 lines)
    Message-ID: <000901ca49ae589d698c059f01a8c0@annlaptop>\r\n
    From: "Ann Dercover" <sneaky33k@aol.com>\r\n
    To: <sec558@gmail.com>\r\n
    Subject: lunch next week\r\n
    Date: Sat, 10 Oct 2009 07:35:30 -0600\r\n
    MIME-Version: 1.0\r\n
    Content-Type: multipart/alternative;\r\n
    \tboundary="-----_NextPart_000_0006_01CA497C.3E486020"\r\n
    X-Priority: 3\r\n
    X-MSMail-Priority: Normal\r\n
    X-Mailer: Microsoft Outlook Express 6.00.2900.2180\r\n
    X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180\r\n
    \r\n
    This is a multi-part message in MIME format.\r\n
0000 00 0c 29 9b ee 14 00 21 70 ad 4f ae 08 00 45 00  --)--- | | p00: | E-
0010 05 6c 00 84 40 00 80 06 8c 26 c0 a8 01 9f 40 0c  -1-@... &...@
0020 66 8e 04 0c 02 4b 91 c9 13 fb 26 36 01 be 50 18  f...K...-86-P
0030 f9 1a d1 a0 00 0d 4d 65 73 73 61 67 65 2d 49 44  -....Me ssage-ID
0040 3a 20 3c 30 30 39 30 31 63 61 34 39 61 65 24  : <000901ca49ae5
0050 38 39 64 36 39 38 63 30 24 39 66 30 31 61 38 63  89d698c0 59f01a8c
0060 30 40 61 6e 6e 6e 61 70 74 6f 70 3e 0d 0a 46 72  0@annlap top>:Fr
0070 6f 6d 3a 20 22 41 6e 6e 20 44 65 72 63 6f 76 65  om: "Ann Dercove
0080 72 22 20 3c 73 6e 65 61 6b 79 67 33 33 6b 40 61  r" <snea kyg33k@a
0090 6f 6c 2e 63 6f 6d 3e 0d 0a 54 6f 3a 20 3c 73 65  ol.com> -To: <se
00a0 63 35 35 38 40 67 6d 61 69 6c 2e 63 6f 6d 3e 0d  c558@ma il.com>
00b0 0a 53 75 62 6a 65 63 74 3a 20 6c 75 6e 63 68 20  -Subject : lunch
00c0 6e 65 78 74 20 77 65 65 6b 0d 0a 44 61 74 65 3a  next wee k-Date:

```

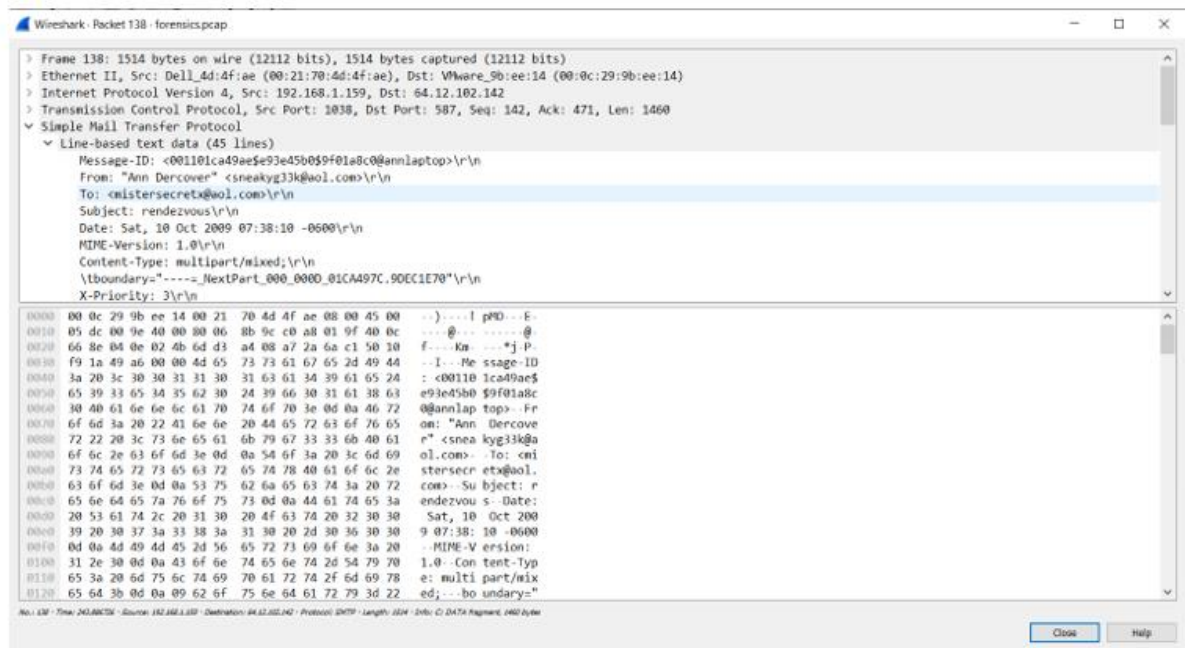
Snapshot 17 - Content of email sent to sec558@gmail.com

- Find the packet that contains the data of the email sent to mistersecretx@aol.com

137	243.884497	64.12.102.142	192.168.1.159	SMTP	110	S: 354 START MAIL INPUT, END WITH "." ON A LINE BY ITSELF
138	243.886726	192.168.1.159	64.12.102.142	SMTP	1514	C: DATA fragment, 1460 bytes
140	243.887693	192.168.1.159	64.12.102.142	SMTP	1514	C: DATA fragment, 1460 bytes

Snapshot 18 - Data fragment that contains the content of email sent to mistersecretx@aol.com

6. Double click on the packet to see the email content



Snapshot 19 - Content of email sent to mistersecretx@aol.com

Q5. What is the name of the file containing the meeting location?

Answer:

The name of the file containing the meeting location is `secretrendezvous.docx`.

Analysis:

By analysing the SMTP packets of email sent to mistersecretx@aol.com, we know that the name of the file containing the meeting location is `secretrendezvous.docx`.

Evidence:

```

Simple Mail Transfer Protocol
├── Line-based text data (25 lines)
│   ├── 1_000E_01CA497C.9DEC1E70--\r\n
│   ├── \r\n
│   ├── -----_NextPart_000_000D_01CA497C.9DEC1E70\r\n
│   ├── Content-Type: application/octet-stream;\r\n
│   ├── \tname="secretrendezvous.docx"\r\n
│   ├── Content-Transfer-Encoding: base64\r\n
│   ├── Content-Disposition: attachment;\r\n
│   ├── \tfilename="secretrendezvous.docx"\r\n
│   ├── \r\n
│   ├── UEsDBBQABgAIAAAAIQDleUAGfwEAAncFAAATAAgCW0NvbnRlbnRfVHlwZXNdLnhjbCCiBAIooAAC\r\n
│   ├── AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\r\n
│   ├── AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\r\n
│   ├── AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\r\n
│   ├── AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\r\n
│   ├── AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\r\n
│   ├── AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\r\n
│   └── AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\r\n

```

Snapshot 20 – Filename

From Snapshot-20, we know that the name of the file containing the meeting location is secretrendezvous.docx. It is a word document file.

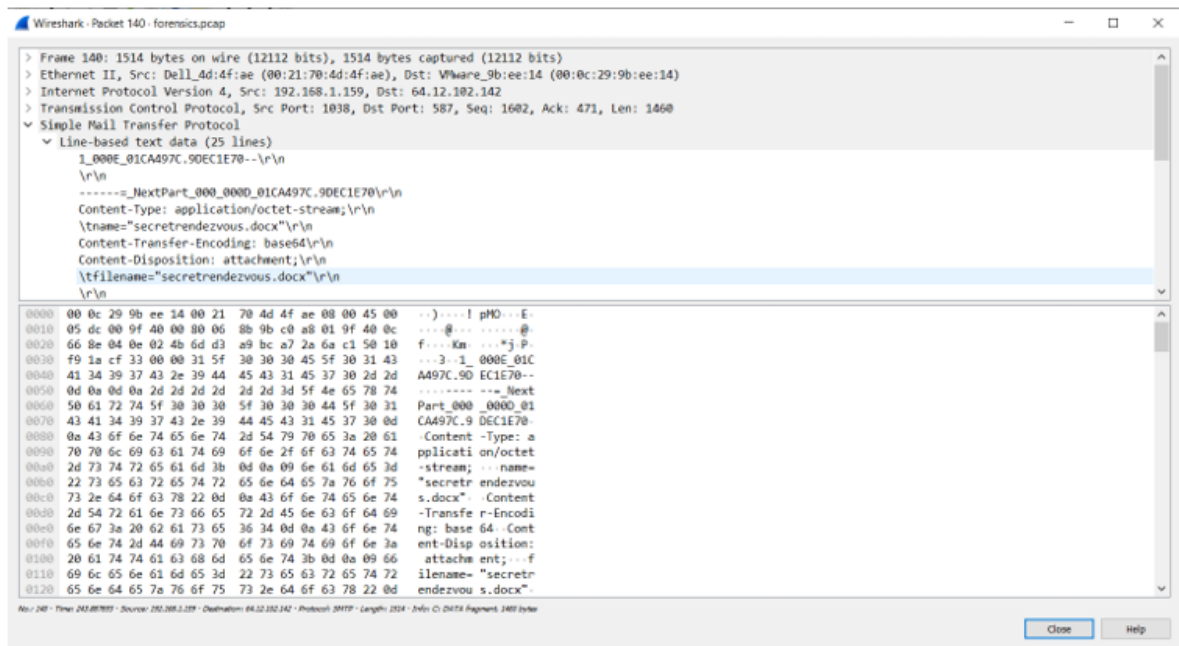
Steps Taken:

1. Follow steps one and two from Q4
2. Find the packet that contains the data relating to the attachment

138	243.886726	192.168.1.159	64.12.102.142	SMTP	1514 C: DATA fragment, 1460 bytes
140	243.887693	192.168.1.159	64.12.102.142	SMTP	1514 C: DATA fragment, 1460 bytes
142	243.888678	192.168.1.159	64.12.102.142	SMTP	1514 C: DATA fragment, 1460 bytes

Snapshot 21 - The packet that contains the data relating to the attachment

3. Double click on the packet to get the information on the attachment



Snapshot 22 - Information on the attachment

Q6. Where are they meeting, and what is the correspondent bringing?

Answer:

They are meeting at the fountain near the address:

Playa del Carmen

1 Av. Constituyentes 1 Calle 10 x la 5ta

Avenida

Playa del Carmen, 77780, Mexico

01 984 873 4000

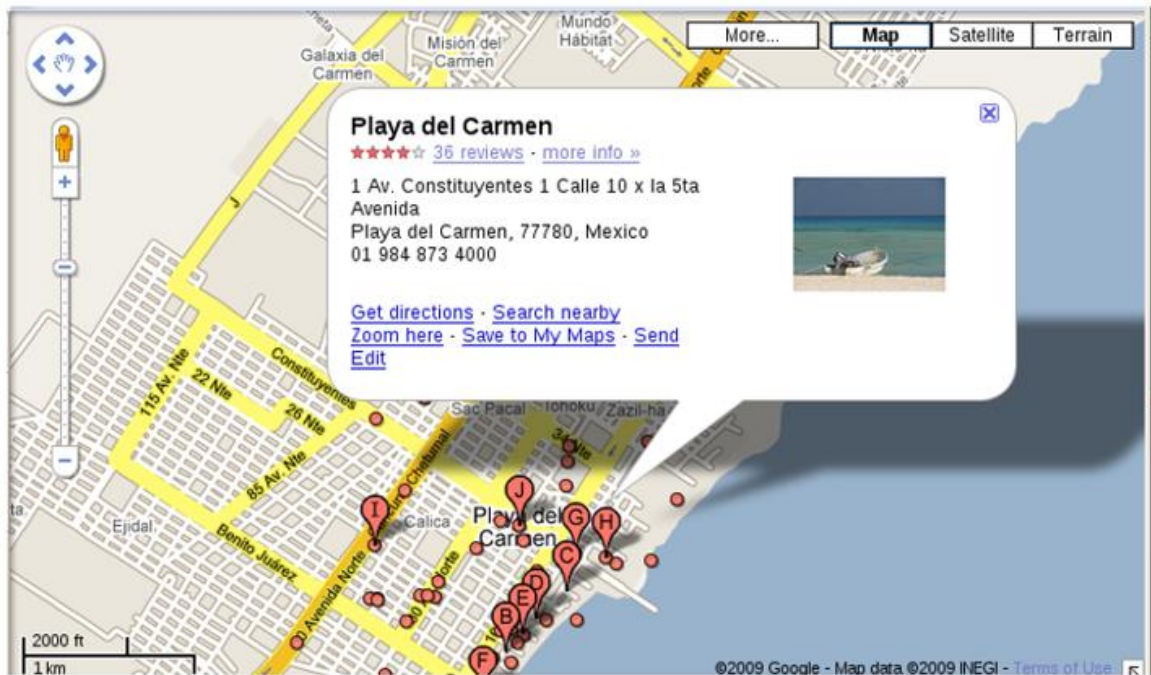
The correspondent is bringing a fake passport and a bathing suit.

Analysis:

We already know that the correspondent is bringing a fake passport and a bathing suit from the previous questions. To get the address from the secretrendezvous.docx file, we have to open the pcap file with NetworkMiner, allowing us to open the secretrendezvous.docx file. Along with the address, we also learn that Ann Dercover is bringing all his/her/their cash.

Evidence:

Meet me at the fountain near the rendezvous point. Address below. I'm bringing all the cash.

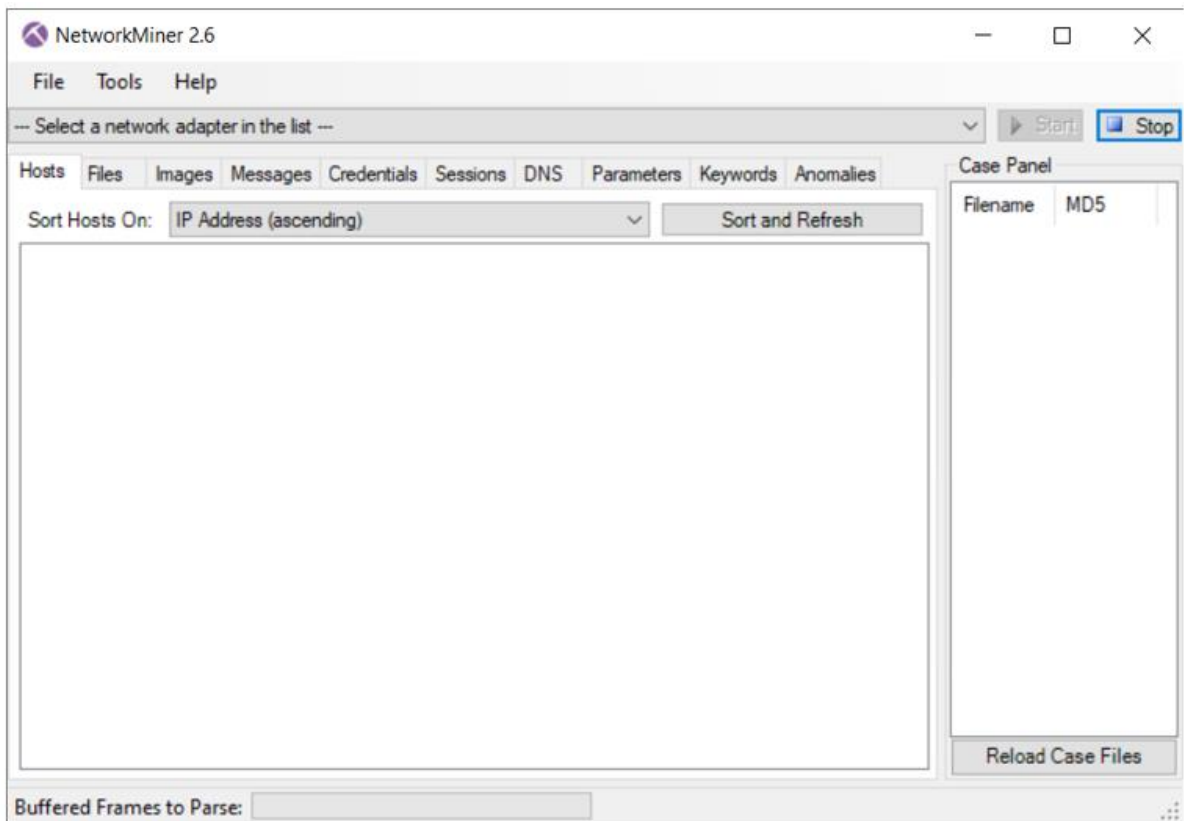


Snapshot 23 - secretrendezvous.docx

From Snapshot-14 and Snapshot-23, we know that the meeting place is a fountain near the address provided in the Snapshot-23, and the correspondent is bringing a fake passport and a bathing suit.

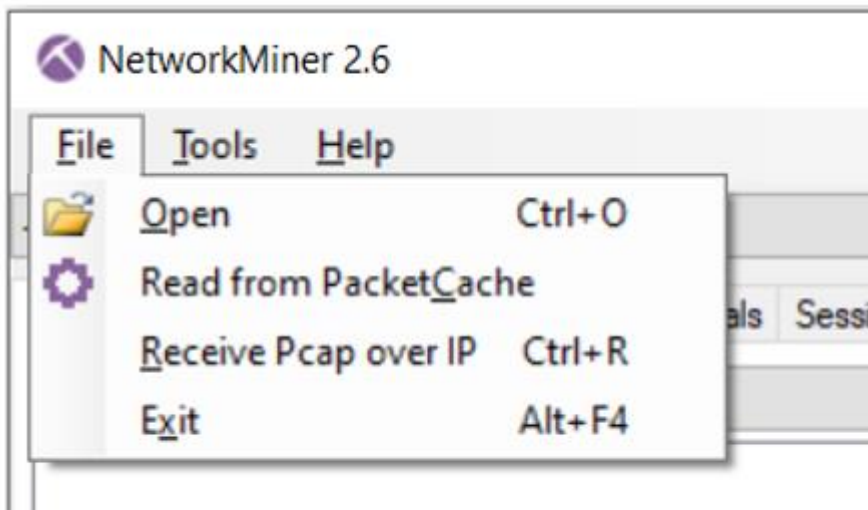
Steps Taken:

1. Follow steps one, two, five and six from Q4.
2. Open Network Miner



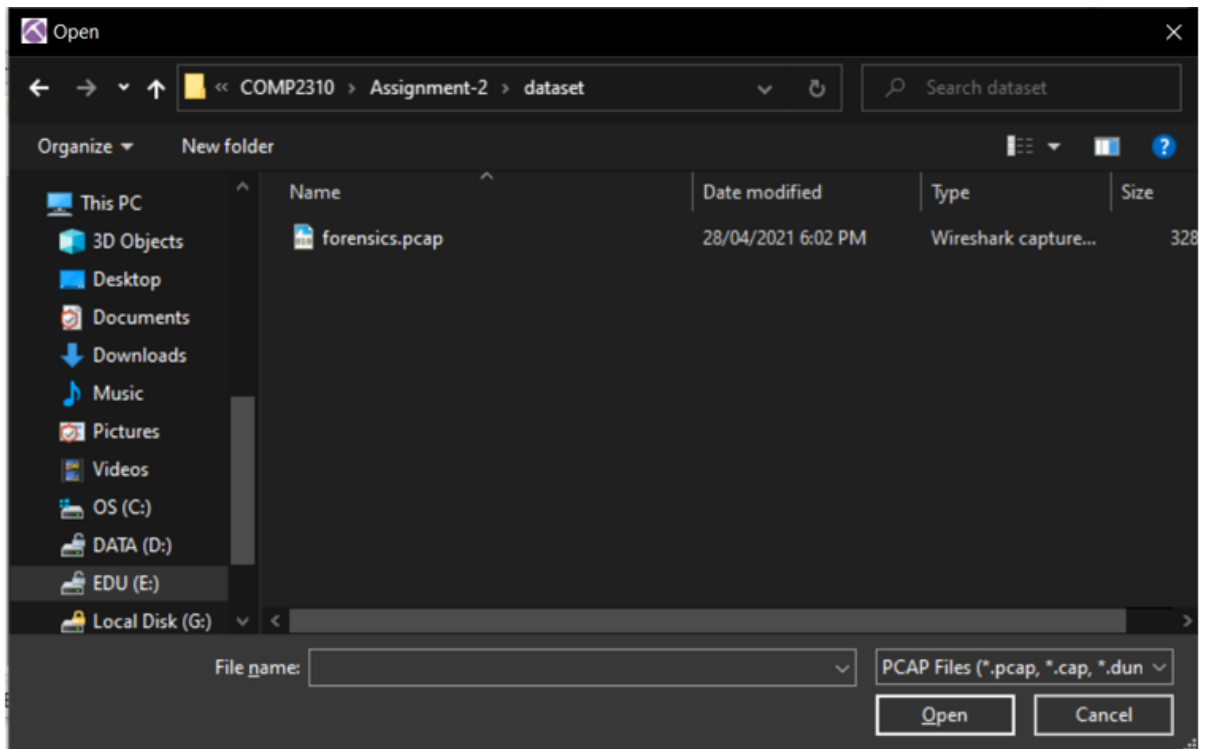
Snapshot 24 – NetworkMiner

3. Click on the File button on the Menu bar



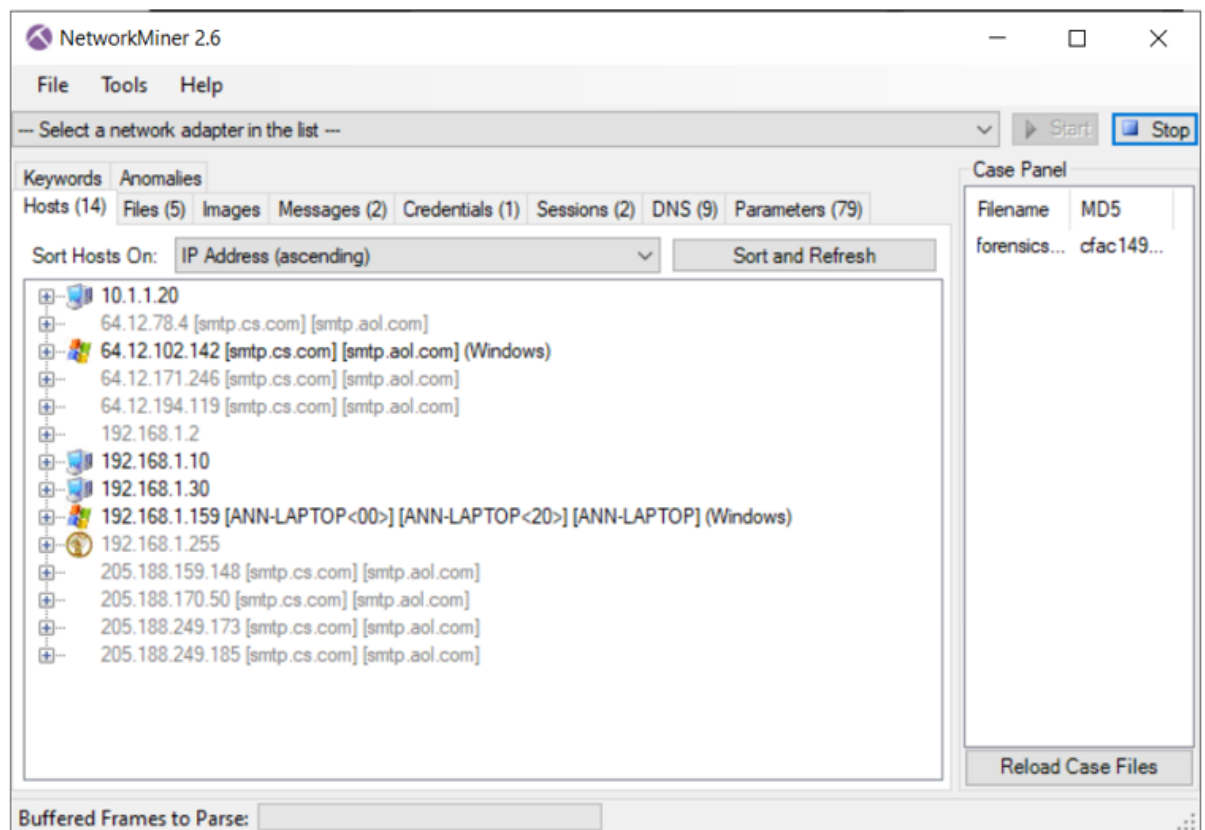
Snapshot 25 - NetworkMiner File Menu

4. Click on the Open button in the File menu and locate to the directory where the pcap file is stored



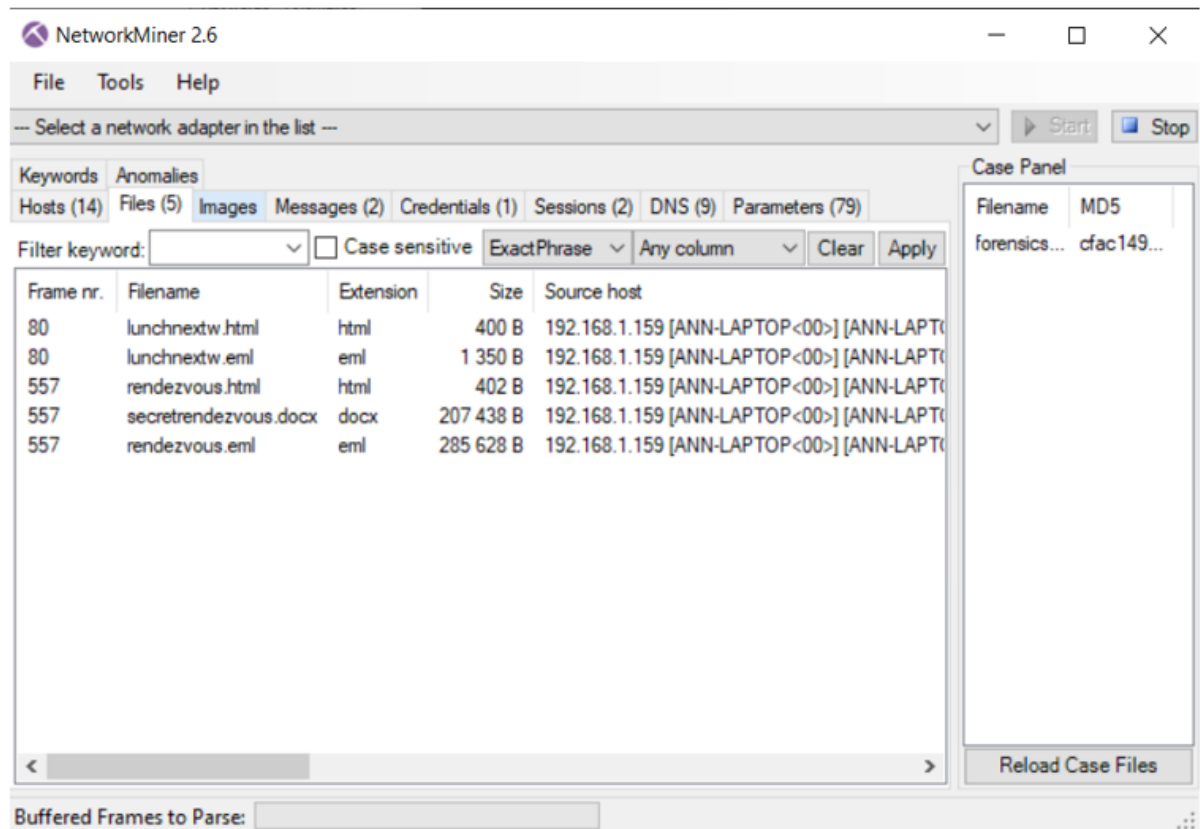
Snapshot 26 - Locating the file with open function

5. Select the file and click on the open button



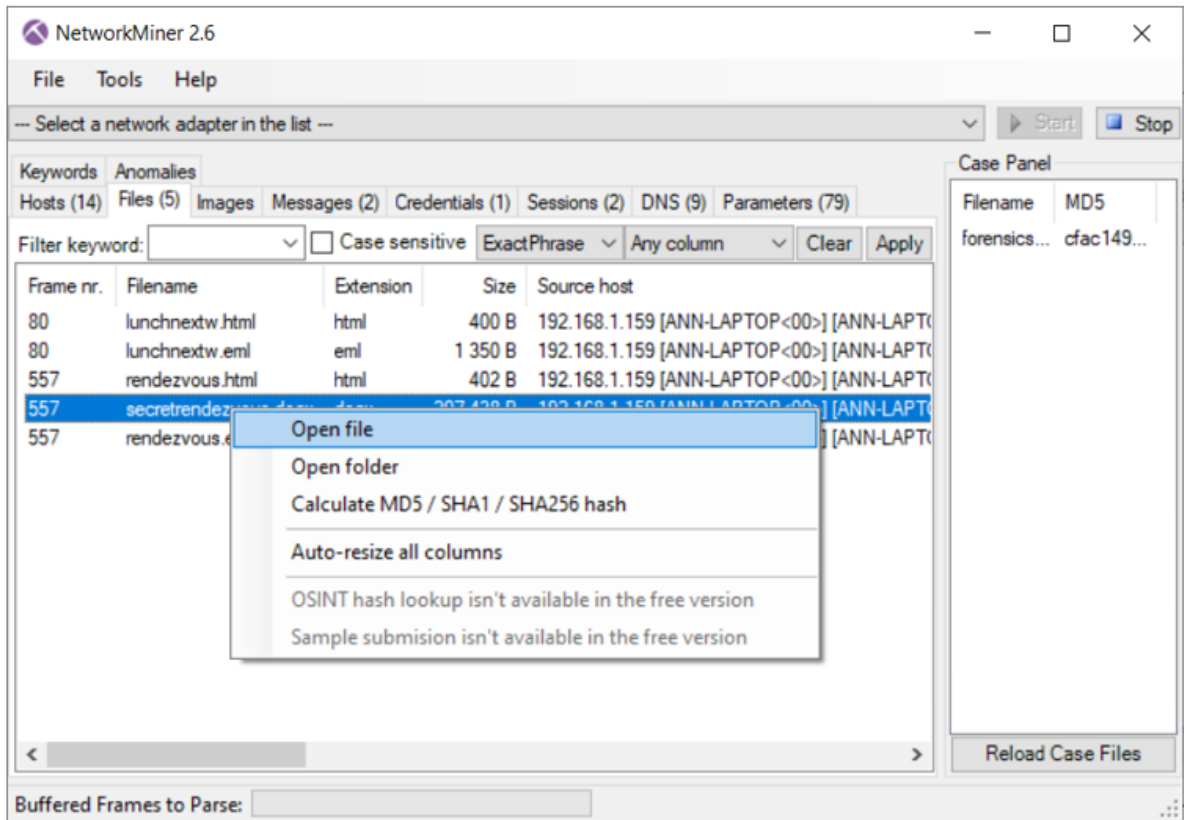
Snapshot 27 - Opened the file with NetworkMiner

- Click on the Files tab in NetworkMiner



Snapshot 28 - Files tab

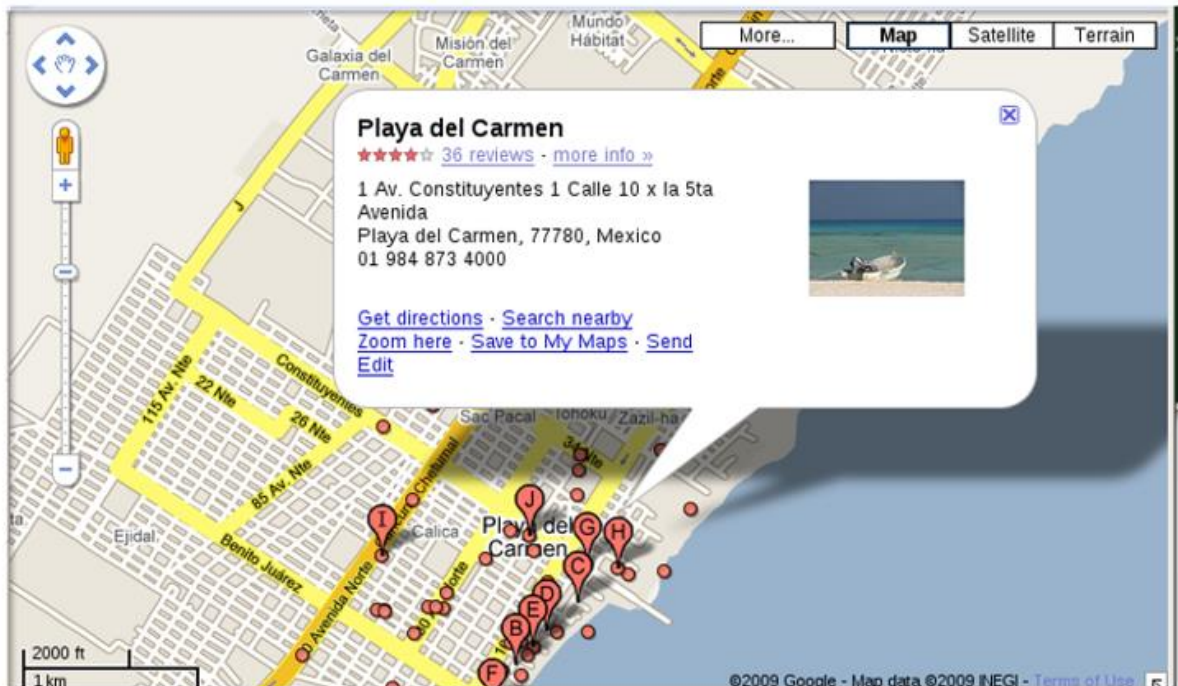
- Right-click on the secretrendezvous.docx file and click on the Open file button



Snapshot 29 - Opening secretrendezvous.docx file

8. The file is opened in Microsoft Word

Meet me at the fountain near the rendezvous point. Address below. I'm bringing all the cash.



Snapshot 30 - Content of secretrendezvous.docx file

App Forensics

Q7. What is the Phone Model and network carrier name (carrierName) on which MobInCube was run?

Answer:

The mobile phone is Samsung Galaxy A7.

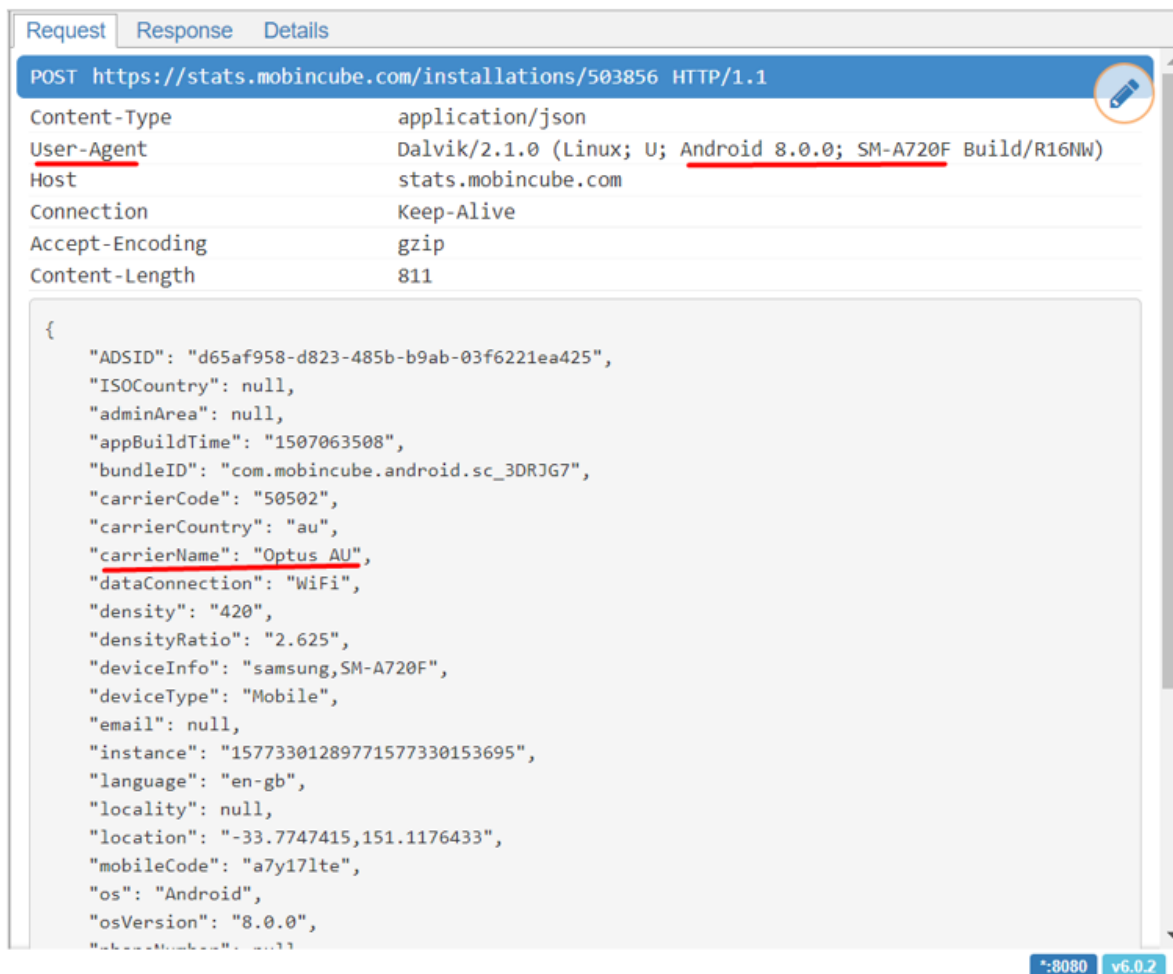
Phone Model: SM-A720F

Carrier Name: Optus AU

Analysis:

After opening the network traffic file with the mitmproxy ui application, I found all the files that were either requested or sent from the app on the mobile to the server. After going through all the files, I found that the mobile phone model is SM-A720F. But the network carrier details are only available in the POST request file. The request must be POST to send any information to the server, and finding the carrier name with the POST request made sense. The network carrier is Optus AU.

Evidence:



Request Response Details

POST https://stats.mobincube.com/installations/503856 HTTP/1.1

Content-Type	application/json
User-Agent	Dalvik/2.1.0 (Linux; U; <u>Android 8.0.0</u> ; <u>SM-A720F</u> Build/R16NW)
Host	stats.mobincube.com
Connection	Keep-Alive
Accept-Encoding	gzip
Content-Length	811

```
{
  "ADSID": "d65af958-d823-485b-b9ab-03f6221ea425",
  "ISOCountry": null,
  "adminArea": null,
  "appBuildTime": "1507063508",
  "bundleID": "com.mobincube.android.sc_3DRJG7",
  "carrierCode": "50502",
  "carrierCountry": "au",
  "carrierName": "Optus AU",
  "dataConnection": "WiFi",
  "density": "420",
  "densityRatio": "2.625",
  "deviceInfo": "samsung,SM-A720F",
  "deviceType": "Mobile",
  "email": null,
  "instance": "15773301289771577330153695",
  "language": "en-gb",
  "locality": null,
  "location": "-33.7747415,151.1176433",
  "mobileCode": "a7y17lte",
  "os": "Android",
  "osVersion": "8.0.0",
  "..."
}
```

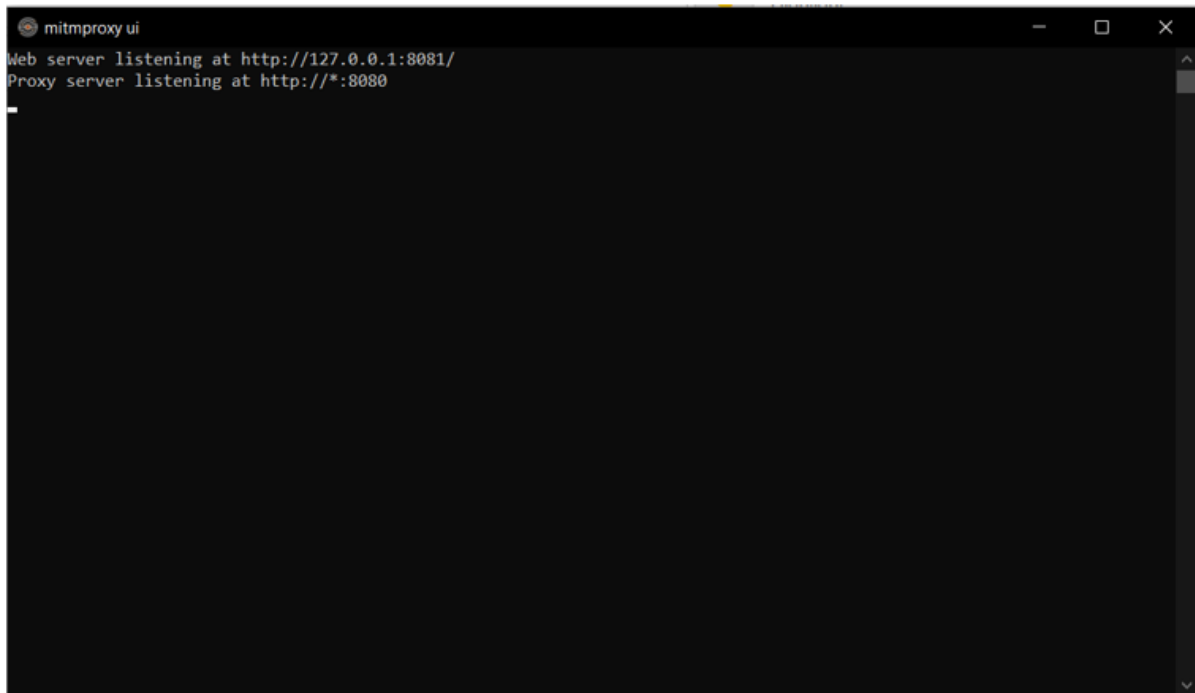
~:8080 v6.0.2

Snapshot 31 - Mobile Phone details

From Snapshot-31, we know that the mobile phone model is SM-A720F, and the network carrier name is Optus AU.

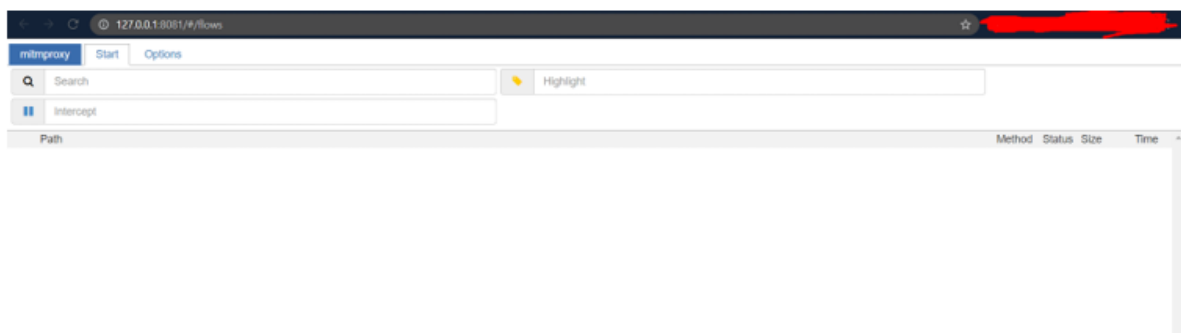
Steps Taken:

1. Open mitmproxy ui application



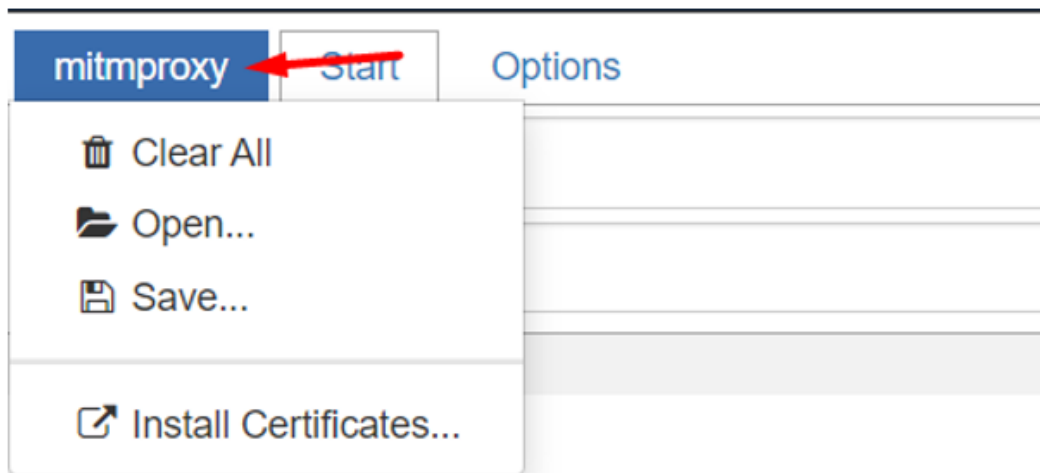
Snapshot 32 - mitmproxy ui terminal

The application will open in the default web browser



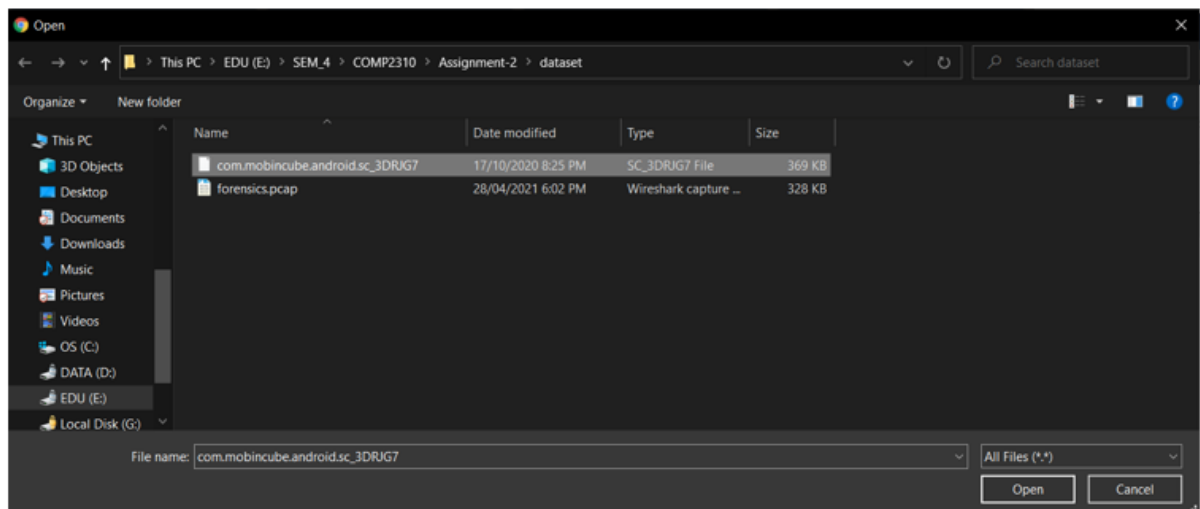
Snapshot 33 - mitmproxy ui application

2. Click in mitmproxy button from the menu bar



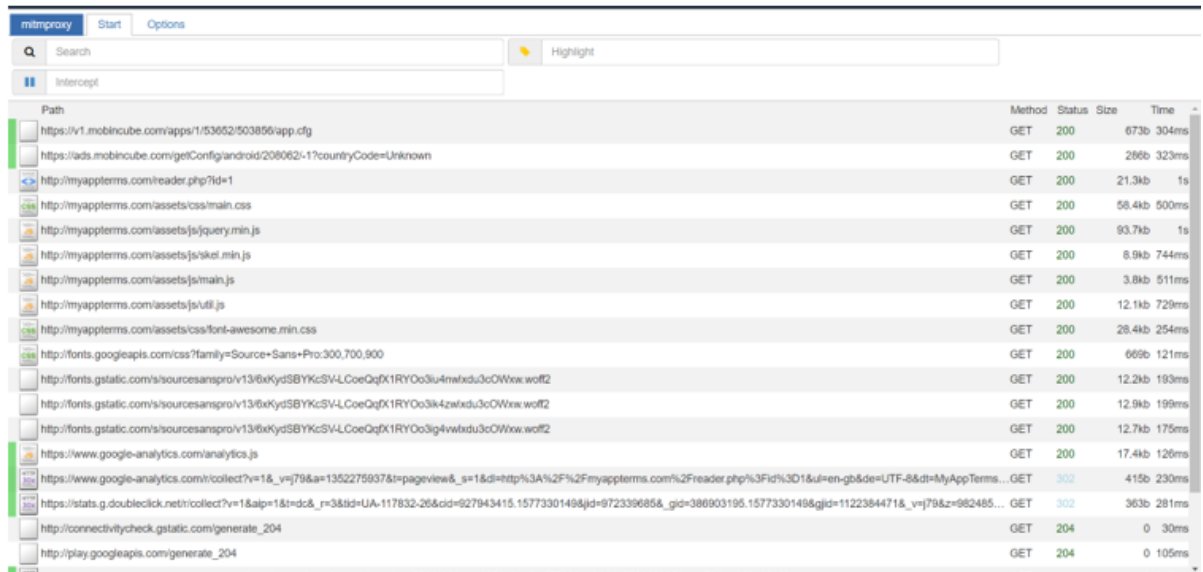
Snapshot 34 - mitmproxy button from the menu bar

3. Click on the Open... button from the drop-down and locate the file that requires analysis.



Snapshot 35 - Finding input file for mitmproxy

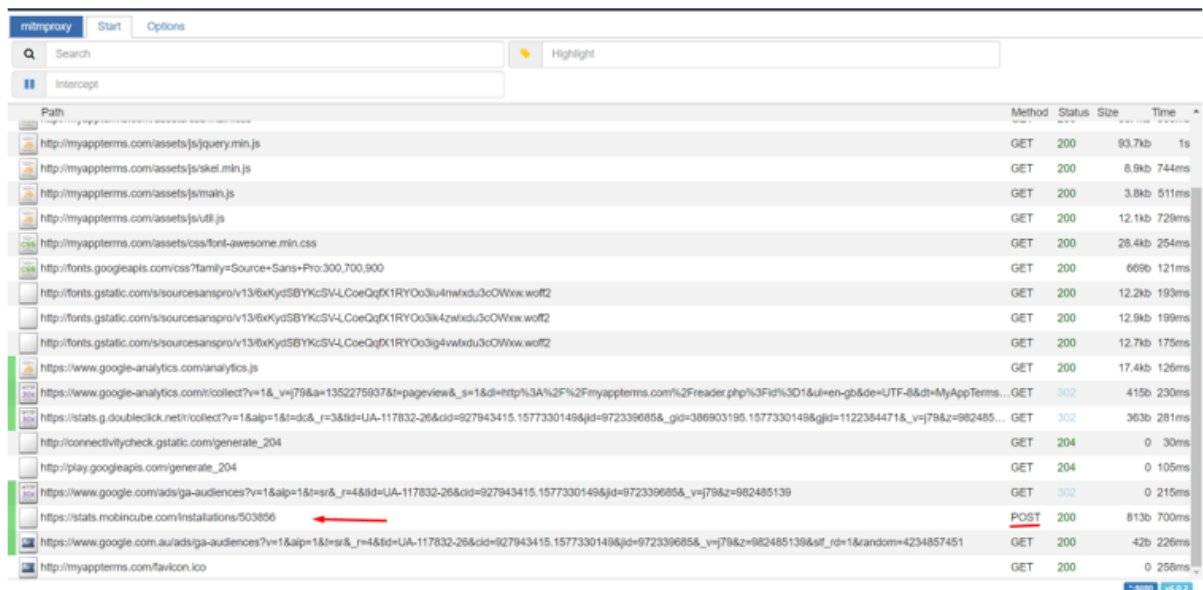
4. Select the file and click on the Open button



Path	Method	Status	Size	Time
https://v1.mobincube.com/apps/1/53652/503856/app.dfg	GET	200	673b	304ms
https://ads.mobincube.com/getConfig/android/208062-1?countryCode=Unknown	GET	200	286b	323ms
http://myappterm.com/reader.php?id=1	GET	200	21.3kb	1s
http://myappterm.com/assets/css/main.css	GET	200	58.4kb	500ms
http://myappterm.com/assets/js/jquery.min.js	GET	200	93.7kb	1s
http://myappterm.com/assets/js/sket.min.js	GET	200	8.9kb	744ms
http://myappterm.com/assets/js/main.js	GET	200	3.8kb	511ms
http://myappterm.com/assets/js/ui.js	GET	200	12.1kb	729ms
http://myappterm.com/assets/css/font-awesome.min.css	GET	200	28.4kb	254ms
http://fonts.googleapis.com/css?family=Source+Sans+Pro:300,700,900	GET	200	669b	121ms
http://fonts.gstatic.com/s/sourcesanspro/v13/6xKydSBYKcSV-LCoeQqX1RYOo3u4nafxdu3cOWw.woff2	GET	200	12.2kb	193ms
http://fonts.gstatic.com/s/sourcesanspro/v13/6xKydSBYKcSV-LCoeQqX1RYOo3k4zafxdu3cOWw.woff2	GET	200	12.9kb	199ms
http://fonts.gstatic.com/s/sourcesanspro/v13/6xKydSBYKcSV-LCoeQqX1RYOo3ig4wafxdu3cOWw.woff2	GET	200	12.7kb	175ms
https://www.google-analytics.com/analytics.js	GET	200	17.4kb	126ms
https://www.google-analytics.com/collected?v=1&_v=j79&a=1352275937&+pageview&_s=1&di=http%3A%2F%2Fmyappterm.com%2Freader.php%3Fid%3D1&ul=en-gb&de=UTF-8&dt=MyAppTerms...	GET	302	415b	230ms
https://stats.g.doubleclick.net/collected?v=1&ai=1&dc&_r=3&id=UA-117832-26&cid=927943415.1577330149&gid=9723396858_gid=386903195.1577330149&gjid=1122384471&_v=j79&z=982485...	GET	302	363b	281ms
http://connectivitycheck.gstatic.com/generate_204	GET	204	0	30ms
http://play.googleapis.com/generate_204	GET	204	0	105ms

Snapshot 36 - mitmproxy ui application with input data

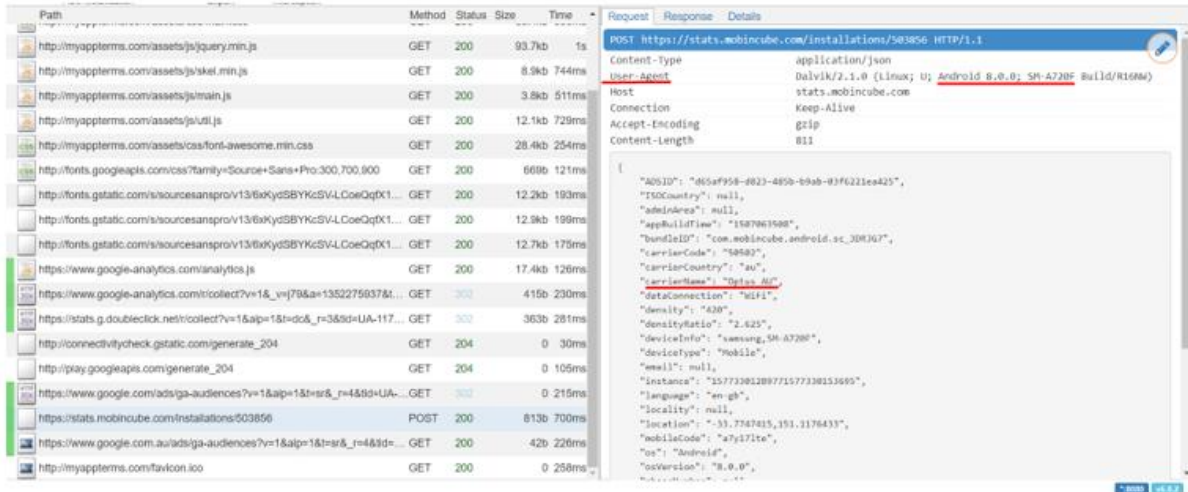
5. Locate the exchange that uses the POST method



Path	Method	Status	Size	Time
http://myappterm.com/assets/js/jquery.min.js	GET	200	93.7kb	1s
http://myappterm.com/assets/js/sket.min.js	GET	200	8.9kb	744ms
http://myappterm.com/assets/js/main.js	GET	200	3.8kb	511ms
http://myappterm.com/assets/js/ui.js	GET	200	12.1kb	729ms
http://myappterm.com/assets/css/font-awesome.min.css	GET	200	28.4kb	254ms
http://fonts.googleapis.com/css?family=Source+Sans+Pro:300,700,900	GET	200	669b	121ms
http://fonts.gstatic.com/s/sourcesanspro/v13/6xKydSBYKcSV-LCoeQqX1RYOo3u4nafxdu3cOWw.woff2	GET	200	12.2kb	193ms
http://fonts.gstatic.com/s/sourcesanspro/v13/6xKydSBYKcSV-LCoeQqX1RYOo3k4zafxdu3cOWw.woff2	GET	200	12.9kb	199ms
http://fonts.gstatic.com/s/sourcesanspro/v13/6xKydSBYKcSV-LCoeQqX1RYOo3ig4wafxdu3cOWw.woff2	GET	200	12.7kb	175ms
https://www.google-analytics.com/analytics.js	GET	200	17.4kb	126ms
https://www.google-analytics.com/collected?v=1&_v=j79&a=1352275937&+pageview&_s=1&di=http%3A%2F%2Fmyappterm.com%2Freader.php%3Fid%3D1&ul=en-gb&de=UTF-8&dt=MyAppTerms...	GET	302	415b	230ms
https://stats.g.doubleclick.net/collected?v=1&ai=1&dc&_r=3&id=UA-117832-26&cid=927943415.1577330149&gid=9723396858_gid=386903195.1577330149&gjid=1122384471&_v=j79&z=982485...	GET	302	363b	281ms
http://connectivitycheck.gstatic.com/generate_204	GET	204	0	30ms
http://play.googleapis.com/generate_204	GET	204	0	105ms
https://stats.mobincube.com/installations/503856	POST	200	813b	700ms
https://www.google.com/ads/ga-audiences?v=1&ai=1&dc&_r=4&id=UA-117832-26&cid=927943415.1577330149&gid=9723396858_v=j79&z=982485139&at_id=1&random=4234857451	GET	200	42b	226ms
http://myappterm.com/favicon.ico	GET	200	0	258ms

Snapshot 37 - Locating the file

6. Click on the exchange to see its details



Snapshot 38 - Details of the Mobile Phone

Q8. What is the location (latitude and longitude) value shared with <https://stats.mobincube.com/>?

Answer:

The location value that is shared with https://stats.mobincube.com is “-33.7747415, 151.1176433”.

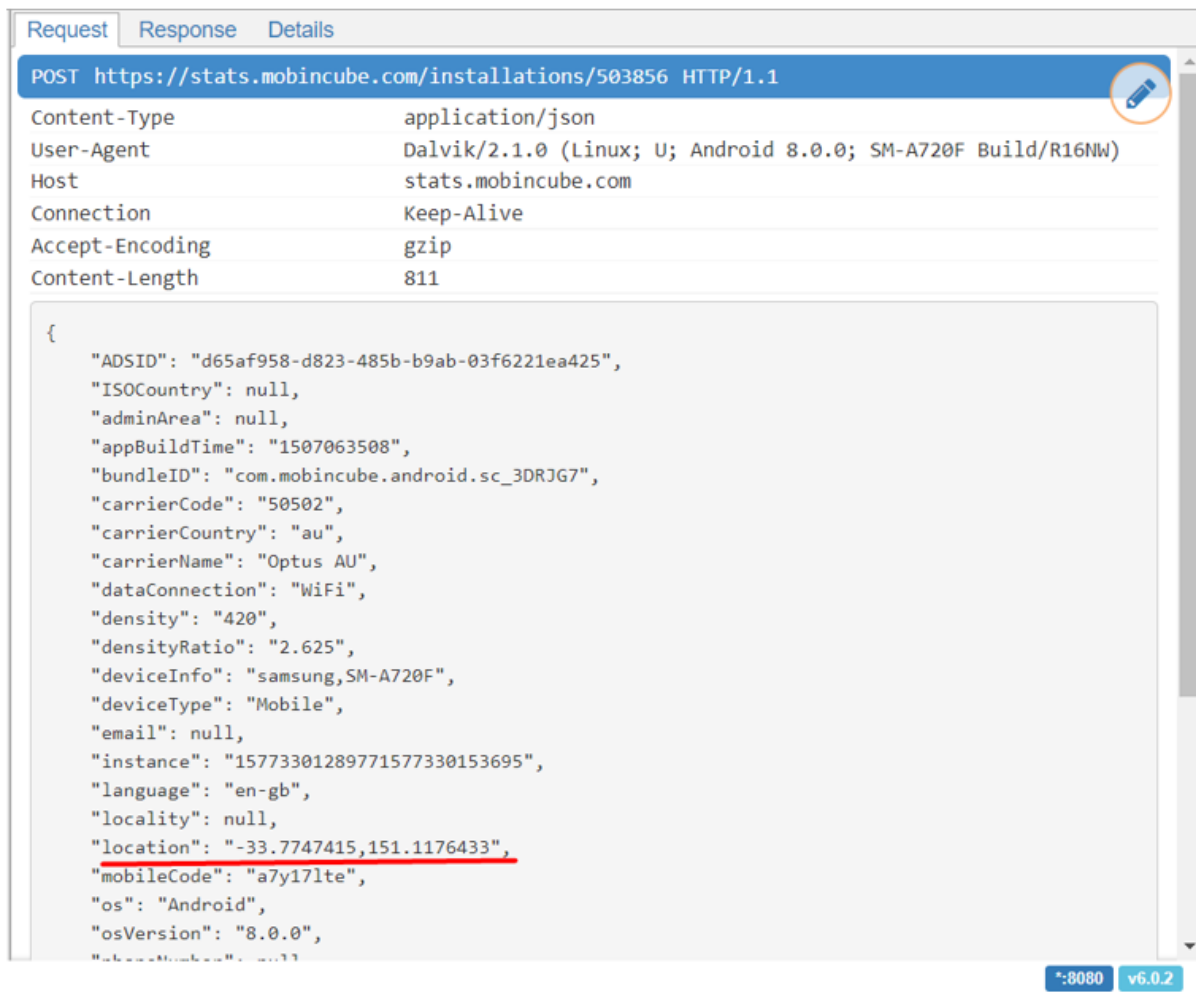
These latitude and longitude values are BD, 4 Research Park Dr, Macquarie Park NSW 2113, Australia.

Analysis:

The location can be found from the details from the

<https://stats.mobincube.com/installations/503856> exchange. The location value is found to be 33.7747415, 151.1176433.

Evidence:



Request Response Details

POST https://stats.mobincube.com/installations/503856 HTTP/1.1

Content-Type	application/json
User-Agent	Dalvik/2.1.0 (Linux; U; Android 8.0.0; SM-A720F Build/R16NW)
Host	stats.mobincube.com
Connection	Keep-Alive
Accept-Encoding	gzip
Content-Length	811

```
{
  "ADSID": "d65af958-d823-485b-b9ab-03f6221ea425",
  "ISOCountry": null,
  "adminArea": null,
  "appBuildTime": "1507063508",
  "bundleID": "com.mobincube.android.sc_3DRJG7",
  "carrierCode": "50502",
  "carrierCountry": "au",
  "carrierName": "Optus AU",
  "dataConnection": "WiFi",
  "density": "420",
  "densityRatio": "2.625",
  "deviceInfo": "samsung,SM-A720F",
  "deviceType": "Mobile",
  "email": null,
  "instance": "15773301289771577330153695",
  "language": "en-gb",
  "locality": null,
  "location": "-33.7747415,151.1176433",
  "mobileCode": "a7y17lte",
  "os": "Android",
  "osVersion": "8.0.0",
  "platform": "android"
}
```

8080 v6.0.2

Snapshot 39 - Location of the Mobile Phone

From Snapshot-39, we know that the location of the Mobile phone is 33.7747415, 151.1176433.

Steps Taken:

- Same as Q7

Q9. Visit the privacy policy of MobInCube

(<http://myappterms.com/reader.php?lang=en>), and report whether or not the app is transparent about the information they collect?

Answer:

Yes, the app is transparent about the information it collects.

Analysis:

I used a web browser to visit the app's privacy policy web page. After reading the web page, I came to the conclusion that the app is transparent about the information it collects.

Evidence:

Please refer to the website (<http://myapptterms.com/reader.php?lang=en>) for evidence.

From the first section, we can understand that the app neither collects any information with malicious purposes nor collects information such as name, email, phone number, etc., unless the user enters intentionally. We can understand that only non-personal information is collected automatically and what data is considered personal from the second section. We can understand that no information is collected from the children under 13 years from the third section. Sections four and five give us information regarding how MobInCube collects the data and how is it used. Section twelve states that the app was not developed to access phone numbers for the users' privacy. All the sections in the website clearly state how MobInCube collects and shares the data and the involvement of any third parties.

Steps Taken:

1. Visit <http://myapptterms.com/reader.php?lang=en> on a web browser

PRIVACY POLICY

Version 3.0 | May 5th, 2021

WHAT DOES THIS DOCUMENT CONTAIN?

For the proper functioning of this app, it is necessary to collect and process certain information obtained from the device where it has been installed. This information enables us to improve the app, to optimally tailor the content to each user, or to contact the user if necessary. In order to make our concern for our users' privacy clear, we have adopted this Privacy Policy which explains in a simple and comprehensible language the manner in which we collect, store, use and disclose the information users entrust us with.

These Privacy Policies attempt to cover the widest possible range of scenarios, including many cases in which the app does not even collect nor process the information described within these Privacy Policies.

1. WHAT INFORMATION DOES THE APP COLLECT?

Snapshot 40 - MobInCube Privacy Policy Webpage

2. Read the information present on the webpage

Q10. What are your recommendations on the security and privacy options of the app?
Would you recommend this app to a user? Why or why not?

Answer:

My recommendations to the security and privacy options of the app are:

1. Build their libraries such that there is no need to share the data with the third parties

2. It is better to send a mail to users stating that there are changes made to the privacy policy
3. Make a one-click button to stop targeted advertising instead of going to a website and following a process.
4. Do not collect location information

I will recommend this app to other users. Most of the apps available on the play store/App Store have similar privacy policies. Some of the apps are not transparent regarding the data they collect and how they use it. In my opinion, this app is safe to use. The privacy policy of the MobInCube app also stated that if any third party misused the user information shared with them, the app would withdraw their relation. Users can also block this app from accessing the location of the phone. This app feels safe to use, and I recommend this app to others.

Conclusion

After analysing the captured packets from my friend, I learned that my friend's neighbour's name is Ann Dercover, and his/her/their email address is sneakyg33k@aol.com. The password of Ann Dercover's email address is 558r00lz. Ann Dercover sent emails to two other correspondents. One is to sec558@gmail.com regarding lunch they had planned for next week, and another is to mistersecretx@aol.com regarding rendezvous. In the email to sec558@gmail.com, Ann Dercover wrote that he/she/they would not be available for the lunch they planned as Ann is going out of town. In the email sent to mistersecretx@aol.com, Ann Dercover asked the correspondent to meet her near a fountain located at the address attached to the email. Ann Dercover also asked the correspondent to bring a fake passport and a bathing suit. Ann Dercover is most likely gone on a vacation with mistersecretx@aol.com. The name of the email attachment that is containing the location information is `secretrendezvous.docx`. The `secretrendezvous.docx` file tells us that the location is Playa del Carmen, Mexico. From the file, we also know that Ann Dercover is bringing all her cash. After analysing the network traffic from the MobInCube app to the server, I learnt that the mobile phone model is SM-A720F, and the network carrier is Optus AU. I also learnt that the location from where the app was used is BD, 4 Research Park Dr, Macquarie Park NSW 2113, Australia. The latitude and longitude coordinates are -33.7747415, 151.1176433. It looked like the MobInCube app is transparent about the information they collect. I also recommend this app to other users. The app is safe to use and has similar security and privacy features to other apps in the market. Users can also block the app from accessing the mobile location.

Glossary

- Wireshark 3.4.4 – Wireshark
- NetworkMiner 2.6 – NetworkMiner

- mitmproxy ui 6.0.2 – mitmproxy ui

Appendix

- SMTP -Secure Mail Transfer Protocol
- PCAP – Packet Capture

References

[1]"Mobincube the best APP BUILDER DIY for Android iPhone/iPAD", Mobincube. [Online]. Available: <https://mobincube.com/>. [Accessed: 01- Jun- 2021].