

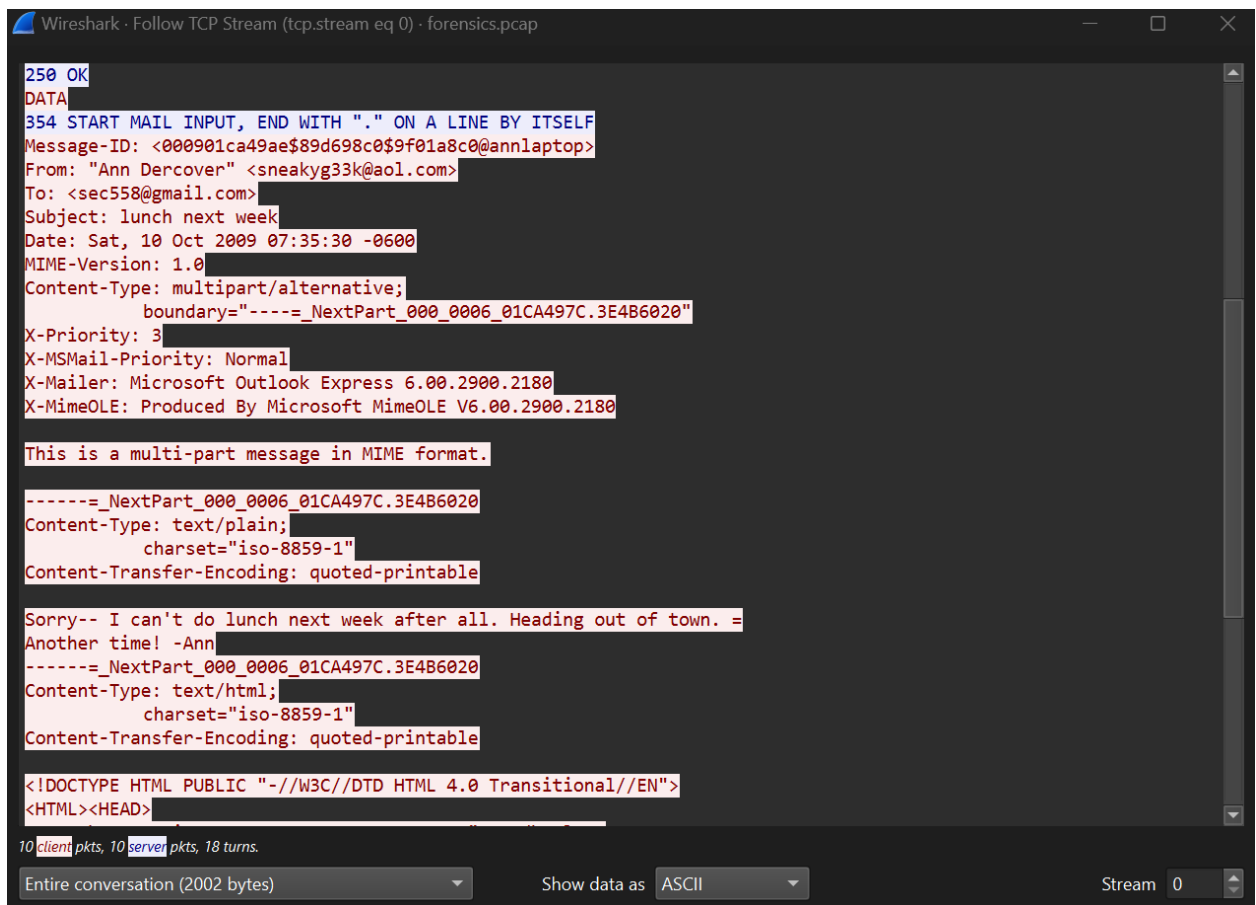
## Lab 3

Narendra Gautam Sontu – 002241534

Git: [https://github.com/gautamsontu/Network\\_Security/tree/main/Lab\\_3](https://github.com/gautamsontu/Network_Security/tree/main/Lab_3)

### Forensics

1. **Neighbour's Name:** Appears in the "From" field of the email i.e. "Ann Dercover."
2. **Neighbour's Email Address:** The email address is "[sneakyg33k@aol.com](mailto:sneakyg33k@aol.com)."



Wireshark · Follow TCP Stream (tcp.stream eq 0) · forensics.pcap

```
250 OK
DATA
354 START MAIL INPUT, END WITH "." ON A LINE BY ITSELF
Message-ID: <000901ca49ae$89d698c0$9f01a8c0@annlaptop>
From: "Ann Dercover" <sneakyg33k@aol.com>
To: <sec558@gmail.com>
Subject: lunch next week
Date: Sat, 10 Oct 2009 07:35:30 -0600
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="-----_NextPart_000_0006_01CA497C.3E4B6020"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.2180
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180

This is a multi-part message in MIME format.

-----_NextPart_000_0006_01CA497C.3E4B6020
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

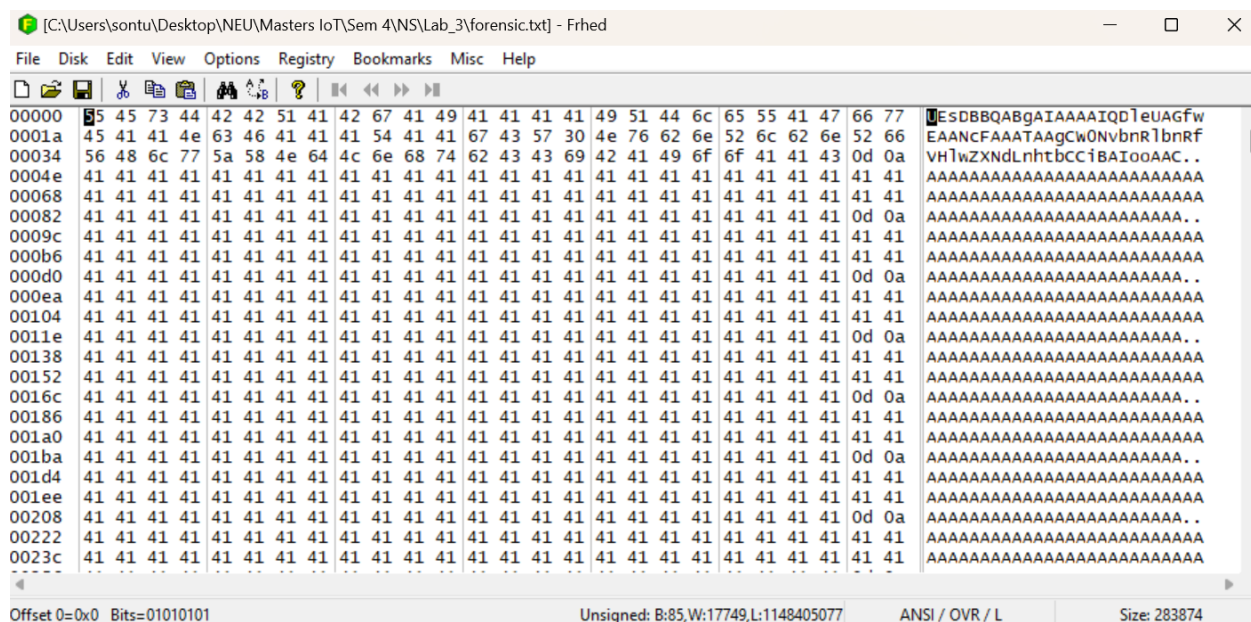
Sorry-- I can't do lunch next week after all. Heading out of town. =
Another time! -Ann
-----_NextPart_000_0006_01CA497C.3E4B6020
Content-Type: text/html;
        charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
```

10 client pkts, 10 server pkts, 18 turns.

Entire conversation (2002 bytes) Show data as ASCII Stream 0

3. **Neighbour's Email Password:** The password for the email is "558r00lz."
4. The email addresses (at least two) of the neighbour's correspondents are,
  - **Correspondent's Email Addresses:** [mistersecretx@aol.com](mailto:mistersecretx@aol.com), [sec558@gmail.com](mailto:sec558@gmail.com)
  - **Email of the Correspondent Most Likely to Visit:** [mistersecretx@aol.com](mailto:mistersecretx@aol.com)
5. The name of the file containing the meeting location **secretrendezvous.docx**
6. To check where they are meeting,



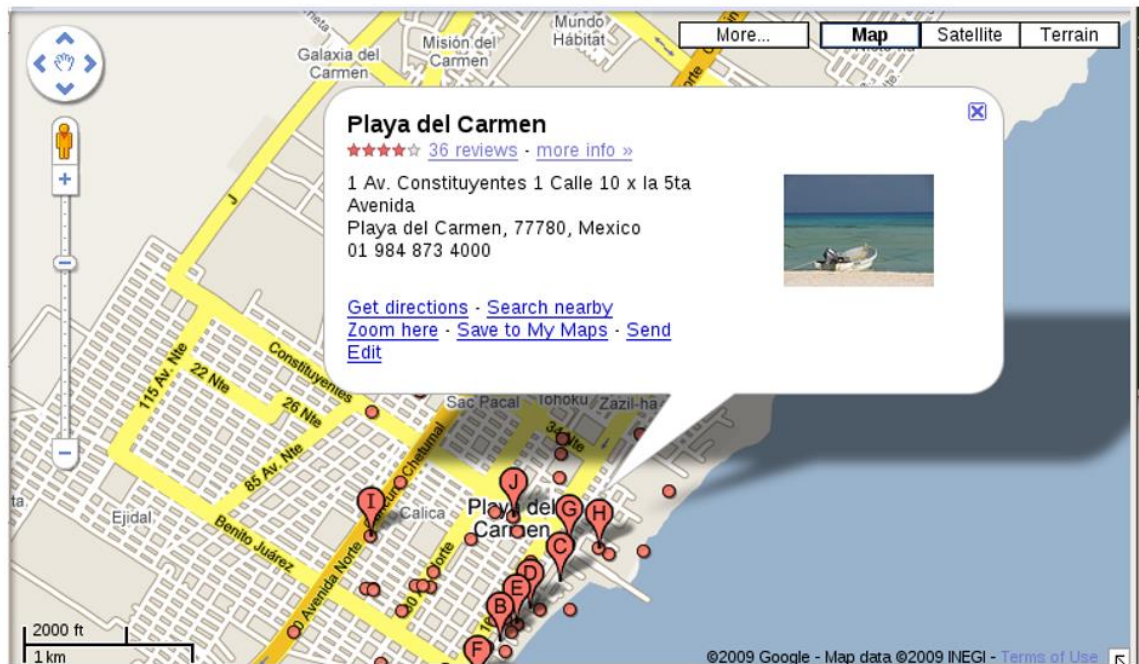
I have decoded the text using a python script,

```
import base64
with open("forensic.txt", "r") as file:
    base64_encoded_str = file.read()
    base64_encoded_str = base64_encoded_str.replace("\n", "")

    decoded_bytes = base64.b64decode(base64_encoded_str)

    with open("decoded.docx", "wb") as file:
        file.write(decoded_bytes)
```

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



In the email, the correspondent is asking to get a **fake passport and a bathing suit**. They are meeting at **'Playa del Carmen' in Mexico**.

## Evidence

1. Name of Ann's IM buddy: **Sec558user1**
2. Comments in the captured IM conversation:

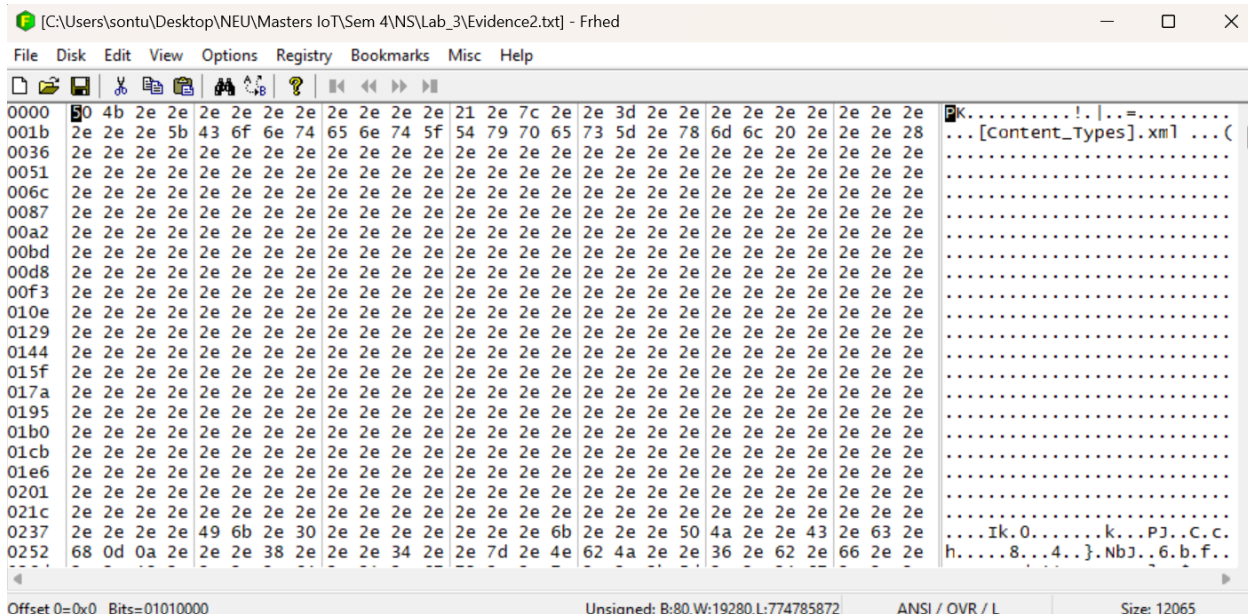
Wireshark · Follow TCP Stream (tcp.stream eq 2) · evidence01.pcap

```
*..`.*.a.....E4628778...Sec558user1.....Here's the secret recipe... I just downloaded it f
rom the file server. Just copy to a thumb drive and you're good to go &gt;:-)....*.b.".....F.....Sec558
user1..*.V.....
...*.A.....E.....P.....p...p.....P.....p...p.&.'.....
...|.....U4.....|.....h.....p...@.&.'.....
...|.....h.....p...@.&.'*.V.....E4628778...Sec558user1*..c.z.....G7174647...Sec558user1.....R.
.7174647. F.CL..."DEST.....F.
.....'.....recipe.docx.*.V.....
...*.c.....G.....P.....p...p...w.....P.....p...p.&a.....
...|.....h.....p...@.&a.....*.V.....G7174647...Sec558user1*.V..{.....*.7174647...Sec558user1...
.....J.H.....+.1n...+.O.....J.....7174647. F.CL..."DEST.....*.V..".....*.1.....
Sec558user1..*.V.....*.y..N...w...Sec558user1.....J.H.....+.1n...+.O.....J.....a...
.....X....<HTML><BODY><FONT FACE="Arial" SIZE=2 COLOR=#000000>thanks dude</FONT></BODY></HTML>.
.....+.1n...+.O.....*.V..".....*.V.....+ Q.....L.....Sec558user1..
.....J.H.....+.1n...+.O.....J.....s.....j....<HTML><BODY><FONT FACE="Arial" SIZE=2 COLOR
=#000000>can't wait to sell it on ebay</FONT></BODY></HTML>.
.....+.1n...+.O.....*.V..".....+
.....Sec558user1..*.V..".....Sec558user1..*.d.".....H.....Sec558user1..*.e.J...
.....I5088496...Sec558user1...".....see you in hawaii!....*.f.".....J.....Sec558user1..*.V
.....
...+ @.....I.....P.....p...p...a.....P.....p...p.&.....
.....V~.....|.....h.....p...@.&.....
...|.....h.....p...@.&...*.V.....I5088496...Sec558user1
```

Packet 25. 7 client pkts, 13 server pkts, 5 turns. Click to select.

Entire conversation (2023 bytes) Show data as ASCII Stream 2

- "Here's the secret recipe... I just downloaded it from the file server. Just copy to a thumb drive and you're good to go >:-)"
  - "thanks dude"
  - "can't wait to sell it on ebay"
  - "see you in hawaii!"
3. Name of the file Ann transferred: **recipe.docx**
4. The **magic number** of the file (first four bytes): **50 4B 03 04** (highlighted in the image)



Instead of ASCII, I have shown data as Raw and copied this Raw data to a file named 'EviRaw'. I have converted EviRaw to a word document called recipe.docx using a simple python script.

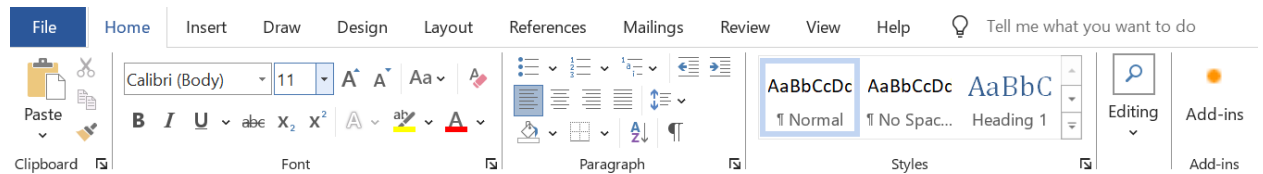
```
with open('EviRaw.txt', 'r') as file:
    hex_string = file.read()

hex_string = ''.join(hex_string.split())
binary_data = bytes.fromhex(hex_string)

with open('recipe_converted.docx', 'wb') as binary_file:
    binary_file.write(binary_data)

print("Conversion complete.")
```

## 5. What is the secret recipe:



### Recipe for Disaster:

*1 serving*

Ingredients:

4 cups sugar

2 cups water

In a medium saucepan, bring the water to a boil. Add sugar. Stir gently over low heat until sugar is fully dissolved. Remove the saucepan from heat. Allow to cool completely. Pour into gas tank. Repeat as necessary.