Lab 7 – Packet Capture Analysis

Shrutika Joshi

University of Maryland Baltimore County

Presented To – Gina Marie

Date – 21st July 2023

Introduction – In this lab, we need to perform packet analysis to check whether a malicious system was on the network. There is a scenario where user Ann disappears. Since investigators were monitoring her network activity they found that she may have communicated with her secret lover, Mr. X, before she left. The packet capture may contain clues to her location and other details. Hence, we need to analyze the network traffic details of Ann's system and check if any communication details are there. Also, have to carve files from the packet to understand network activity and Ann's location details.

Pre-Lab – For this, we have given a Pcap file **"**Evidence-packet-analysis.pcap" of Ann's network activity. I am using a Windows machine and using Wireshark and Network Miner to perform packet analysis using wireshark commands.

Analysis –

1. **Packet Capture Analysis -** As a forensic investigator, analyze the pcap file "Evidence-packet-analysis.pcap", located in the Evidence Drive, under "Packet Analysis". Further, analyze the packet capture and gather information about Ann's activities and plans. For that open the pcap file in Wireshark.

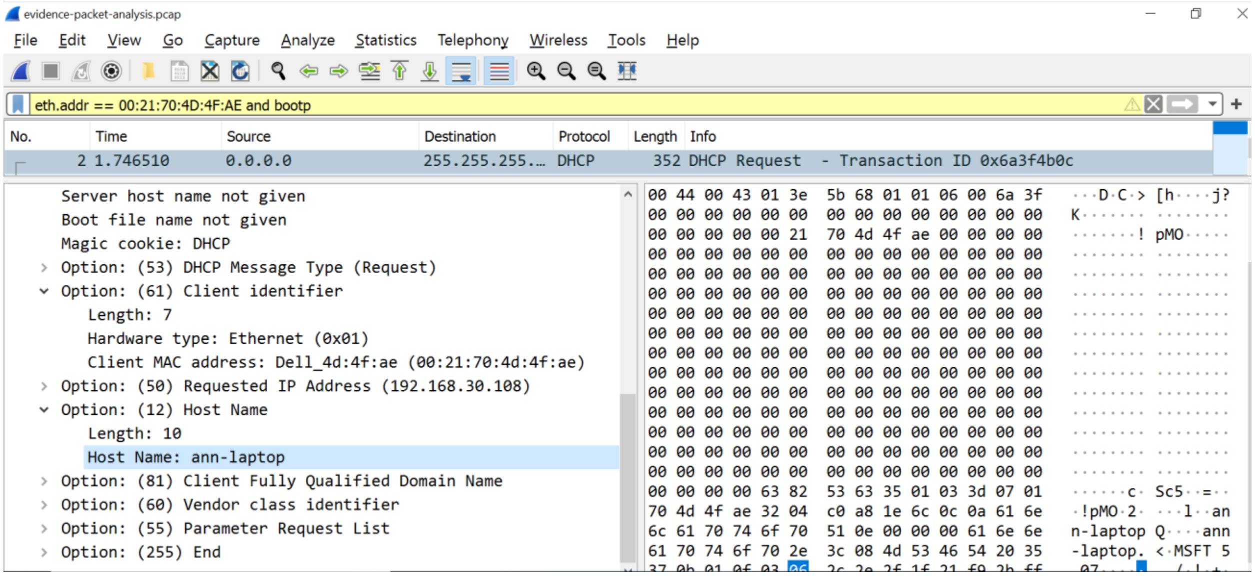
I am using the Wireshark command (eth.addr == 00:21:70:4D:4F:AE and bootp) to filter DHCP packets so that we can extract the IP address assigned to Ann's device and device name.

- BOOTP stands for Bootstrap Protocol, which is used for assigning IP addresses and subnet masks manually. Data of DHCP and BOOTP is transferred over port 67 and port 68.

  From the below packet we can see –

  IP address assigned to Ann’s Device: 192.168.30.108

  Device Name: ann-laptop


evidence-packet-analysis.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
eth.addr == 00:21:70:4D:4F:AE and bootp
```

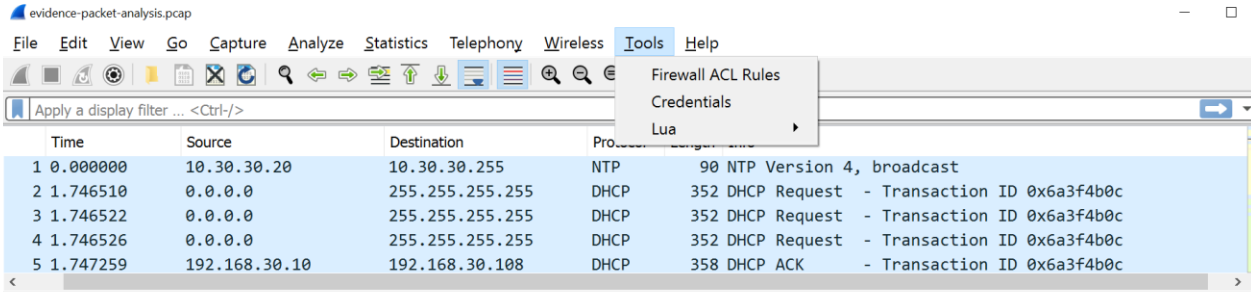
```
No.   Time       Source    Destination    Protocol  Length  Info
    2 1.746510   0.0.0.0   255.255.255.…  DHCP         352  DHCP Request  - Transaction ID 0x6a3f4b0c
```

```
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Request)
  ˅ Option: (61) Client identifier
       Length: 7
       Hardware type: Ethernet (0x01)
       Client MAC address: Dell_4d:4f:ae (00:21:70:4d:4f:ae)
  > Option: (50) Requested IP Address (192.168.30.108)
  ˅ Option: (12) Host Name
       Length: 10
       Host Name: ann-laptop
  > Option: (81) Client Fully Qualified Domain Name
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
  > Option: (255) End
```

```
00 44 00 43 01 3e  5b 68 01 01 06 00 6a 3f   ···D·C·> [h····j?
00 00 00 00 00 00  00 00 00 00 00 00 00 00   K······· ········
00 00 00 00 00 21  70 4d 4f ae 00 00 00 00   ·······! pMO·····
00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00 00 00 00 63 82  53 63 35 01 03 3d 07 01   ······c· Sc5··=··
70 4d 4f ae 32 04  c0 a8 1e 6c 0c 0a 61 6e   ·!pMO·2· ···l··an
6c 61 70 74 6f 70  51 0e 00 00 00 61 6e 6e   n-laptop Q····ann
61 70 74 6f 70 2e  3c 08 4d 53 46 54 20 35   -laptop. <·MSFT 5
37 0b 01 0f 03 06  2c 2e 2f 1f 21 f9 2b ff   07······ ·/·!·+·
```

1. Provide any online aliases or addresses and corresponding account credentials that may be used by the suspect under investigation.

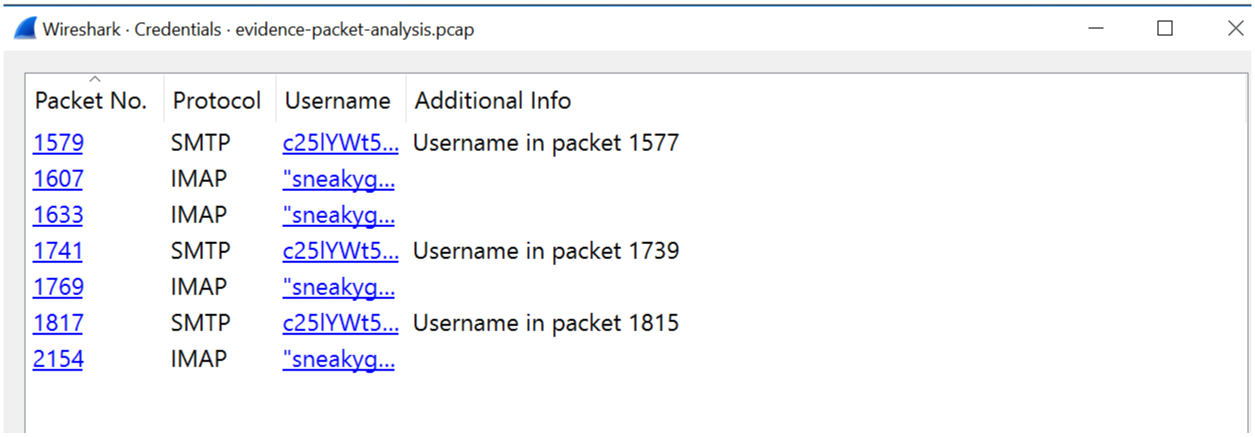
➢ To check credentials and aliases used by the suspect, first, click on the Tools tab provided in the Wireshark. Then click on Tools → Credentials. It will show a popup window having credential details, protocol, and frame number where credentials details contain. This functionality is available on the latest wireshark version.



evidence-packet-analysis.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Firewall ACL Rules
Credentials
Lua
Apply a display filter ... <Ctrl-/>

```
  Time        Source          Destination      Pro...
1 0.000000    10.30.30.20     10.30.30.255     NTP      90 NTP Version 4, broadcast
2 1.746510    0.0.0.0         255.255.255.255  DHCP    352 DHCP Request  - Transaction ID 0x6a3f4b0c
3 1.746522    0.0.0.0         255.255.255.255  DHCP    352 DHCP Request  - Transaction ID 0x6a3f4b0c
4 1.746526    0.0.0.0         255.255.255.255  DHCP    352 DHCP Request  - Transaction ID 0x6a3f4b0c
5 1.747259    192.168.30.10   192.168.30.108   DHCP    358 DHCP ACK      - Transaction ID 0x6a3f4b0c
```

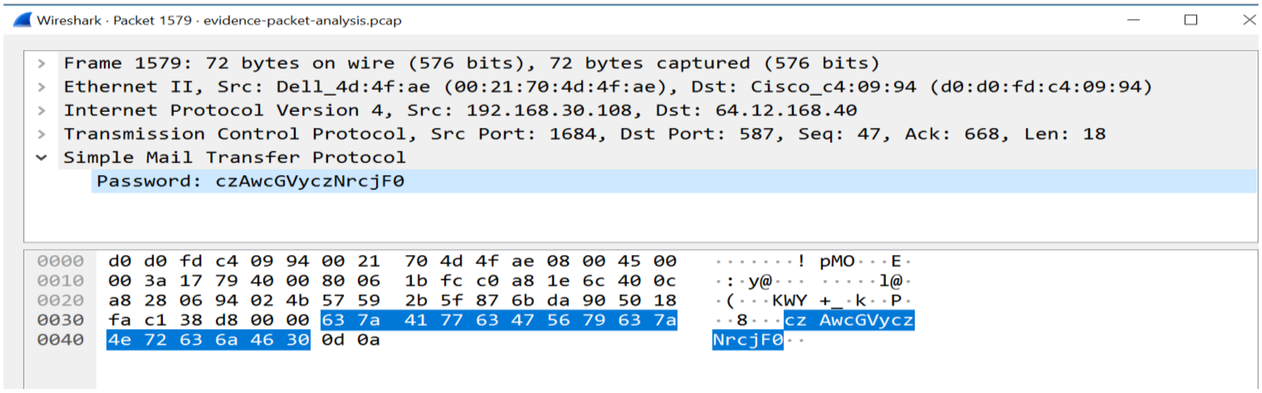
- Here we can see the username and password details and packet number where the username and password are mentioned.



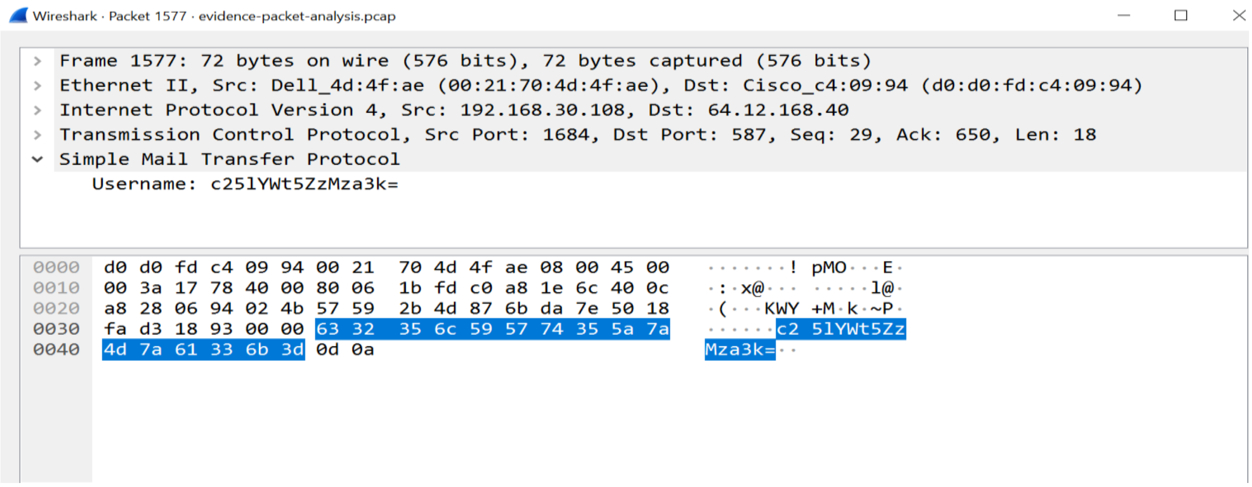
Packet No.	Protocol	Username	Additional Info
1579	SMTP	c25lYWt5...	Username in packet 1577
1607	IMAP	"sneakyg...	
1633	IMAP	"sneakyg...	
1741	SMTP	c25lYWt5...	Username in packet 1739
1769	IMAP	"sneakyg...	
1817	SMTP	c25lYWt5...	Username in packet 1815
2154	IMAP	"sneakyg...	

- Now click on packet number 1577 for username details and packet number 1579 for password details. Here we can see Source IP is 192.168.30.108 which is assigned to Ann’s system and we found below credential details in mail transfer protocol SMTP which is in base64 format. So this should be users email account credentials.

  Username: c25lYWt5ZzMza3k= , Password: czAwcGVyczNrcjF0 (base64 string)

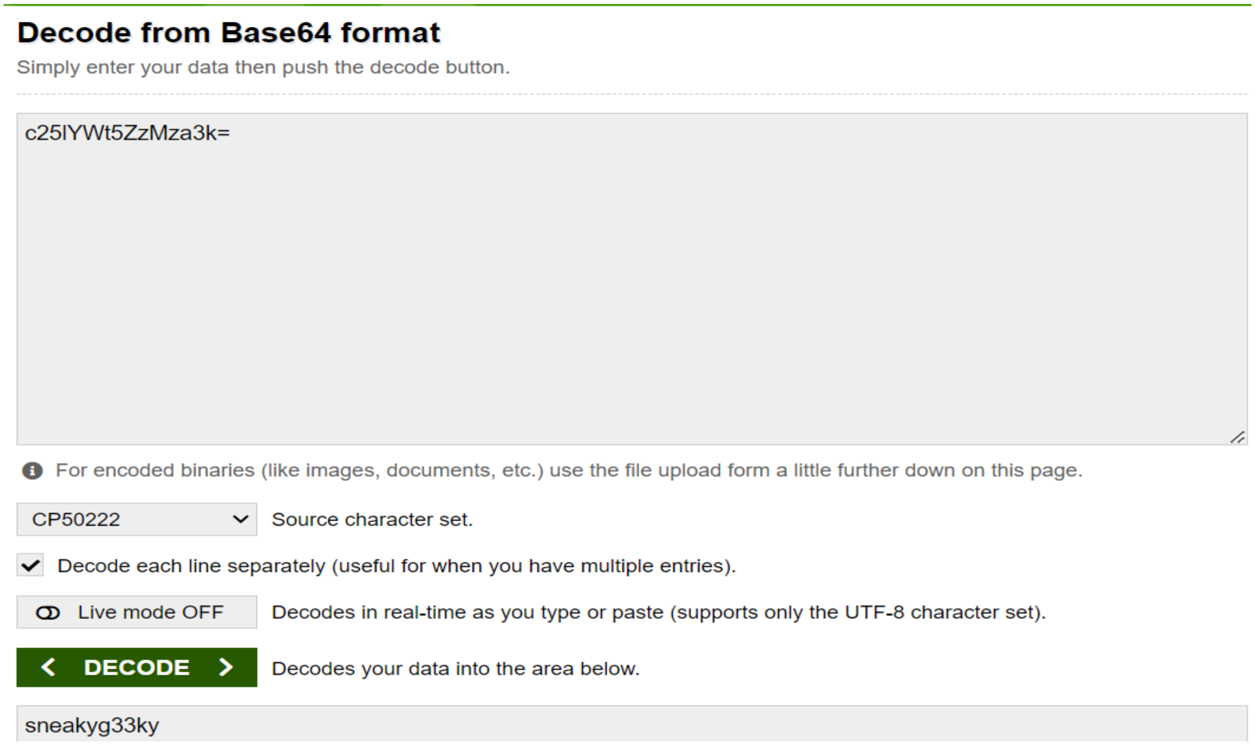

Wireshark · Packet 1579 · evidence-packet-analysis.pcap

```
> Frame 1579: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
> Ethernet II, Src: Dell_4d:4f:ae (00:21:70:4d:4f:ae), Dst: Cisco_c4:09:94 (d0:d0:fd:c4:09:94)
> Internet Protocol Version 4, Src: 192.168.30.108, Dst: 64.12.168.40
> Transmission Control Protocol, Src Port: 1684, Dst Port: 587, Seq: 47, Ack: 668, Len: 18
v Simple Mail Transfer Protocol
     Password: czAwcGVyczNrcjF0

0000  d0 d0 fd c4 09 94 00 21  70 4d 4f ae 08 00 45 00   ·······! pMO···E·
0010  00 3a 17 79 40 00 80 06  1b fc c0 a8 1e 6c 40 0c   ·:·y@··· ·····l@·
0020  a8 28 06 94 02 4b 57 59  2b 5f 87 6b da 90 50 18   ·(···KWY +_·k··P·
0030  fa c1 38 d8 00 00 63 7a  41 77 63 47 56 79 63 7a   ··8···cz AwcGVycz
0040  4e 72 63 6a 46 30 0d 0a                            NrcjF0··
```


Wireshark · Packet 1577 · evidence-packet-analysis.pcap

```
> Frame 1577: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
> Ethernet II, Src: Dell_4d:4f:ae (00:21:70:4d:4f:ae), Dst: Cisco_c4:09:94 (d0:d0:fd:c4:09:94)
> Internet Protocol Version 4, Src: 192.168.30.108, Dst: 64.12.168.40
> Transmission Control Protocol, Src Port: 1684, Dst Port: 587, Seq: 29, Ack: 650, Len: 18
v Simple Mail Transfer Protocol
     Username: c25lYWt5ZzMza3k=

0000  d0 d0 fd c4 09 94 00 21  70 4d 4f ae 08 00 45 00   ·······! pMO···E·
0010  00 3a 17 78 40 00 80 06  1b fd c0 a8 1e 6c 40 0c   ·:·x@··· ·····l@·
0020  a8 28 06 94 02 4b 57 59  2b 4d 87 6b da 7e 50 18   ·(···KWY +M·k·~P·
0030  fa d3 18 93 00 00 63 32  35 6c 59 57 74 35 5a 7a   ······c2 5lYWt5Zz
0040  4d 7a 61 33 6b 3d 0d 0a                            Mza3k=··
```

- Now we have to convert this base64 string into a plaintext. For that, I have used https://www.base64decode.org/.
  - Decoded Username - sneakyg33ky
  - Decoded Password - s00pers3kr1t



Decode from Base64 format

Simply enter your data then push the decode button.

```
c25lYWt5ZzMza3k=
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

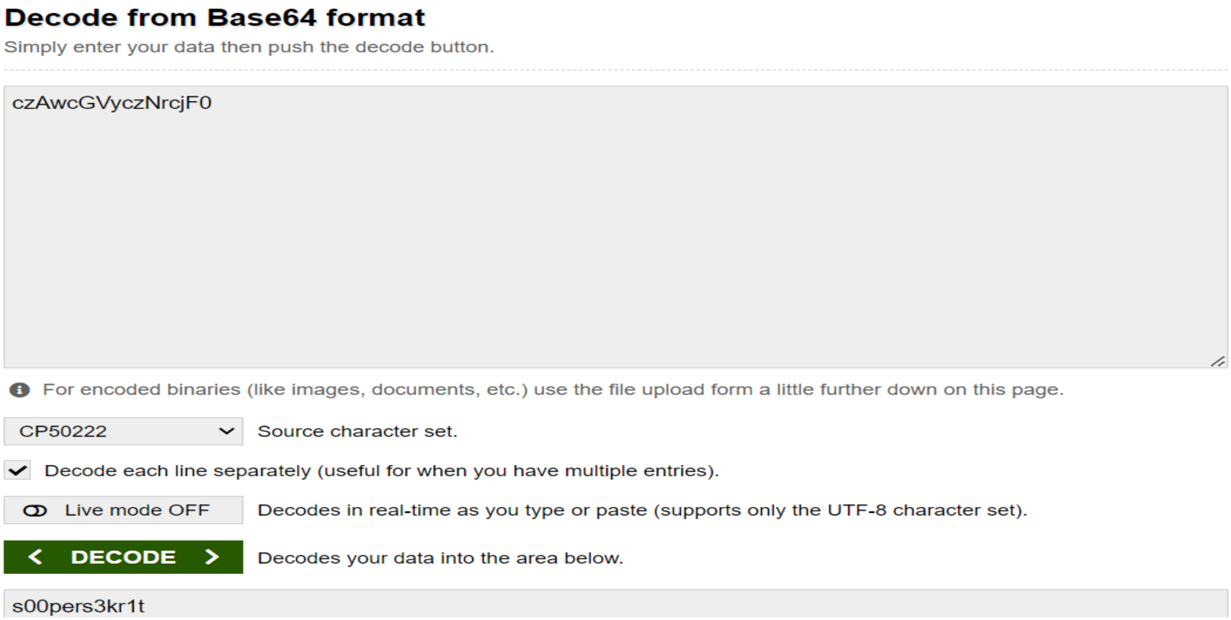
CP50222 Source character set.

☑ Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

```
sneakyg33ky
```



Decode from Base64 format

Simply enter your data then push the decode button.

```
czAwcGVyczNrcjF0
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

CP50222 Source character set.

☑ Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

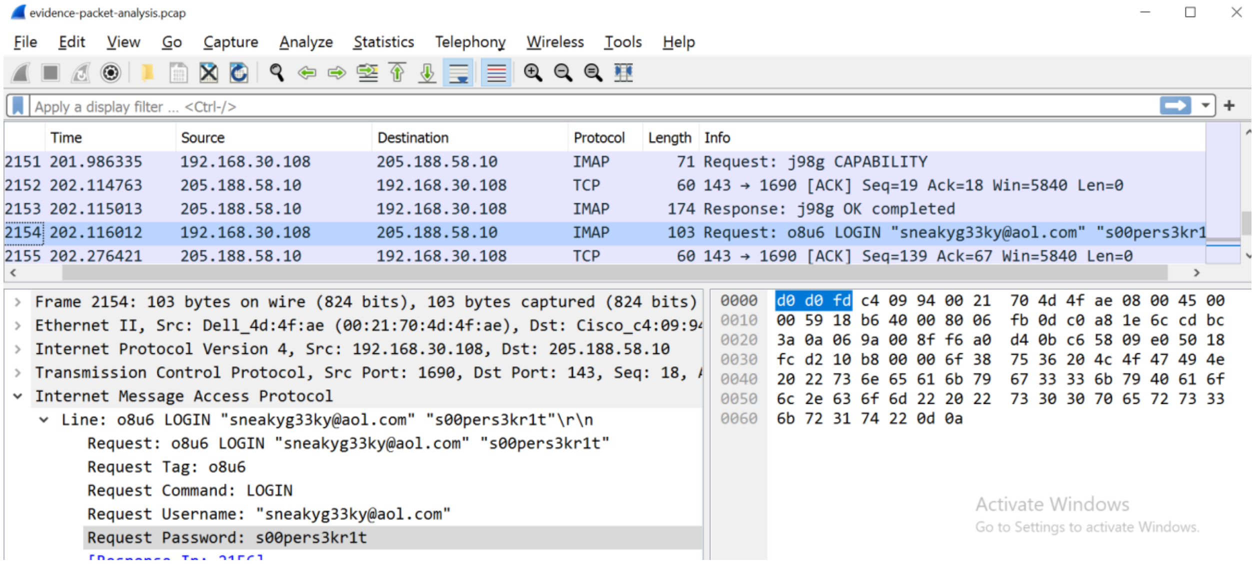
```
s00pers3kr1t
```

[1]

- Now click on packet number 1577 for username details and packet number 1579 for password details. Here we can see Ann’s source IP is mentioned so this should be Ann’s email ID credentials which is already given in plaintext.

Username : "sneakyg33ky@aol.com"

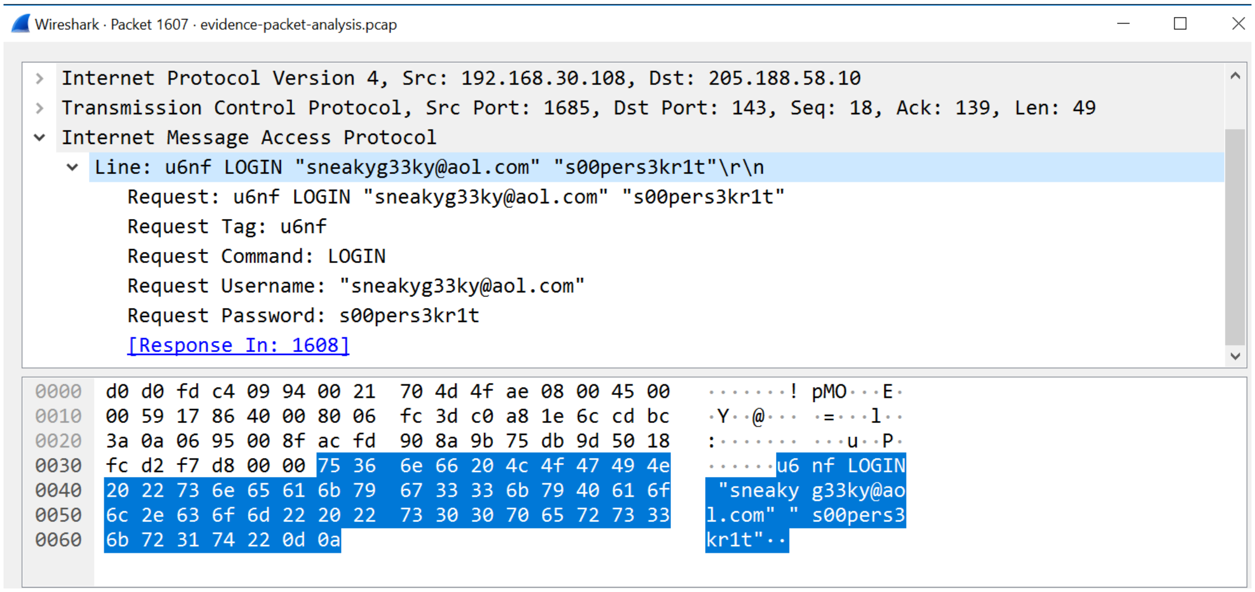
Password :"s00pers3kr1t"


evidence-packet-analysis.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Activate Windows
Go to Settings to activate Windows.

```
      Time         Source           Destination      Protocol  Length Info
2151 201.986335   192.168.30.108   205.188.58.10    IMAP        71 Request: j98g CAPABILITY
2152 202.114763   205.188.58.10    192.168.30.108   TCP         60 143 → 1690 [ACK] Seq=19 Ack=18 Win=5840 Len=0
2153 202.115013   205.188.58.10    192.168.30.108   IMAP       174 Response: j98g OK completed
2154 202.116012   192.168.30.108   205.188.58.10    IMAP       103 Request: o8u6 LOGIN "sneakyg33ky@aol.com" "s00pers3kr1
2155 202.276421   205.188.58.10    192.168.30.108   TCP         60 143 → 1690 [ACK] Seq=139 Ack=67 Win=5840 Len=0
```

```
> Frame 2154: 103 bytes on wire (824 bits), 103 bytes captured (824 bits)
> Ethernet II, Src: Dell_4d:4f:ae (00:21:70:4d:4f:ae), Dst: Cisco_c4:09:94
> Internet Protocol Version 4, Src: 192.168.30.108, Dst: 205.188.58.10
> Transmission Control Protocol, Src Port: 1690, Dst Port: 143, Seq: 18, A
v Internet Message Access Protocol
  v Line: o8u6 LOGIN "sneakyg33ky@aol.com" "s00pers3kr1t"\r\n
      Request: o8u6 LOGIN "sneakyg33ky@aol.com" "s00pers3kr1t"
      Request Tag: o8u6
      Request Command: LOGIN
      Request Username: "sneakyg33ky@aol.com"
      Request Password: s00pers3kr1t
```

```
0000  d0 d0 fd c4 09 94 00 21  70 4d 4f ae 08 00 45 00
0010  00 59 18 b6 40 00 80 06  fb 0d c0 a8 1e 6c cd bc
0020  3a 0a 06 9a 00 8f f6 a0  d4 0b c6 58 09 e0 50 18
0030  fc d2 10 b8 00 00 6f 38  75 36 20 4c 4f 47 49 4e
0040  20 22 73 6e 65 61 6b 79  67 33 33 6b 79 40 61 6f
0050  6c 2e 63 6f 6d 22 20 22  73 30 30 70 65 72 73 33
0060  6b 72 31 74 22 0d 0a
```



```
> Internet Protocol Version 4, Src: 192.168.30.108, Dst: 205.188.58.10
> Transmission Control Protocol, Src Port: 1685, Dst Port: 143, Seq: 18, Ack: 139, Len: 49
v Internet Message Access Protocol
  v Line: u6nf LOGIN "sneakyg33ky@aol.com" "s00pers3kr1t"\r\n
      Request: u6nf LOGIN "sneakyg33ky@aol.com" "s00pers3kr1t"
      Request Tag: u6nf
      Request Command: LOGIN
      Request Username: "sneakyg33ky@aol.com"
      Request Password: s00pers3kr1t
      [Response In: 1608]
```

```
0000  d0 d0 fd c4 09 94 00 21  70 4d 4f ae 08 00 45 00   ·······! pMO···E·
0010  00 59 17 86 40 00 80 06  fc 3d c0 a8 1e 6c cd bc   ·Y··@··· ·=···l··
0020  3a 0a 06 95 00 8f ac fd  90 8a 9b 75 db 9d 50 18   :······· ···u··P·
0030  fc d2 f7 d8 00 00 75 36  6e 66 20 4c 4f 47 49 4e   ······u6 nf LOGIN
0040  20 22 73 6e 65 61 6b 79  67 33 33 6b 79 40 61 6f    "sneaky g33ky@ao
0050  6c 2e 63 6f 6d 22 20 22  73 30 30 70 65 72 73 33   l.com" " s00pers3
0060  6b 72 31 74 22 0d 0a                               kr1t"··
```

2. Who did Ann communicate with? Provide a list of email addresses and any other identifying information.

- ➢ Now that we know email address of user 'Ann'. I have search frames containing Ann's email address 'sneakyg33ky@aol.com'. Below are the users with whom Ann communicated.

Command - ‘frame contains "sneakyg33ky@aol.com".

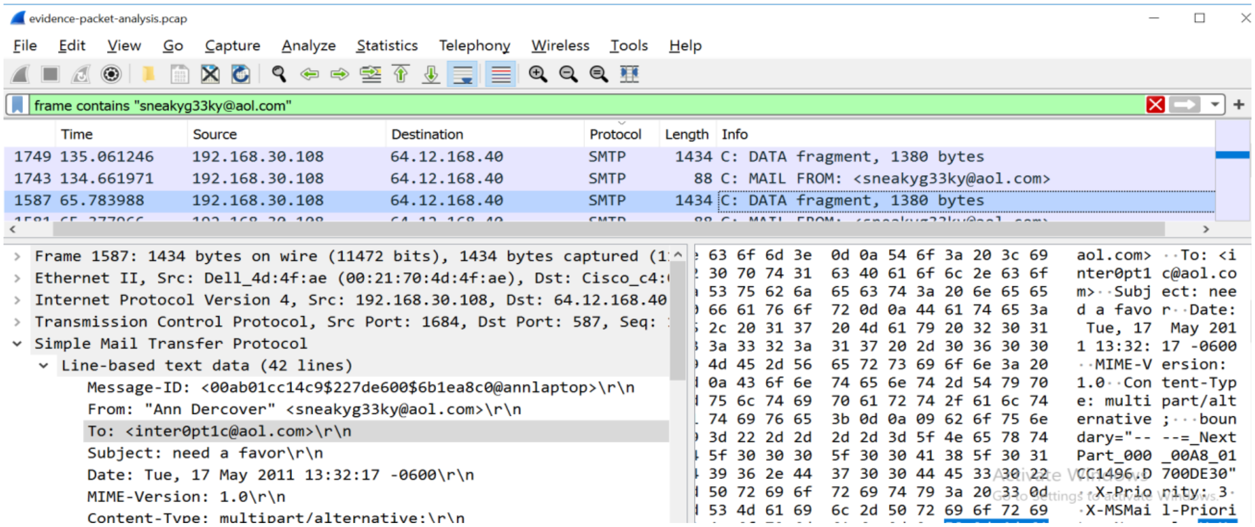
The “frame contains” filter will let you pick out only those packets that contain a sequence of any ASCII or Hex value that you specify. It will show you only those packets that contain the word “sneakyg33ky@aol.com” somewhere in them. [4]

Ann Communicated with -

inter0pt1c@aol.com

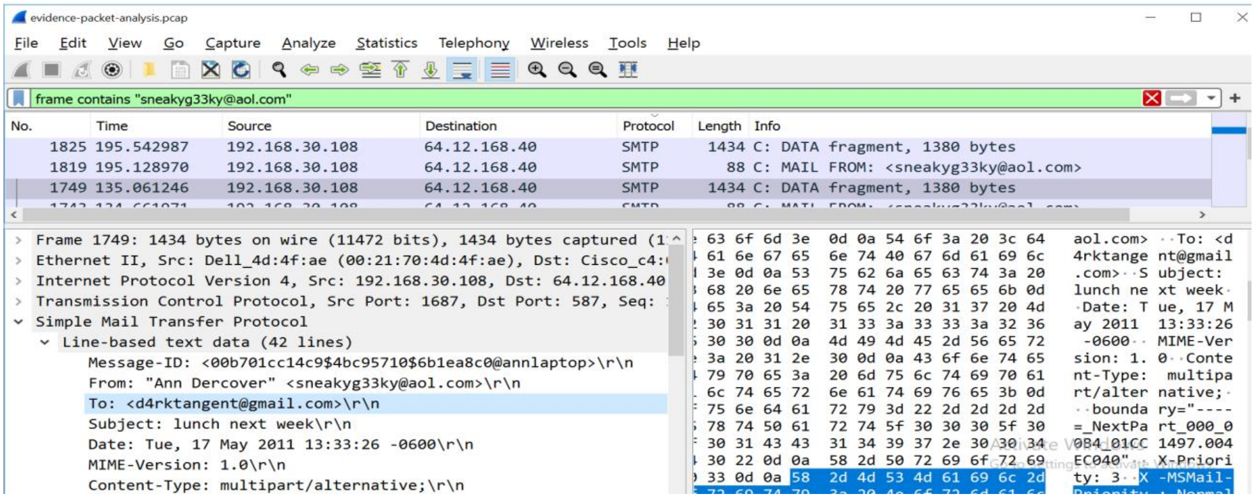
d4rktangent@gmail.com

mistersekritx@aol.com


evidence-packet-analysis.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

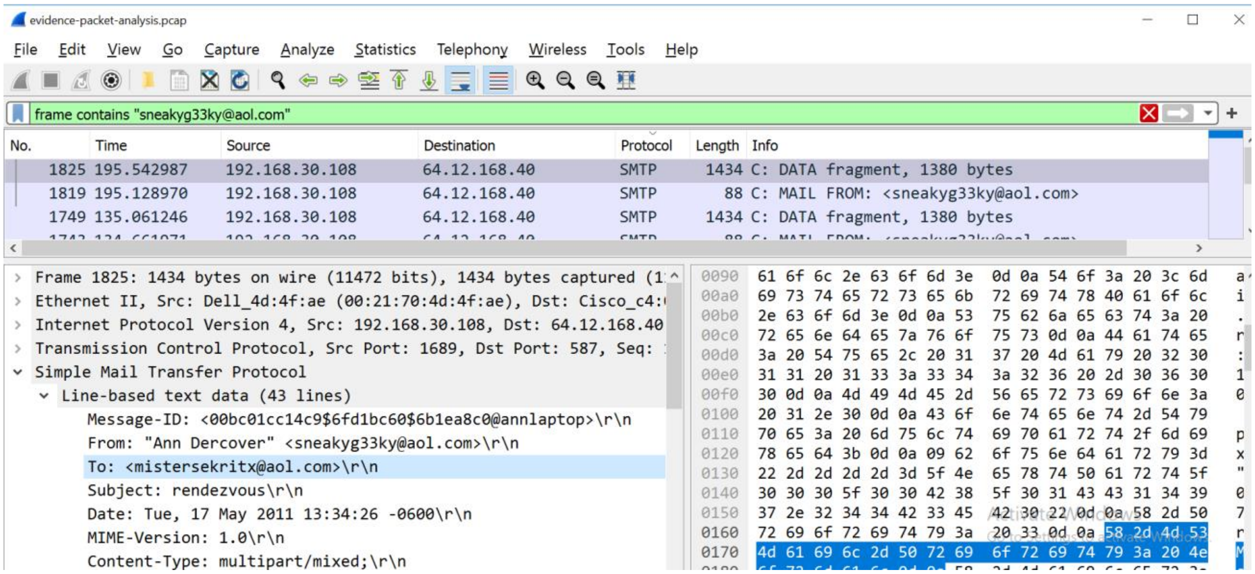
```
frame contains "sneakyg33ky@aol.com"

     Time          Source            Destination     Protocol  Length  Info
1749 135.061246    192.168.30.108    64.12.168.40    SMTP        1434  C: DATA fragment, 1380 bytes
1743 134.661971    192.168.30.108    64.12.168.40    SMTP          88  C: MAIL FROM: <sneakyg33ky@aol.com>
1587 65.783988     192.168.30.108    64.12.168.40    SMTP        1434  C: DATA fragment, 1380 bytes

> Frame 1587: 1434 bytes on wire (11472 bits), 1434 bytes captured (1
> Ethernet II, Src: Dell_4d:4f:ae (00:21:70:4d:4f:ae), Dst: Cisco_c4:
> Internet Protocol Version 4, Src: 192.168.30.108, Dst: 64.12.168.40
> Transmission Control Protocol, Src Port: 1684, Dst Port: 587, Seq:
v Simple Mail Transfer Protocol
  v Line-based text data (42 lines)
      Message-ID: <00ab01cc14c9$227de600$6b1ea8c0@annlaptop>\r\n
      From: "Ann Dercover" <sneakyg33ky@aol.com>\r\n
      To: <inter0pt1c@aol.com>\r\n
      Subject: need a favor\r\n
      Date: Tue, 17 May 2011 13:32:17 -0600\r\n
      MIME-Version: 1.0\r\n
      Content-Type: multipart/alternative;\r\n
```

```
63 6f 6d 3e  0d 0a 54 6f 3a 20 3c 69   aol.com> ··To: <i
30 70 74 31  63 40 61 6f 6c 2e 63 6f   nter0pt1 c@aol.co
53 75 62 6a  65 63 74 3a 20 6e 65 65   m>··Subj ect: nee
66 61 76 6f  72 0d 0a 44 61 74 65 3a   d a favo r··Date:
2c 20 31 37  20 4d 61 79 20 32 30 31    Tue, 17  May 201
3a 33 32 3a  31 37 20 2d 30 36 30 30   1 13:32: 17 -0600
4d 45 2d 56  65 72 73 69 6f 6e 3a 20   ··MIME-V ersion:
0a 43 6f 6e  74 65 6e 74 2d 54 79 70   1.0··Con tent-Typ
75 6c 74 69  70 61 72 74 2f 61 6c 74   e: multi part/alt
74 69 76 65  3b 0d 0a 09 62 6f 75 6e   ernative ;···boun
3d 22 2d 2d  2d 2d 3d 5f 4e 65 78 74   dary="-- --=_Next
5f 30 30 30  5f 30 30 41 38 5f 30 31   Part_000 _00A8_01
39 36 2e 44  37 30 30 44 45 33 30 22   CC1496.D 700DE30"
50 72 69 6f  72 69 74 79 3a 20 33 0d   ·X-Prio rity: 3·
53 4d 61 69  6c 2d 50 72 69 6f 72 69   ·X-MSMai l-Priori
```


evidence-packet-analysis.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
frame contains "sneakyg33ky@aol.com"

No.   Time          Source            Destination     Protocol  Length  Info
1825  195.542987    192.168.30.108    64.12.168.40    SMTP        1434  C: DATA fragment, 1380 bytes
1819  195.128970    192.168.30.108    64.12.168.40    SMTP          88  C: MAIL FROM: <sneakyg33ky@aol.com>
1749  135.061246    192.168.30.108    64.12.168.40    SMTP        1434  C: DATA fragment, 1380 bytes

> Frame 1749: 1434 bytes on wire (11472 bits), 1434 bytes captured (1
> Ethernet II, Src: Dell_4d:4f:ae (00:21:70:4d:4f:ae), Dst: Cisco_c4:
> Internet Protocol Version 4, Src: 192.168.30.108, Dst: 64.12.168.40
> Transmission Control Protocol, Src Port: 1687, Dst Port: 587, Seq:
v Simple Mail Transfer Protocol
  v Line-based text data (42 lines)
      Message-ID: <00b701cc14c9$4bc95710$6b1ea8c0@annlaptop>\r\n
      From: "Ann Dercover" <sneakyg33ky@aol.com>\r\n
      To: <d4rktangent@gmail.com>\r\n
      Subject: lunch next week\r\n
      Date: Tue, 17 May 2011 13:33:26 -0600\r\n
      MIME-Version: 1.0\r\n
      Content-Type: multipart/alternative;\r\n
```

```
63 6f 6d 3e  0d 0a 54 6f 3a 20 3c 64   aol.com> ··To: <d
61 6e 67 65  6e 74 40 67 6d 61 69 6c   4rktange nt@gmail
3e 0d 0a 53  75 62 6a 65 63 74 3a 20   .com>··S ubject:
68 20 6e 65  78 74 20 77 65 65 6b 0d   lunch ne xt week·
65 3a 20 54  75 65 2c 20 31 37 20 4d   ·Date: T ue, 17 M
30 31 31 20  31 33 3a 33 33 3a 32 36   ay 2011  13:33:26
30 30 0d 0a  4d 49 4d 45 2d 56 65 72    -0600·· MIME-Ver
3a 20 31 2e  30 0d 0a 43 6f 6e 74 65   sion: 1. 0··Conte
79 70 65 3a  20 6d 75 6c 74 69 70 61   nt-Type:  multipa
6c 74 65 72  6e 61 74 69 76 65 3b 0d   rt/alter native;·
75 6e 64 61  72 79 3d 22 2d 2d 2d 2d   ··bounda ry="----
78 74 50 61  72 74 5f 30 30 30 5f 30   =_NextPa rt_000_0
30 31 43 43  31 34 39 37 2e 30 30 34   0B4_01CC 1497.004
30 22 0d 0a  58 2d 50 72 69 6f 72 69   EC040"·· X-Priori
33 0d 0a 58  2d 4d 53 4d 61 69 6c 2d   ty: 3··X -MSMail-
```


evidence-packet-analysis.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
frame contains "sneakyg33ky@aol.com"

No.   Time         Source           Destination    Protocol  Length  Info
 1825 195.542987   192.168.30.108   64.12.168.40   SMTP        1434  C: DATA fragment, 1380 bytes
 1819 195.128970   192.168.30.108   64.12.168.40   SMTP          88  C: MAIL FROM: <sneakyg33ky@aol.com>
 1749 135.061246   192.168.30.108   64.12.168.40   SMTP        1434  C: DATA fragment, 1380 bytes
 1743 134.661071   192.168.30.108   64.12.168.40   SMTP          88  C: MAIL FROM: <sneakyg33ky@aol.com>
```

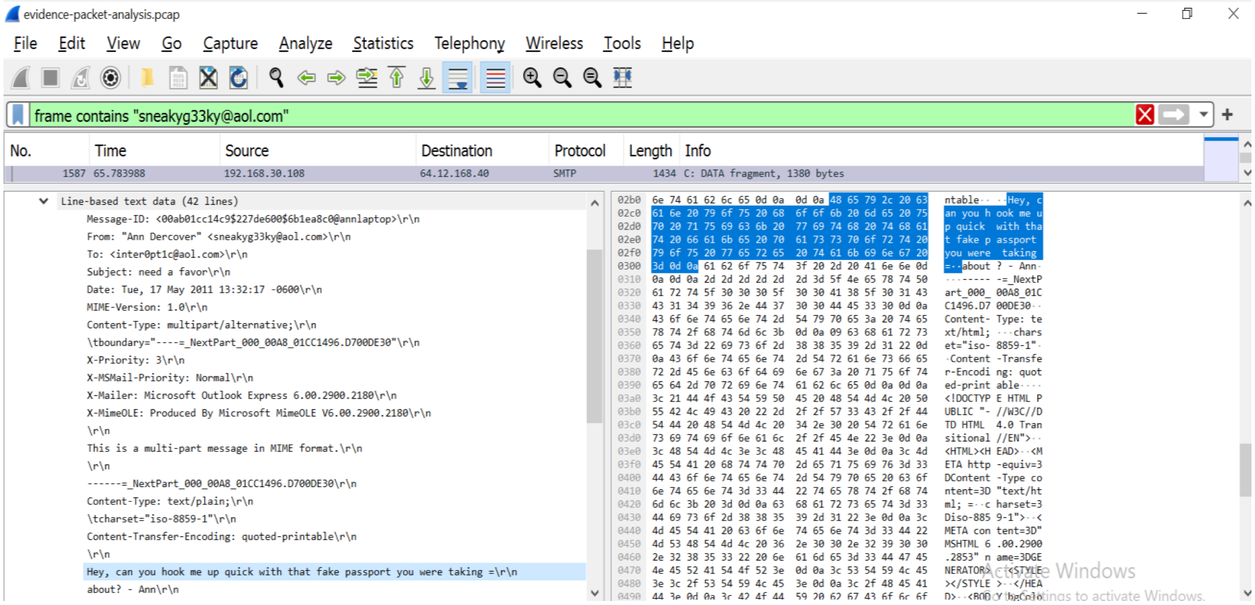
```
> Frame 1825: 1434 bytes on wire (11472 bits), 1434 bytes captured (1
> Ethernet II, Src: Dell_4d:4f:ae (00:21:70:4d:4f:ae), Dst: Cisco_c4:
> Internet Protocol Version 4, Src: 192.168.30.108, Dst: 64.12.168.40
> Transmission Control Protocol, Src Port: 1689, Dst Port: 587, Seq:
v Simple Mail Transfer Protocol
  v Line-based text data (43 lines)
      Message-ID: <00bc01cc14c9$6fd1bc60$6b1ea8c0@annlaptop>\r\n
      From: "Ann Dercover" <sneakyg33ky@aol.com>\r\n
      To: <mistersekritx@aol.com>\r\n
      Subject: rendezvous\r\n
      Date: Tue, 17 May 2011 13:34:26 -0600\r\n
      MIME-Version: 1.0\r\n
      Content-Type: multipart/mixed;\r\n
```

```
0090  61 6f 6c 2e 63 6f 6d 3e  0d 0a 54 6f 3a 20 3c 6d   a
00a0  69 73 74 65 72 73 65 6b  72 69 74 78 40 61 6f 6c   i
00b0  2e 63 6f 6d 3e 0d 0a 53  75 62 6a 65 63 74 3a 20   .
00c0  72 65 6e 64 65 7a 76 6f  75 73 0d 0a 44 61 74 65   r
00d0  3a 20 54 75 65 2c 20 31  37 20 4d 61 79 20 32 30   :
00e0  31 31 20 31 33 3a 33 34  3a 32 36 20 2d 30 36 30   1
00f0  30 0d 0a 4d 49 4d 45 2d  56 65 72 73 69 6f 6e 3a   0
0100  20 31 2e 30 0d 0a 43 6f  6e 74 65 6e 74 2d 54 79
0110  70 65 3a 20 6d 75 6c 74  69 70 61 72 74 2f 6d 69   p
0120  78 65 64 3b 0d 0a 09 62  6f 75 6e 64 61 72 79 3d   x
0130  22 2d 2d 2d 2d 3d 5f 4e  65 78 74 50 61 72 74 5f   "
0140  30 30 30 5f 30 30 42 38  5f 30 31 43 43 31 34 39   0
0150  37 2e 32 34 34 42 33 45  42 30 22 0d 0a 58 2d 50   7
0160  72 69 6f 72 69 74 79 3a  20 33 0d 0a 58 2d 4d 53   r
0170  4d 61 69 6c 2d 50 72 69  6f 72 69 74 79 3a 20 4e   M
```

3. Extract any transcripts of Ann's conversations and present them to investigators.

➢ Below are the snapshots of Ann's email communication over email.

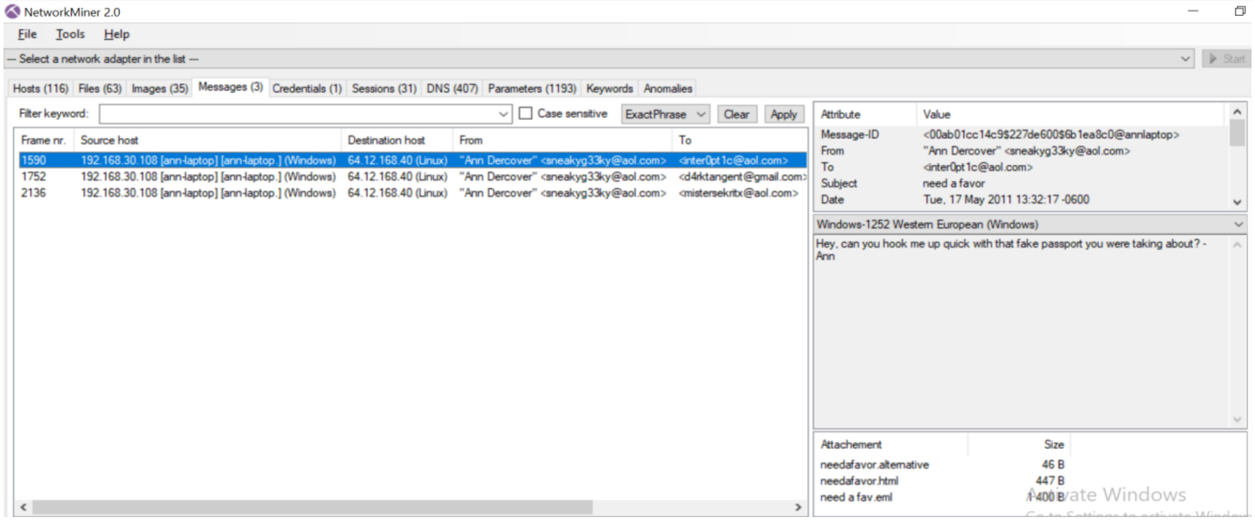
Ann's communication with inter0pt1c@aol.com


evidence-packet-analysis.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
frame contains "sneakyg33ky@aol.com"

No.   Time        Source           Destination    Protocol  Length  Info
 1587 65.783988   192.168.30.108   64.12.168.40   SMTP        1434  C: DATA fragment, 1380 bytes
```

```
v Line-based text data (42 lines)
    Message-ID: <00ab01cc14c9$227de600$6b1ea8c0@annlaptop>\r\n
    From: "Ann Dercover" <sneakyg33ky@aol.com>\r\n
    To: <inter0pt1c@aol.com>\r\n
    Subject: need a favor\r\n
    Date: Tue, 17 May 2011 13:32:17 -0600\r\n
    MIME-Version: 1.0\r\n
    Content-Type: multipart/alternative;\r\n
    \tboundary="----=_NextPart_000_00A8_01CC1496.D700DE30"\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_00A8_01CC1496.D700DE30\r\n
    Content-Type: text/plain;\r\n
    \tcharset="iso-8859-1"\r\n
    Content-Transfer-Encoding: quoted-printable\r\n
    \r\n
    Hey, can you hook me up quick with that fake passport you were taking =\r\n
    about? - Ann\r\n
```

```
02b0  6e 74 61 62 6c 65 0d 0a  0d 0a 48 65 79 2c 20 63   ntable·· ··Hey, c
02c0  61 6e 20 79 6f 75 20 68  6f 6f 6b 20 6d 65 20 75   an you h ook me u
02d0  70 20 71 75 69 63 6b 20  77 69 74 68 20 74 68 61   p quick  with tha
02e0  74 20 66 61 6b 65 20 70  61 73 73 70 6f 72 74 20   t fake p assport
02f0  79 6f 75 20 77 65 72 65  20 74 61 6b 69 6e 67 20   you were  taking
0300  3d 0d 0a 61 62 6f 75 74  3f 20 2d 20 41 6e 6e 0d   =··about ? - Ann·
0310  0a 0d 0a 2d 2d 2d 2d 2d  2d 3d 5f 4e 65 78 74 50   ···----- -=_NextP
0320  61 72 74 5f 30 30 30 5f  30 30 41 38 5f 30 31 43   art_000_ 00A8_01C
0330  43 31 34 39 36 2e 44 37  30 30 44 45 33 30 0d 0a   C1496.D7 00DE30··
0340  43 6f 6e 74 65 6e 74 2d  54 79 70 65 3a 20 74 65   Content- Type: te
0350  78 74 2f 68 74 6d 6c 3b  0d 0a 09 63 68 61 72 73   xt/html; ···chars
0360  65 74 3d 22 69 73 6f 2d  38 38 35 39 2d 31 22 0d   et="iso- 8859-1"·
0370  0a 43 6f 6e 74 65 6e 74  2d 54 72 61 6e 73 66 65   ·Content -Transfe
0380  72 2d 45 6e 63 6f 64 69  6e 67 3a 20 71 75 6f 74   r-Encodi ng: quot
0390  65 64 2d 70 72 69 6e 74  61 62 6c 65 0d 0a 0d 0a   ed-print able····
03a0  3c 21 44 4f 43 54 59 50  45 20 48 54 4d 4c 20 50   <!DOCTYP E HTML P
03b0  55 42 4c 49 43 20 22 2d  2f 2f 57 33 43 2f 2f 44   UBLIC "- //W3C//D
03c0  54 44 20 48 54 4d 4c 20  34 2e 30 20 54 72 61 6e   TD HTML  4.0 Tran
03d0  73 69 74 69 6f 6e 61 6c  2f 2f 45 4e 22 3e 0d 0a   sitional //EN">··
03e0  3c 48 54 4d 4c 3e 3c 48  45 41 44 3e 0d 0a 3c 4d   <HTML><H EAD>··<M
03f0  45 54 41 20 68 74 74 70  2d 65 71 75 69 76 3d 33   ETA http -equiv=3
0400  44 43 6f 6e 74 65 6e 74  2d 54 79 70 65 20 63 6f   DContent -Type co
0410  6e 74 65 6e 74 3d 33 44  22 74 65 78 74 2f 68 74   ntent=3D "text/ht
0420  6d 6c 3b 20 3d 0d 0a 63  68 61 72 73 65 74 3d 33   ml; =··c harset=3
0430  44 69 73 6f 2d 38 38 35  39 2d 31 22 3e 0d 0a 3c   Diso-885 9-1">··<
0440  4d 45 54 41 20 63 6f 6e  74 65 6e 74 3d 33 44 22   META con tent=3D"
0450  4d 53 48 54 4d 4c 20 36  2e 30 30 2e 32 39 30 30   MSHTML 6 .00.2900
0460  2e 32 38 35 33 22 20 6e  61 6d 65 3d 33 44 47 45   .2853" n ame=3DGE
0470  4e 45 52 41 54 4f 52 3e  0d 0a 3c 53 54 59 4c 45   NERATOR> ··<STYLE
0480  3e 3c 2f 53 54 59 4c 45  3e 0d 0a 3c 2f 48 45 41   ></STYLE >··</HEA
0490  44 3e 0d 0a 3c 42 4f 44  59 20 62 67 43 6f 6c 6f   D>··<BOD Y bgColo
```


NetworkMiner 2.0
File Tools Help
--- Select a network adapter in the list ---
Start
Hosts (116) Files (63) Images (35) Messages (3) Credentials (1) Sessions (31) DNS (407) Parameters (1193) Keywords Anomalies
Filter keyword:
□ Case sensitive
ExactPhrase
Clear
Apply

Frame nr.	Source host	Destination host	From	To
1590	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	64.12.168.40 (Linux)	"Ann Dercover" <sneakyg33ky@aol.com>	<inter0pt1c@aol.com>
1752	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	64.12.168.40 (Linux)	"Ann Dercover" <sneakyg33ky@aol.com>	<d4rktangent@gmail.com>
2136	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	64.12.168.40 (Linux)	"Ann Dercover" <sneakyg33ky@aol.com>	<mistersekritx@aol.com>

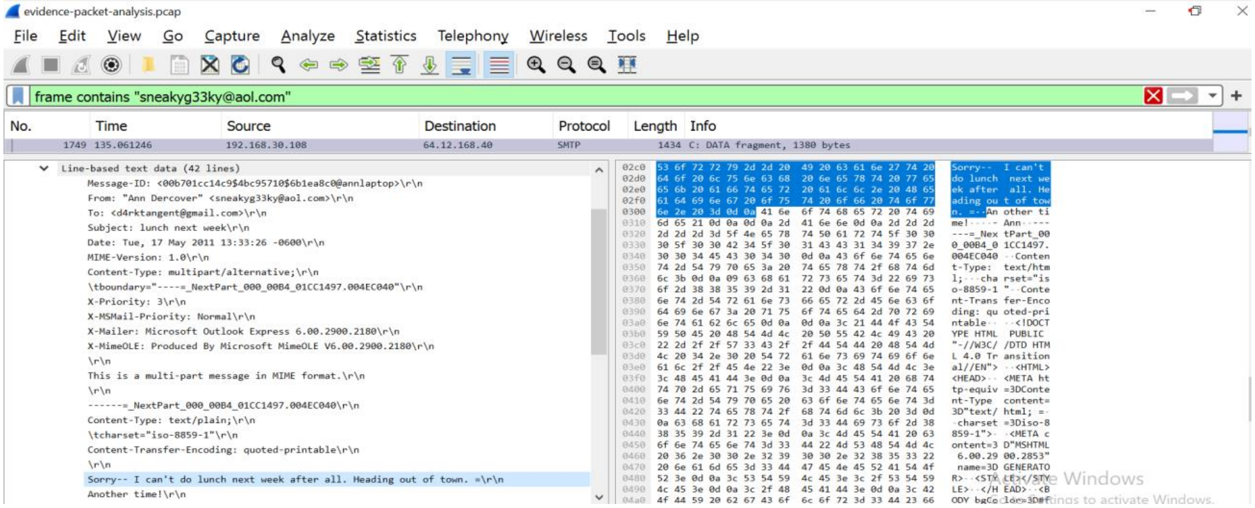
Attribute	Value
Message-ID	<00ab01cc14c9$227de600$6b1ea8c0@annlaptop>
From	"Ann Dercover" <sneakyg33ky@aol.com>
To	<inter0pt1c@aol.com>
Subject	need a favor
Date	Tue, 17 May 2011 13:32:17 -0600

Windows-1252 Western European (Windows)

Hey, can you hook me up quick with that fake passport you were taking about? - Ann

Attachement	Size
needafavor.alternative	46 B
needafavor.html	447 B
need a fav.eml	1400 B

- Ann’s communication with d4rktangent@gmail.com

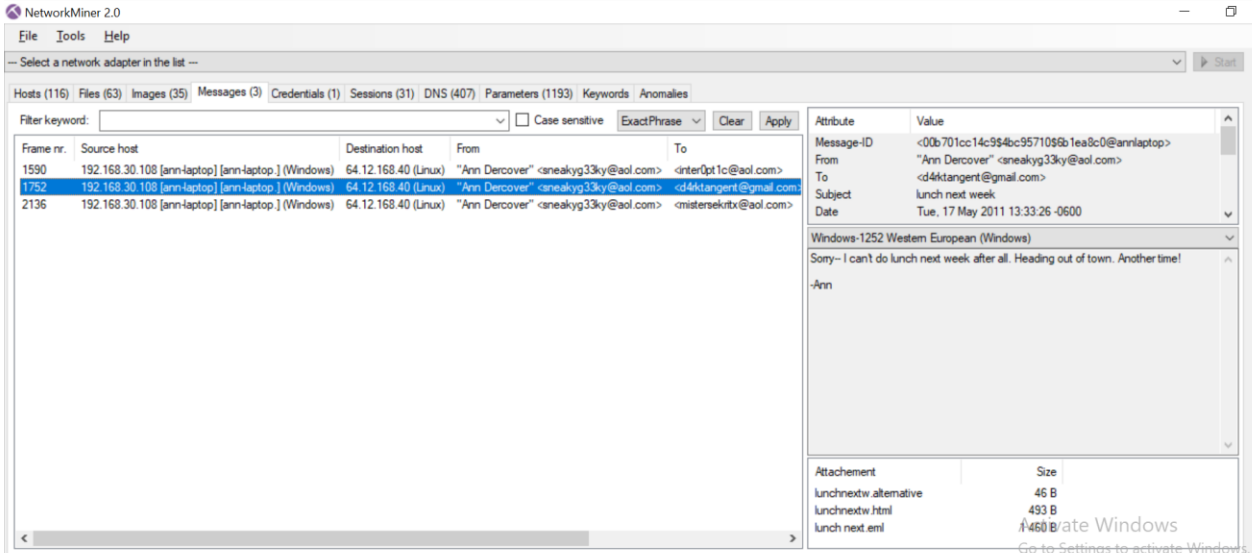

evidence-packet-analysis.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

frame contains "sneakyg33ky@aol.com"

```
No.      Time          Source           Destination     Protocol   Length  Info
   1749  135.061246    192.168.30.108   64.12.168.40    SMTP       1434  C: DATA fragment, 1380 bytes
```

```
  Line-based text data (42 lines)
      Message-ID: <00b701cc14c9$4bc95710$6b1ea8c0@annlaptop>\r\n
      From: "Ann Dercover" <sneakyg33ky@aol.com>\r\n
      To: <d4rktangent@gmail.com>\r\n
      Subject: lunch next week\r\n
      Date: Tue, 17 May 2011 13:33:26 -0600\r\n
      MIME-Version: 1.0\r\n
      Content-Type: multipart/alternative;\r\n
      \tboundary="----=_NextPart_000_00B4_01CC1497.004EC040"\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_00B4_01CC1497.004EC040\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!\r\n
```

```
02c0  53 6f 72 72 79 2d 2d 20  49 20 63 61 6e 27 74 20   Sorry--  I can't 
02d0  64 6f 20 6c 75 6e 63 68  20 6e 65 78 74 20 77 65   do lunch  next we
02e0  65 6b 20 61 66 74 65 72  20 61 6c 6c 2e 20 48 65   ek after  all. He
02f0  61 64 69 6e 67 20 6f 75  74 20 6f 66 20 74 6f 77   ading ou t of tow
0300  6e 2e 20 3d 0d 0a 41 6e  6f 74 68 65 72 20 74 69   n. =··An other ti
0310  6d 65 21 0d 0a 0d 0a 2d  41 6e 6e 0d 0a 2d 2d 2d   me!····- Ann··---
0320  2d 2d 2d 3d 5f 4e 65 78  74 50 61 72 74 5f 30 30   ---=_Nex tPart_00
0330  30 5f 30 30 42 34 5f 30  31 43 43 31 34 39 37 2e   0_00B4_0 1CC1497.
0340  30 30 34 45 43 30 34 30  0d 0a 43 6f 6e 74 65 6e   004EC040 ··Conten
0350  74 2d 54 79 70 65 3a 20  74 65 78 74 2f 68 74 6d   t-Type:  text/htm
0360  6c 3b 0d 0a 09 63 68 61  72 73 65 74 3d 22 69 73   l;···cha rset="is
0370  6f 2d 38 38 35 39 2d 31  22 0d 0a 43 6f 6e 74 65   o-8859-1 "··Conte
0380  6e 74 2d 54 72 61 6e 73  66 65 72 2d 45 6e 63 6f   nt-Trans fer-Enco
0390  64 69 6e 67 3a 20 71 75  6f 74 65 64 2d 70 72 69   ding: qu oted-pri
03a0  6e 74 61 62 6c 65 0d 0a  0d 0a 3c 21 44 4f 43 54   ntable·· ··<!DOCT
03b0  59 50 45 20 48 54 4d 4c  20 50 55 42 4c 49 43 20   YPE HTML  PUBLIC 
03c0  22 2d 2f 2f 57 33 43 2f  2f 44 54 44 20 48 54 4d   "-//W3C/ /DTD HTM
03d0  4c 20 34 2e 30 20 54 72  61 6e 73 69 74 69 6f 6e   L 4.0 Tr ansition
03e0  61 6c 2f 2f 45 4e 22 3e  0d 0a 3c 48 54 4d 4c 3e   al//EN"> ··<HTML>
03f0  3c 48 45 41 44 3e 0d 0a  3c 4d 45 54 41 20 68 74   <HEAD>·· <META ht
0400  74 70 2d 65 71 75 69 76  3d 33 44 43 6f 6e 74 65   tp-equiv =3DConte
0410  6e 74 2d 54 79 70 65 20  63 6f 6e 74 65 6e 74 3d   nt-Type  content=
0420  33 44 22 74 65 78 74 2f  68 74 6d 6c 3b 20 3d 0d   3D"text/ html; =·
0430  0a 63 68 61 72 73 65 74  3d 33 44 69 73 6f 2d 38   ·charset =3Diso-8
0440  38 35 39 2d 31 22 3e 0d  0a 3c 4d 45 54 41 20 63   859-1">· ·<META c
0450  6f 6e 74 65 6e 74 3d 33  44 22 4d 53 48 54 4d 4c   ontent=3 D"MSHTML
0460  20 36 2e 30 30 2e 32 39  30 30 2e 32 38 35 33 22    6.00.29 00.2853"
0470  20 6e 61 6d 65 3d 33 44  47 45 4e 45 52 41 54 4f    name=3D GENERATO
0480  52 3e 0d 0a 3c 53 54 59  4c 45 3e 3c 2f 53 54 59   R>··<STY LE></STY
0490  4c 45 3e 0d 0a 3c 2f 48  45 41 44 3e 0d 0a 3c 42   LE>··</H EAD>··<B
04a0  4f 44 59 20 62 67 43 6f  6c 6f 72 3d 33 44 23 66   ODY bgCo lor=3D#f
```


NetworkMiner 2.0
File Tools Help
--- Select a network adapter in the list ---
Start
Hosts (116) Files (63) Images (35) Messages (3) Credentials (1) Sessions (31) DNS (407) Parameters (1193) Keywords Anomalies
Filter keyword:
□ Case sensitive
ExactPhrase
Clear
Apply

Frame nr.	Source host	Destination host	From	To
1590	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	64.12.168.40 (Linux)	"Ann Dercover" <sneakyg33ky@aol.com>	<inter0pt1c@aol.com>
1752	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	64.12.168.40 (Linux)	"Ann Dercover" <sneakyg33ky@aol.com>	<d4rktangent@gmail.com
2136	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	64.12.168.40 (Linux)	"Ann Dercover" <sneakyg33ky@aol.com>	<mistersekritx@aol.com>

Attribute	Value
Message-ID	<00b701cc14c9$4bc95710$6b1ea8c0@annlaptop>
From	"Ann Dercover" <sneakyg33ky@aol.com>
To	<d4rktangent@gmail.com>
Subject	lunch next week
Date	Tue, 17 May 2011 13:33:26 -0600

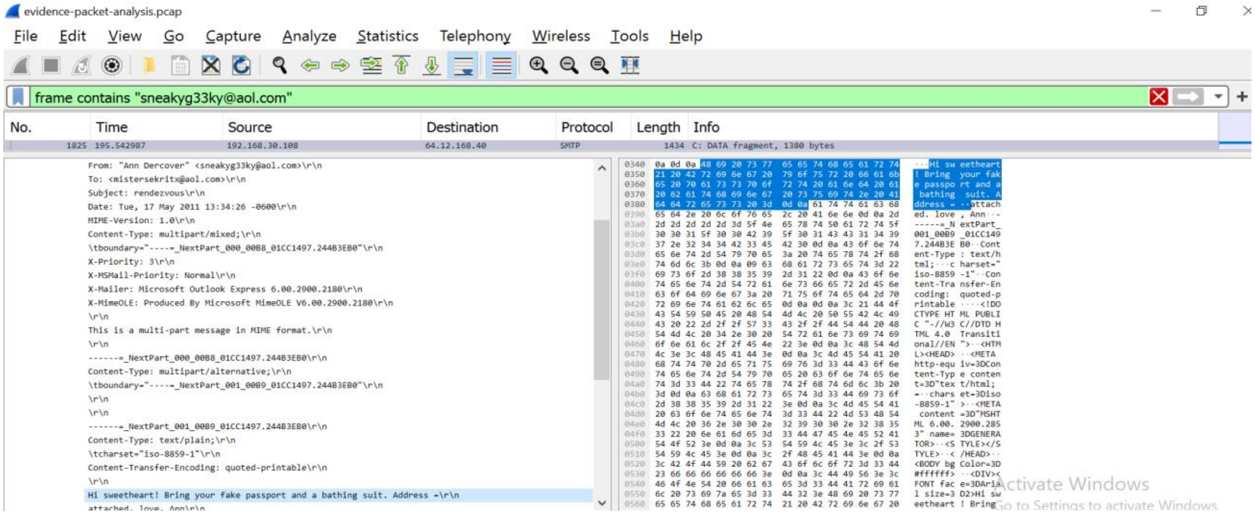
Windows-1252 Western European (Windows)

Sorry-- I can't do lunch next week after all. Heading out of town. Another time!

-Ann

Attachement	Size
lunchnextw.alternative	46 B
lunchnextw.html	493 B
lunch next.eml	1460 B

- Ann’s communication with mistersekritx@aol.com

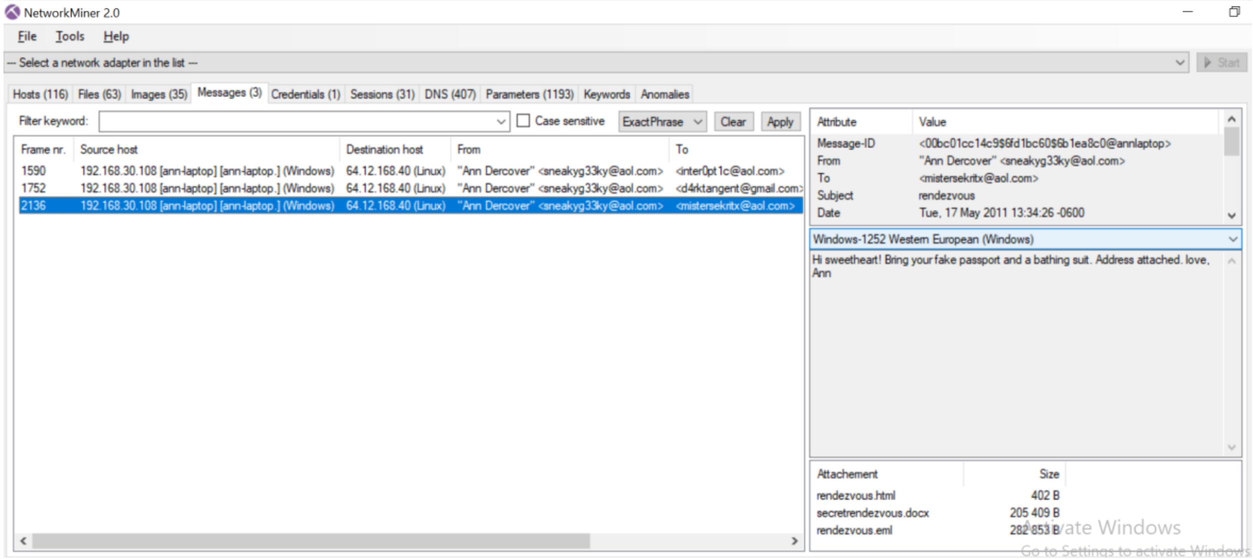

evidence-packet-analysis.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

frame contains "sneakyg33ky@aol.com"

```
No.    Time         Source          Destination   Protocol  Length  Info
1825   195.542987   192.168.30.108  64.12.168.40  SMTP      1434    C: DATA fragment, 1380 bytes
```

```
From: "Ann Dercover" <sneakyg33ky@aol.com>\r\n
To: <mistersekritx@aol.com>\r\n
Subject: rendezvous\r\n
Date: Tue, 17 May 2011 13:34:26 -0600\r\n
MIME-Version: 1.0\r\n
Content-Type: multipart/mixed;\r\n
\tboundary="----=_NextPart_000_00B8_01CC1497.244B3EB0"\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_00B8_01CC1497.244B3EB0\r\n
Content-Type: multipart/alternative;\r\n
\tboundary="----=_NextPart_001_00B9_01CC1497.244B3EB0"\r\n
\r\n
\r\n
------=_NextPart_001_00B9_01CC1497.244B3EB0\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
```

```
0340  0a 0d 0a 48 69 20 73 77  65 65 74 68 65 61 72 74   ···Hi sw eetheart
0350  21 20 42 72 69 6e 67 20  79 6f 75 72 20 66 61 6b   ! Bring  your fak
0360  65 20 70 61 73 73 70 6f  72 74 20 61 6e 64 20 61   e passpo rt and a
0370  20 62 61 74 68 69 6e 67  20 73 75 69 74 2e 20 41    bathing  suit. A
0380  64 64 72 65 73 73 20 3d  0d 0a 61 74 74 61 63 68   ddress = ··attach
0390  65 64 2e 20 6c 6f 76 65  2c 20 41 6e 6e 0d 0a 2d   ed. love , Ann··-
03a0  2d 2d 2d 2d 2d 3d 5f 4e  65 78 74 50 61 72 74 5f   -----=_N extPart_
03b0  30 30 31 5f 30 30 42 39  5f 30 31 43 43 31 34 39   001_00B9 _01CC149
03c0  37 2e 32 34 34 42 33 45  42 30 0d 0a 43 6f 6e 74   7.244B3E B0··Cont
03d0  65 6e 74 2d 54 79 70 65  3a 20 74 65 78 74 2f 68   ent-Type : text/h
03e0  74 6d 6c 3b 0d 0a 09 63  68 61 72 73 65 74 3d 22   tml;···c harset="
03f0  69 73 6f 2d 38 38 35 39  2d 31 22 0d 0a 43 6f 6e   iso-8859 -1"··Con
0400  74 65 6e 74 2d 54 72 61  6e 73 66 65 72 2d 45 6e   tent-Tra nsfer-En
0410  63 6f 64 69 6e 67 3a 20  71 75 6f 74 65 64 2d 70   coding:  quoted-p
0420  72 69 6e 74 61 62 6c 65  0d 0a 0d 0a 3c 21 44 4f   rintable ····<!DO
0430  43 54 59 50 45 20 48 54  4d 4c 20 50 55 42 4c 49   CTYPE HT ML PUBLI
0440  43 20 22 2d 2f 2f 57 33  43 2f 2f 44 54 44 20 48   C "-//W3 C//DTD H
0450  54 4d 4c 20 34 2e 30 20  54 72 61 6e 73 69 74 69   TML 4.0  Transiti
0460  6f 6e 61 6c 2f 2f 45 4e  22 3e 0d 0a 3c 48 54 4d   onal//EN ">··<HTM
0470  4c 3e 3c 48 45 41 44 3e  0d 0a 3c 4d 45 54 41 20   L><HEAD> ··<META 
0480  68 74 74 70 2d 65 71 75  69 76 3d 33 44 43 6f 6e   http-equ iv=3DCon
0490  74 65 6e 74 2d 54 79 70  65 20 63 6f 6e 74 65 6e   tent-Typ e conten
04a0  74 3d 33 44 22 74 65 78  74 2f 68 74 6d 6c 3b 20   t=3D"tex t/html; 
04b0  3d 0d 0a 63 68 61 72 73  65 74 3d 33 44 69 73 6f   =··chars et=3Diso
04c0  2d 38 38 35 39 2d 31 22  3e 0d 0a 3c 4d 45 54 41   -8859-1" >··<META
04d0  20 63 6f 6e 74 65 6e 74  3d 33 44 22 4d 53 48 54    content =3D"MSHT
04e0  4d 4c 20 36 2e 30 30 2e  32 39 30 30 2e 32 38 35   ML 6.00. 2900.285
04f0  33 22 20 6e 61 6d 65 3d  33 44 47 45 4e 45 52 41   3" name= 3DGENERA
0500  54 4f 52 3e 0d 0a 3c 53  54 59 4c 45 3e 3c 2f 53   TOR>··<S TYLE></S
0510  54 59 4c 45 3e 0d 0a 3c  2f 48 45 41 44 3e 0d 0a   TYLE>··< /HEAD>··
0520  3c 42 4f 44 59 20 62 67  43 6f 6c 6f 72 3d 33 44   <BODY bg Color=3D
0530  23 66 66 66 66 66 66 3e  0d 0a 3c 44 49 56 3e 3c   #ffffff> ··<DIV><
0540  46 4f 4e 54 20 66 61 63  65 3d 33 44 41 72 69 61   FONT fac e=3DAria
0550  6c 20 73 69 7a 65 3d 33  44 32 3e 48 69 20 73 77   l size=3 D2>Hi sw
0560  65 65 74 68 65 61 72 74  21 20 42 72 69 6e 67 20   eetheart ! Bring
```



Frame nr.	Source host	Destination host	From	To
1590	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	64.12.168.40 (Linux)	"Ann Dercover" <sneakyg33ky@aol.com>	<inter0pt1c@aol.com>
1752	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	64.12.168.40 (Linux)	"Ann Dercover" <sneakyg33ky@aol.com>	<d4rktangent@gmail.com>
2136	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	64.12.168.40 (Linux)	"Ann Dercover" <sneakyg33ky@aol.com>	<mistersekritx@aol.com>

Attribute	Value
Message-ID	<00bc01cc14c9$6fd1bc60$6b1ea8c0@annlaptop>
From	"Ann Dercover" <sneakyg33ky@aol.com>
To	<mistersekritx@aol.com>
Subject	rendezvous
Date	Tue, 17 May 2011 13:34:26 -0600

Windows-1252 Western European (Windows)

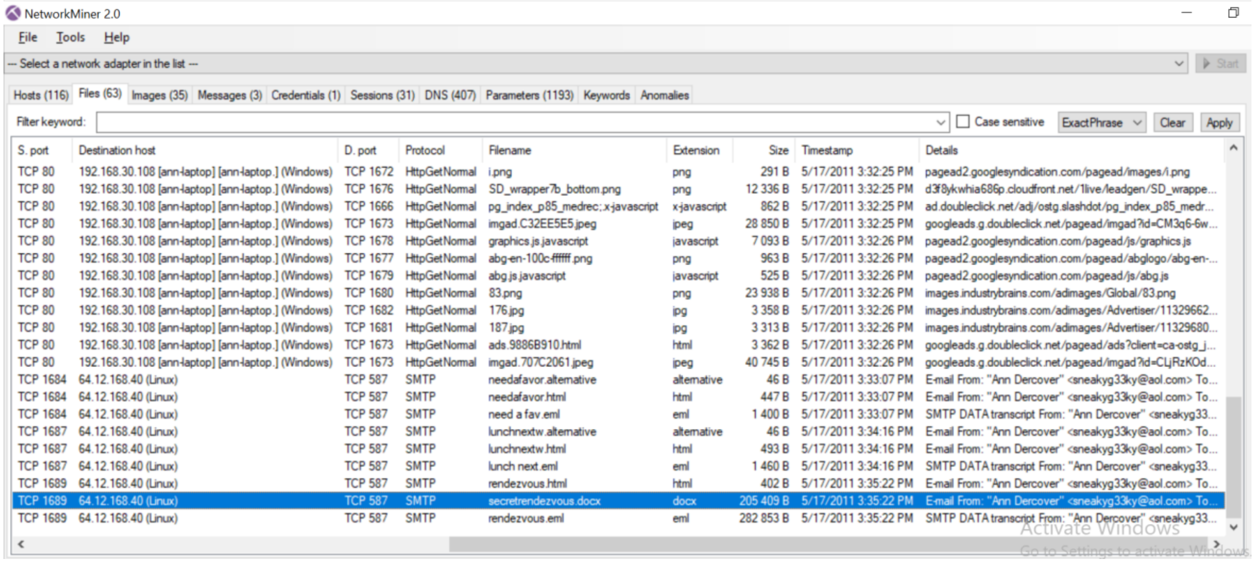
Hi sweetheart! Bring your fake passport and a bathing suit. Address attached. love, Ann

Attachement	Size
rendezvous.html	402 B
secretrendezvous.docx	205 409 B
rendezvous.eml	282 853 B

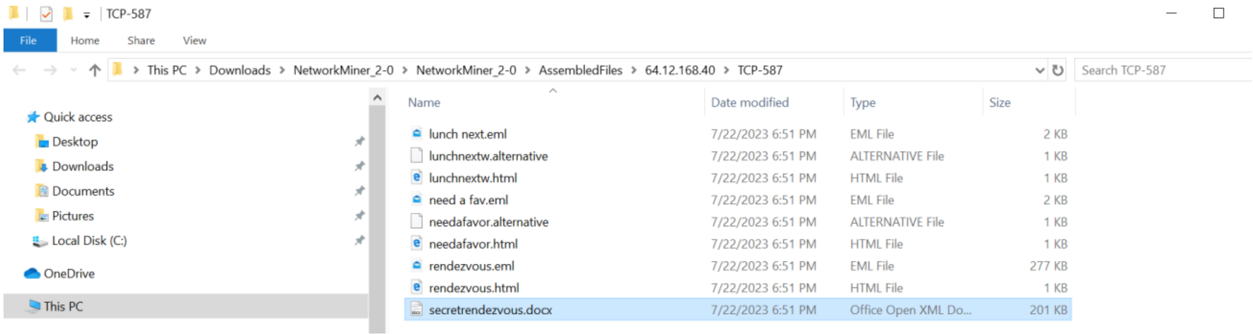
4. If Ann transferred or received any files of interest, recover them.

➢ To recover files transmitted over email, I have used the networkminer tool. To open the ‘evidence-packet-analysis.pcap’ file in Networkminer click on File → Open and select .pcap file from the mentioned folder. Now click on File tab to view details about file transferred.

As per the details provided in tool, User Ann has sent file ‘secretrendezvous.docx’ from the email address "Ann Dercover" sneakyg33ky@aol.com to the email address mistersekritx@aol.com which might contain some information. [2]



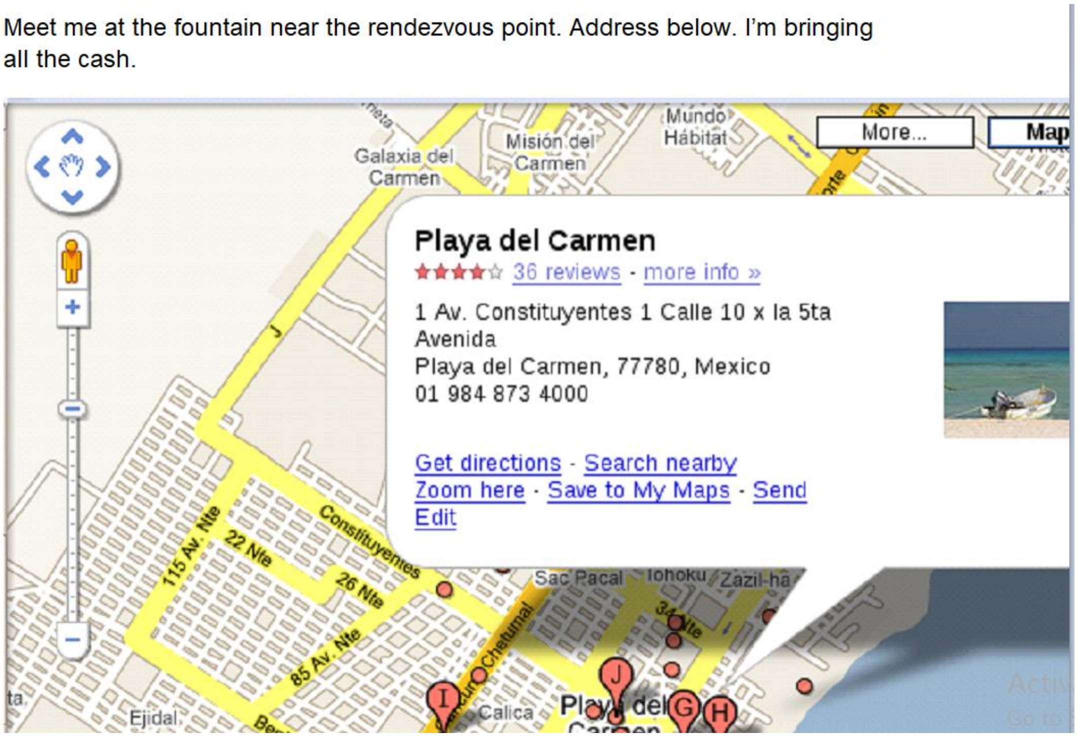
S. port	Destination host	D. port	Protocol	Filename	Extension	Size	Timestamp	Details
TCP 80	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	TCP 1672	HttpGetNormal	i.png	png	291 B	5/17/2011 3:32:25 PM	pagead2.googlesyndication.com/pagead/images/i.png
TCP 80	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	TCP 1676	HttpGetNormal	SD_wrapper7b_bottom.png	png	12 336 B	5/17/2011 3:32:25 PM	d3f8ykwhia686p.cloudfront.net/1live/leadgen/SD_wrappe...
TCP 80	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	TCP 1666	HttpGetNormal	pg_index_p85_medrec;.x-javascript	x-javascript	862 B	5/17/2011 3:32:25 PM	ad.doubleclick.net/adj/ostg.slashdot/pg_index_p85_medr...
TCP 80	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	TCP 1673	HttpGetNormal	imgad.C32EE5E5.jpeg	jpeg	28 850 B	5/17/2011 3:32:25 PM	googleads.g.doubleclick.net/pagead/imgad?id=CM3q6-6w...
TCP 80	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	TCP 1678	HttpGetNormal	graphics.js.javascript	javascript	7 093 B	5/17/2011 3:32:26 PM	pagead2.googlesyndication.com/pagead/js/graphics.js
TCP 80	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	TCP 1677	HttpGetNormal	abg-en-100c-ffffff.png	png	963 B	5/17/2011 3:32:26 PM	pagead2.googlesyndication.com/pagead/abglogo/abg-en-...
TCP 80	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	TCP 1679	HttpGetNormal	abg.js.javascript	javascript	525 B	5/17/2011 3:32:26 PM	pagead2.googlesyndication.com/pagead/js/abg.js
TCP 80	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	TCP 1680	HttpGetNormal	83.png	png	23 938 B	5/17/2011 3:32:26 PM	images.industrybrains.com/adimages/Global/83.png
TCP 80	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	TCP 1682	HttpGetNormal	176.jpg	jpg	3 358 B	5/17/2011 3:32:26 PM	images.industrybrains.com/adimages/Advertiser/11329662...
TCP 80	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	TCP 1681	HttpGetNormal	187.jpg	jpg	3 313 B	5/17/2011 3:32:26 PM	images.industrybrains.com/adimages/Advertiser/11329680...
TCP 80	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	TCP 1673	HttpGetNormal	ads.9886B910.html	html	3 362 B	5/17/2011 3:32:26 PM	googleads.g.doubleclick.net/pagead/ads?client=ca-ostg_j...
TCP 80	192.168.30.108 [ann-laptop] [ann-laptop.] (Windows)	TCP 1673	HttpGetNormal	imgad.707C2061.jpeg	jpeg	40 745 B	5/17/2011 3:32:26 PM	googleads.g.doubleclick.net/pagead/imgad?id=CLjRzKOd...
TCP 1684	64.12.168.40 (Linux)	TCP 587	SMTP	needafavor.alternative	alternative	46 B	5/17/2011 3:33:07 PM	E-mail From: "Ann Dercover" <sneakyg33ky@aol.com> To...
TCP 1684	64.12.168.40 (Linux)	TCP 587	SMTP	needafavor.html	html	447 B	5/17/2011 3:33:07 PM	E-mail From: "Ann Dercover" <sneakyg33ky@aol.com> To...
TCP 1684	64.12.168.40 (Linux)	TCP 587	SMTP	need a fav.eml	eml	1 400 B	5/17/2011 3:33:07 PM	SMTP DATA transcript From: "Ann Dercover" <sneakyg33...
TCP 1687	64.12.168.40 (Linux)	TCP 587	SMTP	lunchnextw.alternative	alternative	46 B	5/17/2011 3:34:16 PM	E-mail From: "Ann Dercover" <sneakyg33ky@aol.com> To...
TCP 1687	64.12.168.40 (Linux)	TCP 587	SMTP	lunchnextw.html	html	493 B	5/17/2011 3:34:16 PM	E-mail From: "Ann Dercover" <sneakyg33ky@aol.com> To...
TCP 1687	64.12.168.40 (Linux)	TCP 587	SMTP	lunch next.eml	eml	1 460 B	5/17/2011 3:34:16 PM	SMTP DATA transcript From: "Ann Dercover" <sneakyg33...
TCP 1689	64.12.168.40 (Linux)	TCP 587	SMTP	rendezvous.html	html	402 B	5/17/2011 3:35:22 PM	E-mail From: "Ann Dercover" <sneakyg33ky@aol.com> To...
TCP 1689	64.12.168.40 (Linux)	TCP 587	SMTP	secretrendezvous.docx	docx	205 409 B	5/17/2011 3:35:22 PM	E-mail From: "Ann Dercover" <sneakyg33ky@aol.com> To...
TCP 1689	64.12.168.40 (Linux)	TCP 587	SMTP	rendezvous.eml	eml	282 853 B	5/17/2011 3:35:22 PM	SMTP DATA transcript From: "Ann Dercover" <sneakyg33...



Name	Date modified	Type	Size
lunch next.eml	7/22/2023 6:51 PM	EML File	2 KB
lunchnextw.alternative	7/22/2023 6:51 PM	ALTERNATIVE File	1 KB
lunchnextw.html	7/22/2023 6:51 PM	HTML File	1 KB
need a fav.eml	7/22/2023 6:51 PM	EML File	2 KB
needafavor.alternative	7/22/2023 6:51 PM	ALTERNATIVE File	1 KB
needafavor.html	7/22/2023 6:51 PM	HTML File	1 KB
rendezvous.eml	7/22/2023 6:51 PM	EML File	277 KB
rendezvous.html	7/22/2023 6:51 PM	HTML File	1 KB
secretrendezvous.docx	7/22/2023 6:51 PM	Office Open XML Do...	201 KB

5. Are there any indications of Ann’s physical whereabouts? If so, provide supporting evidence.

- ➢ Now open the file location of file secretrendezvous.docx. We can see the location of Ann in the image containing address and map location.



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

Playa del Carmen

★★★★☆ 36 reviews - more info »

1 Av. Constituyentes 1 Calle 10 x la 5ta Avenida
Playa del Carmen, 77780, Mexico
01 984 873 4000

Get directions - Search nearby
Zoom here - Save to My Maps - Send
Edit

Citations –

1. Kumari, S. (2023, March 17). TryHackMe Wireshark Traffic Analysis Write-up Part 2. Medium. https://medium.com/@kumarishefu.4507/try-hack-me-wireshark-traffic-analysis-write-up-part-2-11d299b504f3
2. Hjelmvik, E. (2019, November 20). Intro to NetworkMiner. Weberblog. https://weberblog.net/intro-to-networkminer/
3. lastbitcoder. (2022, October 27). DHCP/BOOTP Statistics in Wireshark. GeeksforGeeks. https://www.geeksforgeeks.org/dhcp-bootp-statistics-in-wireshark/
4. QACafe. (n.d.). Search on Any Frame in a Capture. QA Cafe. https://www.qacafe.com/resources/search-on-any-frame-in-a-capture/#:~:text=The%20%E2%80%9Cframe%20contains%E2%80%9D%20filter%20will,%E2%80%9Ccloudshark%E2%80%9D%20somewhere%20in%20them.