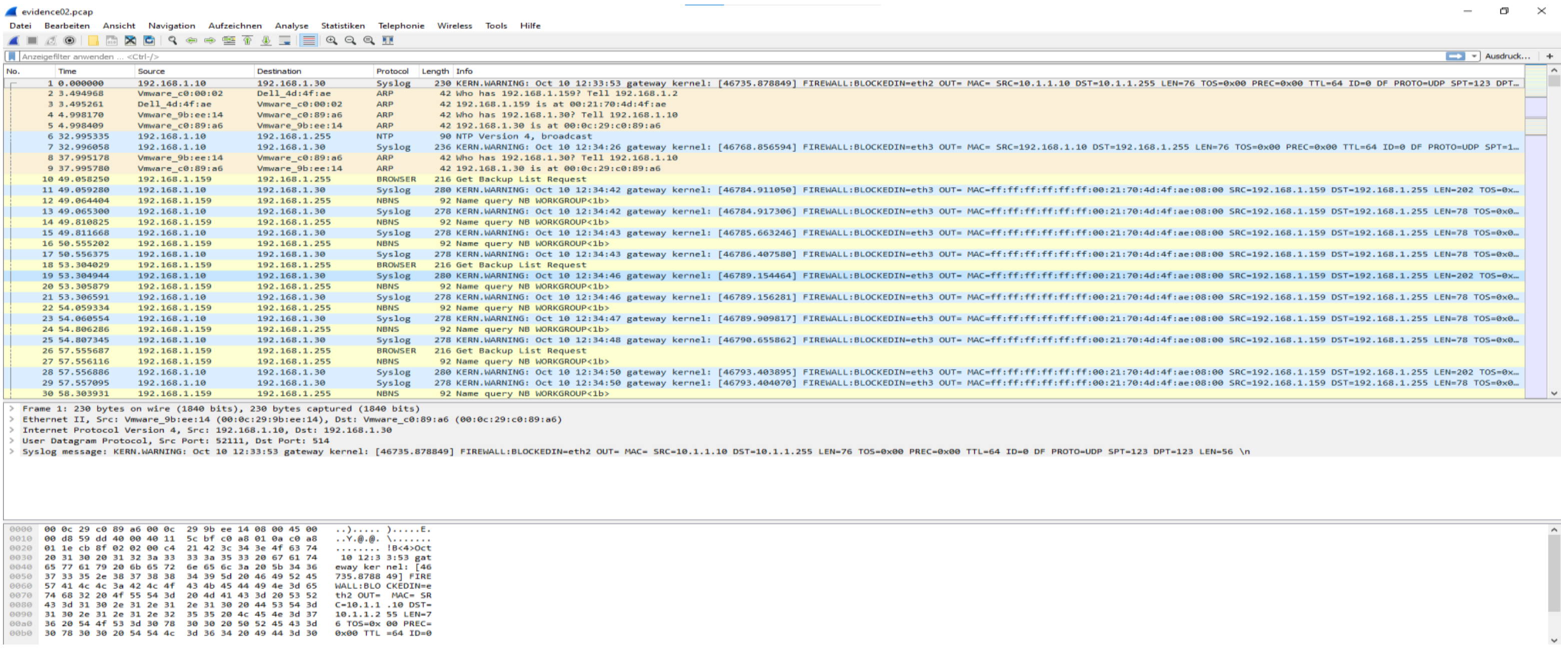
Agency challenge

Areeb Hussain

After downloading the pcap file from moodle, I opened up the file in **wire shark,** which shows us the list of all the network connections that have been captured. Then I started checking tcp streams to look for clues.



evidence02.pcap
Datei Bearbeiten Ansicht Navigation Aufzeichnen Analyse Statistiken Telephonie Wireless Tools Hilfe
Anzeigefilter anwenden ... <Ctrl-/>
Ausdruck...

```
No.   Time         Source             Destination       Protocol  Length Info
    1 0.000000     192.168.1.10       192.168.1.30      Syslog     230 KERN.WARNING: Oct 10 12:33:53 gateway kernel: [46735.878849] FIREWALL:BLOCKEDIN=eth2 OUT= MAC= SRC=10.1.1.10 DST=10.1.1.255 LEN=76 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=123 DPT…
    2 3.494968     Vmware_c0:00:02    Dell_4d:4f:ae     ARP         42 Who has 192.168.1.159? Tell 192.168.1.2
    3 3.495261     Dell_4d:4f:ae      Vmware_c0:00:02   ARP         42 192.168.1.159 is at 00:21:70:4d:4f:ae
    4 4.998170     Vmware_9b:ee:14    Vmware_c0:89:a6   ARP         42 Who has 192.168.1.30? Tell 192.168.1.10
    5 4.998409     Vmware_c0:89:a6    Vmware_9b:ee:14   ARP         42 192.168.1.30 is at 00:0c:29:c0:89:a6
    6 32.995335    192.168.1.10       192.168.1.255     NTP         90 NTP Version 4, broadcast
    7 32.996058    192.168.1.10       192.168.1.30      Syslog     236 KERN.WARNING: Oct 10 12:34:26 gateway kernel: [46768.856594] FIREWALL:BLOCKEDIN=eth3 OUT= MAC= SRC=192.168.1.10 DST=192.168.1.255 LEN=76 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=1…
    8 37.995178    Vmware_9b:ee:14    Vmware_c0:89:a6   ARP         42 Who has 192.168.1.30? Tell 192.168.1.10
    9 37.995780    Vmware_c0:89:a6    Vmware_9b:ee:14   ARP         42 192.168.1.30 is at 00:0c:29:c0:89:a6
   10 49.058250    192.168.1.159      192.168.1.255     BROWSER    216 Get Backup List Request
   11 49.059280    192.168.1.10       192.168.1.30      Syslog     280 KERN.WARNING: Oct 10 12:34:42 gateway kernel: [46784.911050] FIREWALL:BLOCKEDIN=eth3 OUT= MAC=ff:ff:ff:ff:ff:ff:00:21:70:4d:4f:ae:08:00 SRC=192.168.1.159 DST=192.168.1.255 LEN=202 TOS=0x…
   12 49.064404    192.168.1.159      192.168.1.255     NBNS        92 Name query NB WORKGROUP<1b>
   13 49.065300    192.168.1.10       192.168.1.30      Syslog     278 KERN.WARNING: Oct 10 12:34:42 gateway kernel: [46784.917306] FIREWALL:BLOCKEDIN=eth3 OUT= MAC=ff:ff:ff:ff:ff:ff:00:21:70:4d:4f:ae:08:00 SRC=192.168.1.159 DST=192.168.1.255 LEN=78 TOS=0x0…
   14 49.810825    192.168.1.159      192.168.1.255     NBNS        92 Name query NB WORKGROUP<1b>
   15 49.811668    192.168.1.10       192.168.1.30      Syslog     278 KERN.WARNING: Oct 10 12:34:43 gateway kernel: [46785.663246] FIREWALL:BLOCKEDIN=eth3 OUT= MAC=ff:ff:ff:ff:ff:ff:00:21:70:4d:4f:ae:08:00 SRC=192.168.1.159 DST=192.168.1.255 LEN=78 TOS=0x0…
   16 50.555202    192.168.1.159      192.168.1.255     NBNS        92 Name query NB WORKGROUP<1b>
   17 50.556375    192.168.1.10       192.168.1.30      Syslog     278 KERN.WARNING: Oct 10 12:34:43 gateway kernel: [46786.407580] FIREWALL:BLOCKEDIN=eth3 OUT= MAC=ff:ff:ff:ff:ff:ff:00:21:70:4d:4f:ae:08:00 SRC=192.168.1.159 DST=192.168.1.255 LEN=78 TOS=0x0…
   18 53.304029    192.168.1.159      192.168.1.255     BROWSER    216 Get Backup List Request
   19 53.304944    192.168.1.10       192.168.1.30      Syslog     280 KERN.WARNING: Oct 10 12:34:46 gateway kernel: [46789.154464] FIREWALL:BLOCKEDIN=eth3 OUT= MAC=ff:ff:ff:ff:ff:ff:00:21:70:4d:4f:ae:08:00 SRC=192.168.1.159 DST=192.168.1.255 LEN=202 TOS=0x…
   20 53.305879    192.168.1.159      192.168.1.255     NBNS        92 Name query NB WORKGROUP<1b>
   21 53.306591    192.168.1.10       192.168.1.30      Syslog     278 KERN.WARNING: Oct 10 12:34:46 gateway kernel: [46789.156281] FIREWALL:BLOCKEDIN=eth3 OUT= MAC=ff:ff:ff:ff:ff:ff:00:21:70:4d:4f:ae:08:00 SRC=192.168.1.159 DST=192.168.1.255 LEN=78 TOS=0x0…
   22 54.059334    192.168.1.159      192.168.1.255     NBNS        92 Name query NB WORKGROUP<1b>
   23 54.060554    192.168.1.10       192.168.1.30      Syslog     278 KERN.WARNING: Oct 10 12:34:47 gateway kernel: [46789.909817] FIREWALL:BLOCKEDIN=eth3 OUT= MAC=ff:ff:ff:ff:ff:ff:00:21:70:4d:4f:ae:08:00 SRC=192.168.1.159 DST=192.168.1.255 LEN=78 TOS=0x0…
   24 54.806286    192.168.1.159      192.168.1.255     NBNS        92 Name query NB WORKGROUP<1b>
   25 54.807345    192.168.1.10       192.168.1.30      Syslog     278 KERN.WARNING: Oct 10 12:34:48 gateway kernel: [46790.655862] FIREWALL:BLOCKEDIN=eth3 OUT= MAC=ff:ff:ff:ff:ff:ff:00:21:70:4d:4f:ae:08:00 SRC=192.168.1.159 DST=192.168.1.255 LEN=78 TOS=0x0…
   26 57.555687    192.168.1.159      192.168.1.255     BROWSER    216 Get Backup List Request
   27 57.556116    192.168.1.159      192.168.1.255     NBNS        92 Name query NB WORKGROUP<1b>
   28 57.556886    192.168.1.10       192.168.1.30      Syslog     280 KERN.WARNING: Oct 10 12:34:50 gateway kernel: [46793.403895] FIREWALL:BLOCKEDIN=eth3 OUT= MAC=ff:ff:ff:ff:ff:ff:00:21:70:4d:4f:ae:08:00 SRC=192.168.1.159 DST=192.168.1.255 LEN=202 TOS=0x…
   29 57.557095    192.168.1.10       192.168.1.30      Syslog     278 KERN.WARNING: Oct 10 12:34:50 gateway kernel: [46793.404070] FIREWALL:BLOCKEDIN=eth3 OUT= MAC=ff:ff:ff:ff:ff:ff:00:21:70:4d:4f:ae:08:00 SRC=192.168.1.159 DST=192.168.1.255 LEN=78 TOS=0x0…
   30 58.303931    192.168.1.159      192.168.1.255     NBNS        92 Name query NB WORKGROUP<1b>
```

```
> Frame 1: 230 bytes on wire (1840 bits), 230 bytes captured (1840 bits)
> Ethernet II, Src: Vmware_9b:ee:14 (00:0c:29:9b:ee:14), Dst: Vmware_c0:89:a6 (00:0c:29:c0:89:a6)
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.1.30
> User Datagram Protocol, Src Port: 52111, Dst Port: 514
> Syslog message: KERN.WARNING: Oct 10 12:33:53 gateway kernel: [46735.878849] FIREWALL:BLOCKEDIN=eth2 OUT= MAC= SRC=10.1.1.10 DST=10.1.1.255 LEN=76 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=123 DPT=123 LEN=56 \n
```

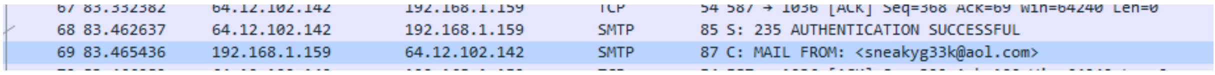
```
0000  00 0c 29 c0 89 a6 00 0c  29 9b ee 14 08 00 45 00   ..)..... ).....E.
0010  00 d8 59 dd 40 00 40 11  5c bf c0 a8 01 0a c0 a8   ..Y.@.@. \.......
0020  01 1e cb 8f 02 02 00 c4  21 42 3c 34 3e 4f 63 74   ........ !B<4>Oct
0030  20 31 30 20 31 32 3a 33  33 3a 35 33 20 67 61 74    10 12:3 3:53 gat
0040  65 77 61 79 20 6b 65 72  6e 65 6c 3a 20 5b 34 36   eway ker nel: [46
0050  37 33 35 2e 38 37 38 38  34 39 5d 20 46 49 52 45   735.8788 49] FIRE
0060  57 41 4c 4c 3a 42 4c 4f  43 4b 45 44 49 4e 3d 65   WALL:BLO CKEDIN=e
0070  74 68 32 20 4f 55 54 3d  20 4d 41 43 3d 20 53 52   th2 OUT=  MAC= SR
0080  43 3d 31 30 2e 31 2e 31  2e 31 30 20 44 53 54 3d   C=10.1.1 .10 DST=
0090  31 30 2e 31 2e 31 2e 32  35 35 20 4c 45 4e 3d 37   10.1.1.2 55 LEN=7
00a0  36 20 54 4f 53 3d 30 78  30 30 20 50 52 45 43 3d   6 TOS=0x 00 PREC=
00b0  30 78 30 30 20 54 54 4c  3d 36 34 20 49 44 3d 30   0x00 TTL =64 ID=0
```

Questions

1. What is Ann’s email address?

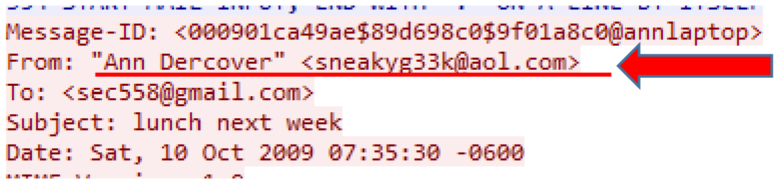
Answer: **sneakyg33k@aol.com**

Method: Filtered the data by SMTP, I found some email addresses in the info, which peeked my interest.



```
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>
```

Followed the tcp stream, The From: "Ann Dercover" section indicates sneakyg33k@aol.com which corresponds to Ann's email address.

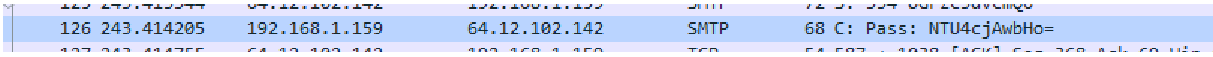


```
Message-ID: <000901ca49ae$89d698c0$9f01a8c0@annlaptop>
From: "Ann Dercover" <sneakyg33k@aol.com>
To: <sec558@gmail.com>
Subject: lunch next week
Date: Sat, 10 Oct 2009 07:35:30 -0600
```

2. What is Ann’s email password?

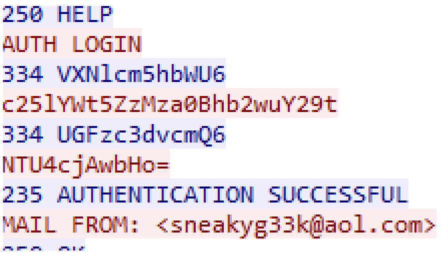
Answer: Ann’s email password is: **558r00lz**

Method: looking at the SMPT filtered data, I saw Pass: NTU4cjAwbHo=



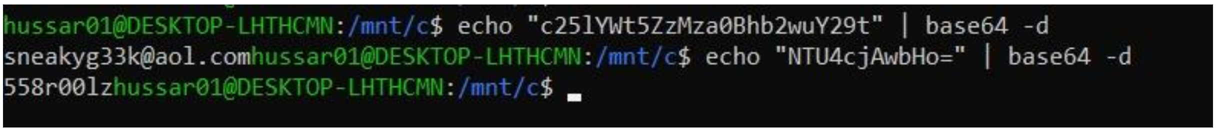
```
126 243.414205    192.168.1.159    64.12.102.142    SMTP    68 C: Pass: NTU4cjAwbHo=
```

Followed the tcp stream and found that the strings **“c25lYWt5ZzMza0Bhb2wuY29t**” and “**NTU4cjAwbHo=**” between AUTH LOGIN and DATA section contains Ann’s login credentials.



```
250 HELP
AUTH LOGIN
334 VXNlcm5hbWU6
c25lYWt5ZzMza0Bhb2wuY29t
334 UGFzc3dvcmQ6
NTU4cjAwbHo=
235 AUTHENTICATION SUCCESSFUL
MAIL FROM: <sneakyg33k@aol.com>
```

Then I decoded the string using **base64 –d** command in terminal.

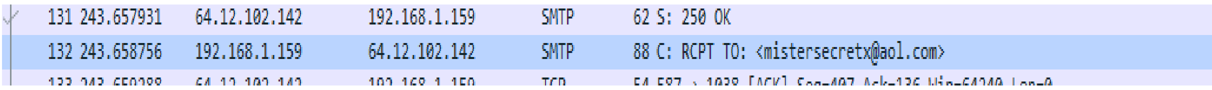


```
hussar01@DESKTOP-LHTHCMN:/mnt/c$ echo "c25lYWt5ZzMza0Bhb2wuY29t" | base64 -d
sneakyg33k@aol.comhussar01@DESKTOP-LHTHCMN:/mnt/c$ echo "NTU4cjAwbHo=" | base64 -d
558r00lzhussar01@DESKTOP-LHTHCMN:/mnt/c$
```

3. What is Ann’s secret lover’s email address?

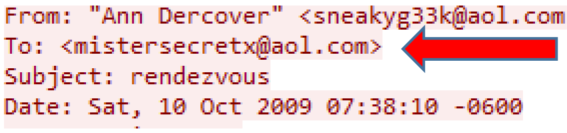
Answer: mistersecretx@aol.com

Method: Look through the data to find something hinting of a secret lover, I found



```
131 243.657931    64.12.102.142    192.168.1.159    SMTP    62 S: 250 OK
132 243.658756    192.168.1.159    64.12.102.142    SMTP    88 C: RCPT TO: <mistersecretx@aol.com>
```

Followed the tcp stream.

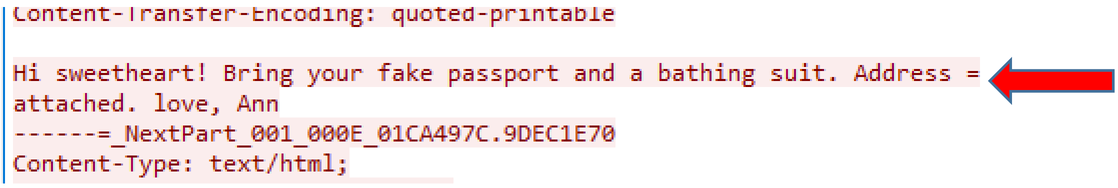


```
From: "Ann Dercover" <sneakyg33k@aol.com>
To: <mistersecretx@aol.com>
Subject: rendezvous
Date: Sat, 10 Oct 2009 07:38:10 -0600
```

4. What two items did Ann tell her secret lover to bring?

Answer: **passport and bathing suit**

Method: found in the same tcp stream under the content of the email.



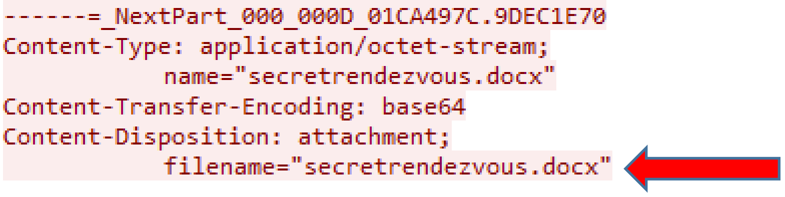
```
Content-Transfer-Encoding: quoted-printable

Hi sweetheart! Bring your fake passport and a bathing suit. Address =
attached. love, Ann
------=_NextPart_001_000E_01CA497C.9DEC1E70
Content-Type: text/html;
```

5. What is the NAME of the attachment Ann sent to her secret lover?

Answer: **secretendezvous.docx**

Method: found in the same tcp stream. From the content of the email Ann said, address is attached. So just scroll down to look for some kind of attachment.

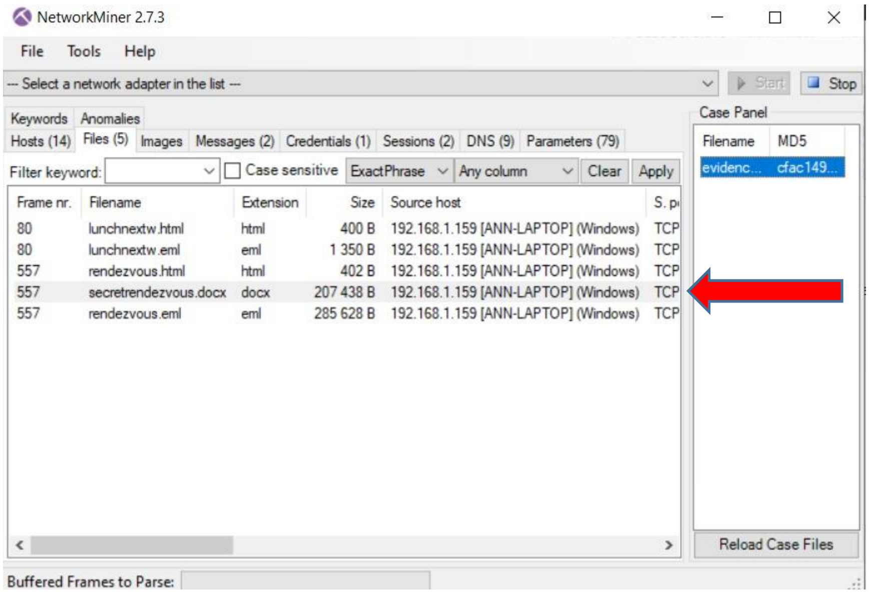


```
------=_NextPart_000_000D_01CA497C.9DEC1E70
Content-Type: application/octet-stream;
           name="secretrendezvous.docx"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
           filename="secretrendezvous.docx"
```

6. What is the MD5sum of the attachment Ann sent to her secret lover?

Answer: **MD5sum 9e423e11db88f01bbff81172839e1923**

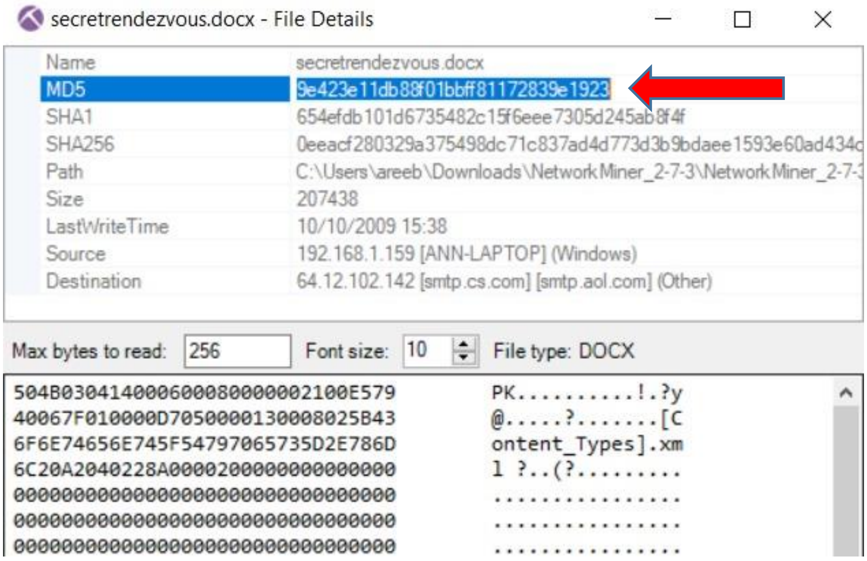
Method: To find the MD5Sum, I used a forensic tool called NetworkMiner. NetworkMiner can extract files, emails and certificates transferred over the network by parsing a PCAP file or by sniffing traffic directly from the network.



Frame nr.	Filename	Extension	Size	Source host	S. p
80	lunchnextw.html	html	400 B	192.168.1.159 [ANN-LAPTOP] (Windows)	TCP
80	lunchnextw.eml	eml	1 350 B	192.168.1.159 [ANN-LAPTOP] (Windows)	TCP
557	rendezvous.html	html	402 B	192.168.1.159 [ANN-LAPTOP] (Windows)	TCP
557	secretrendezvous.docx	docx	207 438 B	192.168.1.159 [ANN-LAPTOP] (Windows)	TCP
557	rendezvous.eml	eml	285 628 B	192.168.1.159 [ANN-LAPTOP] (Windows)	TCP

Filename	MD5
evidenc...	cfac149...

Simply double click on secretrendevouz.docx and it give the file details containing the MD5Sum.



secretrendezvous.docx - File Details

Name	secretrendezvous.docx
MD5	9e423e11db88f01bbff81172839e1923
SHA1	654efdb101d6735482c15f6eee7305d245ab8f4f
SHA256	0eeacf280329a375498dc71c837ad4d773d3b9bdaee1593e60ad434c
Path	C:\Users\areeb\Downloads\NetworkMiner_2-7-3\NetworkMiner_2-7-3
Size	207438
LastWriteTime	10/10/2009 15:38
Source	192.168.1.159 [ANN-LAPTOP] (Windows)
Destination	64.12.102.142 [smtp.cs.com] [smtp.aol.com] (Other)

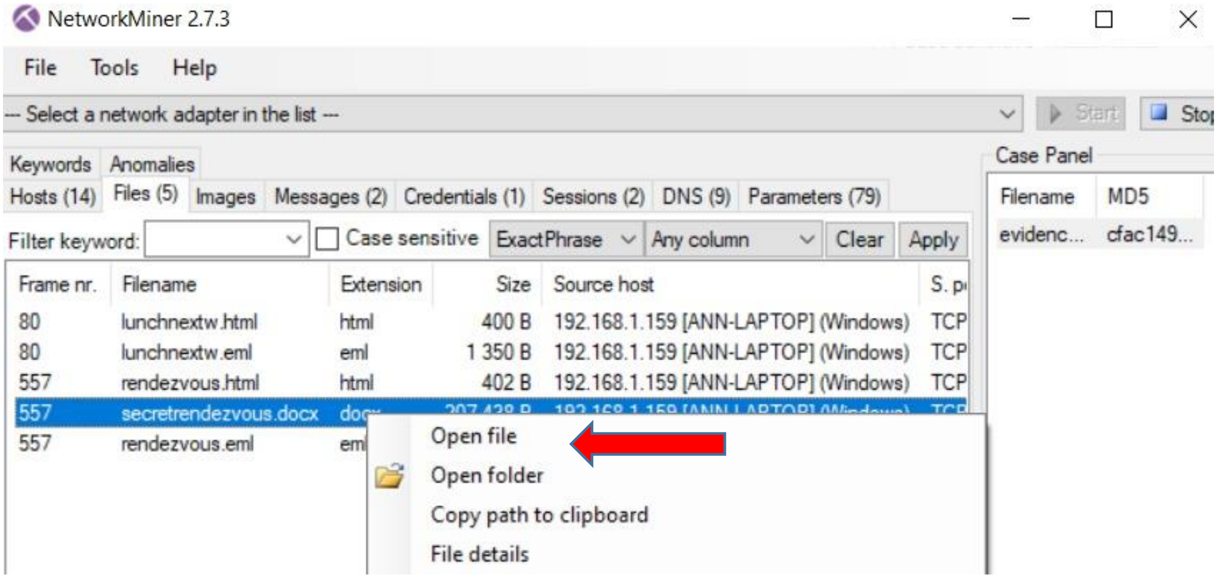
Max bytes to read: 256 Font size: 10 File type: DOCX

```
504B0304140006000800000021 00E579        PK..........!.?y
40067F010000D705000013000 8025B43        @.....?.......[C
6F6E74656E745F54797065735D2E786D        ontent_Types].xm
6C20A2040228A0002000000000000000        l ?..(?.........
00000000000000000000000000000000        ................
00000000000000000000000000000000        ................
00000000000000000000000000000000        ................
```

7. In what CITY and COUNTRY is their rendez-vous point?

Answer: **Playa Del Carmen, Mexico**

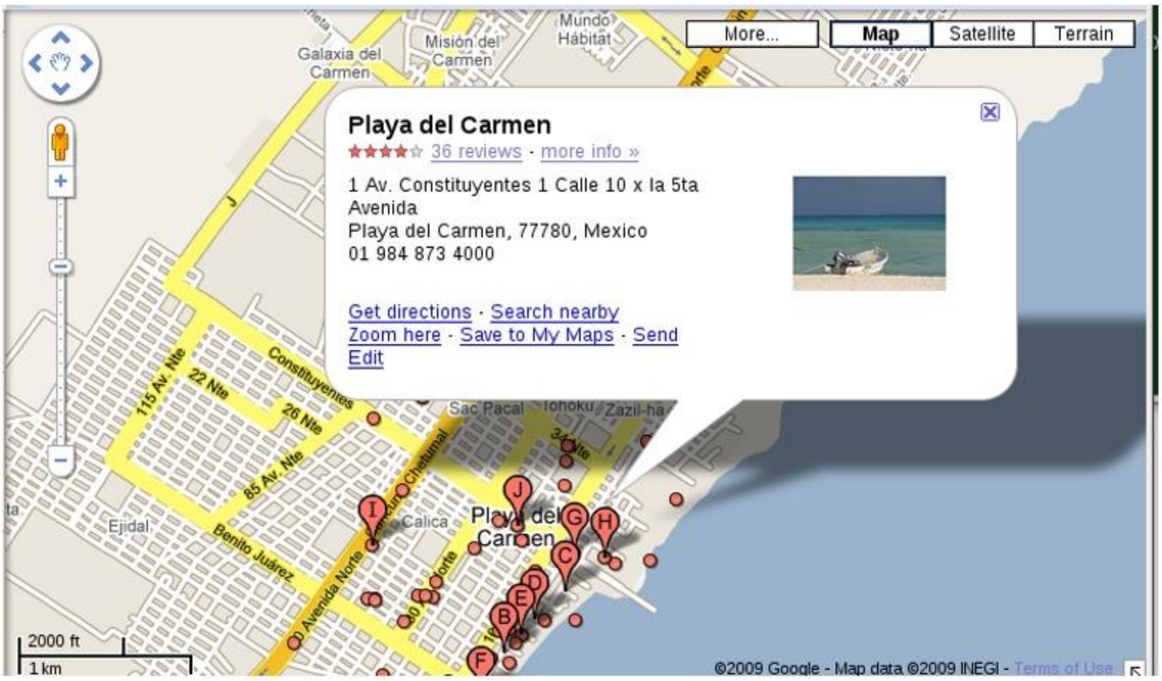
Method: using the same tool, right click on the secretrendesvouz.docx file to open the file. NetworkMiner opens the docx file in Microsoft word automatically.



Frame nr.	Filename	Extension	Size	Source host	S. p
80	lunchnextw.html	html	400 B	192.168.1.159 [ANN-LAPTOP] (Windows)	TCP
80	lunchnextw.eml	eml	1 350 B	192.168.1.159 [ANN-LAPTOP] (Windows)	TCP
557	rendezvous.html	html	402 B	192.168.1.159 [ANN-LAPTOP] (Windows)	TCP
557	secretrendezvous.docx	docx	207 438 B	192.168.1.159 [ANN-LAPTOP] (Windows)	TCP
557	rendezvous.eml	em			

Filename	MD5
evidenc...	cfac149...

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