

Lab 7 – Packet Capture Analysis

Sai Sasaank Srivatsa Pallerla

University of Maryland, Baltimore County

Presented to: Gina Scaldaferri

Date: 10/29/2019

About the Lab

Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible. It is used for network troubleshooting, analysis, software and communications, protocol development. It is one of the most famous tools that is used to monitor network traffic and protocols used. It lets us monitor the network at a microscopic level, both wired and wireless.

NetworkMiner is a Network Forensic Analysis Tool for Windows. NetworkMiner can be used as a passive network sniffer/packet capturing tool in order to detect operating systems, sessions, hostnames, open ports etc. without putting any traffic on the network. NetworkMiner can also parse pcap files for off-line analysis and to regenerate/reassemble transmitted files and certificates from pcap files. In contrast to other sniffers like Wireshark, NetworkMiner's display focuses on hosts and their attributes rather than raw packets.

In this lab we are provided with a fictitious scenario where Ann, possible perpetrator, is disappeared and we as forensic investigators are provided with a pcap that contains her last conversations and whereabouts. We are to analyze and extract as much information as possible about Ann from the network traffic and assist with the investigation.

Part 1. Packet Capture Analysis

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

The Alias that Ann used is sneakyg33, the corresponding email address is sneakyg33@aol.com and its password is s00pers3kr1t

The screenshot shows a Wireshark packet capture analysis of a network traffic file named 'evidence-packet-analysis.pcap'. The filter is set to 'tcp.stream eq 33'. The packet list shows several packets, with packet 2153 selected. The packet details pane shows the 'Internet Message Access Protocol' section, specifically the 'LOGIN' command. The request is: 'oB6 LOGIN "sneakyg33@aol.com" "s00pers3kr1t"'. The packet bytes pane shows the raw data of the packet, with the 'LOGIN' command and the email address 'sneakyg33@aol.com' highlighted. The status bar at the bottom indicates 'Packets: 2487 · Displayed: 337 (13.6%) · Load time: 0:0.99'.

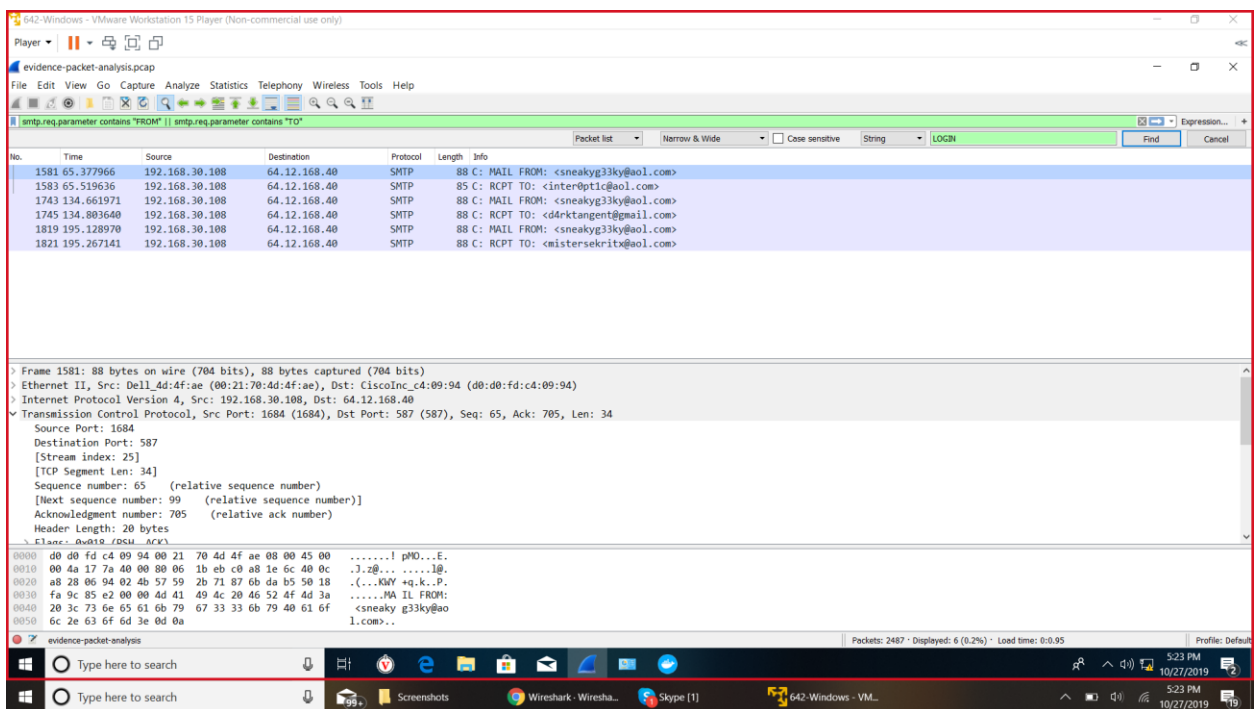
2. Who did Ann communicate with? Provide a list of email addresses and any other identifying information.

Ann was communicating with three users, namely – interOpt1@aol.com, d4rktangent@gmail.com, mistersekritx@aol.com

Filter used: smtp.req.parameter contains "FROM" || smtp.req.parameter contains "TO"

This filter. SMTP request parameters that contains the word FROM and TO, will analyze the whole pcap file for smtp, Simple Mail Transfer Protocol and display only the SMTP based traffic with the "MAIL FROM" and "RCPT TO" strings.

After applying the filter we can see that there are a total of 6 results which contains mail that were sent from sneakyg33@aol.com, Ann, to three different users – interOpt1@aol.com, d4rktangent@gmail.com, mistersekritx@aol.com.



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

Ann has three conversations with users, – interOpt1@aol.com, d4rktangent@gmail.com, mistersekritx@aol.com. The transcript of conversation can be extracted using Wireshark – TCP flow but Network Miner gives a more user-friendly interface to do the same. After uploading the pcap to Network Miner, choose 'message' tab to see any conversations, smtp, within the pcap. Clicking on each row will open the mail on the middle pane, which is more human readable.

Transcript of conversation with interOpt1@aol.com

The screenshot displays the NetworkMiner 2.0 application window. The interface includes a menu bar (File, Tools, Help), a toolbar, and a main workspace. The 'Messages' tab is active, showing a list of email messages. The selected message (Frame 1752) is displayed in the center pane, showing the email header and body. The email is from 'Ann Dercover' (caneaky33ky@aol.com) to 'interOpt1@aol.com' with the subject 'need a favor'. The body text reads: 'Hey, can you hook me up quick with that fake passport you were taking about? - Ann'. The right pane shows the 'Case Panel' with a list of files. The bottom status bar shows 'Live Sniffing Buffer Usage' and the system clock.

| Frame nr. | Source host | Destination host | From | To | Subject | Protocol |
|-----------|----------------|----------------------|--------------------------------------|-------------------------|--------------|----------|
| 1752 | 192.168.30.108 | 64.12.168.40 (Linux) | "Ann Dercover" <caneaky33ky@aol.com> | <interOpt1@aol.com> | need a favor | Smtp |
| 2136 | 192.168.30.108 | 64.12.168.40 (Linux) | "Ann Dercover" <caneaky33ky@aol.com> | <mistersekritx@aol.com> | rendevous | Smtp |

Attribute Value

Message-ID <00ab01cc14c982275e6009b-1ea8c0@amrlaptop>

From "Ann Dercover" <caneaky33ky@aol.com>

To <interOpt1@aol.com>

Subject need a favor

Date Tue, 17 May 2011 13:32:17 -0600

MIME-Version 1.0

Content-Type multipart/alternative

boundary -----_NextPart_000_00A8_01CC1496.D700DE30

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

charset iso-8859-1

Content-Transfer... quoted-printable

Windows-1252 Western European (Windows)

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

Attachment Size

need a favor alternative 46 B

need a favor.html 447 B

need a fav.xml 1 400 B

Transcript of conversation with d4rktangent@gmail.com

The screenshot shows the NetworkMiner 2.0 interface within a VMware Workstation 15 Player. The main window displays a list of captured network traffic. The selected item is frame 1752, which is an SMTP message. The details pane on the right shows the email's metadata and content.

| Frame nr. | Source host | Destination host | From | To | Subject | Protocol |
|-----------|----------------|----------------------|--------------------------------------|-------------------------|-----------------|----------|
| 1590 | 192.168.30.108 | 64.12.168.40 (Linux) | "Ann Dercover" <aneakyg33ky@aol.com> | <interqst1c@aol.com> | need a favor | Smtp |
| 1752 | 192.168.30.108 | 64.12.168.40 (Linux) | "Ann Dercover" <aneakyg33ky@aol.com> | <d4rktangent@gmail.com> | lunch next week | Smtp |
| 2136 | 192.168.30.108 | 64.12.168.40 (Linux) | "Ann Dercover" <aneakyg33ky@aol.com> | <mistersekritx@aol.com> | rendezvous | Smtp |

Message Details (Frame 1752):

- Message-ID: <00b701cc14c964bc957109b1ea8c0@amnlaptop>
- From: "Ann Dercover" <aneakyg33ky@aol.com>
- To: <d4rktangent@gmail.com>
- Subject: lunch next week
- Date: Tue, 17 May 2011 13:33:26 -0600
- MIME-Version: 1.0
- Content-Type: multipart/alternative
- boundary: -----_NextPart_000_0084_01CC1497.004EC040
- 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
- charset: iso-8859-1
- Content-Transfer-Encoding: quoted-printable

Message Content:

Windows-1252 Western European (Windows)

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

-Ann

Attachments:

| Attachment | Size |
|------------------------|---------|
| lunchnextw alternative | 46 B |
| lunchnextw.html | 493 B |
| lunch next.eml | 1 460 B |

Transcript of conversation with mistersekritx@aol.com

The screenshot shows the NetworkMiner 2.0 interface within a VMware Workstation 15 Player. The main window displays a list of captured network traffic. The selected item is frame 2136, which is an SMTP message. The details pane on the right shows the email's metadata and content.

| Frame nr. | Source host | Destination host | From | To | Subject | Protocol |
|-----------|----------------|----------------------|--------------------------------------|-------------------------|-----------------|----------|
| 1590 | 192.168.30.108 | 64.12.168.40 (Linux) | "Ann Dercover" <aneakyg33ky@aol.com> | <interqst1c@aol.com> | need a favor | Smtp |
| 1752 | 192.168.30.108 | 64.12.168.40 (Linux) | "Ann Dercover" <aneakyg33ky@aol.com> | <d4rktangent@gmail.com> | lunch next week | Smtp |
| 2136 | 192.168.30.108 | 64.12.168.40 (Linux) | "Ann Dercover" <aneakyg33ky@aol.com> | <mistersekritx@aol.com> | rendezvous | Smtp |

Message Details (Frame 2136):

- Message-ID: <00bc01cc14c999d1bc609b1ea8c0@amnlaptop>
- From: "Ann Dercover" <aneakyg33ky@aol.com>
- To: <mistersekritx@aol.com>
- Subject: rendezvous
- Date: Tue, 17 May 2011 13:34:26 -0600
- MIME-Version: 1.0
- Content-Type: multipart/mixed
- boundary: -----_NextPart_000_0084_01CC1497.24483EB0
- 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
- charset: iso-8859-1
- Content-Transfer-Encoding: quoted-printable

Message Content:

Windows-1252 Western European (Windows)

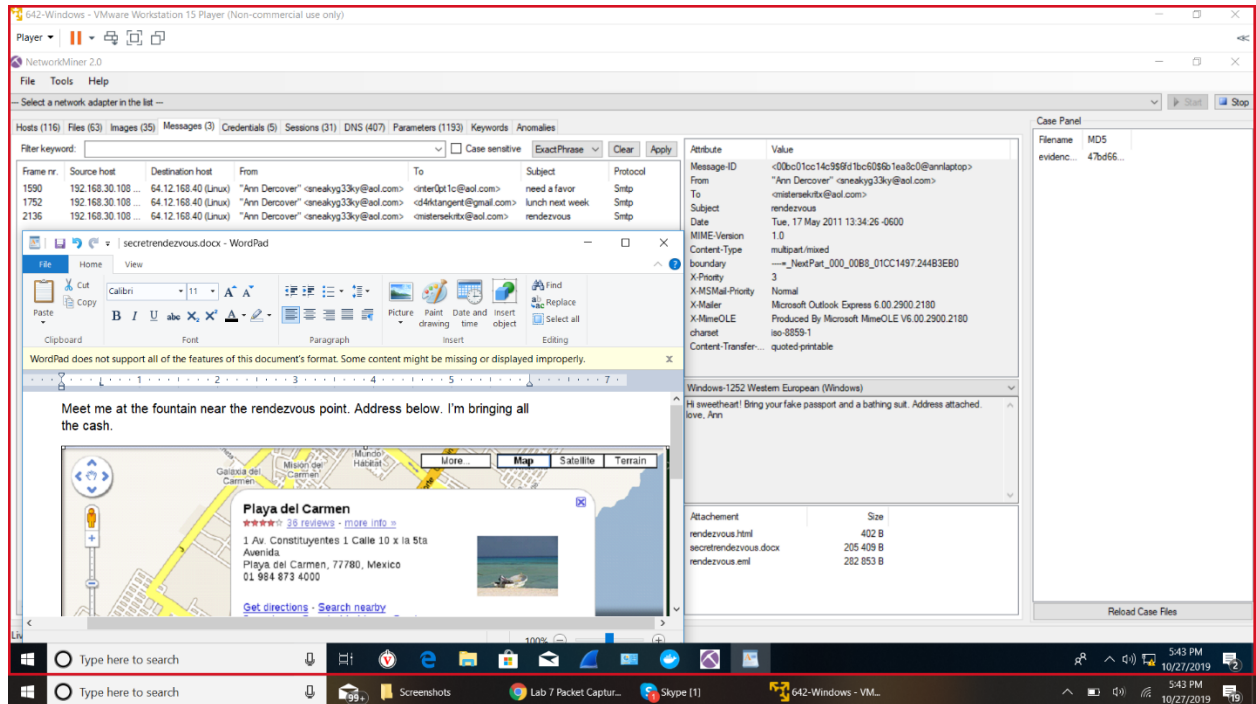
Hi sweetheart! Bring your fake passport and a bathing suit. Address attached. love, Ann

Attachments:

| Attachment | Size |
|-----------------------|-----------|
| rendezvous.html | 402 B |
| secretrendezvous.docx | 205 409 B |
| rendezvous.eml | 282 853 B |

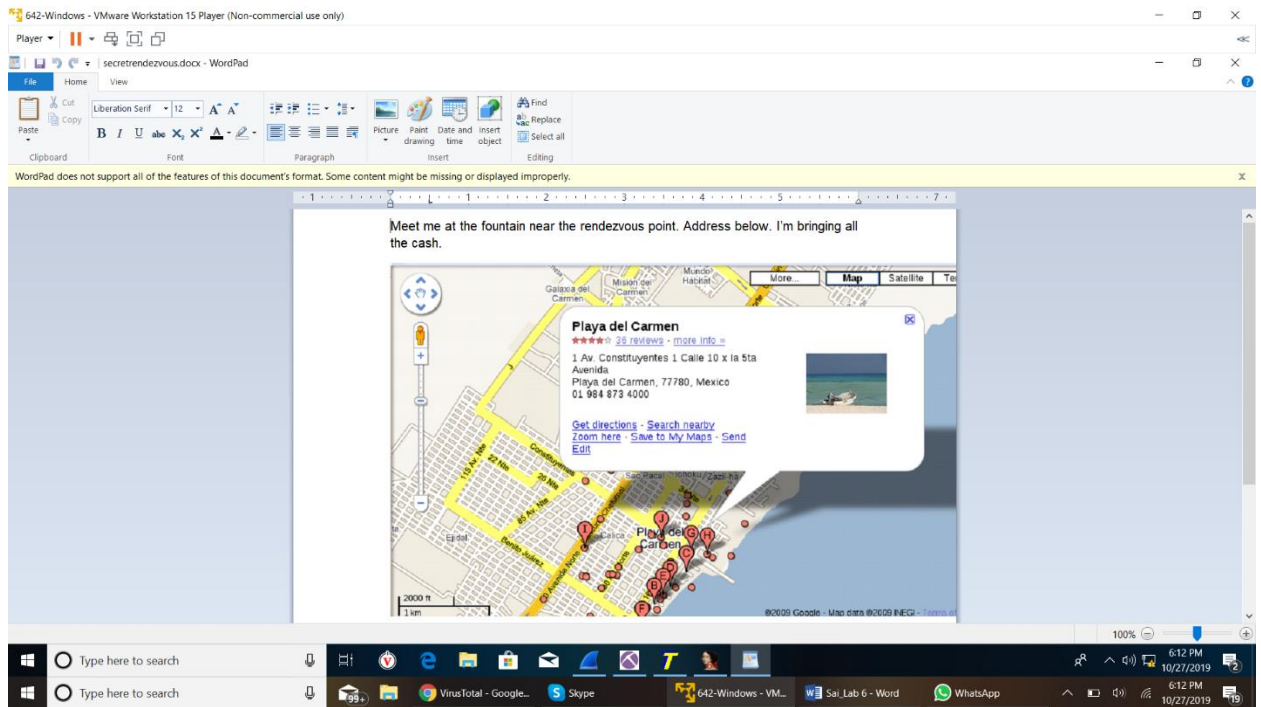
4. If Ann transferred or received any files of interest, recover them.

After uploading the pcap to Network Miner, choose 'message' tab to see any conversations, smtp, within the pcap. Clicking on each row will open the mail on the middle pain, which is more human readable. ON further examining the transcripts we can see the files that were sent by mail, this information is provided in the lower middle pain. We can see that in the conservation with mistersekritx@aol.com there is word document, .doc file, that has been sent from Ann. To recover it we simply right click on it, save it to desktop and open it.



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

The file that we extracted from the conversation with mistersekritx@aol.com has the location that ANN and Mr. X decide to meet which is Playa del Carmen, 777800, Mexico. We know this sure because of the mail's subject "rendezvous" and the content inside the document also said "Meet me near the fountain near rendezvous point"



Conclusion

From this lab we learn how to use Wireshark and Network Miner and how these forensic tools can help investigators solve cases. We also learn how to perform packet analysis to determine whether a malicious system was on the network and analyze network traffic and carve files from the packets to better understand what occurred on the network.

References

- [1] <https://wiki.wireshark.org/SMTP>
- [2] <https://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/>
- [3] https://www.wireshark.org/docs/wsug_html_chunked/ChAdvFollowStreamSection.html