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.

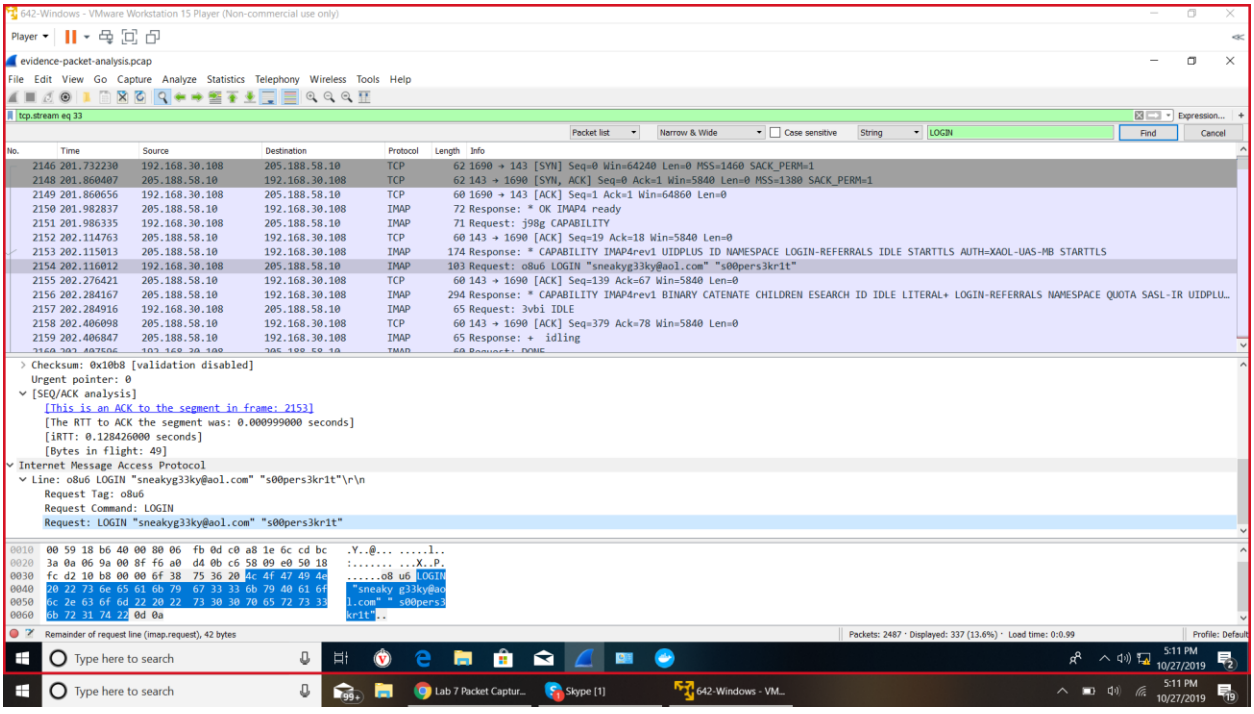
NetworkMiner is a Network Forensic Analysis Tool for Windows. NetworkMiner can be used as a passive network sniffer/packet capturing tool in order to detect operating systems, sessions, hostnames, open ports etc. without putting any traffic on the network. NetworkMiner can also parse pcap files for off-line 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 fictious scenario where Ann, possible perpetrator, is disappeared and we as forensic investigators are provided with a pacp 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



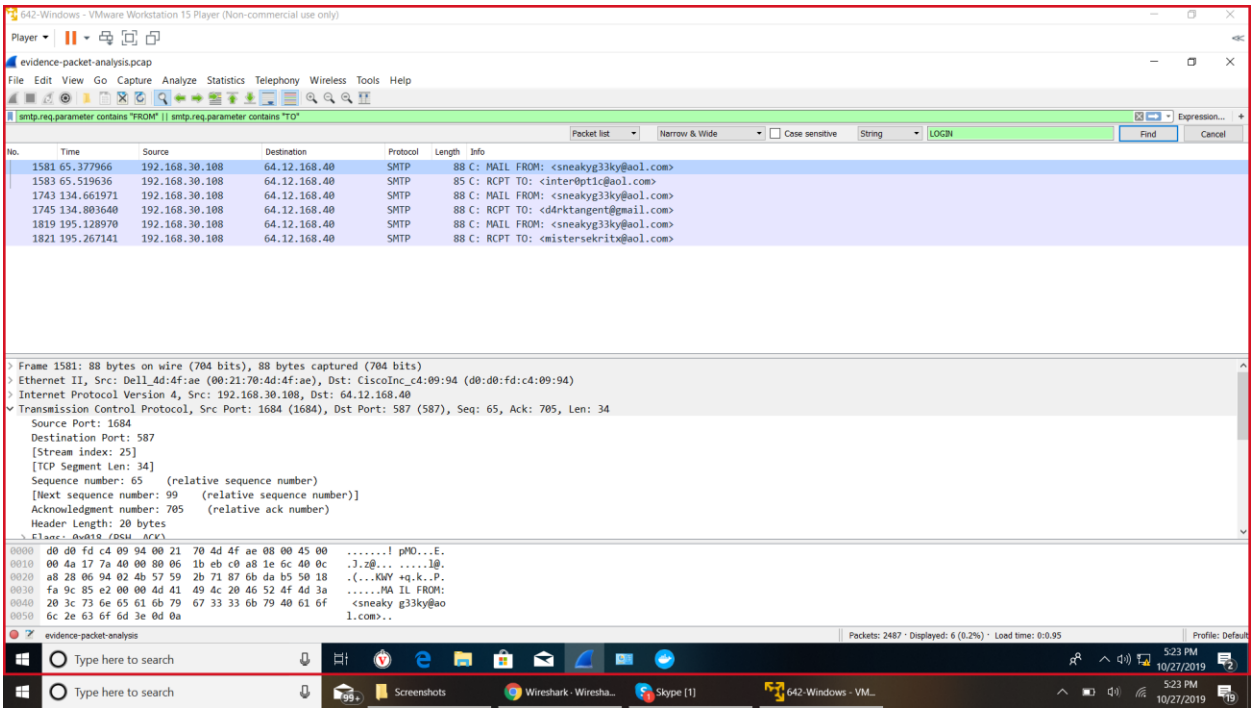
2. Who did Ann communicate with? Provide a list of email addresses and any other identifying information.

   Ann was communicating with three users, namely – inter0pt1@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.

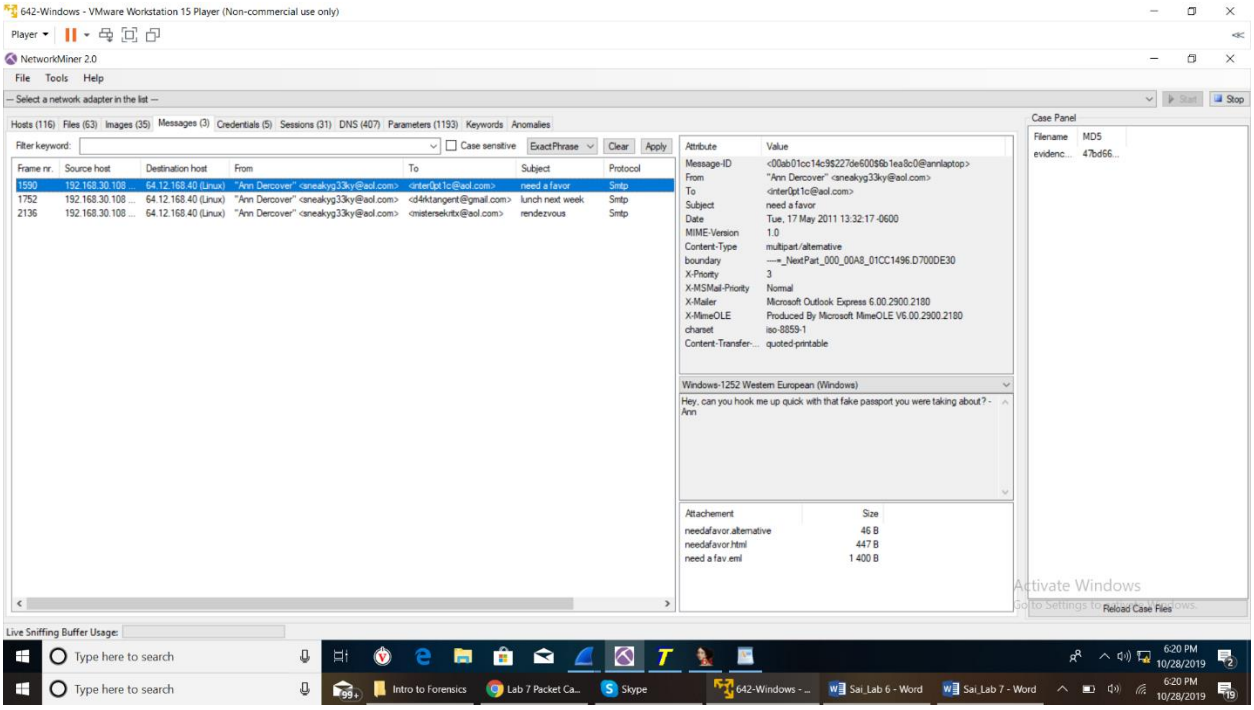
   After applying the filter we can see that there are a total of 6 results which contains mail that were sent from sneakyg33@aol.com, Ann, to three different users – inter0pt1@aol.com, d4rktangent@gmail.com, mistersekritx@aol.com.



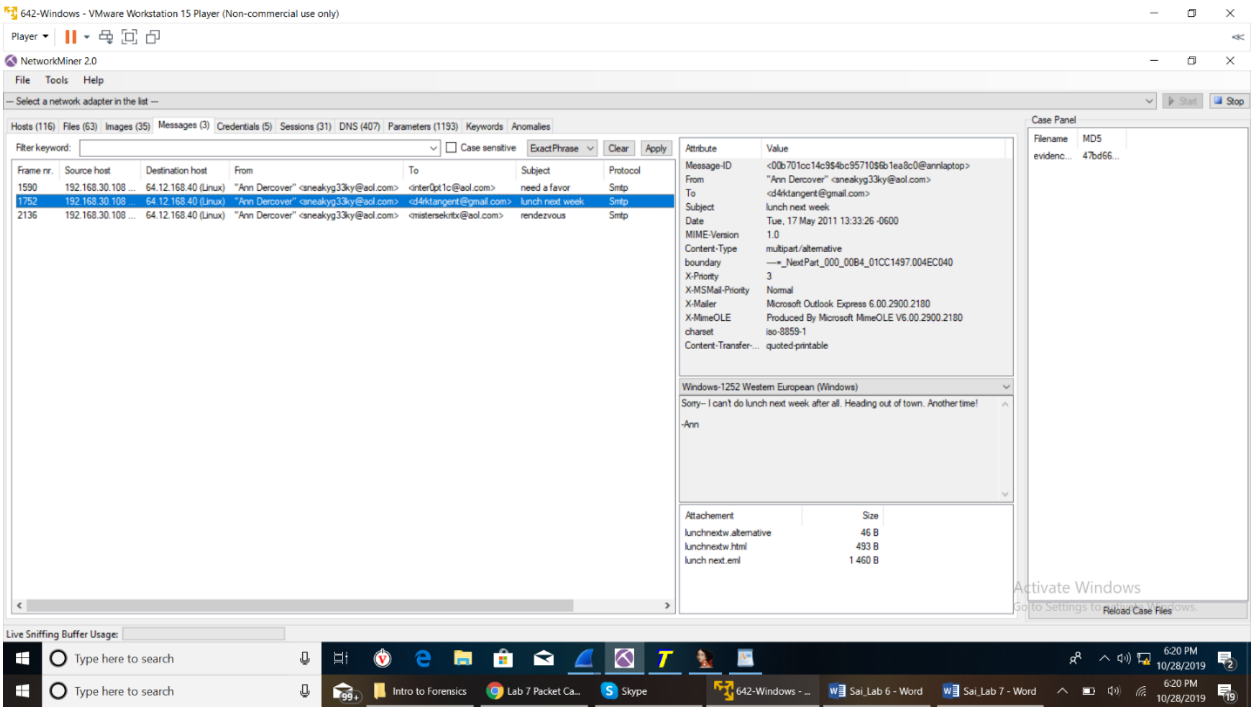
3. Extract any transcripts of Ann's conversations and present them to investigators.

   Ann has three conversation with users, – inter0pt1@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 pain, which is more human readable.

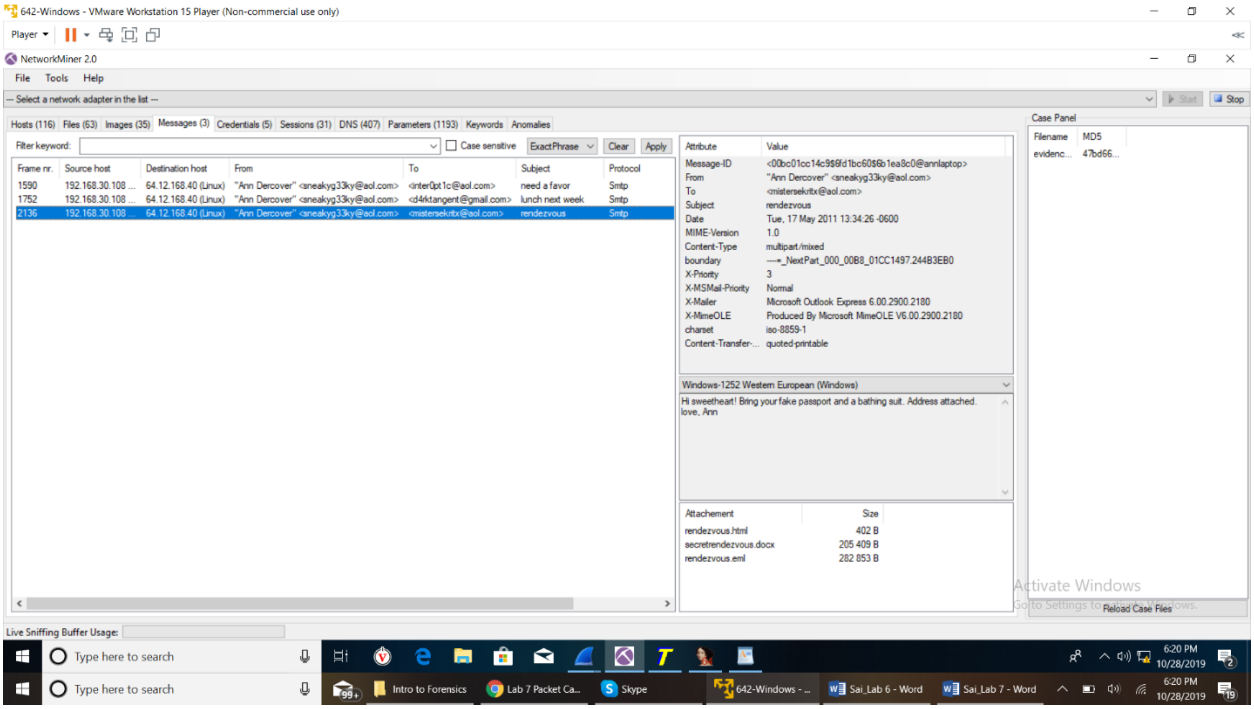
   Transcript of conversation with inter0pt1@aol.com



Transcript of conversation with d4rktangent@gmail.com

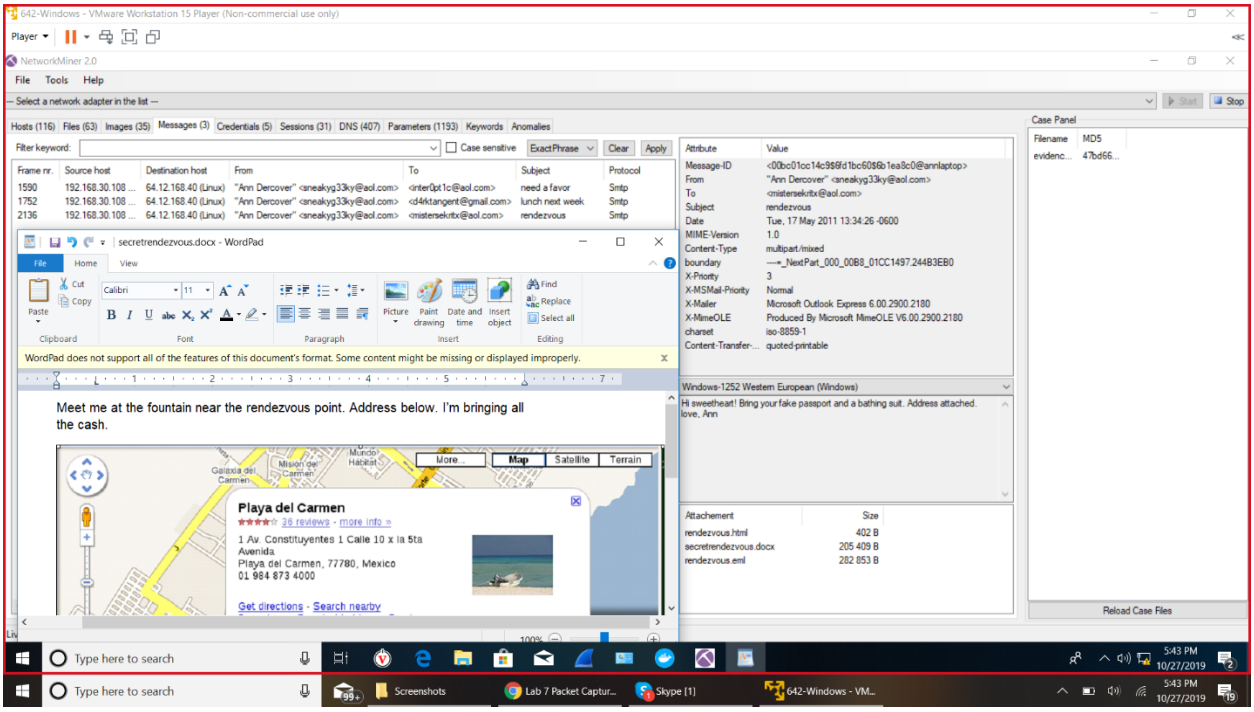


Transcript of conversation with mistersekritx@aol.com



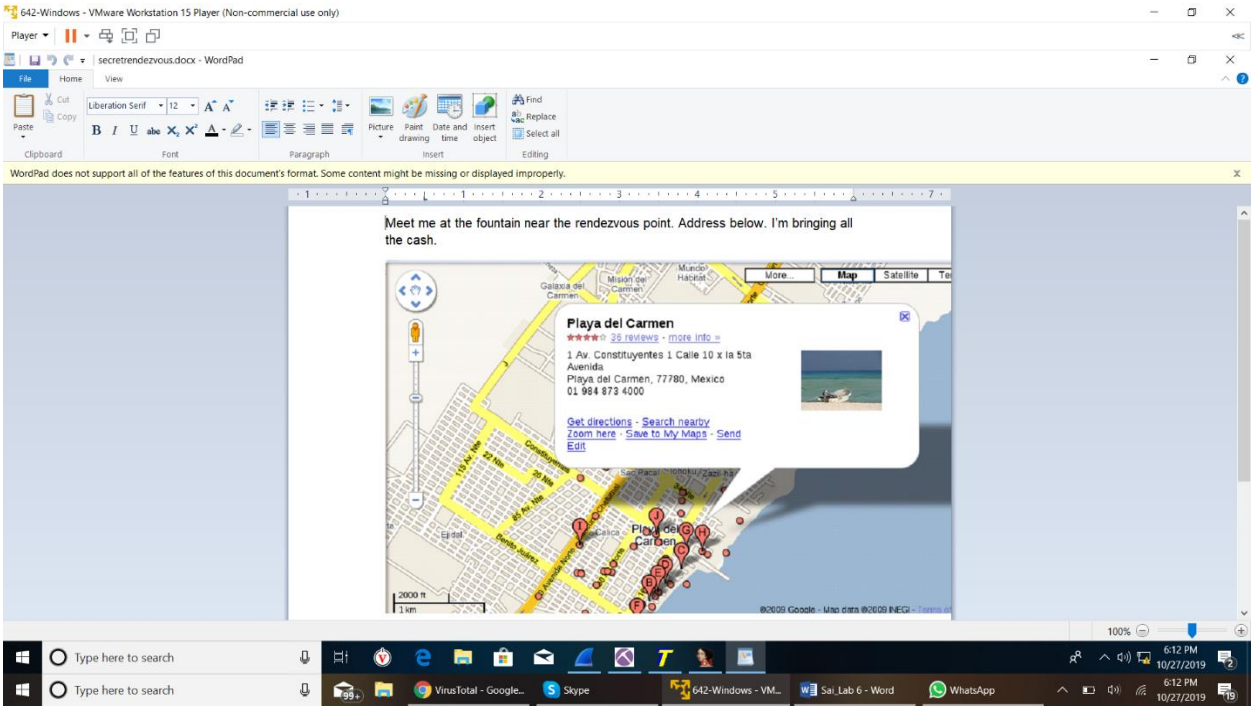
4. If Ann transferred or received any files of interest, recover them.

   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