Lab 01 – Wireshark Introduction

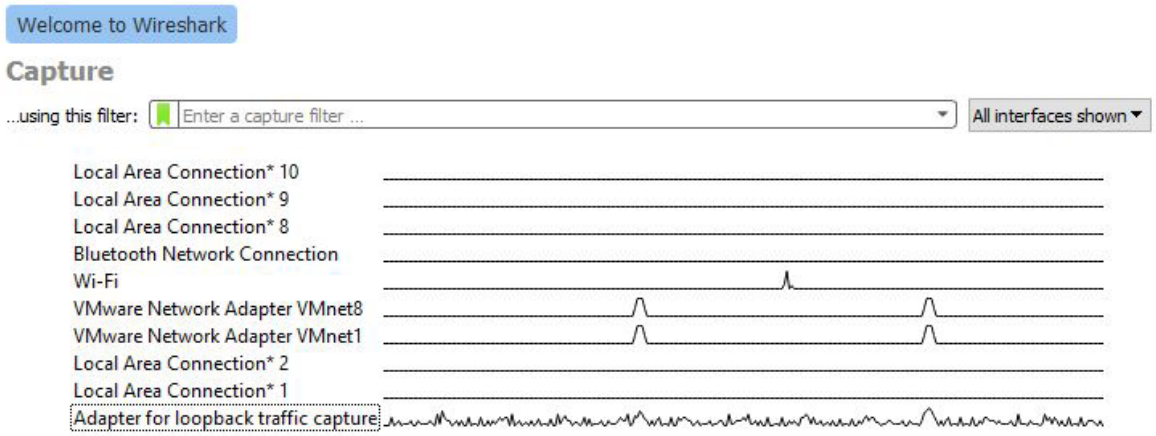
Author: Raymond Ng
Course Number/Section: IS 3413-006
Date: August 23, 2022

INTRODUCTION

The purpose of this lab was to provide the user with an introductory experience to open-source network protocol analyzers, specifically Wireshark. The lab went over basic functionality of Wireshark. Further, it allowed the user to experiment with capturing and examining data packets traveling over network connections.

PROCESS

Breakpoint 01: Below is a screenshot along with a description of my network card interfaces observed via Wireshark:



Observing my network card interfaces via Wireshark, I noticed no activity was detected for following interfaces:

- Local Area Connections
- Bluetooth Network Connection

This makes sense because I was not connected to the Internet via Ethernet, nor was I connected to a network via Bluetooth.

Further observation of my network interfaces, I noticed minimal/moderate activity was detected for the following interfaces:

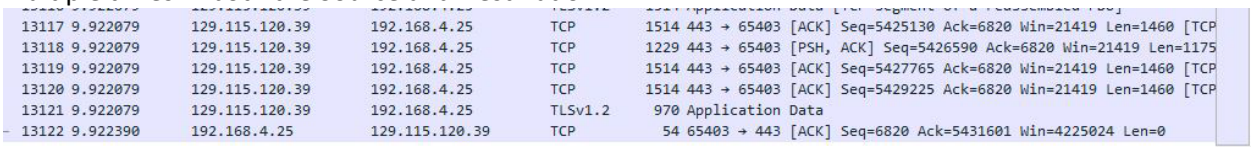
- Wi-Fi
- VMware Network Adapters

It made sense to me that activity would be detected for the Wi-Fi interface because my laptop was connected to the Internet on that medium, but I was surprised to see activity for VMware. However, I would assess the network adapter components of the VMware product maintain a degree of connectivity for product to remain connected to a network.

Lastly, I noticed there was a significant amount of activity for the "Adapter for loopback traffic capture." I was not sure what that component was, so I did a little bit of research to determine what it was and

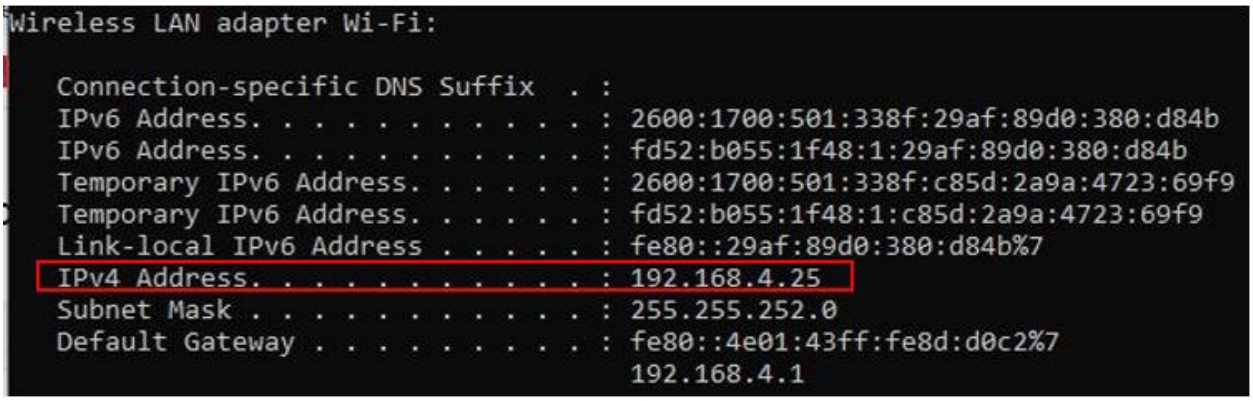
why there was activity. From wiki.wireshark.org, I found it was the component of Wireshark that captures network activity, and it made sense that it was an active component doing what it supposed to do, or I would not see any of the lines of activity depicted in my screenshot [1].

Breakpoint 02: Analyzing the IP addresses in the Packet List Pane I noticed `192.168.4.25` appeared multiple times in both the Source and Destination.



13117	9.922079	129.115.120.39	192.168.4.25	TCP	1514 443 → 65403 [ACK] Seq=5425130 Ack=6820 Win=21419 Len=1460 [TCP
13118	9.922079	129.115.120.39	192.168.4.25	TCP	1229 443 → 65403 [PSH, ACK] Seq=5426590 Ack=6820 Win=21419 Len=1175
13119	9.922079	129.115.120.39	192.168.4.25	TCP	1514 443 → 65403 [ACK] Seq=5427765 Ack=6820 Win=21419 Len=1460 [TCP
13120	9.922079	129.115.120.39	192.168.4.25	TCP	1514 443 → 65403 [ACK] Seq=5429225 Ack=6820 Win=21419 Len=1460 [TCP
13121	9.922079	129.115.120.39	192.168.4.25	TLSv1.2	970 Application Data
13122	9.922390	192.168.4.25	129.115.120.39	TCP	54 65403 → 443 [ACK] Seq=6820 Ack=5431601 Win=4225024 Len=0

I assess that 192.168.4.25 is my IP address. I went into the command prompt and executed `ipconfig` to validate it.

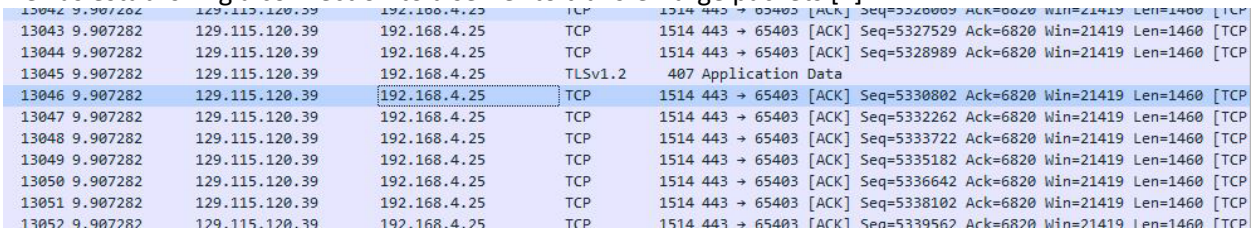


```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2600:1700:501:338f:29af:89d0:380:d84b
   IPv6 Address. . . . . . . . . . . : fd52:b055:1f48:1:29af:89d0:380:d84b
   Temporary IPv6 Address. . . . . . : 2600:1700:501:338f:c85d:2a9a:4723:69f9
   Temporary IPv6 Address. . . . . . : fd52:b055:1f48:1:c85d:2a9a:4723:69f9
   Link-local IPv6 Address . . . . . : fe80::29af:89d0:380:d84b%7
   IPv4 Address. . . . . . . . . . . : 192.168.4.25
   Subnet Mask . . . . . . . . . . . : 255.255.252.0
   Default Gateway . . . . . . . . . : fe80::4e01:43ff:fe8d:d0c2%7
                                       192.168.4.1
```

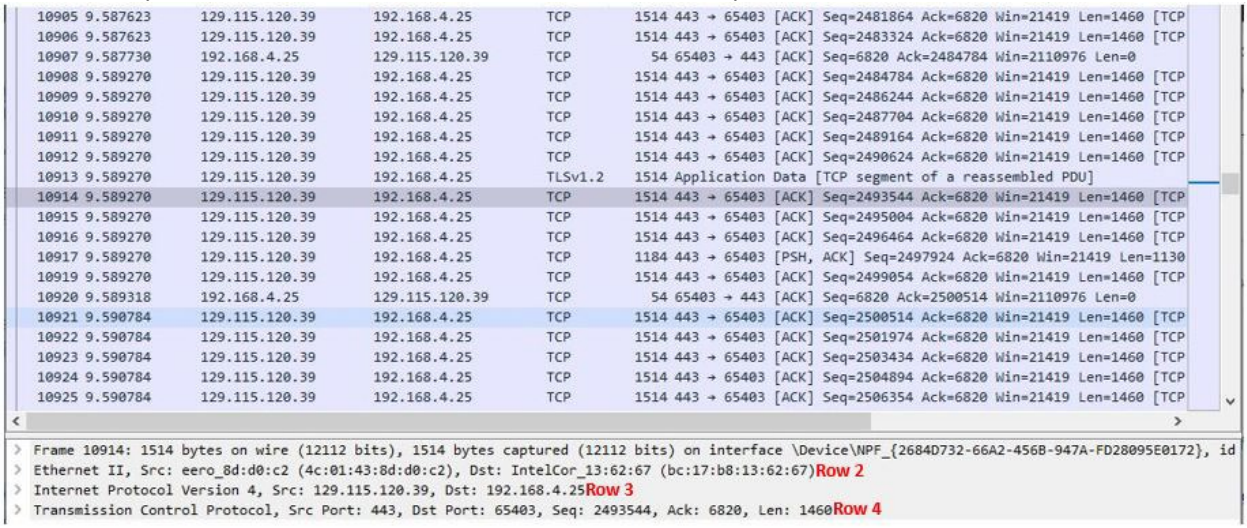
The IP that keeps on repeating likely represents the traffic that was being sent back and forth between my computer and the website I'm attempted to reach.

Breakpoint 03: Further examining the Packets List Pane, I observed that Transmission Control Point (TCP) protocol seemed to be listed the most, rather than the other, Transport Layer Security v1.2 (TLSv1.2). From what I read about TCP on *techtarget.com*, TCP break larger files into smaller packets as well as establishing a connection to a server to transfer large packets [2].



13043	9.907282	129.115.120.39	192.168.4.25	TCP	1514 443 → 65403 [ACK] Seq=5327529 Ack=6820 Win=21419 Len=1460 [TCP
13044	9.907282	129.115.120.39	192.168.4.25	TCP	1514 443 → 65403 [ACK] Seq=5328989 Ack=6820 Win=21419 Len=1460 [TCP
13045	9.907282	129.115.120.39	192.168.4.25	TLSv1.2	407 Application Data
13046	9.907282	129.115.120.39	192.168.4.25	TCP	1514 443 → 65403 [ACK] Seq=5330802 Ack=6820 Win=21419 Len=1460 [TCP
13047	9.907282	129.115.120.39	192.168.4.25	TCP	1514 443 → 65403 [ACK] Seq=5332262 Ack=6820 Win=21419 Len=1460 [TCP
13048	9.907282	129.115.120.39	192.168.4.25	TCP	1514 443 → 65403 [ACK] Seq=5333722 Ack=6820 Win=21419 Len=1460 [TCP
13049	9.907282	129.115.120.39	192.168.4.25	TCP	1514 443 → 65403 [ACK] Seq=5335182 Ack=6820 Win=21419 Len=1460 [TCP
13050	9.907282	129.115.120.39	192.168.4.25	TCP	1514 443 → 65403 [ACK] Seq=5336642 Ack=6820 Win=21419 Len=1460 [TCP
13051	9.907282	129.115.120.39	192.168.4.25	TCP	1514 443 → 65403 [ACK] Seq=5338102 Ack=6820 Win=21419 Len=1460 [TCP

Breakpoint 04: After scrolling toward the middle of the packet capture, I chose one of the packets in the Packets List pane to examine the details in the Packet Details pane.



Based on my interpretation of each row, I associated the rows with the layers of the OSI and Internet Models:

Row 2 – Data Link (Internet Layer 2) information
Row 3 – Network (Internet Layer 3) information
Row 4 – Transport (Internet Layer 4) information

LIMITATIONS/CONCLUSION

As an introductory experiment for the novice user like myself, I thought the labs difficulty was fairly simple. I do not think there were any limitations because everything was executed in a live environment versus a controlled environment, like on a virtual machine. From *comptia.org*, I learned that Wireshark is used to troubleshoot networks with performance issues. Moreover, I learned that cybersecurity professionals often use Wireshark to trace connections, specifically, viewing the contents of suspicious network transaction and identifying bursts of network traffic [3].

REFERENCES

[1] Wireshark [Online]. “Loopback”, August 2020. Available: https://wiki.wireshark.org/CaptureSetup/Loopback [Accessed: 31-Aug-2022]

[2] Yasar, *TechTarget* [Online]. “What is a network packet and how does it work?”, July 2022. Available: https://www.techtarget.com/searchnetworking/definition/packet [Accessed 31-Aug-2022]

[3] CompTIA [Online]. “What is Wireshark and How Is it Used?”, 2022. Available: https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it [Accessed: 01-Sep-2022]

COLLABORATION

The entirety of this lab was executed independently by the author. No additional collaboration to report.