

Name: Md.Abdullah

ID : IT-17015

Lab report no: 2

Name of the lab report: Wireshark display

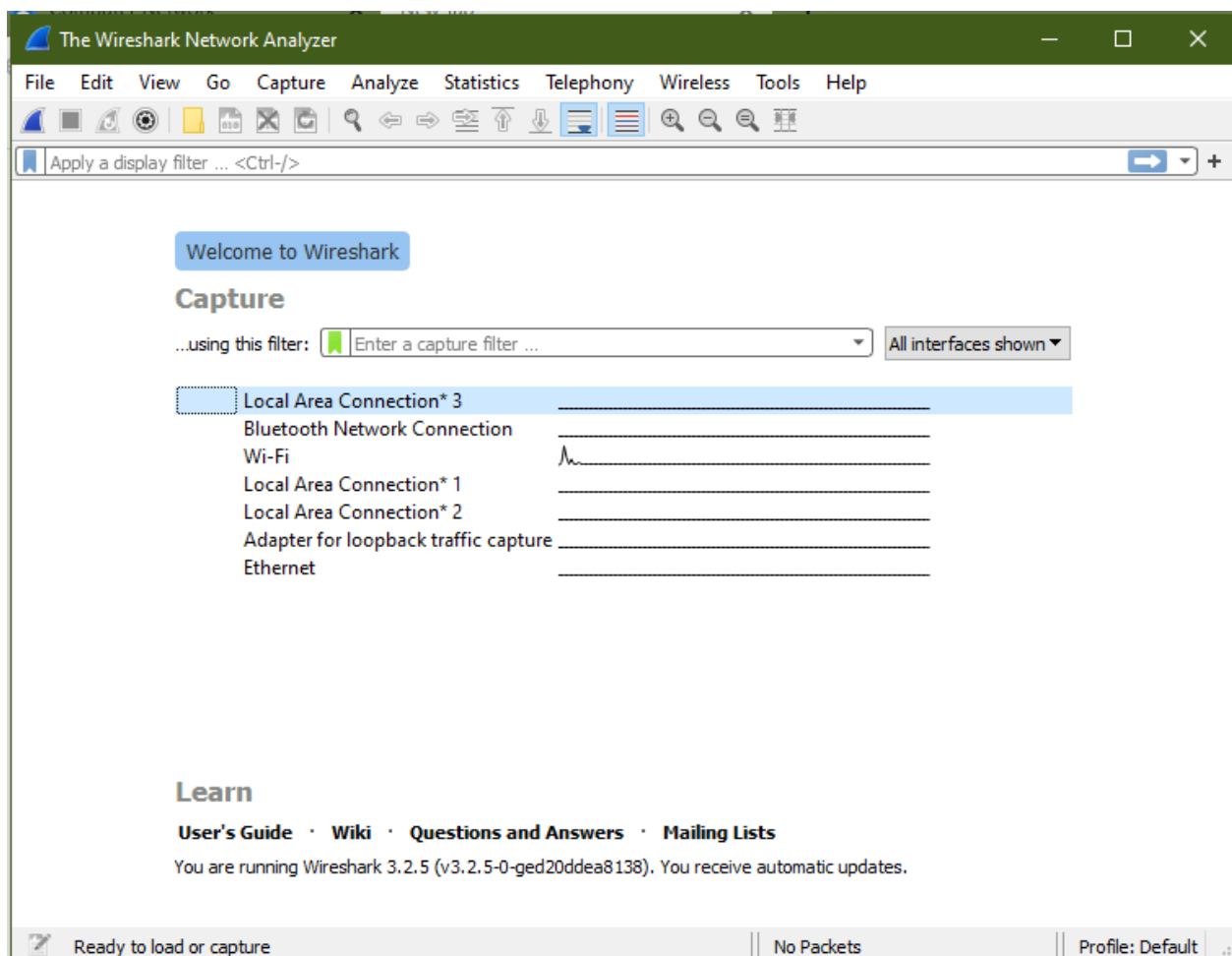
Objectives:

- ❖ To learn basic packet analysis using Wireshark

Theory:

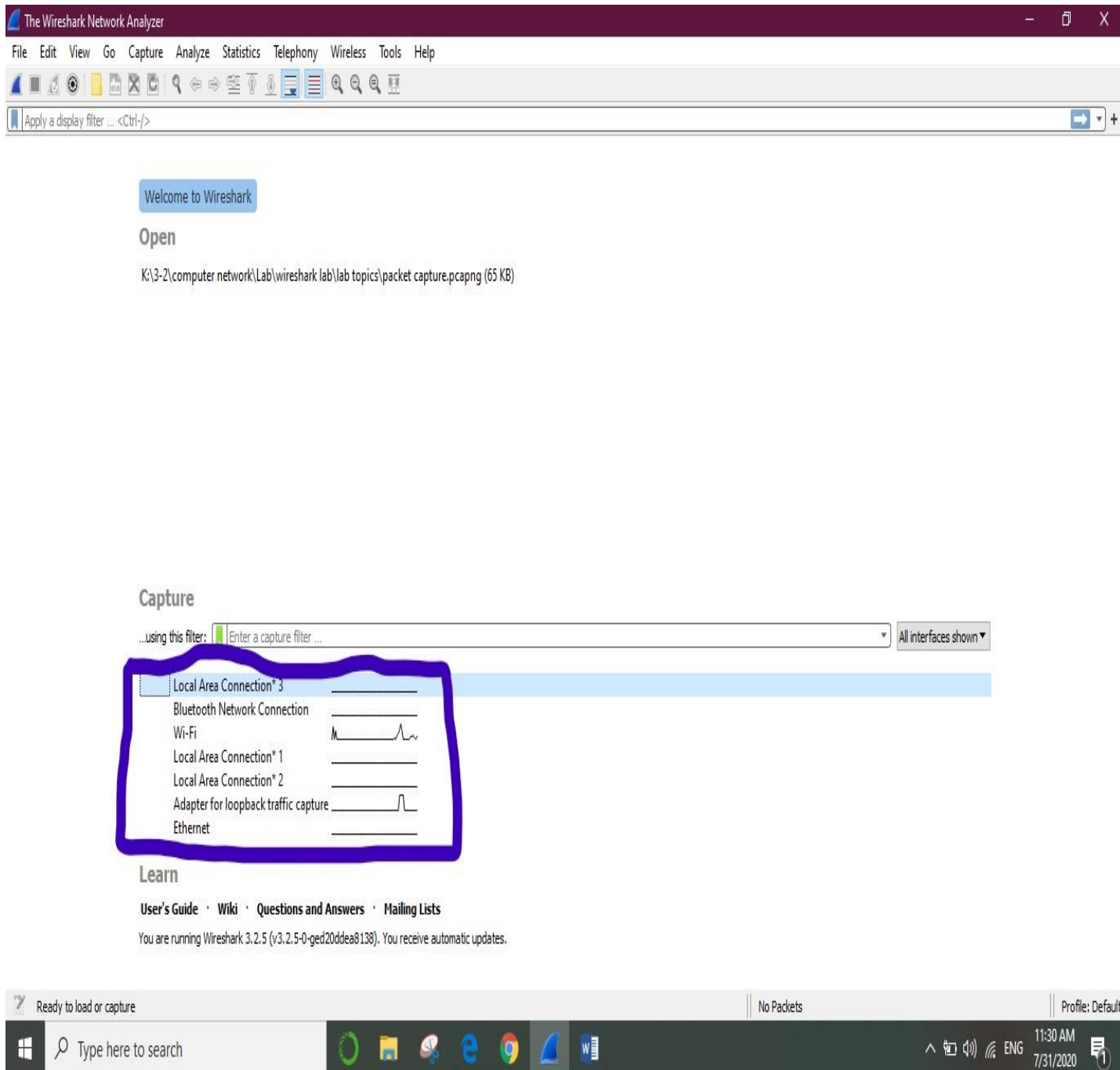
Wireshark is a free and open source network packet analyzer. It is mainly used for network troubleshooting and analysis. In this lab we will learn how to analyze the packets and to find different protocol related information from the captured packets.

Running Wireshark:

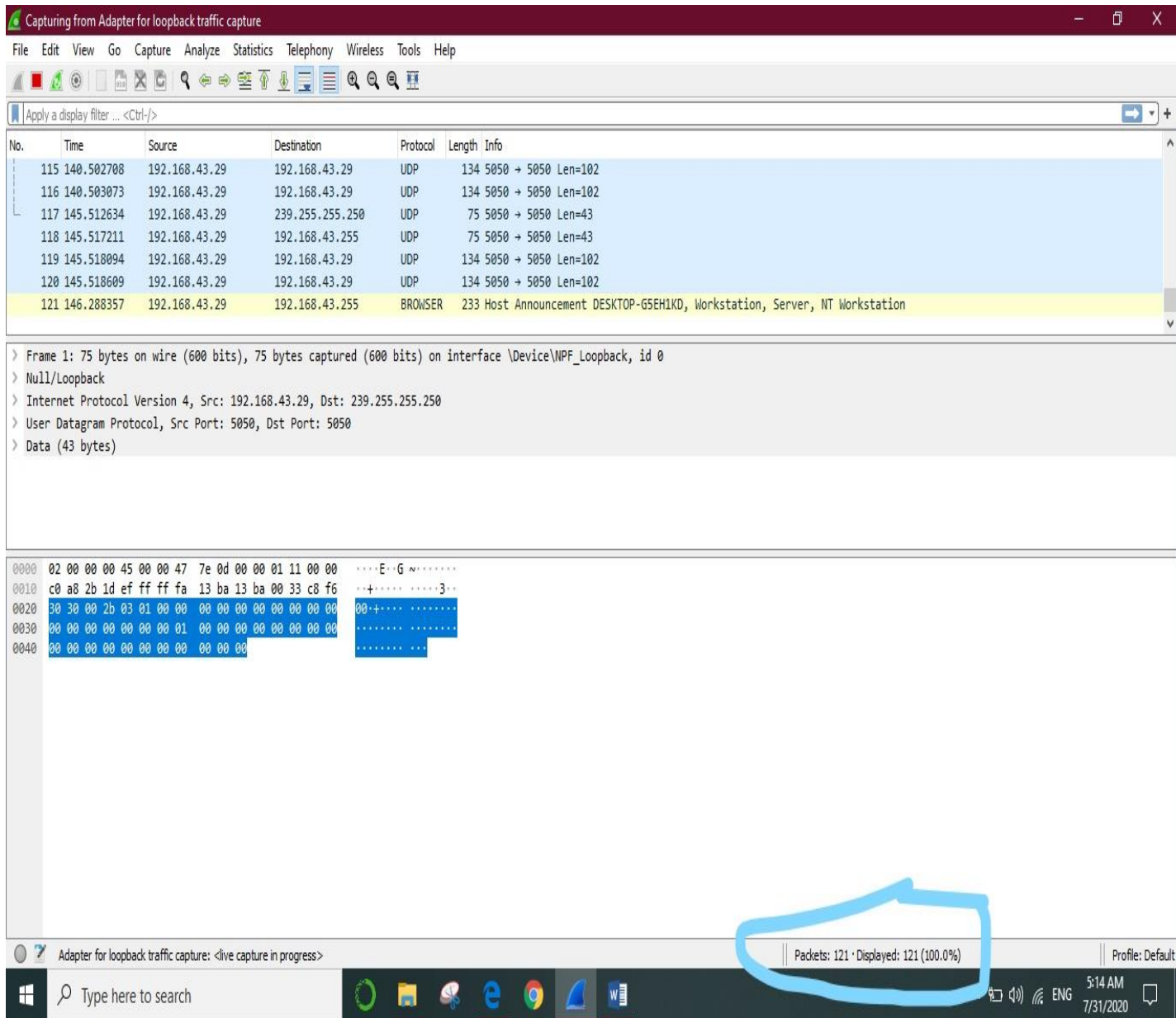


Capturing packet:

First we need to double click on the interfaces shown in below figure marked by blue color.



After double click on any of the item Wireshark is now capturing all packets being sent/received from/by your computer. Here total 121 packet are captured and it will continued.



List of packet that are captured:

Here the name of the file is packet capture.pcapng.

The image shows a Wireshark packet capture window titled "packet capture.pcapng". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar with various icons. A display filter bar shows "Apply a display filter ... <Ctrl-/>".

The packet list table displays the following data:

No.	Time	Source	Destination	Protocol	Length	Info
22	25.080733	192.168.43.29	192.168.43.255	UDP	75	5050 → 5050 Len=43
23	25.081484	192.168.43.29	192.168.43.29	UDP	134	5050 → 5050 Len=102
24	25.081859	192.168.43.29	192.168.43.29	UDP	134	5050 → 5050 Len=102
25	30.082236	192.168.43.29	239.255.255.250	UDP	75	5050 → 5050 Len=43
26	30.087550	192.168.43.29	192.168.43.255	UDP	75	5050 → 5050 Len=43
27	30.087911	192.168.43.29	192.168.43.29	UDP	134	5050 → 5050 Len=102
28	30.088754	192.168.43.29	192.168.43.29	UDP	134	5050 → 5050 Len=102
29	35.091738	192.168.43.29	239.255.255.250	UDP	75	5050 → 5050 Len=43

The details pane for packet 25 shows the following structure:

- > Frame 25: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{...} id 0
- > Null/Loopback
- > Internet Protocol Version 4, Src: 192.168.43.29, Dst: 239.255.255.250
- > User Datagram Protocol, Src Port: 5050, Dst Port: 5050
- > Data (43 bytes)

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 02 00 00 00 45 00 00 7e 13 00 00 01 11 00 00  ....E..G.....
0010 c0 a8 2b 1d ef ff ff fa 13 ba 13 ba 00 33 c8 f6  ..+.....3...
0020 30 30 00 2b 03 01 00 00 00 00 00 00 00 00 00  00+.....
0030 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00  .....
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```

The status bar at the bottom indicates "Packets: 438 · Displayed: 438 (100.0%)" and "Profile: Default". The Windows taskbar shows the time as 11:39 AM on 7/31/2020.

Capturing a packet set and received by HTTP:

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture control, and analysis. The packet list pane shows a list of captured packets, with the first packet (No. 673) selected. The packet details pane shows the structure of the selected packet, which is an HTTP GET request. The packet bytes pane shows the raw hex and ASCII data of the selected packet.

No.	Source	Destination	Protocol	Length	Info
673	192.168.43.29	117.18.237.29	HTTP	300	GET /Omniroot2025.cr1 HTTP/1.1
674	128.141.8956	117.18.237.29	HTTP	328	HTTP/1.1 304 Not Modified
701	141.935387	192.168.43.29	HTTP	520	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
711	142.328478	128.119.245.12	HTTP	491	HTTP/1.1 200 OK (text/html)
713	142.971480	192.168.43.29	HTTP	452	GET /favicon.ico HTTP/1.1
718	143.381754	128.119.245.12	HTTP	537	HTTP/1.1 404 Not Found (text/html)

Frame 671: 300 bytes on wire (2400 bits), 300 bytes captured (2400 bits) on interface \Device\NPF_{1A594714-957C-4125-9B88-6E529C9F6DF9}, id 0
Ethernet II, Src: Azureklav_d7:57:7d (74:c6:3b:d7:57:7d), Dst: 7e:03:ab:e5:06:00 (7e:03:ab:e5:06:00)
Internet Protocol Version 4, Src: 192.168.43.29, Dst: 117.18.237.29
Transmission Control Protocol, Src Port: 51794, Dst Port: 80, Seq: 1, Ack: 1, Len: 246
Hypertext Transfer Protocol

0000 7e 03 ab e5 06 00 74 c6 3b d7 57 7d 08 00 45 00W}..E.
0010 01 1e 59 f7 40 00 80 06 51 ed c0 a8 2b 1d 75 12 ..Y@...Q...+u.
0020 ed 1d ca 52 00 50 bd 43 d1 0b 6c 1c ff 6b 50 18 ...R.P.C...l..kP.
0030 02 02 d5 65 00 00 47 45 54 20 2f 4f 6d 6e 69 72 ...e..GE T /Omni
0040 6f 6f 74 32 30 32 35 2e 63 72 6c 20 48 54 54 50 oot2025. cr1 HTTP
0050 2f 31 2e 31 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 /1.1..Ca che-Cont
0060 72 6f 6c 3a 20 6d 61 78 2d 61 67 65 20 3d 20 31 rol: max -age = 1
0070 37 32 38 30 30 0d 0a 43 6f 6e 6e 65 63 74 69 6f 72800..C onnectio
0080 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 41 n: Keep- Alive..A
0090 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 49 66 2d 4d ccept: * /*..If-M
00a0 6f 64 69 66 69 65 64 2d 53 69 6e 63 65 3a 20 46 odified- Since: F
00b0 72 69 2c 20 32 34 20 4a 75 6c 20 32 30 32 30 20 ri, 24 Jul 2020
00c0 31 37 3a 35 38 3a 30 34 20 47 4d 54 0d 0a 49 66 17:58:04 GMT..If
00d0 2d 4e 6f 6e 65 2d 4d 61 74 63 68 3a 20 22 33 32 -None-Ma tch: "32
00e0 38 34 32 30 31 36 36 37 22 0d 0a 55 73 65 72 2d 84201667 "...User-
00f0 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 Agent: M icrosoft
0100 2d 43 72 79 70 74 6f 41 50 49 2f 31 30 2e 30 0d -CryptoA PI/10.0
0110 0a 48 6f 73 74 3a 20 63 72 6c 33 2e 64 69 67 69 -Host: c rl3.digi
0120 63 65 72 74 2e 63 6f 6d 0d 0a 0d 0a cert.com

Hypertext Transfer Protocol: Protocol

Packets: 813 · Displayed: 6 (0.7%)

Profile: Default

12:01 PM
7/31/2020

TCP packet capture:

Here we show that total number of packet captured are 7342 but displayed 85 because there are 85 TCP packet are send or received.

The image shows a Wireshark packet capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for packet capture and analysis. The packet list pane shows a list of captured packets, with the 'tcp' filter selected. The packet details pane shows the selected packet's structure, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII. The status bar at the bottom indicates 'Packets: 7342 · Displayed: 85 (1.2%)'.

No.	Time	Source	Destination	Protocol	Length	Info
2880	29.257808	192.168.43.29	34.226.70.133	TCP	66	51838 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2881	29.267622	52.109.76.36	192.168.43.29	TCP	1454	443 → 51837 [ACK] Seq=1 Ack=187 Win=131584 Len=1400 [TCP segment of a reassembled PDU]
2882	29.270318	52.109.76.36	192.168.43.29	TCP	1454	443 → 51837 [ACK] Seq=1401 Ack=187 Win=131584 Len=1400 [TCP segment of a reassembled PDU]
2883	29.270359	192.168.43.29	52.109.76.36	TCP	54	51837 → 443 [ACK] Seq=187 Ack=2801 Win=131584 Len=0
2884	29.276818	52.109.76.36	192.168.43.29	TCP	1454	443 → 51837 [ACK] Seq=2801 Ack=187 Win=131584 Len=1400 [TCP segment of a reassembled PDU]
2885	29.278412	52.109.76.36	192.168.43.29	TCP	1454	443 → 51837 [ACK] Seq=4201 Ack=187 Win=131584 Len=1400 [TCP segment of a reassembled PDU]
2886	29.278458	192.168.43.29	52.109.76.36	TCP	54	51837 → 443 [ACK] Seq=187 Ack=5601 Win=131584 Len=0
2920	29.508912	192.168.43.29	34.226.70.133	TCP	66	51839 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

> Frame 2884: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits) on interface \Device\NPF_{1A594714-957C-4125-9888-6E529C9F6DF9}, id 0
> Ethernet II, Src: 7e:03:ab:e5:06:00 (7e:03:ab:e5:06:00), Dst: AzureNav_d7:57:7d (74:c6:3b:d7:57:7d)
> Internet Protocol Version 4, Src: 52.109.76.36, Dst: 192.168.43.29
> Transmission Control Protocol, Src Port: 443, Dst Port: 51837, Seq: 2801, Ack: 187, Len: 1400

0000 74 c6 3b d7 57 7d 7e 03 ab e5 06 00 08 00 45 00 t.;W}~E.
0010 05 a0 24 01 40 00 6a 06 7b 00 34 6d 4c 24 c0 a8 ..\$.@.j. {.4mL\$..
0020 2b 1d 01 bb ca 7d 08 23 cd 7b 03 5a 28 0f 50 10 +....}.# .{Z(.P..
0030 02 02 a4 91 00 00 72 6f 73 6f 66 74 20 49 54 20ro soft IT
0040 54 4c 53 20 43 41 20 31 30 82 02 22 30 0d 06 09 TLS CA 1 0..0..
0050 2a 86 48 86 f7 0d 01 01 01 05 00 03 82 02 0f 00 *.H.....
0060 30 82 02 0a 02 82 02 01 00 8e f3 f1 84 75 77 bc 0.....uw..
0070 be c9 a4 f5 16 a5 53 2b 50 60 99 dc d8 7d d9 24S+ P'....}.\$
0080 b5 e1 72 49 37 48 fe da 86 93 a3 7d 1d 9a 4b 10 ..rI7H.....}~K..
0090 4d 77 79 7e 65 a9 7c 6e 36 e2 47 d4 36 49 d0 cc Mwy~e.|n 6:G:6I..
00a0 24 02 27 14 e2 ae 71 cd d9 57 74 3c 10 56 19 92 \$. '....q. .Wt<V..
00b0 4a 87 62 f9 e3 90 8d 5e de d1 41 1b 1a a6 1f 40 J.b.....^..A.....@
00c0 a2 2c 1e 8e 55 d7 26 d8 68 42 ab ec 0d de dd 5e ,.,.U.&. hB.....^
00d0 61 95 b3 ac 6c 81 ce a8 e0 ad af 5f ca a6 e4 51 a...l...._...Q
00e0 68 2e 27 fd 54 2a 71 a4 cc bb 7e 92 f1 f6 53 51 h.'T*q.~SQ
00f0 05 31 d0 19 82 b0 ca 63 d0 f2 4a 00 0b cd f4 69 .1.....c ..}....i
0100 4b f4 5a 96 56 39 26 c9 9d 4b 0a 63 34 32 80 a5 K.Z.V9&...K.c42..
0110 04 e5 ea 28 b7 c1 00 c0 6d 1a f0 28 d4 4a 8f 80 ...(.m...(.J..
0120 ac 73 19 d8 f5 16 2f ad ae 08 97 62 06 2c fe e7 .s..../.b.,..

Packets: 7342 · Displayed: 85 (1.2%)

UDP packet capture:

Here we show that total number of packet captured are 585 but displayed 85 because there are 517 TCP packet are send or received.

Wireshark packet capture interface showing UDP traffic. The filter bar displays 'udp'. The packet list shows 8 packets. The packet details pane shows the structure of the first packet (Frame 1). The packet bytes pane shows the raw data. The status bar at the bottom indicates 'Packets: 585 · Displayed: 517 (88.4%)'.

No.	Time	Source	Destination	Protocol	Length	Info
575	107.107206	216.58.203.78	192.168.43.29	UDP	393	443 → 59176 Len=351
576	107.107206	216.58.203.78	192.168.43.29	UDP	156	443 → 59176 Len=114
577	107.107518	192.168.43.29	216.58.203.78	UDP	75	59176 → 443 Len=33
578	108.036768	192.168.43.29	172.217.166.142	UDP	75	51625 → 443 Len=33
579	108.485153	172.217.166.142	192.168.43.29	UDP	67	443 → 51625 Len=25
582	111.737844	192.168.43.29	172.217.31.99	UDP	75	56907 → 443 Len=33
583	112.004228	172.217.31.99	192.168.43.29	UDP	67	443 → 56907 Len=25

Frame 1: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{1A594714-957C-4125-9888-6E529C9F6DF9}, id 0
> Ethernet II, Src: AzureWav_d7:57:7d (74:c6:3b:d7:57:7d), Dst: 7e:03:ab:e5:06:00 (7e:03:ab:e5:06:00)
> Internet Protocol Version 4, Src: 192.168.43.29, Dst: 216.58.196.35
> User Datagram Protocol, Src Port: 58831, Dst Port: 443
> Data (33 bytes)

0000 7e 03 ab e5 06 00 74 c6 3b d7 57 7d 08 00 45 00 ~.....t.;W}..E.
0010 00 3d 61 ac 40 00 80 11 10 e0 c0 a8 2b 1d d8 3a ..a@.....+..
0020 c4 23 e5 cf 01 bb 00 29 c6 5b 5d cf f6 16 de 45 .#.....) .[.....E
0030 93 2a b7 38 59 fd 50 f7 c6 90 5a 00 3b a4 e7 ed .*8Y.P..Z;...
0040 6c 5e b7 60 6f 51 8b 64 4a 74 f5 1^..oQ.d Jt.

Packets: 585 · Displayed: 517 (88.4%)

Discussion:

This was an interesting lab. I learned many things from this lab. This lab helps me to understand the basic of wireshark display such as how to use wireshark display, how to capture different types packets such as tcp, udp etc. I also learn how to filter a packet using wireshark. I can successfully capture different types of packets as screenshot given above.