EXPERIMENT NO-8

AIM: Study of packet sniffer tools Wireshark: -

a. Observer performance in promiscuous as well as non-promiscuous mode.
b. Show the packets can be traced based on different filters Port Filters,Address Filters,Protocol Filters,String Filters

Theory:

Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible.

You could think of a network packet analyzer as a measuring device for examining what's happening inside a network cable, just like an electrician uses a voltmeter for examining what's happening inside an electric cable (but at a higher level, of course).

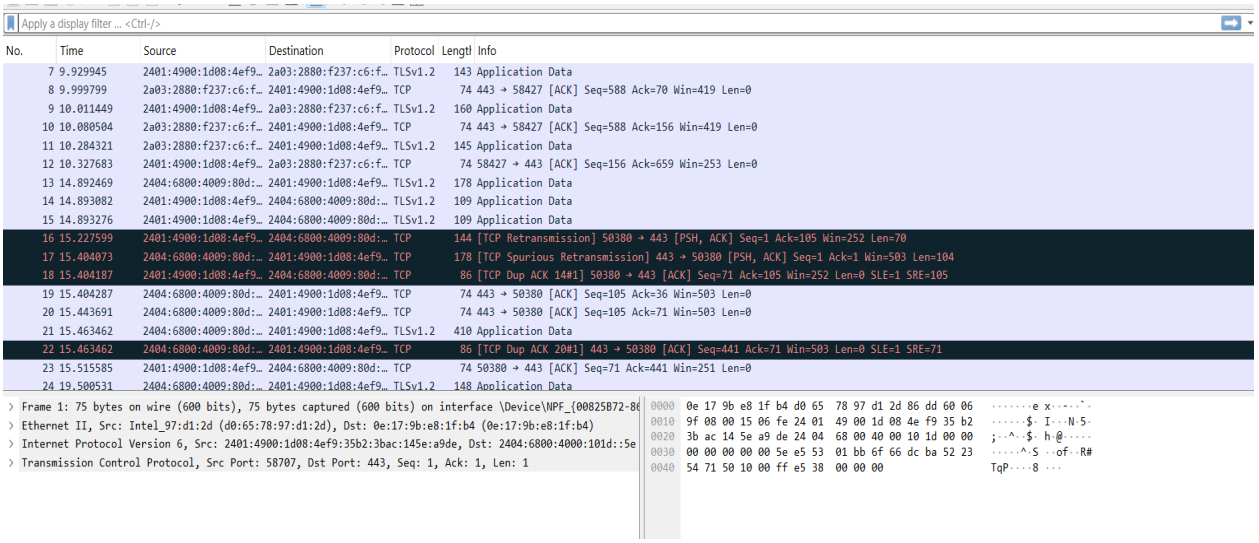
In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.

Applications of wireshark:-

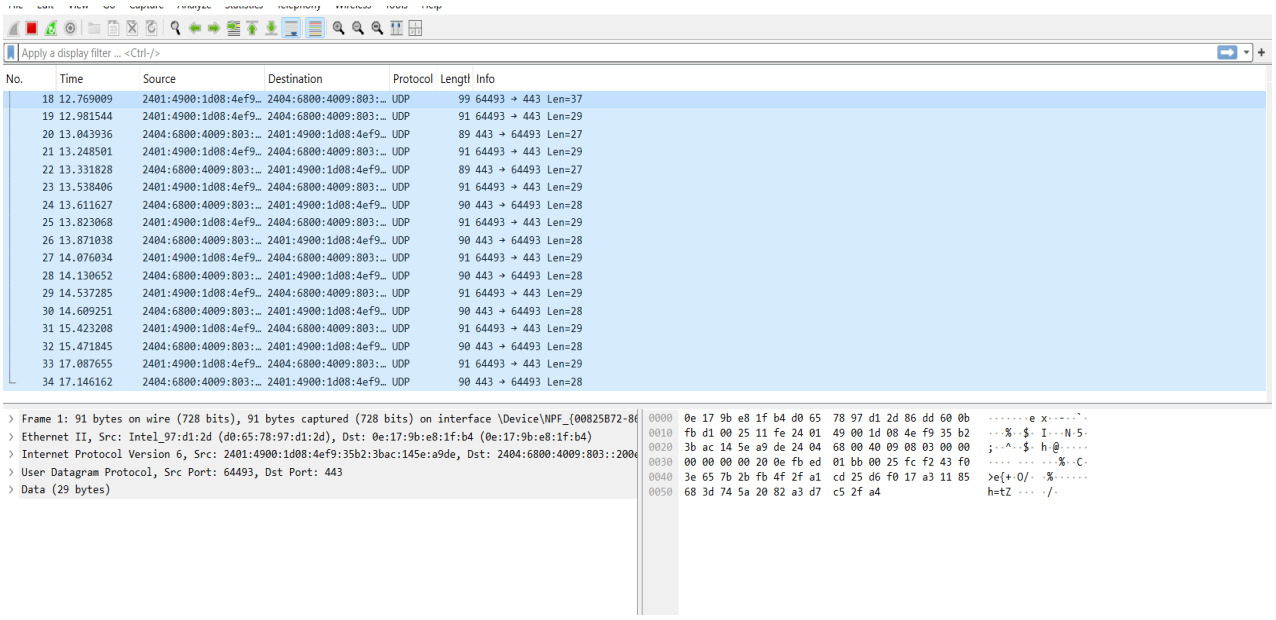
- Network administrators use it to troubleshoot network problems
- Network security engineers use it to examine security problems
- QA engineers use it to verify network applications
- Developers use it to debug protocol implementations
- People use it to learn network protocol internals

a. Observer performance in promiscuous as well as non-promiscuous mode.

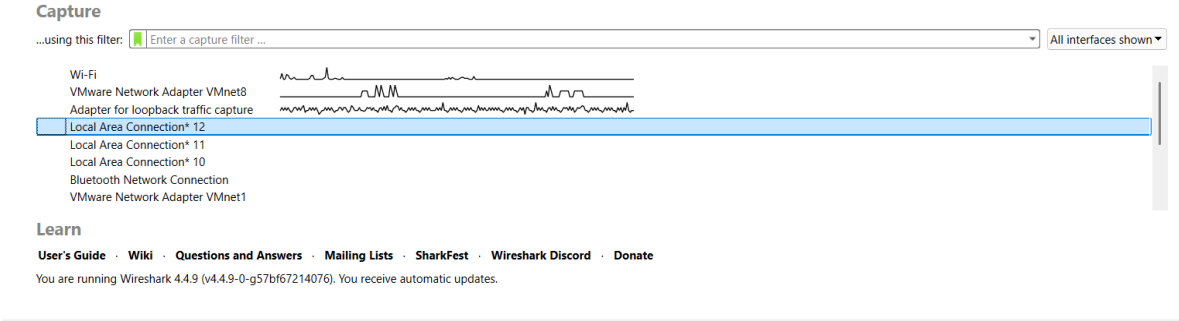
- Promiscuous mode



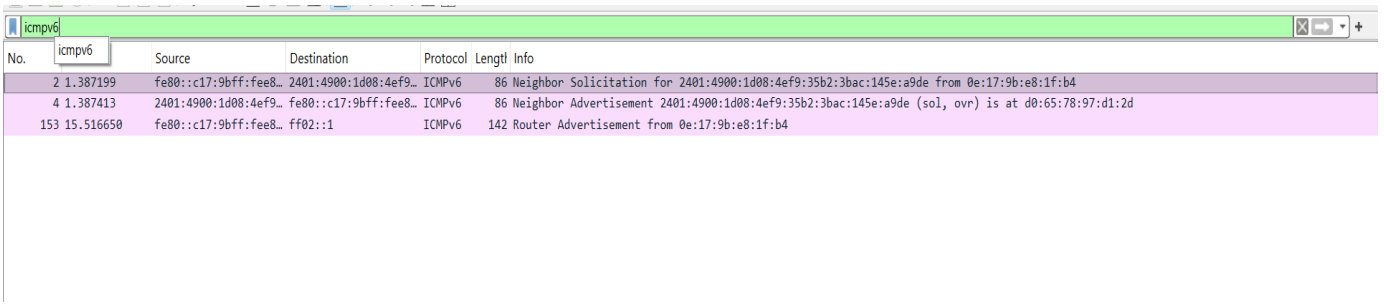
- Non-Promiscuous mode



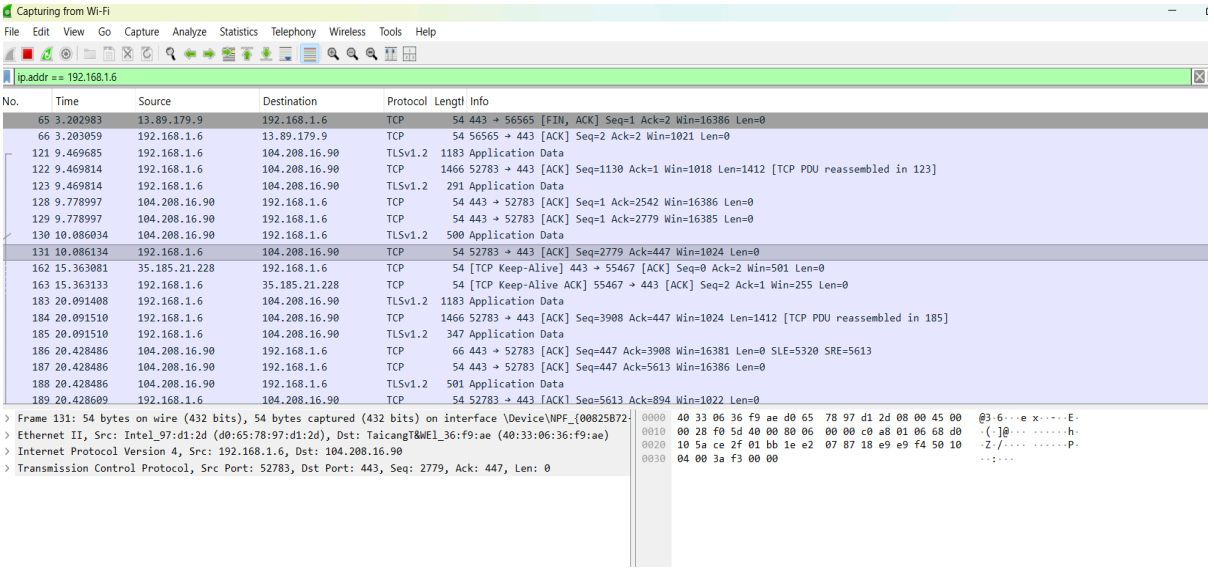
b. Show the packets can be traced based on different filters



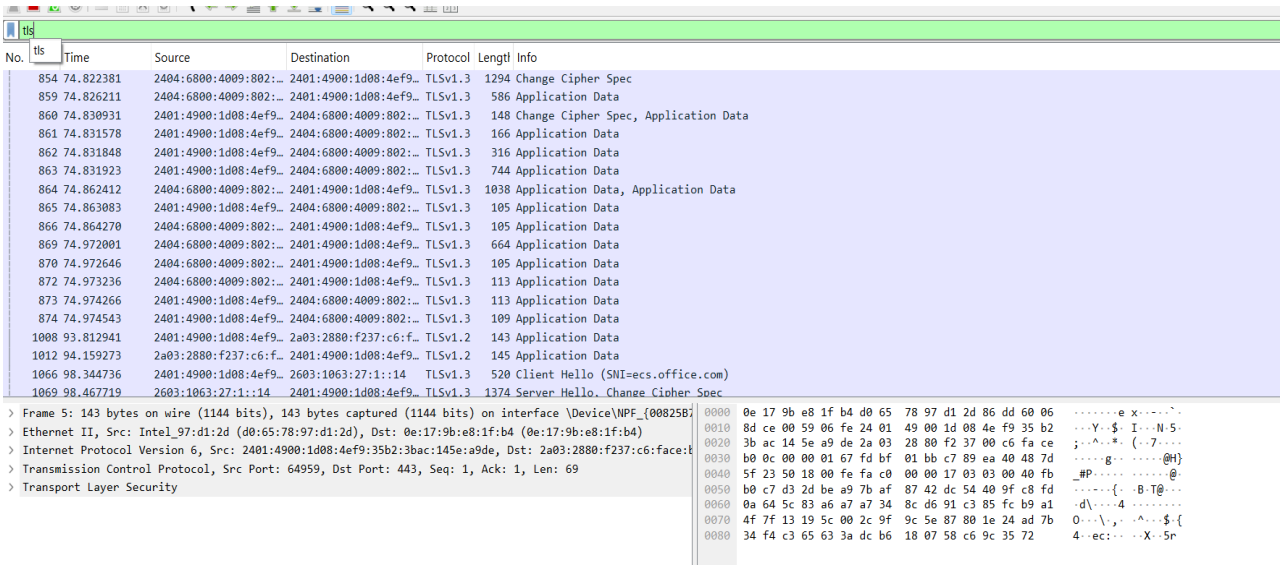
ICMPV6



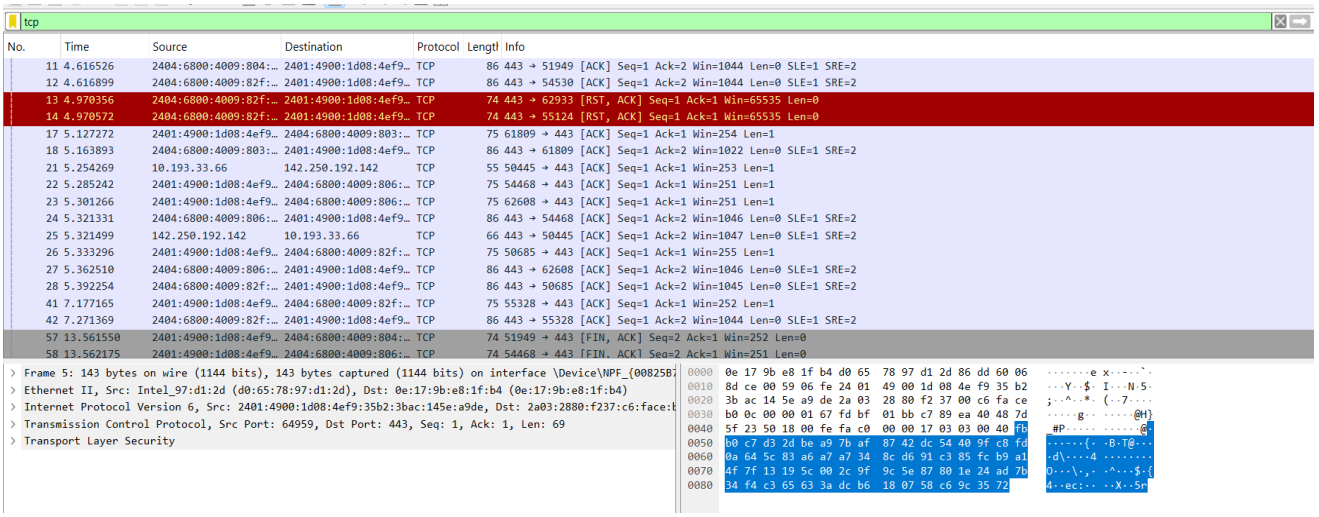
ip.addr == 192.168.1.6



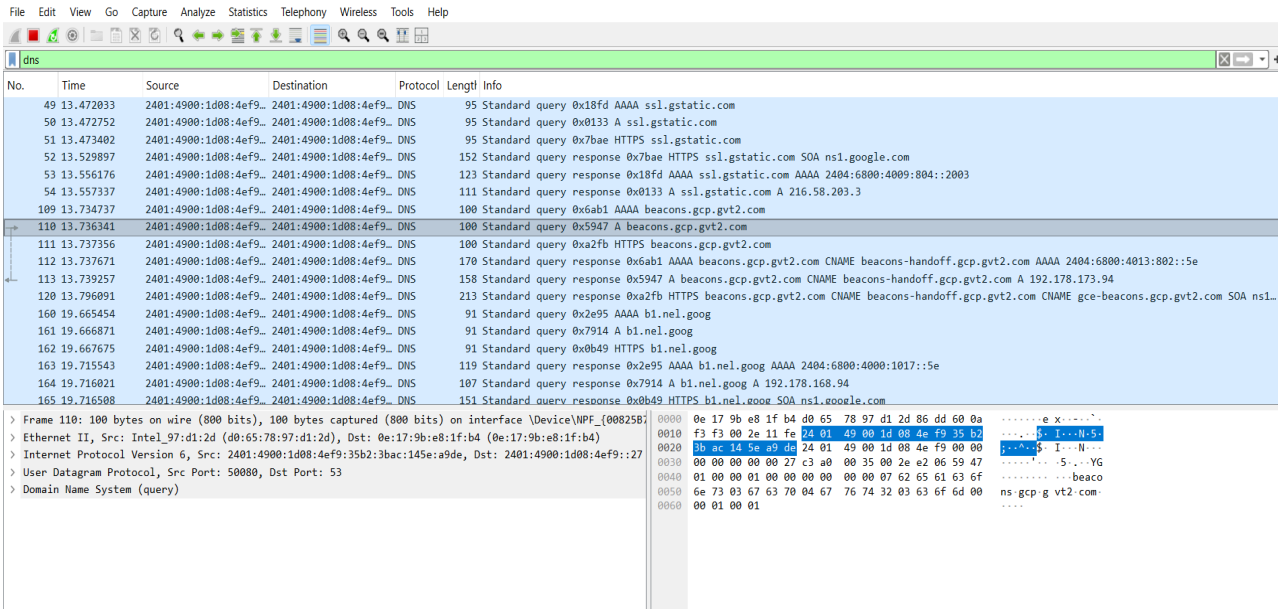
TLS


tls
No. Time Source Destination Protocol Lengtl Info
854 74.822381 2404:6800:4009:802:… 2401:4900:1d08:4ef9… TLSv1.3 1294 Change Cipher Spec
859 74.826211 2404:6800:4009:802:… 2401:4900:1d08:4ef9… TLSv1.3 586 Application Data
860 74.830931 2401:4900:1d08:4ef9… 2404:6800:4009:802:… TLSv1.3 148 Change Cipher Spec, Application Data
861 74.831578 2401:4900:1d08:4ef9… 2404:6800:4009:802:… TLSv1.3 166 Application Data
862 74.831848 2401:4900:1d08:4ef9… 2404:6800:4009:802:… TLSv1.3 316 Application Data
863 74.831923 2401:4900:1d08:4ef9… 2404:6800:4009:802:… TLSv1.3 744 Application Data
864 74.862412 2404:6800:4009:802:… 2401:4900:1d08:4ef9… TLSv1.3 1038 Application Data, Application Data
865 74.863083 2401:4900:1d08:4ef9… 2404:6800:4009:802:… TLSv1.3 105 Application Data
866 74.864270 2404:6800:4009:802:… 2401:4900:1d08:4ef9… TLSv1.3 105 Application Data
869 74.972001 2404:6800:4009:802:… 2401:4900:1d08:4ef9… TLSv1.3 664 Application Data
870 74.972646 2404:6800:4009:802:… 2401:4900:1d08:4ef9… TLSv1.3 105 Application Data
872 74.973236 2404:6800:4009:802:… 2401:4900:1d08:4ef9… TLSv1.3 113 Application Data
873 74.974266 2401:4900:1d08:4ef9… 2404:6800:4009:802:… TLSv1.3 113 Application Data
874 74.974543 2401:4900:1d08:4ef9… 2404:6800:4009:802:… TLSv1.3 109 Application Data
1008 93.812941 2401:4900:1d08:4ef9… 2a03:2880:f237:c6:f… TLSv1.2 143 Application Data
1012 94.159273 2a03:2880:f237:c6:f… 2401:4900:1d08:4ef9… TLSv1.2 145 Application Data
1066 98.344736 2401:4900:1d08:4ef9… 2603:1063:27:1::14 TLSv1.3 520 Client Hello (SNI=ecs.office.com)
1069 98.467719 2603:1063:27:1::14 2401:4900:1d08:4ef9… TLSv1.3 1374 Server Hello, Change Cipher Spec
Frame 5: 143 bytes on wire (1144 bits), 143 bytes captured (1144 bits) on interface \Device\NPF_{00825B7
Ethernet II, Src: Intel_97:d1:2d (d0:65:78:97:d1:2d), Dst: 0e:17:9b:e8:1f:b4 (0e:17:9b:e8:1f:b4)
Internet Protocol Version 6, Src: 2401:4900:1d08:4ef9:35b2:3bac:145e:a9de, Dst: 2a03:2880:f237:c6:face:b
Transmission Control Protocol, Src Port: 64959, Dst Port: 443, Seq: 1, Ack: 1, Len: 69
Transport Layer Security
0000 0e 17 9b e8 1f b4 d0 65 78 97 d1 2d 86 dd 60 06 ·····e x··-··`·
0010 8d ce 00 59 06 fe 24 01 49 00 1d 08 4e f9 35 b2 ···Y··$· I···N·5·
0020 3b ac 14 5e a9 de 2a 03 28 80 f2 37 00 c6 fa ce ;··^··*· (··7····
0030 b0 0c 00 00 01 67 fd bf 01 bb c7 89 ea 40 48 7d ·····g·· ·····@H}
0040 5f 23 50 18 00 fe fa c0 00 00 17 03 03 00 40 fb _#P····· ·····@·
0050 b0 c7 d3 2d be a9 7b af 87 42 dc 54 40 9f c8 fd ···-··{· ·B·T@···
0060 0a 64 5c 83 a6 a7 a7 34 8c d6 91 c3 85 fc b9 a1 ·d\····4 ········
0070 4f 7f 13 19 5c 00 2c 9f 9c 5e 87 80 1e 24 ad 7b O···\·,· ·^···$·{
0080 34 f4 c3 65 63 3a dc b6 18 07 58 c6 9c 35 72 4··ec:·· ··X··5r

TCP


tcp
No. Time Source Destination Protocol Lengtl Info
11 4.616526 2404:6800:4009:804:… 2401:4900:1d08:4ef9… TCP 86 443 → 51949 [ACK] Seq=1 Ack=2 Win=1044 Len=0 SLE=1 SRE=2
12 4.616899 2404:6800:4009:82f:… 2401:4900:1d08:4ef9… TCP 86 443 → 54530 [ACK] Seq=1 Ack=2 Win=1044 Len=0 SLE=1 SRE=2
13 4.970356 2404:6800:4009:82f:… 2401:4900:1d08:4ef9… TCP 74 443 → 62933 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
14 4.970572 2404:6800:4009:82f:… 2401:4900:1d08:4ef9… TCP 74 443 → 55124 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
17 5.127272 2401:4900:1d08:4ef9… 2404:6800:4009:803:… TCP 75 61809 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1
18 5.163893 2404:6800:4009:803:… 2401:4900:1d08:4ef9… TCP 86 443 → 61809 [ACK] Seq=1 Ack=2 Win=1022 Len=0 SLE=1 SRE=2
21 5.254269 10.193.33.66 142.250.192.142 TCP 55 50445 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1
22 5.285242 2401:4900:1d08:4ef9… 2404:6800:4009:806:… TCP 75 54468 → 443 [ACK] Seq=1 Ack=1 Win=251 Len=1
23 5.301266 2401:4900:1d08:4ef9… 2404:6800:4009:806:… TCP 75 62608 → 443 [ACK] Seq=1 Ack=1 Win=251 Len=1
24 5.321331 2404:6800:4009:806:… 2401:4900:1d08:4ef9… TCP 86 443 → 54468 [ACK] Seq=1 Ack=2 Win=1046 Len=0 SLE=1 SRE=2
25 5.321499 142.250.192.142 10.193.33.66 TCP 66 443 → 50445 [ACK] Seq=1 Ack=2 Win=1047 Len=0 SLE=1 SRE=2
26 5.333296 2401:4900:1d08:4ef9… 2404:6800:4009:82f:… TCP 75 50685 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
27 5.362510 2404:6800:4009:806:… 2401:4900:1d08:4ef9… TCP 86 443 → 62608 [ACK] Seq=1 Ack=2 Win=1046 Len=0 SLE=1 SRE=2
28 5.392254 2404:6800:4009:82f:… 2401:4900:1d08:4ef9… TCP 86 443 → 50685 [ACK] Seq=1 Ack=2 Win=1045 Len=0 SLE=1 SRE=2
41 7.177165 2401:4900:1d08:4ef9… 2404:6800:4009:82f:… TCP 75 55328 → 443 [ACK] Seq=1 Ack=1 Win=252 Len=1
42 7.271369 2404:6800:4009:82f:… 2401:4900:1d08:4ef9… TCP 86 443 → 55328 [ACK] Seq=1 Ack=2 Win=1044 Len=0 SLE=1 SRE=2
57 13.561550 2401:4900:1d08:4ef9… 2404:6800:4009:804:… TCP 74 51949 → 443 [FIN, ACK] Seq=2 Ack=1 Win=252 Len=0
58 13.562175 2401:4900:1d08:4ef9… 2404:6800:4009:806:… TCP 74 54468 → 443 [FIN, ACK] Seq=2 Ack=1 Win=251 Len=0
Frame 5: 143 bytes on wire (1144 bits), 143 bytes captured (1144 bits) on interface \Device\NPF_{00825B7
Ethernet II, Src: Intel_97:d1:2d (d0:65:78:97:d1:2d), Dst: 0e:17:9b:e8:1f:b4 (0e:17:9b:e8:1f:b4)
Internet Protocol Version 6, Src: 2401:4900:1d08:4ef9:35b2:3bac:145e:a9de, Dst: 2a03:2880:f237:c6:face:b
Transmission Control Protocol, Src Port: 64959, Dst Port: 443, Seq: 1, Ack: 1, Len: 69
Transport Layer Security
0000 0e 17 9b e8 1f b4 d0 65 78 97 d1 2d 86 dd 60 06 ·····e x··-··`·
0010 8d ce 00 59 06 fe 24 01 49 00 1d 08 4e f9 35 b2 ···Y··$· I···N·5·
0020 3b ac 14 5e a9 de 2a 03 28 80 f2 37 00 c6 fa ce ;··^··*· (··7····
0030 b0 0c 00 00 01 67 fd bf 01 bb c7 89 ea 40 48 7d ·····g·· ·····@H}
0040 5f 23 50 18 00 fe fa c0 00 00 17 03 03 00 40 fb _#P····· ·····@·
0050 b0 c7 d3 2d be a9 7b af 87 42 dc 54 40 9f c8 fd ···-··{· ·B·T@···
0060 0a 64 5c 83 a6 a7 a7 34 8c d6 91 c3 85 fc b9 a1 ·d\····4 ········
0070 4f 7f 13 19 5c 00 2c 9f 9c 5e 87 80 1e 24 ad 7b O···\·,· ·^···$·{
0080 34 f4 c3 65 63 3a dc b6 18 07 58 c6 9c 35 72 4··ec:·· ··X··5r

DNS



CONCLUSION : Thus, by performing this experiment, we have studied and implemented **packet sniffing using the Wireshark tool**.