

## **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

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
7	9.929945	2401:4900:1d08:4ef9..	2a03:2880:f237:c6:f..	TLSv1.2	143	Application Data
8	9.999799	2a03:2880:f237:c6:f..	2401:4900:1d08:4ef9..	TCP	74	443 → 58427 [ACK] Seq=588 Ack=70 Win=419 Len=0
9	10.011449	2401:4900:1d08:4ef9..	2a03:2880:f237:c6:f..	TLSv1.2	160	Application Data
10	10.080504	2a03:2880:f237:c6:f..	2401:4900:1d08:4ef9..	TCP	74	443 → 58427 [ACK] Seq=588 Ack=156 Win=419 Len=0
11	10.284321	2a03:2880:f237:c6:f..	2401:4900:1d08:4ef9..	TLSv1.2	145	Application Data
12	10.327683	2401:4900:1d08:4ef9..	2a03:2880:f237:c6:f..	TCP	74	58427 → 443 [ACK] Seq=156 Ack=659 Win=253 Len=0
13	14.892469	2404:6800:4009:80d..	2401:4900:1d08:4ef9..	TLSv1.2	178	Application Data
14	14.893082	2401:4900:1d08:4ef9..	2404:6800:4009:80d..	TLSv1.2	109	Application Data
15	14.893276	2401:4900:1d08:4ef9..	2404:6800:4009:80d..	TLSv1.2	109	Application Data
16	15.227599	2401:4900:1d08:4ef9..	2404:6800:4009:80d..	TCP	144	[TCP Retransmission] 50380 → 443 [PSH, ACK] Seq=1 Ack=105 Win=252 Len=70
17	15.404073	2404:6800:4009:80d..	2401:4900:1d08:4ef9..	TCP	178	[TCP Spurious Retransmission] 443 → 50380 [PSH, ACK] Seq=1 Ack=1 Win=503 Len=104
18	15.404187	2401:4900:1d08:4ef9..	2404:6800:4009:80d..	TCP	86	[TCP Dup ACK 1#41] 50380 → 443 [ACK] Seq=71 Ack=105 Win=252 Len=0 SLE=1 SRE=105
19	15.404287	2404:6800:4009:80d..	2401:4900:1d08:4ef9..	TCP	74	443 → 50380 [ACK] Seq=105 Ack=36 Win=503 Len=0
20	15.443691	2404:6800:4009:80d..	2401:4900:1d08:4ef9..	TCP	74	443 → 50380 [ACK] Seq=105 Ack=71 Win=503 Len=0
21	15.463462	2404:6800:4009:80d..	2401:4900:1d08:4ef9..	TLSv1.2	410	Application Data
22	15.463462	2404:6800:4009:80d..	2401:4900:1d08:4ef9..	TCP	86	[TCP Dup ACK 2#41] 443 → 50380 [ACK] Seq=441 Ack=71 Win=503 Len=0 SLE=1 SRE=71
23	15.515585	2401:4900:1d08:4ef9..	2404:6800:4009:80d..	TCP	74	50380 → 443 [ACK] Seq=71 Ack=441 Win=251 Len=0
24	19.508531	2404:6800:4009:80d..	2401:4900:1d08:4ef9..	TLSv1.2	148	Application Data

```
> Frame 1: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{000825B72-8d
> 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: 2404:6800:4009:101d::5e
> Transmission Control Protocol, Src Port: 58707, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
```

Hex	Dec	Text
0000	0e 17 9b e8 1f b4 d0 65	.....e x.....
0010	78 97 d1 2d 86 dd 60 06	.....\$ I...N5
0020	9f 08 00 15 06 fe 24 01	.....\$ .I...N5
0030	49 00 1d 08 04 68 00 00	.....\$ .I...N5
0040	00 10 08 4e f9 35 b2	.....\$ .I...N5
0050	00 00 00 00 5e e5 53 01	.....\$ .I...N5
0060	bb 6f 66 dc 52 23	.....\$ .I...N5
0070	54 71 50 10 00 ff e5 38	TqP...8....

## • Non-Promiscuous mode

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
18	12.769009	2401:4900:1d08:4ef9..	2404:6800:4009:803..	UDP	99	64493 → 443 Len=37
19	12.981544	2401:4900:1d08:4ef9..	2404:6800:4009:803..	UDP	91	64493 → 443 Len=29
20	13.043936	2404:6800:4009:803..	2401:4900:1d08:4ef9..	UDP	89	443 → 64493 Len=27
21	13.248501	2401:4900:1d08:4ef9..	2404:6800:4009:803..	UDP	91	64493 → 443 Len=29
22	13.331828	2404:6800:4009:803..	2401:4900:1d08:4ef9..	UDP	89	443 → 64493 Len=27
23	13.538406	2401:4900:1d08:4ef9..	2404:6800:4009:803..	UDP	91	64493 → 443 Len=29
24	13.611627	2404:6800:4009:803..	2401:4900:1d08:4ef9..	UDP	90	443 → 64493 Len=28
25	13.823068	2401:4900:1d08:4ef9..	2404:6800:4009:803..	UDP	91	64493 → 443 Len=29
26	13.871038	2404:6800:4009:803..	2401:4900:1d08:4ef9..	UDP	90	443 → 64493 Len=28
27	14.076034	2401:4900:1d08:4ef9..	2404:6800:4009:803..	UDP	91	64493 → 443 Len=29
28	14.130652	2404:6800:4009:803..	2401:4900:1d08:4ef9..	UDP	90	443 → 64493 Len=28
29	14.537285	2401:4900:1d08:4ef9..	2404:6800:4009:803..	UDP	91	64493 → 443 Len=29
30	14.609251	2404:6800:4009:803..	2401:4900:1d08:4ef9..	UDP	90	443 → 64493 Len=28
31	15.423208	2401:4900:1d08:4ef9..	2404:6800:4009:803..	UDP	91	64493 → 443 Len=29
32	15.471845	2404:6800:4009:803..	2401:4900:1d08:4ef9..	UDP	90	443 → 64493 Len=28
33	17.087655	2401:4900:1d08:4ef9..	2404:6800:4009:803..	UDP	91	64493 → 443 Len=29
34	17.146162	2404:6800:4009:803..	2401:4900:1d08:4ef9..	UDP	90	443 → 64493 Len=28

```
> Frame 1: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{000825B72-8d
> 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: 2404:6800:4009:101d::200
> User Datagram Protocol, Src Port: 64493, Dst Port: 443
> Data (29 bytes)
```

Hex	Dec	Text
0000	0e 17 9b e8 1f b4 d0 65	.....e x.....
0010	78 97 d1 2d 86 dd 60 0b	.....\$ I...N5
0020	9f 08 00 15 06 fe 24 01	.....\$ .I...N5
0030	49 00 1d 08 04 68 00 00	.....\$ .I...N5
0040	00 10 08 4e f9 35 b2	.....\$ .I...N5
0050	00 00 00 00 5e e5 53 01	.....\$ .I...N5
0060	bb 6f 66 dc 52 23	.....\$ .I...N5
0070	54 71 50 10 00 ff e5 38	TqP...8....

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

## Capture

...using this filter:  Enter a capture filter ... All interfaces shown ▾

Wi-Fi  
VMware Network Adapter VMnet8  
Adapter for loopback traffic capture  
**Local Area Connection\* 12**  
Local Area Connection\* 11  
Local Area Connection\* 10  
Bluetooth Network Connection  
VMware Network Adapter VMnet1

**Learn**

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.4.9 (v4.4.9-0-g57bf67214076). You receive automatic updates.

## ICMPv6

No.	icmpv6	Source	Destination	Protocol	Length	Info
2	1.387199	fe80::c17:9bff:fee8...	2401:4900:1d08:4ef9...	ICMPv6	86	Neighbor Solicitation for 2401:4900:1d08:4ef9:35b2:3bac:145e:a9de from 0e:17:9b:e8:1f:b4
4	1.387413	2401:4900:1d08:4ef9...	fe80::c17:9bff:fee8...	ICMPv6	86	Neighbor Advertisement 2401:4900:1d08:4ef9:35b2:3bac:145e:a9de (sol, ovr) is at d0:65:78:97:d1:2d
153	15.516650	fe80::c17:9bff:fee8...	ff02::1	ICMPv6	142	Router Advertisement from 0e:17:9b:e8:1f:b4

ip.addr == 192.168.1.6

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.1.6

No.	Time	Source	Destination	Protocol	Length	Info
65	3.282983	13.89.179.9	192.168.1.6	TCP	54	443 → 56565 [FIN, ACK] Seq=1 Ack=2 Win=16386 Len=0
66	3.203059	192.168.1.6	13.89.179.9	TCP	54	56565 → 443 [ACK] Seq=2 Ack=2 Win=1021 Len=0
121	9.469685	192.168.1.6	104.208.16.90	TLSv1.2	1183	Application Data
122	9.469814	192.168.1.6	104.208.16.90	TCP	1466	52783 → 443 [ACK] Seq=1130 Ack=1 Win=1018 Len=1412 [TCP PDU reassembled in 123]
123	9.469814	192.168.1.6	104.208.16.90	TLSv1.2	291	Application Data
128	9.778997	104.208.16.90	192.168.1.6	TCP	54	443 → 52783 [ACK] Seq=1 Ack=2542 Win=16386 Len=0
129	9.778997	104.208.16.90	192.168.1.6	TCP	54	443 → 52783 [ACK] Seq=1 Ack=2779 Win=16385 Len=0
130	10.086034	104.208.16.90	192.168.1.6	TLSv1.2	508	Application Data
131	10.086134	192.168.1.6	104.208.16.90	TCP	54	52783 → 443 [ACK] Seq=2779 Ack=447 Win=1024 Len=0
162	15.363081	35.185.21.228	192.168.1.6	TCP	54	[TCP Keep-Alive] 443 → 55467 [ACK] Seq=0 Ack=2 Win=501 Len=0
163	15.363133	192.168.1.6	35.185.21.228	TCP	54	[TCP Keep-Alive ACK] 55467 → 443 [ACK] Seq=2 Ack=1 Win=255 Len=0
183	20.091408	192.168.1.6	104.208.16.90	TLSv1.2	1183	Application Data
184	20.091510	192.168.1.6	104.208.16.90	TCP	1466	52783 → 443 [ACK] Seq=3988 Ack=447 Win=1024 Len=1412 [TCP PDU reassembled in 185]
185	20.091510	192.168.1.6	104.208.16.90	TLSv1.2	347	Application Data
186	20.428486	104.208.16.90	192.168.1.6	TCP	66	443 → 52783 [ACK] Seq=447 Ack=3988 Win=16381 Len=0 SLE=5320 SRE=5613
187	20.428486	104.208.16.90	192.168.1.6	TCP	54	443 → 52783 [ACK] Seq=447 Ack=5613 Win=16386 Len=0
188	20.428486	104.208.16.90	192.168.1.6	TLSv1.2	501	Application Data
189	20.428609	192.168.1.6	104.208.16.90	TCP	54	52783 → 443 [ACK] Seq=5613 Ack=894 Win=1022 Len=0

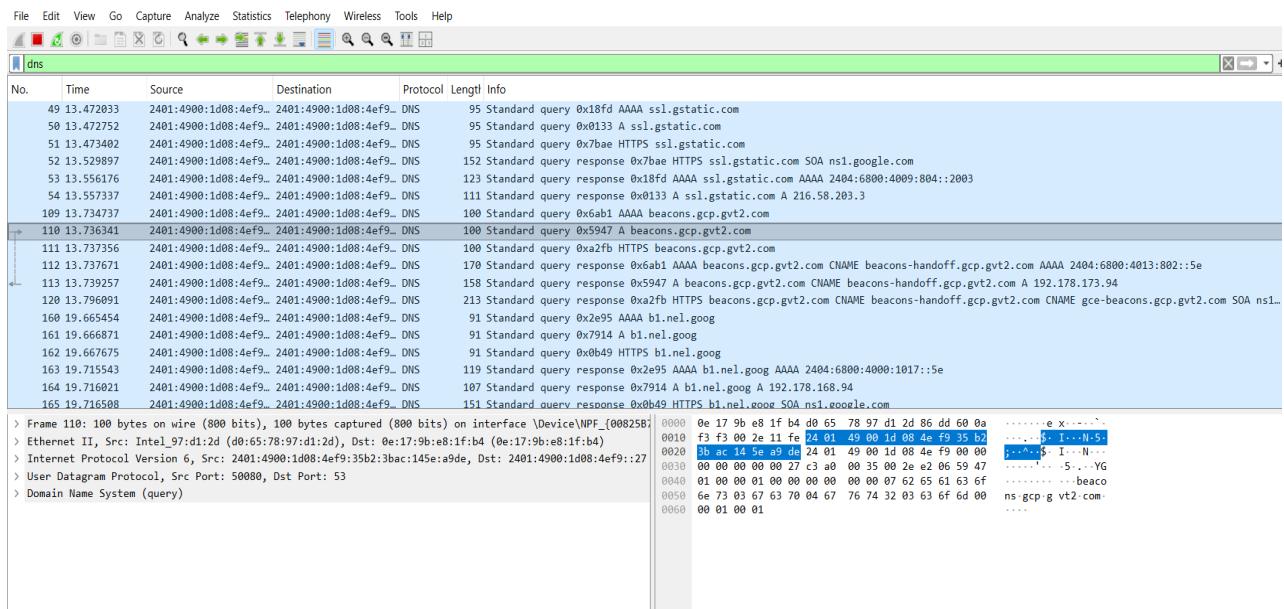
TLS

No.	tts	Time	Source	Destination	Protocol	Length	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_{00825b}							
> Ethernet II, Src: Intel_97:di: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:8							
> 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 0e 00 00 01 67 fd bf 01 bb c7 89 ea 40 48 7d .....g -.....@{}							
0040 5f 23 50 18 00 fe fa c0 00 00 17 03 03 00 40 fb _#P -.....@.							
0050 b6 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 0-\`., . ^...\$. {							
0080 34 f4 c3 65 63 3a dc b6 18 07 58 c6 9c 35 72 4-ec -.. X -5r							

## TCP

No.	tcp	Time	Source	Destination	Protocol	Length	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	5.127772	2401:4900:1d08:4ef9..	2404:6800:4009:803..	TCP	75 61899 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1		
18	5.163893	2404:6800:4009:803..	2401:4900:1d08:4ef9..	TCP	81 443 + 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	61 443 + 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_{00825b}							
> Ethernet II, Src: Intel_97:di: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:8							
> 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 0e 00 00 01 67 fd bf 01 bb c7 89 ea 40 48 7d .....g -.....@{}							
0040 5f 23 50 18 00 fe fa c0 00 00 17 03 03 00 40 fb _#P -.....@.							
0050 b6 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 0-\`., . ^...\$. {							
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**.