

Experiment – 7

Aim: To capture network traffic on your machine and analyze packets to understand how data travels over a network.

Objective: Capture and inspect network packets to understand the protocols in use and identify potential issues in the traffic.

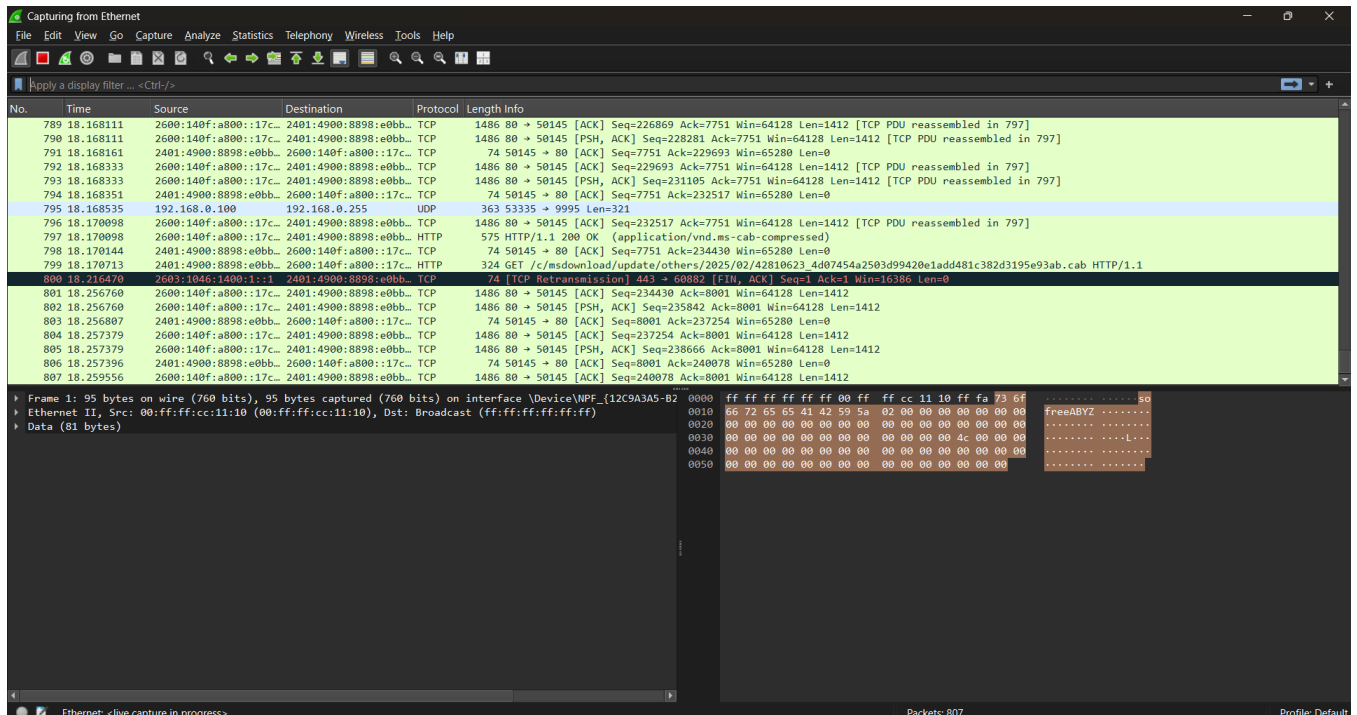
Theory:

Wireshark captures packets transmitted over a network and allows you to inspect them. It provides detailed information about each packet, including source and destination addresses, protocol types, and data payloads. Understanding this data is essential for network troubleshooting, security analysis, and protocol development.

Used **Commands** in Wireshark:

1. Start Capture:

- Go to Capture > Start or use the shortcut Ctrl + E to begin capturing packets.



2. Display Filters (to filter the traffic):

- Use display filters to narrow down the captured traffic based on criteria such as IP address, protocol, or port number.

- Example: `ip.addr == 192.168.1.1` (Filters packets to or from a specific IP address).

No.	Time	Source	Destination	Protocol	Length	Info
10	3.969799	192.168.1.1	192.168.1.6	ICMP	590	Destination unreachable (Fragmentation needed)
115	4.218076	192.168.1.6	192.168.1.1	NBNS	110	Refresh NB CODEINECASKET<00>
118	4.820577	192.168.1.1	192.168.1.255	UDP	363	36890 → 9995 Len=321
145	5.730083	192.168.1.6	192.168.1.1	NBNS	110	Refresh NB CODEINECASKET<00>
179	7.237737	192.168.1.6	192.168.1.1	NBNS	110	Refresh NB CODEINECASKET<00>
198	11.941081	192.168.1.1	192.168.1.255	UDP	363	36890 → 9995 Len=321
321	14.749983	192.168.1.1	192.168.1.6	ICMP	590	Destination unreachable (Fragmentation needed)
322	14.750354	192.168.1.1	192.168.1.6	ICMP	590	Destination unreachable (Fragmentation needed)
323	14.750354	192.168.1.1	192.168.1.6	ICMP	590	Destination unreachable (Fragmentation needed)
458	15.580743	192.168.1.1	192.168.1.6	ICMP	590	Destination unreachable (Fragmentation needed)
459	15.580743	192.168.1.1	192.168.1.6	ICMP	590	Destination unreachable (Fragmentation needed)
460	15.580743	192.168.1.1	192.168.1.6	ICMP	590	Destination unreachable (Fragmentation needed)
461	15.580743	192.168.1.1	192.168.1.6	ICMP	590	Destination unreachable (Fragmentation needed)
462	15.581347	192.168.1.1	192.168.1.6	ICMP	590	Destination unreachable (Fragmentation needed)
463	15.581347	192.168.1.1	192.168.1.6	ICMP	590	Destination unreachable (Fragmentation needed)
464	15.581347	192.168.1.1	192.168.1.6	ICMP	590	Destination unreachable (Fragmentation needed)
465	15.581862	192.168.1.1	192.168.1.6	ICMP	590	Destination unreachable (Fragmentation needed)
757	17.814123	192.168.1.6	192.168.1.1	NBNS	110	Refresh NB WORKGROUP<00>
912	19.163785	192.168.1.1	192.168.1.255	UDP	363	36890 → 9995 Len=321

Frame 10: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface Device\NPF_{12C9A3...}

Ethernet II, Src: ServercomPri_0c:22:40 (78:bb:1c:0c:22:40), Dst: ASUSTECOMPU_81:c3:83 (58:11:22:81:c3:83)

Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.6

Internet Control Message Protocol

```

0000  58 11 22 81 c3 83 78 bb c1 0c 22 40 08 00 45 c0 X "x"x"@E
0010  02 40 47 1d 0f 00 00 01 ad 88 c0 a8 01 01 c0 a8 @.@.@.@E
0020  01 06 03 04 0f 60 00 00 05 c0 45 00 05 dc 32 49 .....E-2I
0030  40 00 80 06 1c bf c0 a8 01 06 03 6f fe ba c2 d0 .....>
0040  01 b5 6e 4d 0e f9 0a 76 cf 4c 50 08 0e fa a4 05 ..FM-v..LP.....
0050  00 00 17 03 03 06 ff cc 60 3a 40 3a 40 3a 40 3a .....?>re:
0060  e9 29 7b 26 1b 93 50 53 8d 5e be 33 3a 5c 81 91 )(&-05<<3:..
0070  4d af 0a f5 ca 9 23 10 3f 3f 04 91 63 82 64 cc M....??cc.d
0080  0a 0e 0d 1f 88 98 53 c8 b4 6b 50 25 2f ef 14 80 .....SKP/...
0090  e1 44 20 11 47 26 7a d8 04 01 da 12 98 39 35 ....D-Pz....9-
00a0  2c 0e 08 48 5c 44 30 15 9b bb bf 6a 9f 07 1c 11 ...H.D@-3j...
00b0  e2 e1 67 c4 c0 06 f1 34 c1 fd 88 56 fc 5d 82 ..g @-4-V.R-...
00c0  fb 2b 4e a5 ce 6e 42 a0 f4 e2 f6 01 1f ea 87 de +N-F...
00d0  17 b8 12 68 55 db 7b 55 13 07 ca 6f 87 ad bf a2 hdu[....o
00e0  5b 36 40 b2 2e 47 0d 43 46 b5 c2 99 33 aa 2d bd kG.....F-z-K
00f0  e3 ae 56 68 4f 5c f1 71 ae 8b b0 b2 9a ba 5a 25 N^H\q...Z%
0100  bd 6f 65 8f b5 46 27 9a 05 8a 7c 7e c3 2e 25 41 oe.F'[]=-.SA
0110  f0 78 2d 28 29 a3 59 0e 0d cf 84 c8 70 e2 f9 a7 x-)Y....p.a
0120  5e 1e 70 7b 9f f3 63 00 fe 66 bb 7a 60 fa c0 64 ^p{...cf z.d
0130  0f 07 cd dd 09 01 c3 9c 6f 23 15 ad da 26 1e ..GF...da.26.
0140  8e 0f d9 ab d1 e1 f4 ee 99 be af f7 7e 06 de 0e ..K^N...O-e
0150  06 f2 d4 6d 33 87 43 83 8e 86 a3 d6 55 d3 5c fe ..m3 C3...U.V
0160  04 56 84 3a 9c 49 44 eb 32 57 21 d7 2f 5d bf V.:D.2W]]/]..

```

- Example: `tcp.port == 80` (Filters TCP packets on port 80, which is HTTP).

The image shows a Wireshark packet capture window titled "tcp.port == 80". The top pane displays a list of captured packets, highlighting packet 7 (HTTP GET) and packet 8 (HTTP 200 OK). The middle pane shows the details of the selected packet (packet 7), displaying the Ethernet II frame, Internet Protocol Version 4 header, and Hypertext Transfer Protocol fields. The bottom pane shows the raw packet bytes in hexadecimal and ASCII.

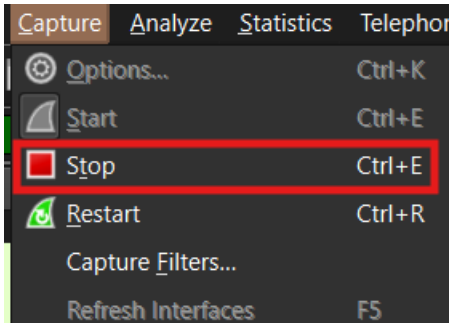
No.	Time	Source	Destination	Protocol	Length Info
180	7.356545	2401:4900:8898:e0bb::2404:6800:4002:811::...	2401:4900:8898:e0bb::2404:6800:4002:811::...	TCP	74 50043 → 80 [FIN, ACK] Seq=1 Ack=1 Win=255 Len=0
181	7.388902	2401:4900:8898:e0bb::2404:6800:4002:811::...	2401:4900:8898:e0bb::2404:6800:4002:811::...	TCP	74 80 → 50043 [FIN, ACK] Seq=1 Ack=2 Win=1052 Len=0
182	7.388943	2401:4900:8898:e0bb::2404:6800:4002:811::...	2401:4900:8898:e0bb::2404:6800:4002:811::...	TCP	74 50043 → 80 [ACK] Seq=2 Ack=2 Win=255 Len=0
178	14.220551	2401:4900:8898:e0bb::2404:6800:4002:811::...	2401:4900:8898:e0bb::2404:6800:4002:811::...	TCP	86 50145 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1432 WS=256 SACK_PERM
279	14.302948	2600:140f:a800::17c::2401:4900:8898:e0bb::2404:6800:4002:811::...	2600:140f:a800::17c::2401:4900:8898:e0bb::2404:6800:4002:811::...	TCP	86 80 → 50145 [SYN, ACK] Seq=0 Ack=1 Win=64800 Len=0 MSS=1440 SACK_PERM WS=128
280	14.303011	2401:4900:8898:e0bb::2404:6800:4002:811::...	2600:140f:a800::17c::2401:4900:8898:e0bb::2404:6800:4002:811::...	TCP	74 50145 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
281	14.303259	2401:4900:8898:e0bb::2404:6800:4002:811::...	2600:140f:a800::17c::2401:4900:8898:e0bb::2404:6800:4002:811::...	HTTP	324 GET /d/msdownload/update/others/2021/01/33356787_6b964b07151d3046dc549a1d3f61141af23bbd8.cab HTTP/1.1
282	14.384052	2600:140f:a800::17c::2401:4900:8898:e0bb::2404:6800:4002:811::...	2600:140f:a800::17c::2401:4900:8898:e0bb::2404:6800:4002:811::...	TCP	74 80 → 50145 [ACK] Seq=1 Ack=251 Win=64640 Len=0
283	14.386105	2600:140f:a800::17c::2401:4900:8898:e0bb::2404:6800:4002:811::...	2600:140f:a800::17c::2401:4900:8898:e0bb::2404:6800:4002:811::...	TCP	1486 80 → 50145 [ACK] Seq=1 Ack=251 Win=64640 Len=1412 [TCP PDU reassembled in 289]
284	14.386105	2600:140f:a800::17c::2401:4900:8898:e0bb::2404:6800:4002:811::...	2600:140f:a800::17c::2401:4900:8898:e0bb::2404:6800:4002:811::...	TCP	1486 80 → 50145 [PSH, ACK] Seq=1413 Ack=251 Win=64640 Len=1412 [TCP PDU reassembled in 289]
285	14.386105	2600:140f:a800::17c::2401:4900:8898:e0bb::2404:6800:4002:811::...	2600:140f:a800::17c::2401:4900:8898:e0bb::2404:6800:4002:811::...	TCP	1486 80 → 50145 [ACK] Seq=2825 Ack=251 Win=64640 Len=1412 [TCP PDU reassembled in 289]
286	14.386105	2600:140f:a800::17c::2401:4900:8898:e0bb::2404:6800:4002:811::...	2600:140f:a800::17c::2401:4900:8898:e0bb::2404:6800:4002:811::...	TCP	1486 80 → 50145 [PSH, ACK] Seq=4237 Ack=251 Win=64640 Len=1412 [TCP PDU reassembled in 289]
287	14.386162	2401:4900:8898:e0bb::2404:6800:4002:811::...	2600:140f:a800::17c::2401:4900:8898:e0bb::2404:6800:4002:811::...	TCP	74 50145 → 80 [ACK] Seq=251 Ack=5649 Win=65280 Len=0
288	14.386928	2600:140f:a800::17c::2401:4900:8898:e0bb::2404:6800:4002:811::...	2600:140f:a800::17c::2401:4900:8898:e0bb::2404:6800:4002:811::...	TCP	1486 80 → 50145 [ACK] Seq=5649 Ack=251 Win=64640 Len=1412 [TCP PDU reassembled in 289]
289	14.386986	2600:140f:a800::17c::2401:4900:8898:e0bb::2404:6800:4002:811::...	2600:140f:a800::17c::2401:4900:8898:e0bb::2404:6800:4002:811::...	HTTP	435 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
290	14.386996	2401:4900:8898:e0bb::2404:6800:4002:811::...	2600:140f:a800::17c::2401:4900:8898:e0bb::2404:6800:4002:811::...	TCP	74 50145 → 80 [ACK] Seq=251 Ack=7422 Win=65280 Len=0
291	14.387742	2401:4900:8898:e0bb::2404:6800:4002:811::...	2600:140f:a800::17c::2401:4900:8898:e0bb::2404:6800:4002:811::...	HTTP	324 GET /c/msdownload/update/others/2021/01/33356784_31f6eaff6d5437fd7700835aa29b58168ae2a3b6.cab HTTP/1.1
292	14.470241	2600:140f:a800::17c::2401:4900:8898:e0bb::2404:6800:4002:811::...	2600:140f:a800::17c::2401:4900:8898:e0bb::2404:6800:4002:811::...	TCP	1486 80 → 50145 [ACK] Seq=7422 Ack=501 Win=64512 Len=1412 [TCP PDU reassembled in 299]
293	14.470241	2600:140f:a800::17c::2401:4900:8898:e0bb::2404:6800:4002:811::...	2600:140f:a800::17c::2401:4900:8898:e0bb::2404:6800:4002:811::...	TCP	1486 80 → 50145 [PSH, ACK] Seq=8834 Ack=501 Win=64512 Len=1412 [TCP PDU reassembled in 299]

Packet Details:

- Ethernet II, Src: ASUSTekCOMPU_Bit:c3:83 (58:11:22:81:c3:83), Dst: ServercomPri_0c:22:40 (78:bb:c1:0c:22:40)**
- Internet Protocol Version 4,**

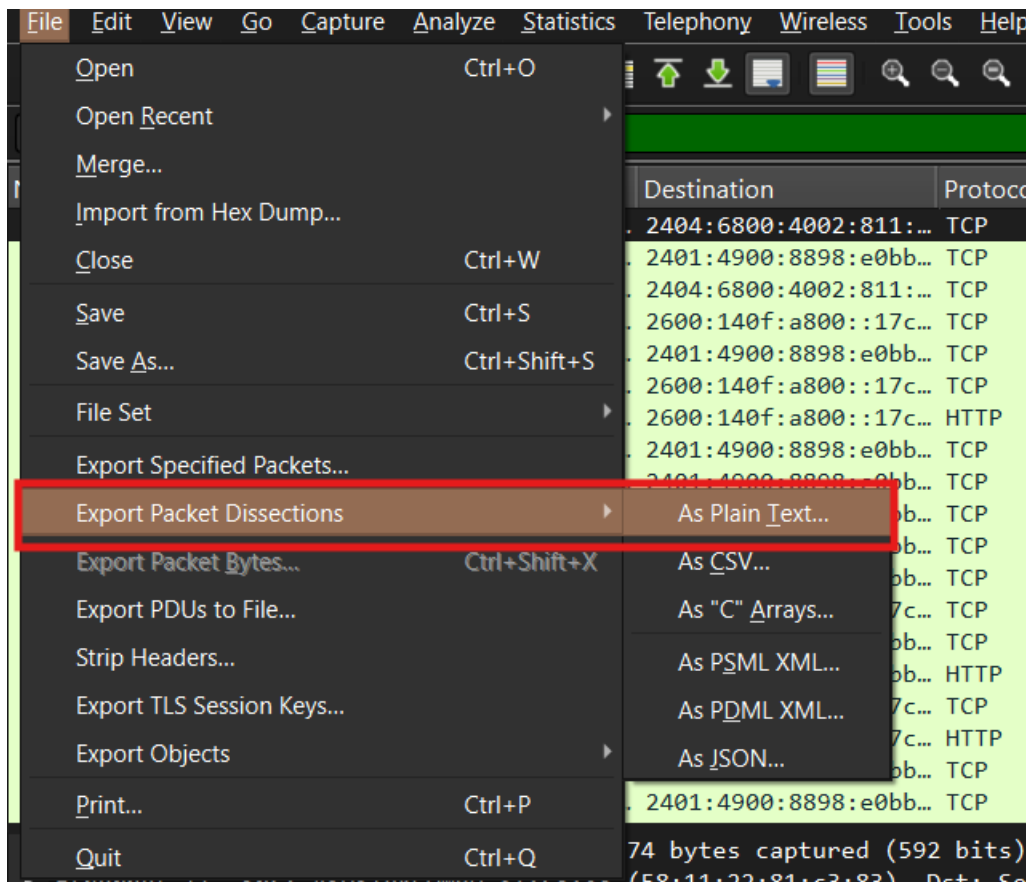
3. Stop Capture:

- Go to Capture > Stop or press Ctrl + E to stop the capture.



4. Export Packet Capture:

- Go to File > Export Packet Dissections > As Plain Text to save captured packets for later analysis.



Conclusion: By capturing and analyzing network packets with Wireshark, we gain insights into data transmission, protocols, and potential network issues. Filtering traffic helps focus on specific IPs, protocols, or ports for detailed inspection. Understanding captured packets is crucial for troubleshooting, security monitoring, and protocol analysis. Wireshark serves as a powerful tool for network analysis and diagnostics.