

Objective: Capture live network packets and identify basic protocols and traffic types.

Tools: Wireshark (free).

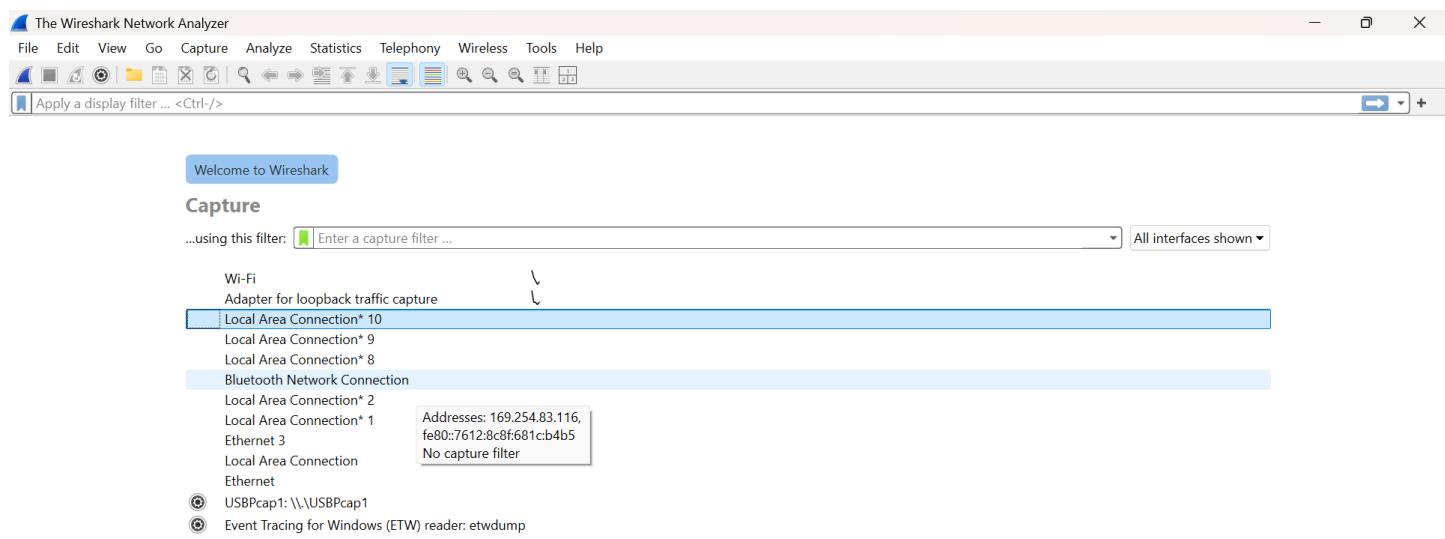
Deliverables: A packet capture (.pcap) file and a short report of protocols identified.

1. Install Wireshark.

Already installed

2. Start capturing on your active network interface.

- a) Open **Wireshark**.
- b) On the home screen, identify your **active interface** (Wi-Fi or Ethernet shows moving lines).
- c) Double-click the active interface to start capturing packets.



Learn

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#) · [SharkFest](#) · [Wireshark Discord](#) · [Donate](#)

You are running Wireshark 4.6.2 (v4.6.2-0-g24d5e2b5a3dc). You receive automatic updates.



3. Browse a website or ping a server to generate traffic.

- Open a web browser and visit any website (e.g., google.com).
- This generates DNS, TCP, and ICMP traffic.

The figure shows a Wireshark interface with the following details:

- Capturing from Wi-Fi**: The main title bar.
- File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help**: The menu bar.
- Apply a display filter ... <Ctrl-/>**: The search/filter bar.
- No. Time Source Destination Protocol Length Info**: The column headers for the packet list.
- Packets: 7**: The total number of captured packets.
- Profile: Default**: The current profile.
- Wi-Fi: live capture in progress**: Status message at the bottom left.
- Packet List (7 entries):**
 - 1 0.000000 192.168.1.7 85.17.155.52 TCP 55 46257 → 9166 [ACK] Seq=1 Ack=1 Win=255 Len=1
 - 2 0.289557 20.195.65.193 192.168.1.7 TLSv1.2 158 Application Data
 - 3 0.289557 20.195.65.193 192.168.1.7 TLSv1.2 158 Application Data
 - 4 0.337531 192.168.1.7 20.195.65.193 TCP 54 54592 → 443 [ACK] Seq=1 Ack=105 Win=511 Len=0
 - 5 0.337538 192.168.1.7 20.195.65.193 TCP 54 13656 → 443 [ACK] Seq=1 Ack=105 Win=255 Len=0
 - 6 1.657666 192.168.1.7 142.251.10.188 TCP 55 40879 → 5228 [ACK] Seq=1 Ack=1 Win=253 Len=1
 - 7 1.732307 142.251.10.188 192.168.1.7 TCP 70 5228 → 40879 [ACK] Seq=1 Ack=2 Win=1047 Len=0 SRE=1 SRE=2
- Selected Hex Dump (Frame 1):**
 - Frame 1: Packet, 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface
 - Ethernet II, Src: Intel_1a:34:4d (a0:51:0b:1a:34:4d), Dst: GenexisInter_8b:4c:70 (bc:6
 - Internet Protocol Version 4, Src: 192.168.1.7, Dst: 85.17.155.52
 - Transmission Control Protocol, Src Port: 46257, Dst Port: 9166, Seq: 1, Ack: 1, Len: 1
 - Data (1 byte)

Hex dump of Frame 1:
0000 bc 62 d2 8b 4c 70 a0 51 0b 1a 34 4d 08 00 45 00 ·b·Lp·Q···4M·E·
0010 00 29 8f 3f 40 00 80 06 b9 9a c0 a8 01 07 55 11 ·)·?@···U·
0020 9b 34 b4 b1 23 ce 04 f7 be 0e 1f c0 5d c2 50 10 ·4·#···]P·
0030 00 ff e3 d7 00 00 00
.....

4. Stop capture after a minute.

The screenshot shows a Wi-Fi network monitor interface with the following details:

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
411	11.586796	185.199.110.154	192.168.1.7	TCP	54	443 → 40044 [ACK] Seq=7529 Ack=2574 Win=152576 Len=0
412	11.586796	185.199.110.154	192.168.1.7	TLSv1.3	4410	Application Data, Application Data, Application Data
413	11.586842	192.168.1.7	185.199.110.154	TCP	54	40044 → 443 [ACK] Seq=2605 Ack=11885 Win=65280 Len=0
414	11.587532	185.199.110.154	192.168.1.7	TLSv1.3	16026	Application Data, Application Data, Application Data, Application Data, Application Data, Application Data
415	11.587532	185.199.110.154	192.168.1.7	TLSv1.3	215	Application Data
416	11.587532	185.199.110.154	192.168.1.7	TLSv1.3	7314	Application Data, Application Data, Application Data, Application Data, Application Data
417	11.587532	185.199.110.154	192.168.1.7	TCP	403	[TCP Previous segment not captured] 443 → 40044 [PSH, ACK] Seq=42538 Ack=2574 Win=152576 Len=0
418	11.587532	185.199.110.154	192.168.1.7	TCP	60	443 → 40044 [ACK] Seq=42887 Ack=2605 Win=152576 Len=0
419	11.587532	185.199.110.154	192.168.1.7	TLSv1.3	7314	[TCP Out-Of-Order] , Application Data, Application Data, Application Data, Application Data, Application Data, Application Data
420	11.587607	192.168.1.7	185.199.110.154	TCP	66	40044 → 443 [ACK] Seq=2605 Ack=35278 Win=65280 Len=0 SLE=42538 SRE=42887
421	11.587661	192.168.1.7	185.199.110.154	TCP	54	40044 → 443 [ACK] Seq=2605 Ack=42887 Win=65280 Len=0
422	11.614652	192.168.1.7	185.199.110.154	TLSv1.3	141	Application Data
423	11.617847	185.199.110.154	192.168.1.7	TCP	60	443 → 40044 [ACK] Seq=42887 Ack=2692 Win=152576 Len=0

Total Length: 7300
Identification: 0xe3c (7740)
> 010. = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 59
Protocol: TCP (6)
Header Checksum: 0xb27 [validation disabled]
[Header checksum status: Unverified]
Source Address: 185.199.110.154
Destination Address: 192.168.1.7
[Stream index: 19]

Transmission Control Protocol, Src Port: 443, Dst Port: 40044, Seq: 35278, Ack: 2574
Source Port: 443
Destination Port: 40044

Packet (7314 bytes) Reassembled TCP (1400 bytes)

Packets: 8777 · Dropped: 0 (0.0%) || Profile: Default

Destination Address (ip.dst), 4 bytes

Search

ENG IN 19:26 16-12-2025

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
357	11.3870306	192.168.1.7	142.250.193.14	QUIC	77	Protected Payload (KPO), DCID=ec200159043d579c
358	11.387401	20.207.73.82	192.168.1.7	TLSv1.3	2926	Application Data, Application Data
359	11.387567	192.168.1.7	20.207.73.82	TCP	54	41769 → 443 [ACK] Seq=2724 Ack=6585 Win=65280 Len=0
360	11.387902	20.207.73.82	192.168.1.7	TLSv1.3	1490	Application Data
361	11.387902	20.207.73.82	192.168.1.7	TLSv1.3	1490	Application Data
362	11.387902	20.207.73.82	192.168.1.7	TLSv1.3	1490	Application Data
363	11.387902	20.207.73.82	192.168.1.7	TLSv1.3	2926	Application Data, Application Data
364	11.388047	192.168.1.7	20.207.73.82	TCP	54	41769 → 443 [ACK] Seq=2724 Ack=13765 Win=65280 Len=0
365	11.388436	20.207.73.82	192.168.1.7	TLSv1.3	1490	Application Data
366	11.388436	20.207.73.82	192.168.1.7	TLSv1.3	1490	Application Data
367	11.388436	20.207.73.82	192.168.1.7	TLSv1.3	1490	Application Data
368	11.388613	192.168.1.7	20.207.73.82	TCP	54	41769 → 443 [ACK] Seq=2724 Ack=18073 Win=65280 Len=0
369	11.404665	142.250.193.14	192.168.1.7	QUIC	70	Protected Payload (KPO)

Internet Protocol Version 4, Src: 192.168.1.7, Dst: 35.163.30.11

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x3a00 (14848)
> 010. = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0xbdb72 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.7
Destination Address: 35.163.30.11
....

0000 bc 62 d2 8b 4c 70 a0 51 0b 1a 34 4d 08 00 45 00 b · Lp Q · 4M · E ·
0010 00 28 3a 00 40 00 80 06 bd 72 c0 a8 01 07 23 a3 (: @ · r · # ·
0020 1e 0b 8f 18 01 bb 10 fb 10 24 78 ff 79 ea 50 14 \$x y P ·
0030 00 00 07 97 00 00

wireshark_Wi-FiBDPUH3.pcapng

Packets: 8777 · Dropped: 0 (0.0%)

Profile: Default

6 19:28 16-12-2025

5. Filter captured packets by protocol (e.g., HTTP, DNS, TCP).
6. Identify at least 3 different protocols in the capture.

a. TCP

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
2311	19.949108	192.168.1.7	185.145.245.53	TCP	54	23586 → 443 [ACK] Seq=3183 Ack=65919 Win=65280 Len=0
2304	19.743582	192.168.1.7	185.145.245.53	TCP	54	23586 → 443 [ACK] Seq=3183 Ack=54303 Win=65280 Len=0
2302	19.743246	192.168.1.7	185.145.245.53	TCP	54	23586 → 443 [ACK] Seq=3183 Ack=32523 Win=65280 Len=0
2268	19.574982	192.168.1.7	185.145.245.53	TCP	54	23586 → 443 [ACK] Seq=3183 Ack=25263 Win=65280 Len=0
2267	19.574900	185.145.245.53	192.168.1.7	TCP	5862	443 → 23586 [PSH, ACK] Seq=19455 Ack=3183 Win=61312 Len=5808 [TCP PDU reassembled in 2301]
2266	19.574752	192.168.1.7	185.145.245.53	TCP	54	23586 → 443 [ACK] Seq=3183 Ack=19455 Win=65280 Len=0
2265	19.574633	185.145.245.53	192.168.1.7	TCP	8766	443 → 23586 [PSH, ACK] Seq=10743 Ack=3183 Win=61312 Len=8712 [TCP PDU reassembled in 2301]
2255	19.403362	85.17.70.38	192.168.1.7	TCP	54	9166 → 63515 [ACK] Seq=1 Ack=966 Win=41472 Len=0
2226	19.215178	192.168.1.7	85.17.70.38	TCP	54	63515 → 9166 [ACK] Seq=1 Ack=1 Win=65280 Len=0
2224	19.215098	85.17.70.38	192.168.1.7	TCP	66	9166 → 63515 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=1452 SACK_PERM WS=512
2102	19.029397	192.168.1.7	85.17.70.38	TCP	66	63515 → 9166 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
2085	18.959620	57.144.49.32	192.168.1.7	TCP	54	443 → 27147 [ACK] Seq=302 Ack=145 Win=376 Len=0
2083	18.863535	192.168.1.7	57.144.49.32	TCP	54	27147 → 443 [ACK] Seq=71 Ack=302 Win=251 Len=0
2081	18.324388	172.64.151.4	192.168.1.7	TCP	60	443 → 1855 [ACK] Seq=438 Ack=496 Win=17 Len=0
2080	18.324388	172.64.151.4	192.168.1.7	TCP	60	443 → 1855 [ACK] Seq=438 Ack=376 Win=17 Len=0

Frame 2224: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface Ethernet II, Src: GenexisInter_8b:4c:70 (bc:62:d2:8b:4c:70), Dst: Intel_1a:34:4d (a0:51:00:00:00:00)
Internet Protocol Version 4, Src: 85.17.70.38, Dst: 192.168.1.7
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 52
Identification: 0x0000 (0)
> 010. = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 47
Protocol: TCP (6)

0000 a0 51 0b 1a 34 4d bc 62 d2 8b 4c 70 08 00 45 00 Q · 4M · b · Lp Q · 4M · E ·
0010 00 34 00 00 40 00 2f 06 ee dd 55 11 46 26 c0 a8 4 · @ / · U · F & ·
0020 01 07 23 ce f8 1b be e6 2c 42 06 08 65 36 80 12 # · , B · e6 ·
0030 a5 64 fa 6a 00 00 02 04 05 ac 01 01 04 02 01 03 d · j ·

0040 03 09

Transmission Control Protocol: Protocol

Packets: 8777 · Displayed: 1143 (13.0%) · Dropped: 0 (0.0%)

Profile: Default

6 19:36 16-12-2025

b. HTTP

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
2229	19.219188	192.168.1.7	85.17.70.38	HTTP	1019	GET /CLogin?key=VUx8QAA1YxtuPDEXWgpwBHBcX203NS0RffVdH3kMV1BUB1pDOSUMUVQdKhJwDndFXWAGUy01LVR8UiEdf...

Frame 2229: Packet, 1019 bytes on wire (8152 bits), 1019 bytes captured (8152 bits) on Ethernet II, Src: Intel_1a:34:4d (a0:51:0b:1a:34:4d), Dst: GenexisInter_8b:4c:70 (bc:62:00:ff:8d:47) Version: 4 Internet Protocol Version 4, Src: 192.168.1.7, Dst: 85.17.70.38

0100 = Version: 4
 ... 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 1005
 Identification: 0xa158 (41304)
 > 010 = Flags: 0x2, Don't fragment
 ... 0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 128
 Protocol: TCP (6)

0000 bc 62 d2 8b 4c 70 a0 51 0b 1a 34 4d 08 00 45 00 -b..Lp.Q ..4M..E.
 0010 03 ed a1 58 40 00 08 06 f8 cb c0 a8 01 07 55 11 ...X@...U.
 0020 46 26 f8 1b 23 ce 06 08 65 36 be e6 2c 43 50 18 F&..#... e6...,CP.
 0030 00 ff 8d 47 00 00 47 45 54 20 2f 43 4c 6f 67 69 ...G..GE T /Clogi
 0040 6a 3f 6b 65 79 3d 56 55 78 38 51 41 41 6c 59 78 n?key=VU x8QAA1Yx
 0050 74 75 50 44 45 58 57 67 70 77 42 48 42 63 58 32 tuPDEXNg pwBHBCx2
 0060 30 33 4e 53 30 52 66 46 56 64 48 33 6b 4d 56 6c 03NS0Rff VdH3kMV1
 0070 42 55 42 31 70 44 4f 53 55 4d 55 56 51 64 4b 68 BU81p0S UMUVQdkh
 0080 4a 77 44 6e 64 46 58 57 41 47 55 79 30 31 4c 56 JwDndFXW AGUy01LV
 0090 52 38 55 69 45 64 66 51 74 2f 56 58 34 48 59 30 R8UiEdfq t/VX4HY0
 00a0 34 74 4e 57 78 58 62 53 41 31 43 47 42 52 66 31 4tNWxxbs A1CBFRf1
 00b0 39 6a 63 33 5a 50 4c 44 49 68 55 6e 68 38 50 52 9jc3ZPLD IhUnh8PR
 00c0 4a 71 4d 6e 51 4d 66 32 4a 6a 41 79 6f 4c 51 67 JqMnQMf2 JjAyoLQg
 00d0 74 75 56 79 46 51 63 41 6c 57 32 70 67 41 67 tuVxFQcA lWv2pgAg
 00e0 67 35 4d 52 4d 4e 59 46 45 54 41 6d 46 55 41 45 g5MRMNYF EPAmFUAE

Hypertext Transfer Protocol: Protocol

Packets: 8777 - Displayed: 1 (0.0%) - Dropped: 0 (0.0%) || Profile: Default

Search

19:37 16-12-2025

c. ICMP

Wireshark.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Protocol	Source	Destination	Length	Info
5490	icmp	192.168.1.1	192.168.1.7	102	Echo (ping) request id=0xd46f, seq=256/1, ttl=64 (no response found!)
6134	icmp	192.168.1.1	192.168.1.7	102	Echo (ping) request id=0xd46f, seq=0/0, ttl=64 (no response found!)
5625	icmp	39.199472	192.168.1.1	102	Echo (ping) request id=0xef6e, seq=256/1, ttl=64 (no response found!)
5623	icmp	38.169683	192.168.1.1	102	Echo (ping) request id=0xef6e, seq=0/0, ttl=64 (no response found!)

Frame 5623: Packet, 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on Ethernet II, Src: GenexisInter_8b:4c:70 (bc:62:d2:8b:4c:70), Dst: Intel_1a:34:4d (a0:51:0b:1a:34:4d) Version: 4 Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.7

0100 = Version: 4
 ... 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 84
 Identification: 0x4deb (19947)
 > 010 = Flags: 0x2, Don't fragment
 ... 0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 64

0000 a0 51 0b 1a 34 4d bc 62 d2 8b 4c 70 81 00 00 00 Q..4M..b ..Lp....
 0010 08 00 45 00 00 54 4d eb 40 00 40 01 69 65 c0 a8 ..E..TM. @..ie..
 0020 01 01 c0 a8 01 07 08 00 76 8c ef 6e 00 00 11 64v..n..d
 0030 41 69 f0 a5 0d 00 08 00 00 00 08 00 00 00 00 00 Ai.....
 0040 00 00 08 00 00 00 08 00 00 00 08 00 00 00 00 00
 0050 00 00 e0 10 f1 7f 38 00 00 00 00 00 00 00 00 008.....
 0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

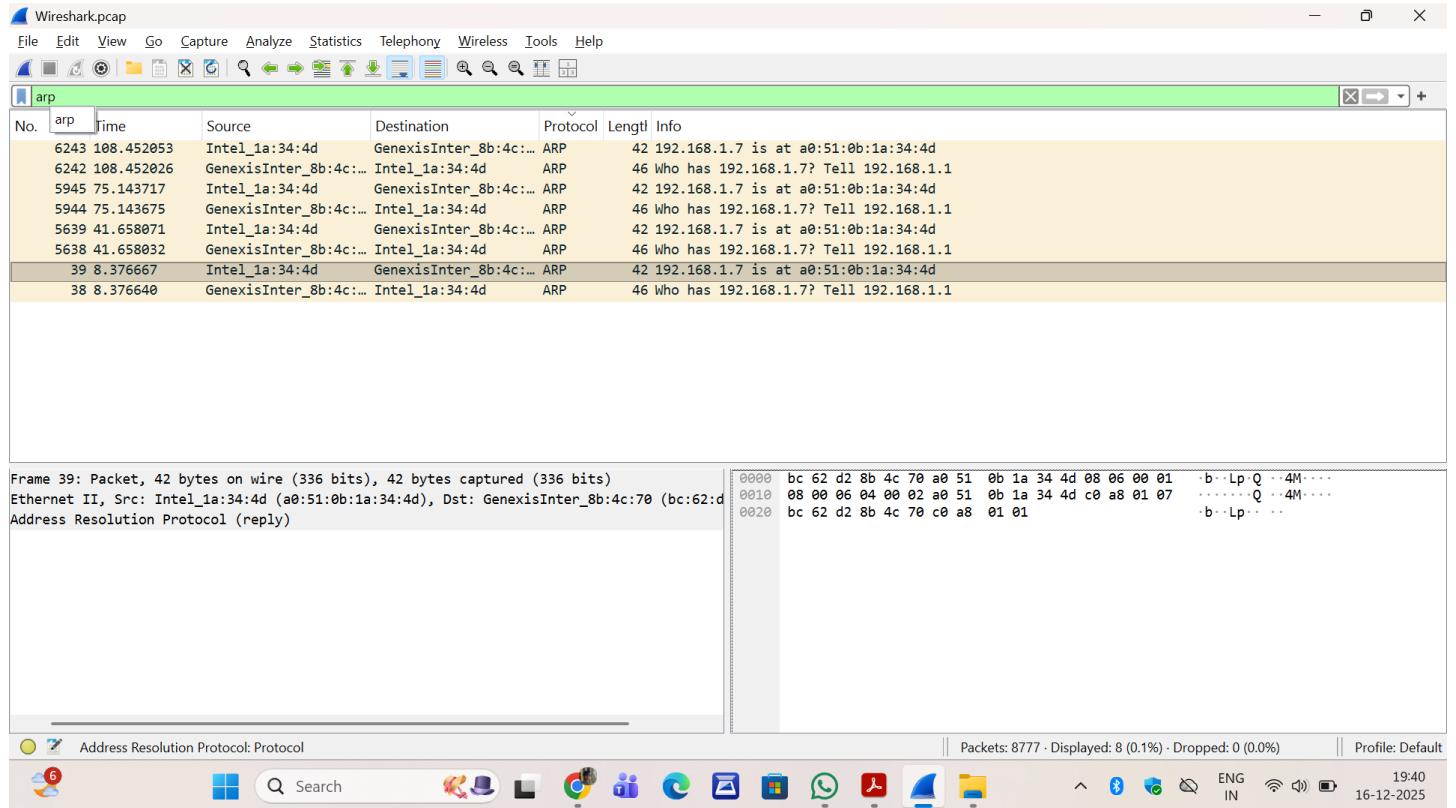
Internet Control Message Protocol: Protocol

Packets: 8777 - Displayed: 4 (0.0%) - Dropped: 0 (0.0%) || Profile: Default

Search

19:39 16-12-2025

d. ARP



7. Save as .pcap file

8. Summarize

Wireshark was used to capture live network traffic on the active network interface. The capture contained multiple protocols including DNS, TCP, and HTTP/ICMP. DNS packets were observed during website access for domain name resolution. TCP packets formed the majority of traffic, indicating reliable data transfer. ICMP packets were captured during ping requests, showing echo request and reply messages. The captured traffic demonstrates normal network communication behavior.