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

Tools: Wireshark (free).

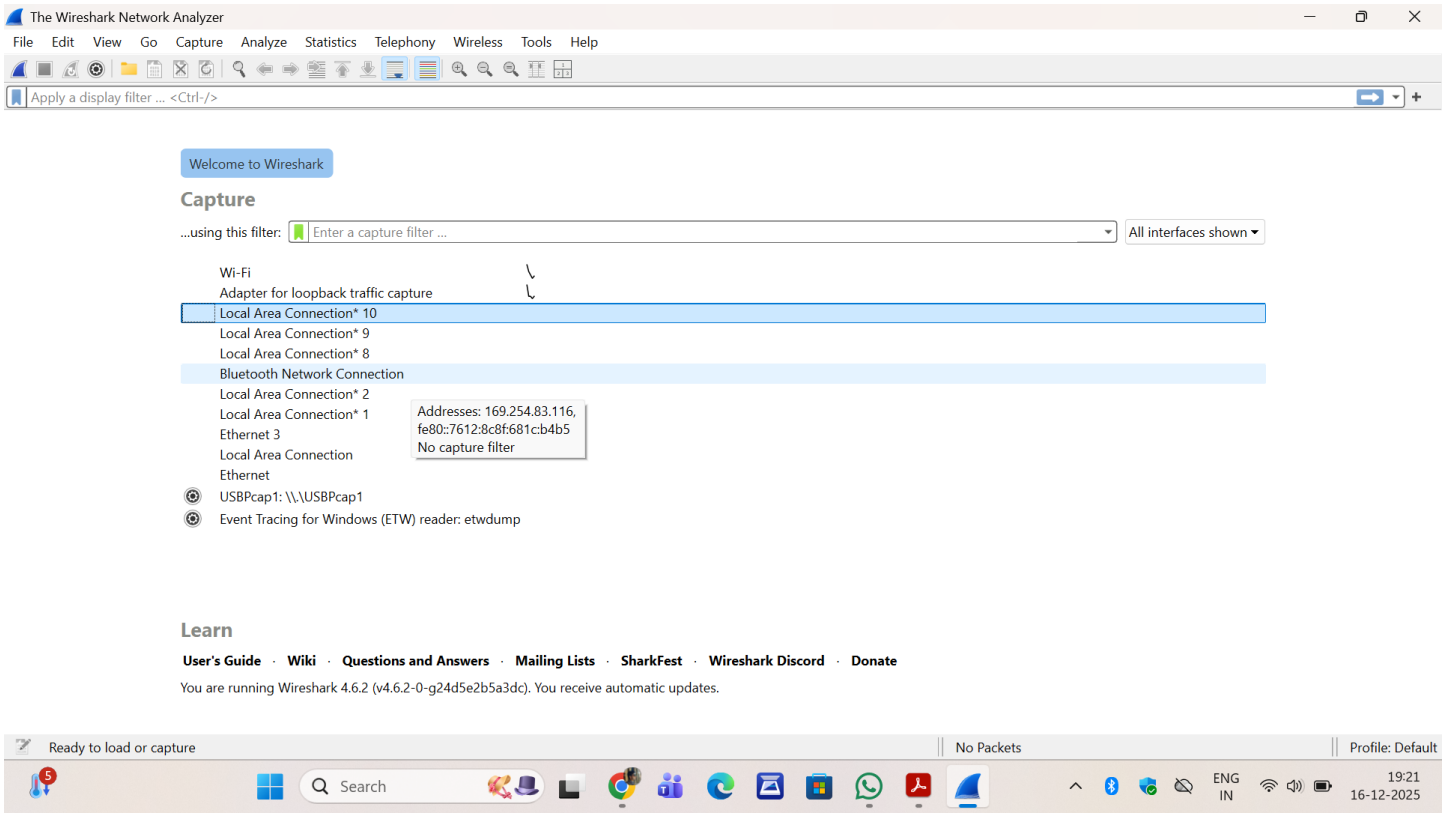
Deliverables: A packet capture (.pcap) file and a short report of protocols identified.

1. Install Wireshark.

Already installed

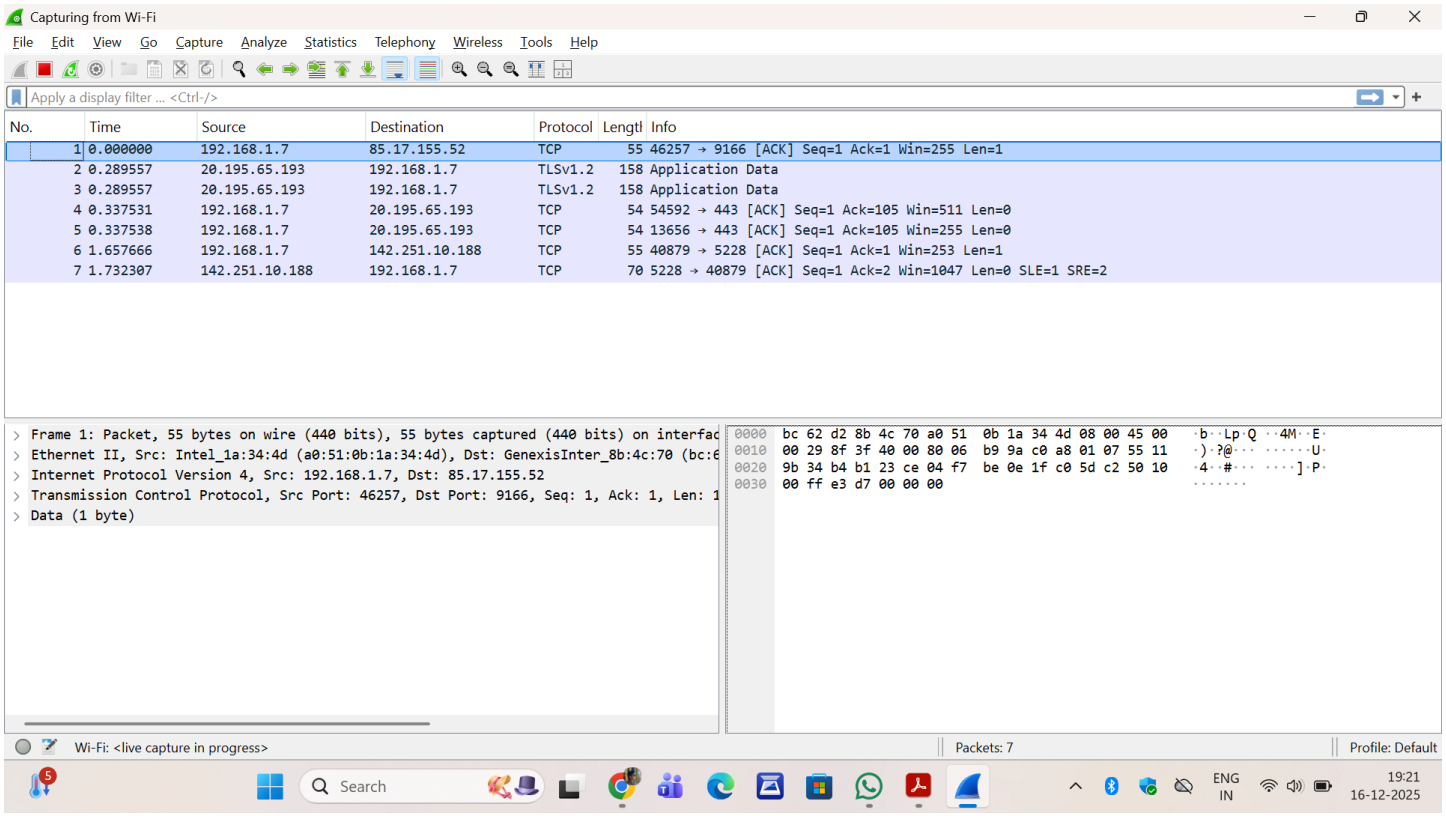
2. Start capturing on your active network interface.

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.

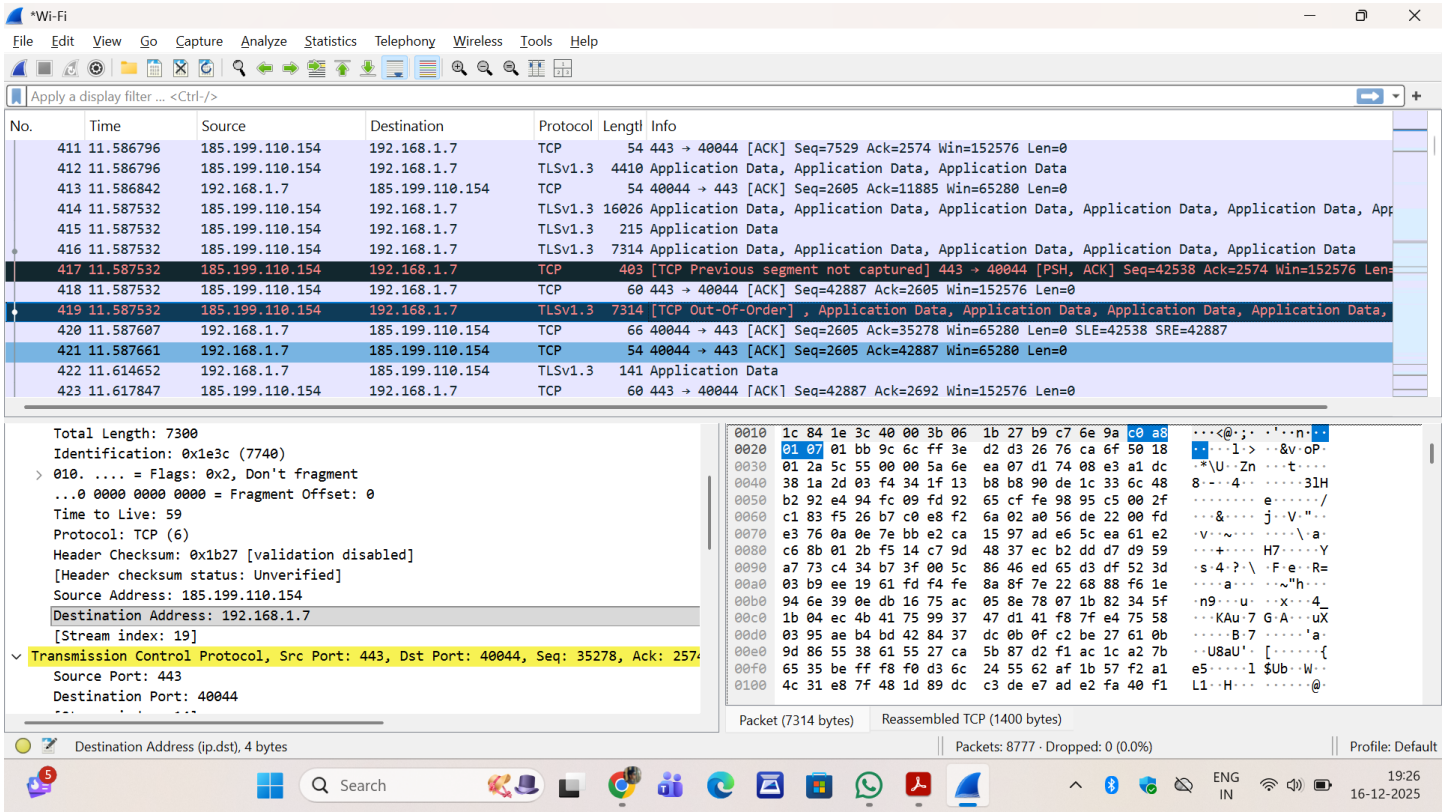


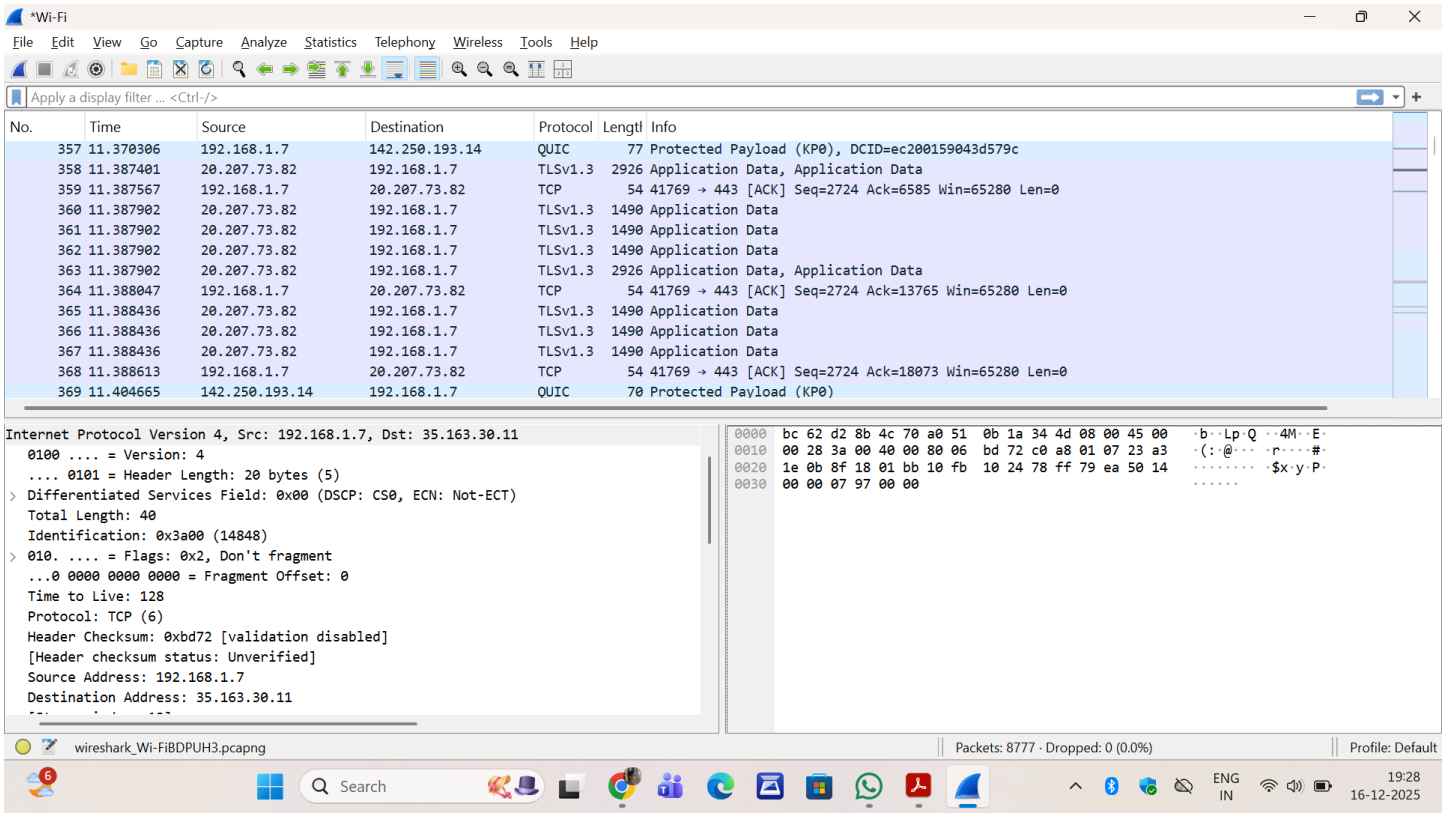
3. Browse a website or ping a server to generate traffic.

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



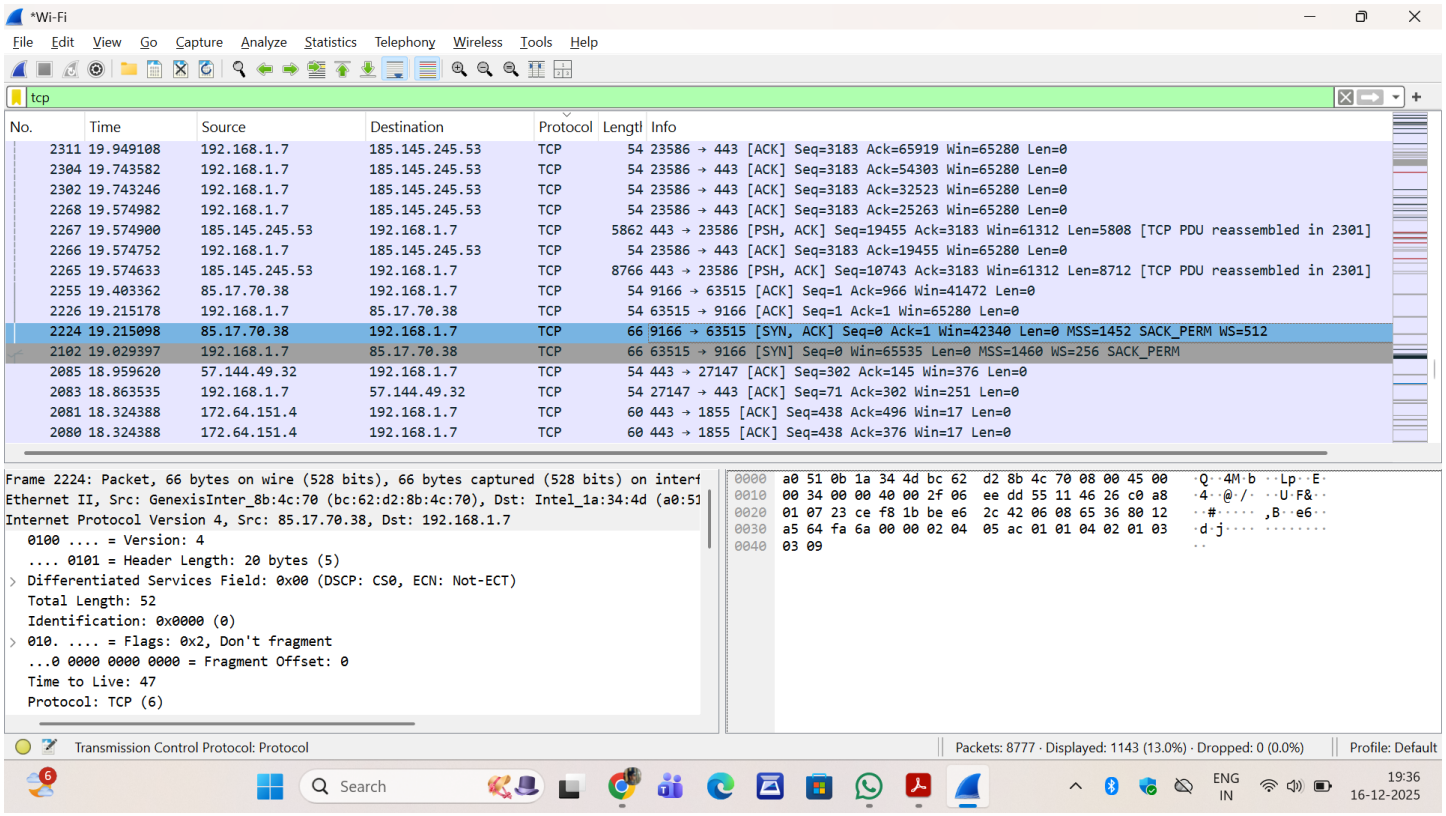
4. Stop capture after a minute.



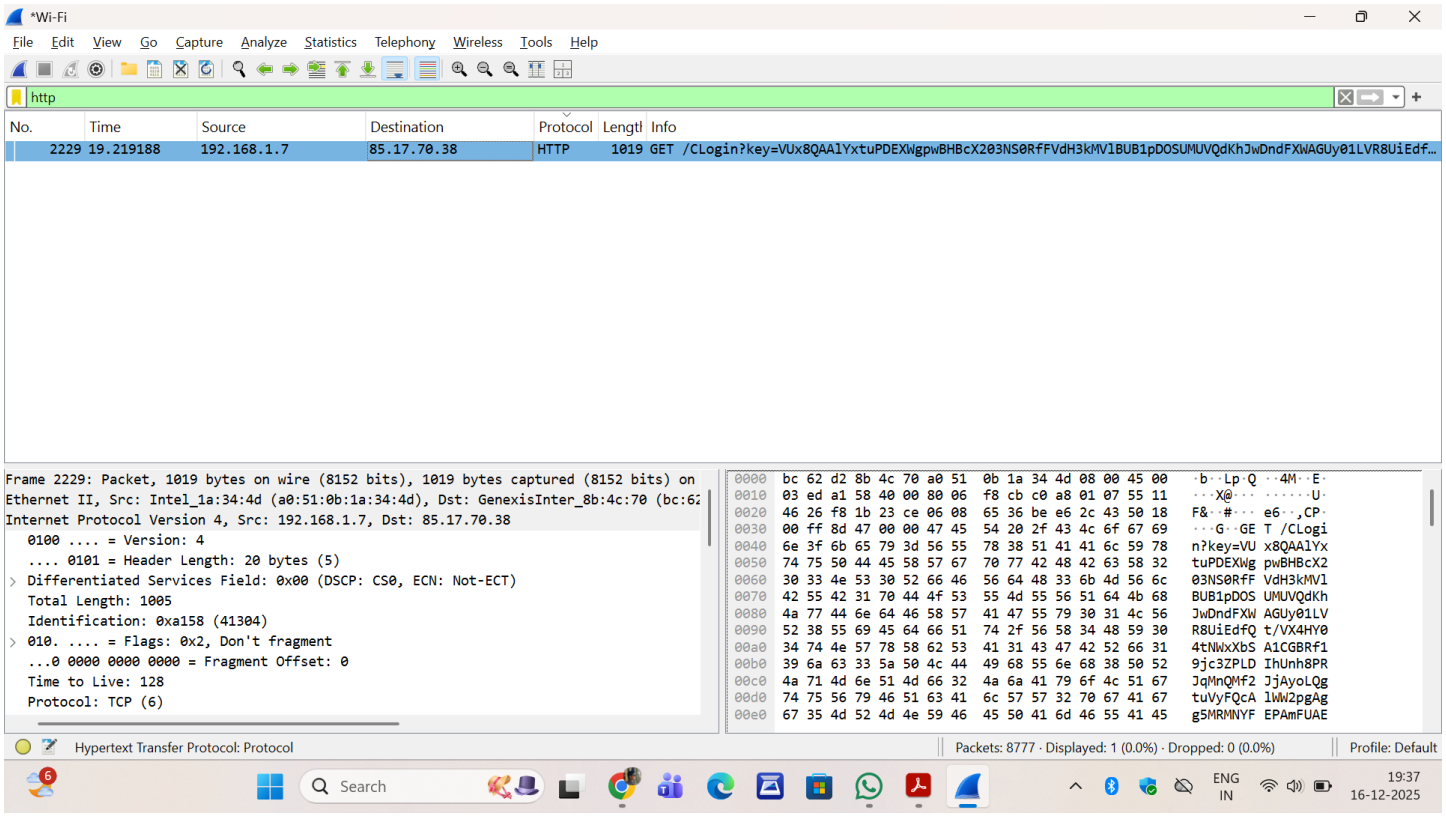


5. **Filter captured packets by protocol (e.g., HTTP, DNS, TCP).**
6. **Identify at least 3 different protocols in the capture.**

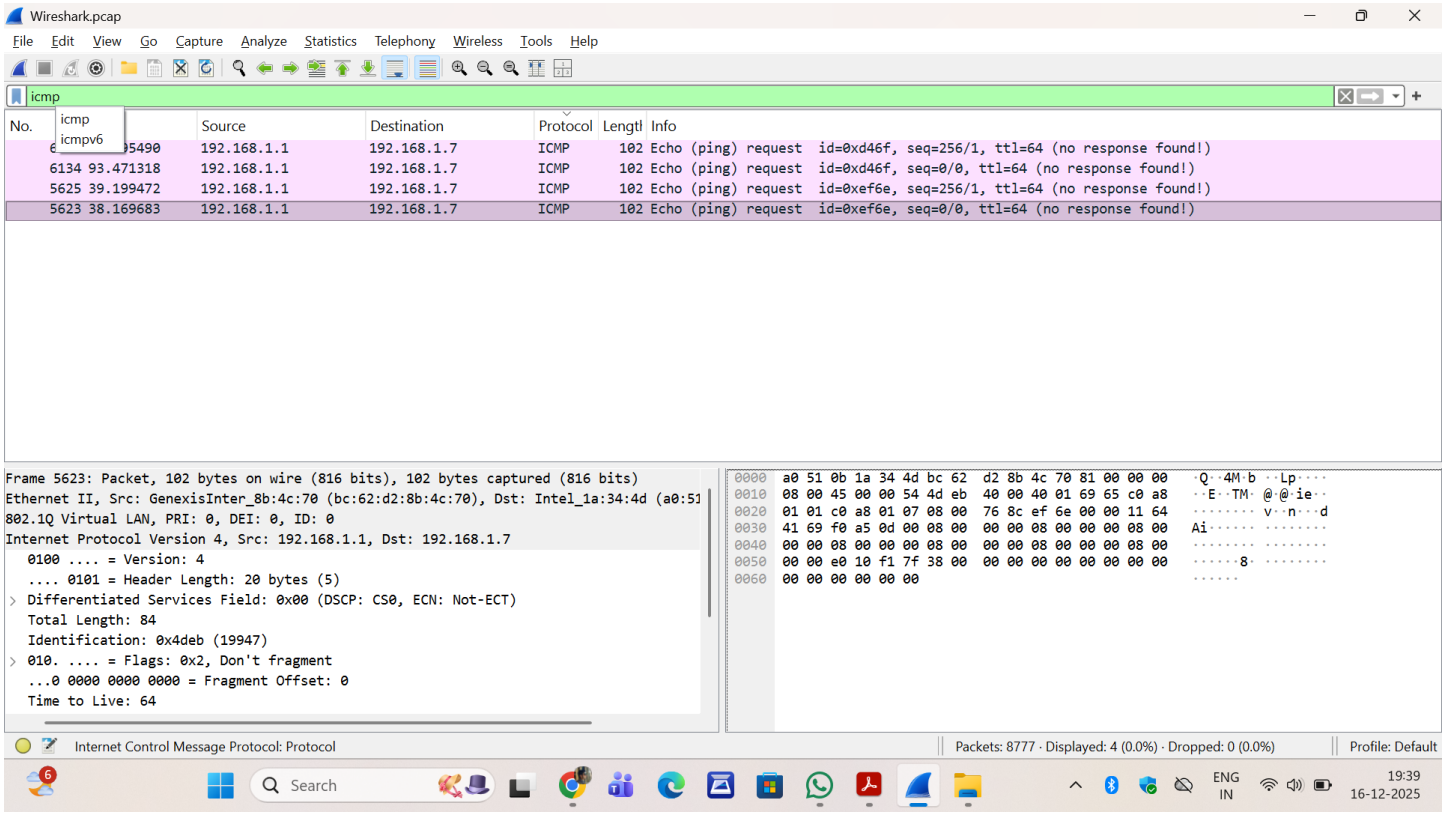
a. TCP



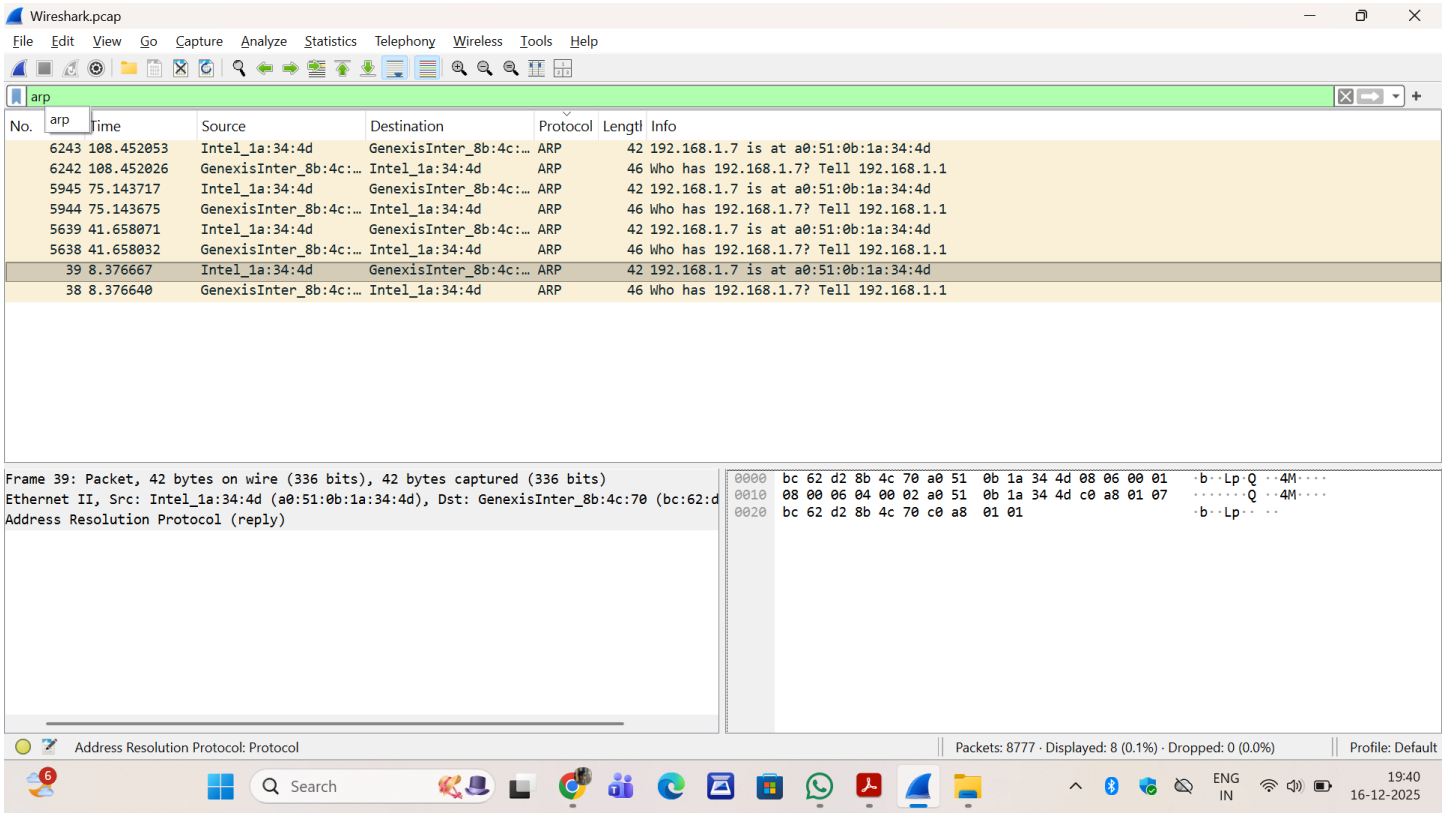
b. HTTP


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Lengtl Info
2229 19.219188 192.168.1.7 85.17.70.38 HTTP 1019 GET /CLogin?key=VUx8QAAlYxtuPDEXWgpwBHBcX203NS0RfFVdH3kMVlBUB1pDOSUMUVQdKhJwDndFXWAGUy01LVR8UiEdf...
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
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 80 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 6e 3f 6b 65 79 3d 56 55 78 38 51 41 41 6c 59 78 n?key=VU x8QAAlYx
0050 74 75 50 44 45 58 57 67 70 77 42 48 42 63 58 32 tuPDEXWg pwBHBcX2
0060 30 33 4e 53 30 52 66 46 56 64 48 33 6b 4d 56 6c 03NS0RfF VdH3kMVl
0070 42 55 42 31 70 44 4f 53 55 4d 55 56 51 64 4b 68 BUB1pDOS 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 A1CGBRf1
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 57 32 70 67 41 67 tuVyFQcA lWW2pgAg
00e0 67 35 4d 52 4d 4e 59 46 45 50 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
ENG IN
19:37 16-12-2025

c. ICMP


Wireshark.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
icmp
icmpv6
No. Source Destination Protocol Lengtl Info
192.168.1.1 192.168.1.7 ICMP 102 Echo (ping) request id=0xd46f, seq=256/1, ttl=64 (no response found!)
6134 93.471318 192.168.1.1 192.168.1.7 ICMP 102 Echo (ping) request id=0xd46f, seq=0/0, ttl=64 (no response found!)
5625 39.199472 192.168.1.1 192.168.1.7 ICMP 102 Echo (ping) request id=0xef6e, seq=256/1, ttl=64 (no response found!)
5623 38.169683 192.168.1.1 192.168.1.7 ICMP 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)
Ethernet II, Src: GenexisInter_8b:4c:70 (bc:62:d2:8b:4c:70), Dst: Intel_1a:34:4d (a0:51
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 0
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 64 ········ v··n···d
0030 41 69 f0 a5 0d 00 08 00 00 00 08 00 00 00 08 00 Ai····· ·····
0040 00 00 08 00 00 00 08 00 00 00 08 00 00 00 08 00 ····· ·····
0050 00 00 e0 10 f1 7f 38 00 00 00 00 00 00 00 00 00 ·····8· ·····
0060 00 00 00 00 00 00 ·····
Internet Control Message Protocol: Protocol
Packets: 8777 · Displayed: 4 (0.0%) · Dropped: 0 (0.0%)
Profile: Default
Search
ENG IN
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.