

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

Tools: Wireshark (free).

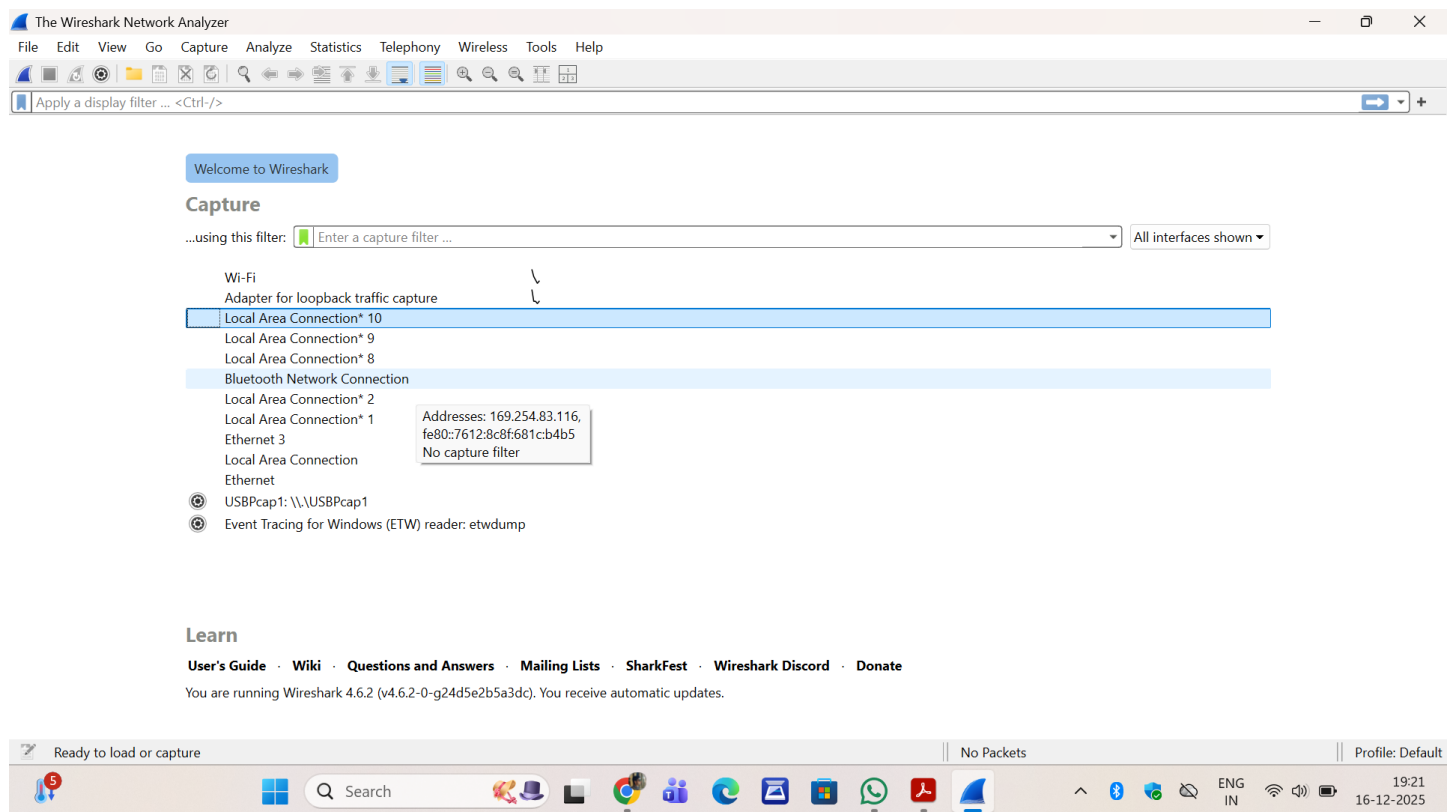
Deliverables: A packet capture (.pcap) file and a short report of protocols identified.

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.

Capturing from 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 |
|-----|----------|----------------|----------------|----------|--------|---|
| 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 SLE=1 SRE=2 |

> 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_Bb:4c:70 (bc:d6:11:00:00:00)
> 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)

0000 bc 62 d2 8b 4c 70 a0 51 0b 1a 34 4d 08 00 45 00 ····Lp:Q···4M··E·
0010 00 29 8f 3f 40 00 00 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 ····#······]·P·
0030 00 ff e3 d7 00 00 00 00 ······

Wi-Fi: <live capture in progress> | Packets: 7 | Profile: Default

19:21 16-12-2025

4. Stop capture after a minute.

*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 |
|-----|-----------|-----------------|-----------------|----------|--------|---|
| 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, App |
| 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 |
| 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: 0x1e3c (7740)
> 010. = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 59
Protocol: TCP (6)
Header Checksum: 0x1b27 [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

0010 1c 84 1e 3c 40 00 3b 06 1b 27 b9 c7 6e 9a c0 a8 ····<@;· ····n···
0020 01 07 01 bb 9c 6c ff 3e d2 d3 26 76 ca 6f 50 18 ····1···>···&v·oP·
0030 01 2a 5c 55 00 00 5a 6e ea 07 d1 74 08 e3 a1 dc ····U·Zn····t···
0040 38 1a 2d 03 f4 34 1f 13 b8 b8 90 de 1c 33 6c 48 8·····4······31H
0050 b2 92 e4 94 fc 09 fd 92 65 cf fe 98 95 c5 00 2f ····&·····e·····/
0060 c1 83 f5 26 b7 c0 e8 f2 6a 02 a0 56 de 22 00 fd ····&·····j·····V···
0070 e3 76 0a 0e 7e bb e2 ca 15 97 ad e6 5c ea 61 e2 ····~·····\·····a·
0080 c6 8b 01 2b f5 14 c7 9d 48 37 ec b2 dd d7 d9 59 ····+·····H7·····Y
0090 a7 73 c4 34 b7 3f 00 5c 86 46 ed 65 d3 df 52 3d ····s·4·?·····F·e·R·
00a0 03 b9 ee 19 61 fd f4 fe 8a 8f 7e 22 68 88 f6 1e ····a·····"·····h···
00b0 94 6e 39 0e db 16 75 ac 05 8e 78 07 1b 82 34 5f ····n9·····u·····x·····4·
00c0 1b 04 ec 4b 41 75 99 37 47 d1 41 f8 7f e4 75 58 ····Kau·7·G·A·····uX
00d0 03 95 ae b4 bd 42 84 37 dc 0b 0f c2 be 27 61 0b ····B·····7·····'a·
00e0 9d 8e 55 38 61 55 27 ca 5b 87 d2 f1 ac 1c a2 7b ····U8au'·[·····({
00f0 65 35 be ff f8 f0 d3 6c 24 55 62 af 1b 57 f2 a1 e5·····1·\$Ub·····W·
0100 4c 31 e8 7f 48 1d 89 dc c3 de e7 ad e2 fa 40 f1 L1·····H·····@·

Packet (7314 bytes) Reassembled TCP (1400 bytes)

Destination Address (ip.dst), 4 bytes | Packets: 8777 · Dropped: 0 (0.0%) | Profile: Default

19:26 16-12-2025

Wireshark capture of network traffic. The packet list shows a QUIC connection (No. 357-369) from 192.168.1.7 to 142.250.193.14. The packet details pane shows the structure of an Internet Protocol Version 4 packet (No. 357) with a header length of 20 bytes. The packet bytes pane shows the raw data in hexadecimal and ASCII.

5. Filter captured packets by protocol (e.g., HTTP, DNS, TCP).

6. Identify at least 3 different protocols in the capture.

a. TCP

Wireshark capture filtered by TCP. The packet list shows a series of TCP packets (No. 2311-2080) from 192.168.1.7 to 185.145.245.53. The packet details pane shows the structure of a Transmission Control Protocol (TCP) packet (No. 2224) with a header length of 20 bytes. The packet bytes pane shows the raw data in hexadecimal and ASCII.

b. HTTP

The image shows a Wireshark capture of an HTTP GET request. The packet list shows a single packet (No. 2229) at time 19.219188, from source 192.168.1.7 to destination 85.17.70.38, protocol HTTP, length 1019 bytes. The packet details pane shows the following structure:

- 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:d2:8b:4c:70), 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)

The packet bytes pane shows the raw data of the HTTP request, starting with the GET method and the URL path: /CLogin?key=Vux8QAA1YxtuPDEXngpwBHBcX203NS0RFFVdH3kMv1BUB1pDOSUMUVQdKhJwDndFXWAGuy01LVR8UiEdf...

c. ICMP

The image shows a Wireshark capture of ICMP Echo (ping) requests. The packet list shows four packets (No. 6134, 5625, 5625, 5625) at times 93.471318, 39.199472, 38.169683, and 38.169683, from source 192.168.1.1 to destination 192.168.1.7, protocol ICMP, length 102 bytes. The packet details pane shows the following structure:

- 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), 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

The packet bytes pane shows the raw data of the ICMP Echo request, starting with the Echo (ping) request and the sequence number: id=0xd46f, seq=256/1, ttl=64 (no response found!).

d. ARP

Wireshark.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

| No. | arp | Time | Source | Destination | Protocol | Length | Info |
|------|-----|------------|------------------------|------------------------|----------|--------|---------------------------------------|
| 6243 | | 108.452053 | Intel_1a:34:4d | GenexisInter_8b:4c:... | ARP | 42 | 192.168.1.7 is at a0:51:0b:1a:34:4d |
| 6242 | | 108.452026 | GenexisInter_8b:4c:... | Intel_1a:34:4d | ARP | 46 | Who has 192.168.1.7? Tell 192.168.1.1 |
| 5945 | | 75.143717 | Intel_1a:34:4d | GenexisInter_8b:4c:... | ARP | 42 | 192.168.1.7 is at a0:51:0b:1a:34:4d |
| 5944 | | 75.143675 | GenexisInter_8b:4c:... | Intel_1a:34:4d | ARP | 46 | Who has 192.168.1.7? Tell 192.168.1.1 |
| 5639 | | 41.658071 | Intel_1a:34:4d | GenexisInter_8b:4c:... | ARP | 42 | 192.168.1.7 is at a0:51:0b:1a:34:4d |
| 5638 | | 41.658032 | GenexisInter_8b:4c:... | Intel_1a:34:4d | ARP | 46 | Who has 192.168.1.7? Tell 192.168.1.1 |
| 39 | | 8.376667 | Intel_1a:34:4d | GenexisInter_8b:4c:... | ARP | 42 | 192.168.1.7 is at a0:51:0b:1a:34:4d |
| 38 | | 8.376640 | GenexisInter_8b:4c:... | Intel_1a:34:4d | ARP | 46 | Who has 192.168.1.7? Tell 192.168.1.1 |

Frame 39: Packet, 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
Ethernet II, Src: Intel_1a:34:4d (a0:51:0b:1a:34:4d), Dst: GenexisInter_8b:4c:70 (bc:62:d2:8b:4c:70)
Address Resolution Protocol (reply)

0000

bc 62 d2 8b 4c 70 a0 51 0b 1a 34 4d 08 06 00 01

-b-Lp-Q--4M----

0010

08 00 06 04 00 02 a0 51 0b 1a 34 4d c0 a8 01 07

-----Q--4M----

0020

bc 62 d2 8b 4c 70 c0 a8 01 01

-b-Lp-- --

Address Resolution Protocol: Protocol

Packets: 8777 · Displayed: 8 (0.1%) · Dropped: 0 (0.0%)

Profile: Default

6

Search

ENG IN

19:40 16-12-2025

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.