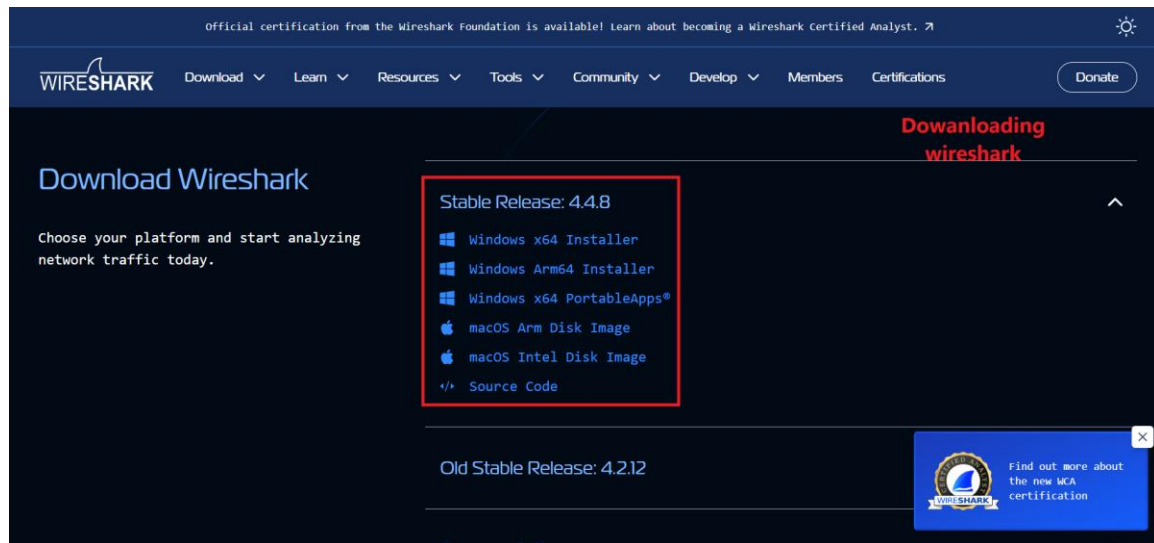
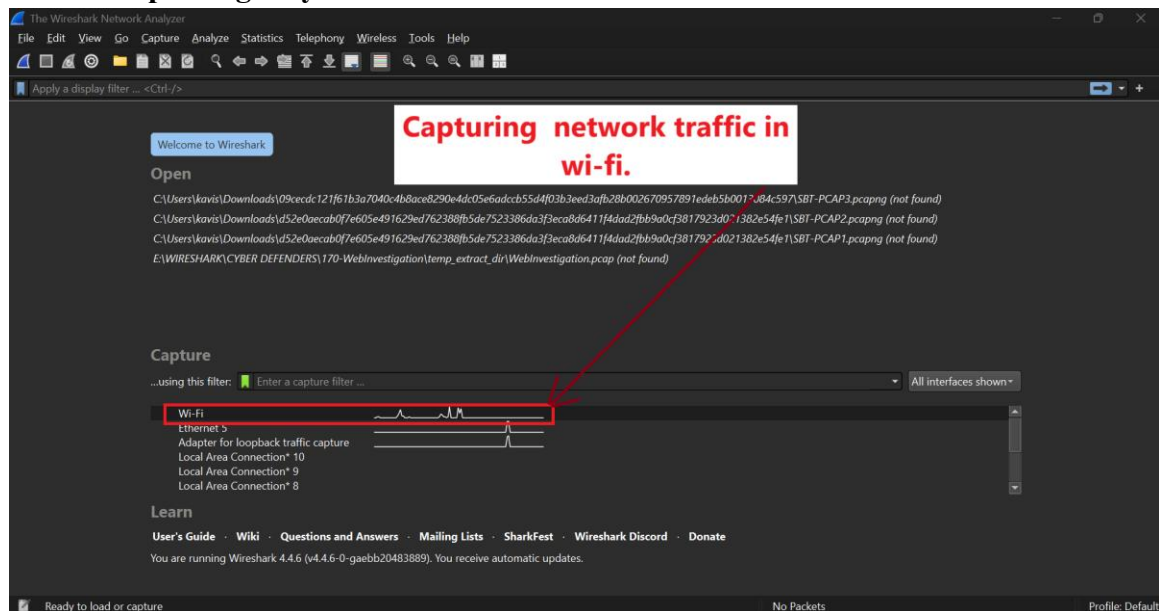


1.Install Wireshark.



2.Start capturing on your active network interface.



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

```
C:\Users\user>ping google.com

Pinging google.com [2404:6800:4009:80a::200e] with 32 bytes of data:
Reply from 2404:6800:4009:80a::200e: time=85ms
Reply from 2404:6800:4009:80a::200e: time=74ms
Reply from 2404:6800:4009:80a::200e: time=68ms
Reply from 2404:6800:4009:80a::200e: time=51ms

Ping statistics for 2404:6800:4009:80a::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 51ms, Maximum = 85ms, Average = 69ms

C:\Users\user>tracert apple.com

Tracing route to apple.com [2620:149:af0::10]
over a maximum of 30 hops:

  0  0 ms  0 ms  0 ms  2409:40f4:215e:ced6::61
  1  3 ms  2 ms  2 ms  2405:200:5218:24:3924:110:3:412
  2  53 ms 17 ms 14 ms 2405:200:5218:24:3925::ff03
  3  32 ms 13 ms 14 ms 2405:200:5218:24:3925::ff03
  4  *      *      *      Request timed out.
  5  *      *      *      Request timed out.
  6  36 ms 13 ms 15 ms 2405:200:801:4f00::1ec
  7  *      *      *      ^C
```

```
C:\WINDOWS\system32\cmd. x + v

Microsoft Windows [Version 10.0.22000.51]
(c) Microsoft Corporation. All rights reserved.

C:\Users\user>curl http://amazon.com
<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>Server</center>
</body>
</html>

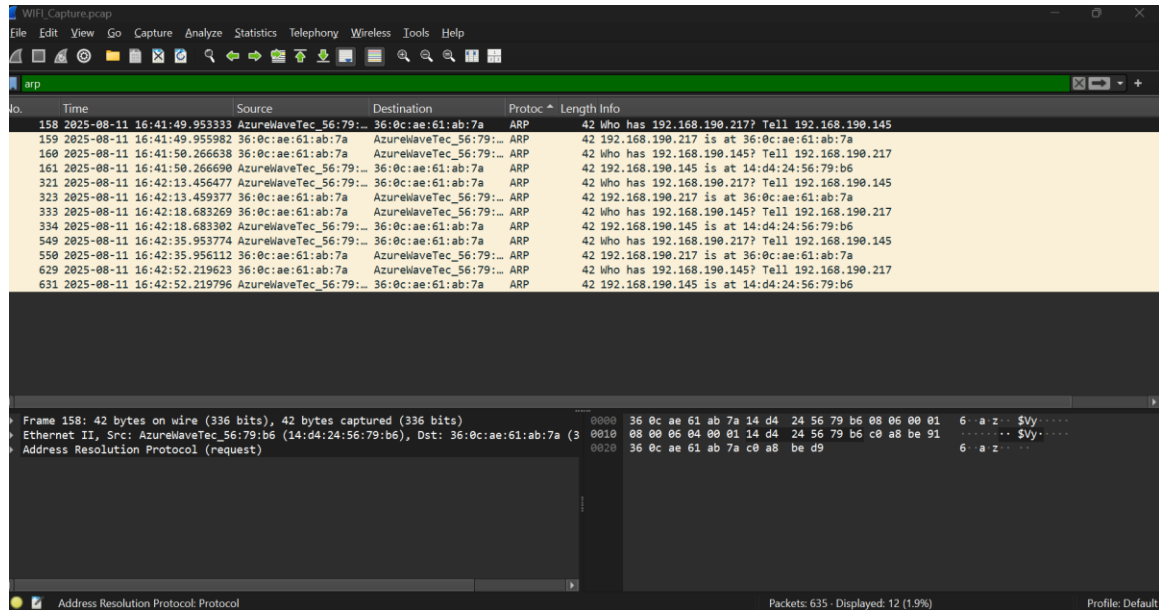
C:\Users\user>nslookup openai.com
Server: UnKnown
Address: 192.168.1.100

Non-authoritative answer:
Name: openai.com
Addresses: 64:0000:0000:0000:0000:0000:0000:0000
           64:ff9b::ac40:9ad3
           172.64.112.100
           104.18.33.100

C:\Users\user>
```

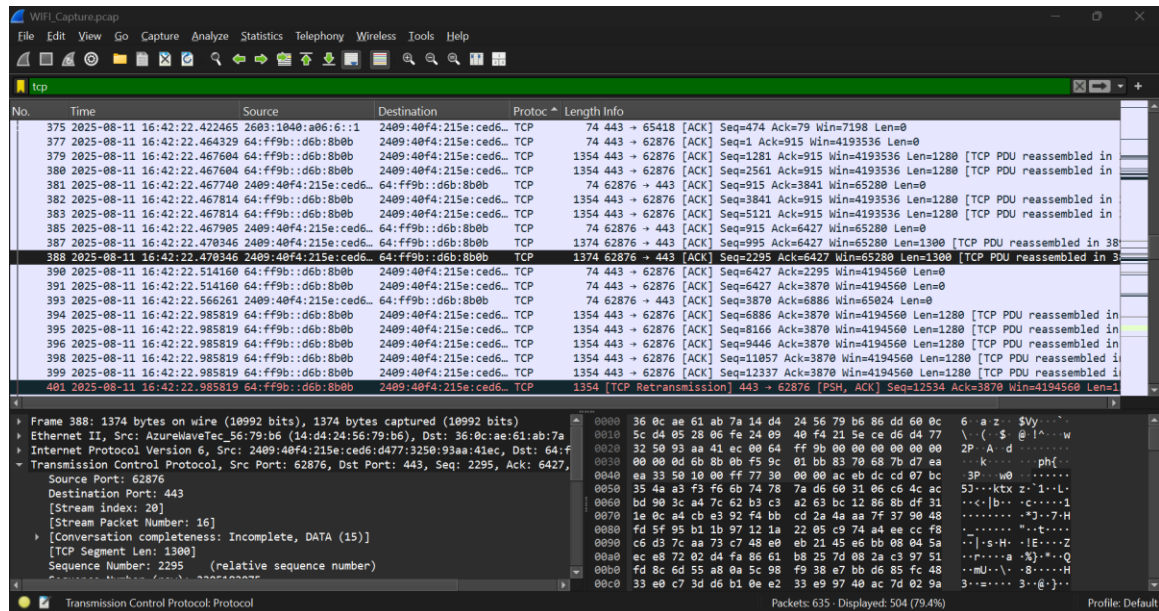
4.Filter captured packets by protocol (e.g., HTTP, DNS, TCP).

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



The screenshot shows the Wireshark interface with the 'arp' filter applied. The packet list pane displays 13 ARP packets. The packet details pane shows the structure of an ARP request, including Ethernet II, Internet Protocol, and Address Resolution Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
158	2025-08-11 16:41:49.953333	AzureWaveTec_56:79:...	36:0c:ae:61:ab:7a	ARP	42	Who has 192.168.190.217? Tell 192.168.190.145
159	2025-08-11 16:41:49.955982	AzureWaveTec_56:79:...	36:0c:ae:61:ab:7a	ARP	42	192.168.190.217 is at 36:0c:ae:61:ab:7a
160	2025-08-11 16:41:50.266638	AzureWaveTec_56:79:...	36:0c:ae:61:ab:7a	ARP	42	Who has 192.168.190.145? Tell 192.168.190.217
161	2025-08-11 16:41:50.266690	AzureWaveTec_56:79:...	36:0c:ae:61:ab:7a	ARP	42	192.168.190.145 is at 14:d4:24:56:79:b6
321	2025-08-11 16:42:13.456477	AzureWaveTec_56:79:...	36:0c:ae:61:ab:7a	ARP	42	Who has 192.168.190.217? Tell 192.168.190.145
323	2025-08-11 16:42:13.459377	AzureWaveTec_56:79:...	36:0c:ae:61:ab:7a	ARP	42	192.168.190.217 is at 36:0c:ae:61:ab:7a
333	2025-08-11 16:42:18.683269	AzureWaveTec_56:79:...	36:0c:ae:61:ab:7a	ARP	42	Who has 192.168.190.145? Tell 192.168.190.217
334	2025-08-11 16:42:18.683382	AzureWaveTec_56:79:...	36:0c:ae:61:ab:7a	ARP	42	192.168.190.145 is at 14:d4:24:56:79:b6
549	2025-08-11 16:42:35.953774	AzureWaveTec_56:79:...	36:0c:ae:61:ab:7a	ARP	42	Who has 192.168.190.217? Tell 192.168.190.145
550	2025-08-11 16:42:35.956112	AzureWaveTec_56:79:...	36:0c:ae:61:ab:7a	ARP	42	192.168.190.217 is at 36:0c:ae:61:ab:7a
629	2025-08-11 16:42:52.219623	AzureWaveTec_56:79:...	36:0c:ae:61:ab:7a	ARP	42	Who has 192.168.190.145? Tell 192.168.190.217
631	2025-08-11 16:42:52.219796	AzureWaveTec_56:79:...	36:0c:ae:61:ab:7a	ARP	42	192.168.190.145 is at 14:d4:24:56:79:b6



The screenshot shows the Wireshark interface with the 'tcp' filter applied. The packet list pane displays 20 TCP packets. The packet details pane shows the structure of a TCP segment, including Ethernet II, Internet Protocol, and Transmission Control Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
375	2025-08-11 16:42:22.422465	2603:1040:a06:6::1	2409:40f4:215e:ced6::...	TCP	74	443 → 65418 [ACK] Seq=474 Ack=79 Win=7198 Len=0
377	2025-08-11 16:42:22.464329	64:ff9b::d6b:8b0b	2409:40f4:215e:ced6::...	TCP	74	443 → 62876 [ACK] Seq=1 Ack=915 Win=4193536 Len=0
379	2025-08-11 16:42:22.467604	64:ff9b::d6b:8b0b	2409:40f4:215e:ced6::...	TCP	1354	443 → 62876 [ACK] Seq=1281 Ack=915 Win=4193536 Len=1280 [TCP PDU reassembled in 380]
380	2025-08-11 16:42:22.467604	64:ff9b::d6b:8b0b	2409:40f4:215e:ced6::...	TCP	1354	443 → 62876 [ACK] Seq=2561 Ack=915 Win=4193536 Len=1280 [TCP PDU reassembled in 381]
381	2025-08-11 16:42:22.467740	2409:40f4:215e:ced6::...	64:ff9b::d6b:8b0b	TCP	74	62876 → 443 [ACK] Seq=915 Ack=3841 Win=65280 Len=0
382	2025-08-11 16:42:22.467814	64:ff9b::d6b:8b0b	2409:40f4:215e:ced6::...	TCP	1354	443 → 62876 [ACK] Seq=3841 Ack=915 Win=4193536 Len=1280 [TCP PDU reassembled in 383]
383	2025-08-11 16:42:22.467814	64:ff9b::d6b:8b0b	2409:40f4:215e:ced6::...	TCP	1354	443 → 62876 [ACK] Seq=5121 Ack=915 Win=4193536 Len=1280 [TCP PDU reassembled in 385]
385	2025-08-11 16:42:22.467905	2409:40f4:215e:ced6::...	64:ff9b::d6b:8b0b	TCP	74	62876 → 443 [ACK] Seq=915 Ack=6427 Win=65280 Len=0
387	2025-08-11 16:42:22.470346	2409:40f4:215e:ced6::...	64:ff9b::d6b:8b0b	TCP	1374	62876 → 443 [ACK] Seq=995 Ack=6427 Win=65280 Len=1300 [TCP PDU reassembled in 388]
388	2025-08-11 16:42:22.470346	2409:40f4:215e:ced6::...	64:ff9b::d6b:8b0b	TCP	1374	62876 → 443 [ACK] Seq=2295 Ack=6427 Win=65280 Len=1300 [TCP PDU reassembled in 390]
390	2025-08-11 16:42:22.514160	64:ff9b::d6b:8b0b	2409:40f4:215e:ced6::...	TCP	74	443 → 62876 [ACK] Seq=6427 Ack=2295 Win=4194560 Len=0
391	2025-08-11 16:42:22.514160	64:ff9b::d6b:8b0b	2409:40f4:215e:ced6::...	TCP	74	443 → 62876 [ACK] Seq=6427 Ack=3870 Win=4194560 Len=0
393	2025-08-11 16:42:22.566261	2409:40f4:215e:ced6::...	64:ff9b::d6b:8b0b	TCP	74	62876 → 443 [ACK] Seq=3870 Ack=6886 Win=65024 Len=0
394	2025-08-11 16:42:22.985819	64:ff9b::d6b:8b0b	2409:40f4:215e:ced6::...	TCP	1354	443 → 62876 [ACK] Seq=6886 Ack=3870 Win=4194560 Len=1280 [TCP PDU reassembled in 395]
395	2025-08-11 16:42:22.985819	64:ff9b::d6b:8b0b	2409:40f4:215e:ced6::...	TCP	1354	443 → 62876 [ACK] Seq=8166 Ack=3870 Win=4194560 Len=1280 [TCP PDU reassembled in 396]
396	2025-08-11 16:42:22.985819	64:ff9b::d6b:8b0b	2409:40f4:215e:ced6::...	TCP	1354	443 → 62876 [ACK] Seq=9446 Ack=3870 Win=4194560 Len=1280 [TCP PDU reassembled in 398]
398	2025-08-11 16:42:22.985819	64:ff9b::d6b:8b0b	2409:40f4:215e:ced6::...	TCP	1354	443 → 62876 [ACK] Seq=11857 Ack=3870 Win=4194560 Len=1280 [TCP PDU reassembled in 399]
399	2025-08-11 16:42:22.985819	64:ff9b::d6b:8b0b	2409:40f4:215e:ced6::...	TCP	1354	443 → 62876 [ACK] Seq=12337 Ack=3870 Win=4194560 Len=1280 [TCP PDU reassembled in 401]
401	2025-08-11 16:42:22.985819	64:ff9b::d6b:8b0b	2409:40f4:215e:ced6::...	TCP	1354	[TCP Retransmission] 443 → 62876 [PSH, ACK] Seq=12534 Ack=3870 Win=4194560 Len=1

