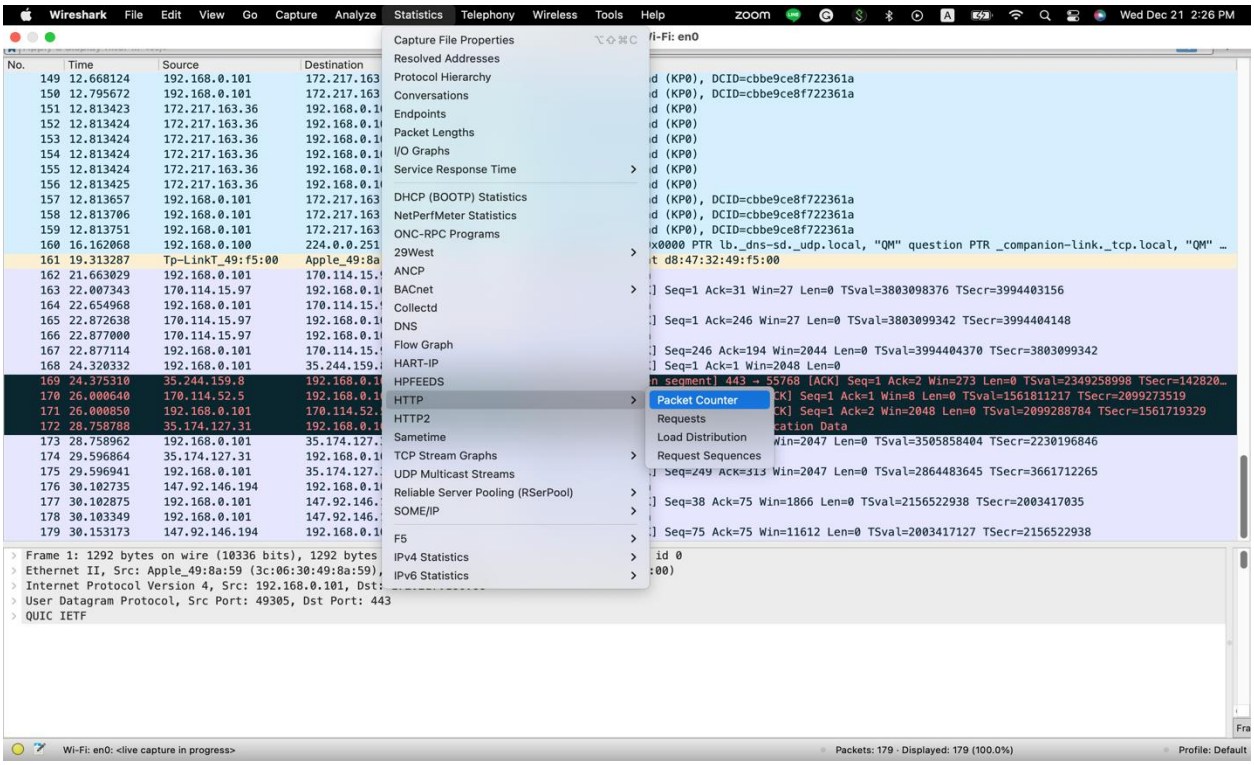
109550198

Intro to computer network

HW3

1)

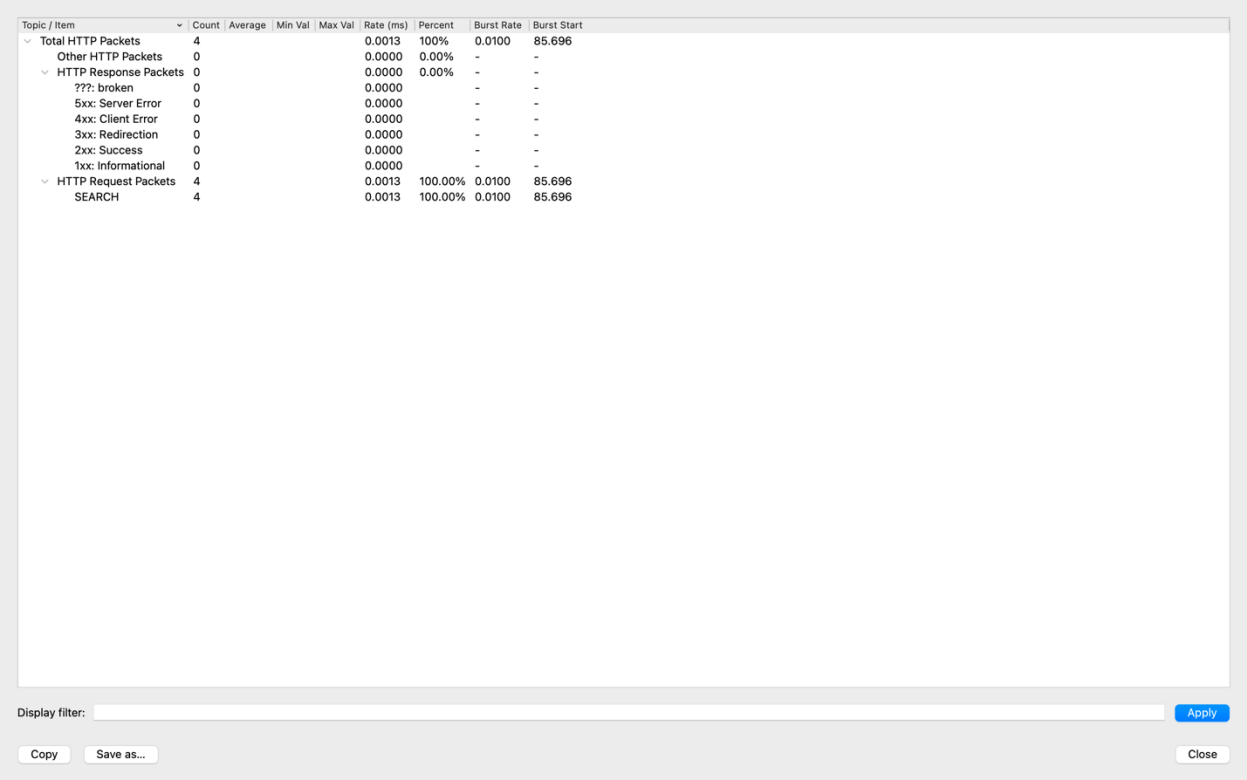
HTTP packet counter statistics using Wireshark
This window can be found under the statistics tab, see the below image:



Analyzing information from HTTP requests and their returning response codes is done using the **Packet counter**.

Here is the screenshot:

Let’s understand the captured data:



Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Total HTTP Packets	4				0.0013	100%	0.0100	85.696
Other HTTP Packets	0				0.0000	0.00%	-	-
HTTP Response Packets	0				0.0000	0.00%	-	-
???: broken	0				0.0000		-	-
5xx: Server Error	0				0.0000		-	-
4xx: Client Error	0				0.0000		-	-
3xx: Redirection	0				0.0000		-	-
2xx: Success	0				0.0000		-	-
1xx: Informational	0				0.0000		-	-
HTTP Request Packets	4				0.0013	100.00%	0.0100	85.696
SEARCH	4				0.0013	100.00%	0.0100	85.696

The image shows that 4 HTTPS packets are delivered, with all of their details being easily readable.

Conclusion:

The data collected shows that some websites are still using the insecure HTTPS protocol, so organizations should switch to HTTPS for secure data transfer that is encrypted to avoid any data leaks.

2)

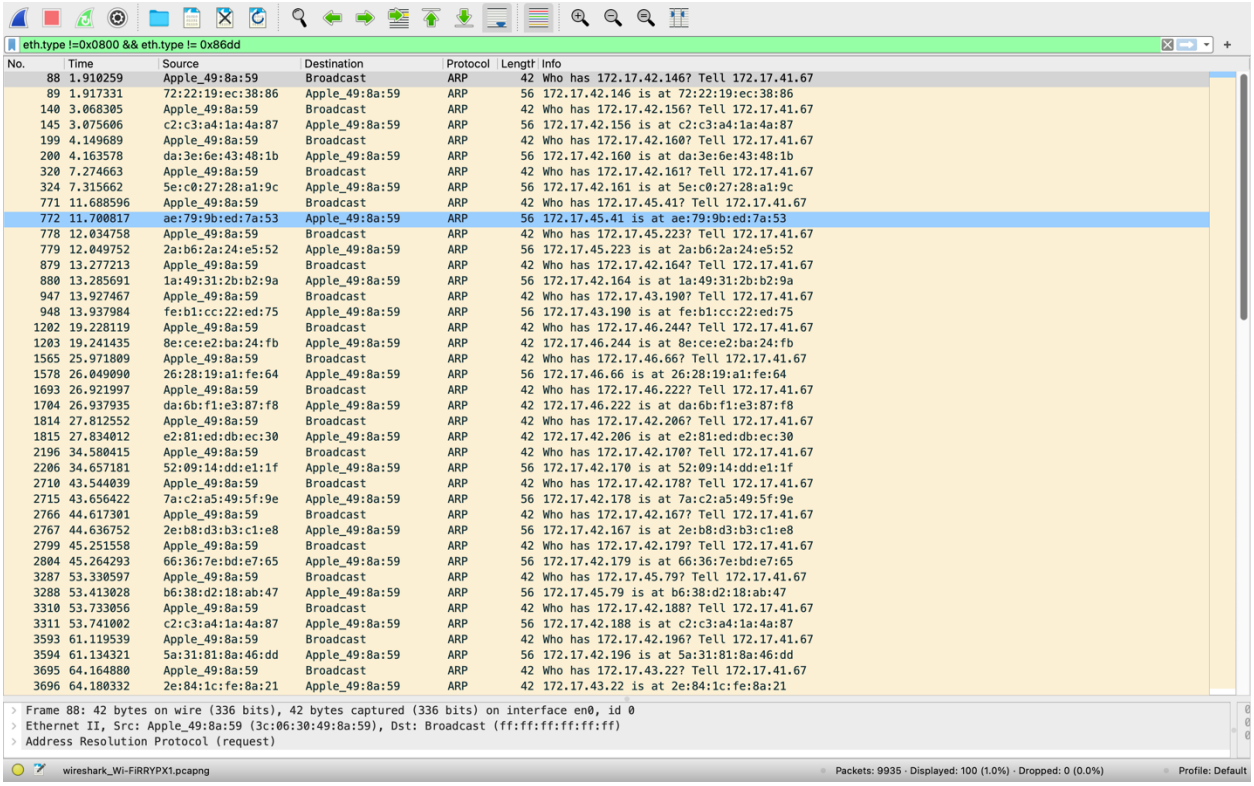
Two benefits to using QUIC protocol instead of traditional TCP protocol:

- Faster connection and setup establishment.
- Reduced sensitivity to packet loss.

3)

We just exclude ipv4 and ipv6 to capture non-IP traffic as seen in the screenshot.

Here is the screenshot:



eth.type !=0x0800 && eth.type != 0x86dd

No.	Time	Source	Destination	Protocol	Length	Info
88	1.910259	Apple_49:8a:59	Broadcast	ARP	42	Who has 172.17.42.146? Tell 172.17.41.67
89	1.917331	72:22:19:ec:38:86	Apple_49:8a:59	ARP	56	172.17.42.146 is at 72:22:19:ec:38:86
140	3.068305	Apple_49:8a:59	Broadcast	ARP	42	Who has 172.17.42.156? Tell 172.17.41.67
145	3.075606	c2:c3:a4:1a:4a:87	Apple_49:8a:59	ARP	56	172.17.42.156 is at c2:c3:a4:1a:4a:87
199	4.149689	Apple_49:8a:59	Broadcast	ARP	42	Who has 172.17.42.160? Tell 172.17.41.67
200	4.163578	da:3e:6e:43:48:1b	Apple_49:8a:59	ARP	56	172.17.42.160 is at da:3e:6e:43:48:1b
320	7.274663	Apple_49:8a:59	Broadcast	ARP	42	Who has 172.17.42.161? Tell 172.17.41.67
324	7.315662	5e:c0:27:28:a1:9c	Apple_49:8a:59	ARP	56	172.17.42.161 is at 5e:c0:27:28:a1:9c
771	11.688596	Apple_49:8a:59	Broadcast	ARP	42	Who has 172.17.45.41? Tell 172.17.41.67
772	11.700817	ae:79:9b:ed:7a:53	Apple_49:8a:59	ARP	56	172.17.45.41 is at ae:79:9b:ed:7a:53
778	12.034758	Apple_49:8a:59	Broadcast	ARP	42	Who has 172.17.45.223? Tell 172.17.41.67
779	12.049752	2a:b6:2a:24:e5:52	Apple_49:8a:59	ARP	56	172.17.45.223 is at 2a:b6:2a:24:e5:52
879	13.277213	Apple_49:8a:59	Broadcast	ARP	42	Who has 172.17.42.164? Tell 172.17.41.67
880	13.285691	1a:49:31:2b:b2:9a	Apple_49:8a:59	ARP	56	172.17.42.164 is at 1a:49:31:2b:b2:9a
947	13.927467	Apple_49:8a:59	Broadcast	ARP	42	Who has 172.17.43.190? Tell 172.17.41.67
948	13.937984	fe:b1:cc:22:ed:75	Apple_49:8a:59	ARP	56	172.17.43.190 is at fe:b1:cc:22:ed:75
1202	19.228119	Apple_49:8a:59	Broadcast	ARP	42	Who has 172.17.46.244? Tell 172.17.41.67
1203	19.241435	8e:ce:e2:ba:24:fb	Apple_49:8a:59	ARP	42	172.17.46.244 is at 8e:ce:e2:ba:24:fb
1565	25.971809	Apple_49:8a:59	Broadcast	ARP	42	Who has 172.17.46.66? Tell 172.17.41.67
1578	26.049090	26:28:19:a1:fe:64	Apple_49:8a:59	ARP	56	172.17.46.66 is at 26:28:19:a1:fe:64
1693	26.921997	Apple_49:8a:59	Broadcast	ARP	42	Who has 172.17.46.222? Tell 172.17.41.67
1704	26.937935	da:6b:f1:e3:87:f8	Apple_49:8a:59	ARP	42	172.17.46.222 is at da:6b:f1:e3:87:f8
1814	27.812552	Apple_49:8a:59	Broadcast	ARP	42	Who has 172.17.42.206? Tell 172.17.41.67
1815	27.834012	e2:81:ed:db:ec:30	Apple_49:8a:59	ARP	42	172.17.42.206 is at e2:81:ed:db:ec:30
2196	34.580415	Apple_49:8a:59	Broadcast	ARP	42	Who has 172.17.42.170? Tell 172.17.41.67
2206	34.657181	52:09:14:dd:e1:1f	Apple_49:8a:59	ARP	56	172.17.42.170 is at 52:09:14:dd:e1:1f
2710	43.544039	Apple_49:8a:59	Broadcast	ARP	42	Who has 172.17.42.178? Tell 172.17.41.67
2715	43.656422	7a:c2:a5:49:5f:9e	Apple_49:8a:59	ARP	56	172.17.42.178 is at 7a:c2:a5:49:5f:9e
2766	44.617301	Apple_49:8a:59	Broadcast	ARP	42	Who has 172.17.42.167? Tell 172.17.41.67
2767	44.636752	2e:b8:d3:b3:c1:e8	Apple_49:8a:59	ARP	56	172.17.42.167 is at 2e:b8:d3:b3:c1:e8
2799	45.251558	Apple_49:8a:59	Broadcast	ARP	42	Who has 172.17.42.179? Tell 172.17.41.67
2804	45.264293	66:36:7e:bd:e7:65	Apple_49:8a:59	ARP	56	172.17.42.179 is at 66:36:7e:bd:e7:65
3287	53.330597	Apple_49:8a:59	Broadcast	ARP	42	Who has 172.17.45.79? Tell 172.17.41.67
3288	53.413028	b6:38:d2:18:ab:47	Apple_49:8a:59	ARP	56	172.17.45.79 is at b6:38:d2:18:ab:47
3310	53.733056	Apple_49:8a:59	Broadcast	ARP	42	Who has 172.17.42.188? Tell 172.17.41.67
3311	53.741002	c2:c3:a4:1a:4a:87	Apple_49:8a:59	ARP	56	172.17.42.188 is at c2:c3:a4:1a:4a:87
3593	61.119539	Apple_49:8a:59	Broadcast	ARP	42	Who has 172.17.42.196? Tell 172.17.41.67
3594	61.134321	5a:31:81:8a:46:dd	Apple_49:8a:59	ARP	56	172.17.42.196 is at 5a:31:81:8a:46:dd
3695	64.164880	Apple_49:8a:59	Broadcast	ARP	42	Who has 172.17.43.22? Tell 172.17.41.67
3696	64.180332	2e:84:1c:fe:8a:21	Apple_49:8a:59	ARP	42	172.17.43.22 is at 2e:84:1c:fe:8a:21

Frame 88: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface en0, id 0
Ethernet II, Src: Apple_49:8a:59 (3c:06:30:49:8a:59), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

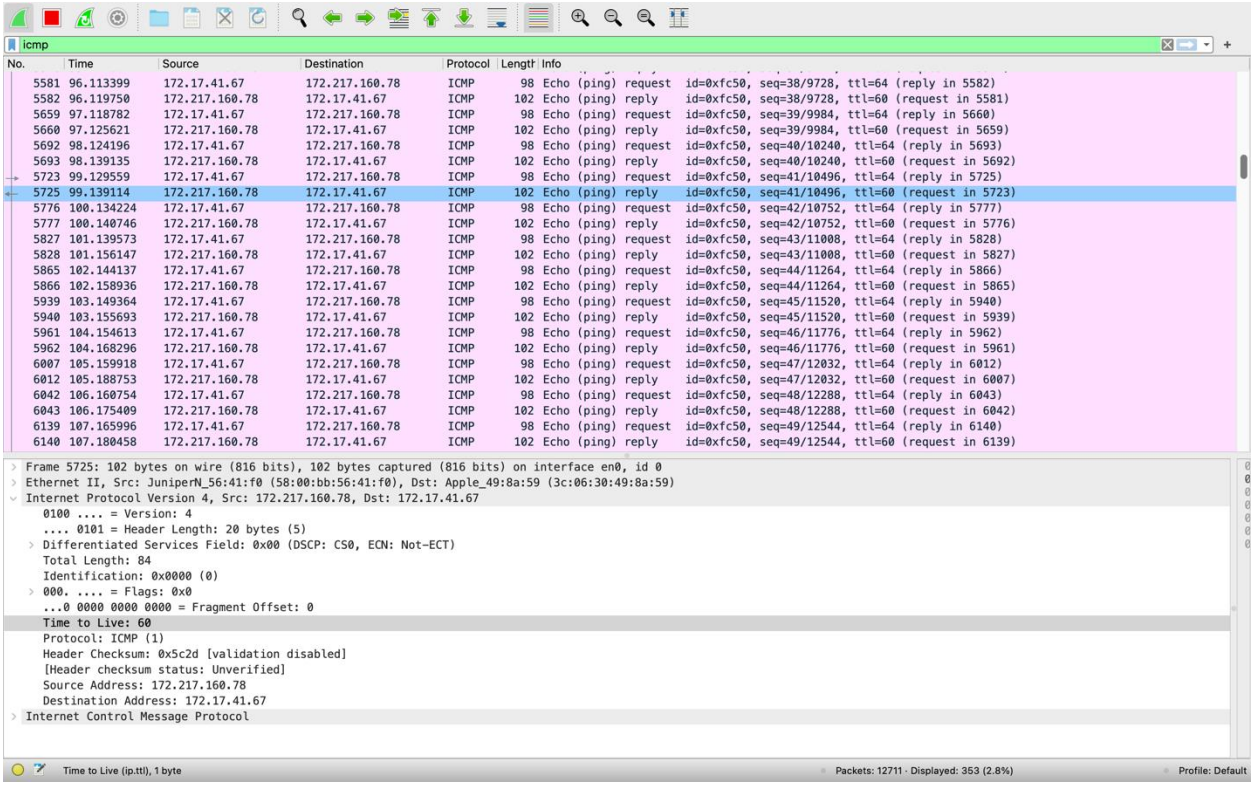
wireshark_Wi-FiRRYPX1.pcapng Packets: 9935 · Displayed: 100 (1.0%) · Dropped: 0 (0.0%) Profile: Default

4)

Time to Live (TTL)of a packet:

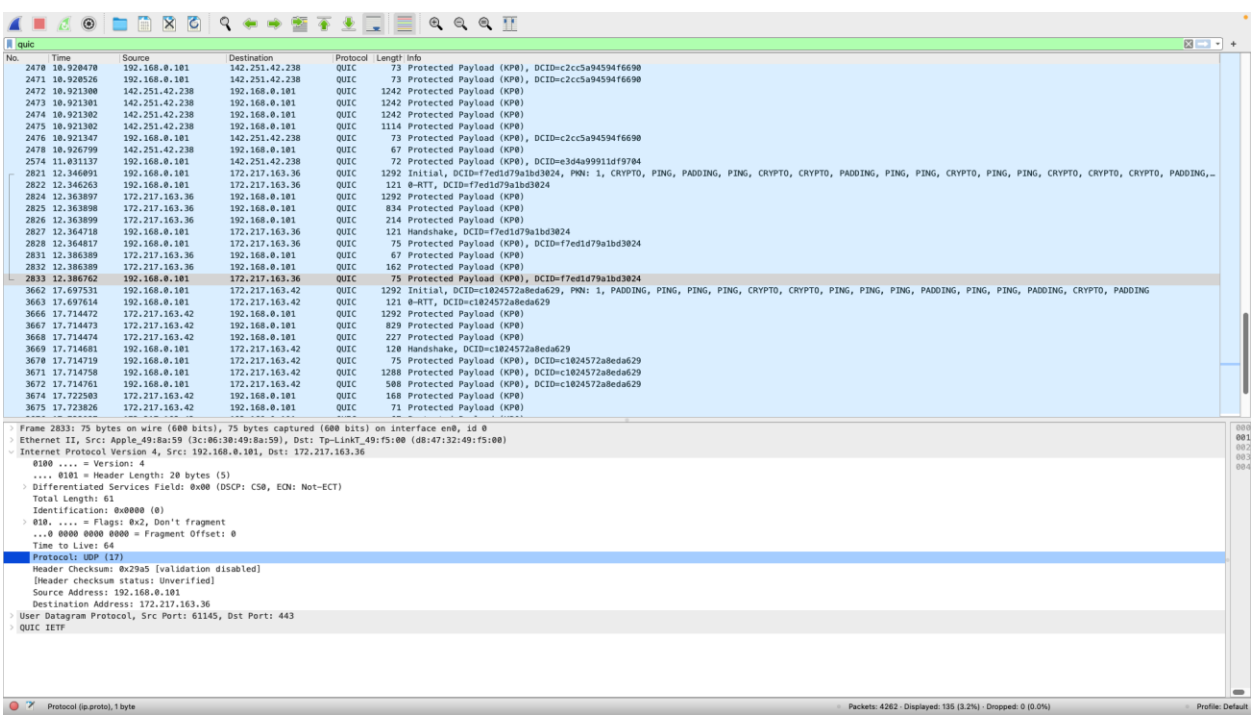
The time-to-live (TTL) specifies the period that a packet of data should remain on a computer or network before being deleted.

Here is the screenshot:



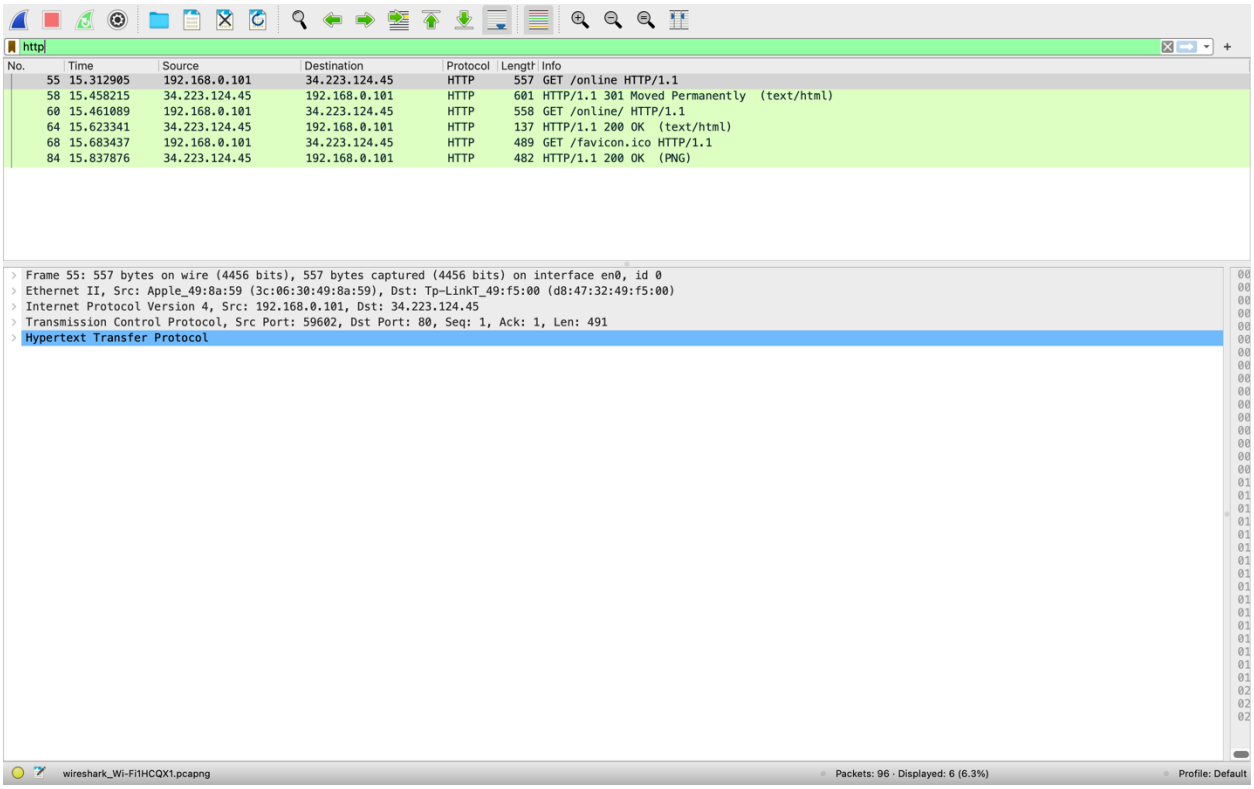
5) HTTP/3 uses QUIC protocol to transmit data. QUIC uses UDP in the transport layer.

Here is the screenshot:



6)
While Wireshark is running, I enter the URL: http://neverssl.com/
HTTP packets exchanges in Wireshark:
Before diving into HTTP, it's important to note that TCP and port 80 are used as transport layer protocols for HTTP. Let's examine what occurs on the network when we enter that URL into the browser and press Enter.

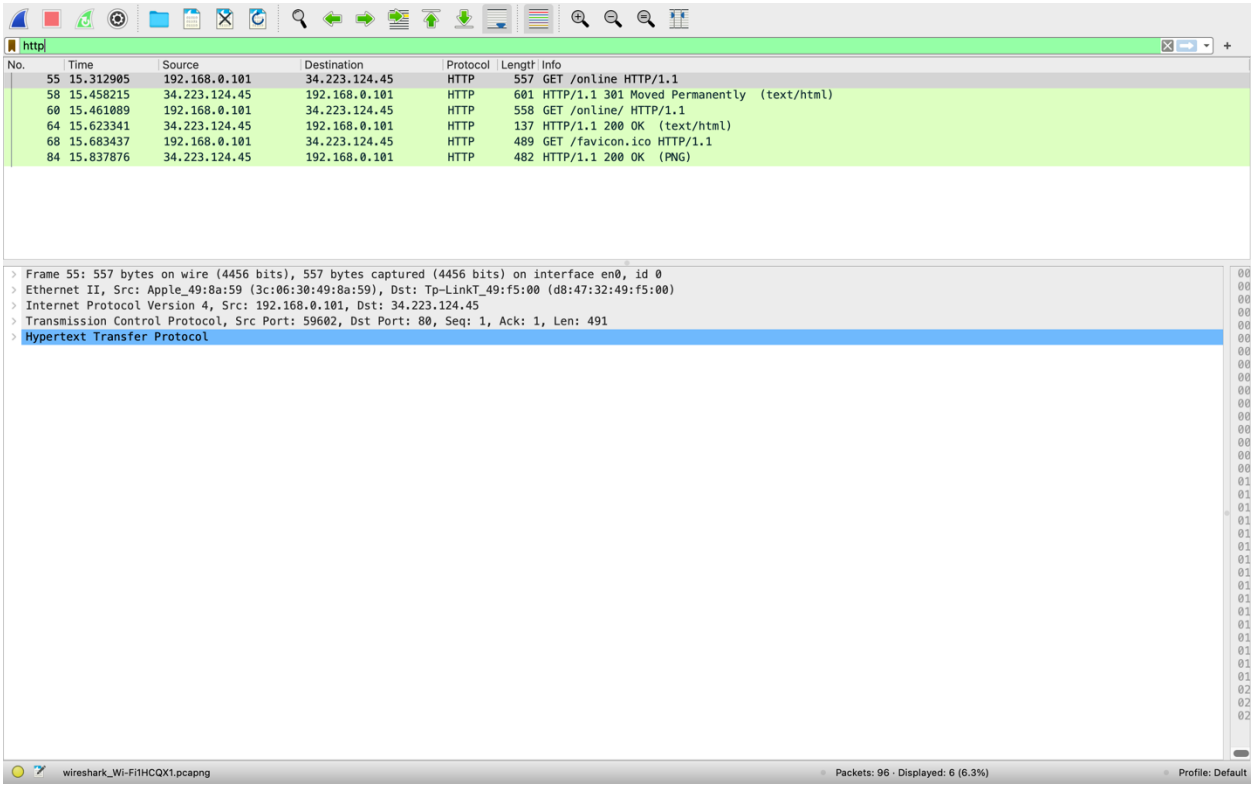
Here is the screenshot:



The time it takes when the HTTP GET message was sent until the HTTP OK reply was received is:

15.623341-15.312905 = 0.310436

Here is the screenshot:

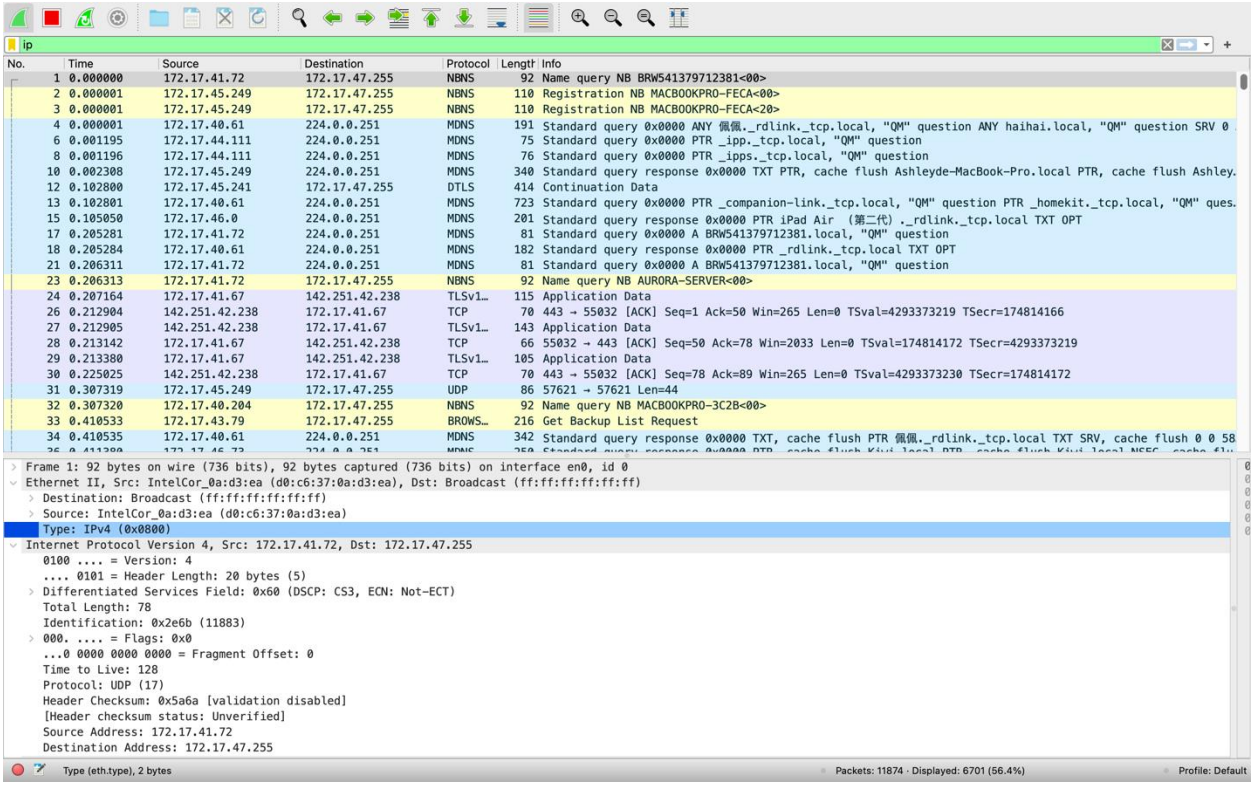


7)

A computer can know if a packet is an IPv4 or IPv6 packet by using ether type in the ethernet header or it can identify it by the version field in the IP header.

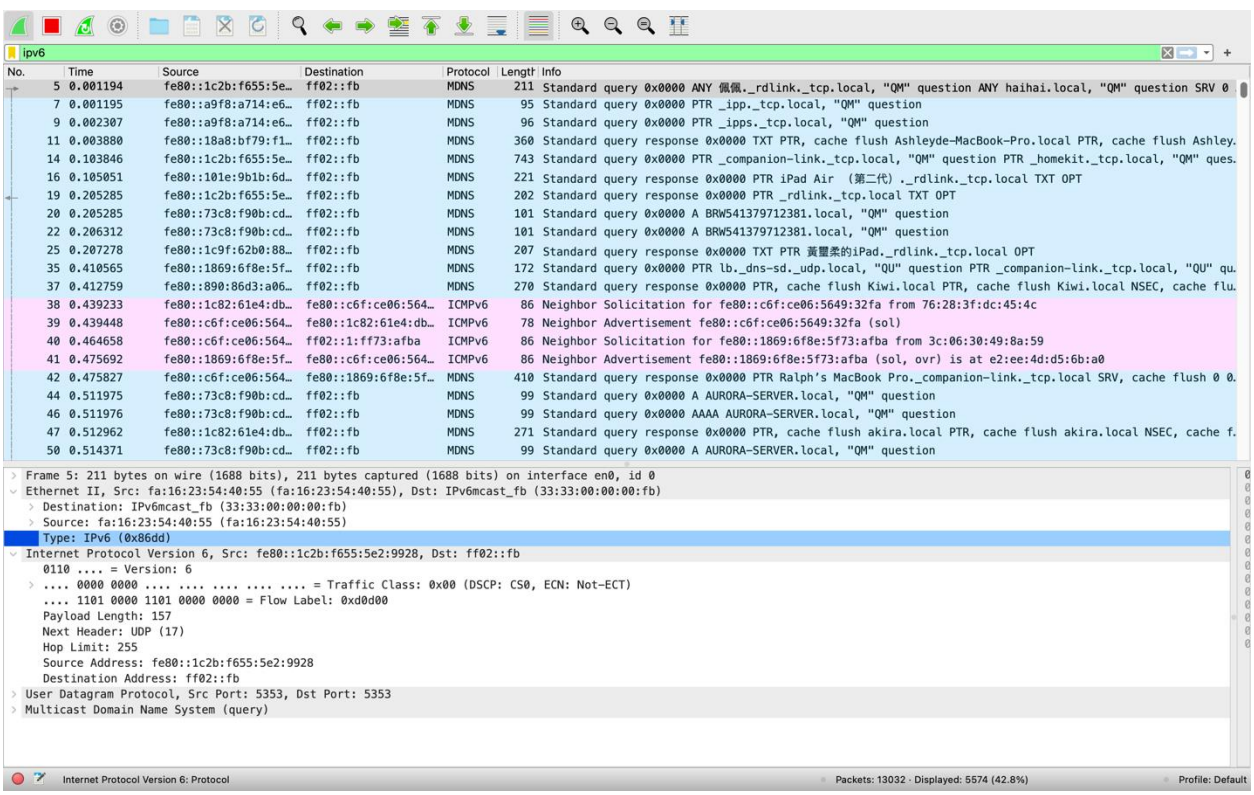
IPv4 packet:

Here is the screenshot:



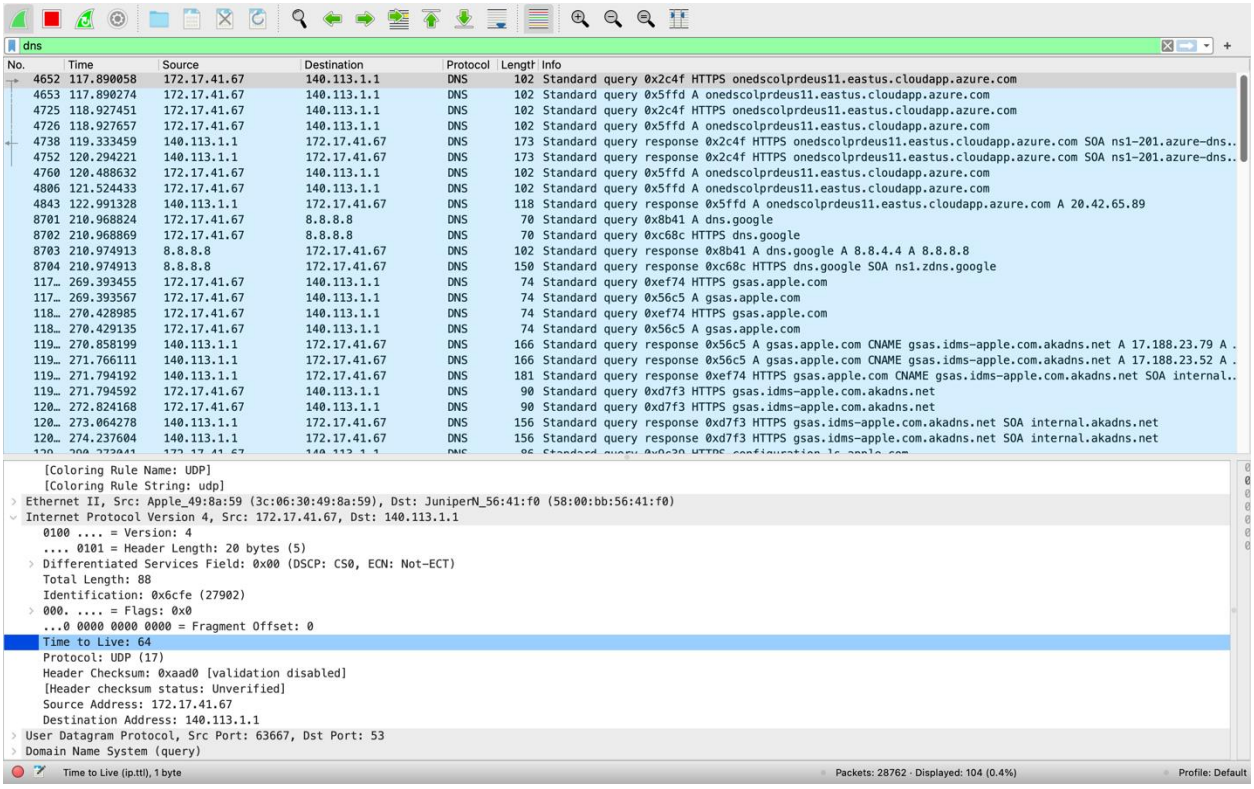
IPv6 packet:

Here is the screenshot:



8) the Time to live field from a DNS packet:

Here is the screenshot:



9)
a) My browser sends 4 HTTP GET request messages as seen in the screenshot. These GET requests were sent to the Destination Address: 128.119.245.12 and the destination address 178.79.137.164 as seen in the screenshot.

b)
By checking the TCP ports, we can see if our files were downloaded serially or in parallel. In this case, they try to use 2 different ports to get 2 different resources, therefore they were downloaded from the two websites in parallel.

Here is the screenshot:

http

No.	Time	Source	Destination	Protocol	Length	Source Port	Info
1980	13.438167	192.168.0.101	128.119.245.12	HTTP	917	62138	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
1999	13.636889	128.119.245.12	192.168.0.101	HTTP	1367	80	HTTP/1.1 200 OK (text/html)
2002	13.646878	192.168.0.101	128.119.245.12	HTTP	837	62138	GET /pearson.png HTTP/1.1
2028	13.848551	128.119.245.12	192.168.0.101	HTTP	781	80	HTTP/1.1 200 OK (PNG)
2048	13.912523	192.168.0.101	178.79.137.164	HTTP	457	62140	GET /8E_cover_small.jpg HTTP/1.1
2056	14.177633	178.79.137.164	192.168.0.101	HTTP	237	80	HTTP/1.1 301 Moved Permanently
2060	14.181283	192.168.0.101	178.79.137.164	HTTP	421	62140	GET /8E_cover_small.jpg HTTP/1.1
2089	14.454130	178.79.137.164	192.168.0.101	HTTP	237	80	HTTP/1.1 301 Moved Permanently

```
    Source Address: 192.168.0.101
    Destination Address: 128.119.245.12
Transmission Control Protocol, Src Port: 62138, Dst Port: 80, Seq: 1, Ack: 1, Len: 851
    Source Port: 62138
    Destination Port: 80
    [Stream index: 11]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 851]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2945921734
    [Next Sequence Number: 852    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2608743633
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x018 (PSH, ACK)
    Window: 2058
    [Calculated window size: 131712]
    [Window size scaling factor: 64]
    Checksum: 0x1435 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [Timestamps]
```

Source Port (tcp.srcport), 2 bytes Packets: 12101 · Displayed: 8 (0.1%) · Dropped: 0 (0.0%) Profile: Default