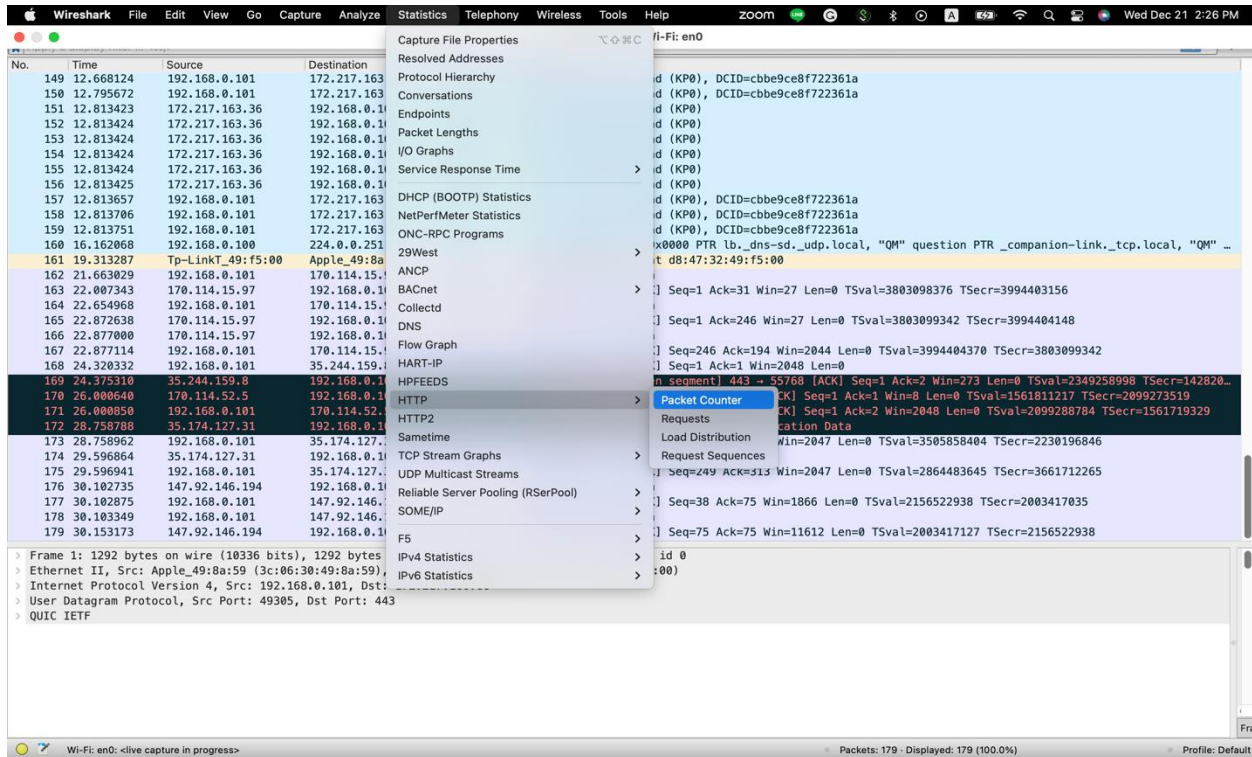


HW3

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

Display filter: Apply

Copy Save as... Close

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 HTTP 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:

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	3.068385	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	27.834812	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:el:1f	Apple_49:8a:59	ARP	56	172.17.42.170 is at 52:09:14:dd:el: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

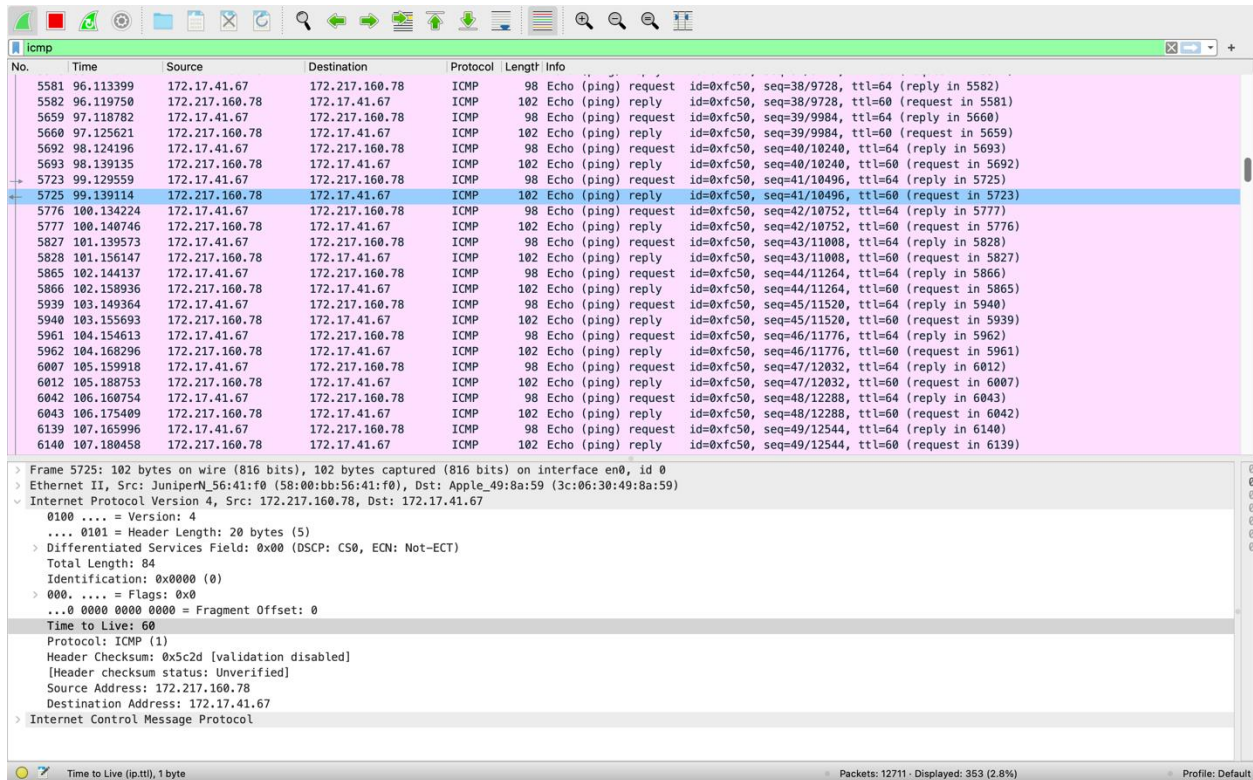
> Frame 88: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface en0, id 0
 > Ethernet II, Src: Apple_49:8a:59 (3c:06:30:49:8a:59), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 > Address Resolution Protocol (request)

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:



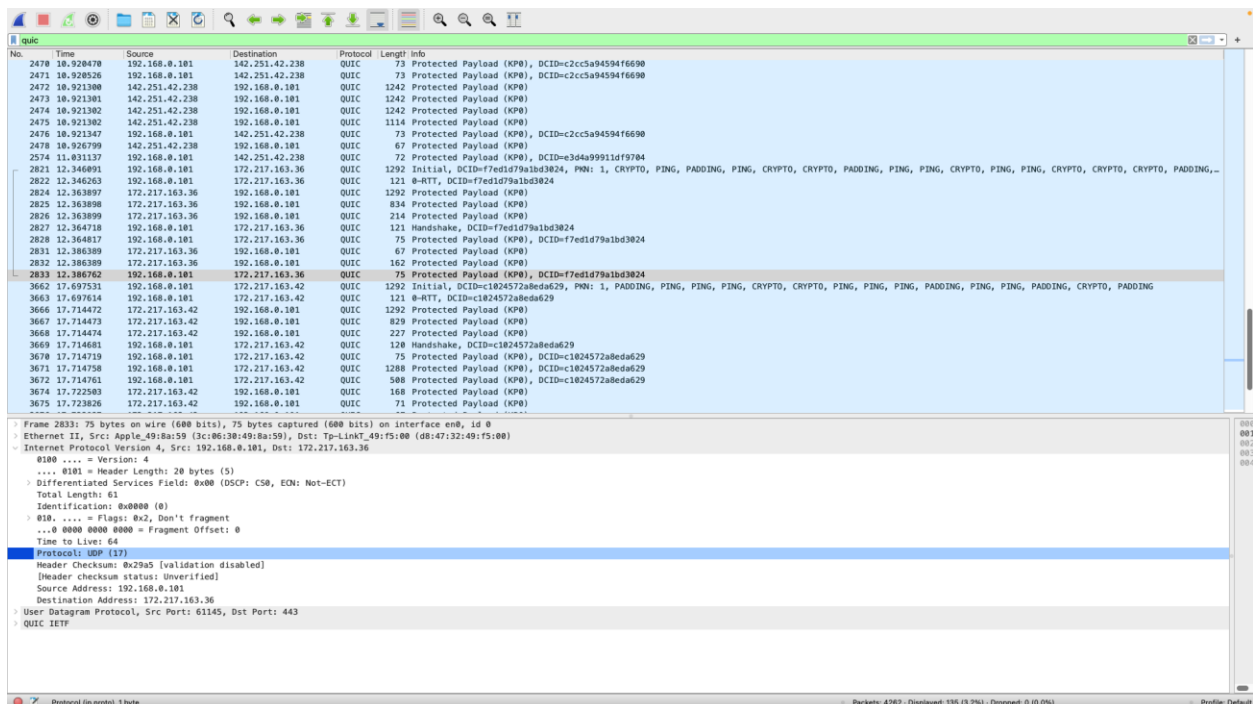
No.	Time	Source	Destination	Protocol	Length	Info
5581	96.113399	172.17.41.67	172.217.160.78	ICMP	98	Echo (ping) request id=0xfc50, seq=38/9728, ttl=64 (reply in 5582)
5582	96.119758	172.217.160.78	172.17.41.67	ICMP	102	Echo (ping) reply id=0xfc50, seq=38/9728, ttl=60 (request in 5581)
5659	97.118782	172.17.41.67	172.217.160.78	ICMP	98	Echo (ping) request id=0xfc50, seq=39/9984, ttl=64 (reply in 5660)
5660	97.125621	172.217.160.78	172.17.41.67	ICMP	102	Echo (ping) reply id=0xfc50, seq=39/9984, ttl=60 (request in 5659)
5692	98.124196	172.17.41.67	172.217.160.78	ICMP	98	Echo (ping) request id=0xfc50, seq=40/10240, ttl=64 (reply in 5693)
5693	98.139135	172.217.160.78	172.17.41.67	ICMP	102	Echo (ping) reply id=0xfc50, seq=40/10240, ttl=60 (request in 5692)
5723	99.129559	172.17.41.67	172.217.160.78	ICMP	98	Echo (ping) request id=0xfc50, seq=41/10496, ttl=64 (reply in 5725)
5725	99.139114	172.217.160.78	172.17.41.67	ICMP	102	Echo (ping) reply id=0xfc50, seq=41/10496, ttl=60 (request in 5723)
5776	100.134224	172.17.41.67	172.217.160.78	ICMP	98	Echo (ping) request id=0xfc50, seq=42/10752, ttl=64 (reply in 5777)
5777	100.140746	172.217.160.78	172.17.41.67	ICMP	102	Echo (ping) reply id=0xfc50, seq=42/10752, ttl=60 (request in 5776)
5827	101.139573	172.17.41.67	172.217.160.78	ICMP	98	Echo (ping) request id=0xfc50, seq=43/11008, ttl=64 (reply in 5828)
5828	101.156147	172.217.160.78	172.17.41.67	ICMP	102	Echo (ping) reply id=0xfc50, seq=43/11008, ttl=60 (request in 5827)
5865	102.144137	172.17.41.67	172.217.160.78	ICMP	98	Echo (ping) request id=0xfc50, seq=44/11264, ttl=64 (reply in 5866)
5866	102.158936	172.217.160.78	172.17.41.67	ICMP	102	Echo (ping) reply id=0xfc50, seq=44/11264, ttl=60 (request in 5865)
5939	103.149364	172.17.41.67	172.217.160.78	ICMP	98	Echo (ping) request id=0xfc50, seq=45/11520, ttl=64 (reply in 5940)
5940	103.155693	172.217.160.78	172.17.41.67	ICMP	102	Echo (ping) reply id=0xfc50, seq=45/11520, ttl=60 (request in 5939)
5961	104.154613	172.17.41.67	172.217.160.78	ICMP	98	Echo (ping) request id=0xfc50, seq=46/11776, ttl=64 (reply in 5962)
5962	104.168296	172.217.160.78	172.17.41.67	ICMP	102	Echo (ping) reply id=0xfc50, seq=46/11776, ttl=60 (request in 5961)
6007	105.159918	172.17.41.67	172.217.160.78	ICMP	98	Echo (ping) request id=0xfc50, seq=47/12032, ttl=64 (reply in 6012)
6012	105.188753	172.217.160.78	172.17.41.67	ICMP	102	Echo (ping) reply id=0xfc50, seq=47/12032, ttl=60 (request in 6007)
6042	106.160754	172.17.41.67	172.217.160.78	ICMP	98	Echo (ping) request id=0xfc50, seq=48/12288, ttl=64 (reply in 6043)
6043	106.175409	172.217.160.78	172.17.41.67	ICMP	102	Echo (ping) reply id=0xfc50, seq=48/12288, ttl=60 (request in 6042)
6139	107.165996	172.17.41.67	172.217.160.78	ICMP	98	Echo (ping) request id=0xfc50, seq=49/12544, ttl=64 (reply in 6140)
6140	107.180458	172.217.160.78	172.17.41.67	ICMP	102	Echo (ping) reply id=0xfc50, seq=49/12544, ttl=60 (request in 6139)

> Frame 5725: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface en0, id 0
 > Ethernet II, Src: JuniperN_56:41:f0 (58:00:bb:56:41:f0), Dst: Apple_49:8a:59 (3c:06:30:49:8a:59)
 > Internet Protocol Version 4, Src: 172.217.160.78, Dst: 172.17.41.67
 > 0100 = Version: 4
 > 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 > Total Length: 84
 > Identification: 0x0000 (0)
 > 0000 = Flags: 0x0
 > ...0 0000 0000 0000 = Fragment Offset: 0
 > Time to Live: 60
 > Protocol: ICMP (1)
 > Header Checksum: 0x5c2d [validation disabled]
 > [Header checksum status: Unverified]
 > Source Address: 172.217.160.78
 > Destination Address: 172.17.41.67
 > Internet Control Message Protocol

Time to Live (ip.ttl), 1 byte Packets: 12711 Displayed: 353 (2.8%) Profile: Default

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

Here is the screenshot:



No.	Time	Source	Destination	Protocol	Length	Info
2470	10.928478	192.168.0.101	142.251.42.238	QUIC	73	Protected Payload (K0), DCID=c2c5a94594f6690
2471	10.928526	192.168.0.101	142.251.42.238	QUIC	73	Protected Payload (K0), DCID=c2c5a94594f6690
2472	10.921300	142.251.42.238	192.168.0.101	QUIC	1242	Protected Payload (K0)
2473	10.921301	142.251.42.238	192.168.0.101	QUIC	1242	Protected Payload (K0)
2474	10.921302	142.251.42.238	192.168.0.101	QUIC	1242	Protected Payload (K0)
2475	10.921302	142.251.42.238	192.168.0.101	QUIC	1114	Protected Payload (K0)
2476	10.921347	192.168.0.101	142.251.42.238	QUIC	73	Protected Payload (K0), DCID=c2c5a94594f6690
2478	10.928799	142.251.42.238	192.168.0.101	QUIC	67	Protected Payload (K0), DCID=c3da99911df9784
2574	11.031137	192.168.0.101	142.251.42.238	QUIC	72	Protected Payload (K0), DCID=c3da99911df9784
2821	12.346091	192.168.0.101	172.217.163.36	QUIC	1292	Initial, DCID=f7ed1d79a1bd3024, PN: 1, CRYPTO, PING, PADDING, PING, CRYPTO, CRYPTO, PADDING, PING, PING, PADDING, PING, PING, CRYPTO, CRYPTO, CRYPTO, PADDING,...
2822	12.346263	192.168.0.101	172.217.163.36	QUIC	121	0-RTT, DCID=f7ed1d79a1bd3024
2824	12.363897	172.217.163.36	192.168.0.101	QUIC	1292	Protected Payload (K0)
2825	12.363898	172.217.163.36	192.168.0.101	QUIC	834	Protected Payload (K0)
2826	12.363899	172.217.163.36	192.168.0.101	QUIC	214	Protected Payload (K0)
2827	12.364718	192.168.0.101	172.217.163.36	QUIC	121	Handshake, DCID=f7ed1d79a1bd3024
2828	12.364817	192.168.0.101	172.217.163.36	QUIC	75	Protected Payload (K0), DCID=f7ed1d79a1bd3024
2831	12.386389	172.217.163.36	192.168.0.101	QUIC	67	Protected Payload (K0)
2832	12.386389	172.217.163.36	192.168.0.101	QUIC	162	Protected Payload (K0)
2833	12.386762	192.168.0.101	172.217.163.36	QUIC	75	Protected Payload (K0), DCID=f7ed1d79a1bd3024
3662	17.697531	192.168.0.101	172.217.163.42	QUIC	1292	Initial, DCID=c1824572a8eda629, PN: 1, PADDING, PING, PING, PING, CRYPTO, CRYPTO, PING, PING, PING, PADDING, PING, PING, PADDING, CRYPTO, PADDING
3663	17.697614	192.168.0.101	172.217.163.42	QUIC	121	0-RTT, DCID=c1824572a8eda629
3666	17.714472	172.217.163.42	192.168.0.101	QUIC	1292	Protected Payload (K0)
3667	17.714473	172.217.163.42	192.168.0.101	QUIC	829	Protected Payload (K0)
3668	17.714474	172.217.163.42	192.168.0.101	QUIC	227	Protected Payload (K0)
3669	17.714681	192.168.0.101	172.217.163.42	QUIC	128	Handshake, DCID=c1824572a8eda629
3670	17.714719	192.168.0.101	172.217.163.42	QUIC	75	Protected Payload (K0), DCID=c1824572a8eda629
3671	17.714758	192.168.0.101	172.217.163.42	QUIC	1288	Protected Payload (K0), DCID=c1824572a8eda629
3672	17.714761	192.168.0.101	172.217.163.42	QUIC	508	Protected Payload (K0), DCID=c1824572a8eda629
3674	17.722503	172.217.163.42	192.168.0.101	QUIC	168	Protected Payload (K0)
3675	17.723826	172.217.163.42	192.168.0.101	QUIC	71	Protected Payload (K0)

> Frame 2833: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface en0, id 0
 > Ethernet II, Src: Apple_49:8a:59 (3c:06:30:49:8a:59), Dst: Tp-Link_A9:f5:00 (08:47:32:49:f5:00)
 > Internet Protocol Version 4, Src: 192.168.0.101, Dst: 172.217.163.36
 > 0100 = Version: 4
 > 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 > Total Length: 61
 > Identification: 0x0000 (0)
 > 0100 = Flags: 0x2, Don't fragment
 > ...0 0000 0000 0000 = Fragment Offset: 0
 > Time to Live: 64
 > Protocol: UDP (17)
 > Header Checksum: 0x29a5 [validation disabled]
 > [Header checksum status: Unverified]
 > Source Address: 192.168.0.101
 > Destination Address: 172.217.163.36
 > User Datagram Protocol, Src Port: 61145, Dst Port: 443
 > QUIC IETF

Protocol (ip.proto), 1 byte Packets: 4262 Displayed: 135 (3.2%) Dropped: 0 (0.0%) Profile: Default

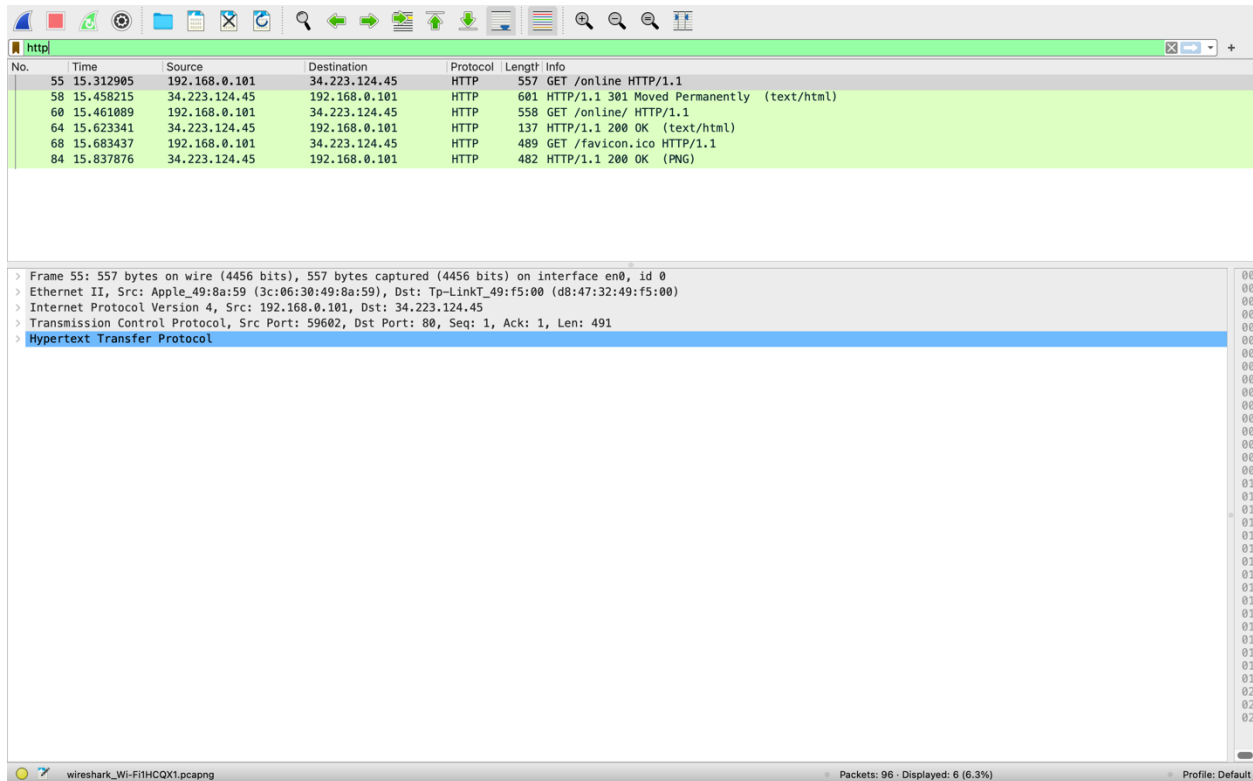
6)

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:

No.	Time	Source	Destination	Protocol	Length	Info
55	15.312905	192.168.0.101	34.223.124.45	HTTP	557	GET /online HTTP/1.1
58	15.458215	34.223.124.45	192.168.0.101	HTTP	601	HTTP/1.1 301 Moved Permanently (text/html)
60	15.461809	192.168.0.101	34.223.124.45	HTTP	558	GET /online/ HTTP/1.1
64	15.623341	34.223.124.45	192.168.0.101	HTTP	137	HTTP/1.1 200 OK (text/html)
68	15.683437	192.168.0.101	34.223.124.45	HTTP	489	GET /favicon.ico HTTP/1.1
84	15.837876	34.223.124.45	192.168.0.101	HTTP	482	HTTP/1.1 200 OK (PNG)

Frame 55: 557 bytes on wire (4456 bits), 557 bytes captured (4456 bits) on interface en0, id 0
Ethernet II, Src: Apple_49:8a:59 (3c:06:30:49:8a:59), Dst: Tp-LinkT_49:f5:00 (d8:47:32:49:f5:00)
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 34.223.124.45
Transmission Control Protocol, Src Port: 59602, Dst Port: 80, Seq: 1, Ack: 1, Len: 491
Hypertext Transfer Protocol

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:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.17.41.72	172.17.47.255	NBNS	92	Name query NB BRW541379712381<00>
2	0.000001	172.17.45.249	172.17.47.255	NBNS	110	Registration NB MACBOOKPRO-FECA<00>
3	0.000001	172.17.45.249	172.17.47.255	NBNS	110	Registration NB MACBOOKPRO-FECA<20>
4	0.000001	172.17.40.61	224.0.0.251	MDNS	191	Standard query 0x0000 ANY 佩佩._rdlink._tcp.local, "QM" question ANY haihai.local, "QM" question SRV 0
6	0.001195	172.17.44.111	224.0.0.251	MDNS	75	Standard query 0x0000 PTR _ipp._tcp.local, "QM" question
8	0.001196	172.17.44.111	224.0.0.251	MDNS	76	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question
10	0.002308	172.17.45.249	224.0.0.251	MDNS	340	Standard query response 0x0000 TXT PTR, cache flush Ashleyde-MacBook-Pro.local PTR, cache flush Ashley.
12	0.102800	172.17.45.241	172.17.47.255	DTLS	414	Continuation Data
13	0.102801	172.17.40.61	224.0.0.251	MDNS	723	Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _homekit._tcp.local, "QM" ques.
15	0.105050	172.17.46.0	224.0.0.251	MDNS	201	Standard query response 0x0000 PTR iPad Air (第二代)._rdlink._tcp.local TXT OPT
17	0.205281	172.17.41.72	224.0.0.251	MDNS	81	Standard query 0x0000 A BRW541379712381.local, "QM" question
18	0.205284	172.17.40.61	224.0.0.251	MDNS	182	Standard query response 0x0000 PTR _rdlink._tcp.local TXT OPT
21	0.206311	172.17.41.72	224.0.0.251	MDNS	81	Standard query 0x0000 A BRW541379712381.local, "QM" question
23	0.206313	172.17.41.72	172.17.47.255	NBNS	92	Name query NB AURORA-SERVER<00>
24	0.207164	172.17.41.67	142.251.42.238	TLSv1	115	Application Data
26	0.212984	142.251.42.238	172.17.41.67	TCP	70	443 → 55032 [ACK] Seq=1 Ack=50 Win=265 Len=0 TSval=4293373219 TSecr=174814166
27	0.212985	142.251.42.238	172.17.41.67	TLSv1	143	Application Data
28	0.213142	172.17.41.67	142.251.42.238	TCP	66	55032 → 443 [ACK] Seq=50 Ack=78 Win=2033 Len=0 TSval=174814172 TSecr=4293373219
29	0.213380	172.17.41.67	142.251.42.238	TLSv1	105	Application Data
30	0.225025	142.251.42.238	172.17.41.67	TCP	70	443 → 55032 [ACK] Seq=78 Ack=89 Win=265 Len=0 TSval=4293373230 TSecr=174814172
31	0.307319	172.17.45.249	172.17.47.255	UDP	86	57621 → 57621 Len=44
32	0.307320	172.17.40.204	172.17.47.255	NBNS	92	Name query NB MACBOOKPRO-3C2B<00>
33	0.410533	172.17.43.79	172.17.47.255	BROWS	216	Get Backup List Request
34	0.410535	172.17.40.61	224.0.0.251	MDNS	342	Standard query response 0x0000 TXT, cache flush PTR 佩佩._rdlink._tcp.local TXT SRV, cache flush 0 0 58

Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface en0, id 0
 Ethernet II, Src: IntelCor_0a:d3:ea (d0:c6:37:0a:d3:ea), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 Source: IntelCor_0a:d3:ea (d0:c6:37:0a:d3:ea)
 Type: IPv4 (0x0008)
 Internet Protocol Version 4, Src: 172.17.41.72, Dst: 172.17.47.255
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x60 (DSCP: CS3, ECN: Not-ECT)
 Total Length: 78
 Identification: 0x2e6b (11883)
 0000 = Flags: 0x0
 ...0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 128
 Protocol: UDP (17)
 Header Checksum: 0x5a6a [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 172.17.41.72
 Destination Address: 172.17.47.255

IPv6 packet:

Here is the screenshot:

No.	Time	Source	Destination	Protocol	Length	Info
5	0.001194	fe80::1c2b:f655:5e2:9928	ff02::fb	MDNS	211	Standard query 0x0000 ANY 佩佩._rdlink._tcp.local, "QM" question ANY haihai.local, "QM" question SRV 0
7	0.001195	fe80::a9f8:a714:e6...	ff02::fb	MDNS	95	Standard query 0x0000 PTR _ipp._tcp.local, "QM" question
9	0.002307	fe80::a9f8:a714:e6...	ff02::fb	MDNS	96	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question
11	0.003800	fe80::18a8:b7f9:f1...	ff02::fb	MDNS	360	Standard query response 0x0000 TXT PTR, cache flush Ashleyde-MacBook-Pro.local PTR, cache flush Ashley.
14	0.103846	fe80::1c2b:f655:5e2:9928	ff02::fb	MDNS	743	Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _homekit._tcp.local, "QM" ques.
16	0.105051	fe80::181e:9b1b:6d...	ff02::fb	MDNS	221	Standard query response 0x0000 PTR iPad Air (第二代)._rdlink._tcp.local TXT OPT
19	0.205285	fe80::1c2b:f655:5e2:9928	ff02::fb	MDNS	202	Standard query response 0x0000 PTR _rdlink._tcp.local TXT OPT
20	0.205285	fe80::73c8:f90b:cd...	ff02::fb	MDNS	101	Standard query 0x0000 A BRW541379712381.local, "QM" question
22	0.206312	fe80::73c8:f90b:cd...	ff02::fb	MDNS	101	Standard query 0x0000 A BRW541379712381.local, "QM" question
25	0.207278	fe80::1c9f:62b0:88...	ff02::fb	MDNS	207	Standard query response 0x0000 TXT PTR 黄墨柔的iPad._rdlink._tcp.local OPT
35	0.410565	fe80::1869:6f8e:5f...	ff02::fb	MDNS	172	Standard query 0x0000 PTR lb._dns-sd._udp.local, "QU" question PTR _companion-link._tcp.local, "QU" qu.
37	0.412759	fe80::890:86d3:a06...	ff02::fb	MDNS	270	Standard query response 0x0000 PTR, cache flush Kiwi.local PTR, cache flush Kiwi.local NSEC, cache flu.
38	0.439233	fe80::1c82:61e4:db...	fe80::c6f:ce06:564...	ICMPv6	86	Neighbor Solicitation for fe80::c6f:ce06:5649:32fa from 76:28:3f:dc:45:4c
39	0.439448	fe80::c6f:ce06:564...	fe80::1c82:61e4:db...	ICMPv6	78	Neighbor Advertisement fe80::c6f:ce06:5649:32fa (sol)
40	0.464658	fe80::c6f:ce06:564...	ff02::1:ff73:afba	ICMPv6	86	Neighbor Solicitation for fe80::1869:6f8e:5f73:afba from 3c:06:30:49:8a:59
41	0.475692	fe80::1869:6f8e:5f...	fe80::c6f:ce06:564...	ICMPv6	86	Neighbor Advertisement fe80::1869:6f8e:5f73:afba (sol, ovr) is at e2:ee:4d:d5:6b:a0
42	0.475827	fe80::c6f:ce06:564...	fe80::1869:6f8e:5f...	MDNS	410	Standard query response 0x0000 PTR Ralph's MacBook Pro._companion-link._tcp.local SRV, cache flush 0 0
44	0.511975	fe80::73c8:f90b:cd...	ff02::fb	MDNS	99	Standard query 0x0000 A AURORA-SERVER.local, "QM" question
46	0.511976	fe80::73c8:f90b:cd...	ff02::fb	MDNS	99	Standard query 0x0000 AAAA AURORA-SERVER.local, "QM" question
47	0.512962	fe80::1c82:61e4:db...	ff02::fb	MDNS	271	Standard query response 0x0000 PTR, cache flush akira.local PTR, cache flush akira.local NSEC, cache f.
50	0.514371	fe80::73c8:f90b:cd...	ff02::fb	MDNS	99	Standard query 0x0000 A AURORA-SERVER.local, "QM" question

Frame 5: 211 bytes on wire (1688 bits), 211 bytes captured (1688 bits) on interface en0, id 0
 Ethernet II, Src: fa:16:23:54:40:55 (fa:16:23:54:40:55), Dst: IPv6mcast_fb (33:33:00:00:00:fb)
 Destination: IPv6mcast_fb (33:33:00:00:00:fb)
 Source: fa:16:23:54:40:55 (fa:16:23:54:40:55)
 Type: IPv6 (0x000d)
 Internet Protocol Version 6, Src: fe80::1c2b:f655:5e2:9928, Dst: ff02::fb
 0110 = Version: 6
 0000 0000 = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
 1101 0000 1101 0000 0000 = Flow Label: 0xd0d00
 Payload Length: 157
 Next Header: UDP (17)
 Hop Limit: 255
 Source Address: fe80::1c2b:f655:5e2:9928
 Destination Address: ff02::fb
 User Datagram Protocol, Src Port: 5353, Dst Port: 5353
 Multicast Domain Name System (query)

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

Here is the screenshot:

No.	Time	Source	Destination	Protocol	Length	Info
4652	117.890058	172.17.41.67	140.113.1.1	DNS	102	Standard query 0x2c4f HTTPS onedscolprdeus11.eastus.cloudapp.azure.com
4653	117.890274	172.17.41.67	140.113.1.1	DNS	102	Standard query 0x5ffd A onedscolprdeus11.eastus.cloudapp.azure.com
4725	118.927451	172.17.41.67	140.113.1.1	DNS	102	Standard query 0x2c4f HTTPS onedscolprdeus11.eastus.cloudapp.azure.com
4726	118.927657	172.17.41.67	140.113.1.1	DNS	102	Standard query 0x5ffd A onedscolprdeus11.eastus.cloudapp.azure.com
4738	119.333459	140.113.1.1	172.17.41.67	DNS	173	Standard query response 0x2c4f HTTPS onedscolprdeus11.eastus.cloudapp.azure.com SOA ns1-201.azure-dns..
4752	120.294221	140.113.1.1	172.17.41.67	DNS	102	Standard query 0x5ffd A onedscolprdeus11.eastus.cloudapp.azure.com
4760	120.488632	172.17.41.67	140.113.1.1	DNS	102	Standard query 0x5ffd A onedscolprdeus11.eastus.cloudapp.azure.com
4806	121.524433	172.17.41.67	140.113.1.1	DNS	102	Standard query 0x5ffd A onedscolprdeus11.eastus.cloudapp.azure.com
4843	122.991328	140.113.1.1	172.17.41.67	DNS	118	Standard query response 0x5ffd A onedscolprdeus11.eastus.cloudapp.azure.com SOA ns1-201.azure-dns..
8701	210.968824	172.17.41.67	8.8.8.8	DNS	70	Standard query 0x8b41 A dns.google
8702	210.968869	172.17.41.67	8.8.8.8	DNS	70	Standard query 0xc68c HTTPS dns.google
8703	210.974913	8.8.8.8	172.17.41.67	DNS	102	Standard query response 0x8b41 A dns.google A 8.8.4.4 A 8.8.8.8
8704	210.974913	8.8.8.8	172.17.41.67	DNS	150	Standard query response 0xc68c HTTPS dns.google SOA ns1.zdns.google
117..	269.393455	172.17.41.67	140.113.1.1	DNS	74	Standard query 0xef74 HTTPS gsas.apple.com
117..	269.393567	172.17.41.67	140.113.1.1	DNS	74	Standard query 0x56c5 A gsas.apple.com
118..	270.428985	172.17.41.67	140.113.1.1	DNS	74	Standard query 0xef74 HTTPS gsas.apple.com
118..	270.429135	172.17.41.67	140.113.1.1	DNS	74	Standard query 0x56c5 A gsas.apple.com
119..	270.858199	140.113.1.1	172.17.41.67	DNS	166	Standard query response 0x56c5 A gsas.apple.com CNAME gsas.idms-apple.com.akadns.net A 17.188.23.79 A ..
119..	271.766111	140.113.1.1	172.17.41.67	DNS	166	Standard query response 0x56c5 A gsas.apple.com CNAME gsas.idms-apple.com.akadns.net A 17.188.23.52 A ..
119..	271.794192	140.113.1.1	172.17.41.67	DNS	181	Standard query response 0xef74 HTTPS gsas.apple.com CNAME gsas.idms-apple.com.akadns.net SOA internal..
119..	271.794592	172.17.41.67	140.113.1.1	DNS	90	Standard query 0xd7f3 HTTPS gsas.idms-apple.com.akadns.net
120..	272.824168	172.17.41.67	140.113.1.1	DNS	90	Standard query 0xd7f3 HTTPS gsas.idms-apple.com.akadns.net
120..	273.064278	140.113.1.1	172.17.41.67	DNS	156	Standard query response 0xd7f3 HTTPS gsas.idms-apple.com.akadns.net SOA internal.akadns.net
120..	274.237604	140.113.1.1	172.17.41.67	DNS	156	Standard query response 0xd7f3 HTTPS gsas.idms-apple.com.akadns.net SOA internal.akadns.net

[Coloring Rule Name: UDP]	
[Coloring Rule String: udp]	
> Ethernet II, Src: Apple_49:8a:59 (3c:06:30:49:8a:59), Dst: JuniperN_56:41:f0 (58:00:bb:56:41:f0)	
> Internet Protocol Version 4, Src: 172.17.41.67, Dst: 140.113.1.1	
0100 = Version: 4	
.... 0101 = Header Length: 20 bytes (5)	
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)	
Total Length: 88	
Identification: 0x6cfe (27902)	
> 000. = Flags: 0x0	
...0 0000 0000 0000 = Fragment Offset: 0	
Time to Live: 64	
Protocol: UDP (17)	
Header Checksum: 0xaa00 [validation disabled]	
[Header checksum status: Unverified]	
Source Address: 172.17.41.67	
Destination Address: 140.113.1.1	
> User Datagram Protocol, Src Port: 63667, Dst Port: 53	
> Domain Name System (query)	

Time to Live (ip.ttl), 1 byte

Packets: 28762 - Displayed: 104 (0.4%)

Profile: Default

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:

The screenshot displays the Wireshark network protocol analyzer interface. The top section, 'Packet List', shows a single captured packet (No. 1) of type HTTP. The packet details pane on the right shows the structure of the packet, including the Ethernet II layer, Internet Protocol Version 4 layer, Transmission Control Protocol layer, and Hypertext Transfer Protocol layer. The packet is a GET request for the file /wreshark-labs/HTTP-wireshark-file4.html.

No.	Time	Source	Destination	Protocol	Length	Source Port	Info
1	1900.13.438167	192.168.0.101	128.119.245.12	HTTP	917	62138	GET /wreshark-labs/HTTP-wireshark-file4.html HTTP/1.1

Packet Details:

- Ethernet II, Src: Intel (08:00:27:00:00:00), Dst: Intel (08:00:27:00:00:00)
- Internet Protocol Version 4, Src: 192.168.0.101, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 62138, Dst Port: 80, Seq: 1, Ack: 1, Len: 851
- Hypertext Transfer Protocol
 - GET /wreshark-labs/HTTP-wireshark-file4.html HTTP/1.1