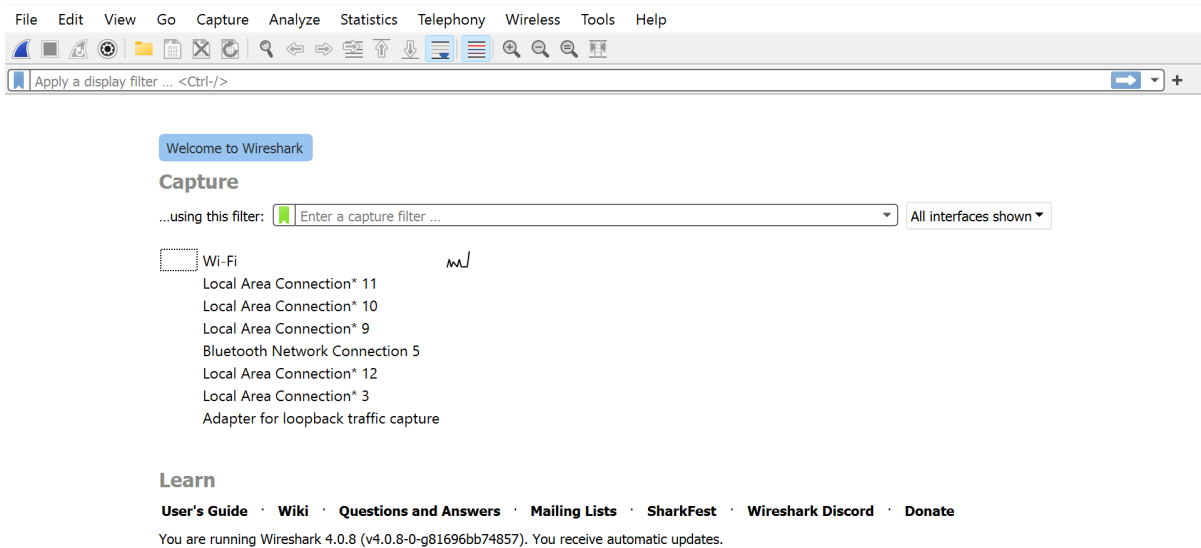
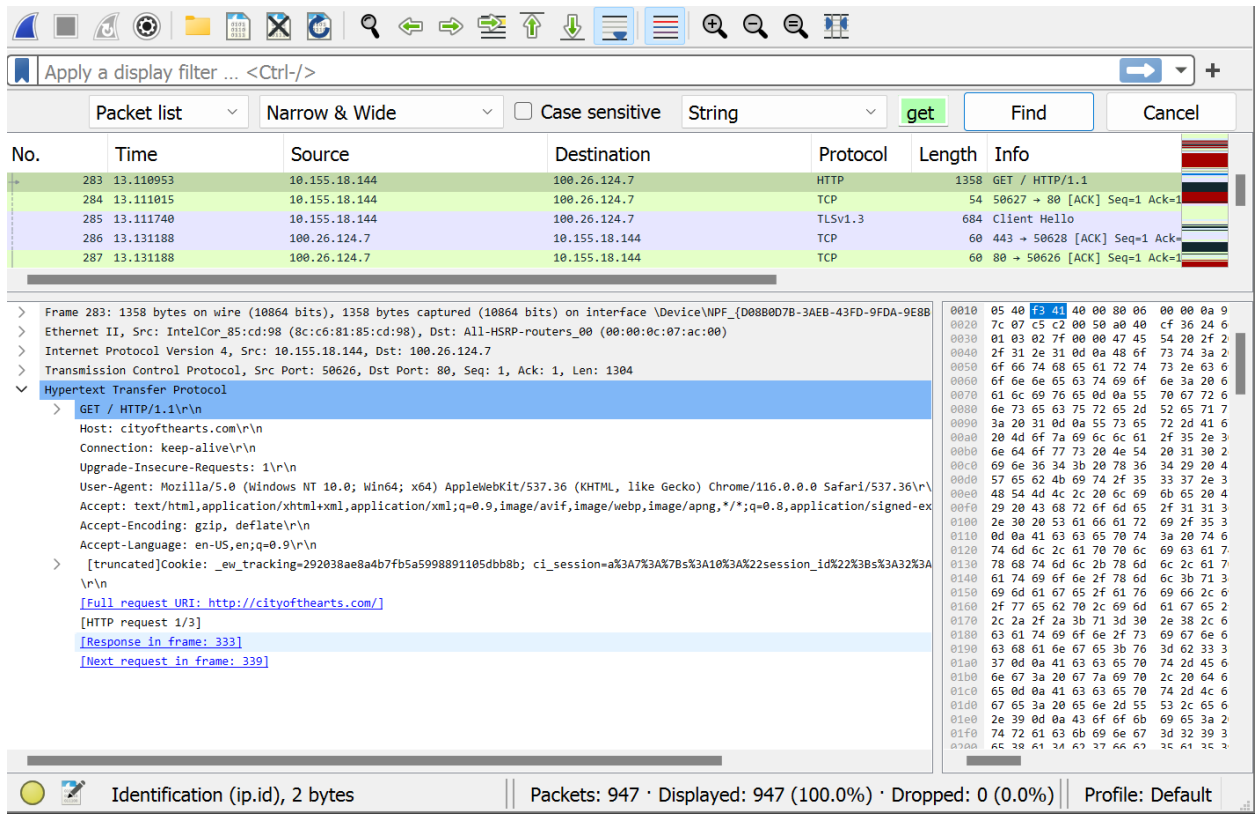


Section 1: Packet Capture (wireshark)

- Step 7:



- Step 14:



- Step 15:

Apply a display filter ... <Ctrl-/>

Packet list Narrow & Wide Case sensitive String get Find Cancel

No.	Time	Source	Destination	Protocol	Length	Info
283	13.110953	10.155.18.144	100.26.124.7	HTTP	1358	GET / HTTP/1.1
284	13.111015	10.155.18.144	100.26.124.7	TCP	54	50627 → 80 [ACK] Seq=1 Ack=1
285	13.111740	10.155.18.144	100.26.124.7	TLSv1.3	684	Client Hello
286	13.131188	100.26.124.7	10.155.18.144	TCP	60	443 → 50628 [ACK] Seq=1 Ack=1
287	13.131188	100.26.124.7	10.155.18.144	TCP	60	80 → 50626 [ACK] Seq=1 Ack=1

Internet Protocol Version 4, Src: 10.155.18.144, Dst: 100.26.124.7

Transmission Control Protocol, Src Port: 50626, Dst Port: 80, Seq: 1, Ack: 1, Len: 1304

Source Port: 50626
Destination Port: 80
[Stream index: 23]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 1304]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 2688601910
[Next Sequence Number: 1305 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 610675714
0101 = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 259
[Calculated window size: 66304]
[Window size scaling factor: 256]
Checksum: 0x027f [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
TCP payload (1304 bytes)

Identification (ip.id), 2 bytes

Packets: 947 · Displayed: 947 (100.0%) · Dropped: 0 (0.0%) Profile: Default

- Step 16:

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Packet list Narrow & Wide Case sensitive String get Find Cancel

No.	Time	Source	Destination	Protocol	Length	Info
283	13.110953	10.155.18.144	100.26.124.7	HTTP	1358	GET / HTTP/1.1
284	13.111015	10.155.18.144	100.26.124.7	TCP	54	50627 → 80 [ACK] Seq=1 Ack=1
285	13.111740	10.155.18.144	100.26.124.7	TLSv1.3	684	Client Hello
286	13.131188	100.26.124.7	10.155.18.144	TCP	60	443 → 50628 [ACK] Seq=1 Ack=1
287	13.131188	100.26.124.7	10.155.18.144	TCP	60	80 → 50626 [ACK] Seq=1 Ack=1

Frame 283: 1358 bytes on wire (10864 bits), 1358 bytes captured (10864 bits) on interface \Device\NPF_{D08B0D7B-3AEB-43FD-9FDA-9EBB}

Ethernet II, Src: IntelCor_85:cd:98 (8c:c6:81:85:cd:98), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)

Internet Protocol Version 4, Src: 10.155.18.144, Dst: 100.26.124.7

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1344
Identification: 0xf341 (62273)
010. = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.155.18.144
Destination Address: 100.26.124.7

Transmission Control Protocol, Src Port: 50626, Dst Port: 80, Seq: 1, Ack: 1, Len: 1304

Hypertext Transfer Protocol

Sequence Number (tcp.seq), 4 bytes

Packets: 947 · Displayed: 947 (100.0%) · Dropped: 0 (0.0%) Profile: Default

Section 1: Questions

1. A. My IP address is 10.155.18.144 the destination IP (cityofhearts.com) address is 100.26.124.7

```
Internet Protocol Version 4, Src: 10.155.18.144, Dst: 100.26.124.7
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1344
Identification: 0xf341 (62273)
> 010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.155.18.144
Destination Address: 100.26.124.7
```

- B. I am using HTTP version 4.

```
Internet Protocol Version 4, Src: 10.155.18.144, Dst: 100.26.124.7
0100 .... = Version: 4
```

- C. My computer's port number is 50626

```
Transmission Control Protocol, Src Port: 50626, Dst Port: 80, Seq: 1, Ack: 1, Len: 1304
Source Port: 50626
Destination Port: 80
```

- D. The destination server port number is 80.

```
Transmission Control Protocol, Src Port: 50626, Dst Port: 80, Seq: 1, Ack: 1, Len: 1304
Source Port: 50626
Destination Port: 80
```

E. By keeping alive, it means it is just keeping the connection until all information is given to be able to download the webpage.

2. My wireshark captured 947 packets.

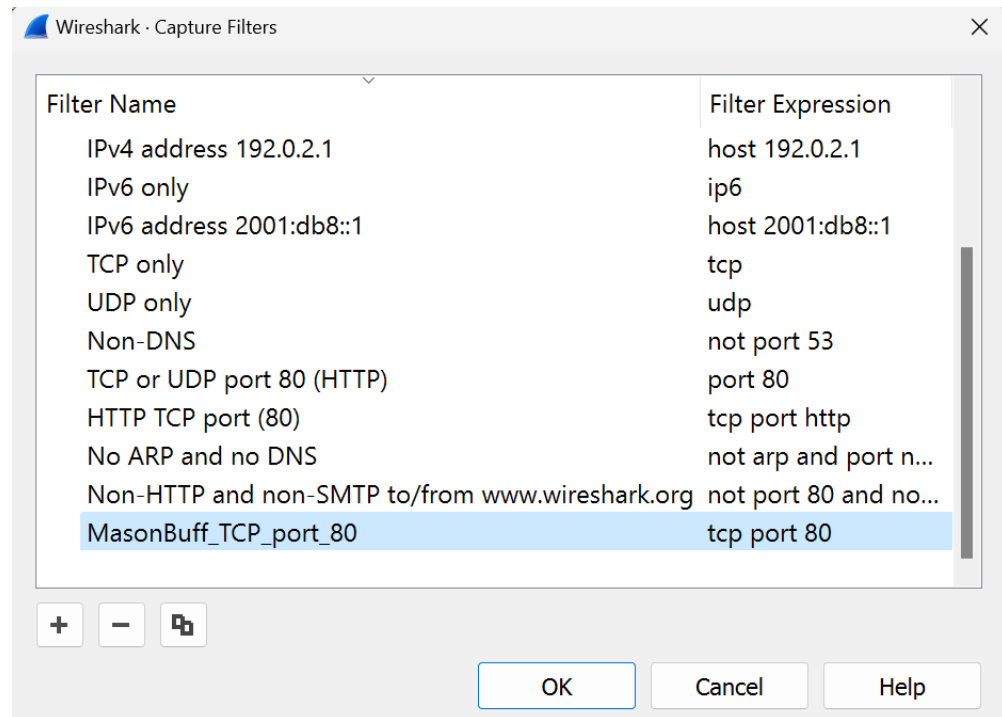
No.	Time	Source	Destination	Protocol	Length	Info
944	24.435621	172.253.122.139	10.155.18.144	UDP	68	443 → 51283 Len=26
945	24.664270	10.155.18.144	172.253.122.139	UDP	71	51283 → 443 Len=29
946	24.703388	172.253.122.139	10.155.18.144	UDP	68	443 → 51283 Len=26
947	24.912309	10.155.18.144	10.155.57.208	TCP	66	[TCP Retransmission] 50640 →

3. Yes, some other IP addresses are 104.106.164.76, 152.1.14.14, and 172.253.62.95.
These IP addresses could be coming from the google doc webpage which I'm using to type this or possibly IP addresses for DNS servers or other switches and routers.
4. Some protocol types used include: DNS, TLSv1.2, TCP, and QUIC.
5. A. TCP uses purple
B. HTTP uses green
C. UDP uses blue

- D. ARP uses yellow
- E. TCP RST uses red

Section 2: Capturing Web Traffic

- **Step 4:**



- Step 14:

Apply a display filter ... <Ctrl-/>

Packet list Narrow & Wide Case sensitive String get Find Cancel

No.	Time	Source	Destination	Protocol	Length	Info
218	5.229843	192.168.1.168	104.219.248.3	HTTP	691	GET / HTTP/1.1
219	5.259485	2607:f8b0:4002:c08::5b	2603:6081:23f0:a580:349a:25b5:82a2:47fc	QUIC	86	Protected Payload (KP0)
220	5.251214	2603:6081:23f0:a580:349a:25b5:82a2:47fc	2607:f8b0:4002:c2c::5e	QUIC	131	Protected Payload (KP0), DCID=e99611765
221	5.253519	2607:f8b0:4002:c03::5f	2603:6081:23f0:a580:349a:25b5:82a2:47fc	QUIC	87	Protected Payload (KP0)
222	5.276681	2607:f8b0:4002:c2c::5e	2603:6081:23f0:a580:349a:25b5:82a2:47fc	QUIC	87	Protected Payload (KP0)
223	5.358087	104.219.248.3	192.168.1.168	TCP	54	80 → 56617 [ACK] Seq=1 Ack=638 Win=1636
224	5.734376	192.168.1.16	239.255.255.250	UDP	698	52446 → 3702 Len=656
225	6.246951	2607:f8b0:4002:c11::64	2603:6081:23f0:a580:349a:25b5:82a2:47fc	UDP	99	443 → 56924 Len=37
226	6.257627	2603:6081:23f0:a580:349a:25b5:82a2:47fc	2607:f8b0:4002:c11::64	UDP	95	56924 → 443 Len=33
227	6.274916	2607:f8b0:4002:c11::64	2603:6081:23f0:a580:349a:25b5:82a2:47fc	UDP	99	443 → 56924 Len=37
228	6.275448	2603:6081:23f0:a580:349a:25b5:82a2:47fc	2607:f8b0:4002:c11::64	UDP	96	56924 → 443 Len=34
229	6.553637	fe80::e010:308a:4a74:b333	ff02::c	MDNS	718	52447 → 3702 Len=656
230	6.759896	192.168.1.23	224.0.0.251	UDP	782	Standard query response 0x0000 TXT, ca

Ready to load or capture Packets: 544 · Displayed: 544 (100.0%) · Dropped: 0 (0.0%) Profile: Default

- Step 15: There were 544 packets captured.

544	13.206466	fe80::42b8:9057:ffc7:2026	fe80::2eea:dcff:fe31:1492	ICMPv6	86	Neighbor Solicitation for fe80::2eea:dcff:fe31:1492
-----	-----------	---------------------------	---------------------------	--------	----	---

- Step 20: 8 packets captured here.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	104.219.248.3	192.168.1.168	TCP	66	80 → 56244 [SYN, ACK] Seq=0 Ack=1 Win=1460
2	0.202576	104.219.248.3	192.168.1.168	TCP	54	80 → 56244 [ACK] Seq=1 Ack=632 Win=15872
3	0.359246	104.219.248.3	192.168.1.168	TCP	11510	80 → 56244 [ACK] Seq=1 Ack=632 Win=15872
4	0.359246	104.219.248.3	192.168.1.168	HTTP	818	HTTP/1.1 200 OK (text/html)
5	1.004916	104.219.248.3	192.168.1.168	TCP	66	80 → 56245 [SYN, ACK] Seq=0 Ack=1 Win=1460
6	15.373017	104.219.248.3	192.168.1.168	TCP	54	80 → 56244 [FIN, ACK] Seq=12221 Ack=632 Win=0
7	16.136776	104.219.248.3	192.168.1.168	HTTP	287	HTTP/1.1 408 Request Time-out (text/html)
8	16.136776	104.219.248.3	192.168.1.168	TCP	54	80 → 56245 [FIN, ACK] Seq=234 Ack=1 Win=0

Wi-Fi: <live capture in progress>

Packets: 8 · Displayed: 8 (100.0%) Profile: Default

- Step 30: 6 captured packets this time.

Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	104.219.248.3	192.168.1.168	TCP	54	80 → 56263 [RST] Seq=1 Win=0 Len=0
2	14.166950	104.219.248.3	192.168.1.168	TCP	66	80 → 56267 [SYN, ACK] Seq=0 Ack=1 Win=1460
3	14.175103	104.219.248.3	192.168.1.168	TCP	54	80 → 56264 [RST] Seq=1 Win=0 Len=0
4	14.331787	104.219.248.3	192.168.1.168	TCP	54	80 → 56267 [ACK] Seq=1 Ack=648 Win=16384
5	14.629310	104.219.248.3	192.168.1.168	TCP	11510	80 → 56267 [ACK] Seq=1 Ack=648 Win=16384
6	14.629310	104.219.248.3	192.168.1.168	HTTP	818	HTTP/1.1 200 OK (text/html)

wireshark_Wi-FiH44FB2.pcapng

Packets: 6 · Displayed: 6 (100.0%) Profile: Default

• **Step 35:**

Wireshark · Capture Filters	
Filter Name	Filter Expression
TCP only	tcp
UDP only	udp
Non-DNS	not port 53
TCP or UDP port 80 (HTTP)	port 80
HTTP TCP port (80)	tcp port http
No ARP and no DNS	not arp and por...
Non-HTTP and non-SMTP to/from www.wireshark.org	not port 80 and...
MasonBuff_TCP_port_80	tcp port 80
MasonBuff_TCP_port_80_and_walnutcreekamphitheatre.com	tcp port 80
MasonBuff_TCP_port_80_and_walnutcreekamphitheatre.com	tcp port 80 and ...
MasonBuff_port_53	port 53

<C:/Users/mason/AppData/Roaming/Wireshark/cfilters>

OK Cancel Help

- **Step 44: 680 Packets were captured.**

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
53	2.689894	192.168.1.168	192.168.1.1	DNS	73	Standard query 0x6fe2 A udc.ya
54	2.689895	192.168.1.168	192.168.1.1	DNS	73	Standard query 0x81d7 AAAA udc
55	2.698300	2603:6081:23f0:a580::1	2603:6081:23f0:a580:349a:25b5:82a2:47fc	DNS	164	Standard query response 0x6fe2
56	2.698300	192.168.1.1	192.168.1.168	DNS	144	Standard query response 0x6fe2
57	2.719834	2603:6081:23f0:a580::1	2603:6081:23f0:a580:349a:25b5:82a2:47fc	DNS	176	Standard query response 0x01d7
58	2.719834	192.168.1.1	192.168.1.168	DNS	156	Standard query response 0x01d7
59	2.846138	2603:6081:23f0:a580:349a:25b5:82a2:47fc	2603:6081:23f0:a580::1	DNS	108	Standard query 0xf44f A v-ahoi
60	2.846190	2603:6081:23f0:a580:349a:25b5:82a2:47fc	2603:6081:23f0:a580::1	DNS	108	Standard query 0x6db2 A v-b1x9
61	2.855570	2603:6081:23f0:a580:349a:25b5:82a2:47fc	2603:6081:23f0:a580::1	DNS	108	Standard query 0x617b AAAA v-b
62	2.855570	2603:6081:23f0:a580:349a:25b5:82a2:47fc	2603:6081:23f0:a580::1	DNS	108	Standard query 0xcfc3c AAAA v-c
63	2.855570	2603:6081:23f0:a580:349a:25b5:82a2:47fc	2603:6081:23f0:a580::1	DNS	112	Standard query 0x18b0 A dns-u9
64	2.855572	2603:6081:23f0:a580:349a:25b5:82a2:47fc	2603:6081:23f0:a580::1	DNS	102	Standard query 0x74be A cerebr
65	2.855574	2603:6081:23f0:a580:349a:25b5:82a2:47fc	2603:6081:23f0:a580::1	DNS	108	Standard query 0x9229 AAAA v-al
66	2.855600	2603:6081:23f0:a580:349a:25b5:82a2:47fc	2603:6081:23f0:a580::1	DNS	108	Standard query 0x11db A v-cm1k

Frame 13: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{D08E...}

Ethernet II, Src: IntelCor_85:cd:98 (8c:c6:81:85:cd:98), Dst: AskeyCom_31:14:92 (2c:ea:dc:31:14:92)

Internet Protocol Version 6, Src: 2603:6081:23f0:a580:349a:25b5:82a2:47fc, Dst: 2603:6081:23f0:a580:349a:25b5:82a2:47fc

0110 = Version: 6

.... 0000 0000 = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)

.... 0111 0010 0001 0101 = Flow Label: 0x72115

Payload Length: 36

Next Header: UDP (17)

Hop Limit: 64

Source Address: 2603:6081:23f0:a580:349a:25b5:82a2:47fc

Destination Address: 2603:6081:23f0:a580::1

User Datagram Protocol, Src Port: 61474, Dst Port: 53

Domain Name System (query)

0000 2c ea dc 31 14 92 8c c6 81 85 cd 98 86 dd 60 071.....
0010 21 15 00 24 11 40 26 03 60 81 23 f0 a5 80 34 9a\$&...4..
0020 25 b5 82 a2 47 fc 26 03 60 81 23 f0 a5 80 00 00G&...#....
0030 00 00 00 00 01 f0 22 00 35 00 24 c5 0e a7 49*..5\$...I
0040 01 00 00 01 00 00 00 00 00 01 73 04 79 69 6d-s-yin
0050 67 03 63 6f 6d 00 00 01 00 01g.com....

wireshark_Wi-FiWP0QB2.pcapng | Packets: 680 · Displayed: 680 (100.0%) | Profile: Default

Section 2: Questions

1. A. When filtering for port 80 with the walnutcreekamphitheatre.com website up, I got 544 packets.

Wireshark interface showing a packet capture. The top bar indicates "Apply a display filter ... <Ctrl-/>". The packet list pane shows 544 packets, with the first packet being a GET request to walnutcreekamphitheatre.com. The packet details pane shows the structure of the first packet, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data of the first packet.

No.	Time	Source	Destination	Protocol	Length	Info
218	5.229843	192.168.1.168	104.219.248.3	HTTP	691	GET / HTTP/1.1
219	5.250485	2607:f8b0:4002:c08::5b	2603:6081:23f0:a580:349a:25b5:82a2:47fc	QUIC	86	Protected Payload (KP0)
220	5.251214	2603:6081:23f0:a580:349a:25b5:82a2:47fc	2607:f8b0:4002:c2c::5e	QUIC	131	Protected Payload (KP0), DCID=e99611761
221	5.253519	2607:f8b0:4002:c03::5f	2603:6081:23f0:a580:349a:25b5:82a2:47fc	QUIC	87	Protected Payload (KP0)
222	5.276681	2607:f8b0:4002:c2c::5e	2603:6081:23f0:a580:349a:25b5:82a2:47fc	QUIC	87	Protected Payload (KP0)
223	5.358087	104.219.248.3	192.168.1.168	TCP	54	80 → 56617 [ACK] Seq=1 Ack=638 Win=1638
224	5.734376	192.168.1.16	239.255.255.250	UDP	698	52446 → 3702 Len=656
225	6.246951	2607:f8b0:4002:c11::64	2603:6081:23f0:a580:349a:25b5:82a2:47fc	UDP	99	443 → 56924 Len=37
226	6.257627	2603:6081:23f0:a580:349a:25b5:82a2:47fc	2607:f8b0:4002:c11::64	UDP	95	56924 → 443 Len=33
227	6.274916	2607:f8b0:4002:c11::64	2603:6081:23f0:a580:349a:25b5:82a2:47fc	UDP	99	443 → 56924 Len=37
228	6.275448	2603:6081:23f0:a580:349a:25b5:82a2:47fc	2607:f8b0:4002:c11::64	UDP	96	56924 → 443 Len=34
229	6.553637	fe80::e018:3d8a:4a74:b333	ff02::c	UDP	718	52447 → 3702 Len=656
230	6.759896	192.168.1.23	224.0.0.251	MDNS	782	Standard query response 0x0000 TXT, ca

Ready to load or capture | Packets: 544 · Displayed: 544 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

- B. There were only 8 packets from walnutcreekamphitheatre.com with port 80.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	104.219.248.3	192.168.1.168	TCP	66	80 → 56244 [SYN, ACK] Seq=0 Ack=1 Win=1466
2	0.202576	104.219.248.3	192.168.1.168	TCP	54	80 → 56244 [ACK] Seq=1 Ack=632 Win=15872
3	0.359246	104.219.248.3	192.168.1.168	TCP	11510	80 → 56244 [ACK] Seq=1 Ack=632 Win=15872
4	0.359246	104.219.248.3	192.168.1.168	HTTP	818	HTTP/1.1 200 OK (text/html)
5	1.004916	104.219.248.3	192.168.1.168	TCP	66	80 → 56245 [SYN, ACK] Seq=0 Ack=1 Win=1466
6	15.373017	104.219.248.3	192.168.1.168	TCP	54	80 → 56244 [FIN, ACK] Seq=12221 Ack=632 W
7	16.136776	104.219.248.3	192.168.1.168	HTTP	287	HTTP/1.1 408 Request Time-out (text/html)
8	16.136776	104.219.248.3	192.168.1.168	TCP	54	80 → 56245 [FIN, ACK] Seq=234 Ack=1 Win=3

Wireshark interface showing a live capture of 8 packets over Wi-Fi. The top bar indicates "Wi-Fi: <live capture in progress>". The packet list pane shows 8 packets, with the first packet being a SYN packet to port 80. The packet details pane shows the structure of the first packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data of the first packet.

Wi-Fi: <live capture in progress> | Packets: 8 · Displayed: 8 (100.0%) | Profile: Default

C. when filtering for DNS I got 680 packets.

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
53	2.689094	192.168.1.168	192.168.1.1	DNS	73	Standard query 0x6fe2 A udc.ya
54	2.689095	192.168.1.168	192.168.1.1	DNS	73	Standard query 0x81d7 AAAA udc
55	2.698300	2603:6081:23f0:a580::1	2603:6081:23f0:a580:349a:25b5:82a2:47fc	DNS	164	Standard query response 0x6fe2
56	2.698300	192.168.1.1	192.168.1.168	DNS	144	Standard query response 0x6fe2
57	2.719834	2603:6081:23f0:a580::1	2603:6081:23f0:a580:349a:25b5:82a2:47fc	DNS	176	Standard query response 0x81d7
58	2.719834	192.168.1.1	192.168.1.168	DNS	156	Standard query response 0x81d7
59	2.846138	2603:6081:23f0:a580:349a:25b5:82a2:47fc	2603:6081:23f0:a580::1	DNS	108	Standard query 0xf44f A v-ahoi
60	2.846190	2603:6081:23f0:a580:349a:25b5:82a2:47fc	2603:6081:23f0:a580::1	DNS	108	Standard query 0x6db2 A v-b1x9
61	2.855570	2603:6081:23f0:a580:349a:25b5:82a2:47fc	2603:6081:23f0:a580::1	DNS	108	Standard query 0x617b AAAA v-b
62	2.855570	2603:6081:23f0:a580:349a:25b5:82a2:47fc	2603:6081:23f0:a580::1	DNS	108	Standard query 0xcfc3c AAAA v-c
63	2.855570	2603:6081:23f0:a580:349a:25b5:82a2:47fc	2603:6081:23f0:a580::1	DNS	112	Standard query 0x18b0 A dns-u9
64	2.855572	2603:6081:23f0:a580:349a:25b5:82a2:47fc	2603:6081:23f0:a580::1	DNS	102	Standard query 0x74be A cerebr
65	2.855574	2603:6081:23f0:a580:349a:25b5:82a2:47fc	2603:6081:23f0:a580::1	DNS	108	Standard query 0x9229 AAAA v-a
66	2.855600	2603:6081:23f0:a580:349a:25b5:82a2:47fc	2603:6081:23f0:a580::1	DNS	108	Standard query 0x11db A v-cmk

Frame 13: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{008E...}

Ethernet II, Src: IntelCor_85:cd:98 (8c:c6:81:85:cd:98), Dst: AskeyCom_31:14:92 (2c:ea:dc:31:14:92)

Internet Protocol Version 6, Src: 2603:6081:23f0:a580:349a:25b5:82a2:47fc, Dst: 2603:6081:23f0:a580:0110::: Version: 6

0110::: = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)

Flow Label: 0x72115

Payload Length: 36

Next Header: UDP (17)

Hop Limit: 64

Source Address: 2603:6081:23f0:a580:349a:25b5:82a2:47fc

Destination Address: 2603:6081:23f0:a580::1

User Datagram Protocol, Src Port: 61474, Dst Port: 53

Domain Name System (query)

wireshark_Wi-FiWPOQB2.pcapng

Packets: 680 · Displayed: 680 (100.0%) Profile: Default

2. A. Row 218 contained the initial get request. .

No.	Time	Source	Destination	Protocol	Length	Info
218	5.229843	192.168.1.168	104.219.248.3	HTTP	691	GET / HTTP/1.1
219	5.250485	2607:f8b0:4002:c08::5b	2603:6081:23f0:a580:349a:25b5:82a2:47fc	QUIC	86	Protected Payload (KP0)
220	5.251214	2603:6081:23f0:a580:349a:25b5:82a2:47fc	2607:f8b0:4002:c2c::5e	QUIC	131	Protected Payload (KP0), DCID=e996117
221	5.253519	2607:f8b0:4002:c03::5f	2603:6081:23f0:a580:349a:25b5:82a2:47fc	QUIC	87	Protected Payload (KP0)
222	5.276681	2607:f8b0:4002:c2c::5e	2603:6081:23f0:a580:349a:25b5:82a2:47fc	QUIC	87	Protected Payload (KP0)
223	5.358087	104.219.248.3	192.168.1.168	TCP	54	80 → 56617 [ACK] Seq=1 Ack=638 Win=16
224	5.734376	192.168.1.16	239.255.255.250	UDP	698	52446 → 3702 Len=656
225	6.246951	2607:f8b0:4002:c11::64	2603:6081:23f0:a580:349a:25b5:82a2:47fc	UDP	99	443 → 56924 Len=37
226	6.257627	2603:6081:23f0:a580:349a:25b5:82a2:47fc	2607:f8b0:4002:c11::64	UDP	95	56924 → 443 Len=33
227	6.274916	2607:f8b0:4002:c11::64	2603:6081:23f0:a580:349a:25b5:82a2:47fc	UDP	99	443 → 56924 Len=37
228	6.275448	2603:6081:23f0:a580:349a:25b5:82a2:47fc	2607:f8b0:4002:c11::64	UDP	96	56924 → 443 Len=34
229	6.553637	fe80::e010:3d8a:4a74:b333	ff02::c	UDP	718	52447 → 3702 Len=656
230	6.759896	192.168.1.23	224.0.0.251	MDNS	782	Standard query response 0x0000 TXT, c

Frame 218: 691 bytes on wire (5528 bits), 691 bytes captured (5528 bits) on interface \Device\NPF_{...}

Ethernet II, Src: IntelCor_85:cd:98 (8c:c6:81:85:cd:98), Dst: AskeyCom_31:14:92 (2c:ea:dc:31:14:92)

Internet Protocol Version 4, Src: 192.168.1.168, Dst: 104.219.248.3

Transmission Control Protocol, Src Port: 56617, Dst Port: 80, Seq: 1, Ack: 1, Len: 637

Hypertext Transfer Protocol

GET / HTTP/1.1\r\n

Host: walnutcreekamphitheatre.com\r\n

Connection: keep-alive\r\n

B. My computer used port 56617.

Transmission Control Protocol, Src Port: 56617, Dst Port: 80, Seq: 1, Ack: 1, Len: 637

Hypertext Transfer Protocol

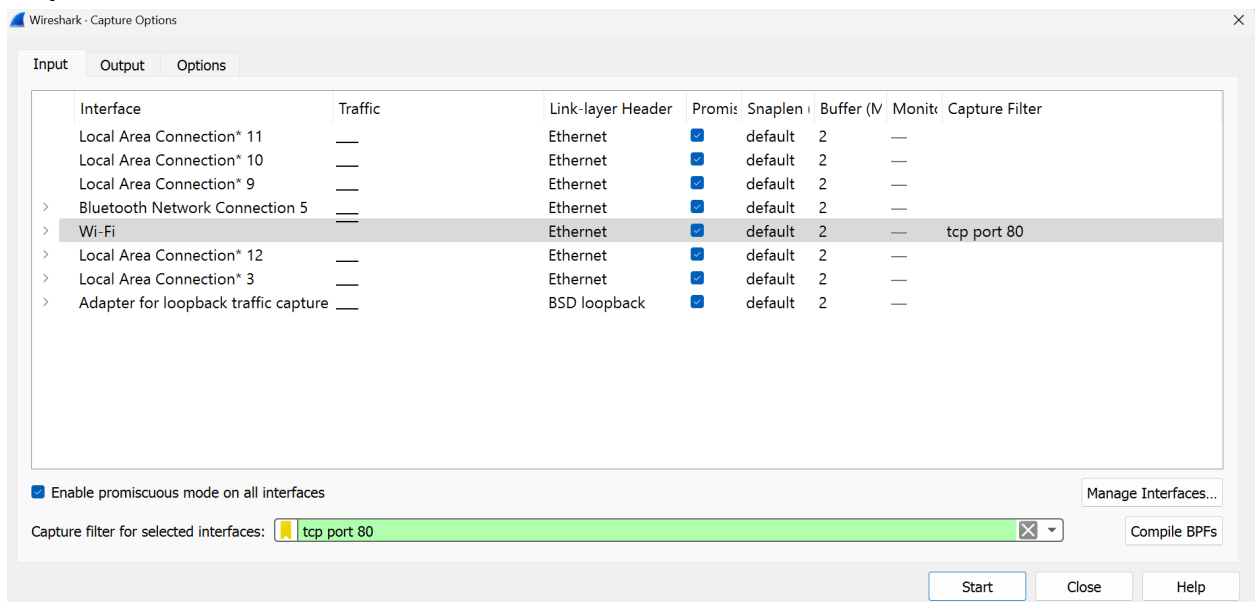
GET / HTTP/1.1\r\n

3. For this exercise, my IP address was 192.168.1.168.

4. The reason for this many HTTP packets was because, for me, this was the first time I've opened the walnut creek amphitheater website on my computer. Therefore, I needed to send multiple HTTP get requests to access this website.
5. As mentioned while going through the steps, many of these packets (when searching yahoo) were to transmit pictures and other links that may have been on the website.
6. In the first part of this section, we filtered packets based on port 80 which is very common and explains why we got so many packets. In the second part, we only filtered packets between us and the walnut creek amphitheater website with port 80 which narrowed the amount of packets down greatly. Lastly, we filtered for only DNS packets from the Yahoo search engine with port 53 which is the DNS port. The numerous links on the yahoo page explains why we got so many DNS packets.

Section 3: Packet Inspection

- **Step 4:**



Step 14:

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Packet list Narrow & Wide Case sensitive String get Find Cancel

No.	Time	Source	Destination	Protocol	Length	Info
23	16.285324	192.168.1.168	104.219.248.3	HTTP	701	GET / HTTP/1.1
24	16.229070	104.219.248.3	192.168.1.168	TCP	66	80 → 58114 [SYN, ACK] Seq=0 Ack=1 Win=
25	16.229517	192.168.1.168	104.219.248.3	TCP	54	58114 → 80 [ACK] Seq=1 Ack=1 Win=13184
26	16.325842	104.219.248.3	192.168.1.168	TCP	54	80 → 58112 [ACK] Seq=1 Ack=648 Win=163
27	16.567038	104.219.248.3	192.168.1.168	TCP	7214	80 → 58112 [ACK] Seq=1 Ack=648 Win=163
28	16.567211	192.168.1.168	104.219.248.3	TCP	54	58112 → 80 [ACK] Seq=648 Ack=7161 Win=
29	16.567680	104.219.248.3	192.168.1.168	TCP	4350	80 → 58112 [ACK] Seq=7161 Ack=648 Win=
30	16.567680	104.219.248.3	192.168.1.168	HTTP	819	HTTP/1.1 200 OK (text/html)
31	16.567845	192.168.1.168	104.219.248.3	TCP	54	58112 → 80 [ACK] Seq=648 Ack=12222 Win=
32	17.055230	192.168.1.168	104.219.248.3	TCP	54	[TCP Retransmission] 57886 → 80 [FIN, 4
33	17.056672	104.219.248.3	192.168.1.168	TCP	54	80 → 57886 [RST] Seq=1 Win=0 Len=0

> Frame 23: 701 bytes on wire (5608 bits), 701 bytes captured (5608 bits) on interface 0

> Ethernet II, Src: IntelCor_85:cd:98 (8c:c6:81:85:cd:98), Dst: AskeyCom_31:14:92

> Internet Protocol Version 4, Src: 192.168.1.168, Dst: 104.219.248.3

> Transmission Control Protocol, Src Port: 58112, Dst Port: 80, Seq: 1, Ack: 1

> Hypertext Transfer Protocol

GET / HTTP/1.1

Host: walnutcreekamphitheatre.com

Connection: keep-alive

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.81 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Accept-Encoding: gzip, deflate

Accept-Language: en-US,en;q=0.9

Cookie: __utmc=5520821; __utmz=5520821.1695331040.1.1.utmcsr=(direct)|__utmsr=

[Full request URI: http://walnutcreekamphitheatre.com/]

[HTTP request 1/1]

[Response in frame 30]

Text item (text), 16 bytes

Packets: 35 · Displayed: 35 (100.0%) · Dropped: 0 (0.0%) Profile: Default

Step 16:

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Packet list Narrow & Wide Case sensitive String get Find Cancel

No.	Time	Source	Destination	Protocol	Length	Info
23	16.285324	192.168.1.168	104.219.248.3	HTTP	701	GET / HTTP/1.1
24	16.229070	104.219.248.3	192.168.1.168	TCP	66	80 → 58114 [SYN, ACK] Seq=0 Ack=1 Win=
25	16.229517	192.168.1.168	104.219.248.3	TCP	54	58114 → 80 [ACK] Seq=1 Ack=1 Win=13184
26	16.325842	104.219.248.3	192.168.1.168	TCP	54	80 → 58112 [ACK] Seq=1 Ack=648 Win=163
27	16.567038	104.219.248.3	192.168.1.168	TCP	7214	80 → 58112 [ACK] Seq=1 Ack=648 Win=163
28	16.567211	192.168.1.168	104.219.248.3	TCP	54	58112 → 80 [ACK] Seq=648 Ack=7161 Win=
29	16.567680	104.219.248.3	192.168.1.168	TCP	4350	80 → 58112 [ACK] Seq=7161 Ack=648 Win=
30	16.567680	104.219.248.3	192.168.1.168	HTTP	819	HTTP/1.1 200 OK (text/html)
31	16.567845	192.168.1.168	104.219.248.3	TCP	54	58112 → 80 [ACK] Seq=648 Ack=12222 Win=
32	17.055230	192.168.1.168	104.219.248.3	TCP	54	[TCP Retransmission] 57886 → 80 [FIN, 4
33	17.056672	104.219.248.3	192.168.1.168	TCP	54	80 → 57886 [RST] Seq=1 Win=0 Len=0

> Frame 23: 701 bytes on wire (5608 bits), 701 bytes captured (5608 bits) on interface 0

> Ethernet II, Src: IntelCor_85:cd:98 (8c:c6:81:85:cd:98), Dst: AskeyCom_31:14:92

> Destination: AskeyCom_31:14:92 (2c:ea:dc:31:14:92)

> Source: IntelCor_85:cd:98 (8c:c6:81:85:cd:98)

Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 192.168.1.168, Dst: 104.219.248.3

> Transmission Control Protocol, Src Port: 58112, Dst Port: 80, Seq: 1, Ack: 1

> Hypertext Transfer Protocol

GET / HTTP/1.1

Host: walnutcreekamphitheatre.com

Connection: keep-alive

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.81 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Accept-Encoding: gzip, deflate

Accept-Language: en-US,en;q=0.9

Cookie: __utmc=5520821; __utmz=5520821.1695331040.1.1.utmcsr=(direct)|__utmsr=

[Full request URI: http://walnutcreekamphitheatre.com/]

[HTTP request 1/1]

[Response in frame 30]

HTTP Connection (http.connection), 24 bytes

Packets: 35 · Displayed: 35 (100.0%) · Dropped: 0 (0.0%) Profile: Default

- Step 19:

```

C:\ Command Prompt

Link-local IPv6 Address . . . . . : fe80::42b8:9057:ffc7:2026%16(Preferred)
IPv4 Address. . . . . : 192.168.1.168(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Thursday, September 21, 2023 5:11:53 PM
Lease Expires . . . . . : Saturday, September 23, 2023 1:48:49 AM
Default Gateway . . . . . : fe80::2eea:dcff:fe31:1492%16
                          192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 143443585
DHCPv6 Client DUID. . . . . : 00-01-00-01-28-D2-61-94-8C-C6-81-85-CD-98
DNS Servers . . . . . : 2603:6081:23f0:a580::1
                          192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled
Connection-specific DNS Suffix Search List :
                          lan

Ethernet adapter Bluetooth Network Connection 5:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Bluetooth Device (Personal Area Network) #5
Physical Address. . . . . : 8C-C6-81-85-CD-9C
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

C:\Users\mason>
  
```

- Step 22:

Packet list
Narrow & Wide
☐ Case sensitive
String

No.	Time	Source	Destination	Protocol	Length	Info
23	16.205324	192.168.1.168	104.219.248.3	HTTP	701	GET / HTTP/1.1
24	16.229070	104.219.248.3	192.168.1.168	TCP	66	80 → 58114 [SYN, ACK] Seq=0 Ack=1 Win=0
25	16.229517	192.168.1.168	104.219.248.3	TCP	54	58114 → 80 [ACK] Seq=1 Ack=1 Win=131840
26	16.325842	104.219.248.3	192.168.1.168	TCP	54	80 → 58112 [ACK] Seq=1 Ack=648 Win=1636
27	16.567038	104.219.248.3	192.168.1.168	TCP	7214	80 → 58112 [ACK] Seq=1 Ack=648 Win=1636
28	16.567211	192.168.1.168	104.219.248.3	TCP	54	58112 → 80 [ACK] Seq=648 Ack=7161 Win=
29	16.567680	104.219.248.3	192.168.1.168	TCP	4350	80 → 58112 [ACK] Seq=7161 Ack=648 Win=
30	16.567680	104.219.248.3	192.168.1.168	HTTP	819	HTTP/1.1 200 OK (text/html)
31	16.567845	192.168.1.168	104.219.248.3	TCP	54	58112 → 80 [ACK] Seq=648 Ack=12222 Win=
32	17.055230	192.168.1.168	104.219.248.3	TCP	54	[TCP Retransmission] 57886 → 80 [FIN, A
33	17.055672	104.219.248.3	192.168.1.168	TCP	54	80 → 57886 [RST] Seq=1 Win=0 Len=0

Transmission Control Protocol, Src Port: 58112, Dst Port: 80, Seq: 1, Ac
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Host: walnutcreekamphitheatre.com\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image
Accept-Encoding: gzip, deflate\r\n
Cookie: __utmc=5520821; __utms=5520821.1695331040.1.1.utmcsrc=(dire
Cookie pair: __utmc=5520821
Cookie pair: __utms=5520821.1695331040.1.1.utmcsrc=(direct)u
Cookie pair: __utms=5520821.1023673162.1695331040.1695335458
Cookie pair: __utmt=1
Cookie pair: __utmb=5520821.2.10.1695408311
\r\n
[Full request URI: http://walnutcreekamphitheatre.com/]
[HTTP request 1/1]
[Response in frame: 30]

0080 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 Upgrade-Insecu
0090 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 e-Request: 1.0
00a0 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c ser-Agent: Mozil
00b0 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 la/5.0 (Window
00c0 4e 54 20 31 30 2e 30 3b 20 2f 69 6e 36 34 3b 20 NT 10.0; Win64;
00d0 78 36 34 29 20 41 70 70 6c 65 57 65 62 4b 69 74 x64) AppleWebKit
00e0 2f 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 /537.36 (KHTML,
00f0 6c 69 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f like Gec ko) Chro
0100 6d 65 2f 31 31 36 2e 30 2e 30 2e 30 20 53 61 66 me/116.0 .0.0 Saf
0110 61 72 69 2f 35 33 37 2e 33 36 00 0a 41 63 63 65 ari/537. 36-Acce
0120 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 pt: text /html,ap
0130 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b plicatio n/xhtmll=
0140 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f xml,application/
0150 78 6d 6c 30 71 34 30 2e 39 2c 69 6d 61 67 65 2f xml;q=0.9,image/
0160 61 76 69 66 2c 69 6d 61 67 65 2f 77 65 62 70 2c avif,image/webp,
0170 69 6d 61 67 65 2f 61 70 6e 67 2c 2a 2f 2a 3b 71 image/ap ng,/*;jq
0180 3d 30 2e 38 2c 61 70 70 6c 69 63 61 74 69 6f 6e =0.8,application
0190 2f 73 69 6f 6e 65 64 2d 65 78 63 68 61 6e 67 65 /signed-exchange
01a0 3b 76 3d 62 33 30 71 3d 30 2e 37 0d 0a 41 63 63 ;v=b3;q= 0.7-Acc
01b0 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a ept-Encod ing: gz
01c0 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 41 63 63 ip, defl ate-Acc
01d0 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e ept-Lang uage: en
01e0 2d 55 53 2c 65 6e 3b 71 3d 30 2e 39 0d 0a 43 6f -US,en;q =0.9-Co
01f0 6f 6b 69 65 3a 20 5f 5f 75 74 6d 63 3d 35 35 32 okie; __ utmc=552
0200 30 38 32 31 3b 20 5f 5f 75 74 6d 7a 3d 35 35 32 0821; __ utms=552
0210 30 38 32 31 2e 31 36 39 35 33 33 31 30 34 30 2e 0821.169 5331040.
0220 31 2e 31 2e 75 74 6d 63 73 72 3d 28 64 69 72 65 1.1.utmc src=(dire

Request line (http.request.line), 30 bytes
Packets: 35 · Displayed: 35 (100.0%) · Dropped: 0 (0.0%)
Profile: Defau

- Step 24:

Wireshark · Follow TCP Stream (tcp.stream eq 2) · Wi-Fi (tcp port 80)

GET / HTTP/1.1
Host: walnutcreekamphitheatre.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: __utmc=5520821; __utmr=5520821.1695331040.1.1.utmcsr=(direct)|utmccn=(direct)|utmcid=(none); __utma=5520821.1023673162.1695331040.1695335450.1695408311.3; __utmt=1; __utmb=5520821.2.10.1695408311

HTTP/1.1 200 OK
date: Fri, 22 Sep 2023 19:18:01 GMT
server: Apache
x-powered-by: PHP/7.4.33
link: <http://walnutcreekamphitheatre.com/wp-json/>; rel="https://api.w.org/", <http://walnutcreekamphitheatre.com/wp-json/wp/v2/pages/38>; rel="alternate"; type="application/json", <http://walnutcreekamphitheatre.com/>; rel=shortlink
vary: Accept-Encoding
content-encoding: gzip
content-length: 11777
content-type: text/html; charset=UTF-8

.....v.8.s.....i.....e9r.q.n.\$qv.L.\$..! E.y.v.....t....x.L.....L.E..B.P(.@....'g.;b.x...m...Z..3`n,.....a..E=.;\$=(<...
e.....o.LgY...2...<>>.../.\...fK.m...\$1.O...' b..h.N...8....aO.^.....l\$.MX..E.ADqP..%.EO;.Xxq.l..
p.[O..e\G.{...0.q....ZGcuB....X...GL?...&...z..p.Q...9...;..E.wE.a.:K"...;C.TD.B...G.....%.' k.mc...w.H....I..c'v../.....B[e..`..P.8....A...B.....y
...].[...co..c.@.)..{.....8b...D..Ce.IT..Hh..y...Q.s..~.....c~Ys.|(jA(P)..CQR...N.....H,b.....P...`..z"d.6'.c.._8..}9..
..b.....:7..w...9l..].X7..&eI3.YV...._Y(..fq...Po..B1.i.....l.j.b..6.KZw(.B<..B..u.... .Ve.(...C...=?r@..k.Z.....=.`.z.....w...D.Q.y
...z.H...e.)i.\$.....F.O.Ou b..P...C...G.F"...#e.....b.ql../.....~V....jcDt..1Tw...C..D..\...&6\$-....E..A.]...cK..O...
Sw.A..1..\$tWg.....W.\$..r....YW..lY%...X.S....d"...^_`e..9.....l..rA.."....6.....l....G..5.F..h..[g.V...6w~0..ij....~..@....
..5v..N...@....."Y...4=*...~|.....p.N...P...v. 5.L...(.k7.LWE..CE)2...].lc.0"r.tC....a..p9.....b...!-...+.....:p9..~;.....mM.,U....8L>..~.e
.....q>8v.a.z.J..H|..T.....Our.O@3...T.S..6L..T.i^4Iq..n.....n.. a..#.....OBK.....b+k.\$9..&6...Q.a.A..
..1v<.K..B.=...it..c...'.{WX...0..6.....?.....~y..5.{A..G}.. ,...{...2_t..3".Wq8..w.w.%.....?G]A.j.Cm..OL.K@\5....A.z...(4....D
..w..Q...OO..Q.B.:i%.V.Ad...}_g..
..@..@J:s.T..s..u.CE\...{-^.....

1 client pkt, 3 server pkts, 1 turn.

Entire conversation (12 kB) Show data as ASCII Stream 2

Find: Find Next

- **Step 34:**

The image shows a Wireshark packet capture analysis of a TCP segment. The packet list on the left shows a packet of 83 bytes. The packet details pane on the right shows the structure of the TCP segment, including the header and options. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
1000	0.000000	192.168.1.1	192.168.1.2	TCP	83	83 bytes [RST] Seq=1000000000, Win=0, Len=0

Packet Details:

- Ethernet II, Src: Intel (08:00:00:00:00:00), Dst: Intel (08:00:00:00:00:00)**
- TCP, Seq: 1000000000, Win: 0, Len: 0**
- Flags: 0x012 (SYN, ACK)**
- Window: 14600**
- [Calculated window size: 14600]**
- Checksum: 0x27b4 [unverified]**
- [Checksum Status: Unverified]**
- Urgent Pointer: 0**
- Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No-Operation (NOP), Window scale**
- [Timestamps]**
- [SEQ/ACK analysis]**
 - [This is an ACK to the segment in frame: 16]**
 - [The RTT to ACK the segment was: 0.080799000 seconds]**
 - [iRTT: 0.081175000 seconds]**

Packet Bytes:

```

0000  8c c6 81 85 cd 98 2c ea  dc 31 14 92 08 00 45 00  .....1....E.
0010  00 34 16 dd 40 00 30 06  10 b8 68 db f8 03 c0 a8  -4...@...h....
0020  01 a8 00 50 e3 00 02 ze  d7 e6 7d 9d b0 38 80 12  ...P....:..8..
0030  39 08 27 b4 00 00 02 04  05 8c 01 01 04 02 01 03  9.....
0040  03 09
  
```

Packet Info:

an acknowledgement to the prior GET request (1000000000) · Protocol Version 4 (ip), 20 bytes · Packets: 35 · Displayed: 35 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

- **Step 39:**

Wireshark · Packet 21 · Wi-Fi (tcp port 80)

```
> 0101 .... = Header Length: 20 bytes (5)
> Flags: 0x010 (ACK)
Window: 515
[Calculated window size: 131840]
[Window size scaling factor: 256]
Checksum: 0x234a [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> [Timestamps]
✓ [SEQ/ACK analysis]
  [This is an ACK to the segment in frame: 19]
  [The RTT to ACK the segment was: 0.000376000 seconds]
  [iRTT: 0.081175000 seconds]
```

```
0000 2c ea dc 31 14 92 8c c6 81 85 cd 98 08 00 45 00 ,.-1....-...E-
0010 00 28 6f 7b 40 00 80 06 00 00 c0 a8 01 a8 68 db -(o[@:---...h-
0020 f8 03 e3 00 00 50 7d 9d b0 38 02 2e d7 e7 50 10 ---P)-.8...P-
0030 02 03 23 4a 00 00                ..#3..
```

☒ Show packet bytes

Close

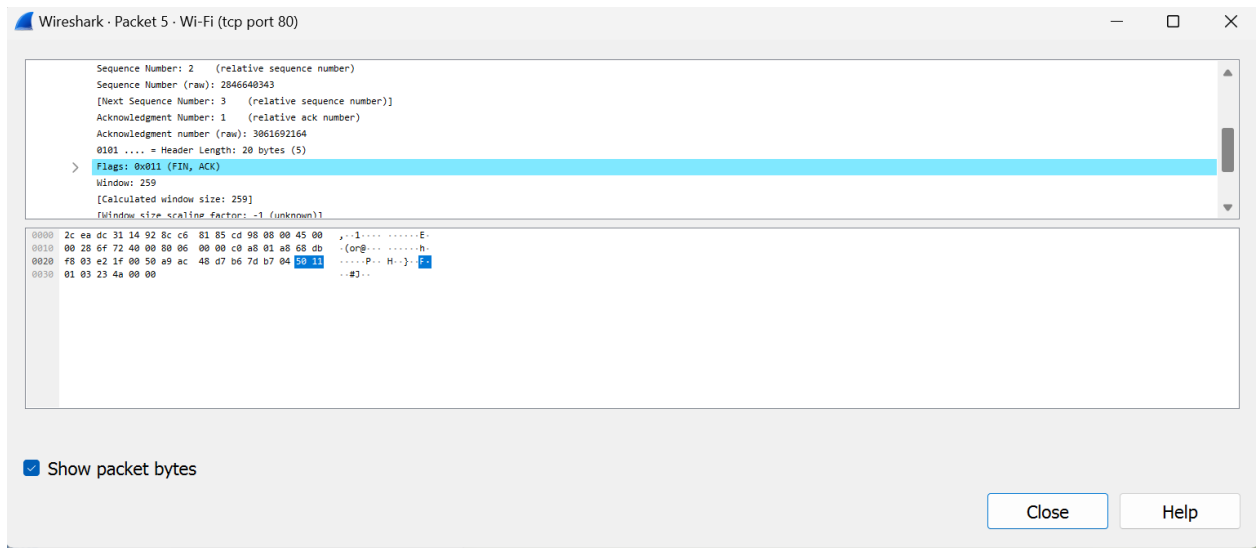
- Step 40:

The image shows a Wireshark packet capture window titled "Wireshark - Packet 26 - Wi-Fi (tcp port 80)". The packet list on the left shows 35 packets. Packet 23 is highlighted in green. The packet details pane on the right shows the "SEQ/ACK analysis" section expanded, with the text "[This is an ACK to the segment in frame: 23]" highlighted in blue. Below this, it says "[The RTT to ACK the segment was: 0.120518000 seconds]" and "[iRTT: 0.081175000 seconds]". The packet bytes pane at the bottom shows the raw data of the packet.

- Step 44:

The image shows a Wireshark packet capture window titled "Wireshark - Packet 26 - Wi-Fi (tcp port 80)". The packet list on the left shows 35 packets. Packet 23 is highlighted in green. The packet details pane on the right shows the "SEQ/ACK analysis" section expanded, with the text "[This is an ACK to the segment in frame: 23]" highlighted in blue. Below this, it says "[The RTT to ACK the segment was: 0.120518000 seconds]" and "[iRTT: 0.081175000 seconds]". The packet bytes pane at the bottom shows the raw data of the packet.

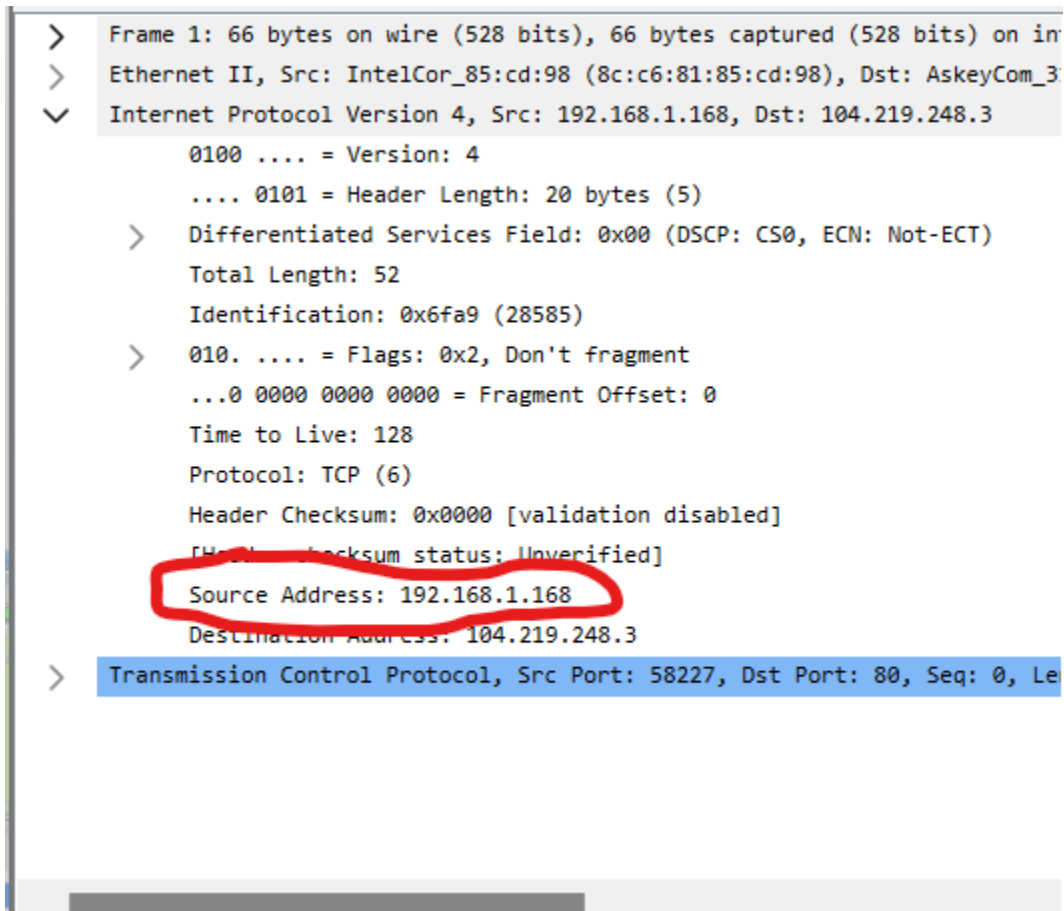
- **Step 48:**



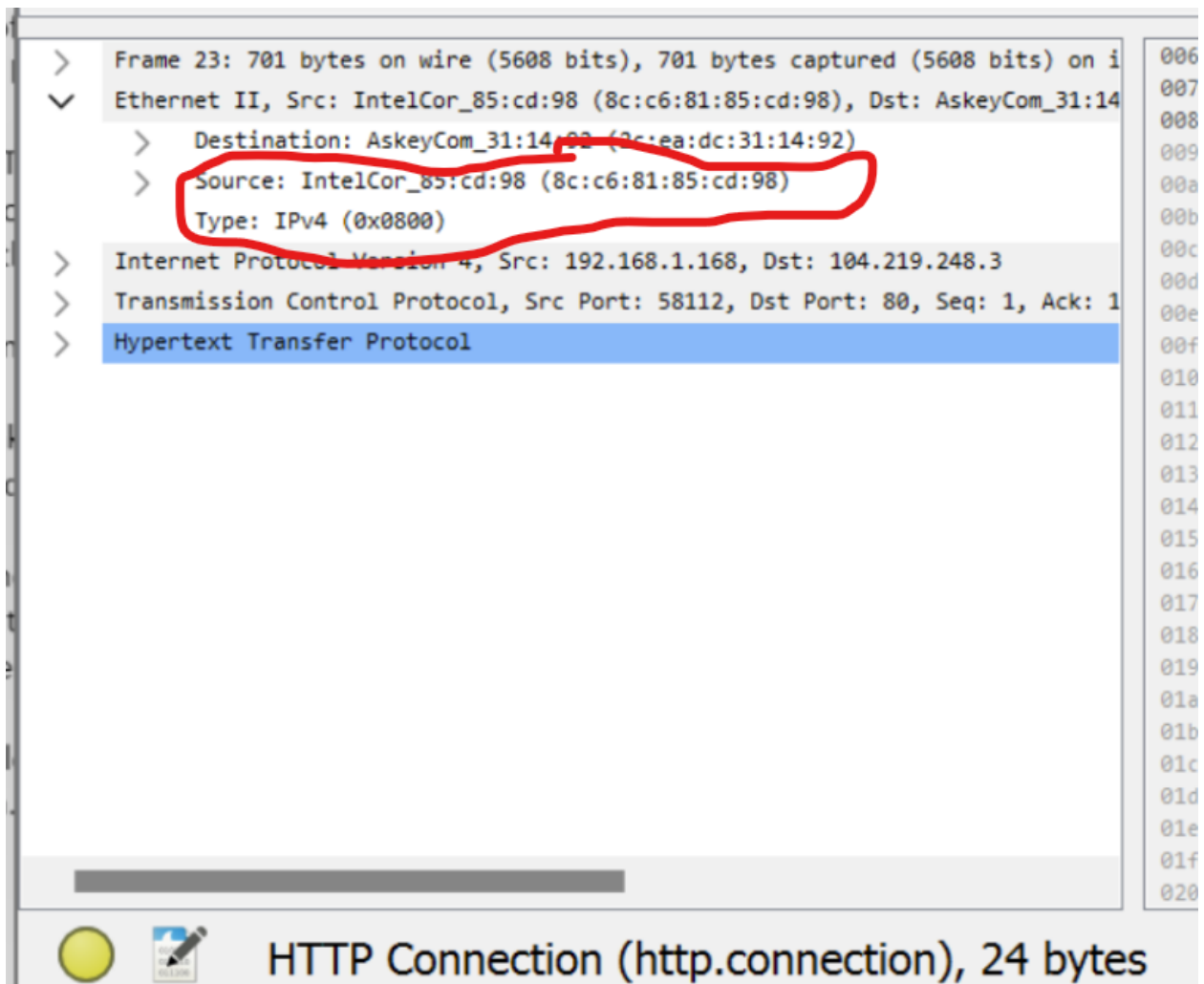
- **Step 51: There was no [SEQ,ACK] analysis option for me on this step.**

Section 3: Questions

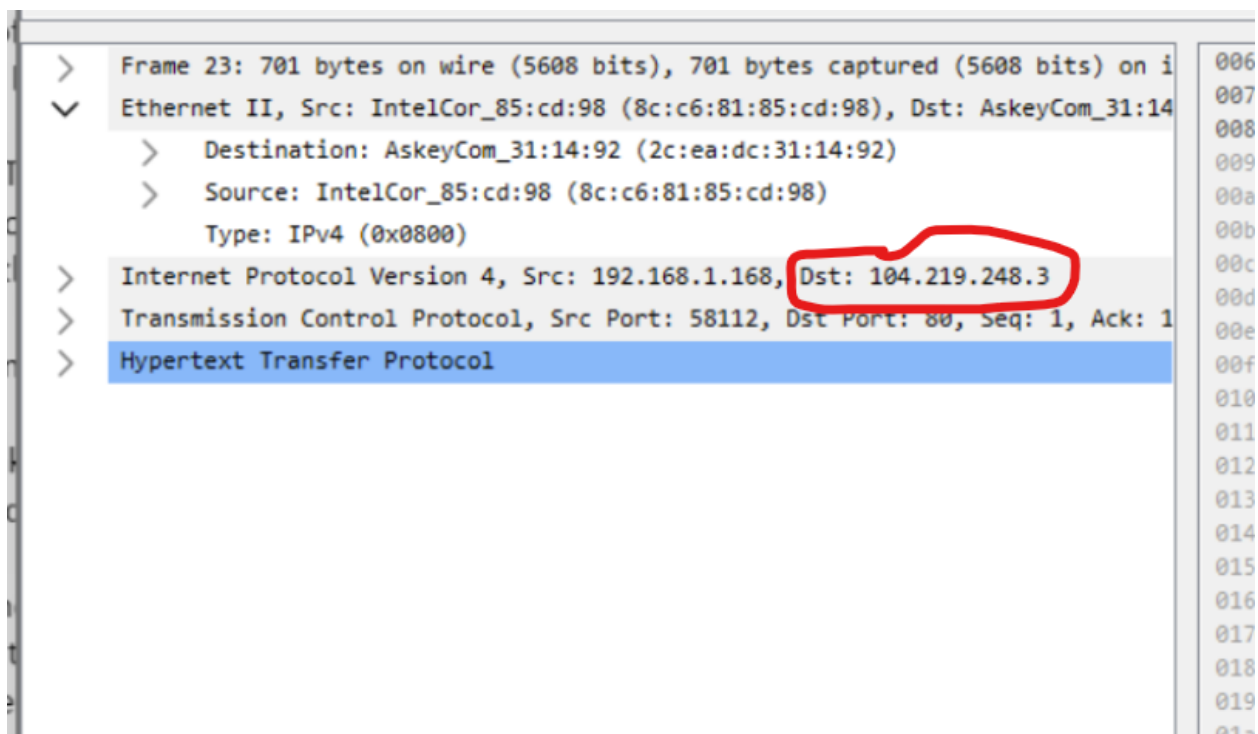
1. My IP address during this part was 192.168.1.168.



2. My physical address for this part was 8c:c6:81:85:cd:98.



3. The IP address for the walnut creek amphitheater website is 104.219.248.3.



- Step 4:

dhcp							
No.	Time	Source	Destination	Protocol	Length	Info	
470	16.814389	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request	- Transaction ID 0xe1577111
749	48.264496	192.168.1.168	192.168.1.1	DHCP	342	DHCP Release	- Transaction ID 0x8c297797
919	56.851514	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover	- Transaction ID 0xa9a811e9
953	57.290066	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover	- Transaction ID 0xe2277c5
995	58.593443	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request	- Transaction ID 0xe1577113
1048	60.433843	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request	- Transaction ID 0xe1577113
1050	60.675179	192.168.1.1	192.168.1.168	DHCP	342	DHCP Offer	- Transaction ID 0xa9a811e9
1051	60.675179	192.168.1.1	192.168.1.168	DHCP	342	DHCP Offer	- Transaction ID 0xe2277c5
1052	60.677565	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request	- Transaction ID 0xe2277c5
1053	60.680678	192.168.1.1	192.168.1.168	DHCP	363	DHCP ACK	- Transaction ID 0xe2277c5

> Frame 470: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)	0000 ff ff ff ff ff ff 86 7f 26 f5 ac 5c 08 00 45 00&..E..
> Ethernet II, Src: 86:f7:26:f5:ac:5c (86:f7:26:f5:ac:5c), Dst: Broadcast	0010 01 48 c6 30 00 00 ff 11 f4 74 00 00 00 00 ff ff	..H.0....t....
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255	0020 ff ff 00 44 00 43 01 34 61 17 01 01 06 00 e1 57	...D.C.4 a.....W
> User Datagram Protocol, Src Port: 68, Dst Port: 67	0030 71 11 00 00 00 00 00 00 00 00 00 00 00 00 00	q.....&..
> Dynamic Host Configuration Protocol (Request)	0040 00 00 00 00 00 00 00 26 f5 ac 5c 00 00 00 00&..
	0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	0110 00 00 00 00 00 63 82 53 63 35 01 03 37 09 01c 5c5-7...
	0120 79 03 06 0f 6c 72 77 fc 39 02 05 dc 3d 07 01 86	y...lhw: 9.....
	0130 7f 26 f5 ac 5c 32 04 c0 a8 01 16 33 04 00 76 a7	&..2...-3...v..
	0140 00 ff 00 00 00 00 00 00 00 00 00 00 00 00 00
	0150 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Section 4: Questions

1. Frame 470 carried the DHCP request.

470	16.814389	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request	- Transaction ID 0xe1577111
749	48.264496	192.168.1.168	192.168.1.1	DHCP	342	DHCP Release	- Transaction ID 0x8c297797
919	56.851514	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover	- Transaction ID 0xa9a811e9
953	57.290066	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover	- Transaction ID 0xe2277c5
995	58.593443	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request	- Transaction ID 0xe1577113
1048	60.433843	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request	- Transaction ID 0xe1577113
1050	60.675179	192.168.1.1	192.168.1.168	DHCP	342	DHCP Offer	- Transaction ID 0xa9a811e9
1051	60.675179	192.168.1.1	192.168.1.168	DHCP	342	DHCP Offer	- Transaction ID 0xe2277c5
1052	60.677565	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request	- Transaction ID 0xe2277c5
1053	60.680678	192.168.1.1	192.168.1.168	DHCP	363	DHCP ACK	- Transaction ID 0xe2277c5

2. After doing the ipconfig/ renewl was given the 192.168.1.168 IP address again since my IP address is private.

Wireless LAN adapter Wi-Fi:

```

Connection-specific DNS Suffix  . : lan
IPv6 Address. . . . . : 2603:6081:23f0:a580:1aaa
IPv6 Address. . . . . : 2603:6081:23f0:a580:d858:64b7:a873:9b54
Temporary IPv6 Address. . . . . : 2603:6081:23f0:a580:349a:25b5:82a2:47fc
Link-local IPv6 Address . . . . . : fe80::42b8:9057:ffc7:2026%16
IPv4 Address. . . . . : 192.168.1.168
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::2eea:dcff:fe31:1492%16
                             192.168.1.1

```

C:\Users\mason>

3. The reason we see the IP address 0.0.0.0 is because this is the default gateway. Considering I had no IP address during the time of the ipconfig/ release I had no IP address and had to go through the gateway one.

Section 5:

1. For this assignment, my computer is using Windows 11.
2. For section 1, I was located on campus in Nelson hall. For all other sections, I was located in my off-campus house.
3. My home ISP is Spectrum.