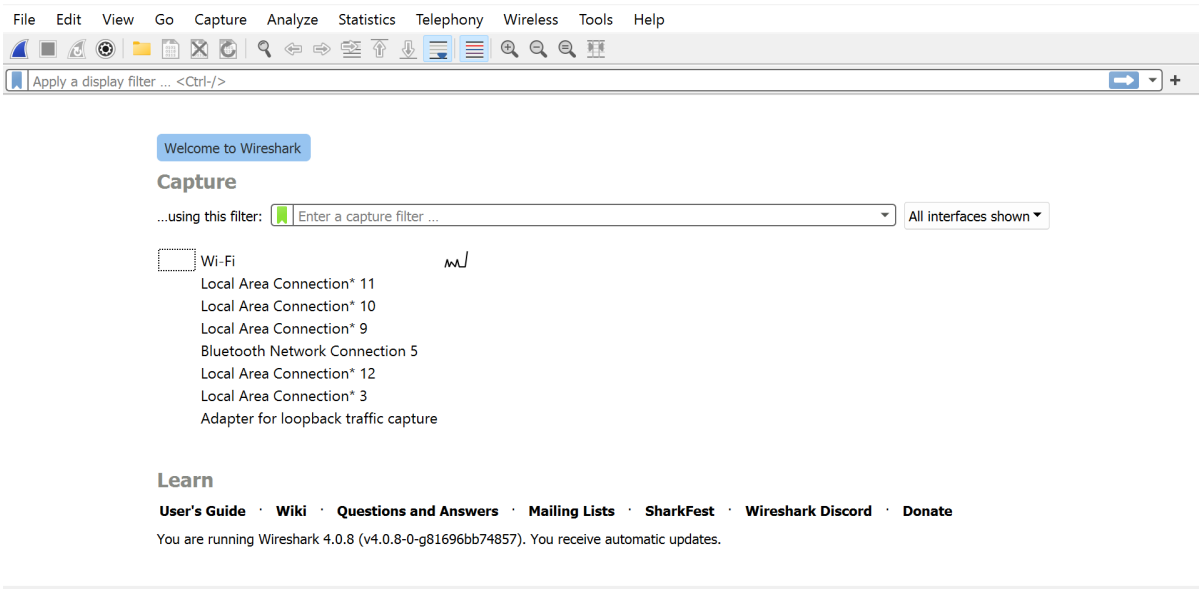
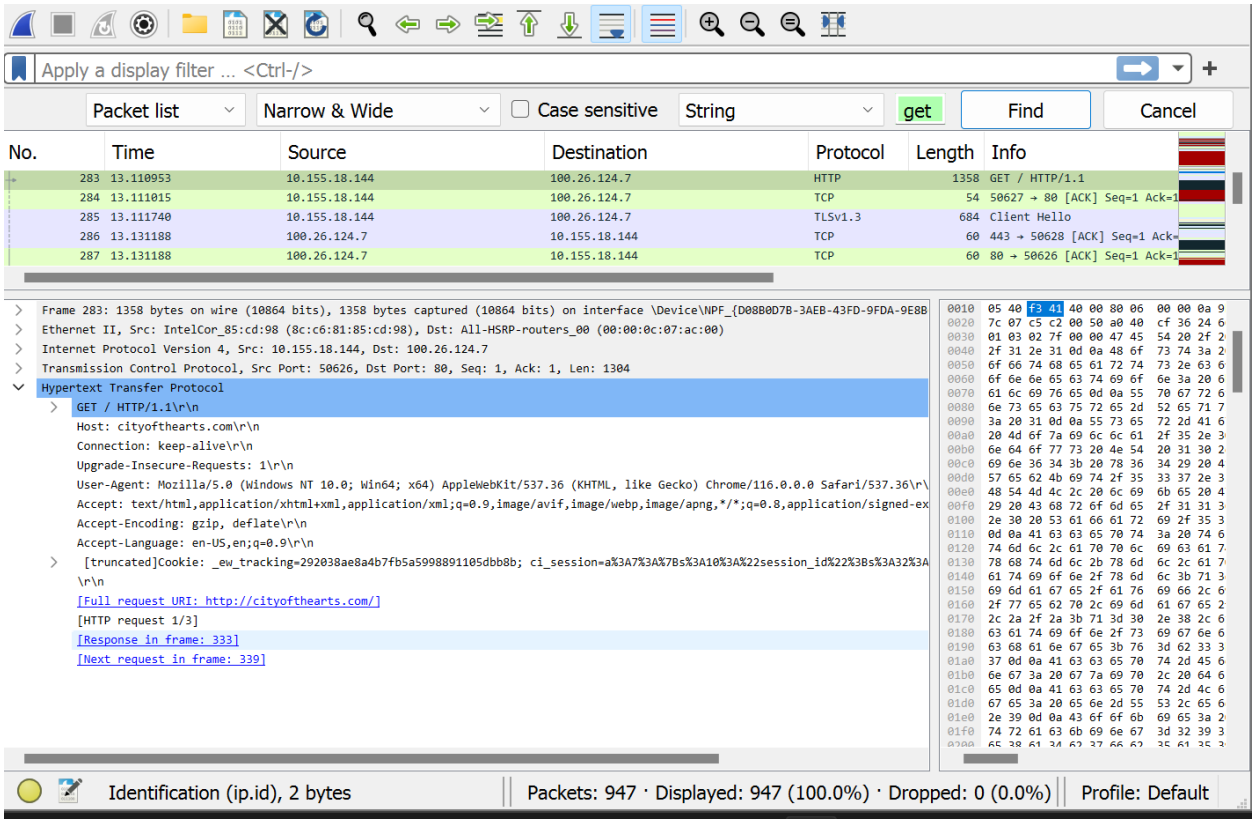
Section 1: Packet Capture (wireshark)

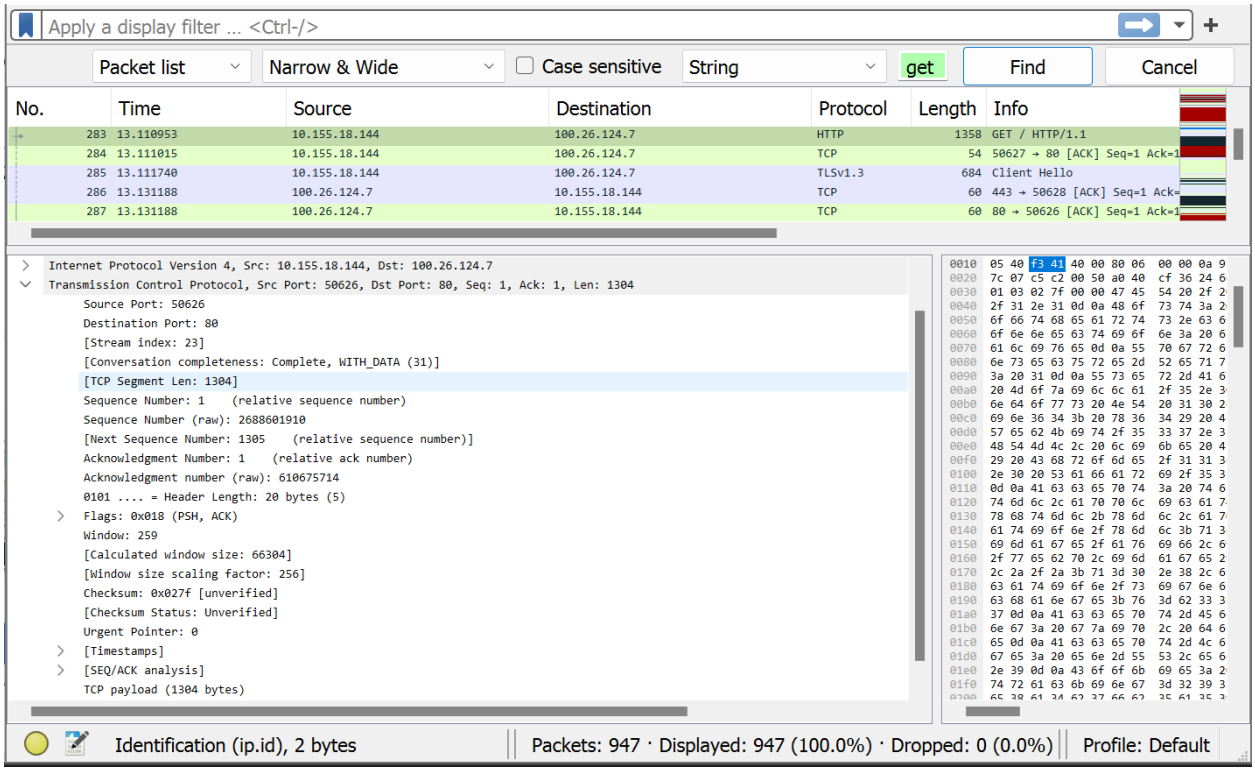
- **Step 7:**



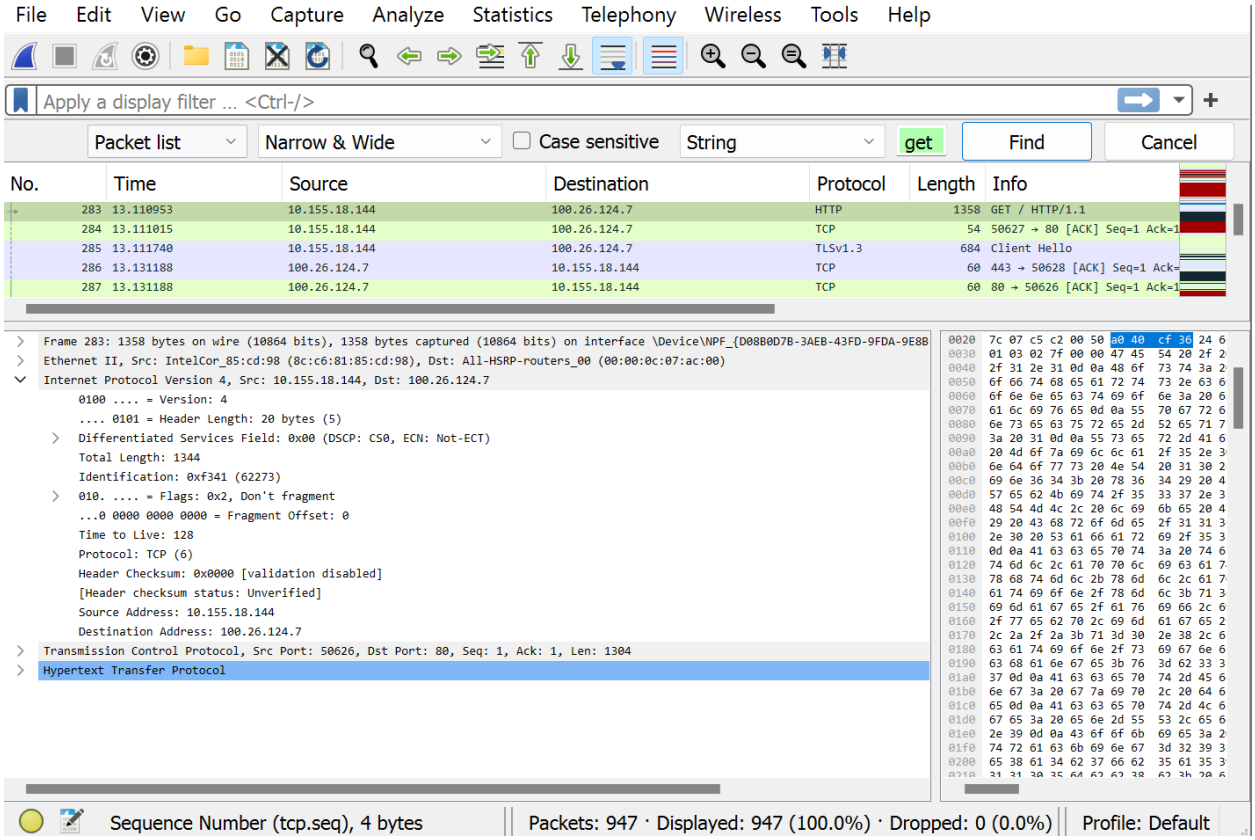
- **Step 14:**



- **Step 15:**

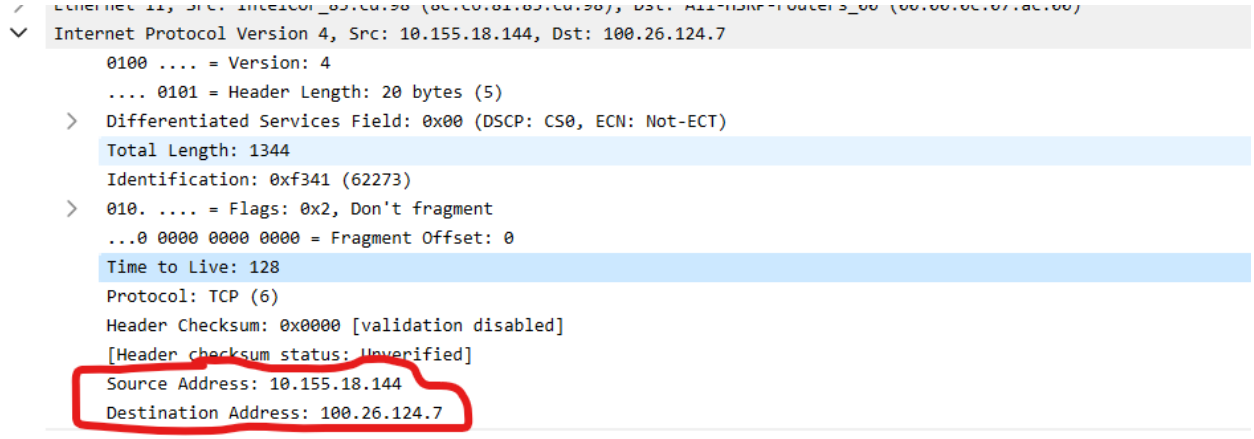


- **Step 16:**

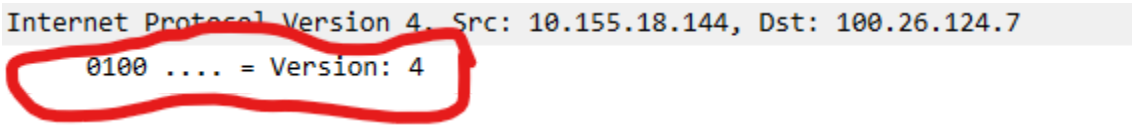


Section 1: Questions

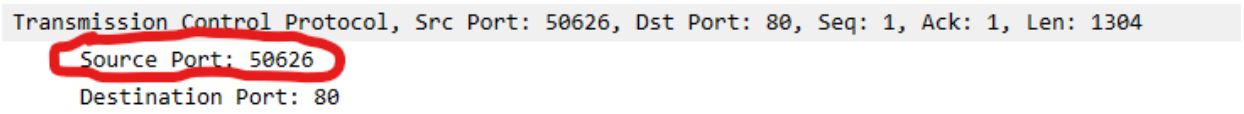
1. **A.** My IP address is 10.155.18.144 the destination IP (cityofhearts.com) address is 100.26.124.7



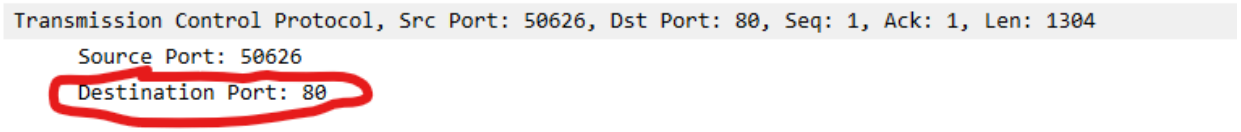
B. I am using HTTP version 4.



C. My computer's port number is 50626



D. The destination server port number is 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.

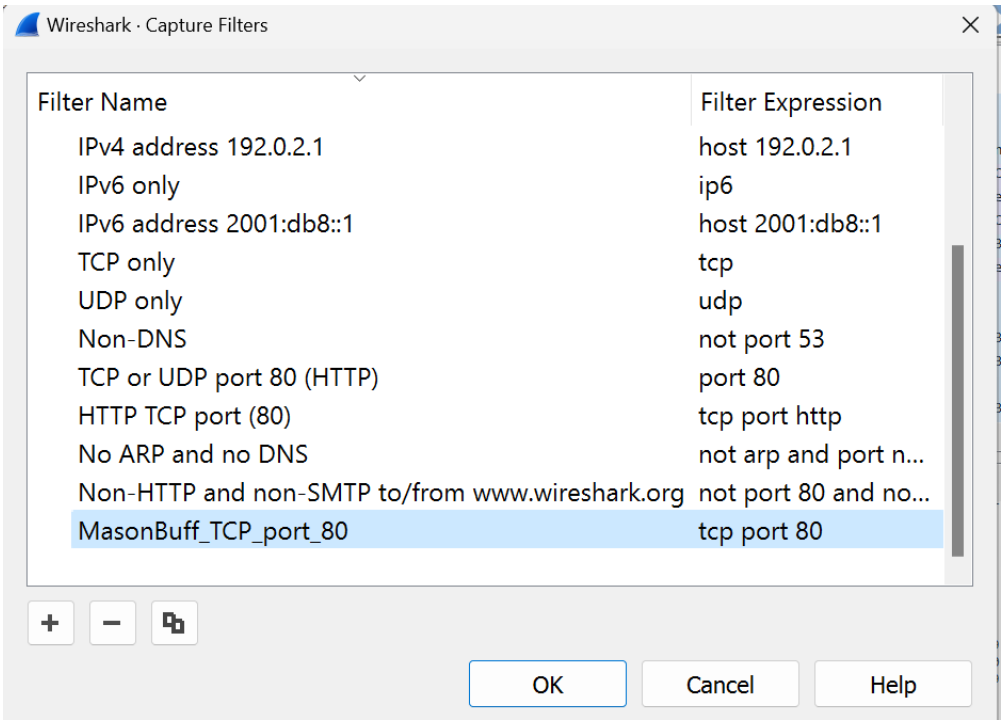
No.	Time	Source	Destination	Protocol	Length	Info
944	24.435621	172.253.122.139	10.155.18.144	UDP	68	443 → 51283 Len=26
945	24.664270	10.155.18.144	172.253.122.139	UDP	71	51283 → 443 Len=29
946	24.703388	172.253.122.139	10.155.18.144	UDP	68	443 → 51283 Len=26
947	24.912309	10.155.18.144	10.155.57.208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

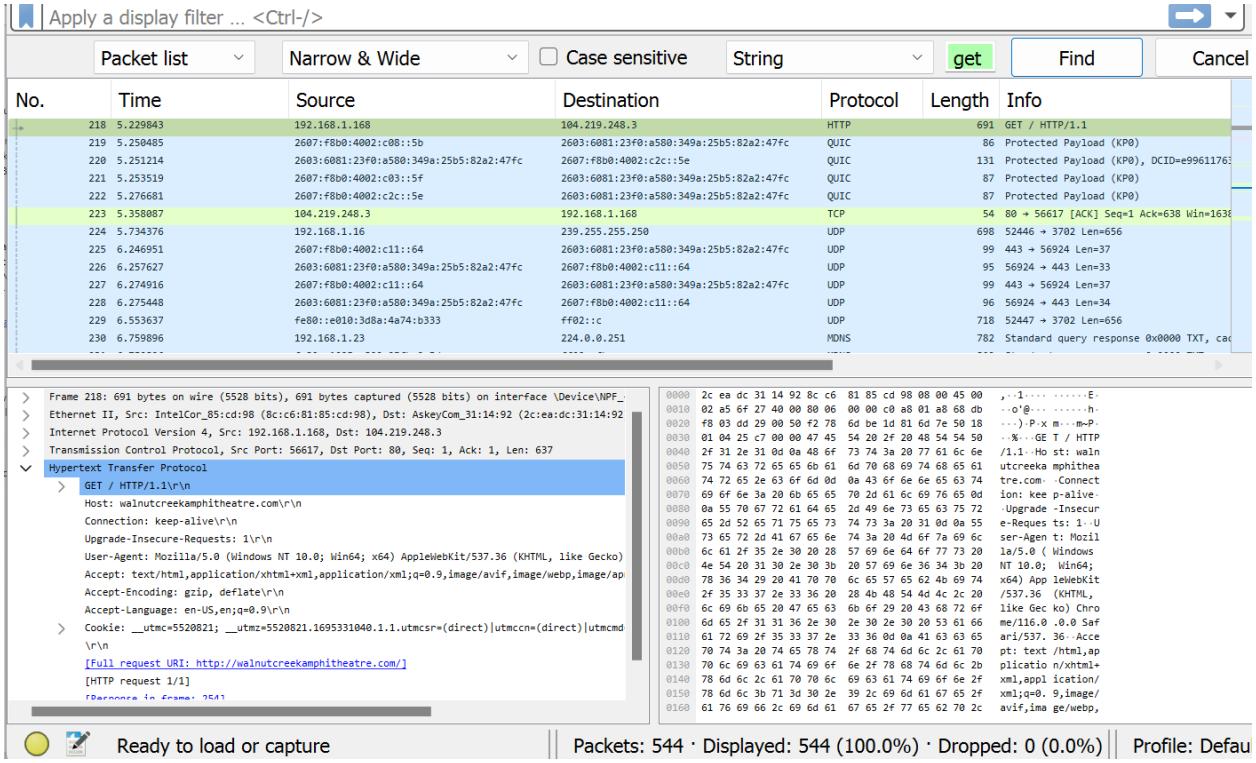
D. ARP uses yellow
E. TCP RST uses red

Section 2: Capturing Web Traffic

- **Step 4:**

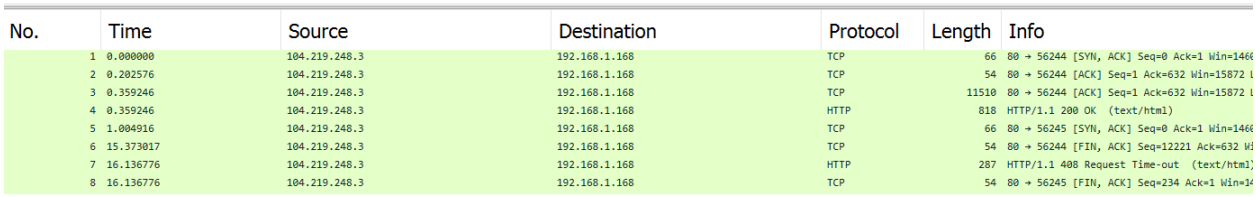


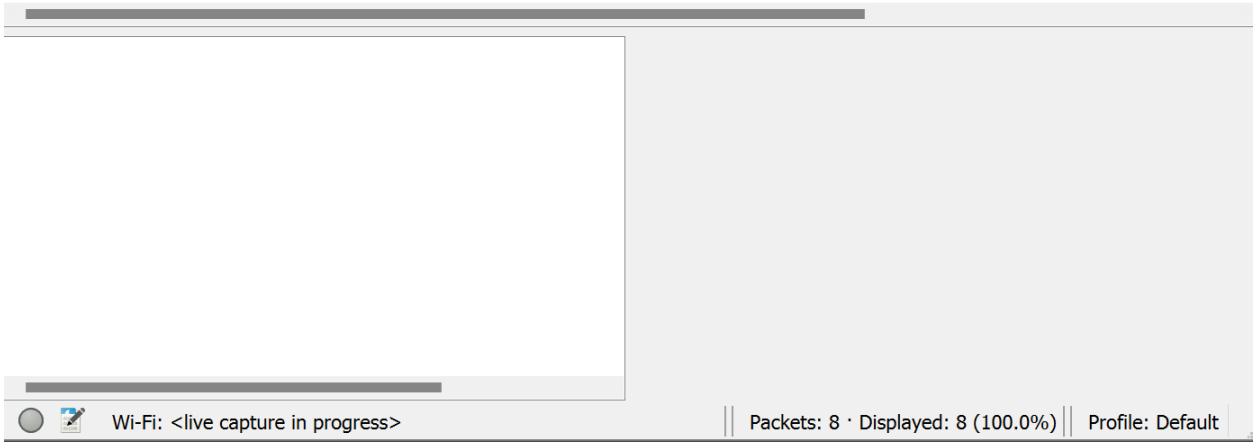
- **Step 14:**



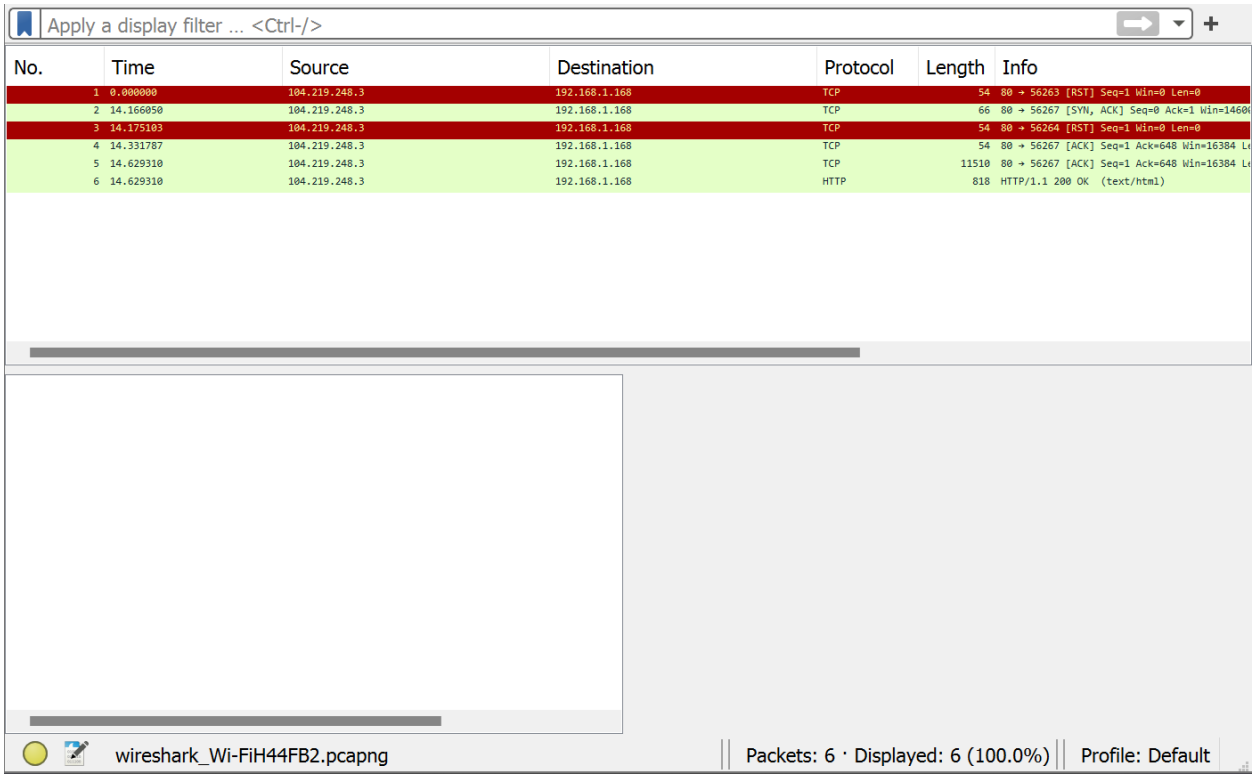
- **Step 15:** There were 544 packets captured.

- **Step 20:** 8 packets captured here.

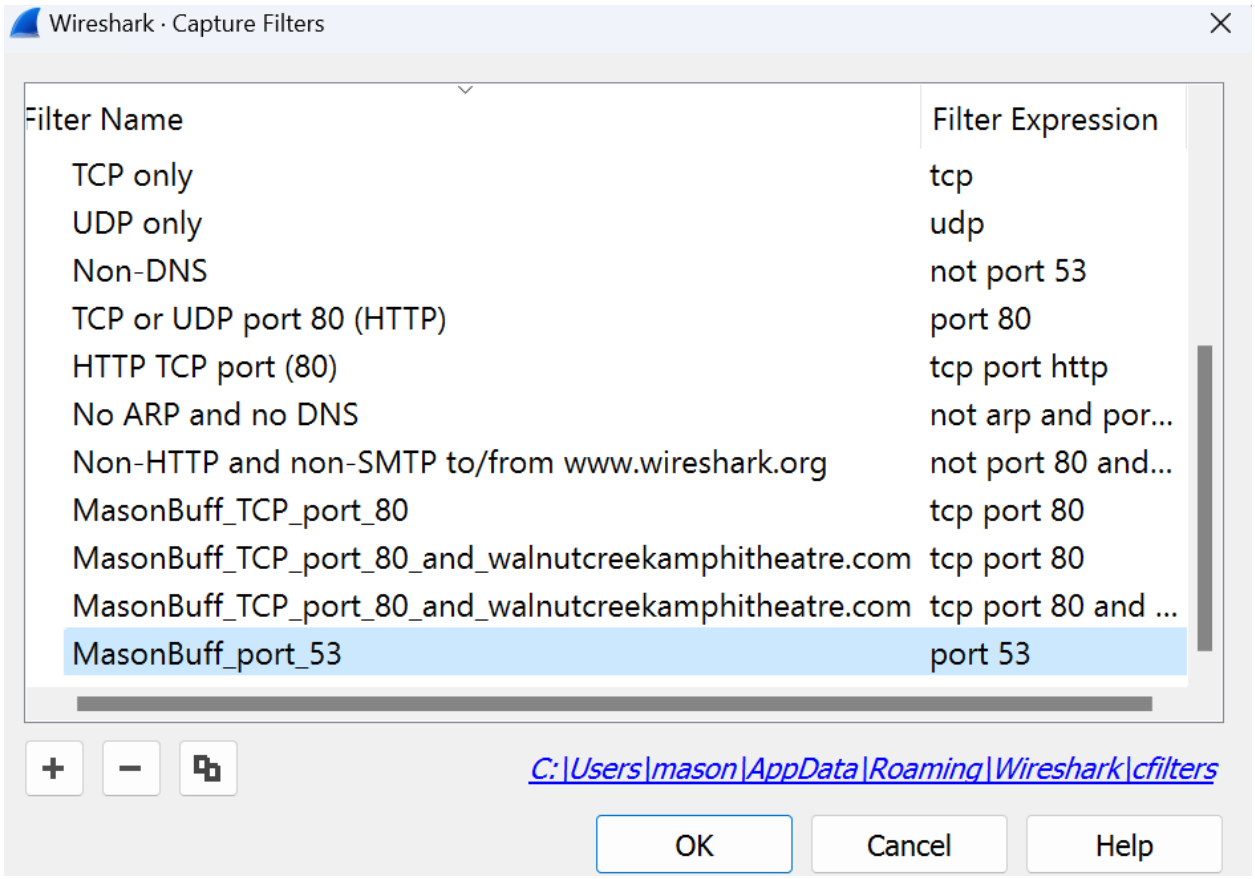




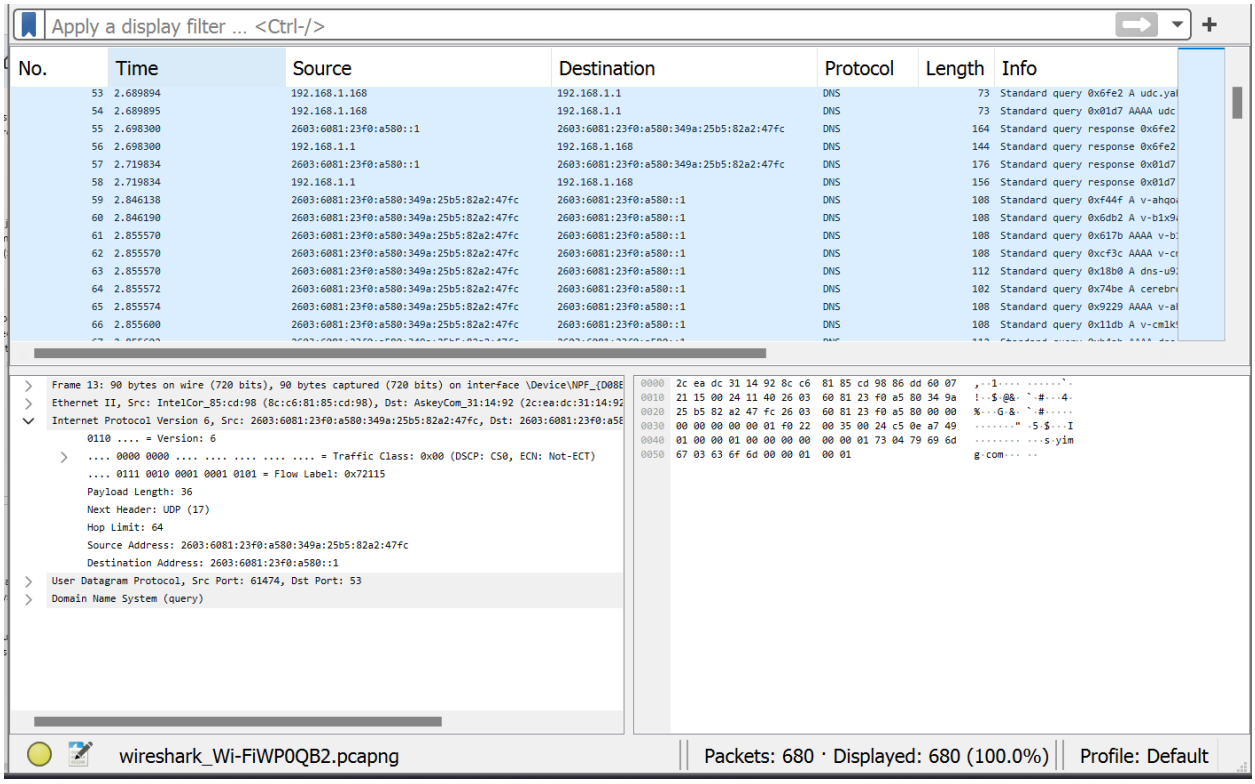
- **Step 30:** 6 captured packets this time.


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 14.166050 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 L
5 14.629310 104.219.248.3 192.168.1.168 TCP 11510 80 → 56267 [ACK] Seq=1 Ack=648 Win=16384 L
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:**

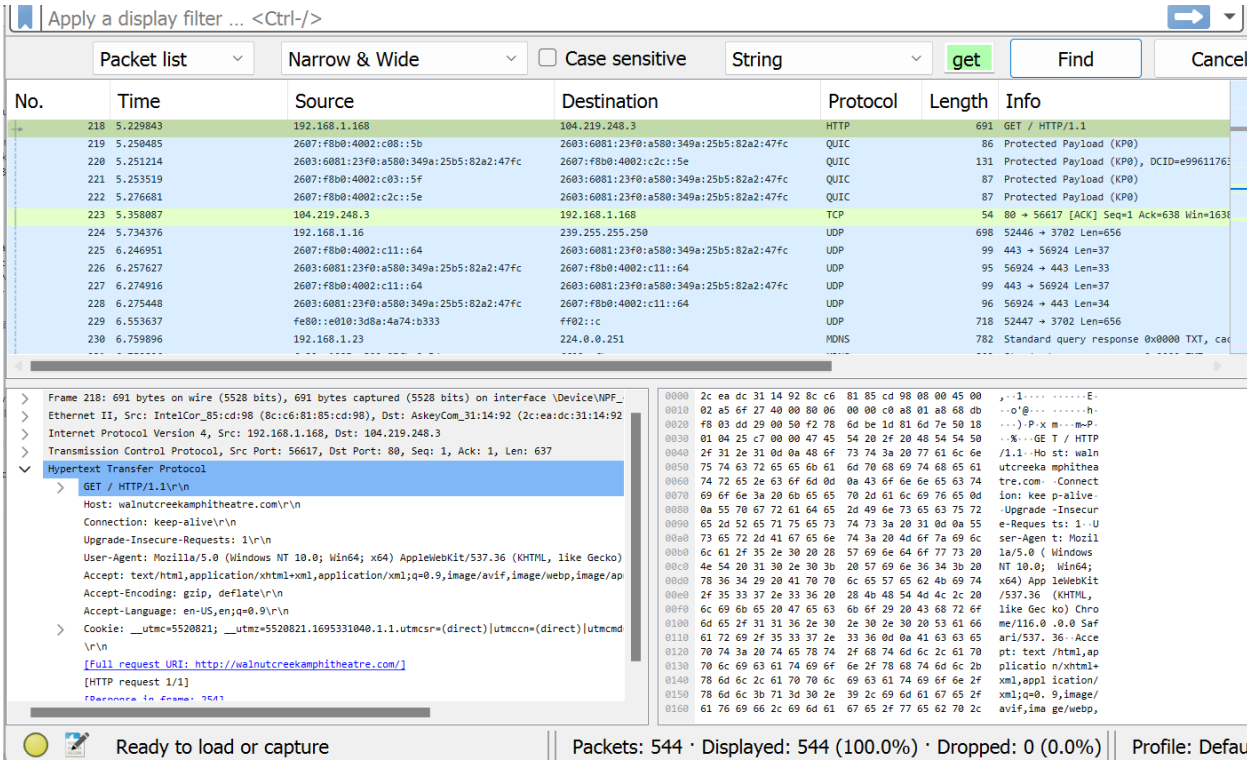

Wireshark · Capture Filters
Filter Name
Filter Expression
TCP only
tcp
UDP only
udp
Non-DNS
not port 53
TCP or UDP port 80 (HTTP)
port 80
HTTP TCP port (80)
tcp port http
No ARP and no DNS
not arp and por...
Non-HTTP and non-SMTP to/from www.wireshark.org
not port 80 and...
MasonBuff_TCP_port_80
tcp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

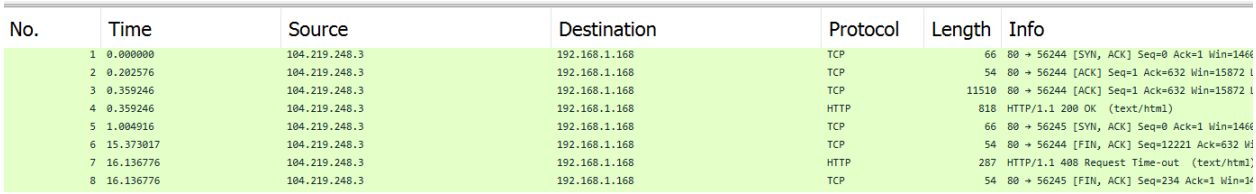


Section 2: Questions

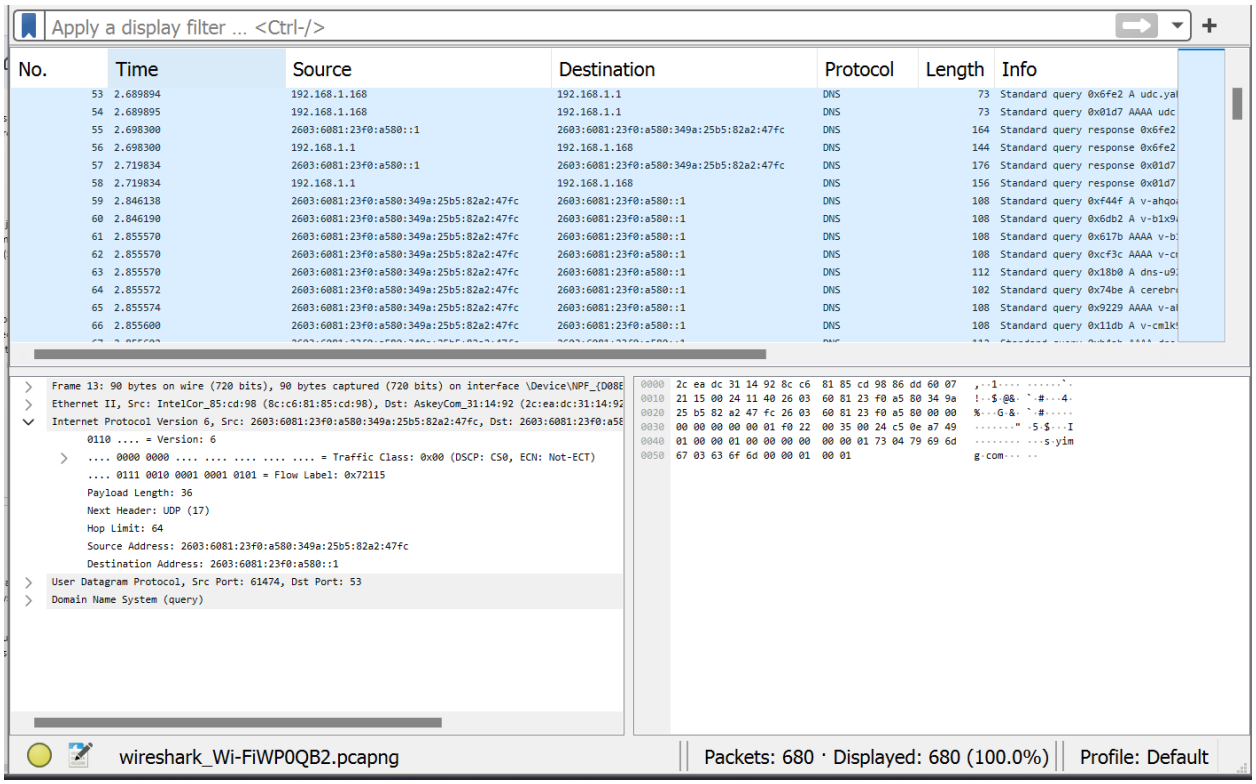
1. **A.** When filtering for port 80 with the walnutcreekamphitheatre.com website up, I got 544 packets.



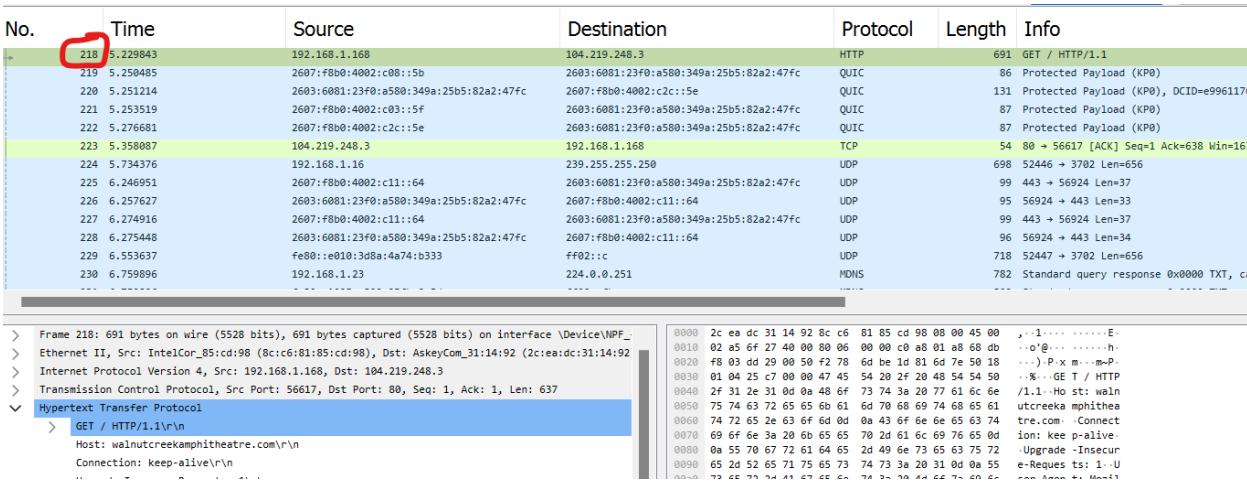
B. There were only 8 packets from walnutcreekampitheater.com with port 80.



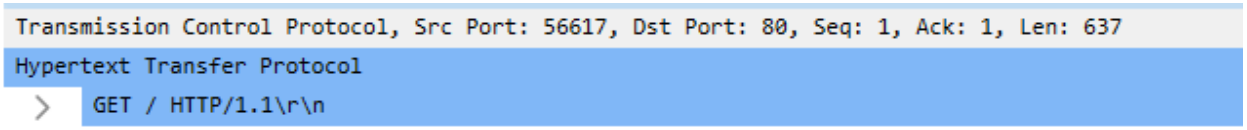
C. when filtering for DNS I got 680 packets.



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



B. My computer used port 56617.

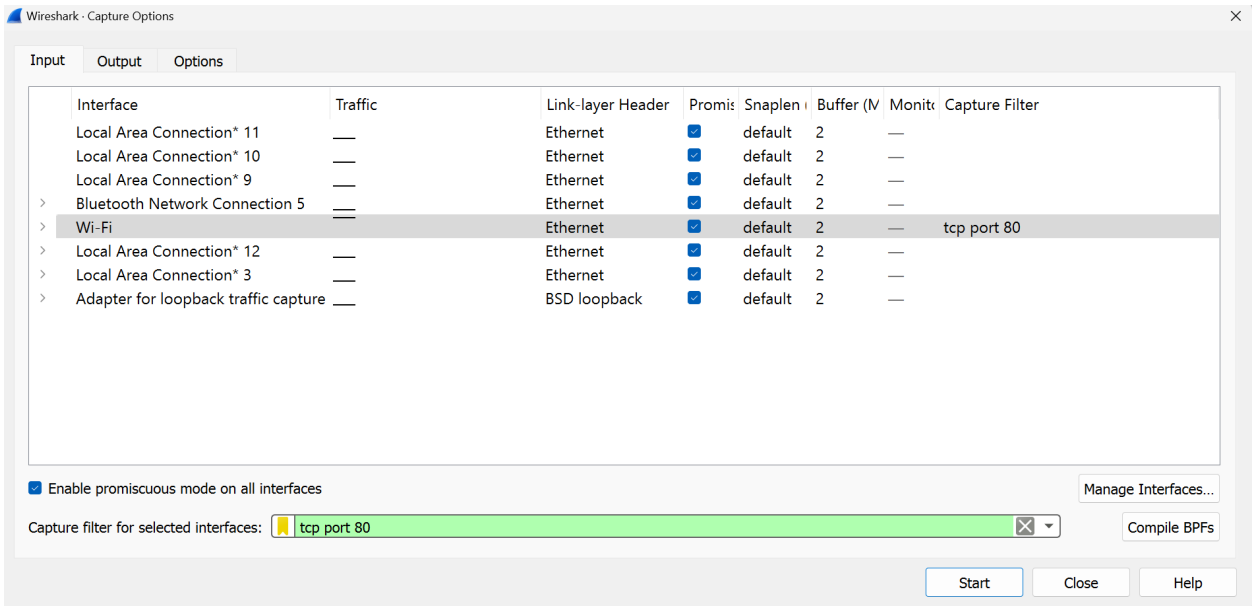


3. For this exercise, my IP address was 192.168.1.168.

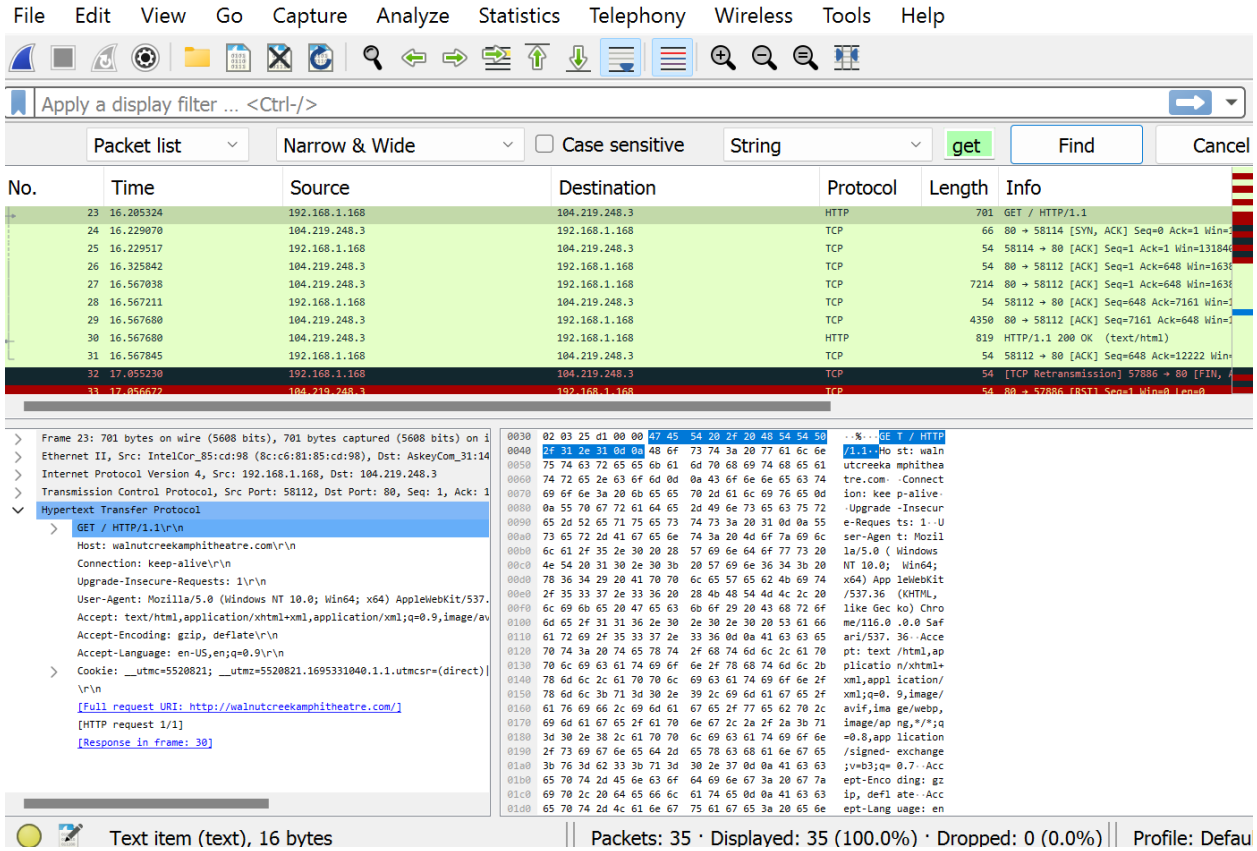
4. The reason for this many HTTP packets was because, for me, this was the first time I've opened the walnut creek amphitheater website on my computer. Therefore, I needed to send multiple HTTP get requests to access this website.
5. As mentioned while going through the steps, many of these packets (when 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

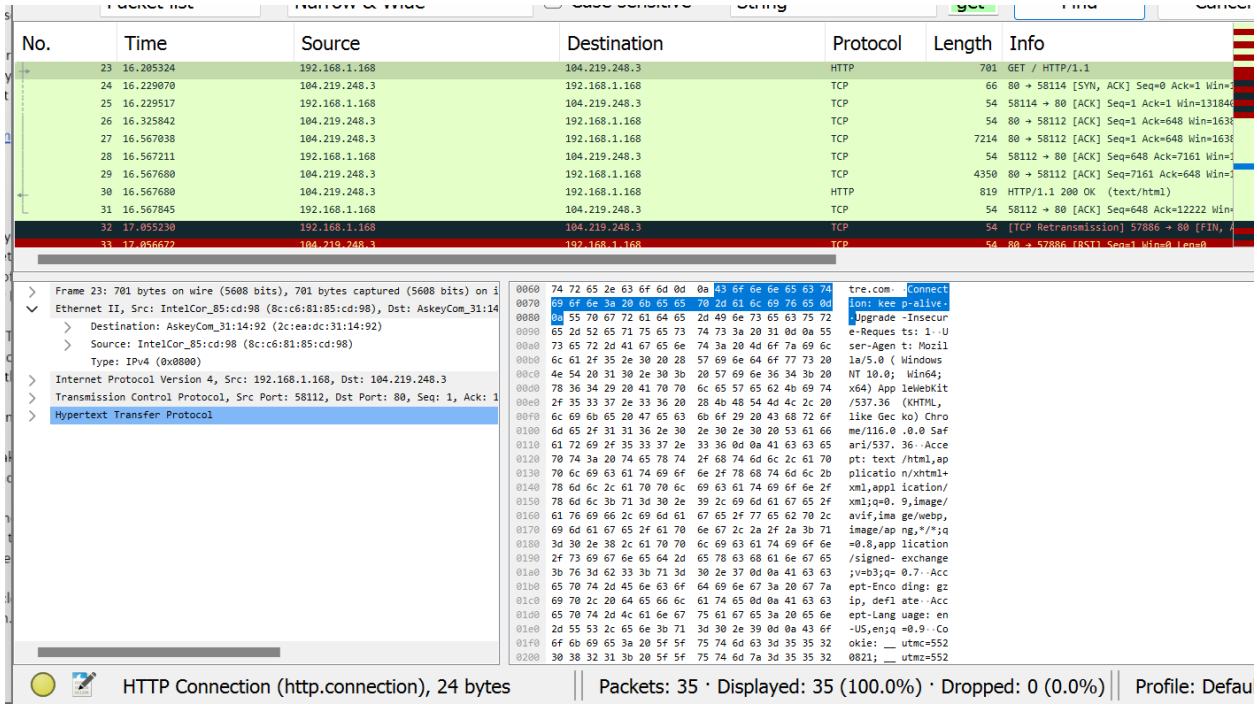
- **Step 4:**



- **Step 14:**



- **Step 16:**

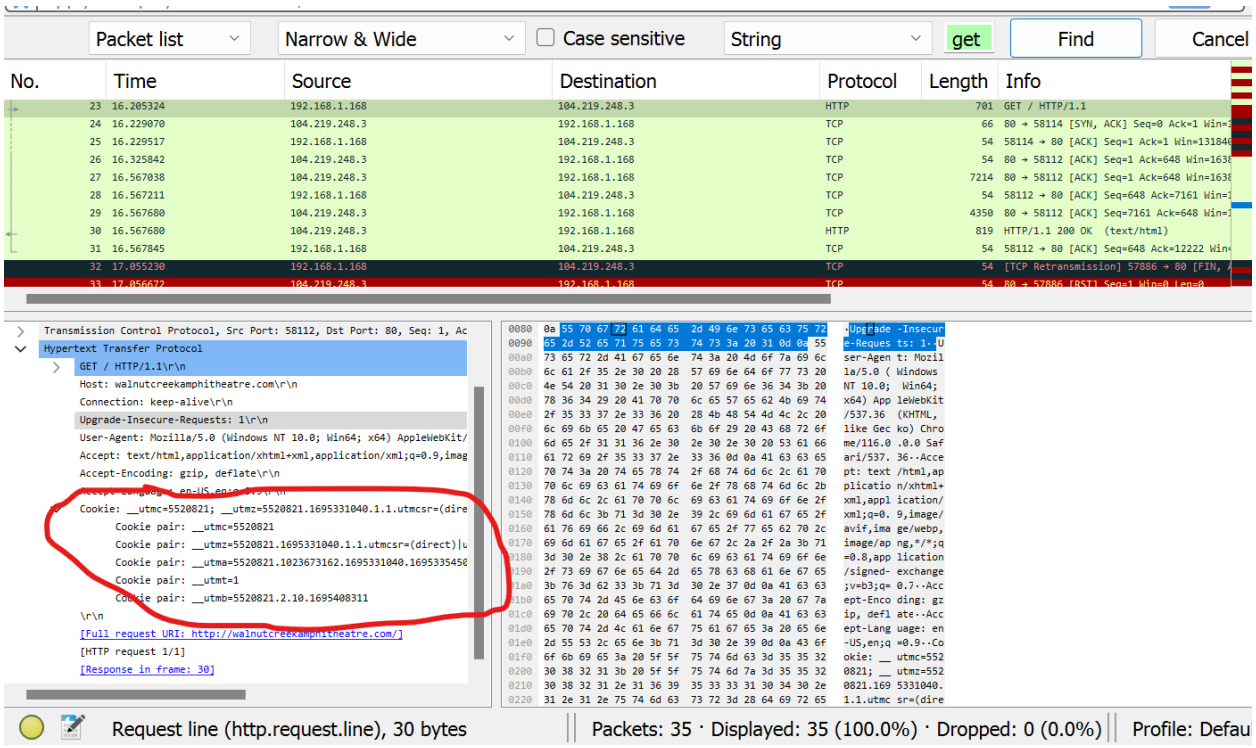


- **Step 19:**

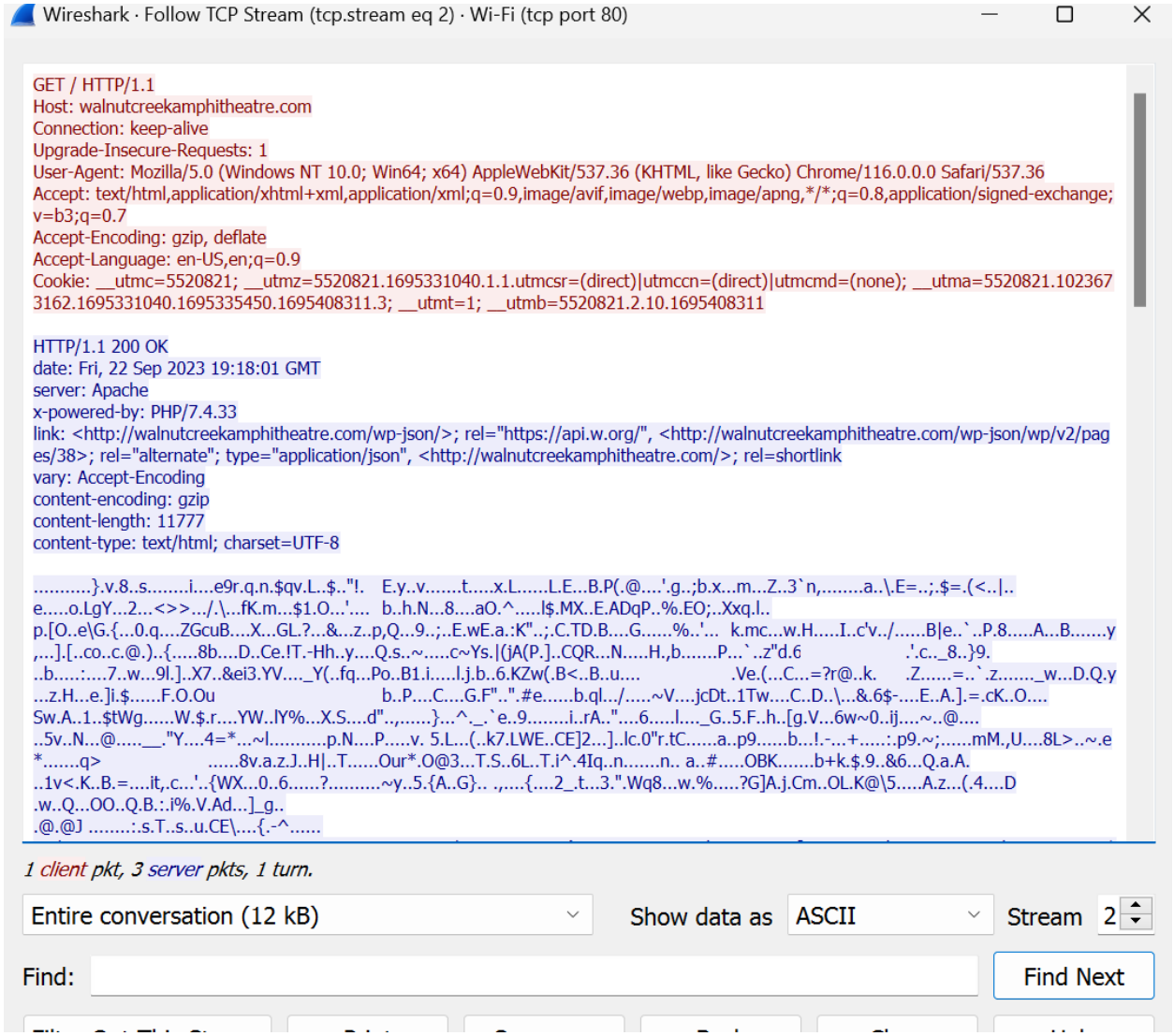
Command Prompt

```
   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>
```

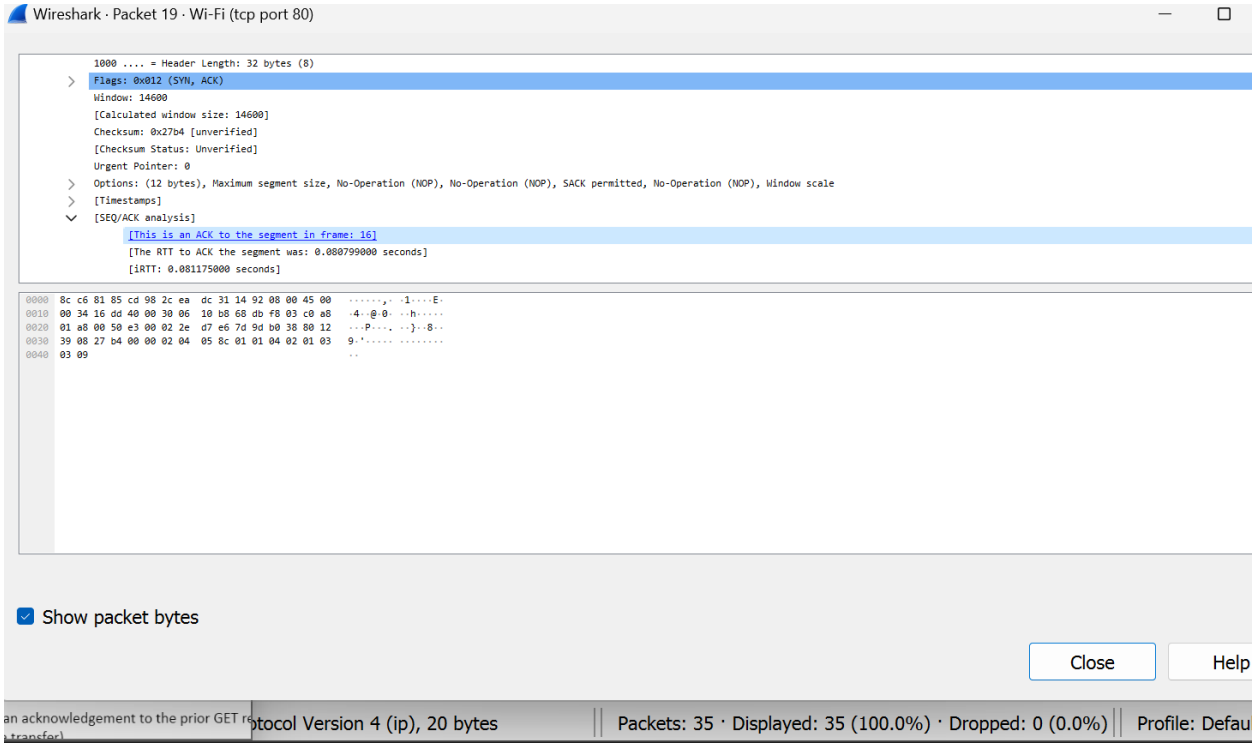
- **Step 22:**



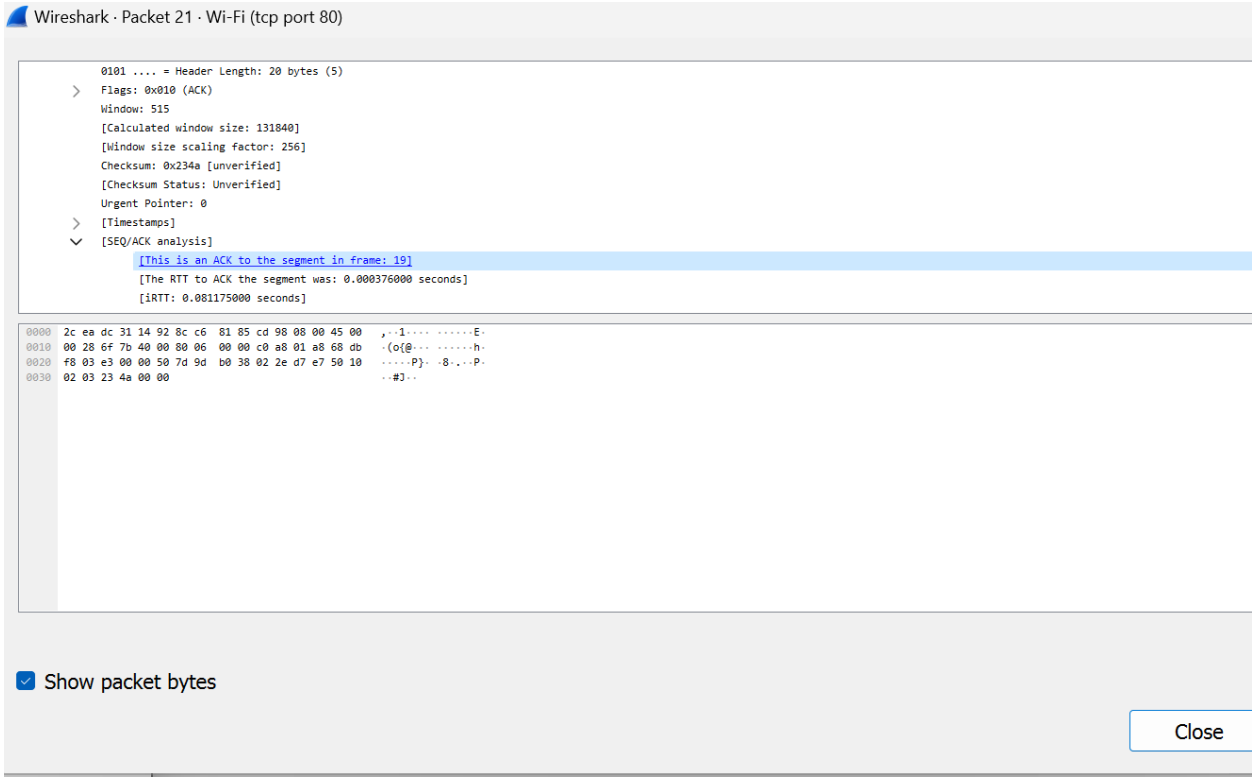
- **Step 24:**


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; __utmz=5520821.1695331040.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(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
1 client pkt, 3 server pkts, 1 turn.
Entire conversation (12 kB)
Show data as
ASCII
Stream
2
Find:
Find Next

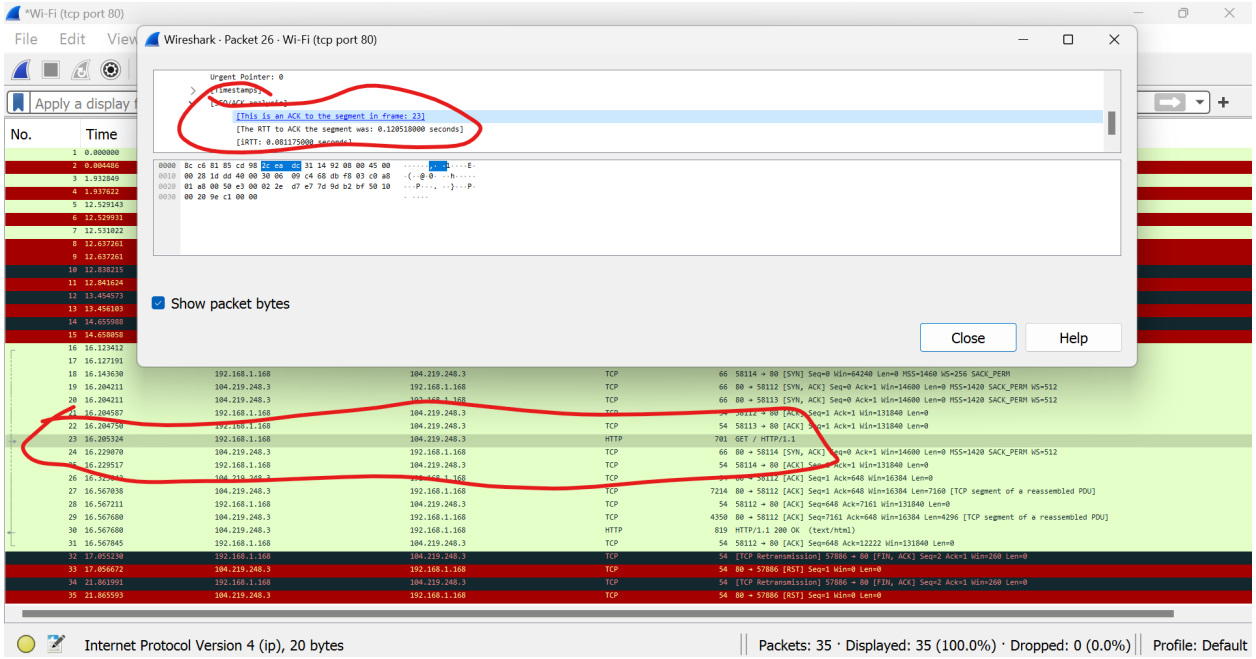
- **Step 34:**



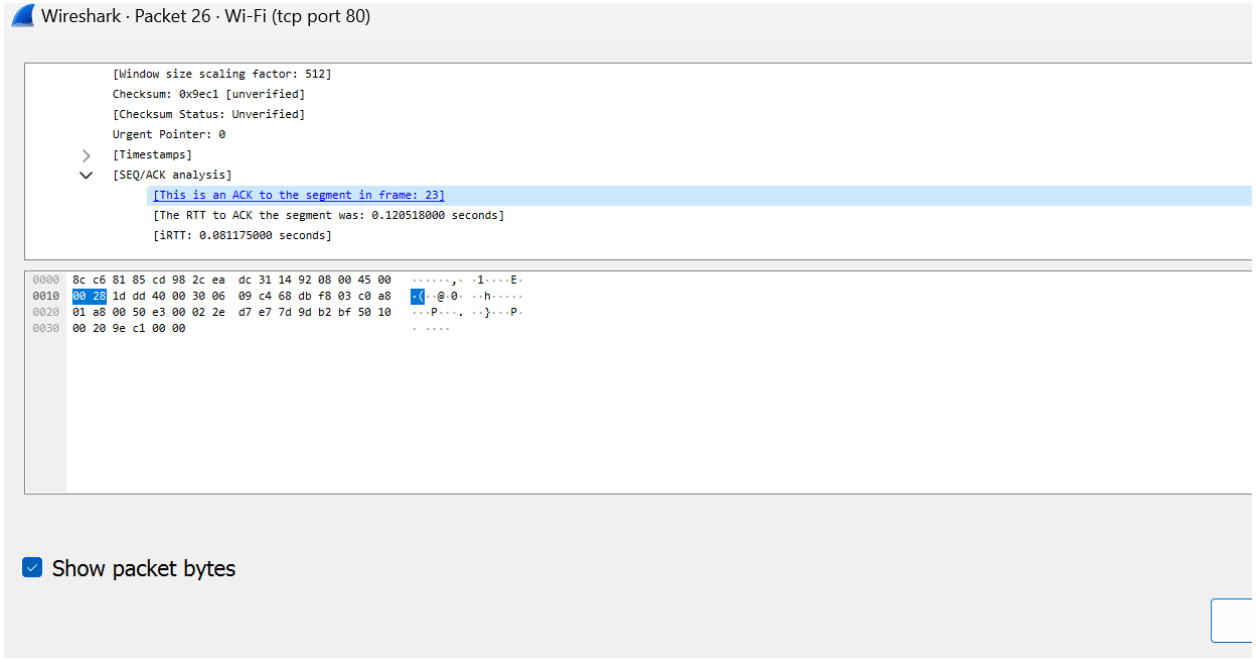
- **Step 39:**



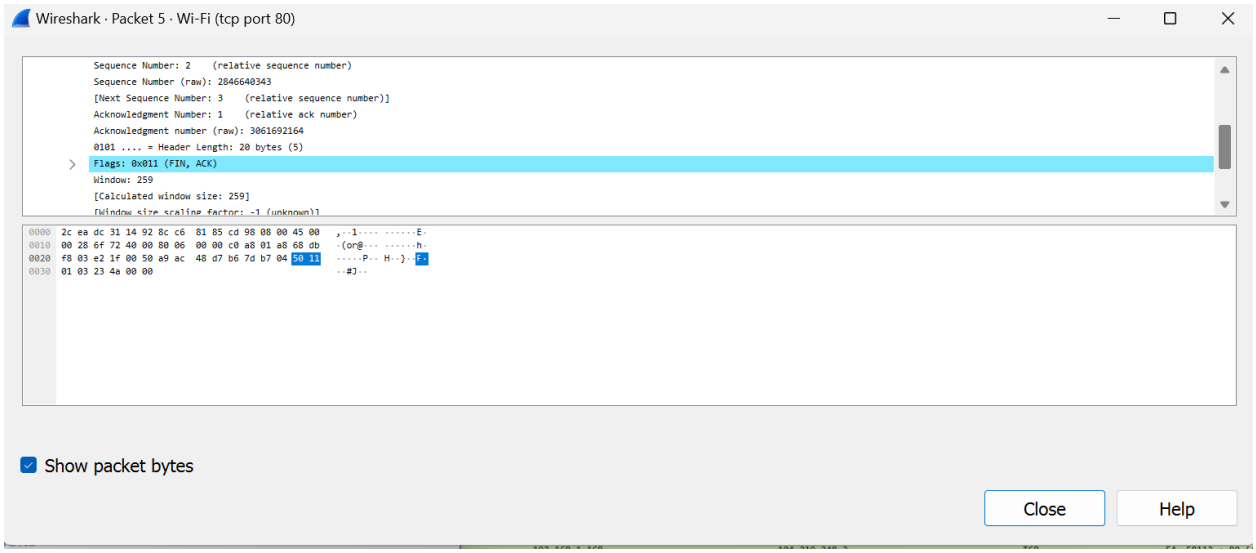
- **Step 40:**



- **Step 44:**



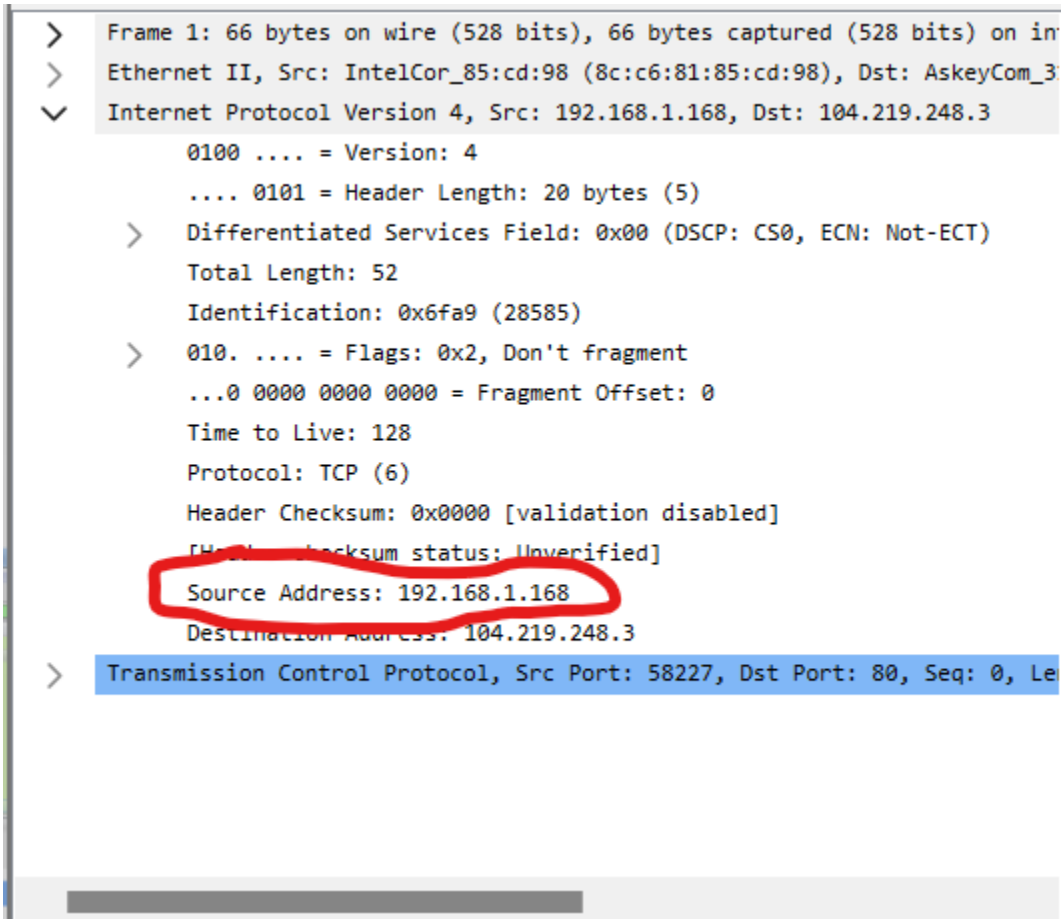
- **Step 48:**



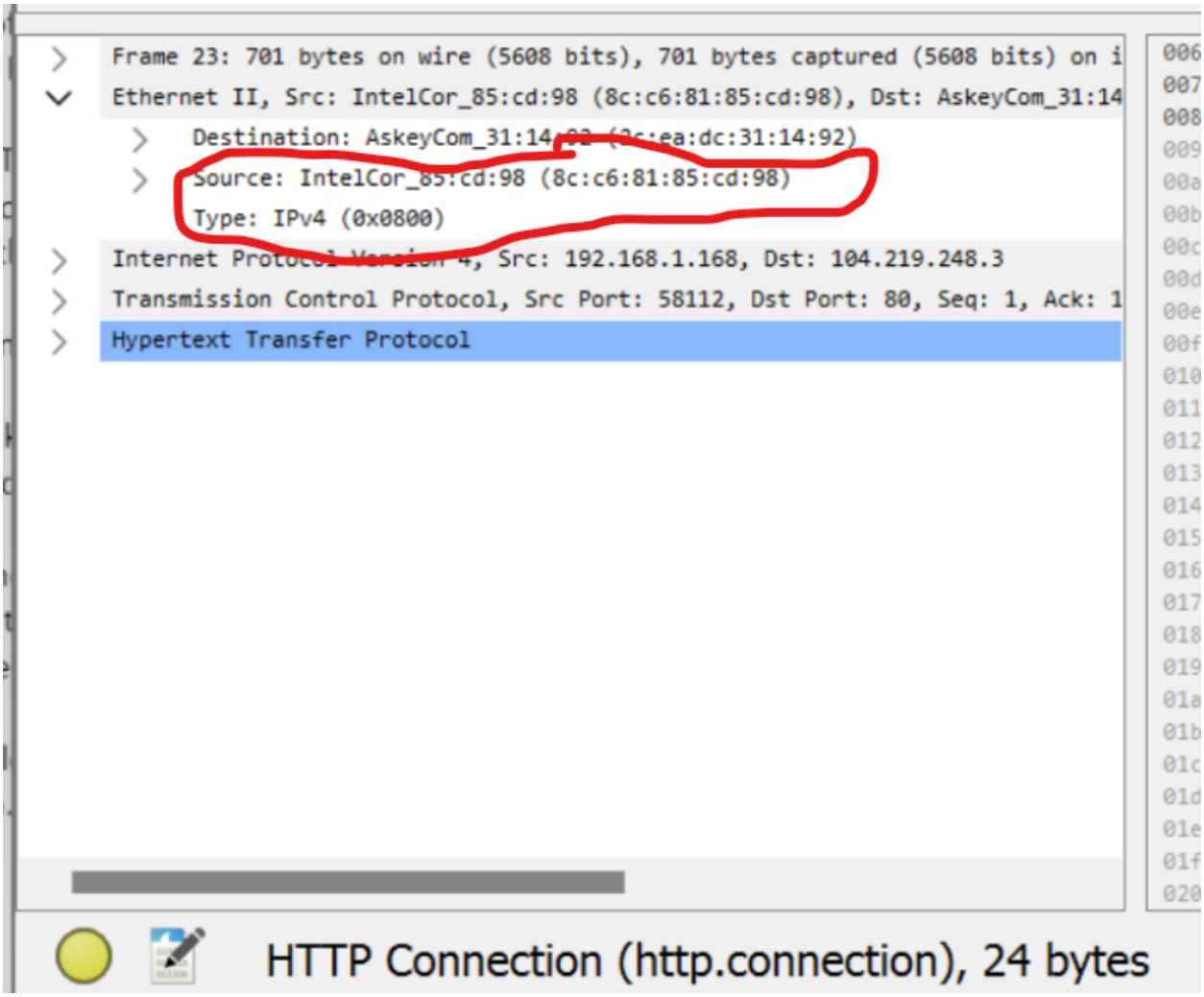
- **Step 51: There was no [SEQ,ACK] analysis option for me on this step.**

Section 3: Questions

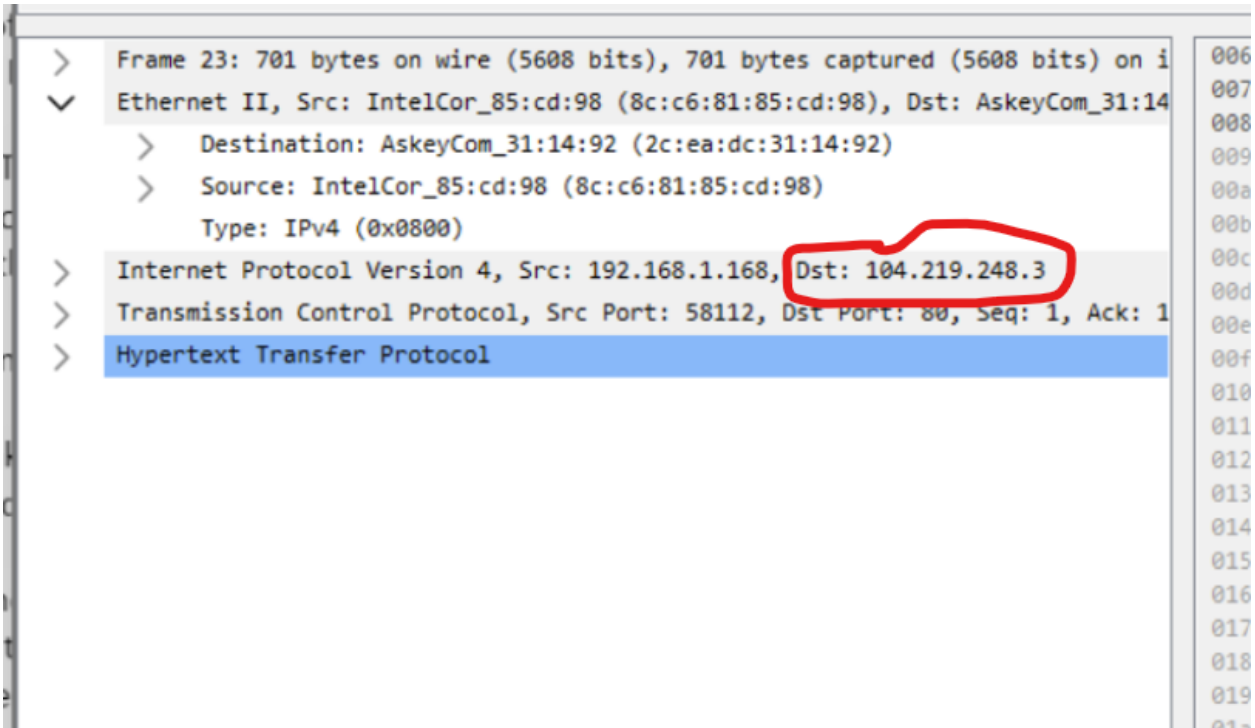
1. My IP address during this part was 192.168.1.168.



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



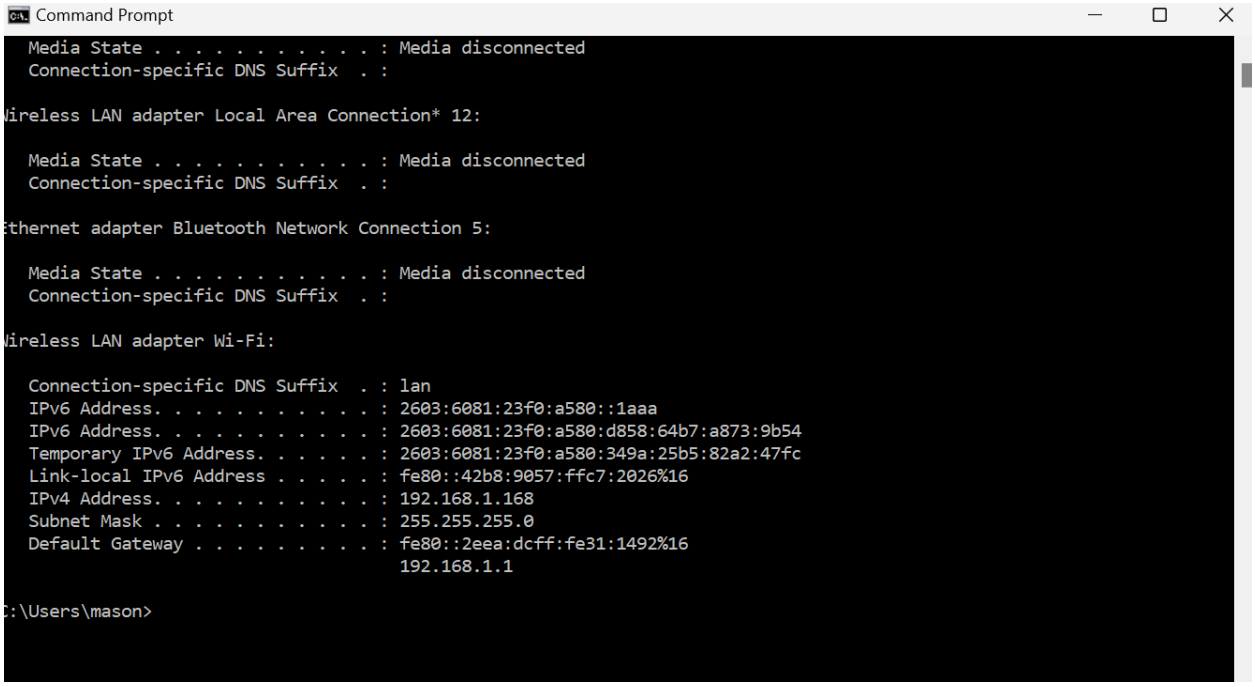
3. The IP address for the walnut creek amphitheater website is 104.219.248.3.



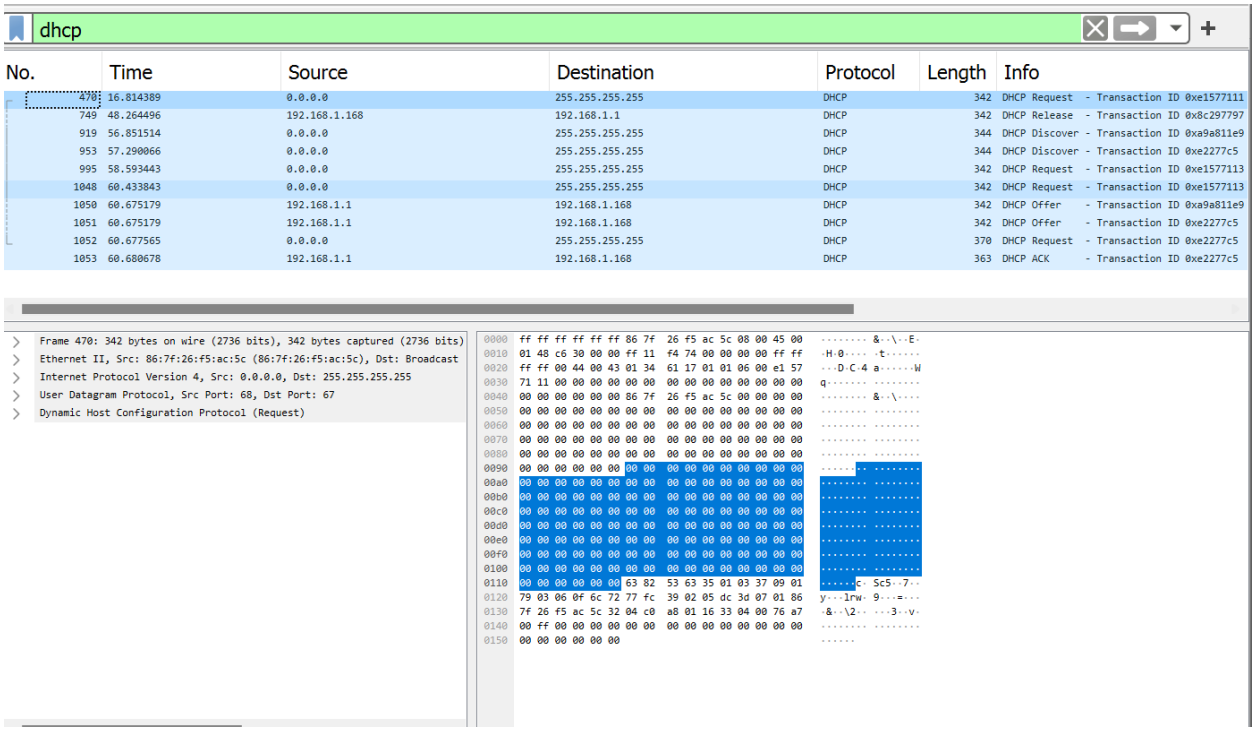
4. The “Follow TCP Stream” feature in Wireshark organizes and displays all communication between my computer and the destination's computer and shows it as a single conversation. It includes things such as the Get request and what browser I’m using. This way it is easier to understand the data exchange between them.
5. When you use the SEQ/ACK option,you are gathering all the SYN and ACK messages between my computer and the destination’s computer. What the feature does is show you the three way handshake from beginning to end.

Section 4:

- **Step 2:**

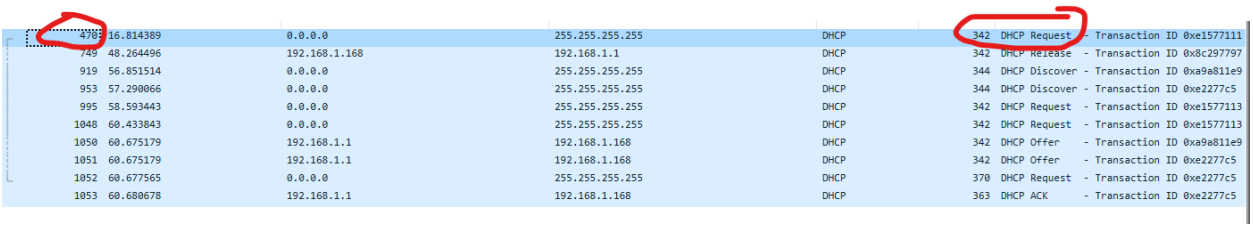


- **Step 4:**

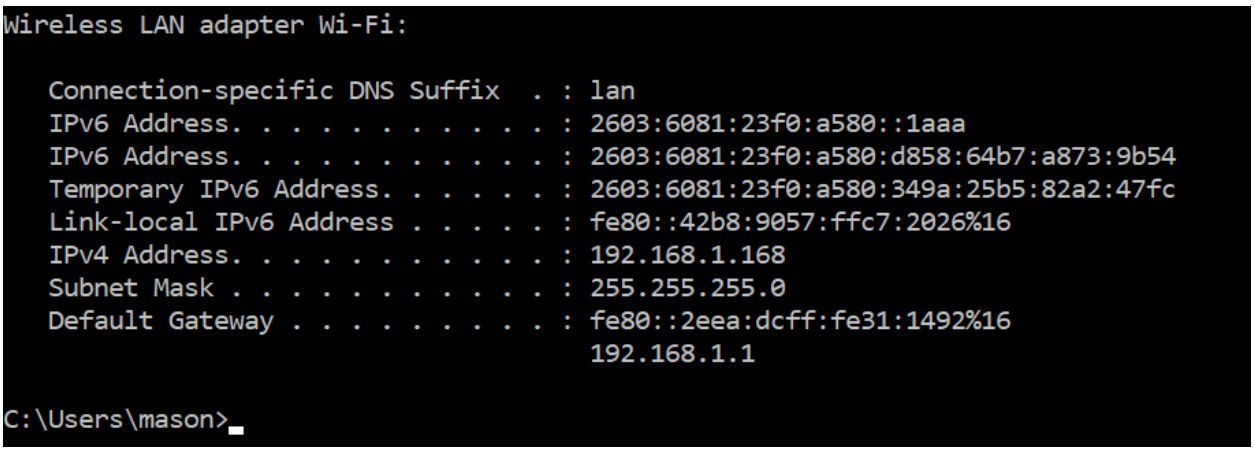


Section 4: Questions

1. Frame 470 carried the DHCP request.



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



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.