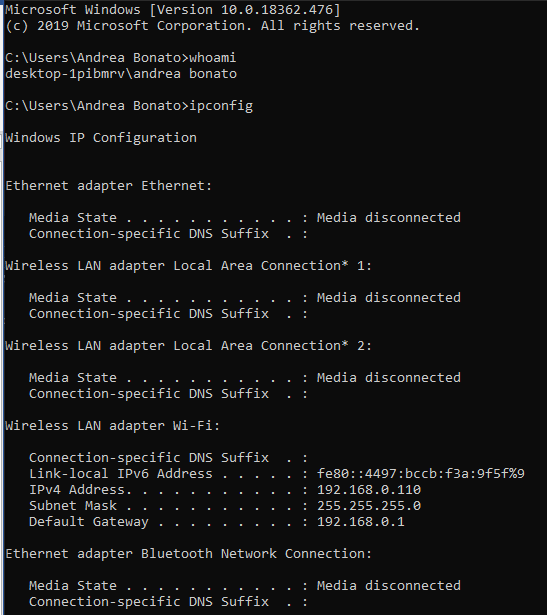
# COMP-3670 Fall 2019 Assignment 3

Andrea Bonato

104760390

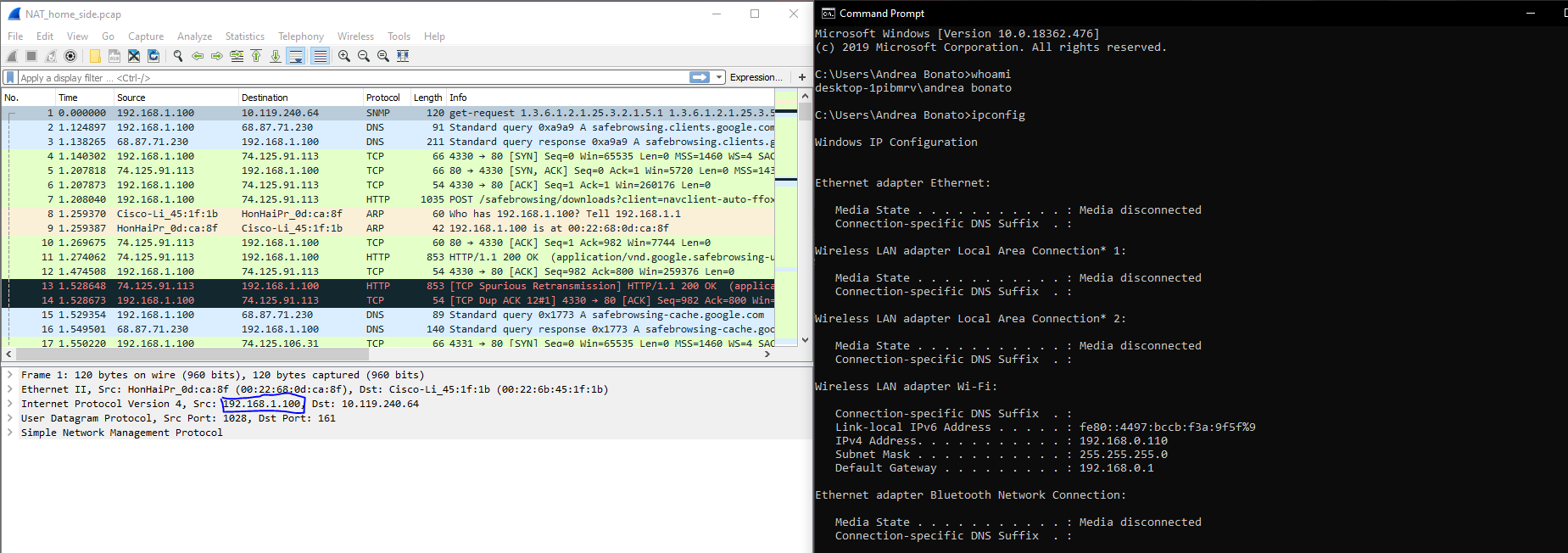


With this assignment, since I was unable to get a NAT device and unable to get two devices to continue with it, I did as the assignment prompted and used the traces that they provide.

# Wireshark Lab: NAT

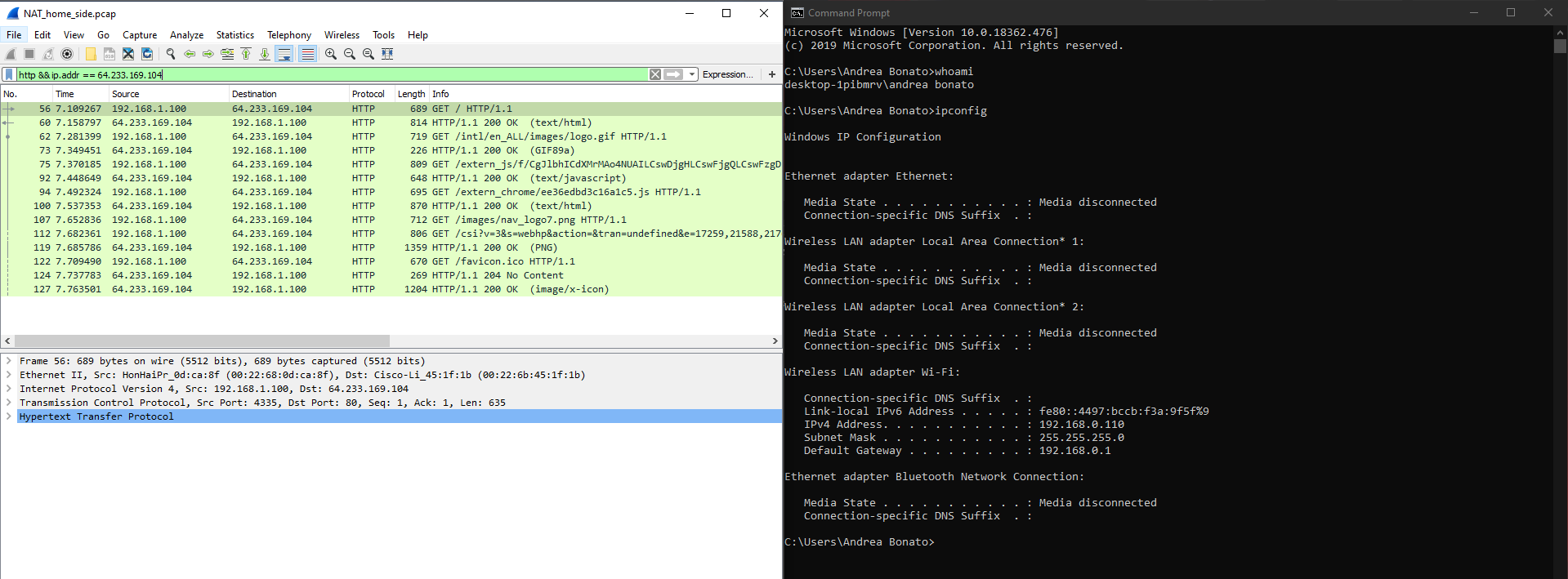
### What is the IP address of the client?

The IP address of the client is 192.168.1.100 as shown in the screenshot below.



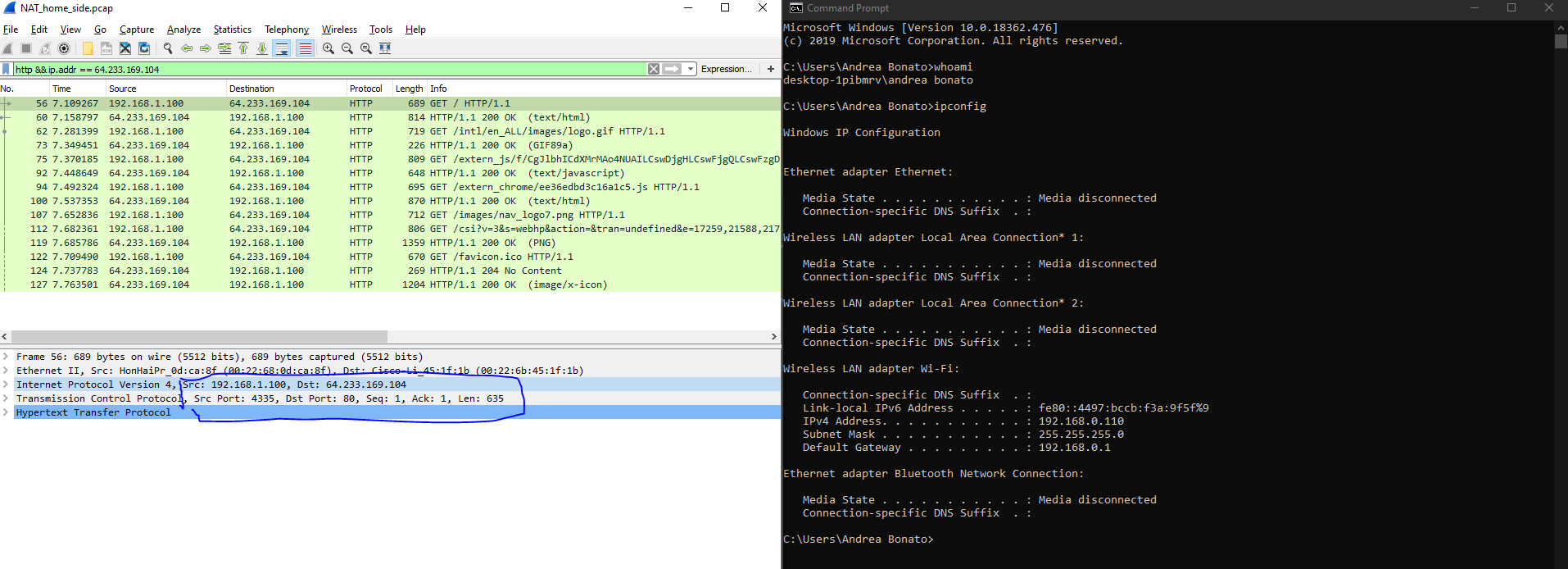
### The client actually communicates with several different Google servers in order to implement “safe browsing.” (See extra credit section at the end of this lab). The main Google server that will serve up the main Google web page has IP address 64.233.169.104. In order to display only those frames containing HTTP messages that are sent to/from this Google, server, enter the expression “http && ip.addr == 64.233.169.104” (without quotes) into the Filter: field in Wireshark .

The filter will be shown in the following screenshot:



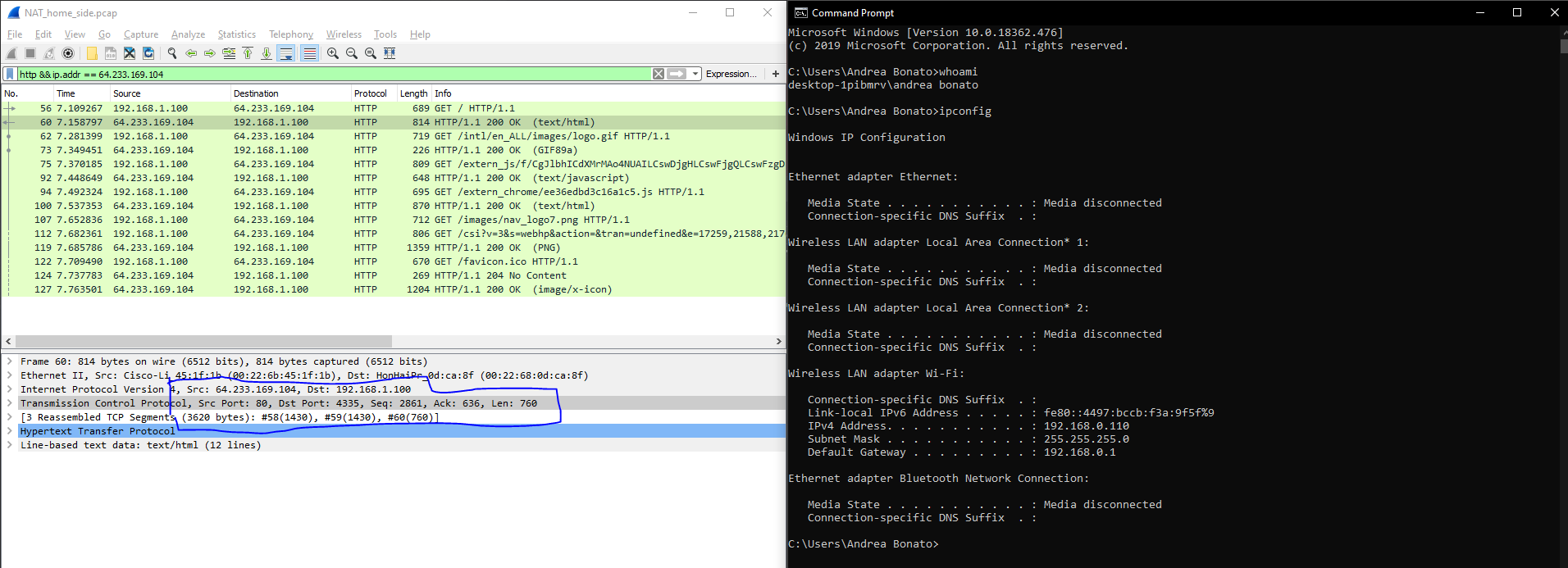
### Consider now the HTTP GET sent from the client to the Google server (whose IP address is IP address 64.233.169.104) at time 7.109267. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?

As shown in the screenshot below, the source IP is 192.168.1.100 and the destination IP is 64.233.169.104. The source port is 4335 and the destination port is 80.

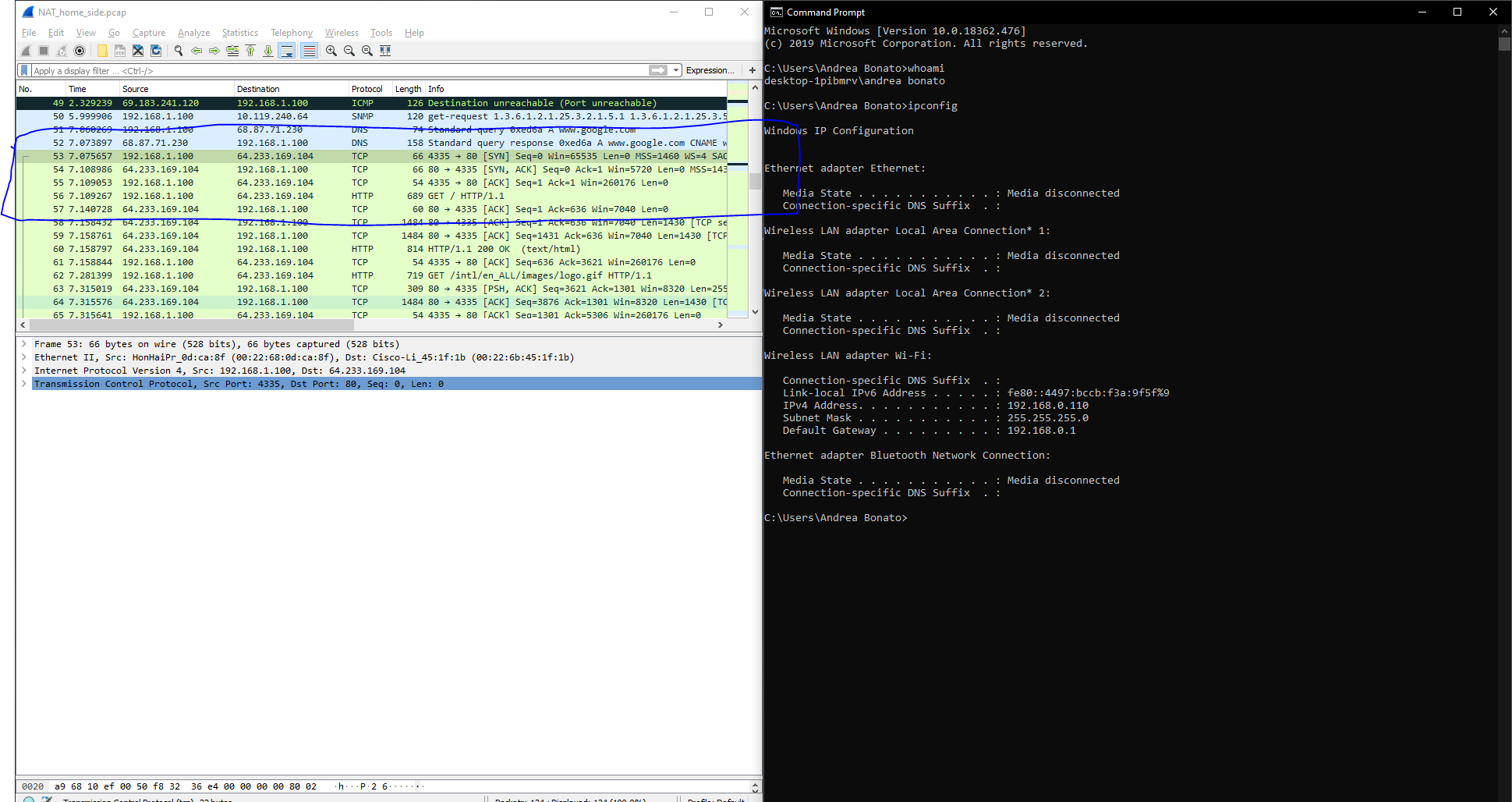


### At what time is the corresponding 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

According to the screenshot below, the source IP address is 64.233.169.104 and the destination IP is 192.168.1.100. The source port is 80 and the destination port is 4335.



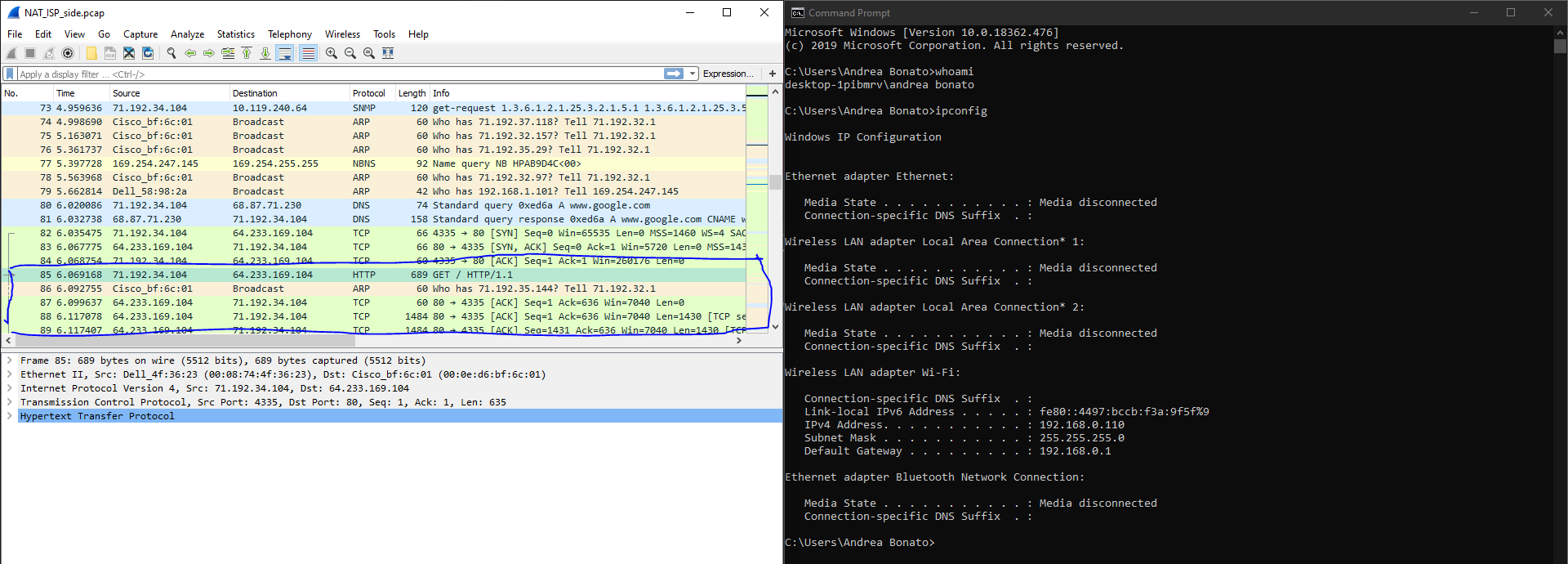
### Recall that before a GET command can be sent to an HTTP server, TCP must first set up a connection using the three-way SYN/ACK handshake. At what time is the client-to-server TCP SYN segment sent that sets up the connection used by the GET sent at time 7.109267? What are the source and destination IP addresses and source and destination ports for the TCP SYN segment? What are the source and destination IP addresses and source and destination ports of the ACK sent in response to the SYN. At what time is this ACK received at the client? (Note: to find these segments you will need to clear the Filter expression you entered above in step 2. If you enter the filter “tcp”, only TCP segments will be displayed by Wireshark).



The time that the client-to-server TCP SYN segment is sent that sets up the connection used by the GET sent at time 7.109267 is 7.075657. The source IP address of the TCP SYN segment is 192.168.1.100 (port 4335) and the destination IP is 64.233.169.104 (port 80). The source IP address of the ACK segment is 64.233.169.104 (port 80) and the destination IP is 192.168.1.100 (port 4335). The ACK is received at 7.108986.

### In the NAT\_ISP\_side trace file, find the HTTP GET message was sent from the client to the Google server at time 7.109267 (where t=7.109267 is time at which this was sent as recorded in the NAT\_home\_side trace file). At what time does this message appear in the NAT\_ISP\_side trace file? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET (as recording in the NAT\_ISP\_side trace file)? Which of these fields are the same, and which are different, than in your answer to question 3 above?

The time at which this was sent was at 6.069168, as shown in the screenshot below. The source IP is 71.192.34.104, port 4335, and the destination IP is 64.233.169.104, port 80. The only field that changes is the source IP address. The destination, and the ports, are the same.

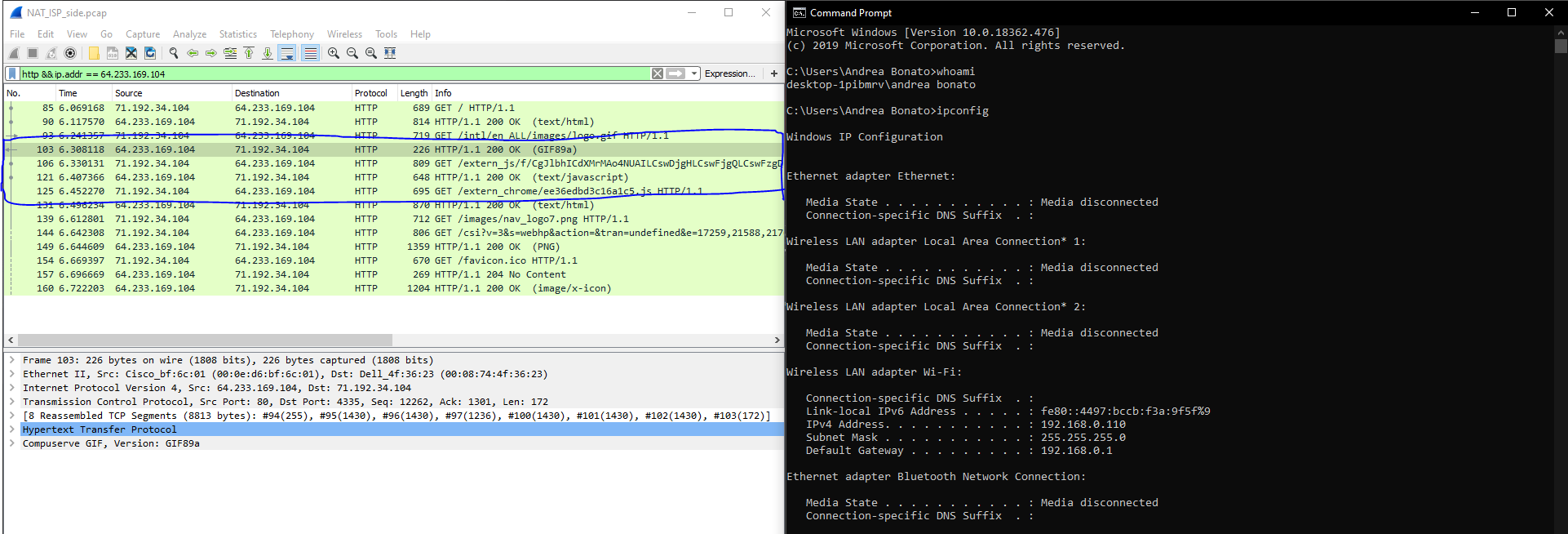


### Are any fields in the HTTP GET message changed? Which of the following fields in the IP datagram carrying the HTTP GET are changed: Version, Header Length, Flags, Checksum. If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change.

None of the fields in the HTTP GET message has changed. When comparing the fields itself in the datagram, the version, header length and flags did not change. However, the checksum flag did end up changing. This is because the source IP address changes, and the checksum includes the value of this specific IP address.

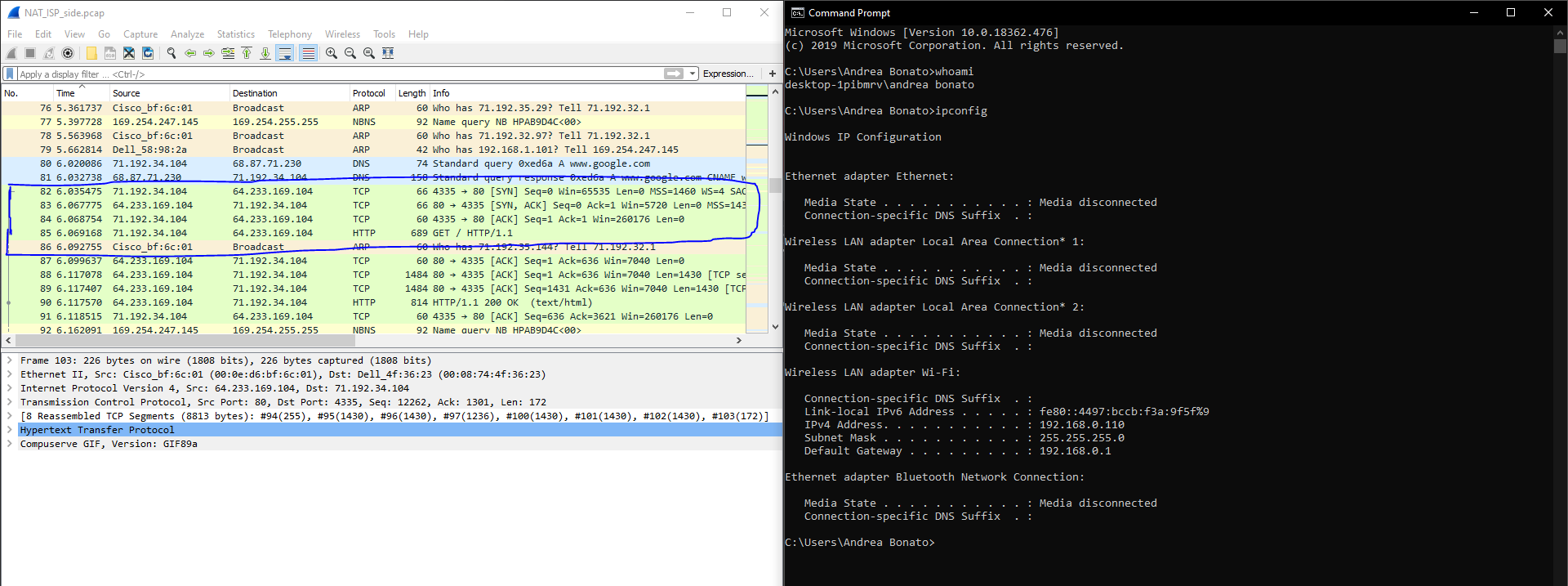
### In the NAT\_ISP\_side trace file, at what time is the first 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message? Which of these fields are the same, and which are different than your answer to question 4 above?

The time that the first 200 OK HTTP message was received was 6.308118. The source address for this was 64.233.169.104, port 80, and the destination IP was 71.192.34.104, port 4335. In this case, only the destination IP is different.



### In the NAT\_ISP\_side trace file, at what time were the client-to-server TCP SYN segment and the server-to-client TCP ACK segment corresponding to the segments in question 5 above captured? What are the source and destination IP addresses and source and destination ports for these two segments? Which of these fields are the same, and which are different than your answer to question 5 above?

The time that the client-to-server TCP SYN segment were captured was at 6.035475 and the TCP ACK was captured at 6.067775.

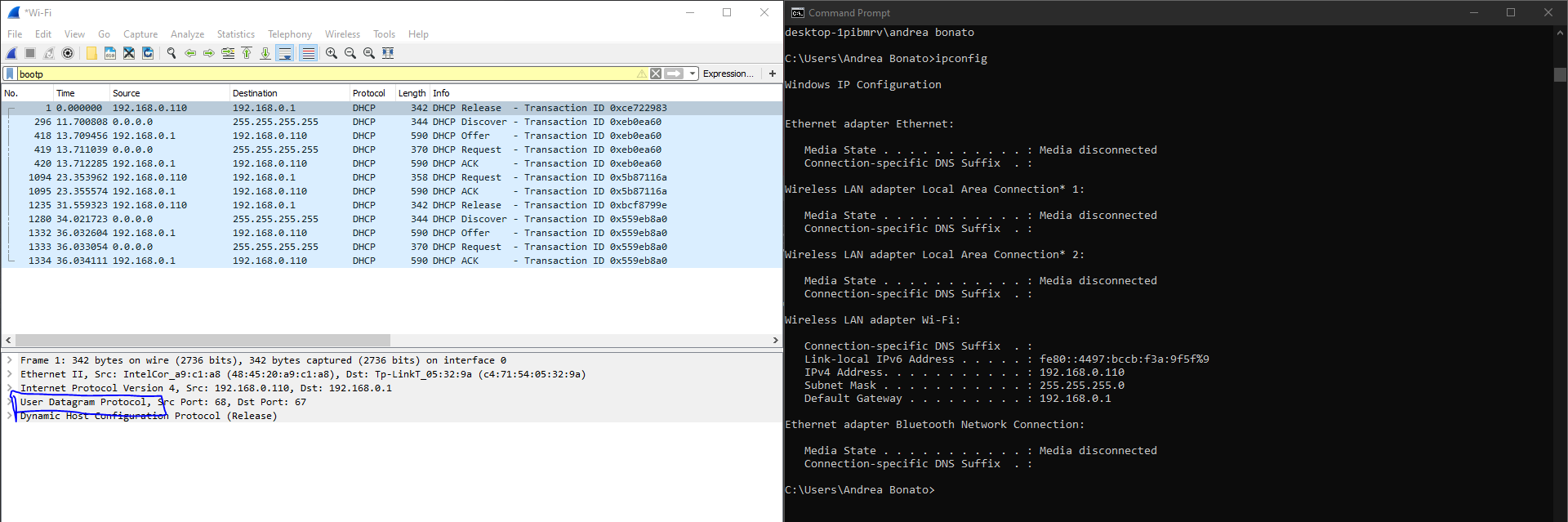


The source IP for the SYN is 71.192.34.104, port 4335, and the destination IP is 64.233.69.104 port, 80. The source Ip for the ACK is 64.233.69.104, port 80, and the destination IP is 71.192.34.104, port 4335. In these cases, the port number remains the same, and in comparison to the solution in question 5, the source IP for the SYN source IP has changed and the destination IP for the ACK has also changed.

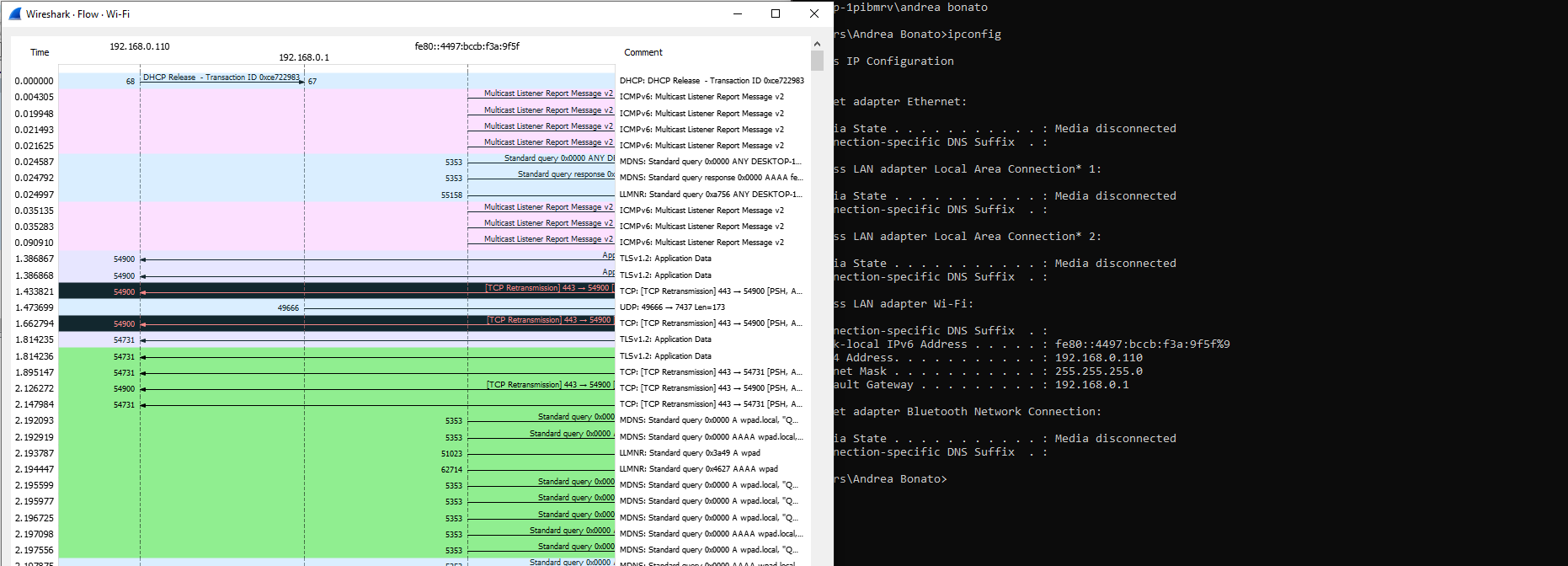
# Wireshark Lab: DHCP

### 1. Are DHCP messages sent over UDP or TCP?

The messages are sent over UDP.

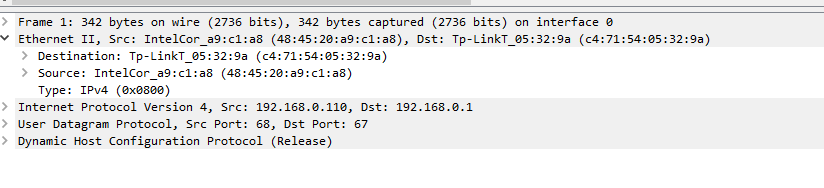


### 2. Draw a timing datagram illustrating the sequence of the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server. For each packet, indicated the source and destination port numbers. Are the port numbers the same as in the example given in this lab assignment?



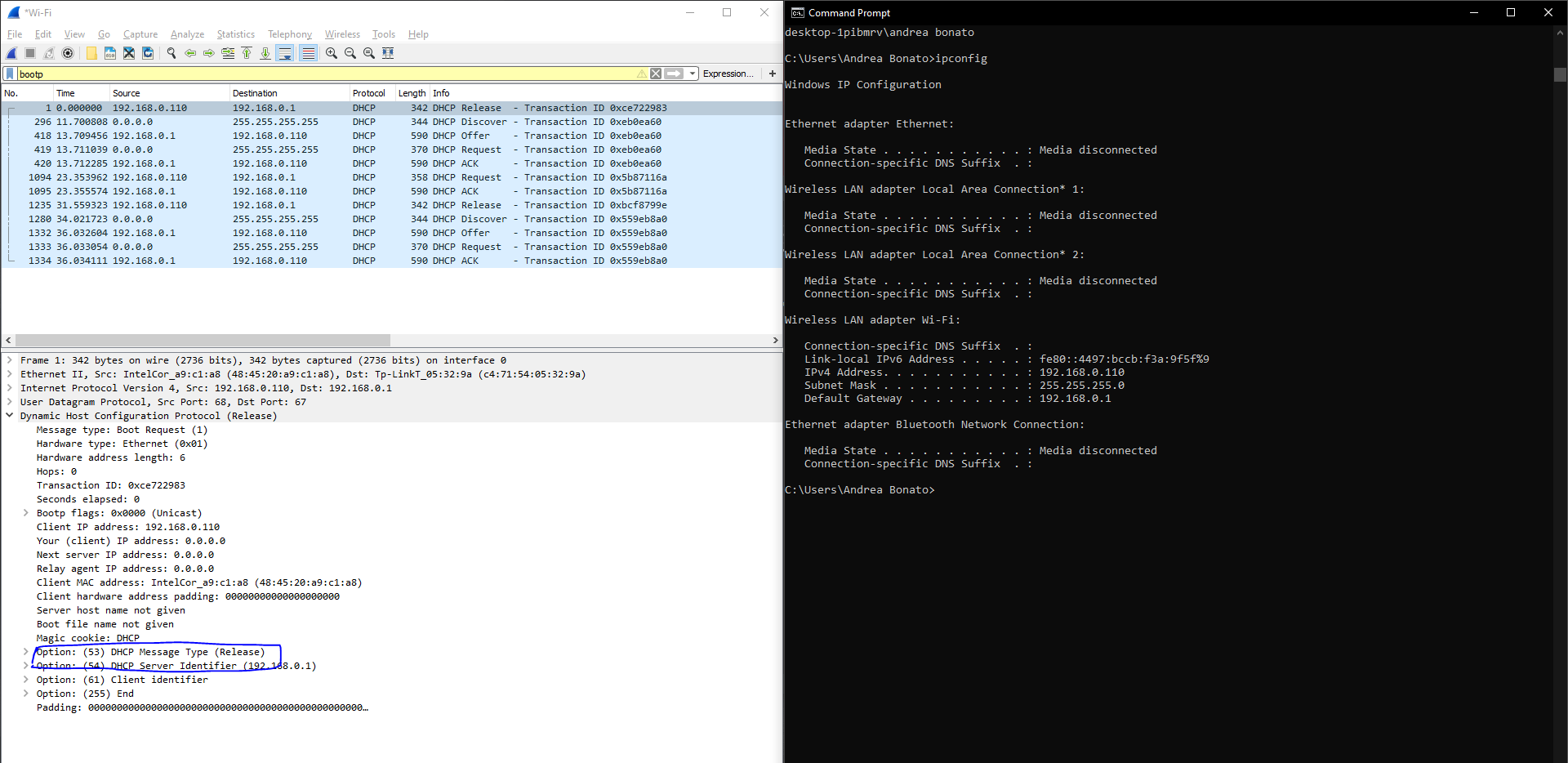
### 3. What is the link-layer (e.g., Ethernet) address of your host?

The link layer address of my workstation is 48:45:20:a9:c1:a8.



### 4. What values in the DHCP discover message differentiate this message from the DHCP request message?

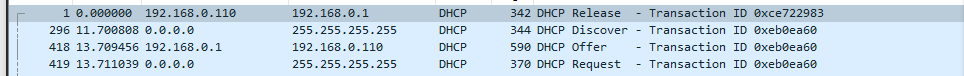
The value that differentiates this message from the DHCP request message to the discover message is the DHCP Message Type.





### 5. What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What are the values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field?

The value of the Transaction-ID in each of the first four is 0xce722983, and the rest is 0xeb0ea60.



The values of the second Transaction-ID is 0xeb0ea60. A Transaction-ID is used to determine whether the requests are from the server and client.

### 6. A host uses DHCP to obtain an IP address, among other things. But a host’s IP address is not confirmed until the end of the four-message exchange! If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? For each of the four DHCP messages (Discover/Offer/Request/ACK DHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.

### 

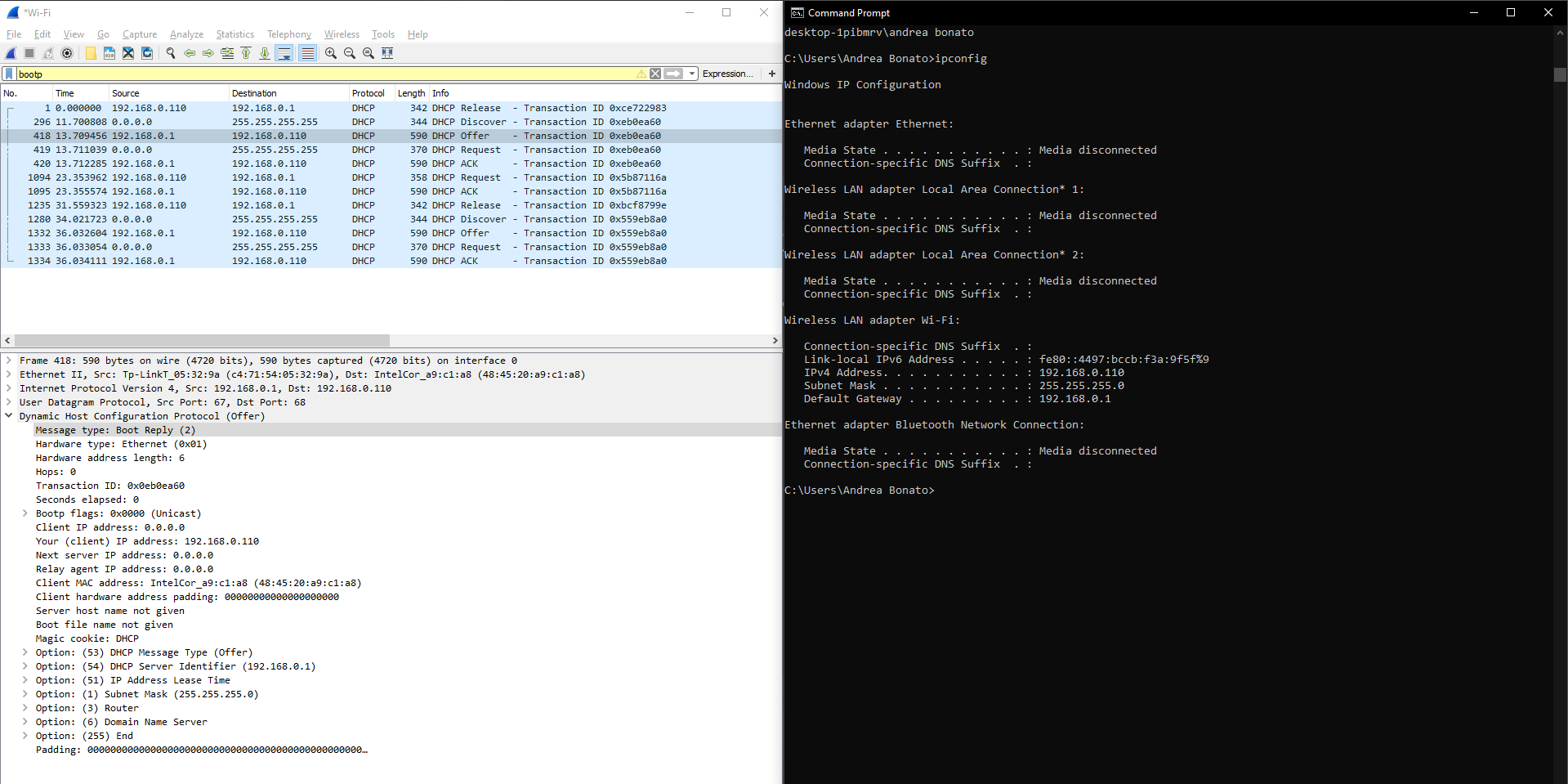
As shown above, the DCHP client and server both use 255.255.255.255 as the destination address. The client uses source IP addresses 0.0.0.0 and the actual server uses it’s own IP.

### 7. What is the IP address of your DHCP server?

The address of the server is 192.168.0.1.

### 8. What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address.

The IP address that the DHCP server is offering is 192.168.0.110. The DHCP message type is equal to DHCP offer



### 9. In the example screenshot in this assignment, there is no relay agent between the host and the DHCP server. What values in the trace indicate the absence of a relay agent? Is there a relay agent in your experiment? If so, what is the IP address of the agent?

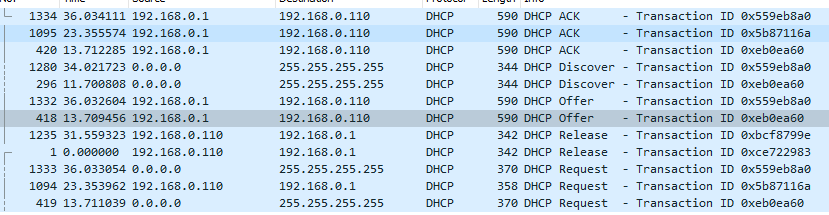
As shown in the screenshot in question 8, there is a relay agent, and it is set to the IP address 0.0.0.0. Thus, in my experiment there is a relay agent.

### 10. Explain the purpose of the router and subnet mask lines in the DHCP offer message.

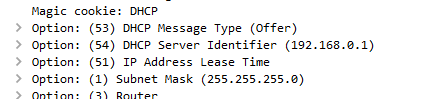
The router line indicates what the default gateway should be to the client and the subnet mask lines determine which subnet mask the client should use.

### 11. In the DHCP trace file noted in footnote 2, the DHCP server offers a specific IP address to the client (see also question 8. above). In the client’s response to the first server OFFER message, does the client accept this IP address? Where in the client’s RESPONSE is the client’s requested address?

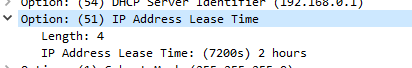
The host requests the offered IP address in the DHCP request message . The client’s respone message is accepted in order to get to this section.



### 12. Explain the purpose of the lease time. How long is the lease time in your experiment?



The lease time is the amount of time that the DHCP server assigns an IP address to a client for. In this time, the server will not change the given address to another client, unless the client ha already given up the IP address that it was assigned.



In this case, the lease time is 2 hours,

### 13. What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client’s DHCP request? What would happen if the client’s DHCP release message is lost?

As states in question 12, the lease time is the amount of time that the DHCP server takes between the assigning and requesting of the IP addresses. The DHCP release message is the message that the client sends to cancel its lease on the IP address given to it by the DHCP sever. However, the DHCP, in this case, did not acknowledge the request. In this case, because it was list, the DHCP server would have to wait the lease time to reassign the IP address.

### 14. Clear the bootp filter from your Wireshark window. Were any ARP packets sent or received during the DHCP packet-exchange period? If so, explain the purpose of those ARP packets.

In this case, there were several ARP requests made by the DHCP server.



The purpose of the ARP packets is to make sure that the IP addresses that are being assigned, isn’t already assigned.