Sidarth Shahri
CMPE 148 – Computer Networks I

Lab Assignment #2 – DHCP

1) Are DHCP messages sent over UDP or TCP?

A: DHCP messages are sent in UDP. Evidence in screenshot below.

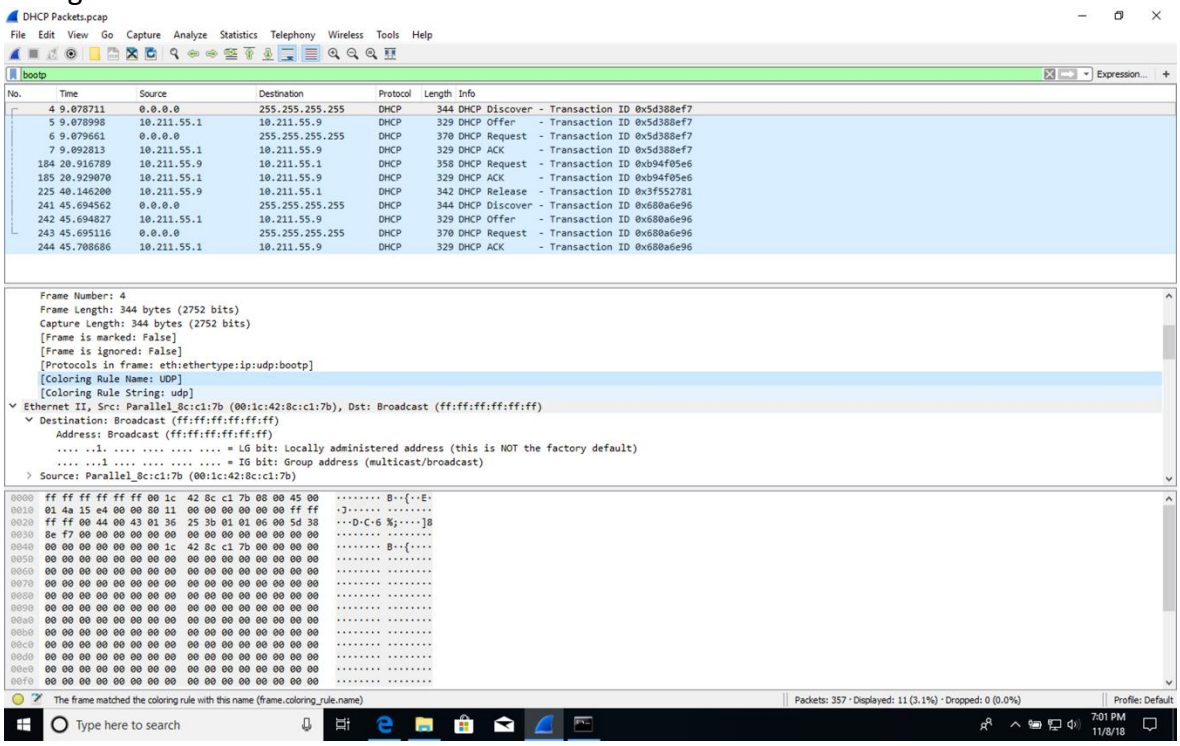

Figure 1: Coloring rule shows UDP in datagram frame.

2) Draw a timing diagram illustrating the sequence of the first four-packet.

A: The port and destination numbers match the example in the lab assignment.

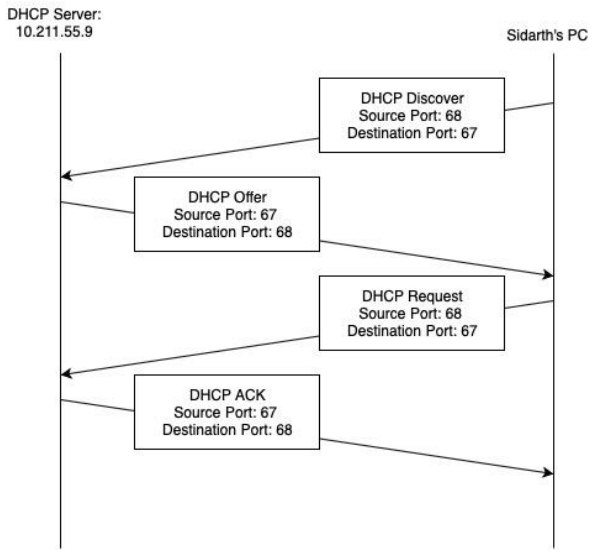

Figure 2: Timing Diagram showing four packets sent with ipconfig /renew command.

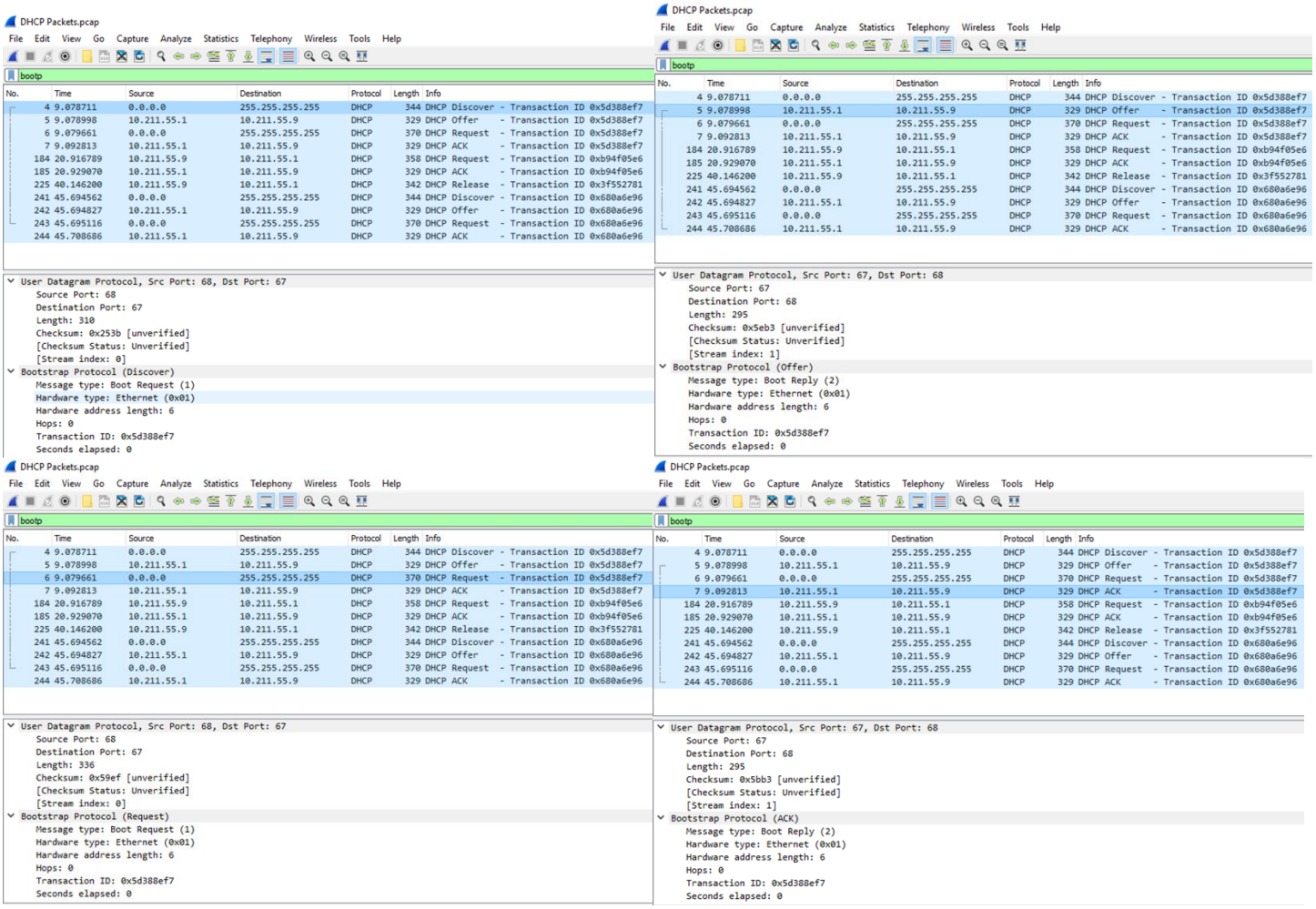

Figure 3: Four screenshots showing port data from Wireshark. Each image shows its own packet from DHCP Discover to DHCP ACK.

3) What is the link-layer address of your host?

A: My computer's link-layer address is 00:1C:42:8C:C1:7B. Note that I am using Windows in a virtual machine which assigns Windows a virtual address to communicate with macOS.

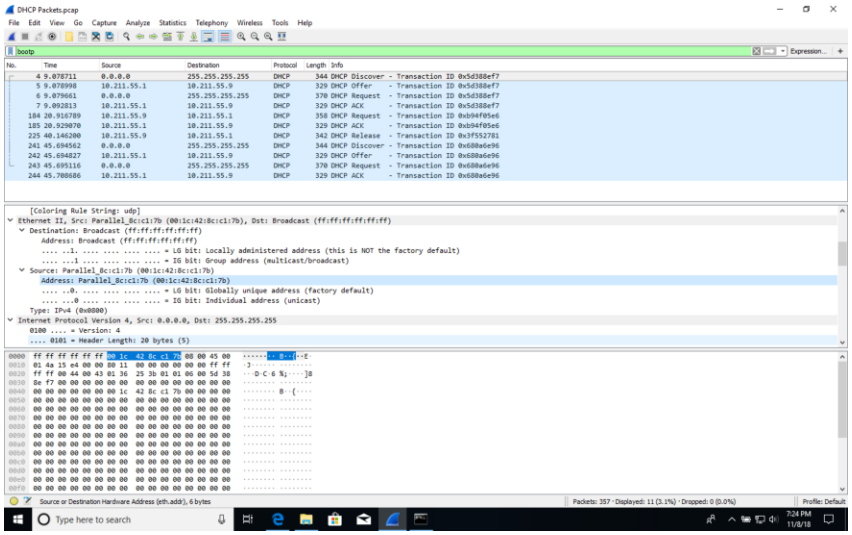

Figure 4: Screenshot showing link-layer address. Note that I am actually using WiFi through my base OS while Windows sees the connection as an Ethernet link.

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

A: The frame length for the DHCP Offer message is smaller at 329 bytes while the DHCP Discover message is 344 bytes. Additionally, the DHCP Option (53) is defined accordingling for Discover and Offer. See screenshot below:

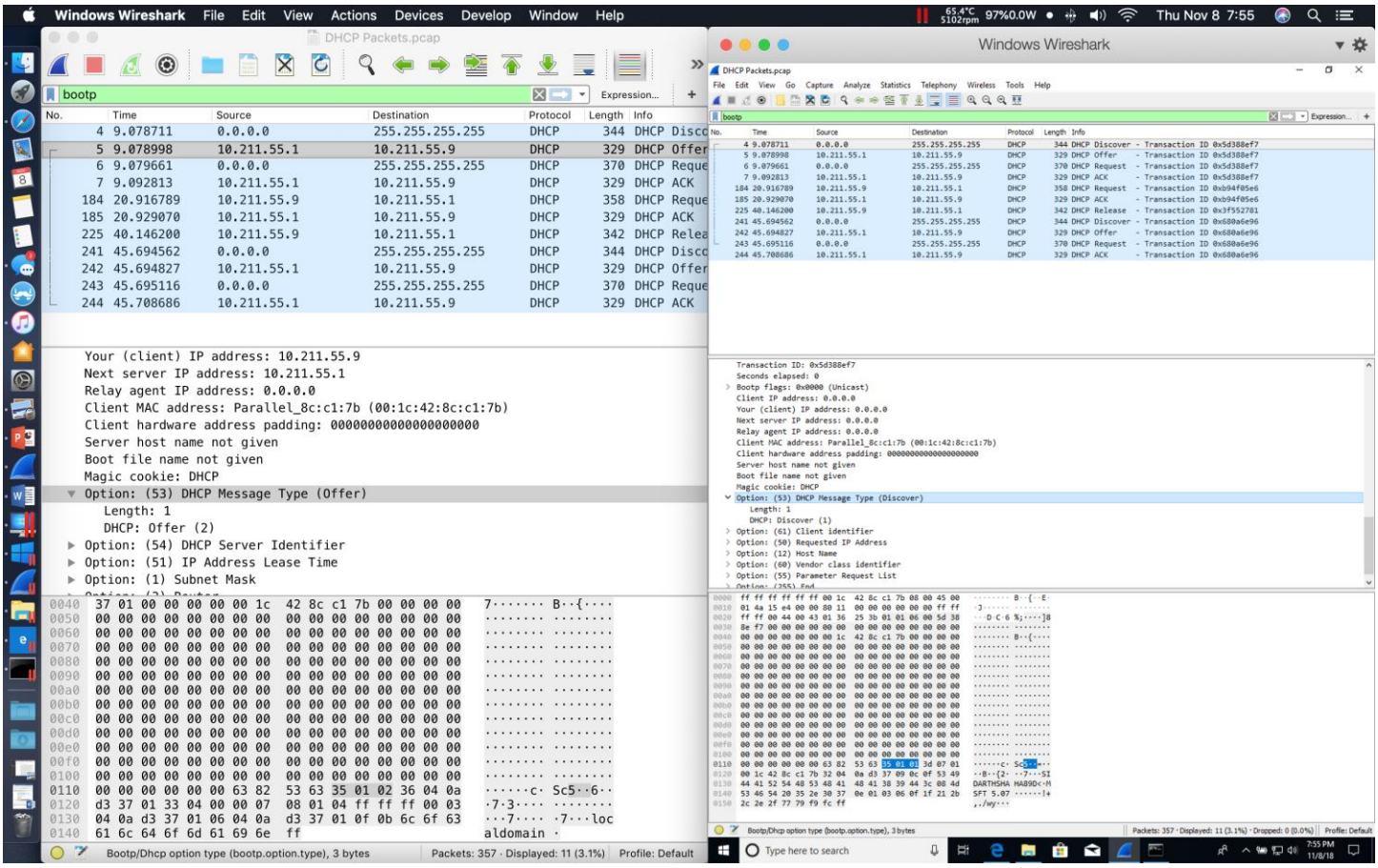

Figure 5: Screenshot showing pcap side by side in two instances of Wireshark. On the right, DHCP Discover is highlighted. On the left, DHCP Offer is highlighted.

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?

A:
1st DHCP Renew
Discover - Transaction ID: 0x5d388ef7
Offer - Transaction ID: 0x5d388ef7
Request - Transaction ID: 0x5d388ef7
ACK - Transaction ID: 0x5d388ef7

2nd DHCP Renew
Request - Transaction ID: 0xb94f05e6
ACK - Transaction ID: 0xb94f05e6

The Transaction-ID field helps to keep track of a set of messages that are related to each other. As such, the first DHCP renew generates four transactions all with the same ID. The difference in ID between the first and second renew is used to keep track of different sets of messages.

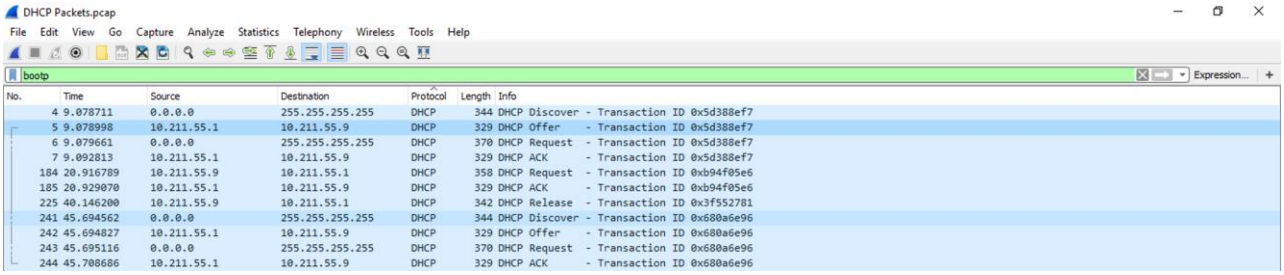

Figure 6: Screenshot from pcap opened in Wireshark showing Transaction IDs.

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.

A:

Discover	Source	0.0.0.0
	Destination	255.255.255.255
Offer	Source	10.211.55.1
	Destination	10.211.55.9
Request	Source	0.0.0.0
	Destination	255.255.255.255
ACK	Source	10.211.55.1
	Destination	10.211.55.9

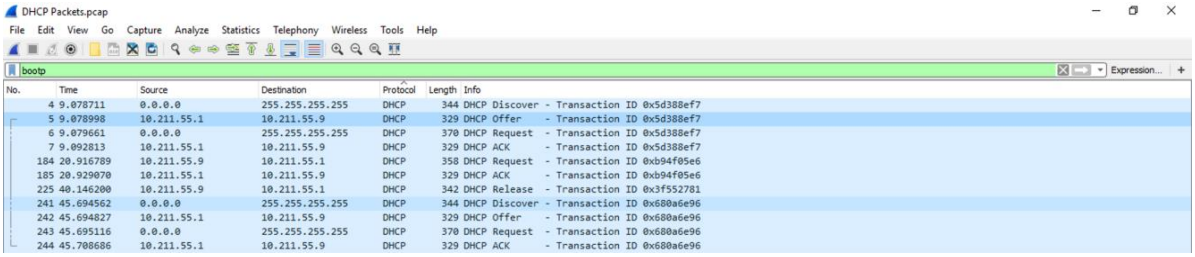

Figure 7: Screenshot showing Source and Destination IP addresses for all DHCP messages. The top four are relevant for this question.

7) What is the IP address of your DHCP server?

A: At the time of doing this lab, I was on SJSU's campus. The DCHP server is located at 10.211.55.1.

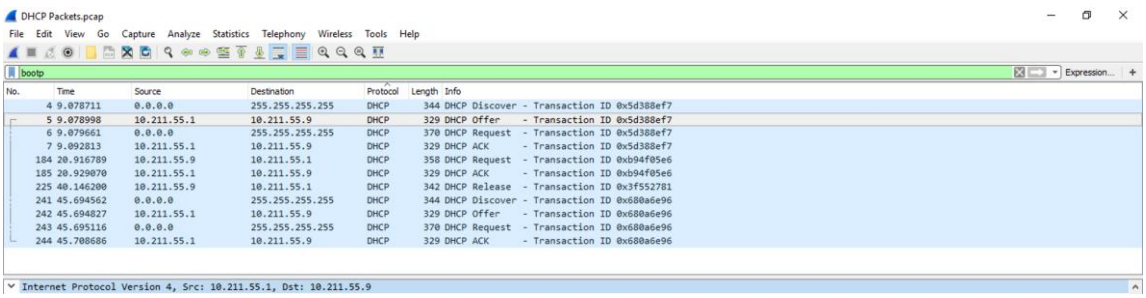

Figure 8: Screenshot showing IP address of DHCP server.

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.

A: Offered IP Address: 10.211.55.9

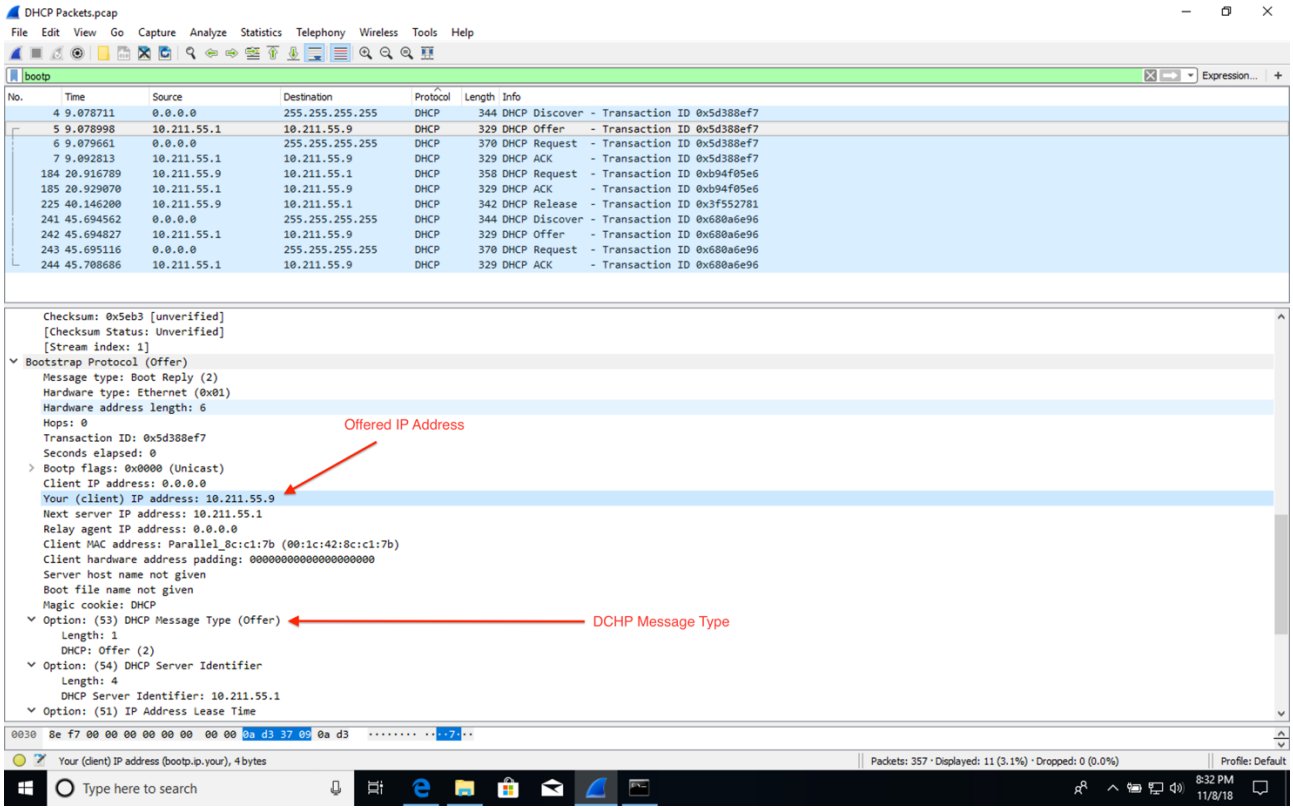

Figure 9: Screenshot showing offered IP address.

9) In the example screenshot shown 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?

A: The relay agent is present in the Bootstrap Protocol. In my case, there was no relay agent.

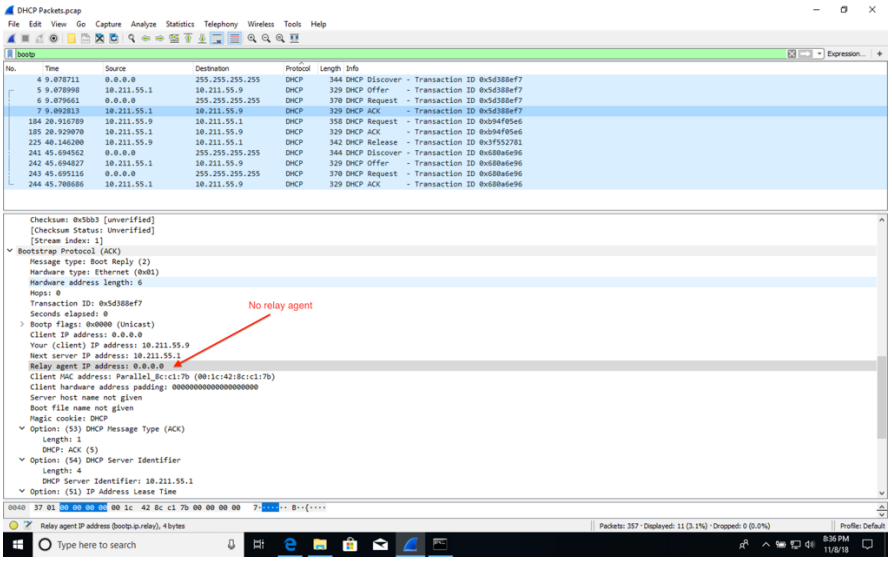

Figure 10: Screenshot showing no relay agent.

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

A: The subnet mask line tells the client which subnet mask to use. The router line tells the client where to send messages by default.

11) In the DHCP trace file noted in footnote 2, the DHCP server offers a specific IP address to the client. 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?

A: My host computer does not accept the IP address during the OFFER message. Instead, it makes a note of the given IP address and sends a REQUEST message to the DHCP server to request the ability to use that specific IP address. Only after the ACK has been given does my host accept the IP address. See screenshot:

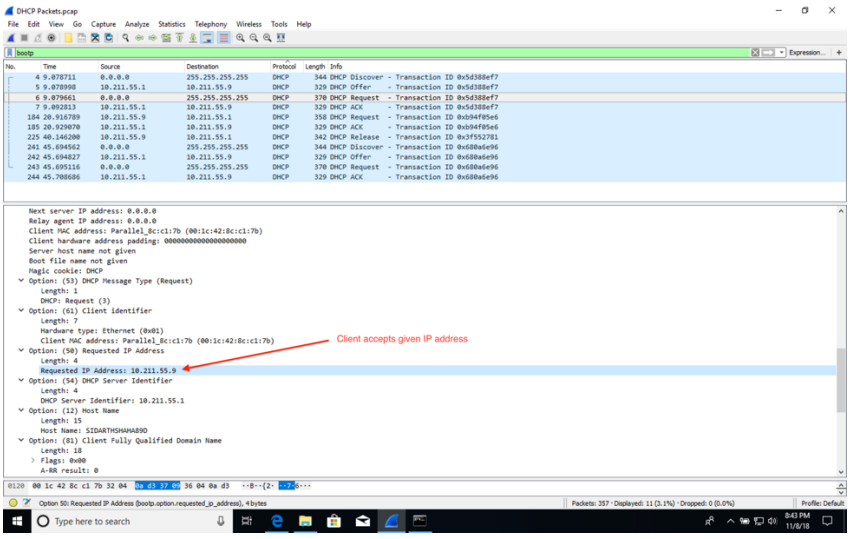

Figure 11: Screenshot showing the REQUEST message sent from my host. It contains the given IP address from the OFFER message.

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

A: The lease time tells the host how long they can use that specific IP address before a new one is issued to it. My given lease time is 30 minutes.

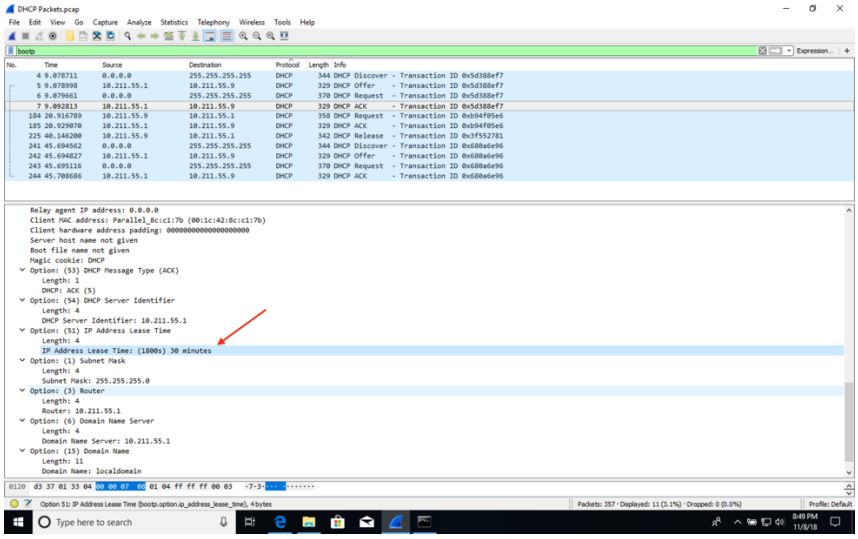

Figure 12: Screenshot showing lease time in ACK message.

13) What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgement of receipt of the client's DHCP request? What would happen if the client's DHCP release message is lost?

A: The DHCP release message sends a message to the DHCP server that my client will no longer use its IP address. The DHCP server can then reuse that IP address for another client. There is no acknowledgement message from the server back to my client. In the event that the release message is not received by the server, my client's old IP address would be inaccessible and unable to be reassigned by the server until the lease expires on the IP address.

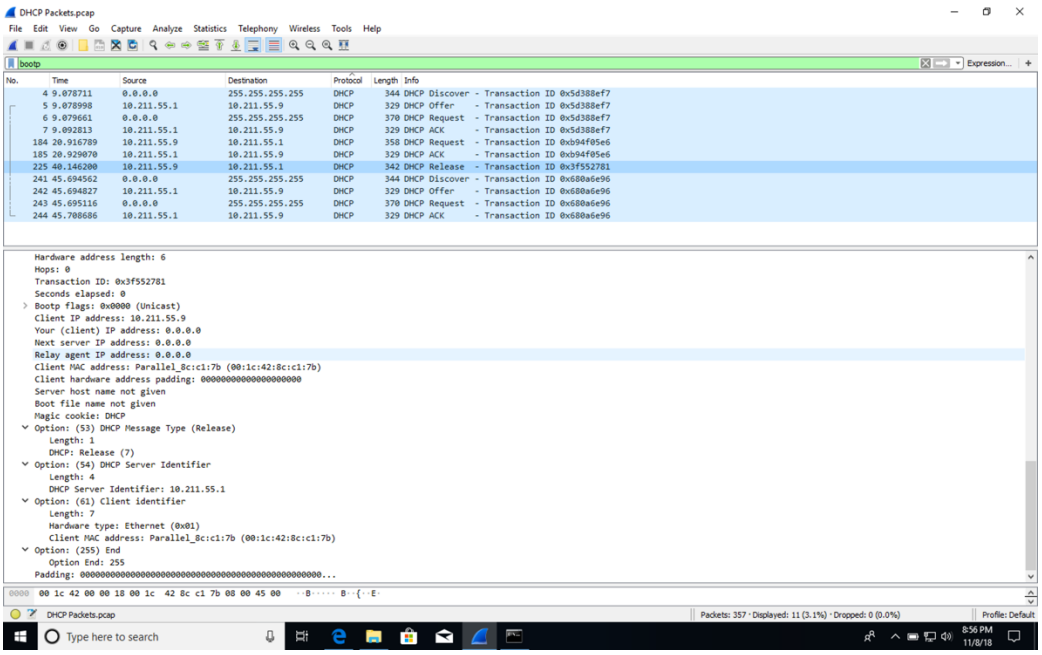

Figure 13: Screenshot showing DHCP Release message from my client.

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.

A: I see no ARP packets sent between my client's exchange with the DHCP server. Instead, I see ARP packets before my messages were sent. They appear to by the DISCOVER broadcast message at work. My client PC is requesting the address of the DHCP server and other devices are replying with it's address on the network.

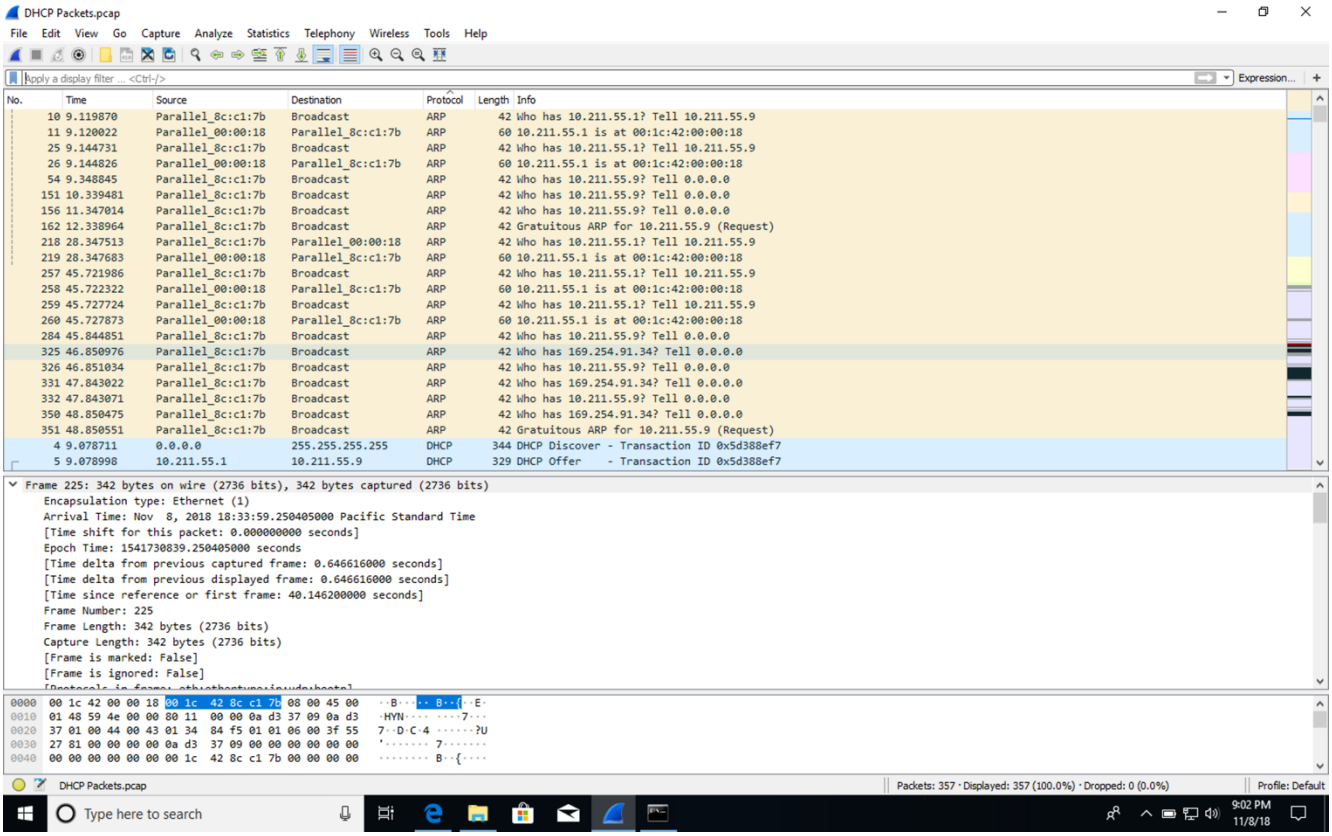

Figure 14: Screenshot showing ARP messages BEFORE my client's DHCP messages.