Wireshark DHCP

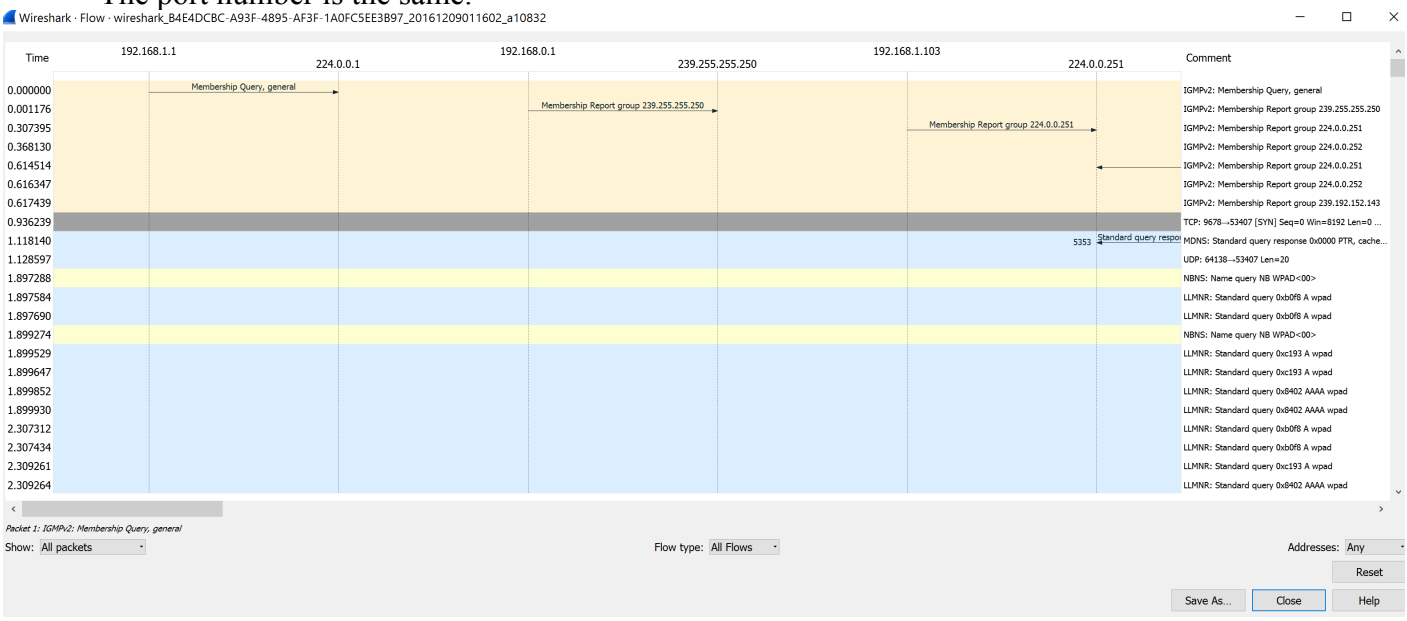
```
   Connection-specific DNS Suffix  . :

C:\Windows\System32>ipconfig /renew

Windows IP Configuration

No operation can be performed on Local Area Connection* 2 while it has its media disconnected.
No operation can be performed on Ethernet 3 while it has its media disconnected.
No operation can be performed on Bluetooth Network Connection while it has its media disconnected.

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : Fcname
   Link-local IPv6 Address . . . . . : fe80::78f3:ba61:5d0f:5b6b%9
   IPv4 Address. . . . . . . . . . . : 192.168.1.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Tunnel adapter isatap.Fcname:

   Connection-specific DNS Suffix  . : Fcname
   Link-local IPv6 Address . . . . . : fe80::5efe:192.168.1.10%13
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 4:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Windows\System32>
```

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

   DHCP messgage sent via UDP

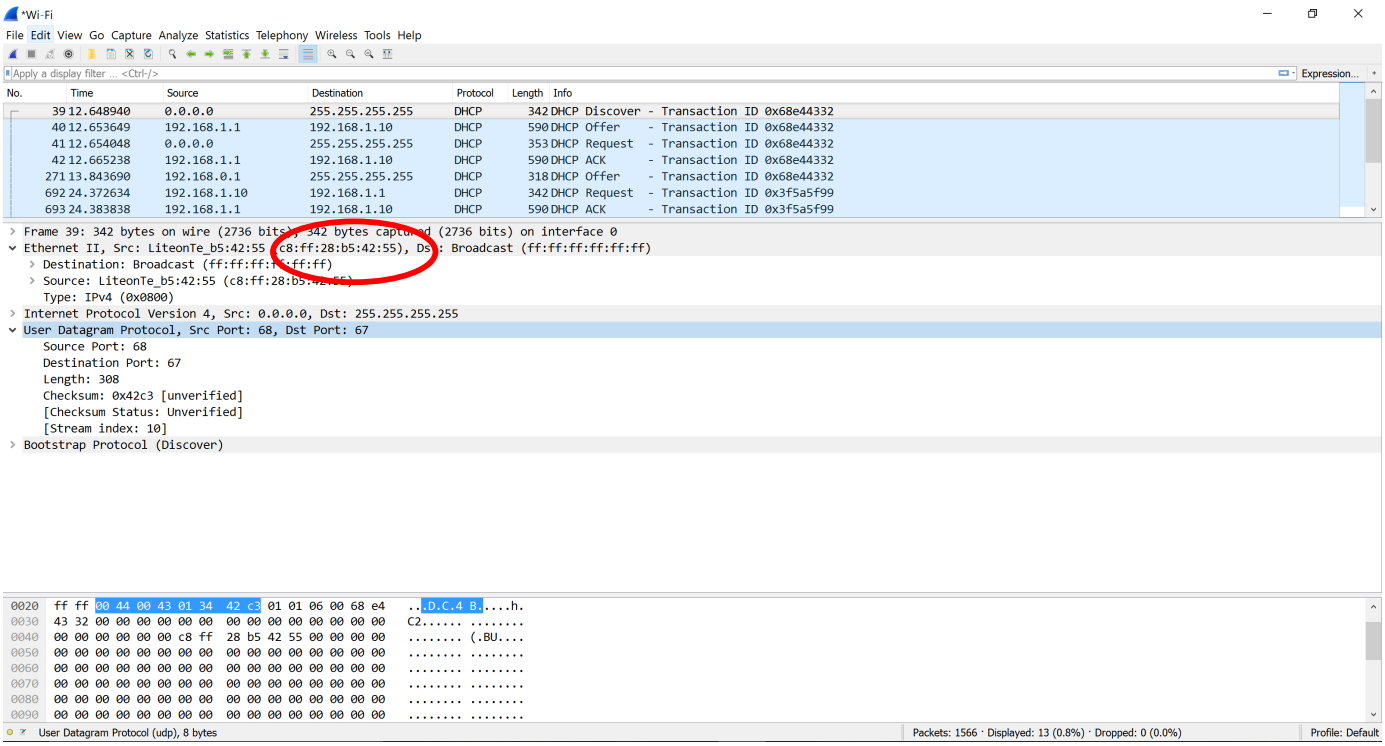
2. **Draw a timing datagram illustrating the sequence of the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server. For each packet, indicated the source and destination port numbers. Are the port numbers the same as in the example given in this lab assignment?**

   The port number is the same.



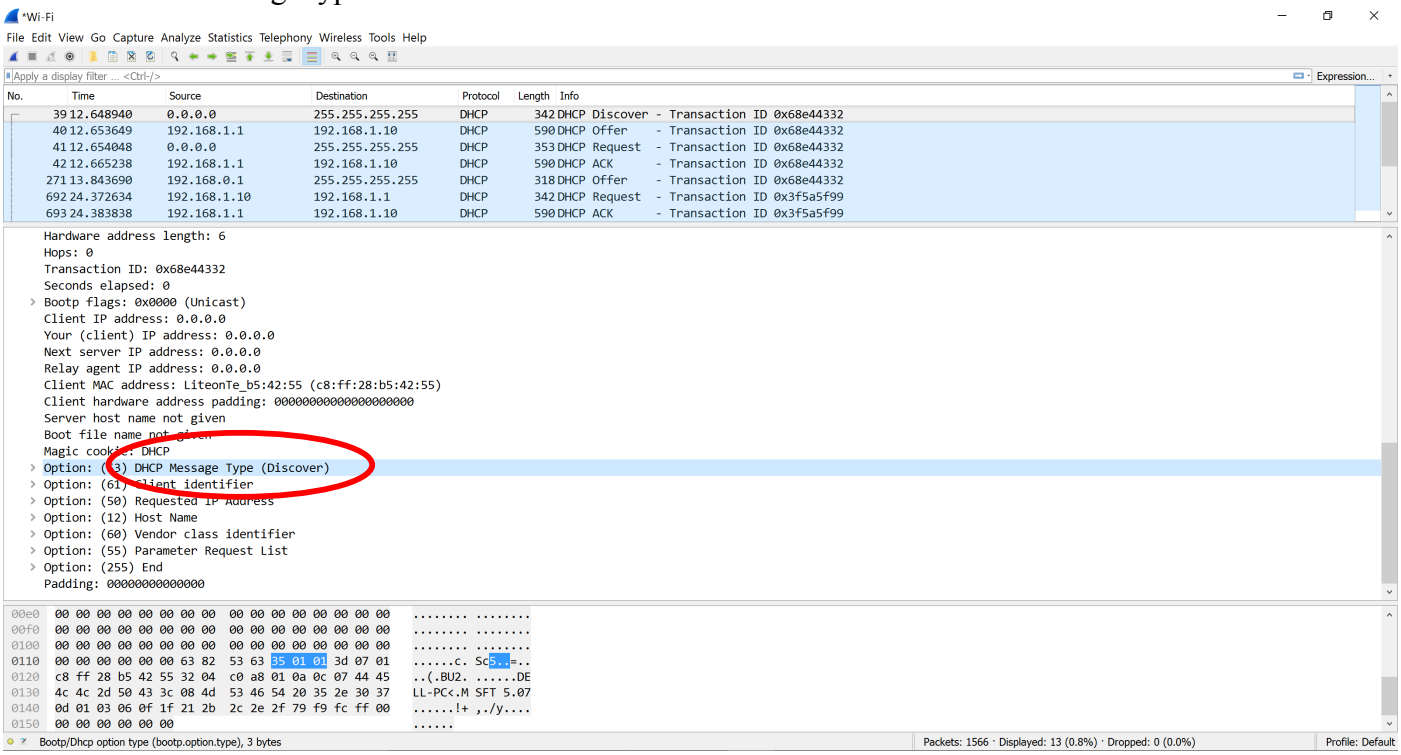
3. **What is the link-layer (e.g., Ethernet) address of your host?**

The ethernet address host: c8:ff:28:b5:42:55



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

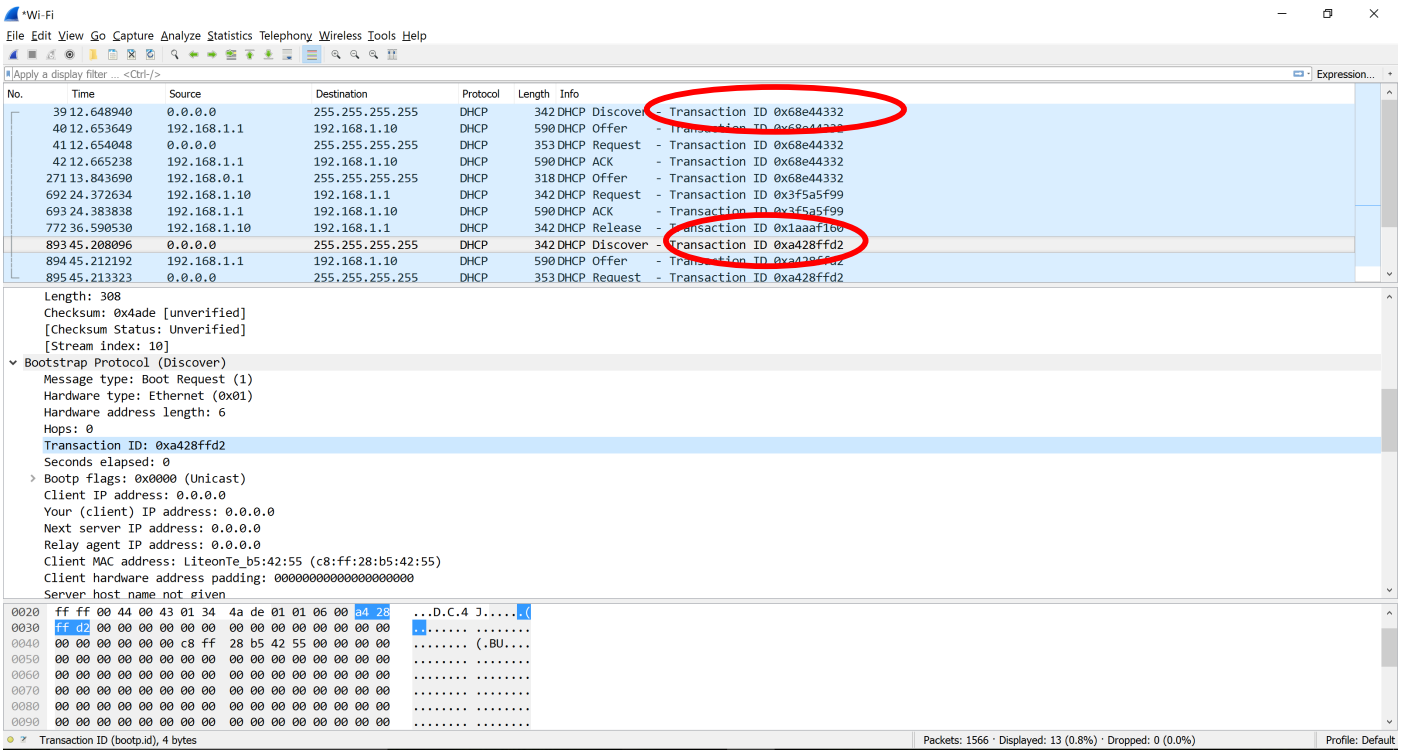
DHCP message type



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?**

DHCP message type

First set: Transaction ID: 0x68e44332
Second set: Transaction ID: 0xa428ffd2



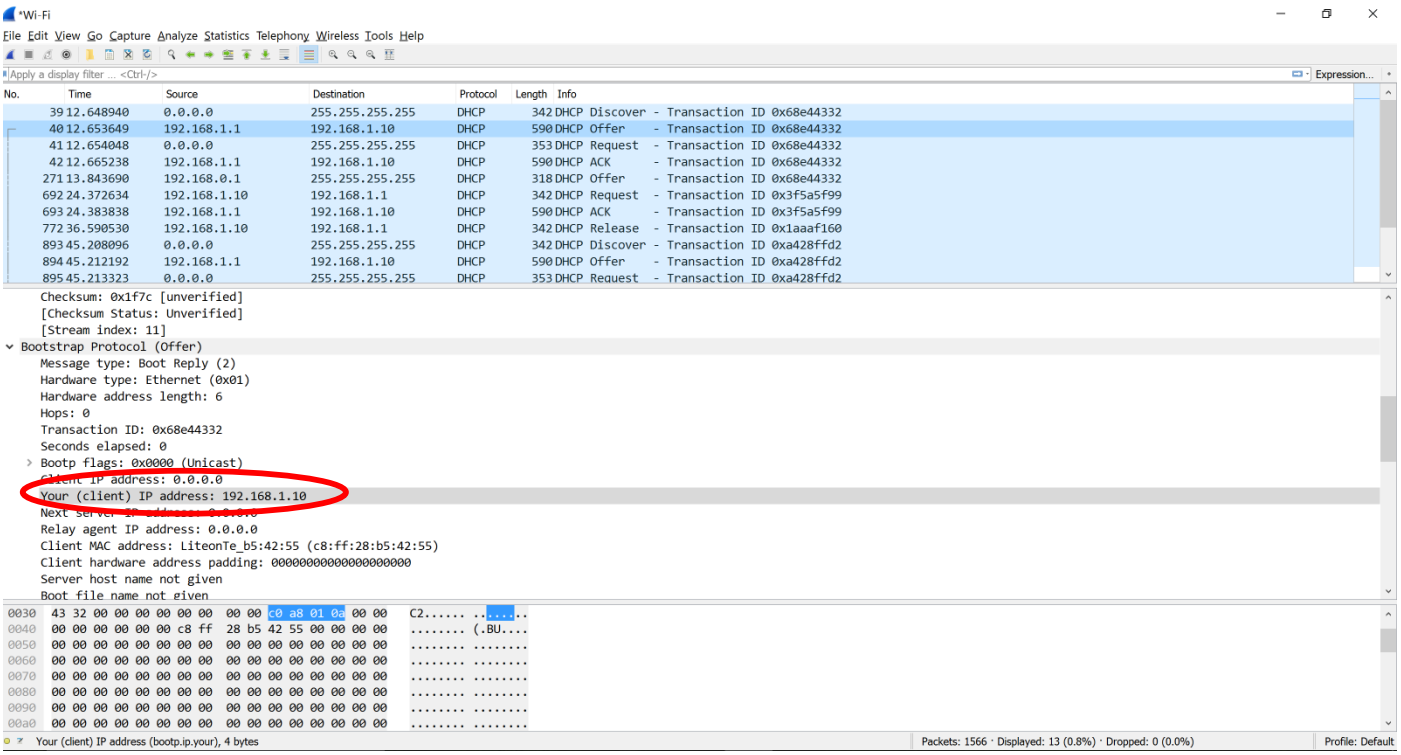
The purpose is for the host to differentiate between different requests from user.

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.**

39	12.648940	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID 0x68e44332
40	12.653649	192.168.1.1	192.168.1.10	DHCP	590 DHCP Offer - Transaction ID 0x68e44332
41	12.654048	0.0.0.0	255.255.255.255	DHCP	353 DHCP Request - Transaction ID 0x68e44332
42	12.665238	192.168.1.1	192.168.1.10	DHCP	590 DHCP ACK - Transaction ID 0x68e44332

7. **What is the IP address of your DHCP server?**
   192.168.1.1

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.
   IP: 192.168.1.10



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?**

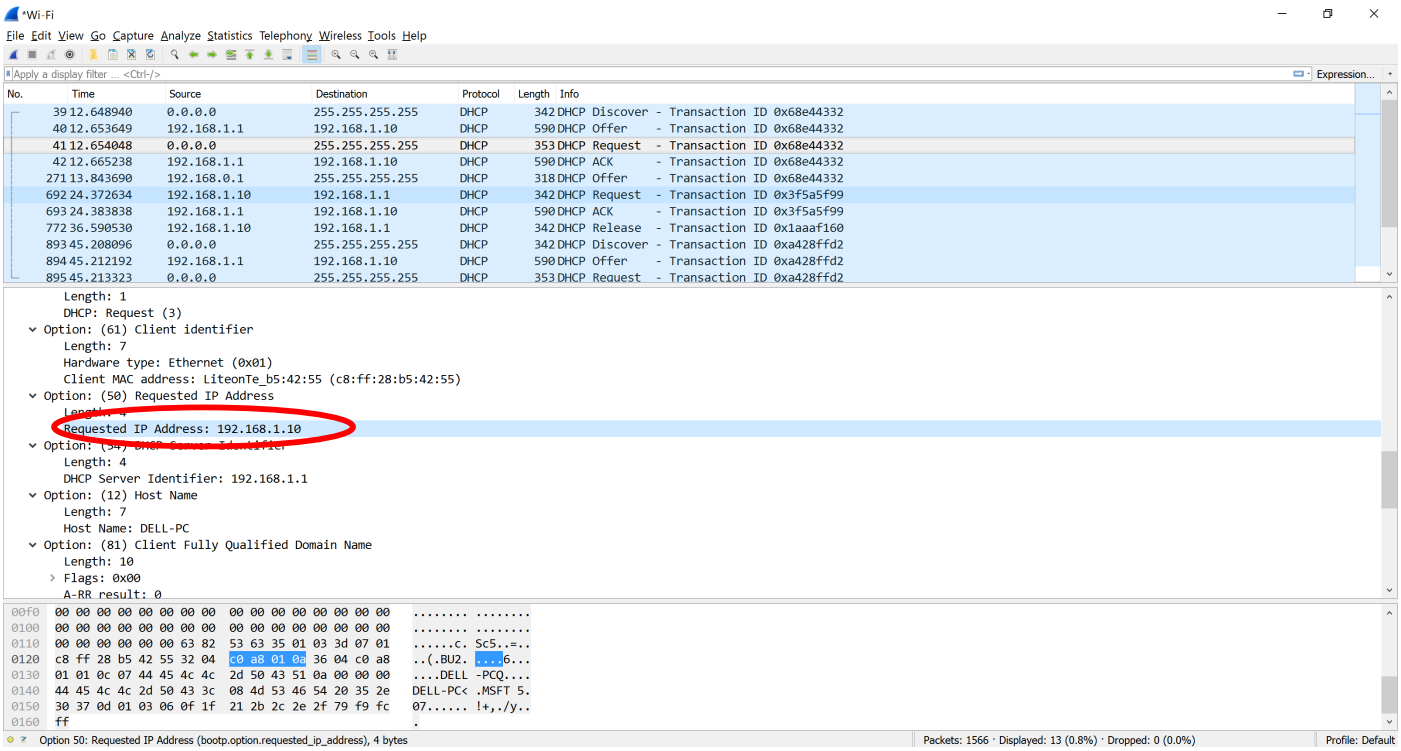
   The value that indicate no relay agents is 0.0.0.0

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

    The router line indicates to the client what its default gateway should be. The subnet mask line tells the client which subnet mask it 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?**

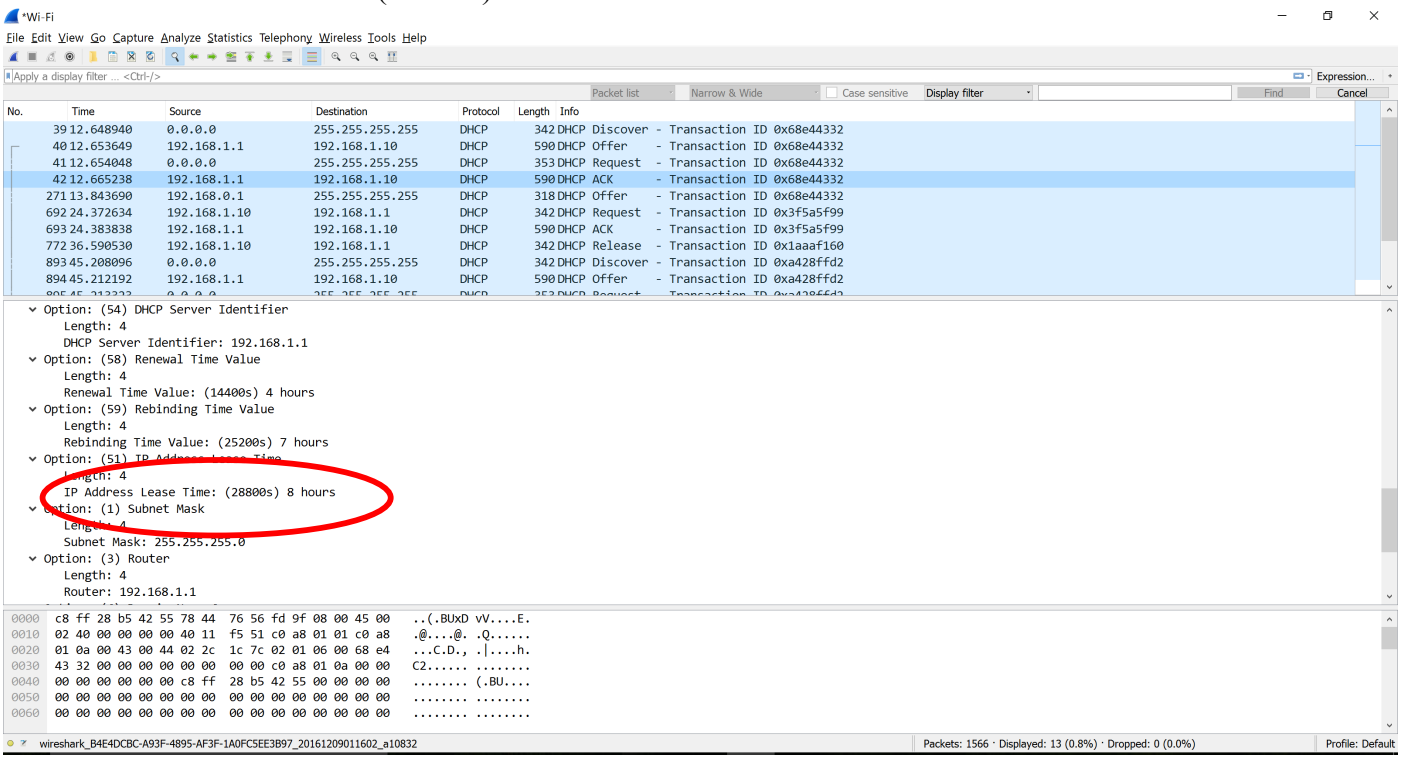
    The client accepts the ip address.
    Requested IP Address: 192.168.1.10



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

How long they can use the address assigned by the server before they will have to be assigned a new one.

Lease time is 28800s (8 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 happe if the client's DHCP release message is lost?

The purose is to releasr the IP address back to the server.
The DHCP server does not send a message back to the client acknowledging the DHCP Release message.
If the DHCP Release message from the client is lost, the DHCP server would have to wait until the lease period is over for that IP address until it could reuse it for another 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.

Yes. Before offering an IP address to a client, the DHCP server issues an ARP request for the offered IP to make sure the IP address is not already in use by another workstation.