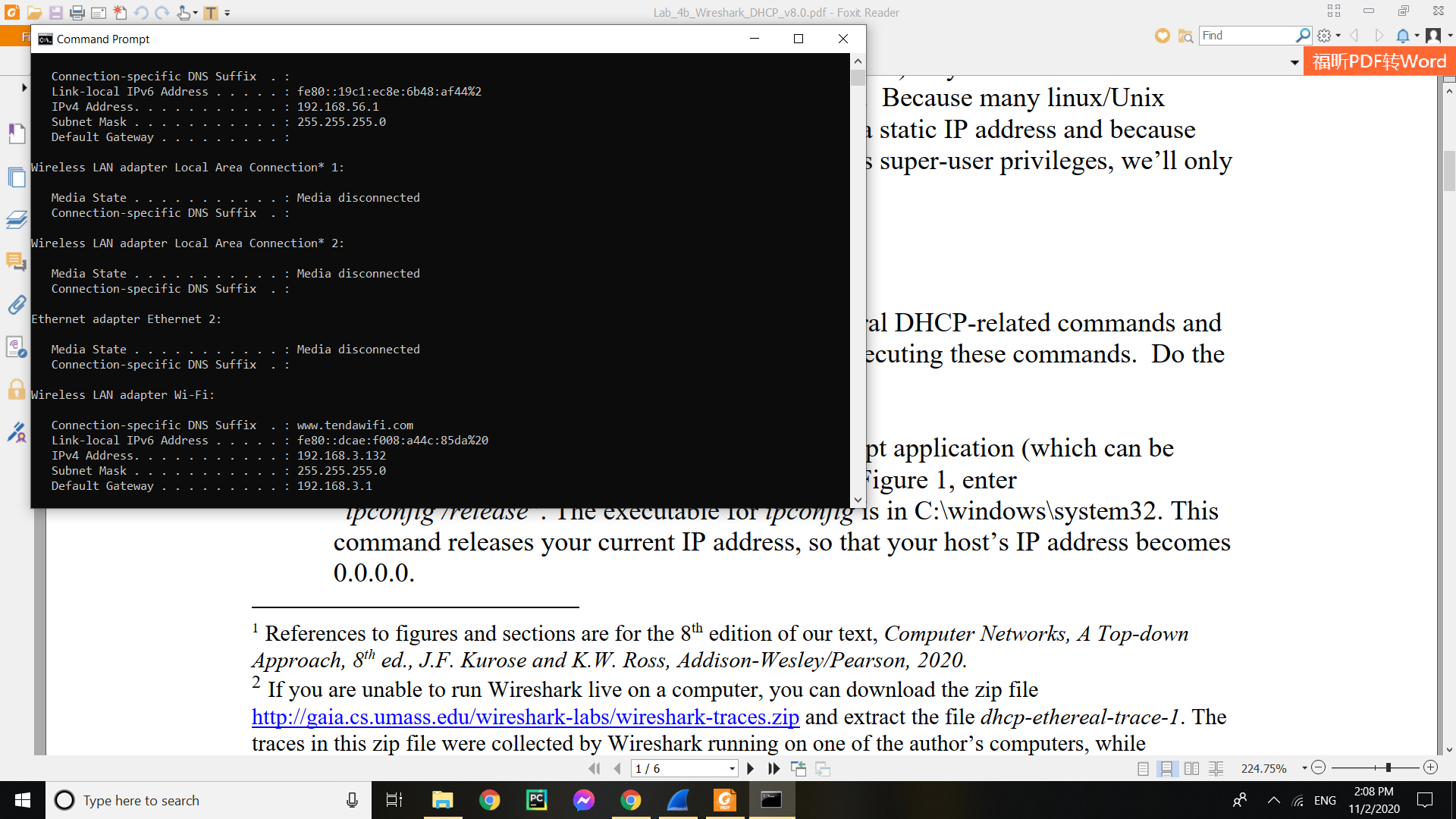
**Computer Network**

**Wireshark Lab 3a: UDP v8.0**

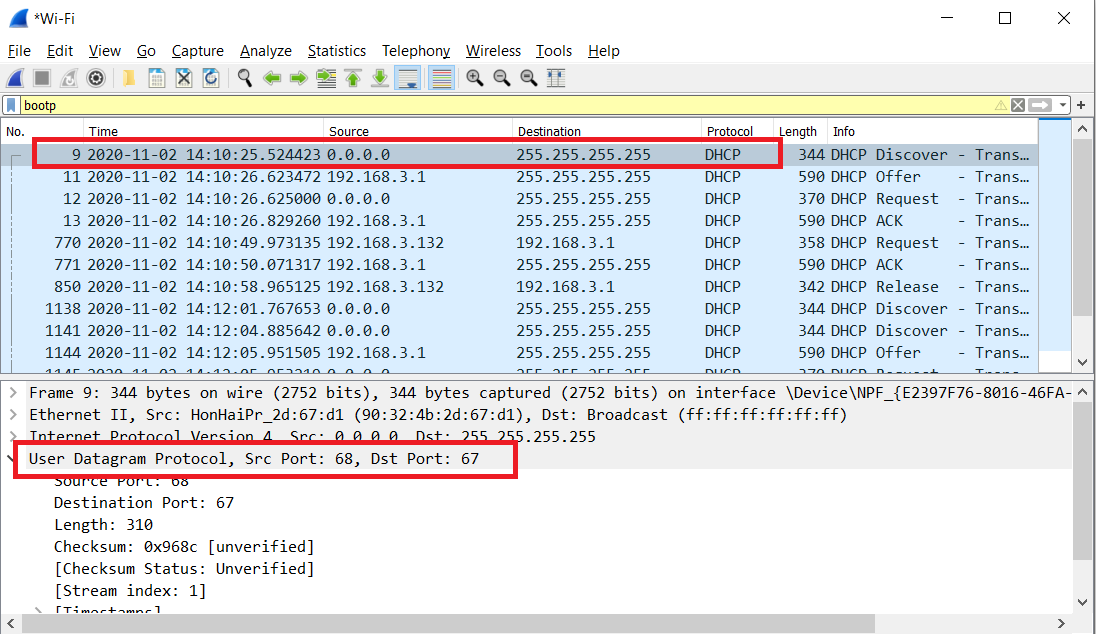
***Lecturer: Mr. Nguyễn Mạnh Thìn***

***Student: Trần Quốc Anh - 1852247***



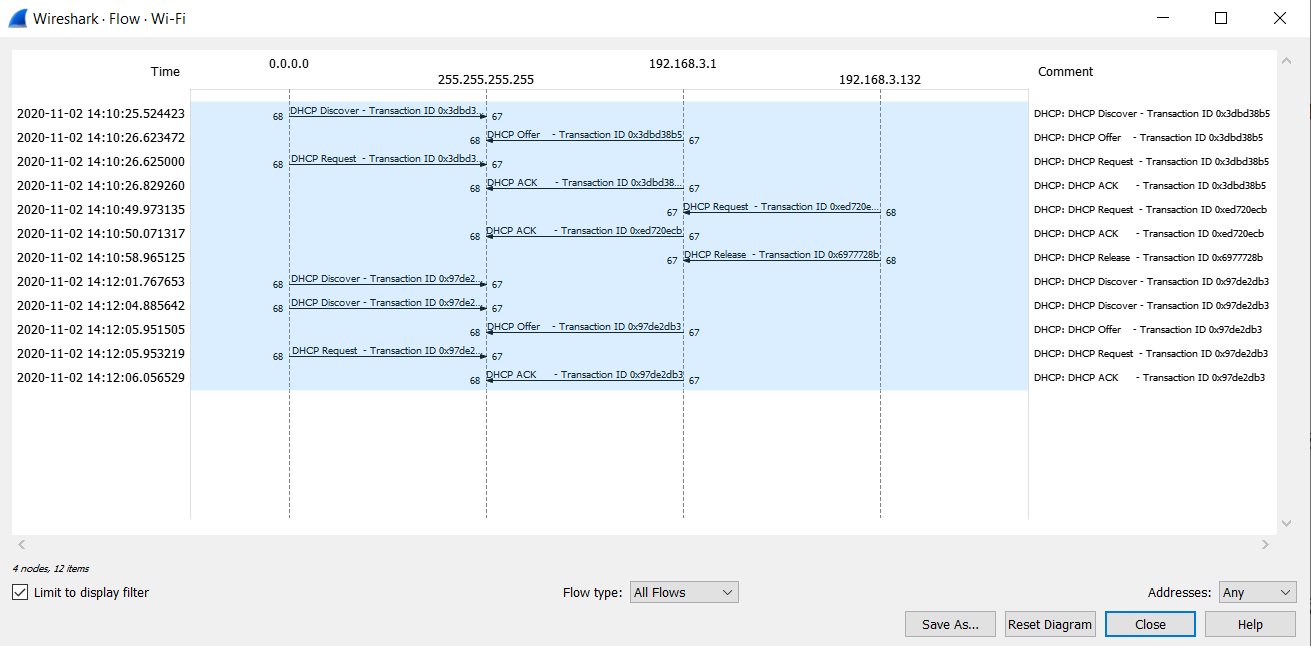
1. **Are DHCP messages sent over UDP or TCP?**

* DHCP messages are sent over UDP



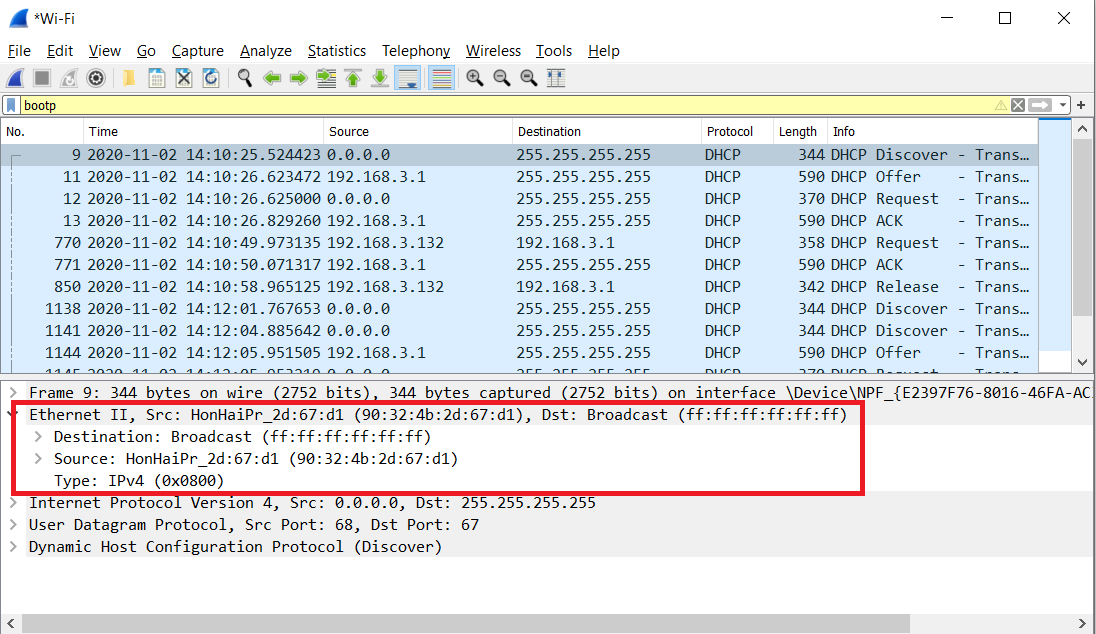
1. **Draw a timing datagram illustrating the sequence of the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server. For each packet, indicated the source and destination port numbers. Are the port numbers the same as in the example given in this lab assignment?**

* The Discover packet has a source port of 68 and destination port of 67
* The Offer packet has a source port of 67 and a destination port of 68
* The Request packet has a source port of 68 and a destination of 67
* The ACK packet has a source port of 67 and a destination of 68



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

* The link-layer address of my host is: 90:32:4b:2d:67:d1



1. **What values in the DHCP discover message differentiate this message from the**

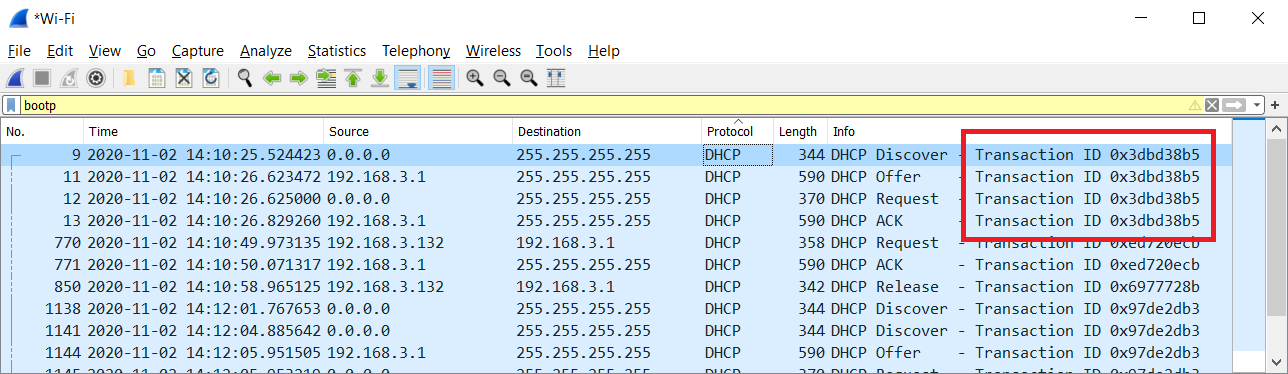
**DHCP request message?**

* DHCP Message Type
* Request includes a server identifier field

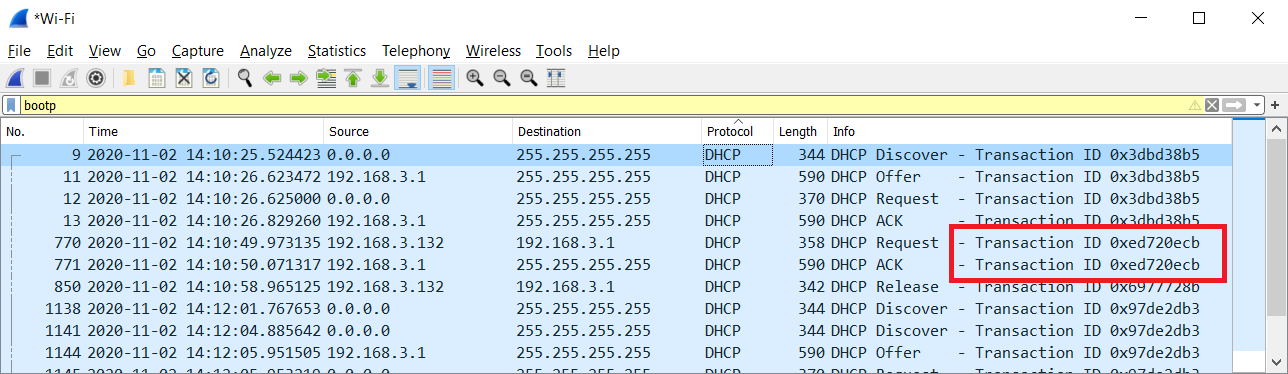
1. **What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What are the values of the**

**Transaction-ID in the second set (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field?**

* First set of messages: 0x3dbd38b5



* Second set of messages: 0xed720ecb



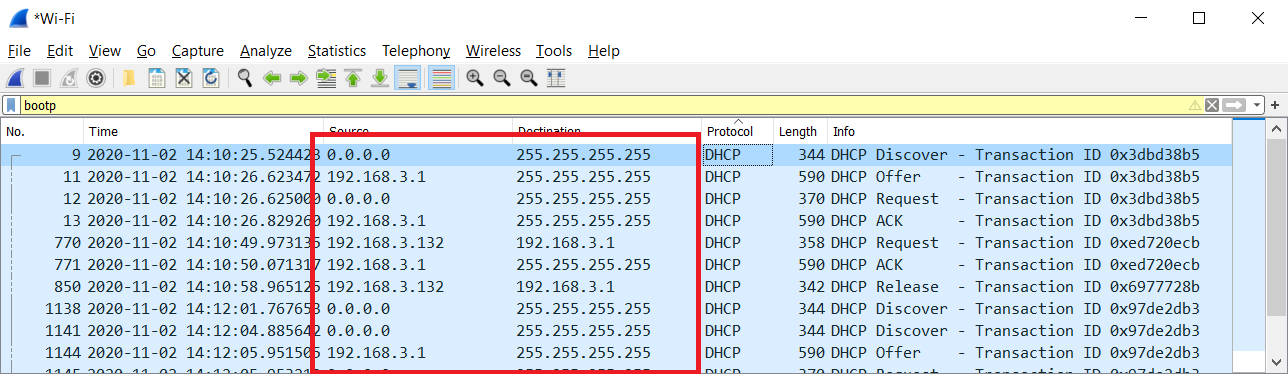
* Purpose: The transaction ID is different so that the host can differentiate between different requests made by the user.

1. **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**

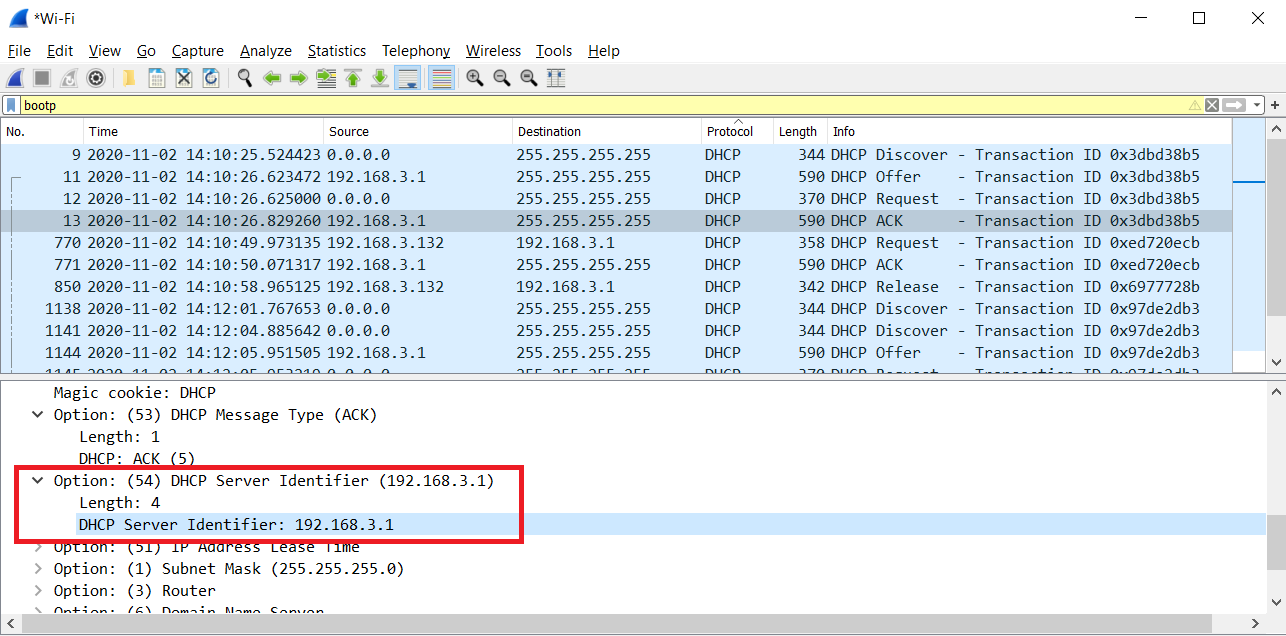
**address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? For each of the four DHCP messages (Discover/Offer/Request/ACK DHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.**

* Discover: 0.0.0.0/255.255.255.255
* Offer: 192.168.3.1/255.255.255.255
* Request: 0.0.0.0/255.255.255.255
* ACK:192.168.3.1/255.255.255.255



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

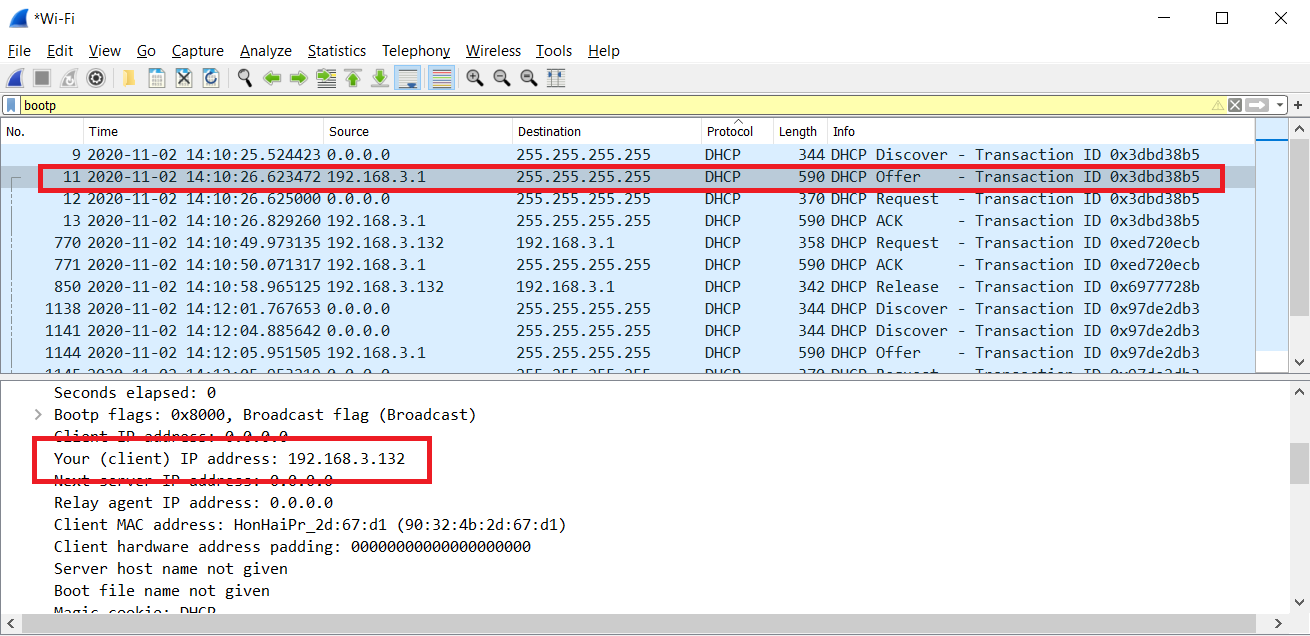
* The IP address of my DHCP server is: 192.168.3.1



1. **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.**

* My client is offered 192.168.3.132 by the DHCP server. The offer message contains the DHCP address offered by the server



1. **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?**

* In the example given, the value that indicates there is no relay agent is 0.0.0.0, in the case of my capture, I also have a value for the relay agent of 0.0.0.0 indicating that I too did not have a relay agent.

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

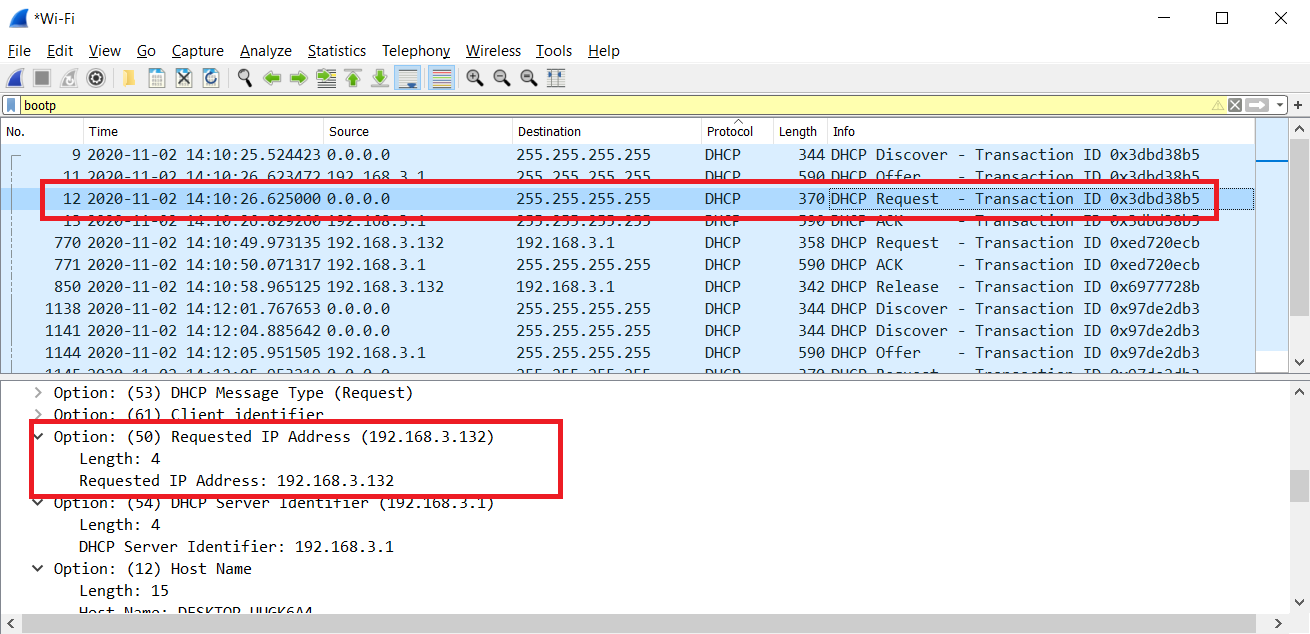
**message.**

* The subnet mask line tells the client which subnet mask to use.
* The router line indicates where the client should send messages by default.

1. **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?**

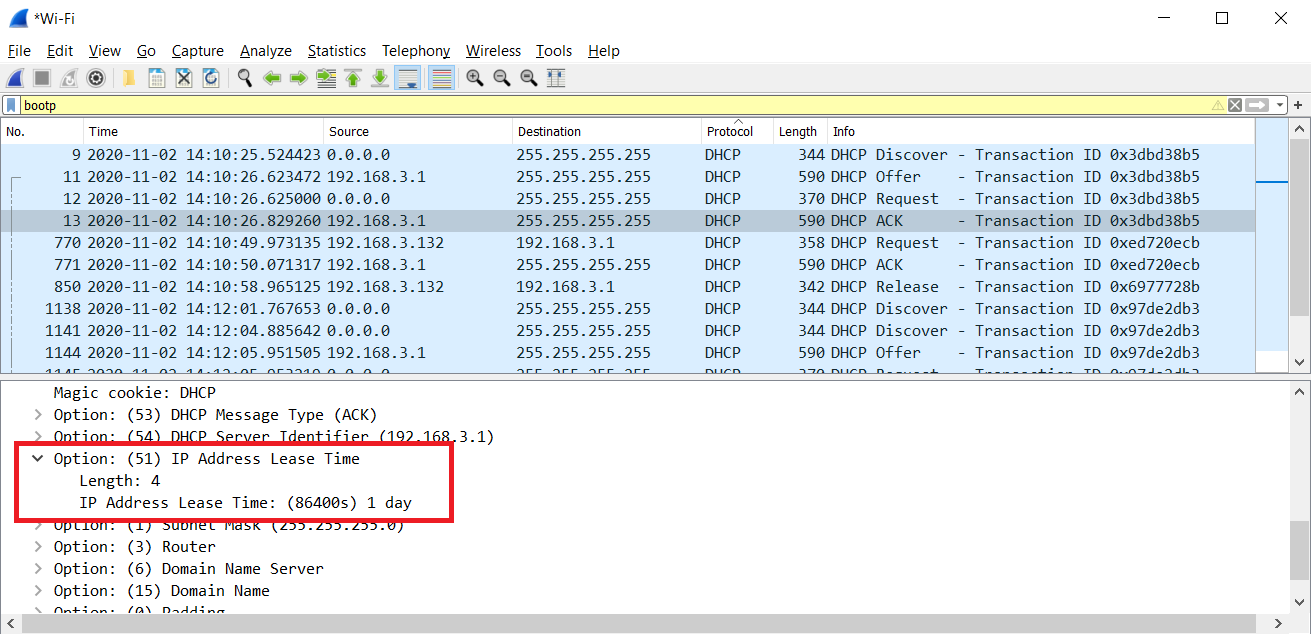
* The client accepts the IP address given in the offer message within the request message. After being offered the IP address 192.168.3.132 in the offer message, my client sent back a message further requesting that specific IP address.



1. **Explain the purpose of the lease time. How long is the lease time in your**

**experiment?**

* The purpose of lease time is to tell the client how long they can use the specific IP address assigned by the server before they will have to be assigned a new one.
* The lease time in my experiment is 86400 seconds or 1 day



1. **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?**

* The purpose of the release message is to release the IP address back to the server.
* There is no verification that the release message has been received by the server.
* If the message is lost, the client releases the IP address, but the server will not reassign that address until the clients lease on the address expires.

1. **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, they appear to be broadcasts sent out by the network to build up the known IP addresses by the clients network.

