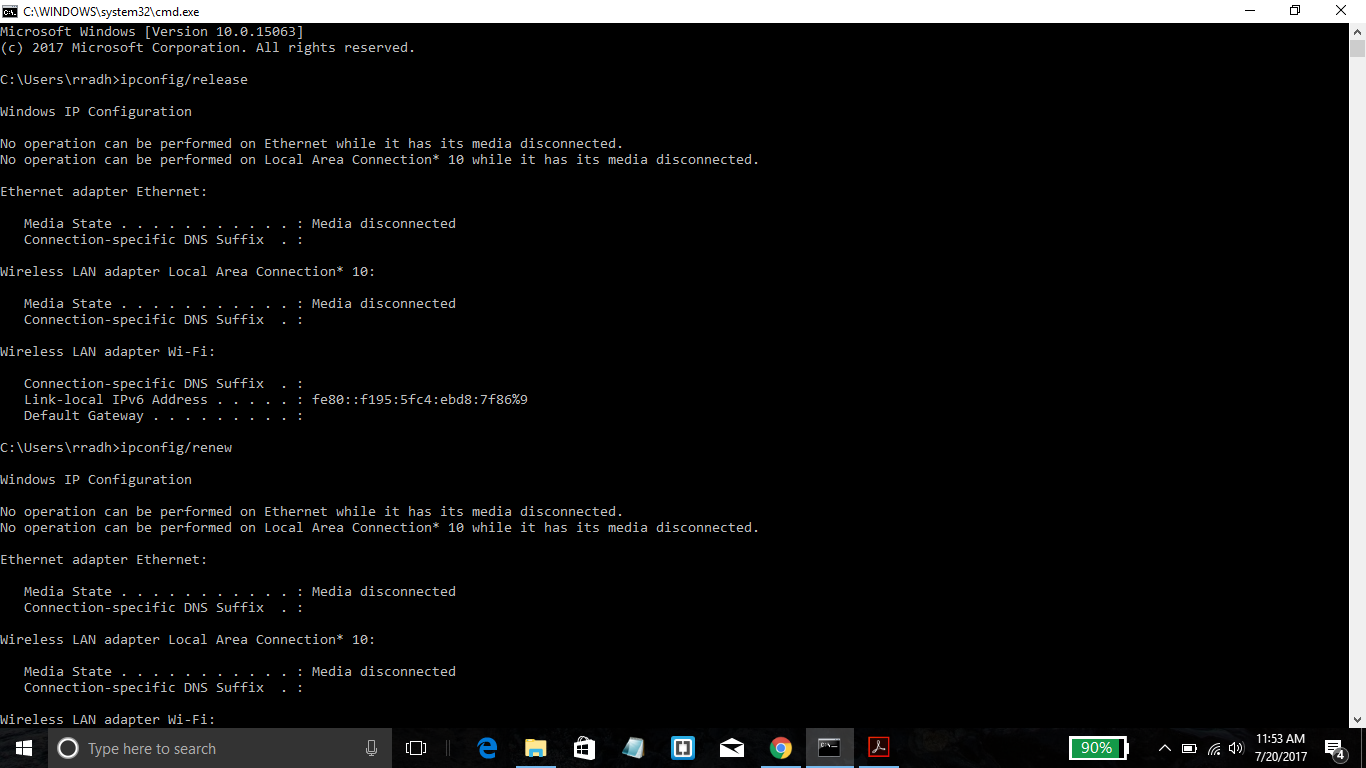
**CMD PROMPT SCREENSHOT**



**Part 1 : DHCP**

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

UDP

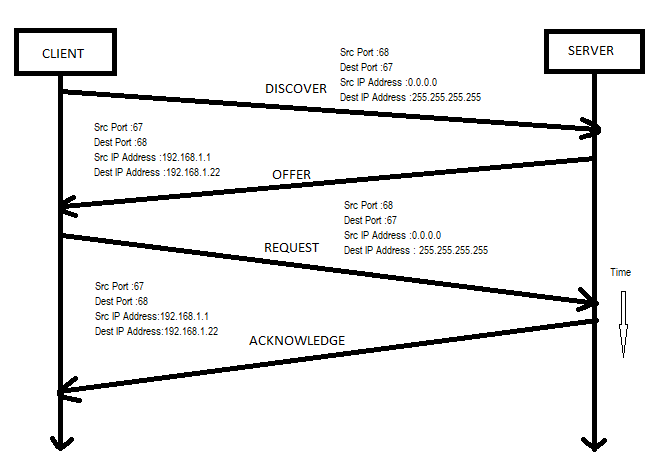


**2.Does DHCP use client-server or peer to peer architecture? No snapshot needed.**

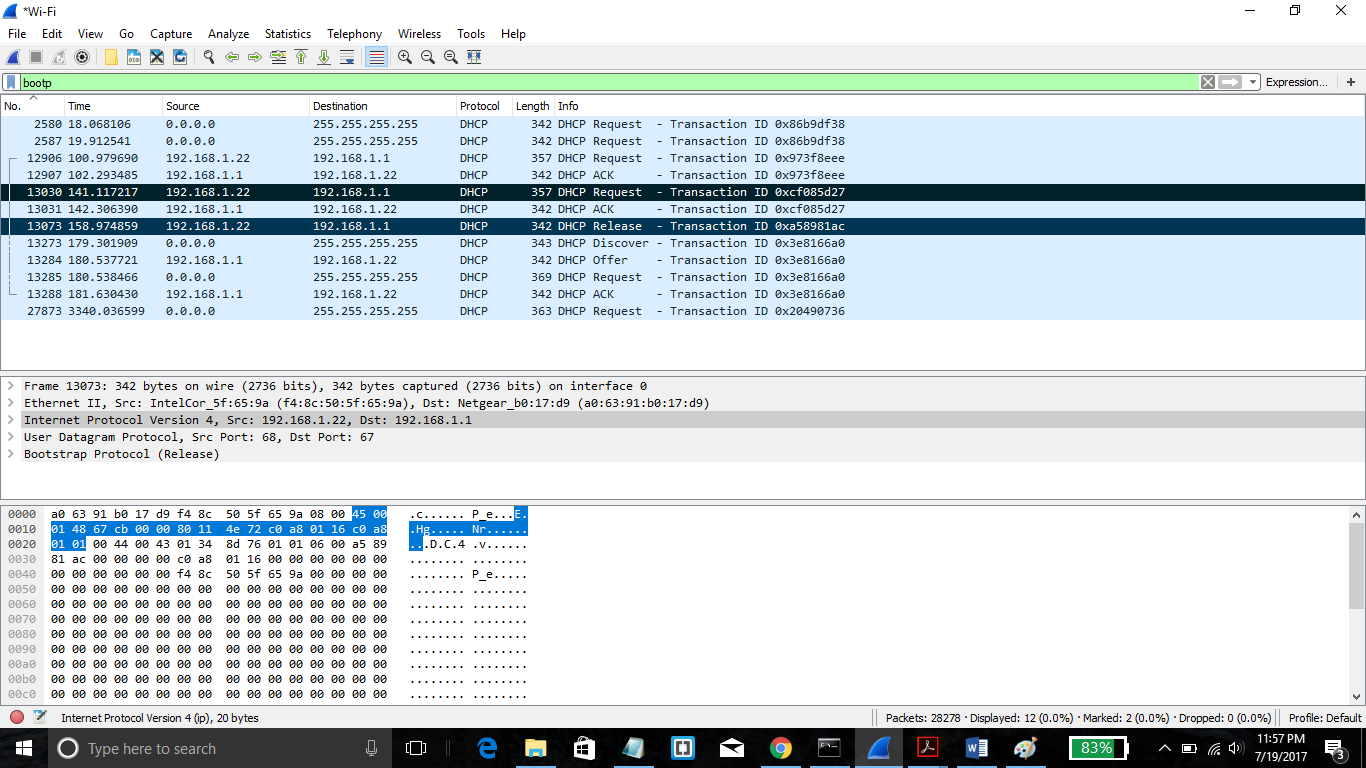
DHCP uses client-server architecture

**3.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 and IP addresses.**

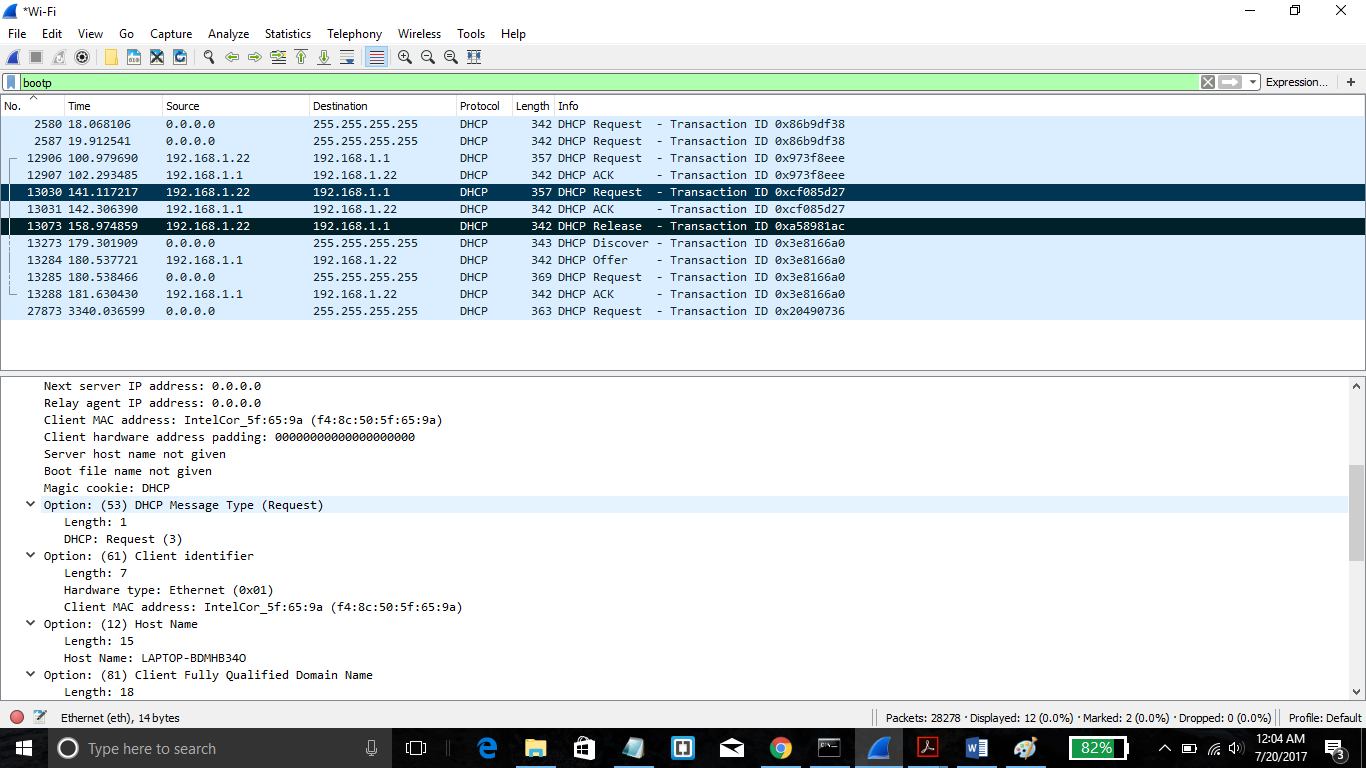
**4. What is the link-layer (e.g., Ethernet) address of your host in hex format?**

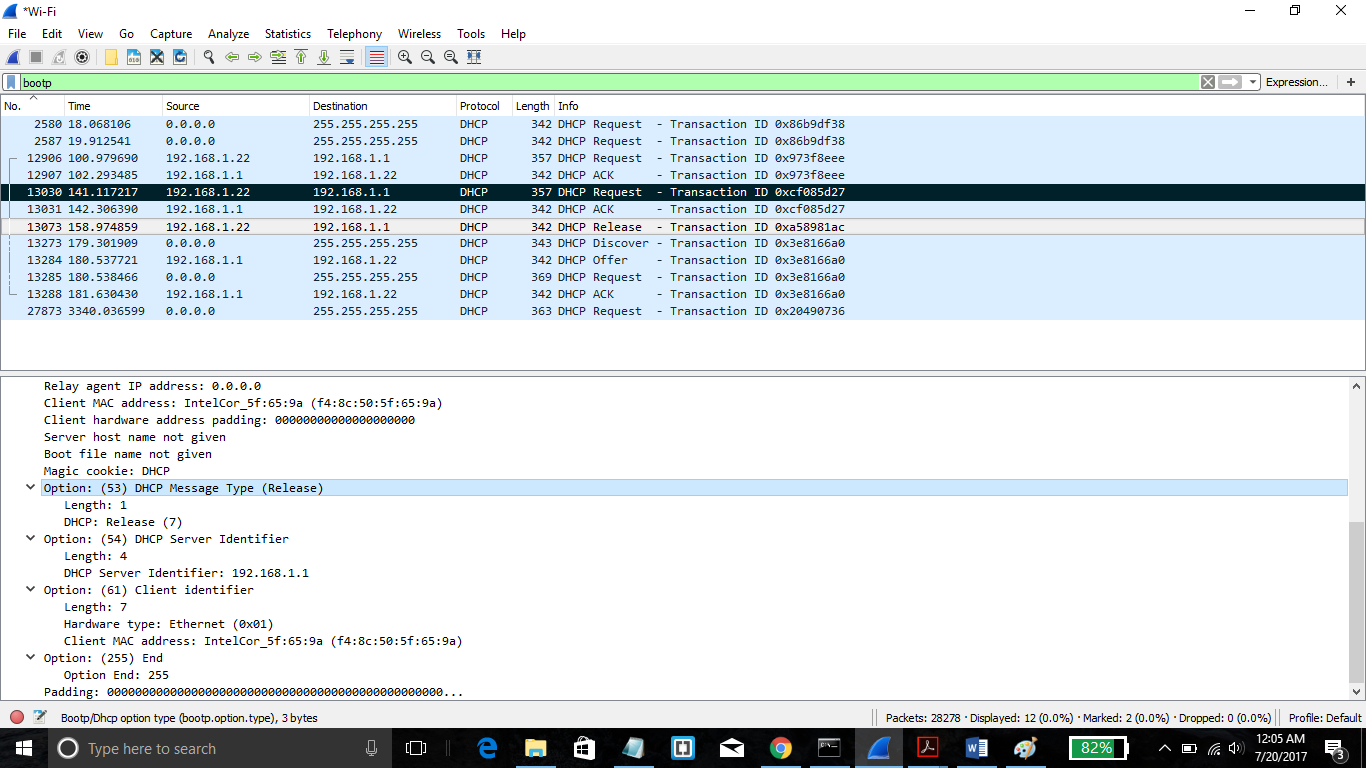
The link layer address of my host is f4:8c:50:5f:65:9a



**5. What values in the DHCP Discover message differentiate this message from the**

**DHCP Request message?**





The value in the DHCP Discover message that differentiates this message from the

DHCP Request message is option 53.

**6. What is the value of the Transaction-ID in each of the first four DHCP messages?**

**What are the values of the Transaction-ID in the second set (Request/ACK) set of**

**DHCP messages? Why do we need the Transaction-ID field?**



The value of the Transaction-ID in each of the first four DHCP messages is 0x973f8eee. The values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages is 0x3e8166a0.

**7. 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 first four**

DHCP messages (Discover/Offer/Request/ACK DHCP), indicate the source and

destination IP addresses that are carried in the encapsulating IP packet.



**Discover IP address   =  255.255.255.255**  
**Offer IP address          =  192.168.1.22**  
**Request IP address    =  255.255.255.255**  
**ACK IP address           =  192.168.1.22**

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



The IP address of my DHCP server is 192.168.1.1

**9. What IP address is the DHCP server offering to your host in the DHCP Offer**

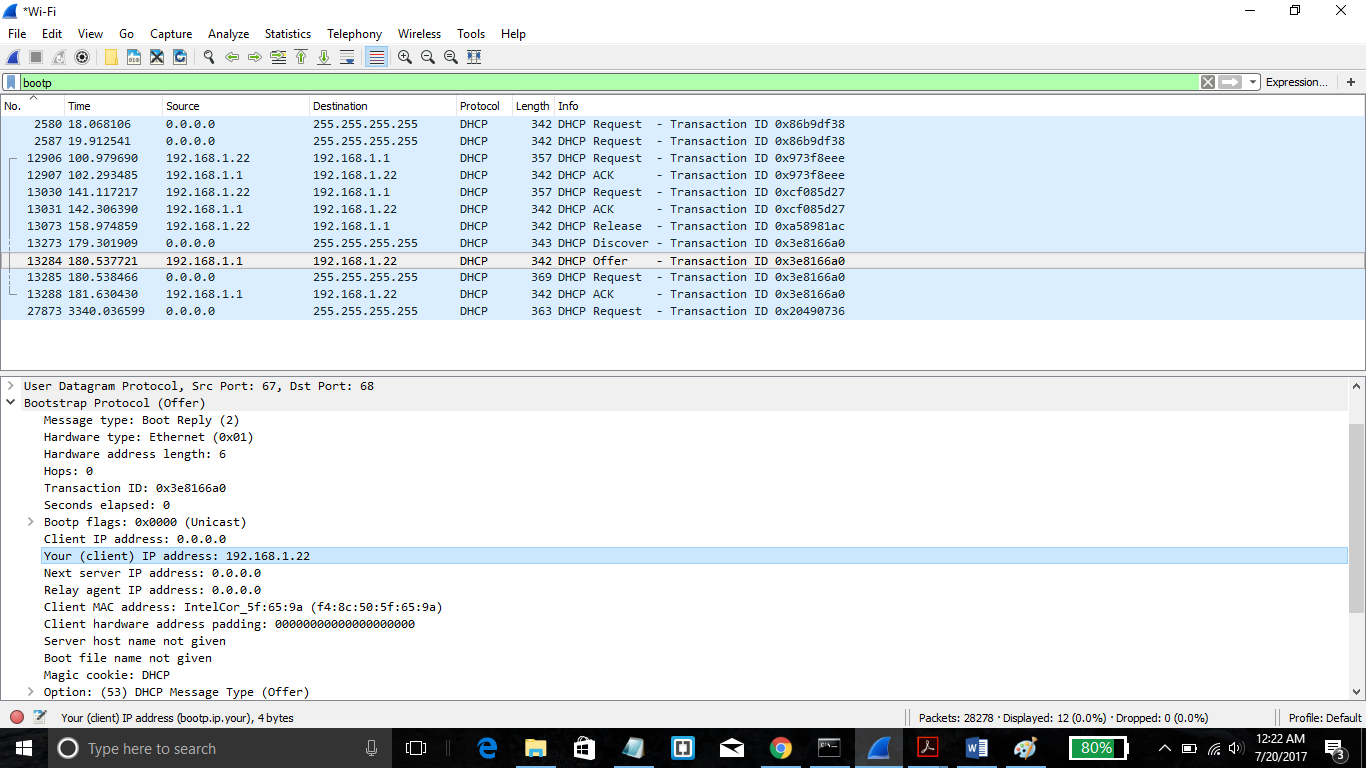
**message and what is the lease time? Which DHCP messages have this IP Address**

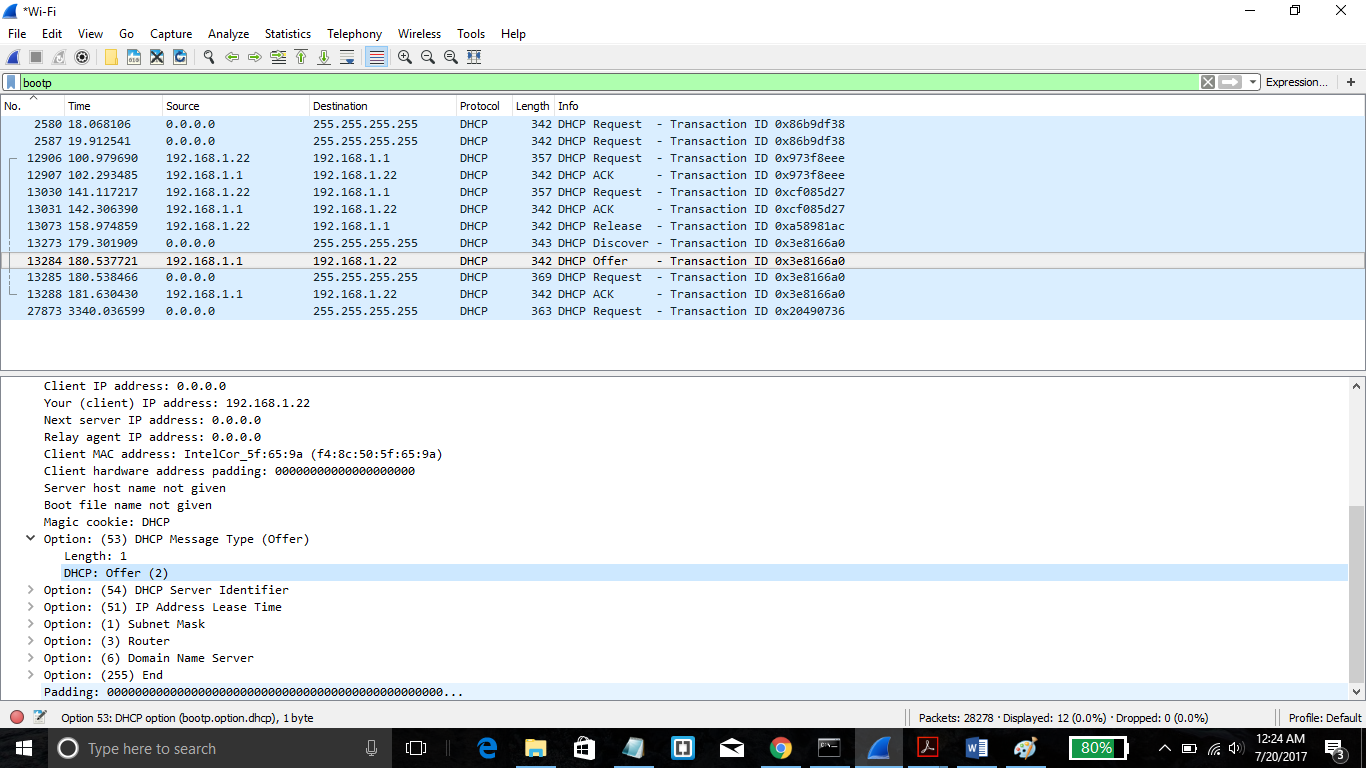
**in them?**

**The IP address in which the DHCP server is offering to my host in the DHCP Offer message is**

**192.168.1.1.**

**Option 53 contains the DHCP Message type with a length of 1 and the DHCP offer is (2).**





**10. Apart from IP Address, what other information does DHCP server provide to the**

**client?**

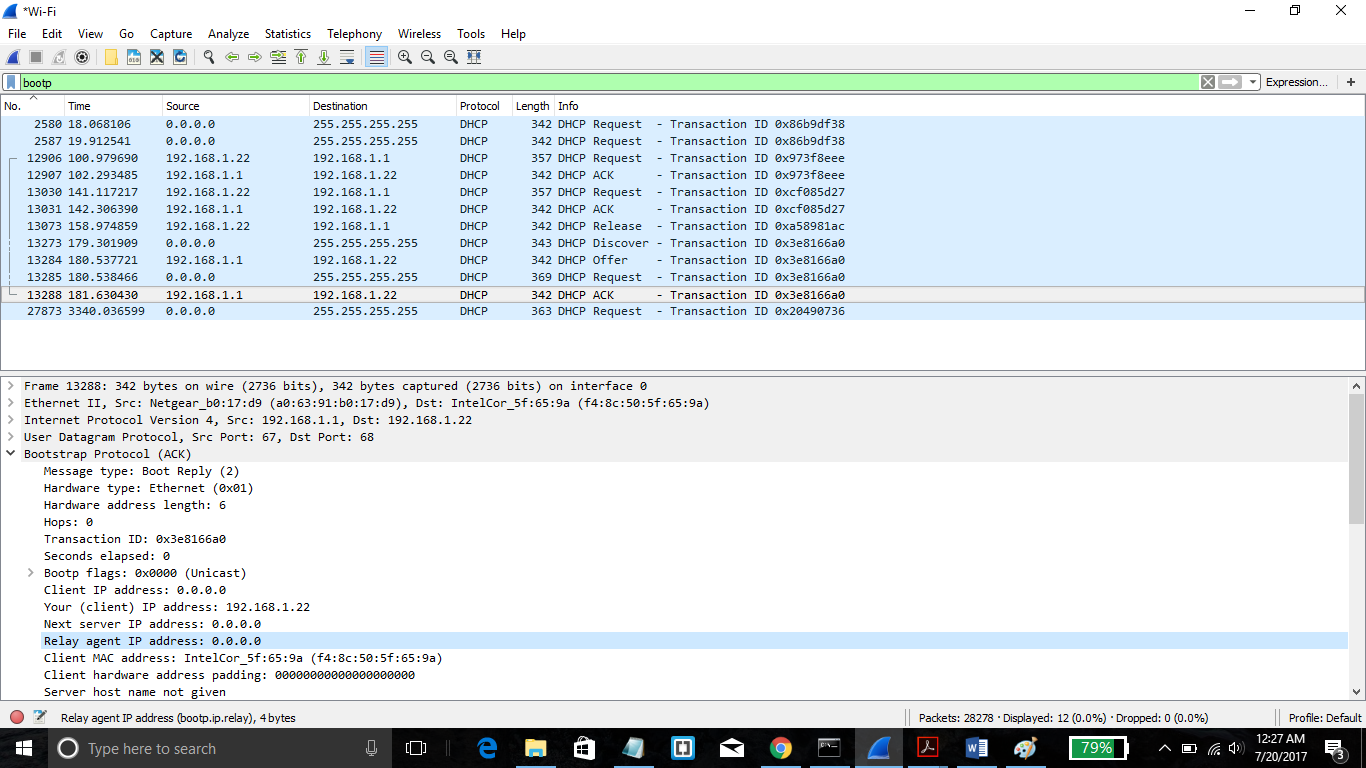
Apart from IP address DHCP provides subnet mask, Default Gateway IP address, DNS server IP address. In case of IP phones DHCP plays an important role by directly or indirectly providing the Call server IP address on which the IP phones can register themselves.

**11. 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**

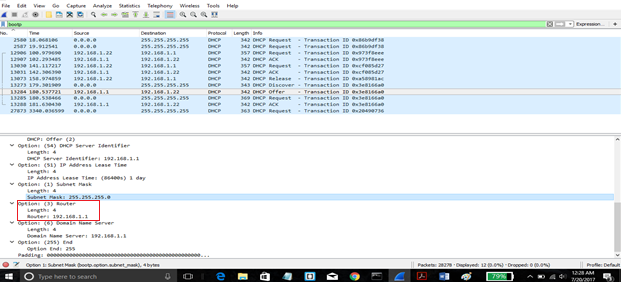
**the agent?**



There is no relay agent in my experiment. The relay agent value is 0.0.0.0 which denotes the absence of it.

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

**message and indicate the IP address of the default gateway (router).**

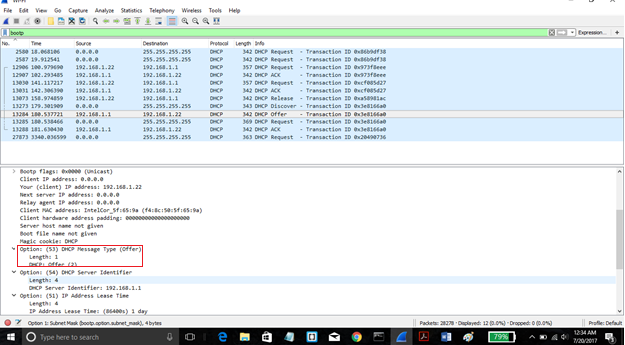


**The subnet mask line tells the client which subnet mask should be used.**

**13. In the client’s response to the first server DHCP Offer message, does the client**

**accept this IP address? Where in the DHCP Request is the client’s requested IP**

**address?**



**The client does not accept this IP address.**

**14. What is the purpose of the DHCP Release message? Does the DHCP server issue**

**an acknowledgment of receipt of the client’s DHCP Release message? What**

**would happen if the client’s DHCP Release message is lost?**

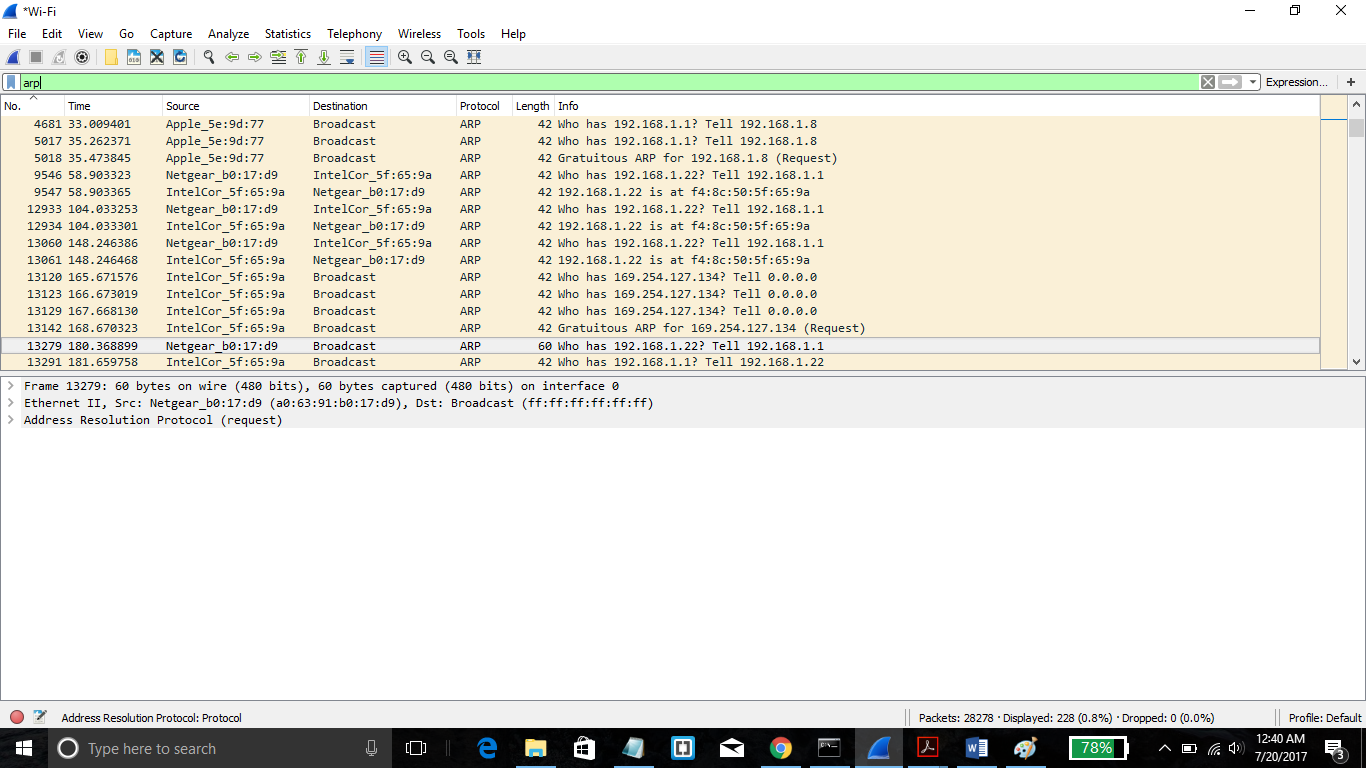
A DHCP release message is sent by the client to release its hold on the IP address given to it by the DHCP server.

**15. 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.**

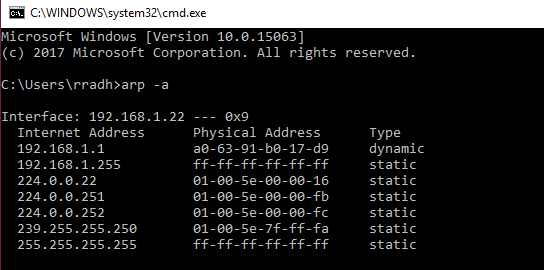
**No ARP packets packets were sent or received during the DHCP packet-exchange period**



**Part 2: Address Resolution Protocol**

**16. Write down the contents of your computer’s ARP cache. What is the meaning of**

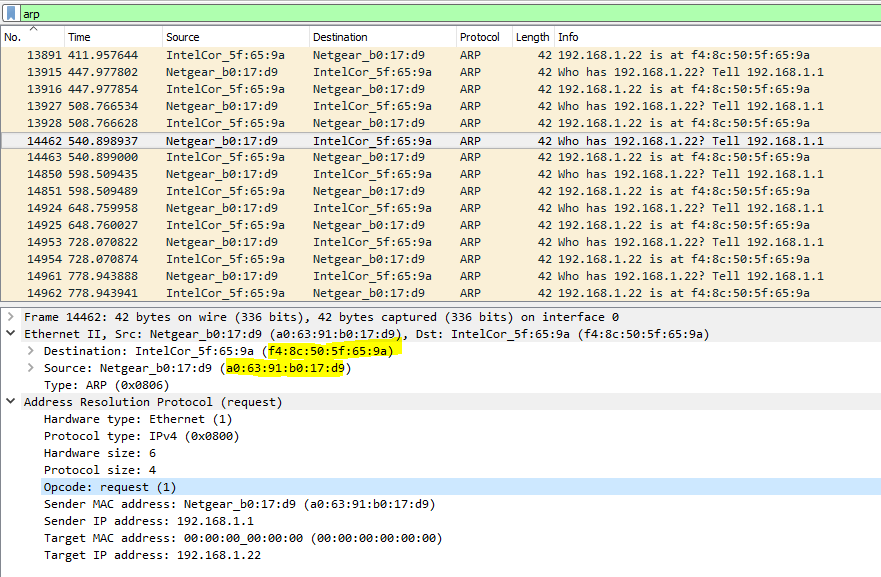
**each column value?**



The Internet Address column contains the IP address, the Physical Address column contains the MAC address, and the type indicates the protocol type.

**17. What are the hexadecimal values for the source and destination addresses in the**

**Ethernet frame containing the ARP request message?**

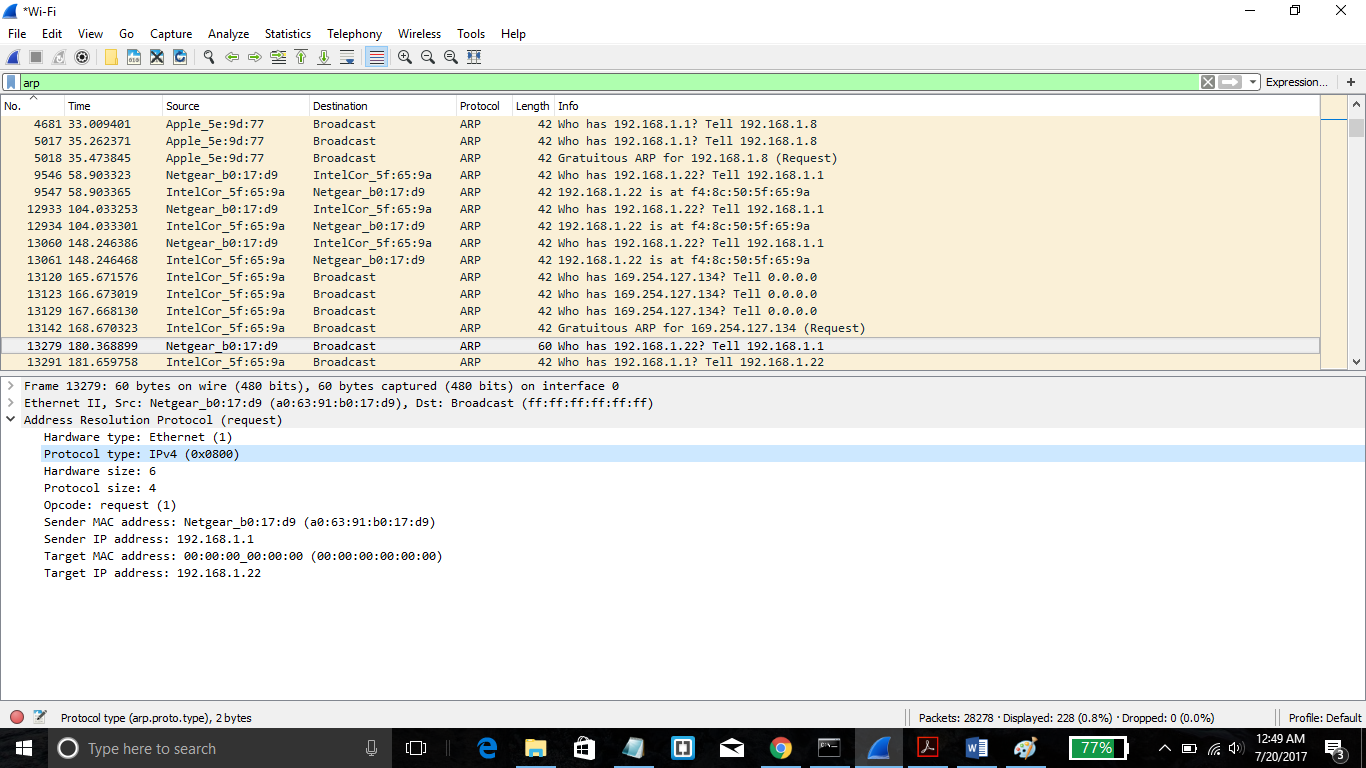


The hex value for the source address is a0:63:91:b0:17:d9. The hex value for the destination address is f4:8c:50:5f:65:9a.

**18. Give the hexadecimal value for the two-byte Ethernet Frame type field. What do**

**the bit(s) whose value is 1 mean within the flag field?**

The hex value for the Frame type field is 0x0800



**19. Download the ARP specification from ftp://ftp.rfc-editor.org/innotes/std/std37.txt. A readable, detailed discussion of ARP is also at http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html.**

**a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?**

ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.

**b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?**

The hex value for opcode field within the ARP-payload of the request is 0x0001, for request.

**c) Does the ARP message contain the IP address of the sender?**

Yes, the ARP message containing the IP address 192.168.1.105 for the sender.

**d) Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?**

The field “Target MAC address” is set to 00:00:00:00:00:00 to question the machine whose corresponding IP address (192.168.1.1) is being queried.

**20. Now find the ARP reply that was sent in response to the ARP request.**

1. **How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?**

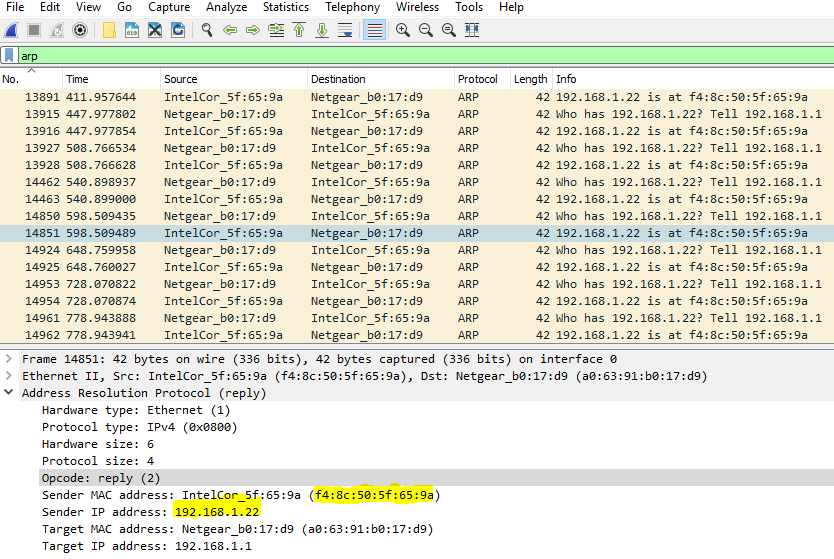
The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.

**b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?**

The hex value for opcode field within the ARP-payload of the request is 0x0002, for reply.

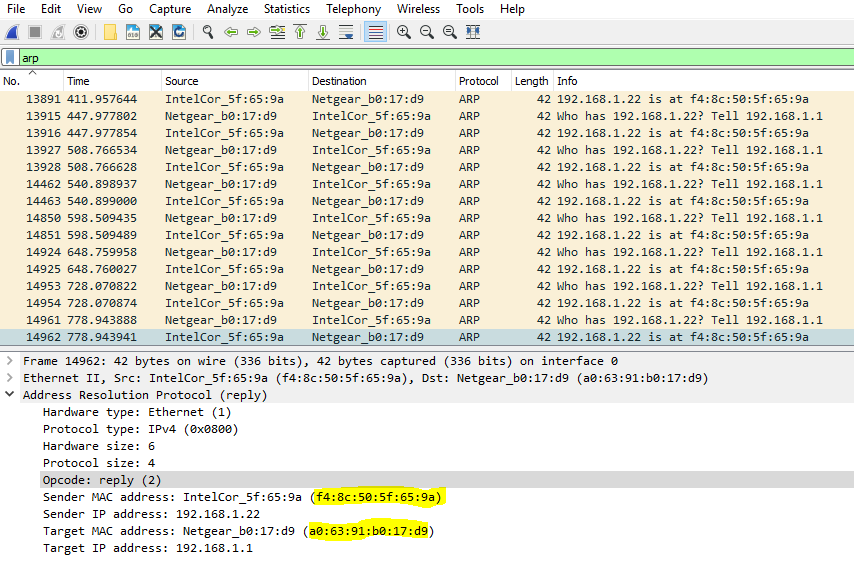
**c) Where in the ARP message does the “answer” to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?**

The answer to the earlier ARP request appears in the ”Sender MAC address” field, which contains the Ethernet address f4:8c:50:5f:65:9a for the sender with IP address 192.168.1.22.



**21. What are the hexadecimal values for the source and destination addresses in the**

**Ethernet frame containing the ARP reply message?**



The hex value for the source address is f4:8c:50:5f:65:9a and for the destination is a0:63:91:b0:17:d9 .

**22. Open the ethernet-ethereal-trace-1 trace file in http://gaia.cs.umass.edu/wiresharklabs/**

**wireshark-traces.zip. The first and second ARP packets in this trace correspond**

**to an ARP request sent by the computer running Wireshark, and the ARP reply sent to**

**the computer running Wireshark by the computer with the ARP-requested Ethernet**

**address. But there is yet another computer on this network, as initiated by packet 6 –**

**another ARP request. Why is there no ARP reply (sent in response to the ARP request**

**in packet 6) in the packet trace?**

We cannot view the trace as we are not the source which sent the request. The ARP request is a broadcast, but the ARP reply is sent back directly to the sender’s Ethernet address. So we cannot view it.