

University of Tehran

School of Electrical and Computer Engineering



Computer Networks

Wireshark Lab 1

Student Name

Alireza Javid

Student ID

810198375

Instructor:

Dr. Shahmansouri

Contents

1	Capturing and analyzing Ethernet and IP headers	2
2	The Address Resolution Protocol	5
3	DHCP	9

1 Capturing and analyzing Ethernet and IP headers

After follow given steps we have:

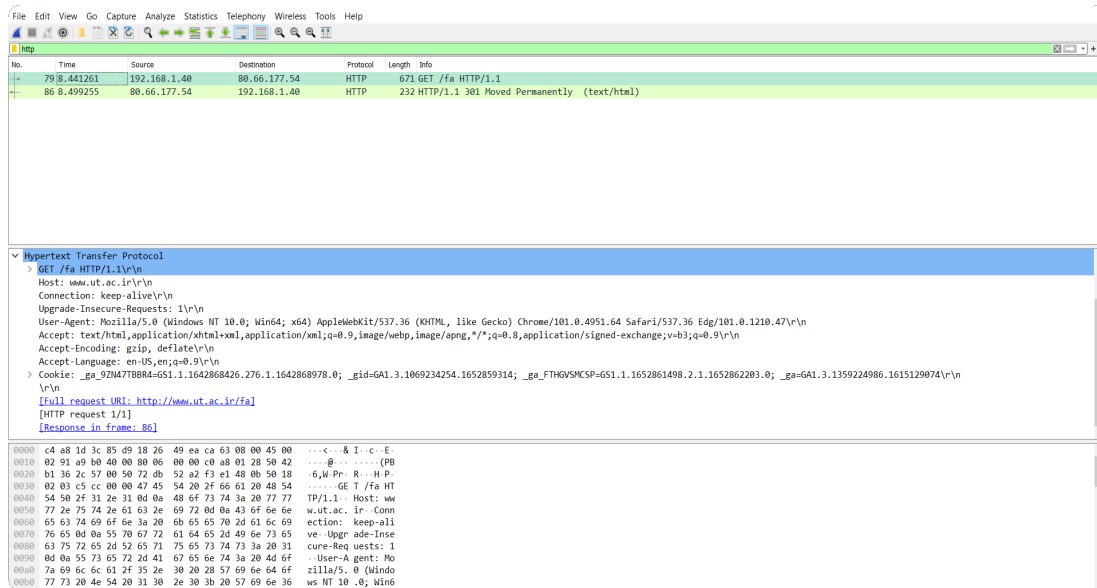


Figure 1: HTTP GET message in Wireshark

As we can see first GET request and Get response packet numbers are 79 and 86. Now we can answer to given questions:

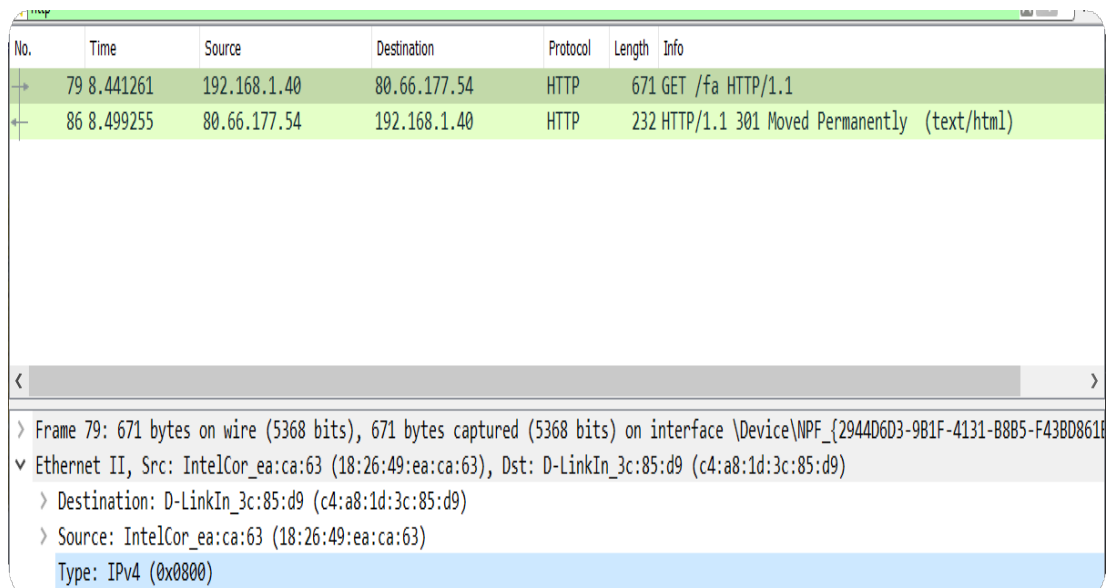


Figure 2: MAC address of the source and destination

1. According to figure 2:

MAC address of the source = 18 : 26 : 49 : ea : ca : 63

MAC address of the destination = c4 : a8 : 1d : 3c : 85 : d9

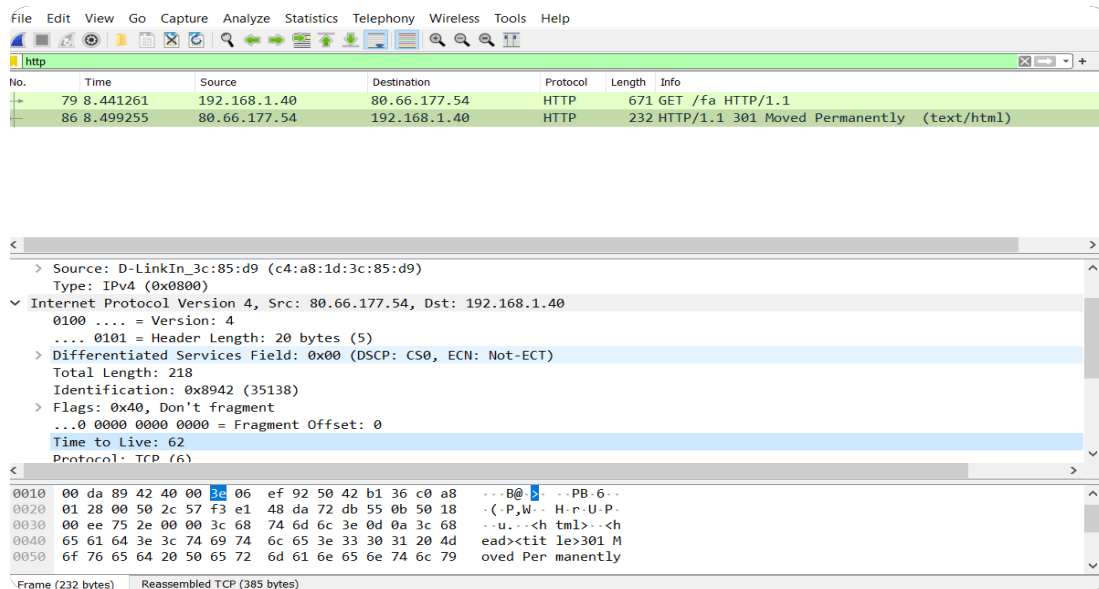


Figure 3: Time to Live of the response message

2. Again according to figure 2:

$$IP \text{ address of the source} = 192.168.1.40$$

3. According to figure 3:

$$Time \text{ to Live of the response message } (TTL) = 62$$

we can say for meaning of TTL as Time to live or hop limit is a mechanism which limits the lifespan or lifetime of data in a computer or network. TTL may be implemented as a counter or timestamp attached to or embedded in the data. Once the prescribed event count or timespan has elapsed, data is discarded or revalidated. also for Get request TTL is equal 128.

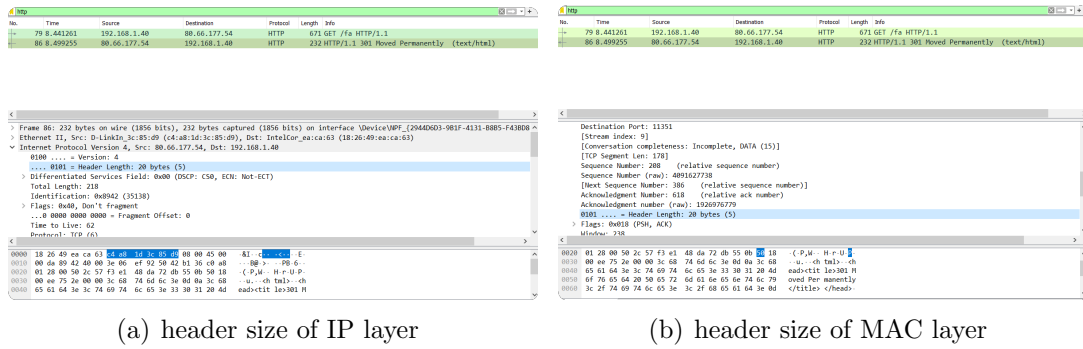


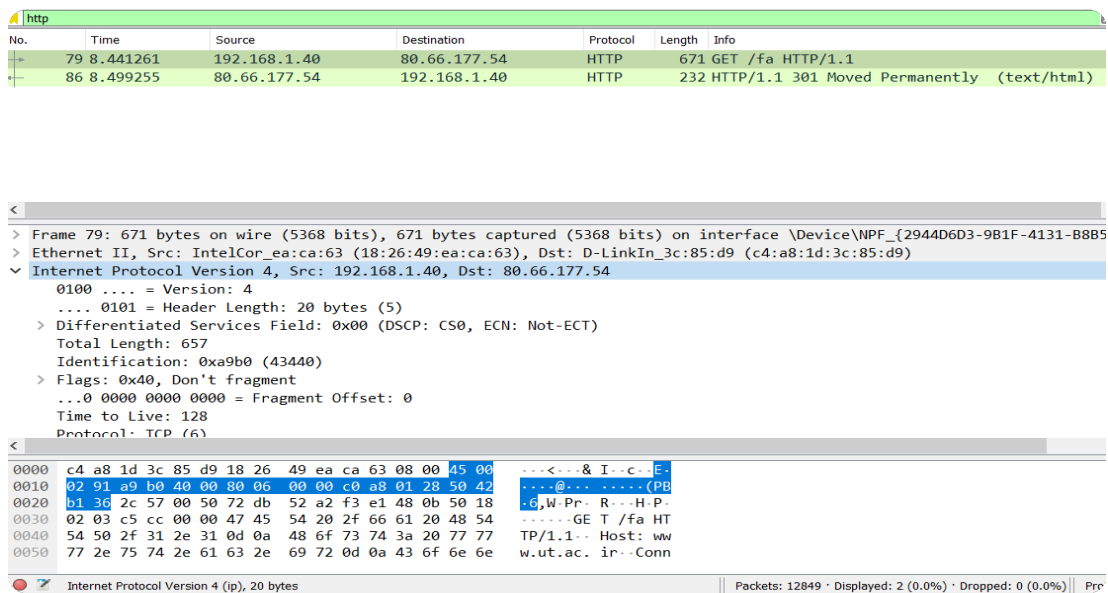
Figure 4: header size of IP and MAC layer

4. according to figure 4:

Header size of IP layer = 20 byte

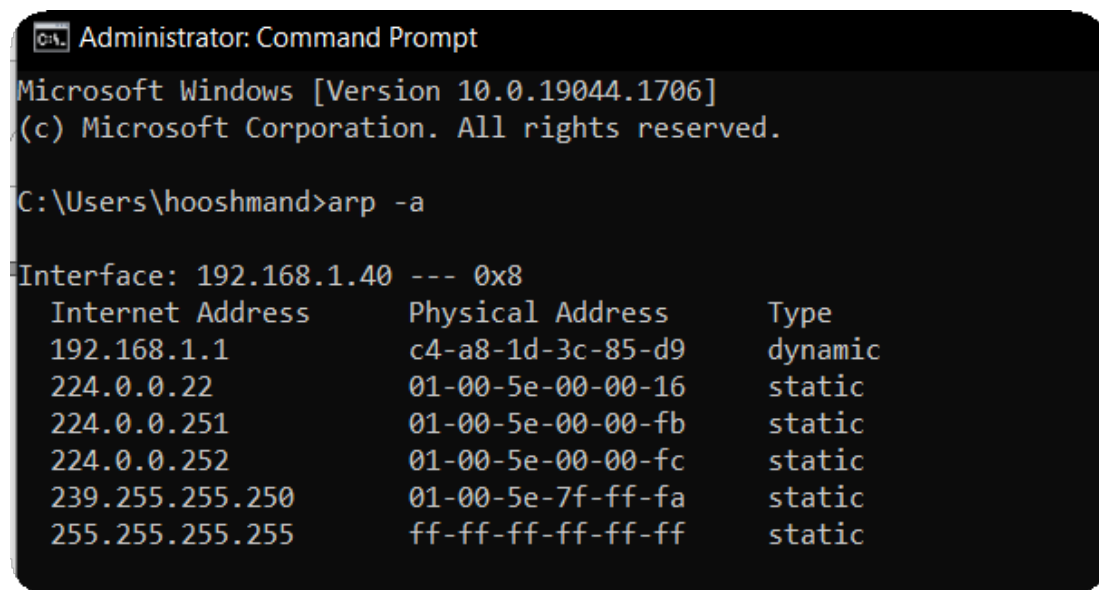
Header size of MAC layer = 20 byte

Another solution for problem can be:
 The ASCII “O” appears 52 bytes from the start of the Ethernet frame.
 Again, there are 14 bytes of Ethernet frame, and then 20 bytes of IP header
 followed by 20 bytes of TCP header before the HTTP data is encountered.



5. According to figure 5, IP length is 20 byte and there is not any option in IP header.

2 The Address Resolution Protocol



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19044.1706]
(c) Microsoft Corporation. All rights reserved.

C:\Users\hooshmand>arp -a

Interface: 192.168.1.40 --- 0x8
Internet Address      Physical Address      Type
192.168.1.1           c4-a8-1d-3c-85-d9    dynamic
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static
```

Figure 6: ARP table

1. The first column shows the IP addresses in the ARP cache. The second column shows the physical (MAC) addresses (48 bit Ethernet Address) and the last column shows the type of ARP entries :

ARP entries can be Dynamic or Static :

- Dynamic : Which means that the ARP entry (the Ethernet MAC to IP address link) has been learned (usually from the default gateway).dynamic entry can be overwritten by a static ARP entry and is kept on a device for some period of time, as long as it is being used.
- Static : A static ARP entry is the opposite of a dynamic ARP entry. With a static ARP entry, the computer is manually entering the link between the Ethernet MAC address and the IP address. it does not age out or cannot be overwritten by a dynamic ARP entry. Software in your computer will pre-define these static entries such as multi-cast addresses and broadcast addresses.

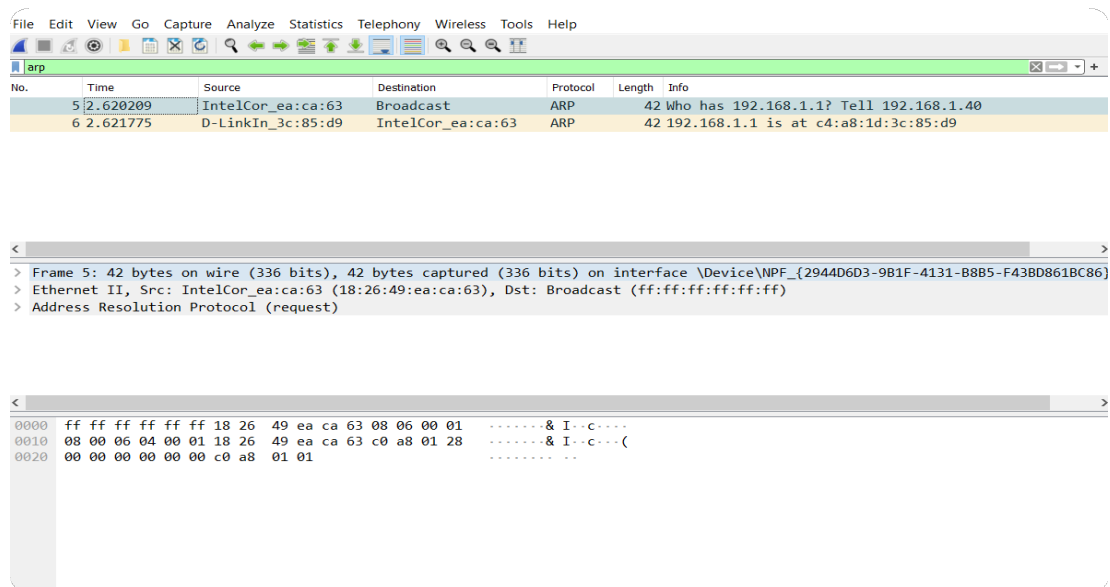


Figure 7: ARP Packet in wireshark

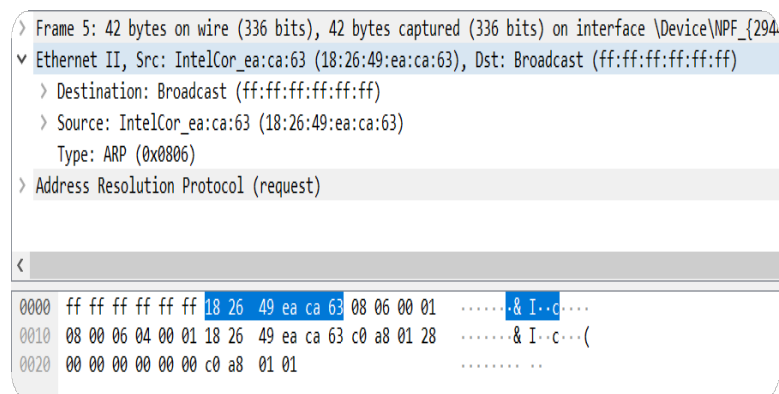


Figure 8: Hexadecimal Values of the Source and Destination

2. (a) As we can see in figure 8.

The hex value for the source address is 18:26:49:ea:ca:63 .

The hex value for the destination address is ff:ff:ff:ff:ff:ff, the broadcast address.
- (b) ARP is a protocol which belongs to the Data link layer (DLL) and it saves the mappings of IP address in Network Layer ([The Upper Layer](#)) to MAC address in Data link Layer ([The below Layer](#)), So upper layer protocol ARP corresponds to, is IP protocols.

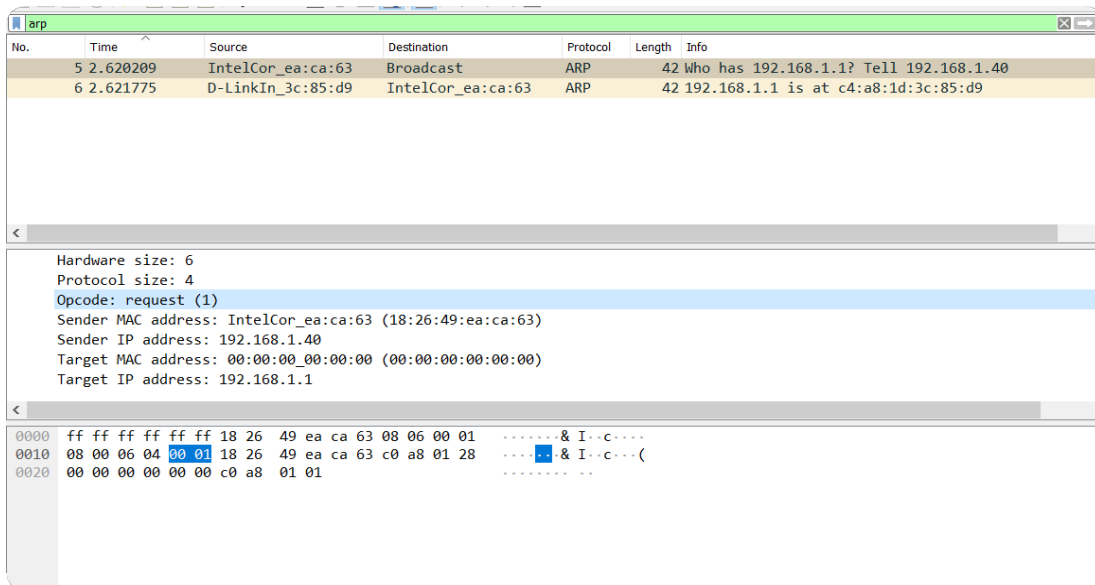


Figure 9: opcode field in ARP request

- (c) According to figure 9 value of the opcode field within the ARP-Payload part of the Ethernet frame is 0001

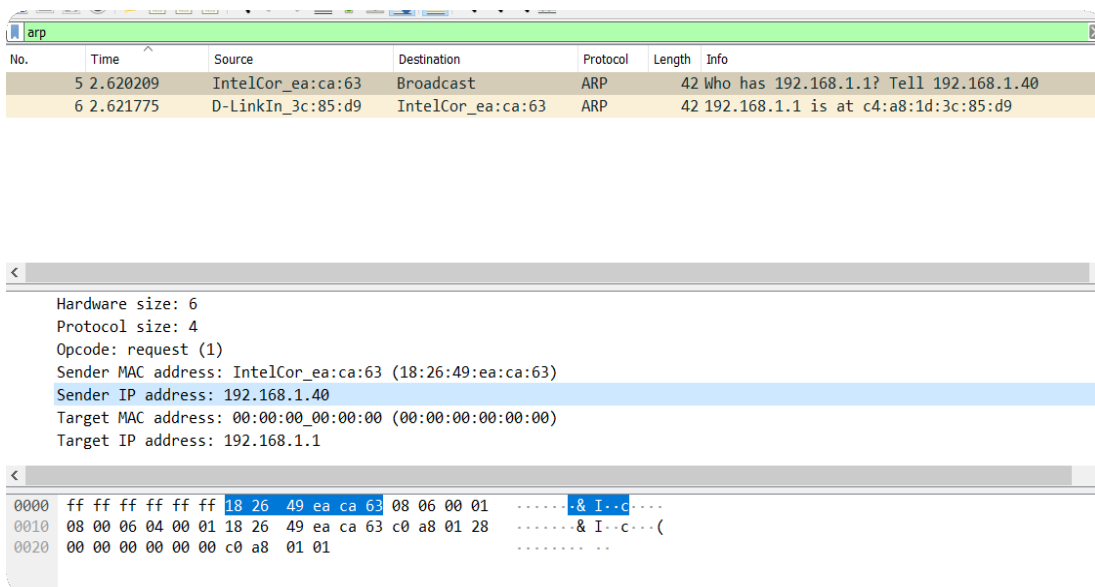


Figure 10: IP address of the sender in ARP request

- (d) As we can see in figure 10, ARP message contains the IP address of the sender and it is 192.168.1.40 .
- (e) As we can see in figure 10, 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.
3. Now for the ARP reply that was sent in response to the ARP request, we have:

- (a) According to figure 11 value of opcode is 0002

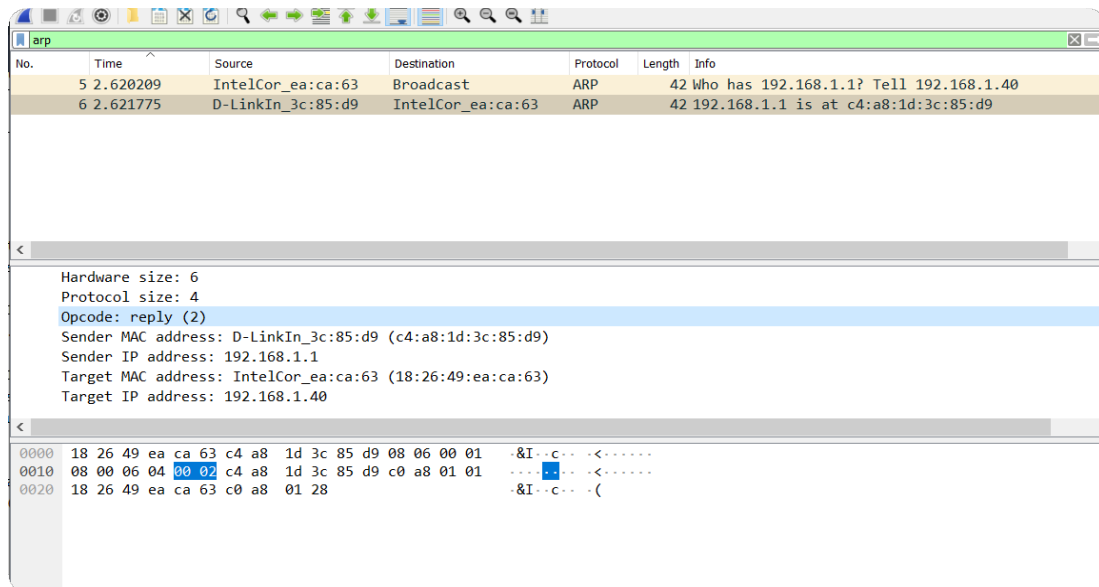


Figure 11: opcode field in ARP request

- (b) The answer to the earlier ARP request appears in the "Sender MAC address" field, which contains the Ethernet address c4:a8:1d:3c:85:d9 for the sender with IP address 192.168.1.1 . (also we can see this in figure 11)

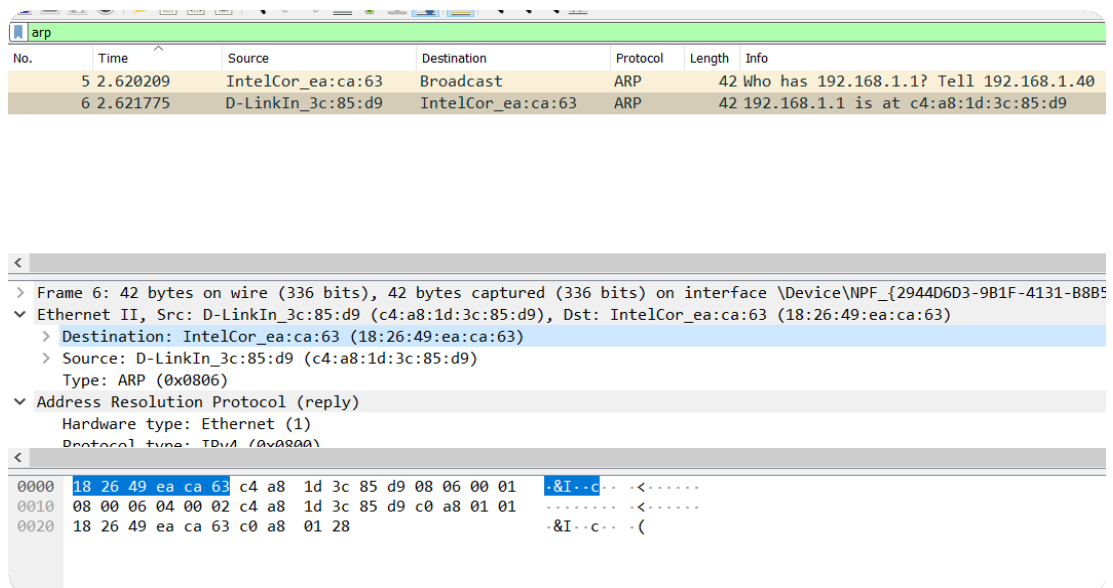


Figure 12: Hexadecimal Values of the Source and Destination

- (c) As we can see in figure 12.
 The hex value for the source address is c4:a8:1d:3c:85:d9 .
 The hex value for the destination address is 18:26:49:ea:ca:63 .

3 DHCP

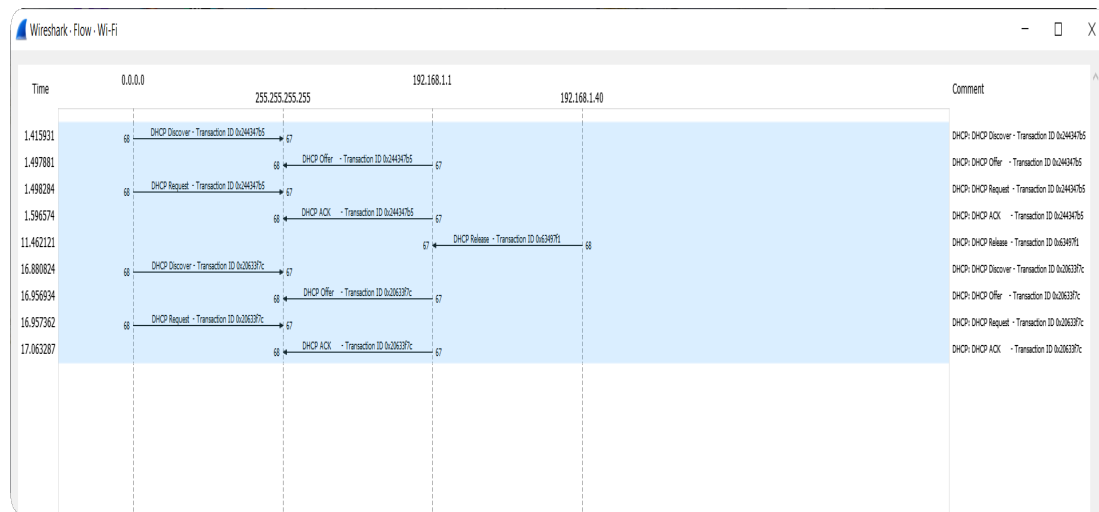
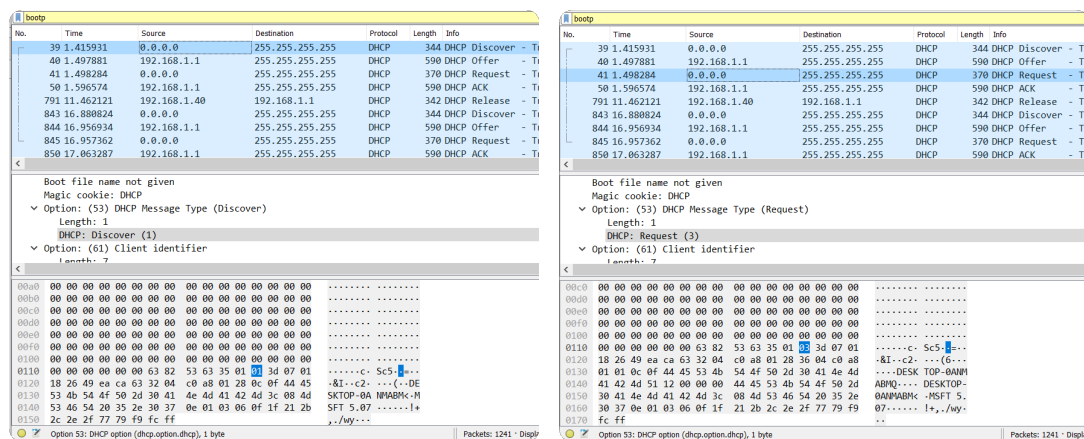


Figure 13: timing diagram

1. In figure 13 we draw timing diagram using flow graph in wireshark in Statistics tab.



(a) DHCP discover message

(b) DHCP request message

Figure 14: differentiate DHCP discover and request message

2. As we can see in figure 14, option (53) shows DHCP message type and we can distinguish between DHCP discover and request messages.

No.	Time	Source	Destination	Protocol	Length	Info
39	1.415931	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x244347b5
40	1.497881	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x244347b5
41	1.498284	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x244347b5
50	1.596574	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x244347b5
791	11.462121	192.168.1.40	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0x63497f1
843	16.880824	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x20633f7c
844	16.956934	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x20633f7c
845	16.957362	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x20633f7c
850	17.063287	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x20633f7c

Figure 15: Transaction-ID in 2 set of DHCP messages

- The value of the transaction id in the first four DHCP messages is 0x244347b5. The value of the transaction id in the second set of DHCP messages is 0x20633f7c.

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

- As we can see in figure 13 and 14:

- Discover and Request :
Source IP : 0.0.0.0
Destination IP : 255.255.255.255 (means message is sent broadcast)
- Offer and ACK :
Source IP : 192.168.1.1
Destination IP : 255.255.255.255 (means message is sent broadcast)

- As the request message is a broadcast message in order to find the DHCP server and request an IP from it and offer message is answer to this message, source IP of Offer message is IP address of my DHCP server, which is 192.168.1.1 .

No.	Time	Source	Destination	Protocol	Length	Info
39	1.415931	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x244347b5
40	1.497881	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x244347b5
41	1.498284	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x244347b5
50	1.596574	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x244347b5

```

> Bootp flags: 0x8000, Broadcast flag (Broadcast)
Client IP address: 0.0.0.0
Your (client) IP address: 192.168.1.40
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: IntelCor_ea:ca:63 (18:26:49:ea:ca:63)
Client hardware address padding: 000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (Offer)
  Length: 1
  DHCP: Offer (2)
  Option: (54) DHCP Server Identification (192.168.1.1)
  
```

Figure 16: IP address in offer message

- My client is offered 192.168.1.40 by the DHCP server. The offer message contains the DHCP address offered by the server.

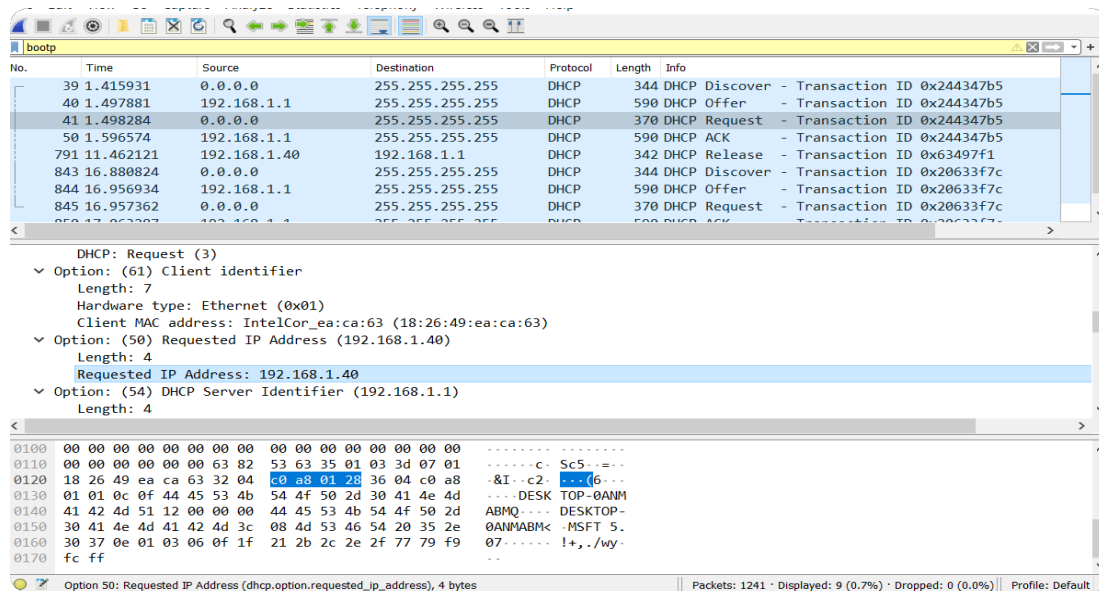


Figure 17: IP address in offer message

7. As we can see in figure 17, The client accepts the IP address given in the offer message within the request message. After being offered the IP address 192.168.1.40 in the offer message, my client sent back a message further requesting that specific IP address.

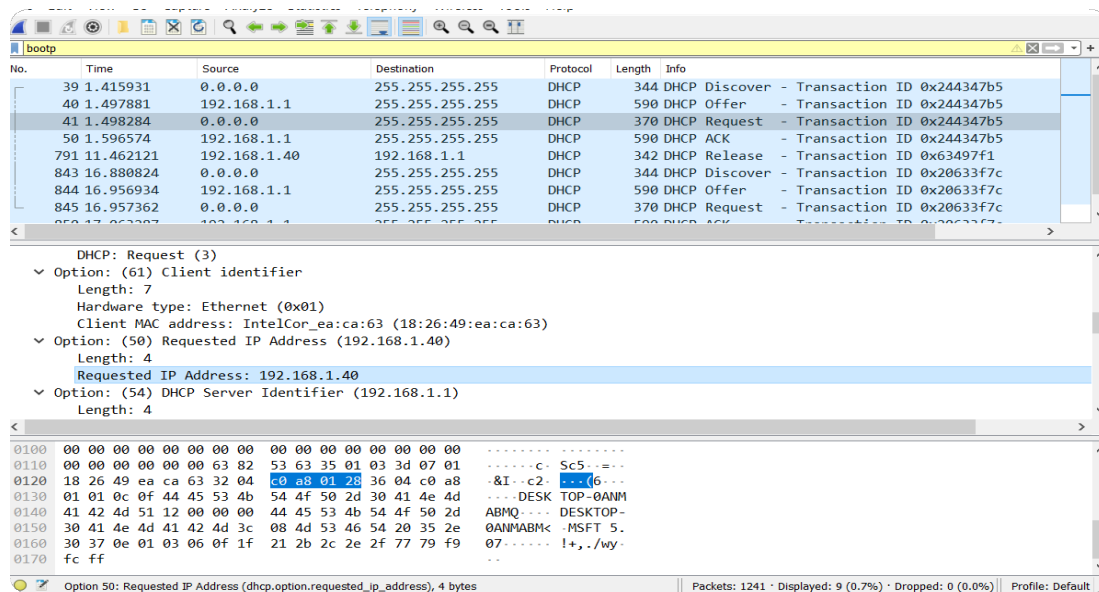


Figure 18: lease time

8. The lease time is the amount of time the DHCP server assigns an IP address to a client. During the lease time, the DHCP server will not assign the IP given to the client to another client, unless it is released by the client. Once the lease time has expired, the IP address can be reused by the DHCP server to give to another client.

The lease time in my experiment is 43200 seconds or 12 hours.