In the Name of God

University of Tehran

School of Electrical and
Computer Engineering

Computer Networks

Wireshark Lab

Amirhossein Mohammadi

810197689

Spring 2021

Table of Contents

Abstract

Goal of the computer assignment is to get familiar with different internet protocols and packet transition inside network. More specifically we will dig in to ARP and DHCP protocols.

Part 1. Capturing and analyzing Ethernet and IP headers

1. What is IP address of the source and destination?

As show in figure one IP address of source is : 192.168.1.4 and IP address of destination is 80.66.177.54 .

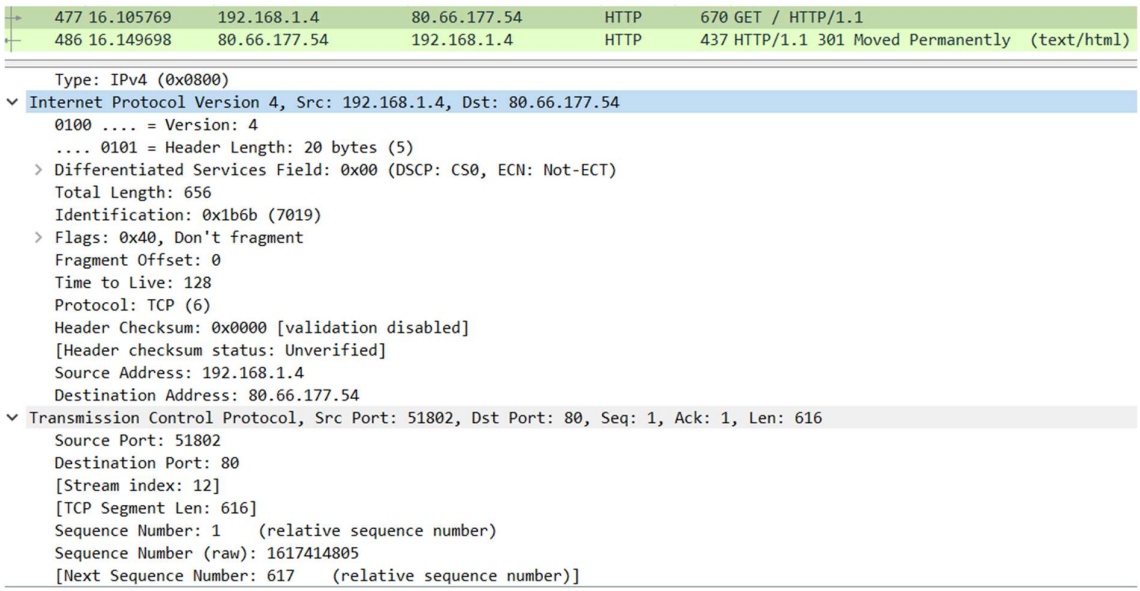


Figure 1, Internet Protocol V4 and TCP

2. What is Time to Live?

Time to live is 128.

3. What is the 48-bit Ethernet address of your computer?

As shown in figure 2, MAC address of source is:

MAC address : 50:76:af:7e:e6:45

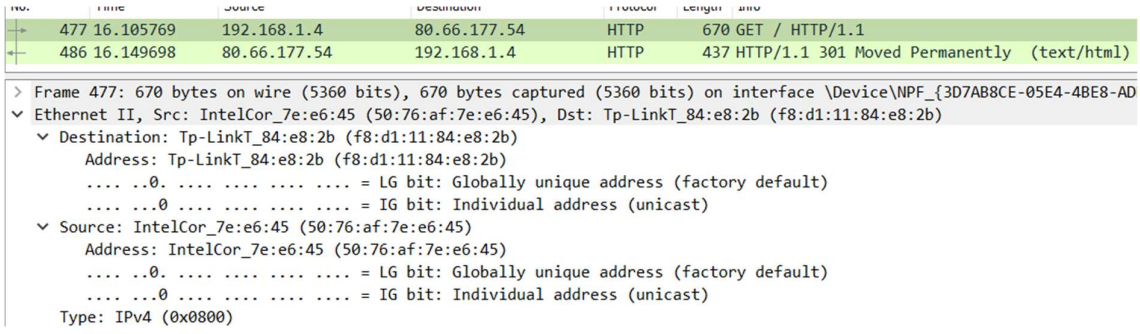


Figure 2, Ethernet II

4. What is the 48-bit destination address in the Ethernet frame? What device has this as its Ethernet address?

The address and device are:

Address: f8:d1:11:84:e8:2b

Device: Tp-LinkT_84:e8:2b

5. What is the header size?

As shown in figure 1 header length is 20 bytes.

6. How many bytes are from the start of the Ethernet frame until the ASCII "O" in "OK" (i.e., the HTTP response code)? This shows the total header of the frame.

In this packages GET request has been cached but, the O in OK appear 52 bytes in the Ethernet frame.

Part 2. The Address Resolution Protocol

1. Write down the contents of your computer's ARP cache. What is the meaning of column value?

As shown figure 3 we can see ARP cache of computer,

Internet address is IP, Physical Address is MAC address, Type is protocol type.

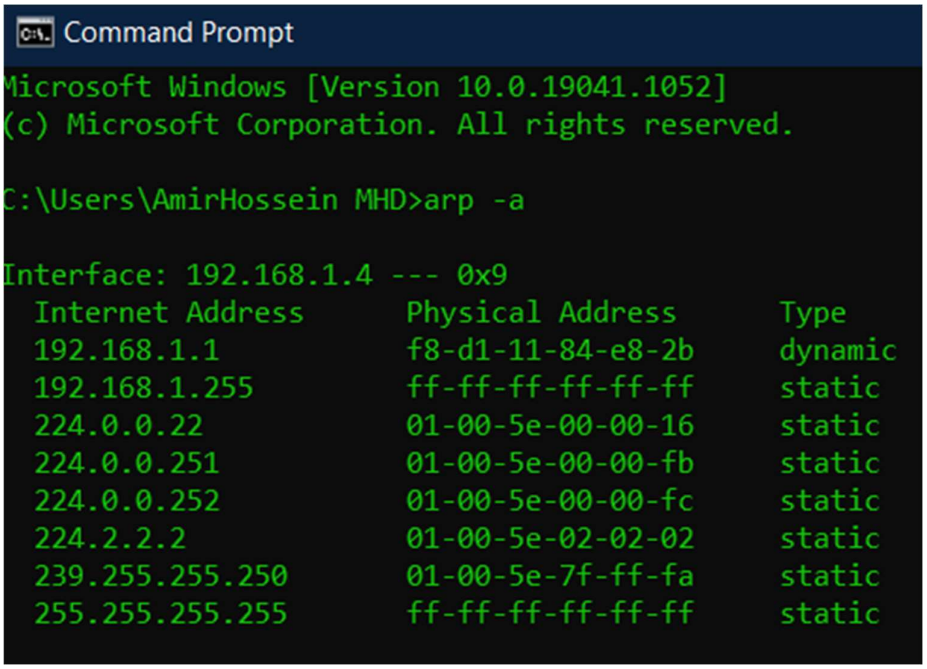


Figure 3, ARP Cache Table

2. Find the ARP request and answer the following questions:

a) What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

As shown in figure 4, destination address is ff:ff:ff:ff:ff:ff, since client is broadcasting request to all nodes in network in order to get an IP address.

b) Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?

Protocol type is ARP as we expected:

Type: ARP(0x0806)

It is clear at figure 4.

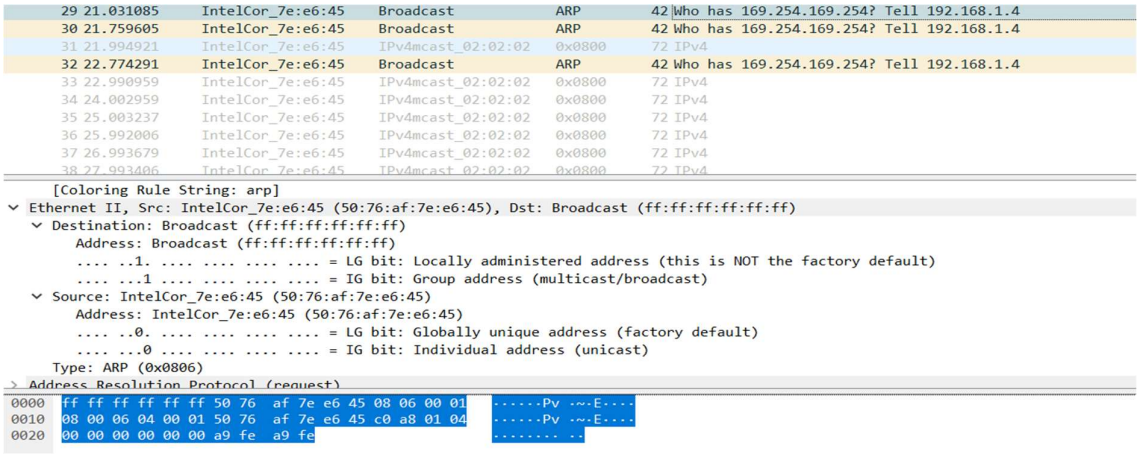


Figure 4

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

value for opcode field withing the ARP-payload of the request is 1.

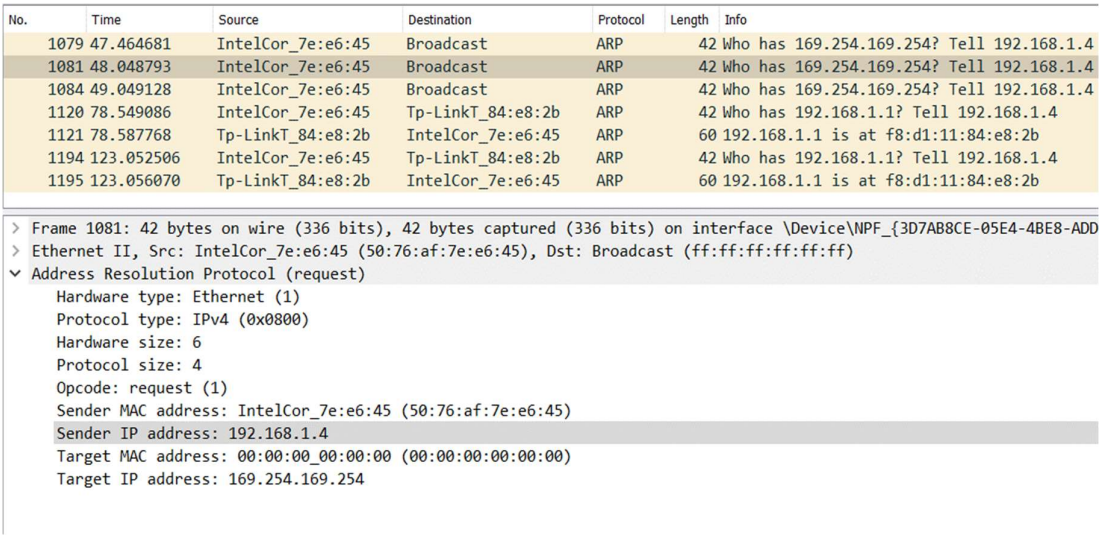


Figure 5

d) Does the ARP message contain the IP address of the sender?

Yes, Sender IP address is 192.168.1.4

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

The field of Target MAC address 00:00:00:00:00:00, this broadcast will queries the machine which IP address is 169.254.169.254.

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

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

Opcode for reply is 2.

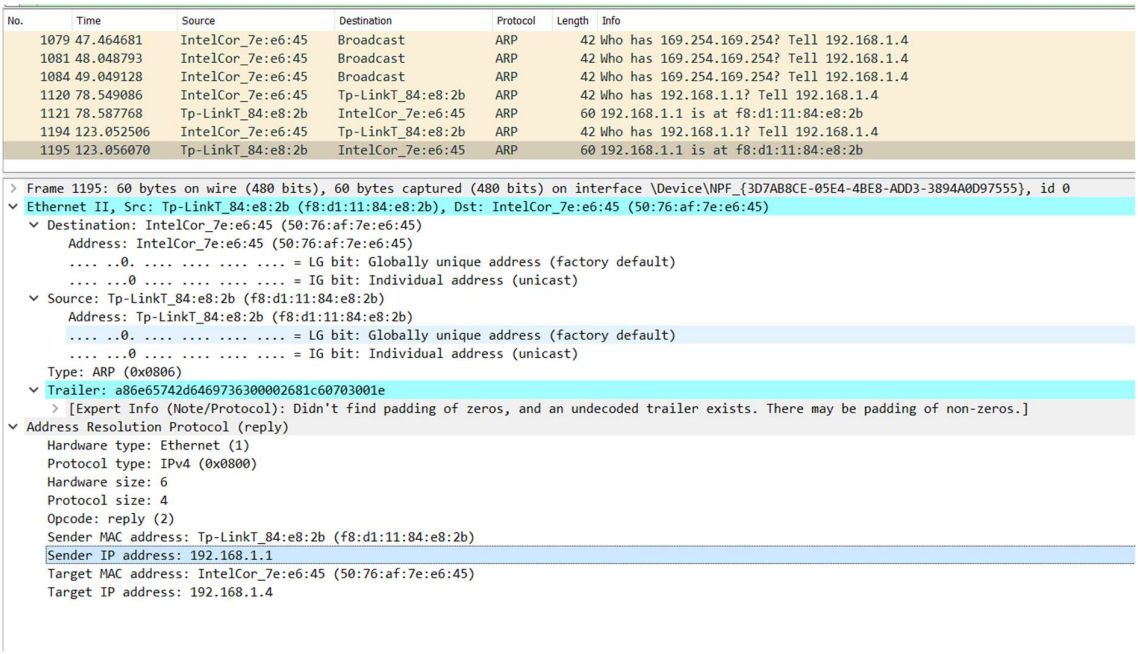


Figure 6, ARP Reply

b) 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 f8:d1:11:84:e8:2b for the sender with IP address 192.168.1.1.

c) What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

MAC address of source: f8:d1:11:84:e8:2b

MAC address of destination: 50:76:af:e6:45

Part 3. DHCP

1. Draw a timing datagram illustrating the sequence of the DHCP packets.

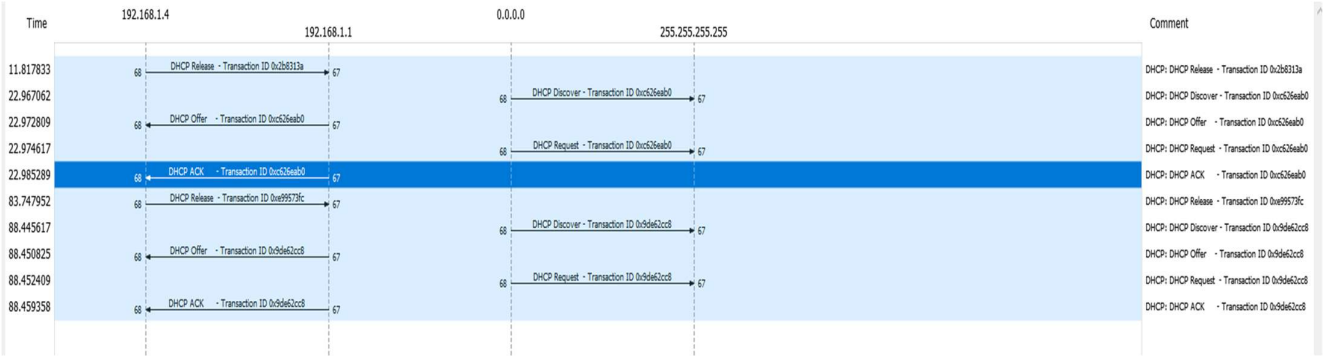


Figure7 , Timing Diagram

From above it we can obtain that, we have four stages:

I. **Discover**: client sending request to find out is there any DHCP server to dedicate an IP to client or not.
II. **Offer**: DHCP server is telling to the client the is an available IP.
III. **Request**: Client accepts DHCP servers offer.
IV. **ACK:** Server accept clients request, and from now client has the given IP

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

Message type differentiate discover message from request. Message for DHCP Discover is 1 and for request is 3.

3. 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?

Transaction ids are clear in figure 7. As we can see each set of transactions has unique id in order to distinguish requests from another.

We had two sets of transactions:

First set: 0xc626eab0
Second set: 0x9de62cc8

4. For each of the four DHCP messages (Discover/ Offer/ Request/ ACKDHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.

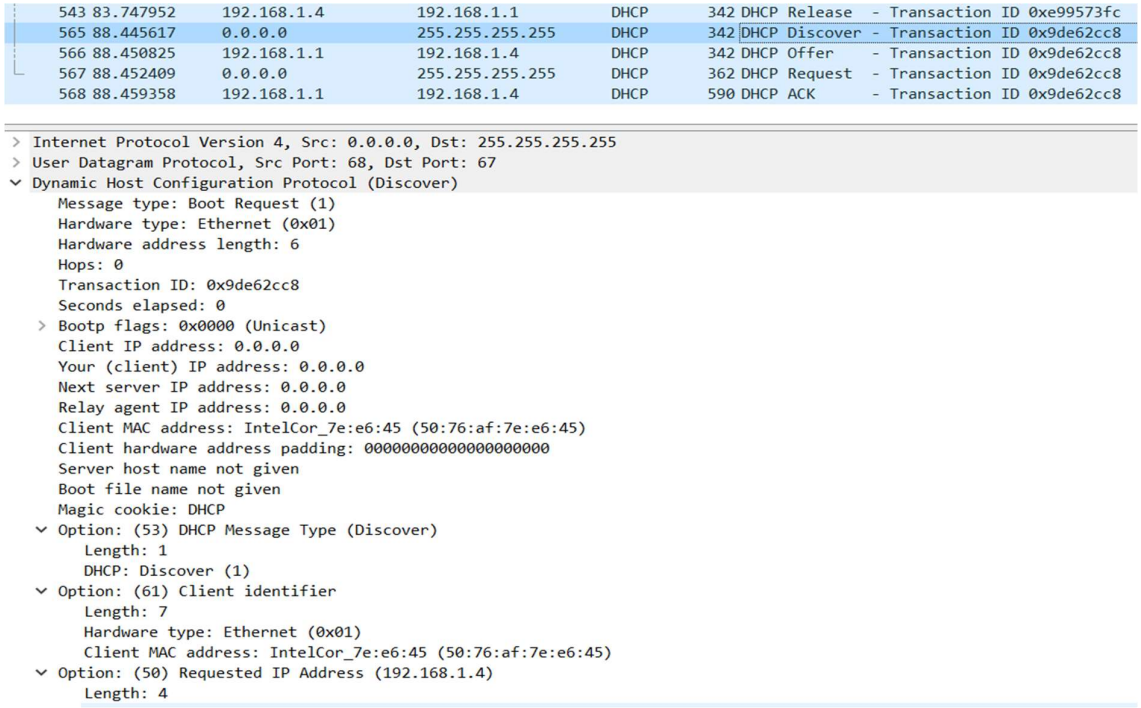


Figure 8, DHCP DISCOVER

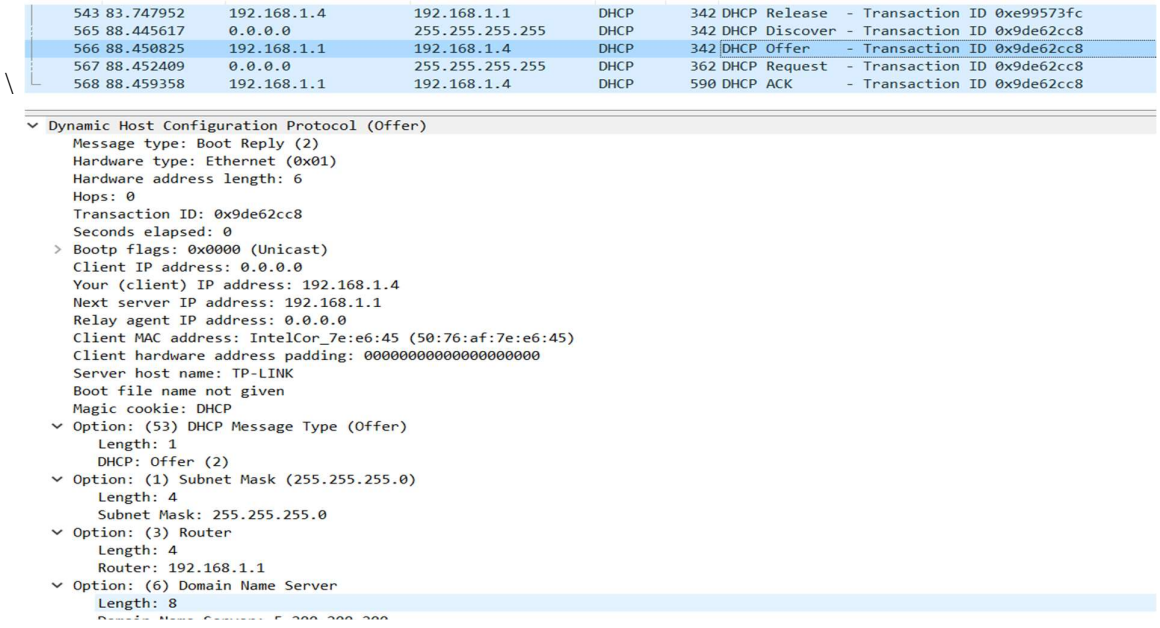
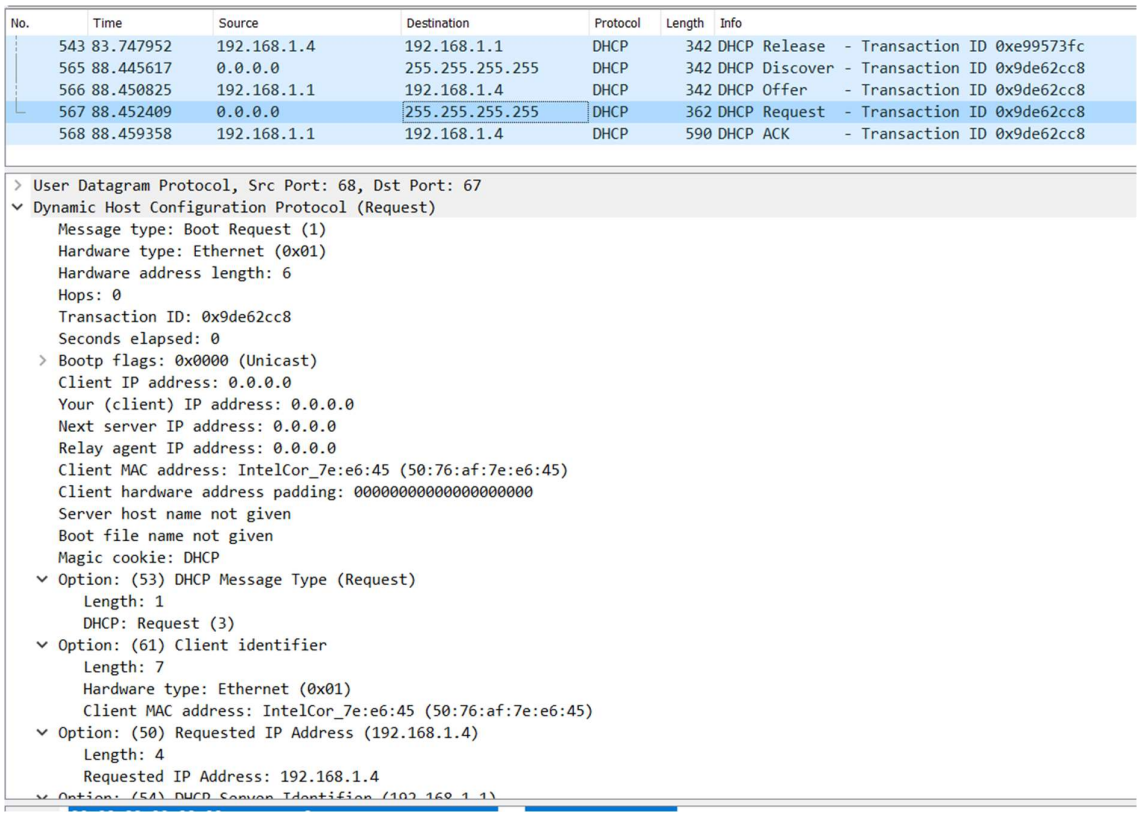


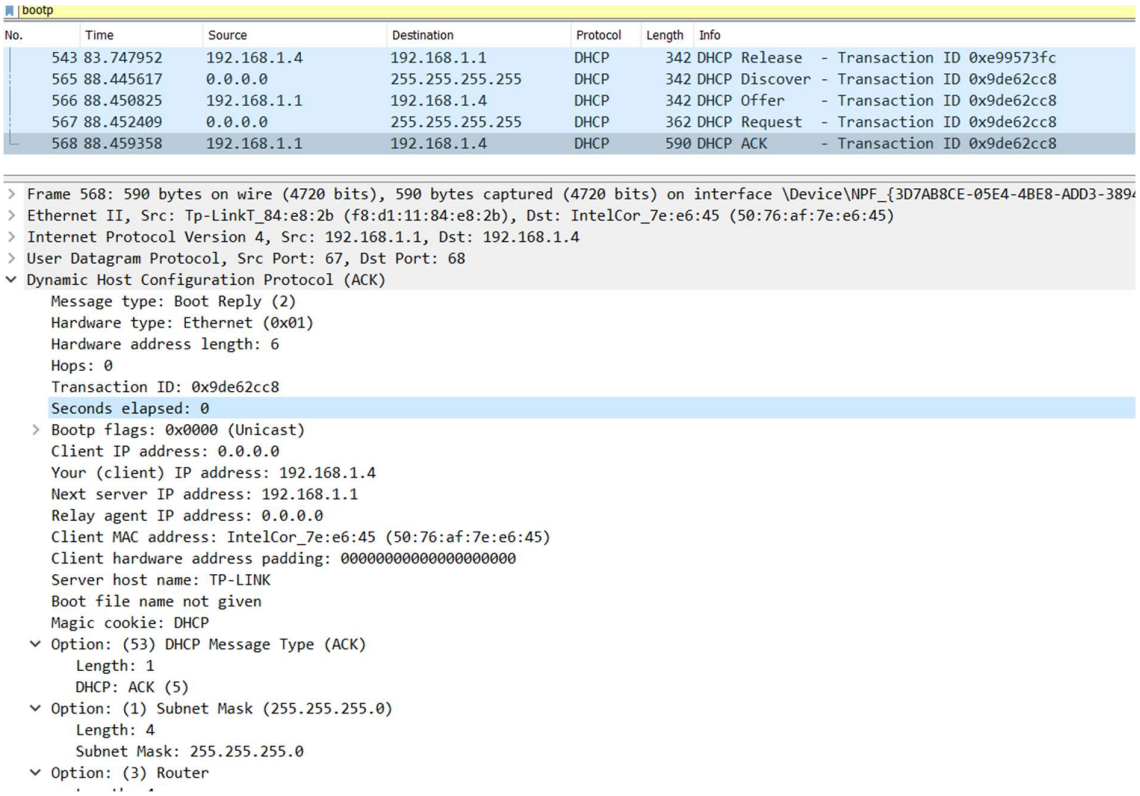
Figure9 , Offer



No.	Time	Source	Destination	Protocol	Length	Info
543	83.747952	192.168.1.4	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0xe99573fc
565	88.445617	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x9de62cc8
566	88.450825	192.168.1.1	192.168.1.4	DHCP	342	DHCP Offer - Transaction ID 0x9de62cc8
567	88.452409	0.0.0.0	255.255.255.255	DHCP	362	DHCP Request - Transaction ID 0x9de62cc8
568	88.459358	192.168.1.1	192.168.1.4	DHCP	590	DHCP ACK - Transaction ID 0x9de62cc8

```
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x9de62cc8
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: IntelCor_7e:e6:45 (50:76:af:7e:e6:45)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  v Option: (53) DHCP Message Type (Request)
      Length: 1
      DHCP: Request (3)
  v Option: (61) Client identifier
      Length: 7
      Hardware type: Ethernet (0x01)
      Client MAC address: IntelCor_7e:e6:45 (50:76:af:7e:e6:45)
  v Option: (50) Requested IP Address (192.168.1.4)
      Length: 4
      Requested IP Address: 192.168.1.4
```

Figure 10, Request



bootp

No.	Time	Source	Destination	Protocol	Length	Info
543	83.747952	192.168.1.4	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0xe99573fc
565	88.445617	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x9de62cc8
566	88.450825	192.168.1.1	192.168.1.4	DHCP	342	DHCP Offer - Transaction ID 0x9de62cc8
567	88.452409	0.0.0.0	255.255.255.255	DHCP	362	DHCP Request - Transaction ID 0x9de62cc8
568	88.459358	192.168.1.1	192.168.1.4	DHCP	590	DHCP ACK - Transaction ID 0x9de62cc8

```
> Frame 568: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface \Device\NPF_{3D7AB8CE-05E4-4BE8-ADD3-389
> Ethernet II, Src: Tp-LinkT_84:e8:2b (f8:d1:11:84:e8:2b), Dst: IntelCor_7e:e6:45 (50:76:af:7e:e6:45)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.4
> User Datagram Protocol, Src Port: 67, Dst Port: 68
v Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x9de62cc8
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.1.4
    Next server IP address: 192.168.1.1
    Relay agent IP address: 0.0.0.0
    Client MAC address: IntelCor_7e:e6:45 (50:76:af:7e:e6:45)
    Client hardware address padding: 00000000000000000000
    Server host name: TP-LINK
    Boot file name not given
    Magic cookie: DHCP
  v Option: (53) DHCP Message Type (ACK)
      Length: 1
      DHCP: ACK (5)
  v Option: (1) Subnet Mask (255.255.255.0)
      Length: 4
      Subnet Mask: 255.255.255.0
  v Option: (3) Router
```

Figure 11, DHCP ACK

As we can see in figures above:

IP \ Transaction	Discover	Offer	Request	Acknolegment
Source IP	0.0.0.0	192.168.1.1	0.0.0.0	192.168.1.1
Destination IP	192.168.1.1	255.255.255.255	255.255.255.255	192.168.1.4

5. What is the IP address of your DHCP server?

DHCP Server IP Adress is 192.168.1.1.

6. 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.

Offering IP Address: 192.168.1.4.

Offer message contains IP address.

7. 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?

Client answer to offer message in request packet (figure 9) .

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

Since users may leave network and we have limited number of IPs, DHCP server allocate each client an IP for a limited time. This time indicates that how much time users have been given an specific IP address. After this lease time, if user requests, process will be repeated.

Supplementary HTTP

1. How many HTTP GET request messages did your browser send?

My browser Sent 5 GET request messages.

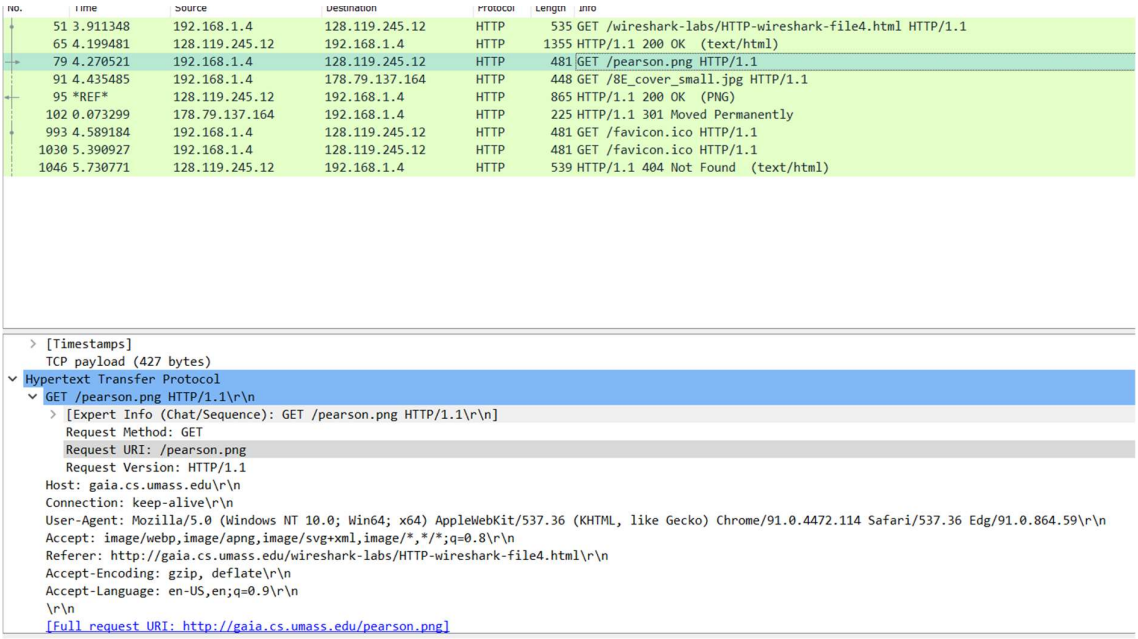


Figure 12

2. Explain the purposes of all GET messages.

GET is used to retrieve and request data from a specified resource in a server.

Packet 51: getting html file.

Packet 79: Pearson book image.

Packet 91: cover_small.jpg

Packet 993,1030: favicon.ico

3. Explain the GET responses. What is the content of these messages?

All of GET response is with code 1xx and are INFORMATIONAL, it means request was received and the process is continuing.