CS 3873: Net-Centric Computing
Lab 3: Examining DHCP and NAT with Wireshark

Student Name: Mahmoud Moustafa Student Number: 3648276

[Mandatory] Declaration: "I warrant that this is my own work."

Signed by Mahmoud Moustafa

[Optional] "I hereby give my permission for this work to be used (with my name and identifying information removed) for UNB Faculty of Computer Science program accreditation purposes."

Signed by _____

Report for Lab Exercise 3:
Examining DHCP and NAT with Wireshark

LAB ACTIVITIES:

In this lab, we used Wireshark to examine two important network-layer protocols for address administration: DHCP and NAT.

ANSWERS TO LAB QUESTIONS:

The following gives you one example on how to draft your answer to the lab questions.

ANSWERS TO LAB QUESTIONS:

2. The following questions are answered by referring to file ***dhcp-ethereal-trace-1.pcap*** I downloaded from D2L:

   a. A host uses DHCP to obtain an IP address, among other things. But a host's IP address is not confirmed until the DHCP ACK is exchanged between the client and server! **For the first four DHCP messages** (DHCP Discover/Offer/Request/ACK), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram, also indicate the source and destination port numbers that can be found in the UDP segment header. What is the IP address of the DHCP server?

   Answer: Referring to the following figures, I have the answer in the following table. The IP address of the DHCP server is 192.168.1.1.

Message	Source Address	Destination Address	Source Port	Destination Port
DHCP Discover	0.0.0.0	255.255.255.255	68	67
DHCP Offer	192.168.1.1	255.255.255.255	67	68
DHCP Request	0.0.0.0	255.255.255.255	68	67
DHCP ACK	192.168.1.1	255.255.255.255	67	68

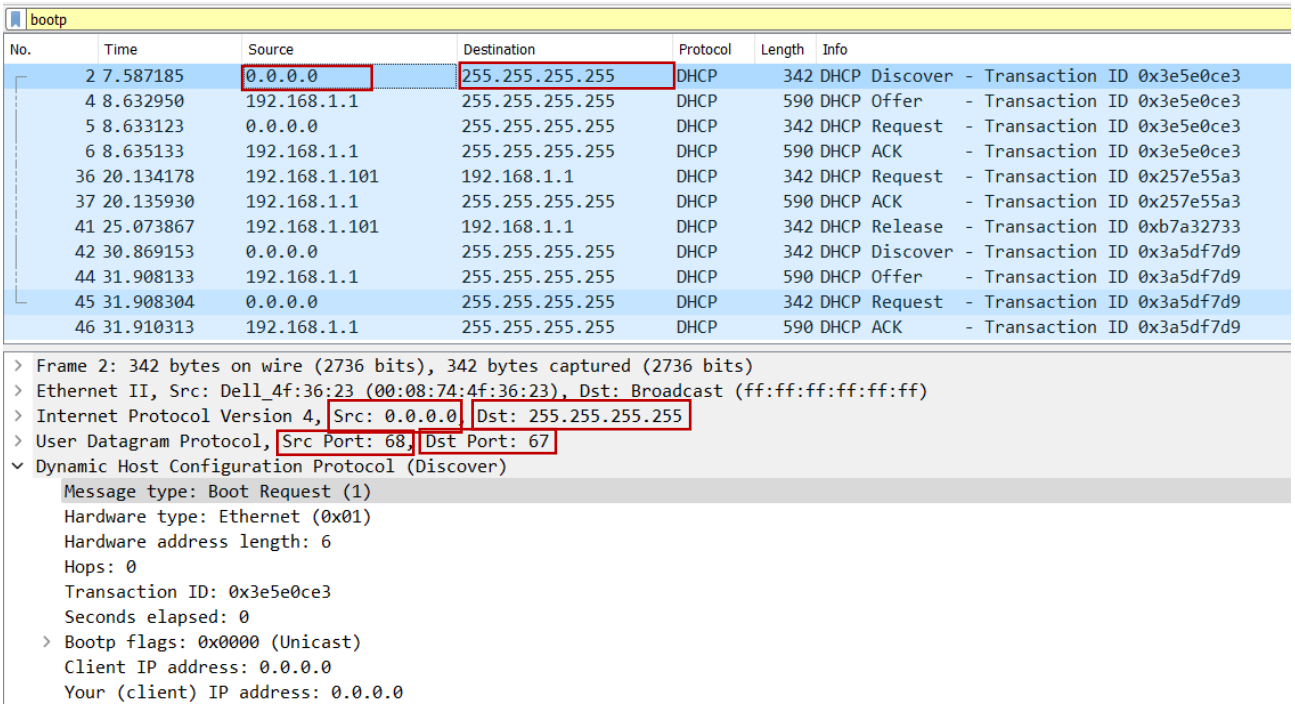


Fig. 1. DHCP Discover.

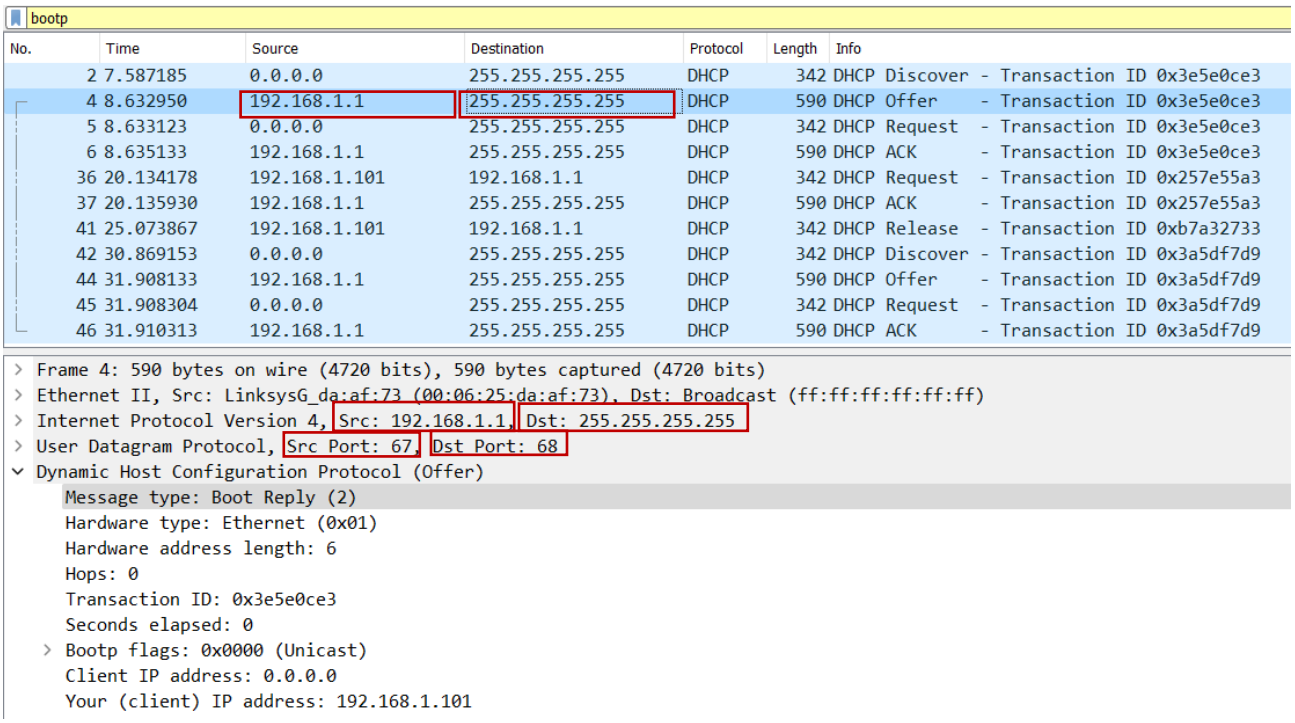
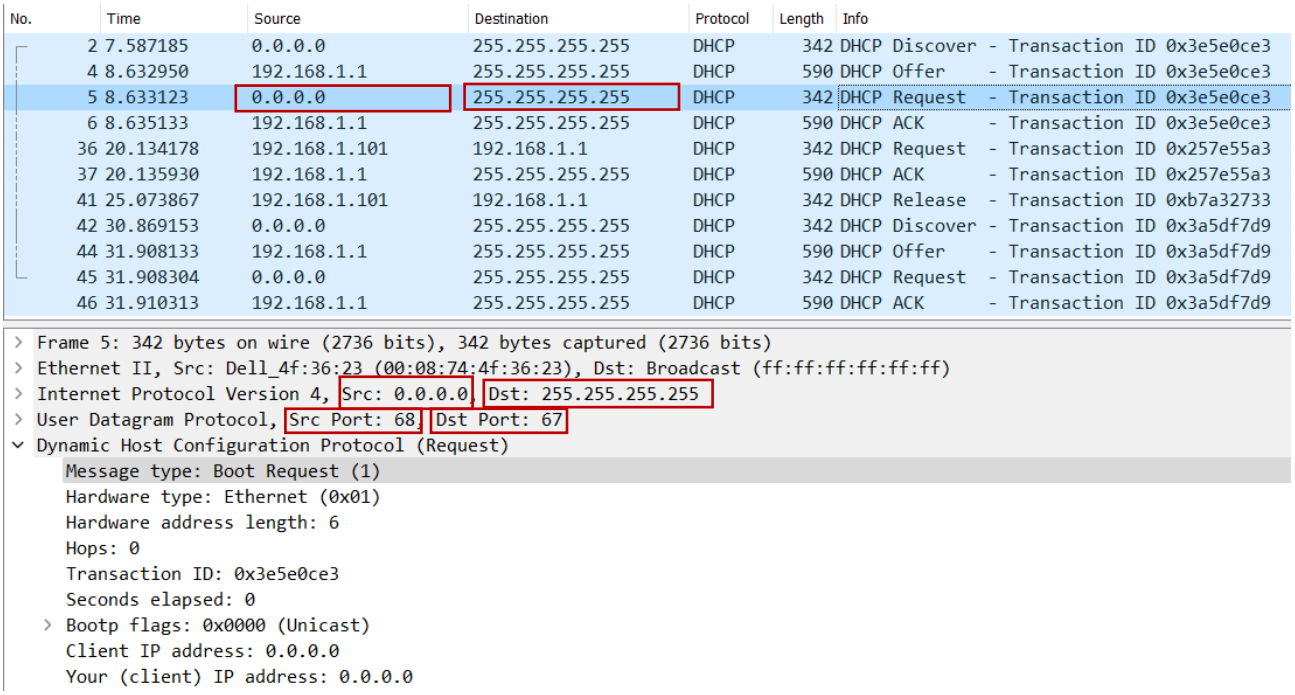


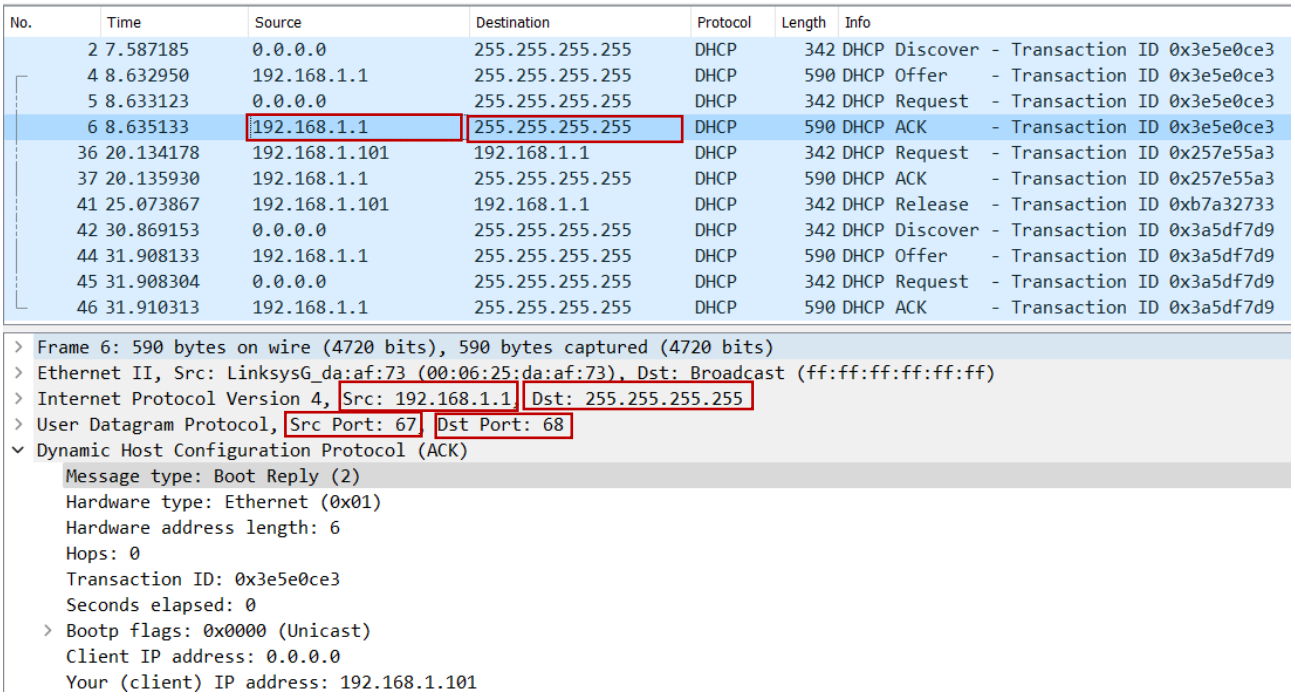
Fig. 2. DHCP Offer.



No.	Time	Source	Destination	Protocol	Length	Info
2	7.587185	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3e5e0ce3
4	8.632950	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3e5e0ce3
5	8.633123	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3e5e0ce3
6	8.635133	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x3e5e0ce3
36	20.134178	192.168.1.101	192.168.1.1	DHCP	342	DHCP Request - Transaction ID 0x257e55a3
37	20.135930	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x257e55a3
41	25.073867	192.168.1.101	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0xb7a32733
42	30.869153	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3a5df7d9
44	31.908133	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3a5df7d9
45	31.908304	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3a5df7d9
46	31.910313	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x3a5df7d9

```
> Frame 5: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> 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: 0x3e5e0ce3
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
```

Fig. 3. DHCP Request.



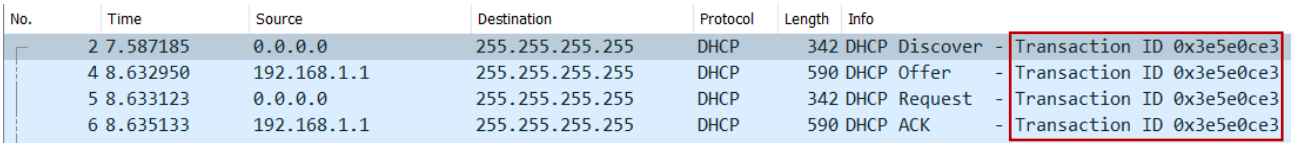
No.	Time	Source	Destination	Protocol	Length	Info
2	7.587185	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3e5e0ce3
4	8.632950	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3e5e0ce3
5	8.633123	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3e5e0ce3
6	8.635133	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x3e5e0ce3
36	20.134178	192.168.1.101	192.168.1.1	DHCP	342	DHCP Request - Transaction ID 0x257e55a3
37	20.135930	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x257e55a3
41	25.073867	192.168.1.101	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0xb7a32733
42	30.869153	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3a5df7d9
44	31.908133	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3a5df7d9
45	31.908304	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3a5df7d9
46	31.910313	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x3a5df7d9

```
> Frame 6: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 255.255.255.255
> 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: 0x3e5e0ce3
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.1.101
```

Fig. 4. DHCP ACK.

b. What is the value of the Transaction-ID in the first four DHCP messages (DHCP Discover/Offer/Request/ACK)? What are the values of the Transaction-ID in the second set of messages (DHCP Request/ACK)? What is the purpose of the Transaction-ID field?

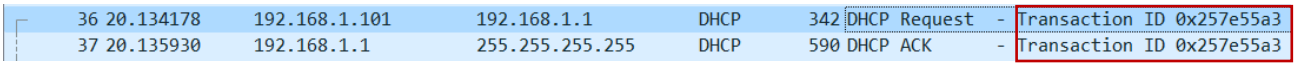
According to Fig.5, the value of the Transaction-ID in the first four DHCP messages (DHCP Discover/Offer/Request/ACK) is `0x3e5e0ce3`



No.	Time	Source	Destination	Protocol	Length	Info
2	7.587185	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3e5e0ce3
4	8.632950	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3e5e0ce3
5	8.633123	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3e5e0ce3
6	8.635133	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x3e5e0ce3

Fig.5 Transaction IDs of the first four DHCP messages

According to Fig.6 the values of the Transaction-ID in the second set of messages (DHCP Request/ACK) is `0x257e55a3`



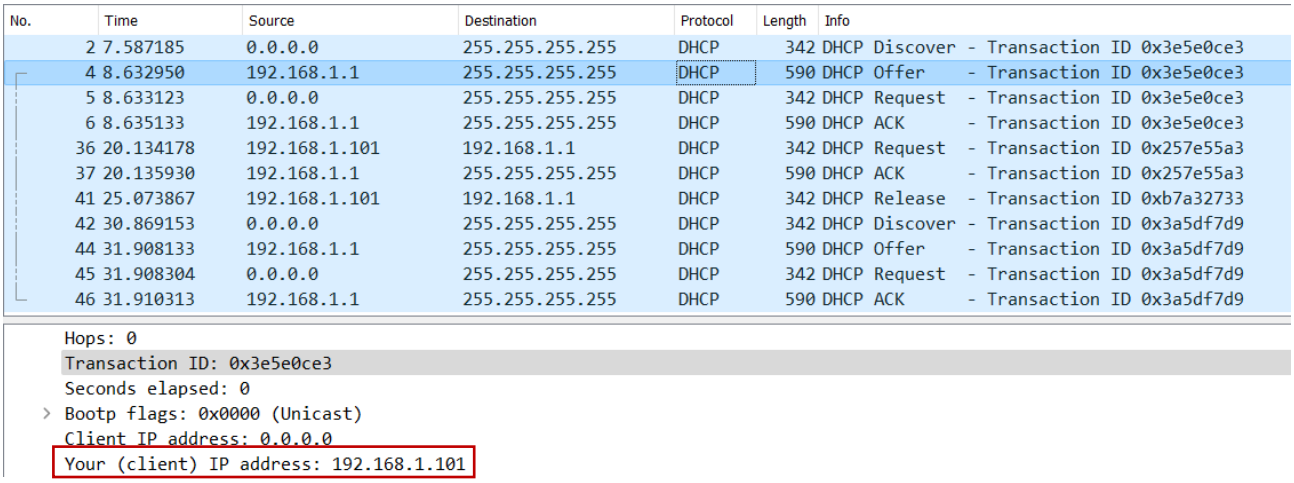
36	20.134178	192.168.1.101	192.168.1.1	DHCP	342	DHCP Request - Transaction ID 0x257e55a3
37	20.135930	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x257e55a3

Fig.6. Transaction IDs of the second set of DHCP messages

The purpose of the Transaction-ID is that the host can differentiate between the different requests made by the user.

c. The DHCP server offers a specific IP address to the client with the DHCP Offer message. What IP address is the DHCP server offering to the host in the first DHCP Offer message? In addition, what are the router address, subnet mask, domain name, and Domain Name Server given in the DHCP Offer message?

According to Fig.7, the IP address offered to the host in the first DHCP Offer message is `192.168.1.101` .



No.	Time	Source	Destination	Protocol	Length	Info
2	7.587185	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3e5e0ce3
4	8.632950	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3e5e0ce3
5	8.633123	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3e5e0ce3
6	8.635133	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x3e5e0ce3
36	20.134178	192.168.1.101	192.168.1.1	DHCP	342	DHCP Request - Transaction ID 0x257e55a3
37	20.135930	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x257e55a3
41	25.073867	192.168.1.101	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0xb7a32733
42	30.869153	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3a5df7d9
44	31.908133	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3a5df7d9
45	31.908304	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3a5df7d9
46	31.910313	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x3a5df7d9

```
Hops: 0
Transaction ID: 0x3e5e0ce3
Seconds elapsed: 0
> Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 192.168.1.101
```

Fig.7. the IP address offered to the host in the first DHCP message

According to Fig.8 the router address is `192.168.1.1` , subnet mask is `255.255.255.0`, domain name is `ne2.client2.attbi.com` , and the Domain Name Server is `63.240.76.19` `204.127.198.19` .

No.	Time	Source	Destination	Protocol	Length	Info
2	7.587185	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3e5e0ce3
4	8.632950	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3e5e0ce3
5	8.633123	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3e5e0ce3
6	8.635133	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x3e5e0ce3
36	20.134178	192.168.1.101	192.168.1.1	DHCP	342	DHCP Request - Transaction ID 0x257e55a3
37	20.135930	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x257e55a3
41	25.073867	192.168.1.101	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0xb7a32733
42	30.869153	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3a5df7d9
44	31.908133	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3a5df7d9
45	31.908304	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3a5df7d9
46	31.910313	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x3a5df7d9

```
Magic cookie: DHCP
Option: (53) DHCP Message Type (Offer)
    Length: 1
    DHCP: Offer (2)
Option: (1) Subnet Mask (255.255.255.0)
    Length: 4
    Subnet Mask: 255.255.255.0
Option: (3) Router
    Length: 4
    Router: 192.168.1.1
Option: (6) Domain Name Server
    Length: 8
    Domain Name Server: 63.240.76.19
    Domain Name Server: 204.127.198.19
Option: (15) Domain Name
    Length: 22
    Domain Name: ne2.client2.attbi.com
```

Fig.8. The router address, subnet mask, domain name, and Domain Name Server

d. In the client's response (DHCP Request) to the server's first DHCP Offer message, does the client accept the offered IP address? How can you tell?

According to Fig.9, the client has accepted the offered IP Address. You can tell that it matches the IP address in the previous offer message.

4	8.632950	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3e5e0ce3
5	8.633123	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3e5e0ce3
6	8.635133	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x3e5e0ce3
36	20.134178	192.168.1.101	192.168.1.1	DHCP	342	DHCP Request - Transaction ID 0x257e55a3
37	20.135930	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x257e55a3
41	25.073867	192.168.1.101	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0xb7a32733
42	30.869153	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3a5df7d9
44	31.908133	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3a5df7d9
45	31.908304	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3a5df7d9
46	31.910313	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x3a5df7d9

```
> Frame 4: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 67, Dst Port: 68
v Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x3e5e0ce3
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.1.101
```

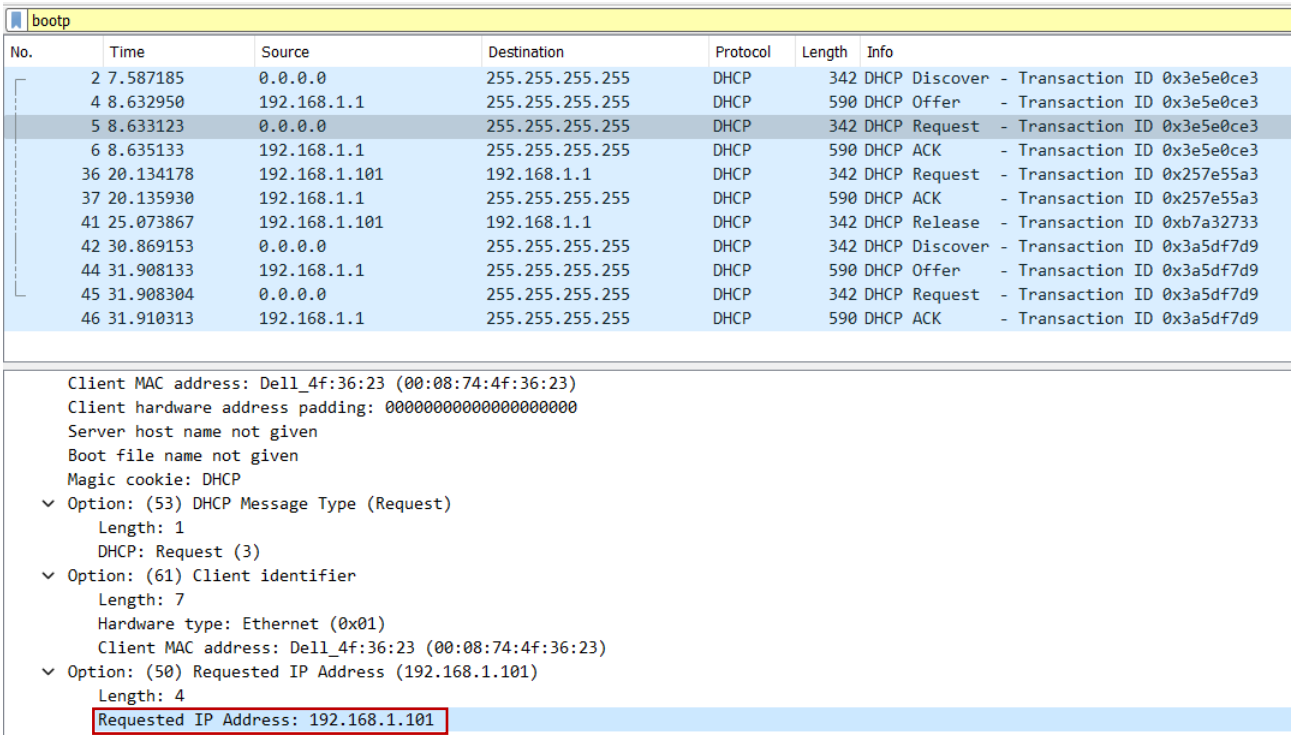


Fig.9 Response to offered IP Address

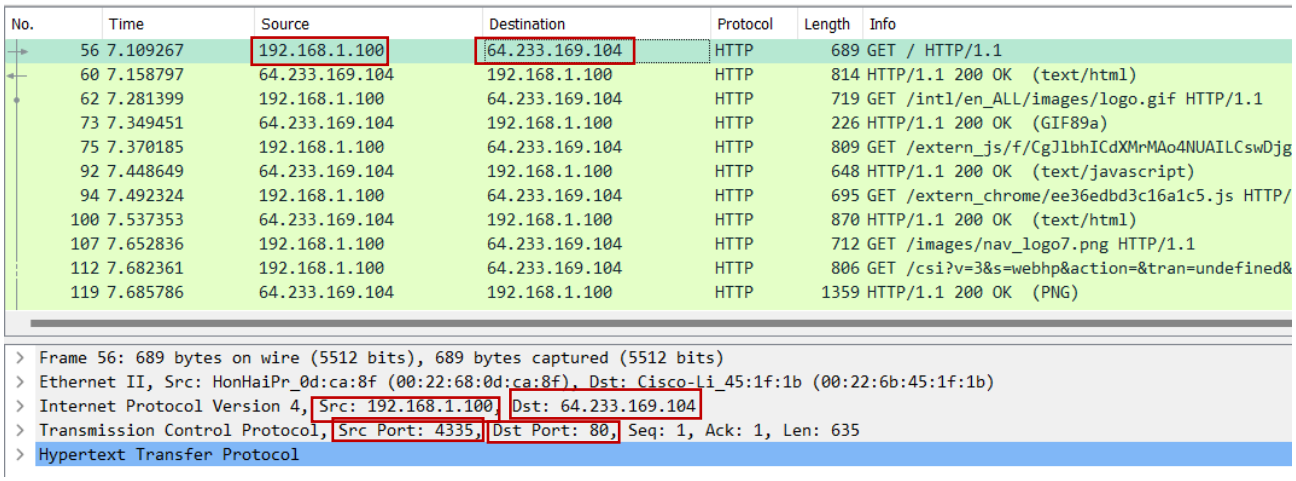
e. To release an allocated IP address, a client sends a DHCP Release message to the DHCP server. Does the DHCP server issue an acknowledgment of receipt of the client's DHCP request? What would happen if the client's DHCP Release message is lost?

The server does not send an ACK of the receipt of the client's DHCP Release message. If the client's DHCP Release message is lost the client will release the IP address, however, the server will not assign that IP address to someone else until the lease time expires.

4.

a. Consider now the HTTP GET sent from the client to the Google server (whose IP address is 64.233.169.104) at time 7.109267. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?
According to Fig.10,

Message	Source Address	Destination Address	Source Port	Destination Port
HTTP Get	192.168.1.100	64.233.169.104	4335	80



No.	Time	Source	Destination	Protocol	Length	Info
56	7.109267	192.168.1.100	64.233.169.104	HTTP	689	GET / HTTP/1.1
60	7.158797	64.233.169.104	192.168.1.100	HTTP	814	HTTP/1.1 200 OK (text/html)
62	7.281399	192.168.1.100	64.233.169.104	HTTP	719	GET /intl/en_ALL/images/logo.gif HTTP/1.1
73	7.349451	64.233.169.104	192.168.1.100	HTTP	226	HTTP/1.1 200 OK (GIF89a)
75	7.370185	192.168.1.100	64.233.169.104	HTTP	809	GET /extern_js/f/CgJlbhICdXMrMAo4NUAILCswDjg
92	7.448649	64.233.169.104	192.168.1.100	HTTP	648	HTTP/1.1 200 OK (text/javascript)
94	7.492324	192.168.1.100	64.233.169.104	HTTP	695	GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/
100	7.537353	64.233.169.104	192.168.1.100	HTTP	870	HTTP/1.1 200 OK (text/html)
107	7.652836	192.168.1.100	64.233.169.104	HTTP	712	GET /images/nav_logo7.png HTTP/1.1
112	7.682361	192.168.1.100	64.233.169.104	HTTP	806	GET /csi?v=3&s=webhp&action=&tran=undefined&
119	7.685786	64.233.169.104	192.168.1.100	HTTP	1359	HTTP/1.1 200 OK (PNG)

```
> Frame 56: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)
> Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
> Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104
> Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
> Hypertext Transfer Protocol
```

Fig.10. IP addresses and Ports

b. At what time is the corresponding HTTP 200 OK message for the above HTTP GET message received from the HTTP server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

According to Fig.11. Time OK message was received, `7.158797`. The source and destination IP addresses and TCP source and destination ports have the answer in the following table

Message	Source Address	Destination Address	Source Port	Destination Port
HTTP 200 OK	64.233.169.104	192.168.1.100	80	4335

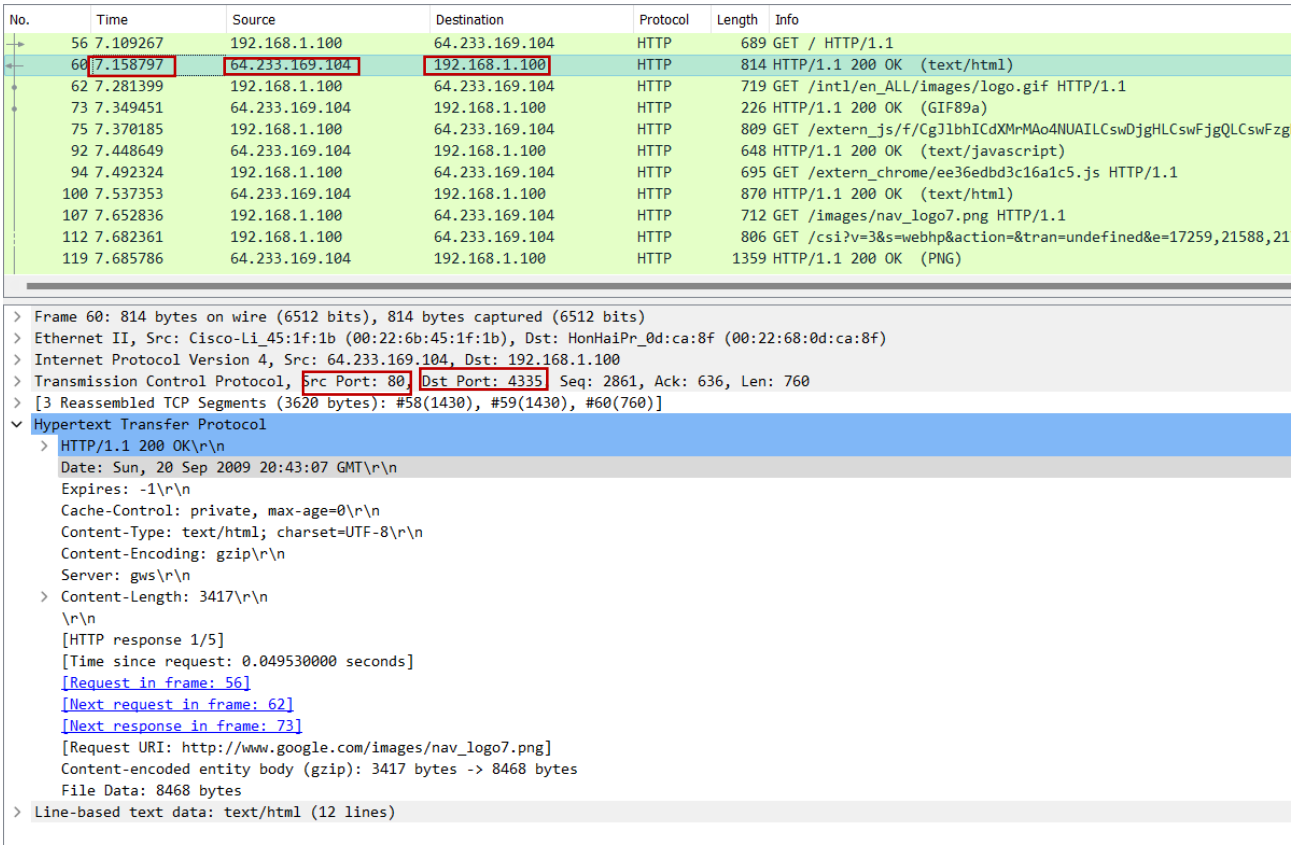


Fig.11

c.

i. - At what time is the client-to-server TCP SYN segment sent that sets up the connection used by the HTTP GET sent at time 7.109267? What are the source and destination IP addresses and source and destination ports for the TCP SYN segment?

According to fig.12, SYN segment time was sent at 7.075657 and the source and destination IP addresses and source and destination ports for the TCP SYN segment are as follows.

Message	Source Address	Destination Address	Source Port	Destination Port
TCP SYN	192.168.1.100	64.233.169.104	Src Port: 4335,	Dst Port: 80,

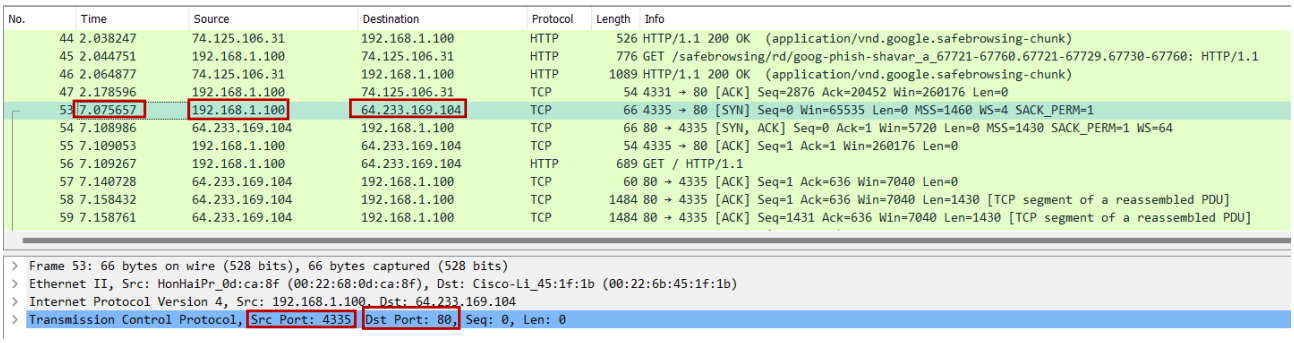


Fig.12

ii. What are the source and destination IP addresses and source and destination ports of the TCP SYN/ACK sent in response to the TCP SYN? At what time is this TCP SYN/ACK sent from the server?
According to Fig.13, the source and destination IP addresses and source and destination ports of the TCP SYN/ACK sent in response to the TCP SYN are as follows. And the time this TCP SYN/ACK is sent from the server is 7.108986.

Message	Source Address	Destination Address	Source Port	Destination Port
TCP SYN/ACK	64.233.169.104	192.168.1.100	Src Port: 80,	Dst Port: 4335,

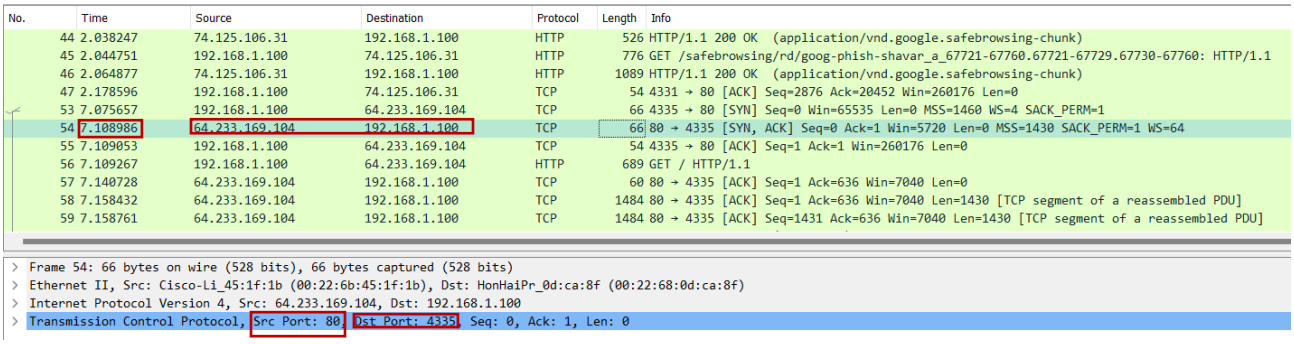


Fig.13

iii. What are the source and destination IP addresses and source and destination ports of the TCP ACK segment sent at the end of the three-way handshake? At what time is this TCP ACK sent from the client?
According to Fig.14, the source and destination IP addresses and source and destination ports of the TCP ACK segment sent at the end of the three-way handshake are as follows. The time this TCP ACK sent from the client is 7.109053.

Message	Source Address	Destination Address	Source Port	Destination Port
TCP ACK	192.168.1.100	64.233.169.104	Src Port: 4335,	Dst Port: 80,

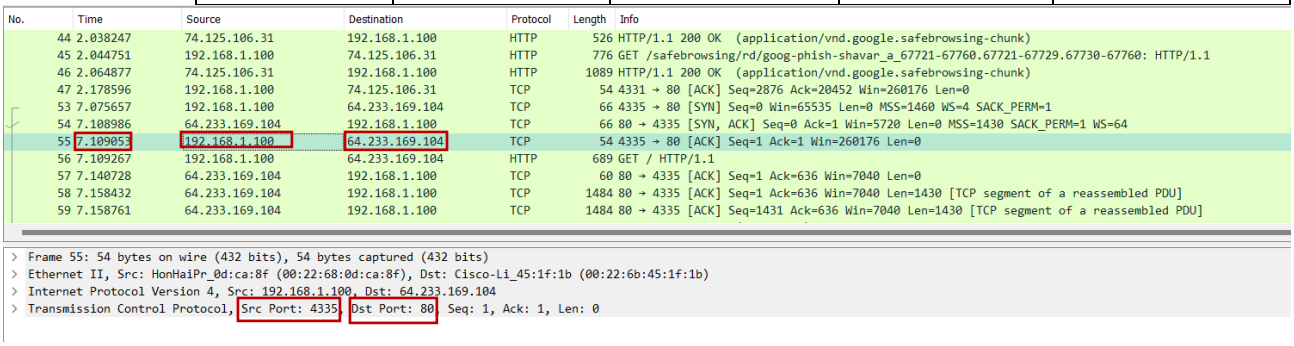


Fig.14

5. NAT_ISP_side.pcap
   a. In the trace file NAT_ISP_side.pcap, find the HTTP GET message was sent from the client to the Google server (whose IP address is 64.233.169.104) at time 7.109267 (where t=7.109267 is time at which this was sent as recorded in the trace file NAT_home_side.pcap). At what time does this message appear in the trace file NAT_ISP_side.pcap? What are the source and destination IP addresses and TCP source and

destination ports on the IP datagram carrying this HTTP GET (as recording in the trace file NAT_ISP_side.pcap)? Which of these fields are the same as, and which are different from, your answer to question 4.a) above?

According to fig. 15, the message appears in the trace file at 6.069168 and the source and destination IP addresses and TCP source and destination ports on the IP datagram is as follows. The source address and time are the different fields. All the rest (destination address and port and source port) are the same.

Message	Source Address	Destination Address	Source Port	Destination Port
HTTP GET	71.192.34.104	64.233.169.104	Src Port: 4335,	Dst Port: 80,

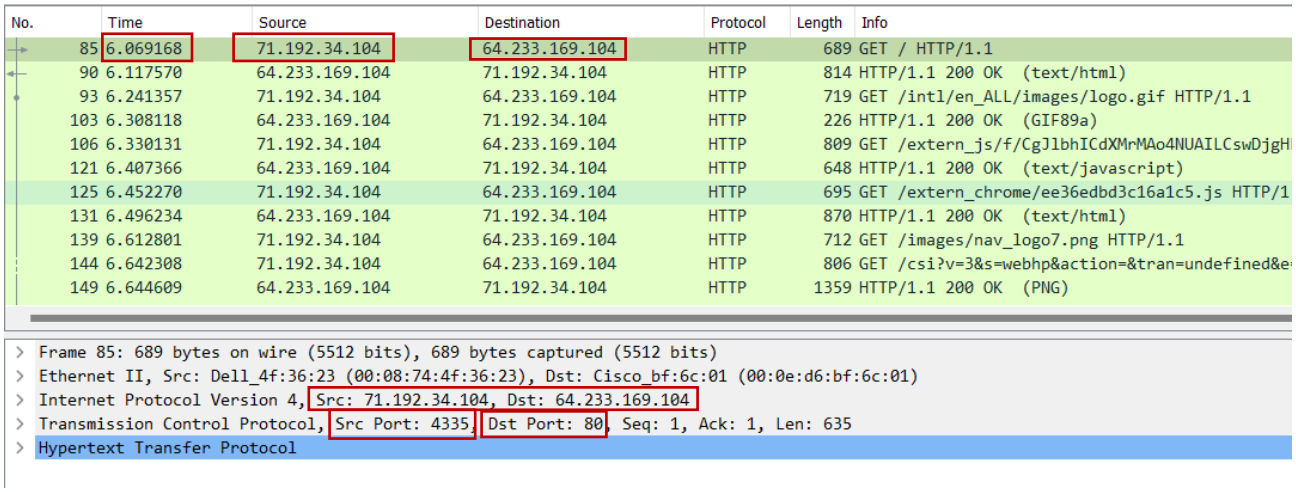
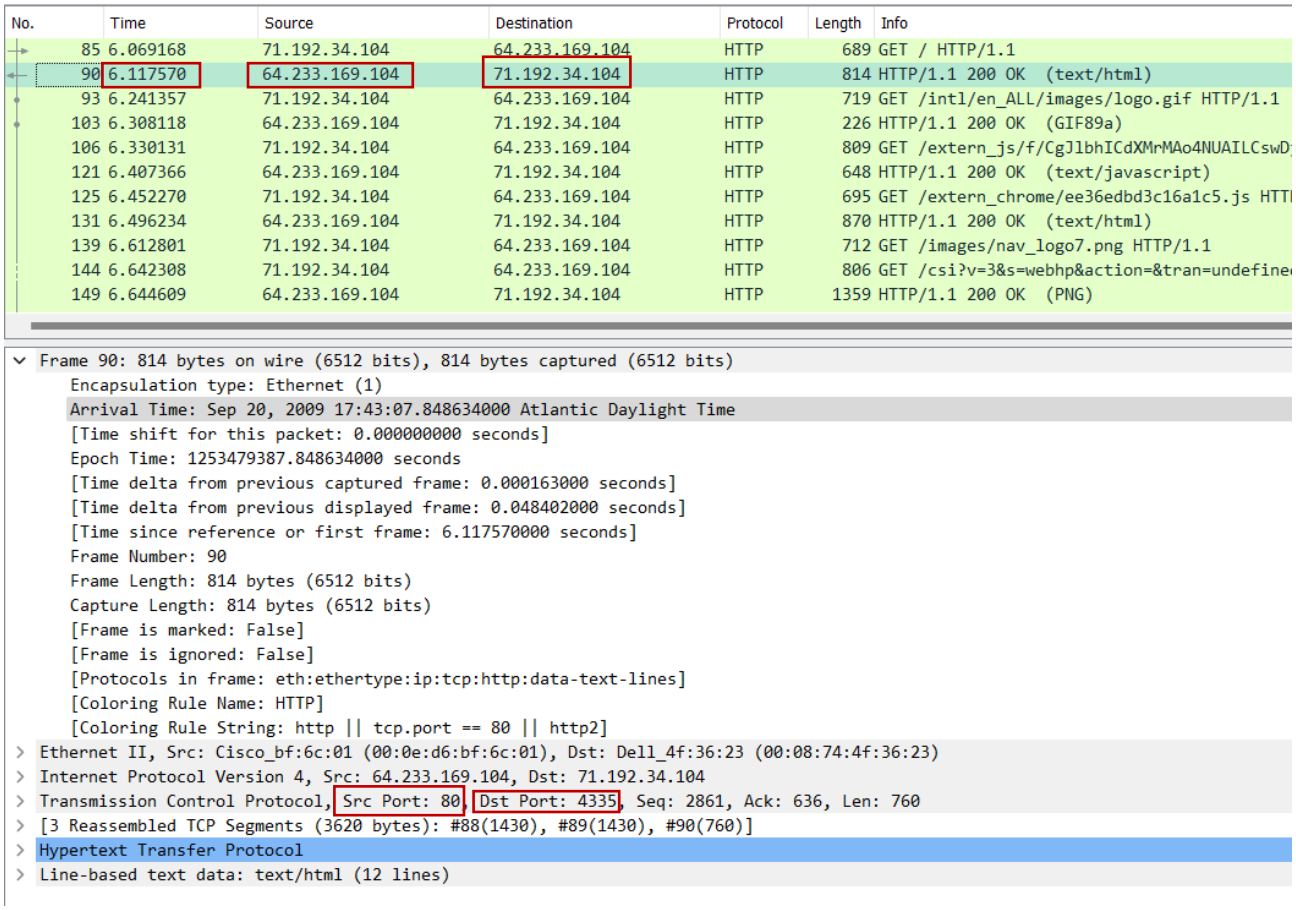


Fig.15

b. In the trace file NAT_ISP_side.pcap, at what time is the first HTTP 200 OK message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message? Which of these fields are the same as, and which are different from, your answer to question 4.b) above?

According to fig.16, the time the first HTTP 200 OK message received from the Google server is 6.117570. The source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message are as follows. The destination address and time fields are different. All the other fields (source address and port and destination port) are the similar.

Message	Source Address	Destination Address	Source Port	Destination Port
HTTP 200 OK	64.233.169.104	71.192.34.104	Src Port: 80	Dst Port: 4335



No.	Time	Source	Destination	Protocol	Length	Info
85	6.069168	71.192.34.104	64.233.169.104	HTTP	689	GET / HTTP/1.1
90	6.117570	64.233.169.104	71.192.34.104	HTTP	814	HTTP/1.1 200 OK (text/html)
93	6.241357	71.192.34.104	64.233.169.104	HTTP	719	GET /intl/en_ALL/images/logo.gif HTTP/1.1
103	6.308118	64.233.169.104	71.192.34.104	HTTP	226	HTTP/1.1 200 OK (GIF89a)
106	6.330131	71.192.34.104	64.233.169.104	HTTP	809	GET /extern_js/f/CgJlbhICdXMrMAo4NUAILCswD
121	6.407366	64.233.169.104	71.192.34.104	HTTP	648	HTTP/1.1 200 OK (text/javascript)
125	6.452270	71.192.34.104	64.233.169.104	HTTP	695	GET /extern_chrome/ee36edbd3c16a1c5.js HTT
131	6.496234	64.233.169.104	71.192.34.104	HTTP	870	HTTP/1.1 200 OK (text/html)
139	6.612801	71.192.34.104	64.233.169.104	HTTP	712	GET /images/nav_logo7.png HTTP/1.1
144	6.642308	71.192.34.104	64.233.169.104	HTTP	806	GET /csi?v=3&s=webhp&action=&tran=undefine
149	6.644609	64.233.169.104	71.192.34.104	HTTP	1359	HTTP/1.1 200 OK (PNG)

```
Frame 90: 814 bytes on wire (6512 bits), 814 bytes captured (6512 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 20, 2009 17:43:07.848634000 Atlantic Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1253479387.848634000 seconds
    [Time delta from previous captured frame: 0.000163000 seconds]
    [Time delta from previous displayed frame: 0.048402000 seconds]
    [Time since reference or first frame: 6.117570000 seconds]
    Frame Number: 90
    Frame Length: 814 bytes (6512 bits)
    Capture Length: 814 bytes (6512 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
> Ethernet II, Src: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
> Internet Protocol Version 4, Src: 64.233.169.104, Dst: 71.192.34.104
> Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 2861, Ack: 636, Len: 760
> [3 Reassembled TCP Segments (3620 bytes): #88(1430), #89(1430), #90(760)]
> Hypertext Transfer Protocol
> Line-based text data: text/html (12 lines)
```

Fig.16

c. In the trace file NAT_ISP_side.pcap, answer the same question as in 4.c)? Which of these fields are the same as, and which are different from, your answer to question 4.c) above?

   i. According to fig.17, SYN segment time was sent at 6.035475 and the source and destination IP addresses and source and destination ports for the TCP SYN segment are as follows. The source address and time fields are the same. All the other fields (destination address and port and source port) are similar.

Message	Source Address	Destination Address	Source Port	Destination Port
TCP SYN	71.192.34.104	64.233.169.104	Src Port: 4335	Dst Port: 80

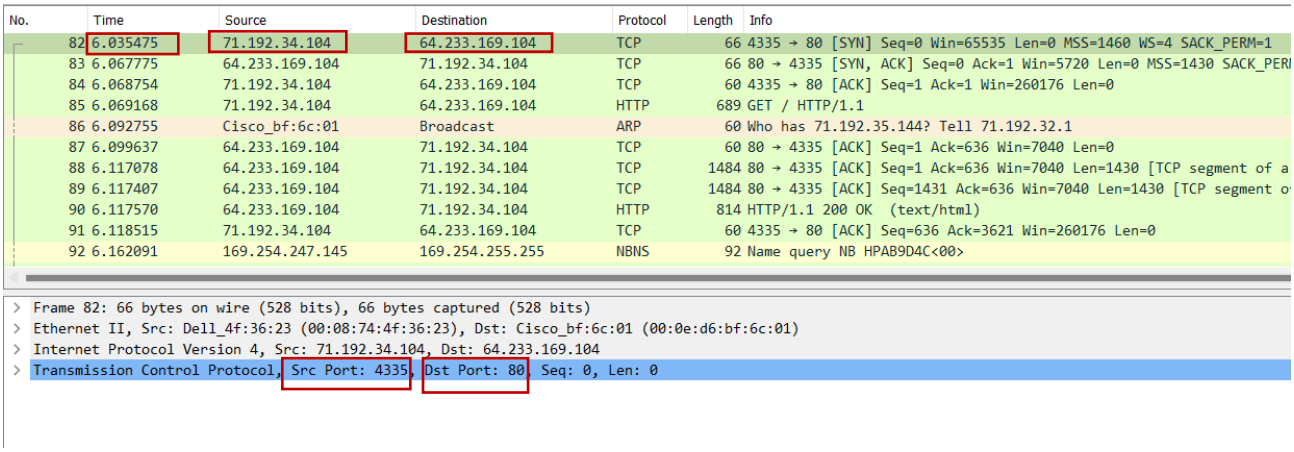


Fig17

ii. What are the source and destination IP addresses and source and destination ports of the TCP SYN/ACK sent in response to the TCP SYN? At what time is this TCP SYN/ACK sent from the server?

According to Fig.18, the source and destination IP addresses and source and destination ports of the TCP SYN/ACK sent in response to the TCP SYN are as follows. And the time this TCP SYN/ACK is sent from the server is 6.067775. The destination address and time fields are different. All the other (source address and port and destination port) fields are similar.

Message	Source Address	Destination Address	Source Port	Destination Port
TCP SYN/ACK	64.233.169.104	71.192.34.104	Src Port: 80	Dst Port: 4335

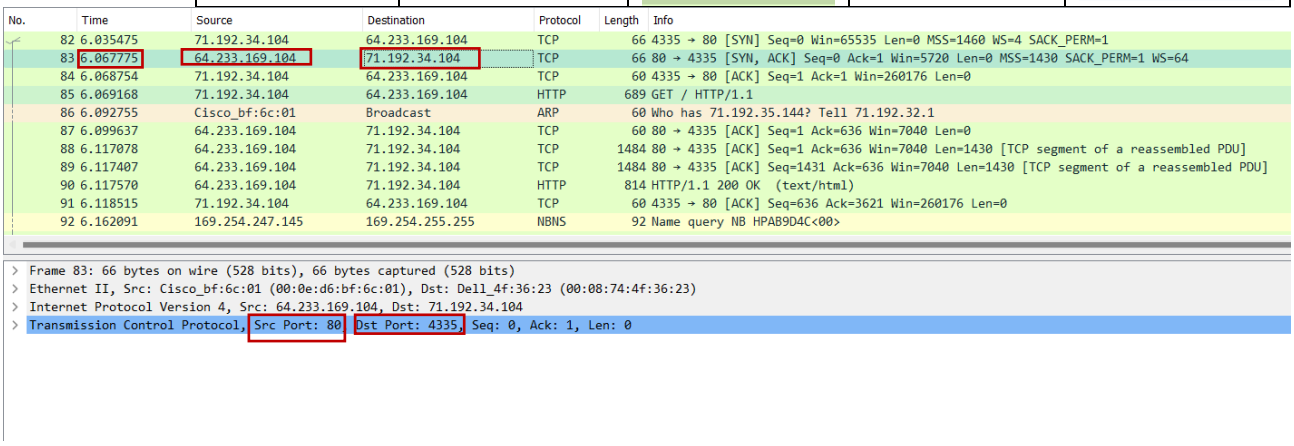


FIG18

iii. What are the source and destination IP addresses and source and destination ports of the TCP ACK segment sent at the end of the three-way handshake? At what time is this TCP ACK sent from the client?

According to Fig.19, the source and destination IP addresses and source and destination ports of the TCP ACK segment sent at the end of the three-way handshake are as follows. The time this TCP ACK sent from the client is 6.068754. The source address and time fields are the same. All the other fields (destination address and port and source port) are similar.

Message	Source Address	Destination Address	Source Port	Destination Port
TCP ACK	71.192.34.104	64.233.169.104	Src Port: 4335,	Dst Port: 80,

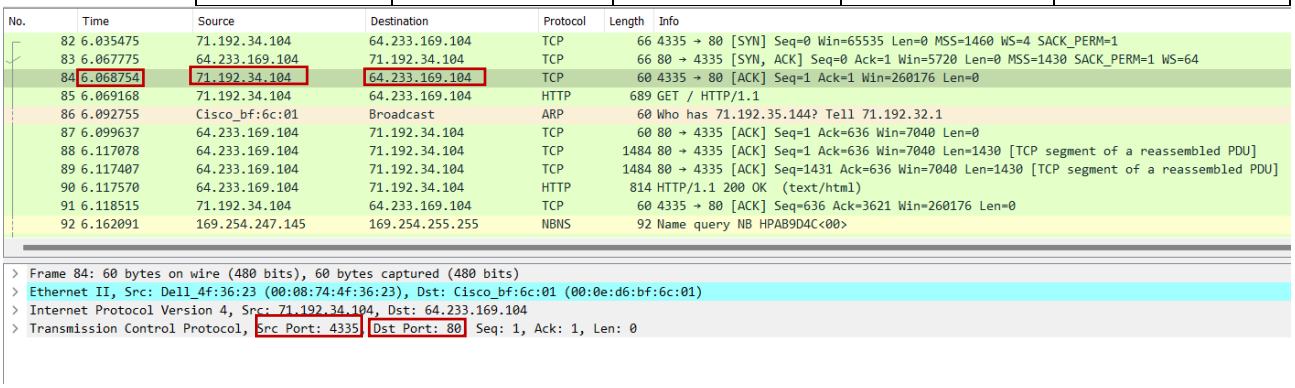


Fig19

d.

NAT Translation Table	
WAN Side	LAN Side
71.192.34.104 ,4335	192.168.1.100 ,4335