VIETNAM NATIONAL UNIVERSITY, HO CHI MINH CITY
UNIVERSITY OF TECHNOLOGY
FACULTY OF COMPUTER SCIENCE AND ENGINEERING

COMPUTER NETWORKING (CO3094)

LAB REPORT - WEEK 2

Advisor: Ths. Lê Bảo Thịnh
Students: Nguyễn Hữu Hiếu - 2013149.

HO CHI MINH CITY, MARCH 2023

Contents

1 Task 4a **2**

2 Task 4b **8**

3 Task 4c **15**

4 Task 5 **25**

5 Task 6 **30**

1 Task 4a

1. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window.

What is the IP address of your computer?

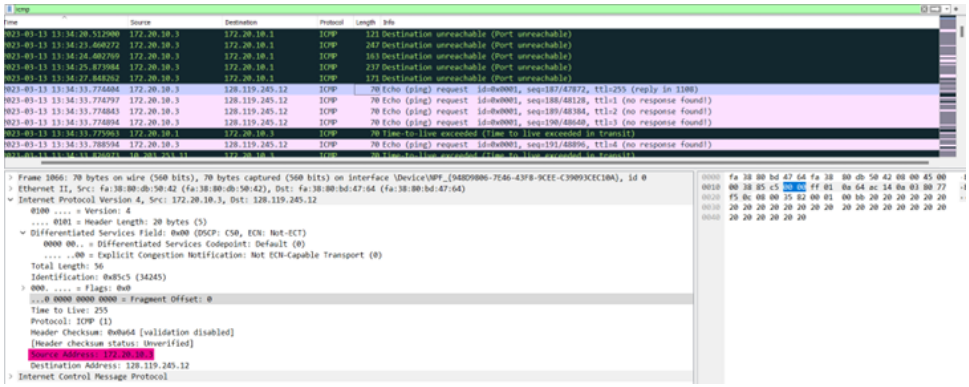

Figure. 1: The first ICMP Echo Request message

The IP address of my computer is 172.20.10.3

2. Within the IP packet header, what is the value in the upper layer protocol field?

Within the header, the value in the upper layer protocol field is ICMP (1)

3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.

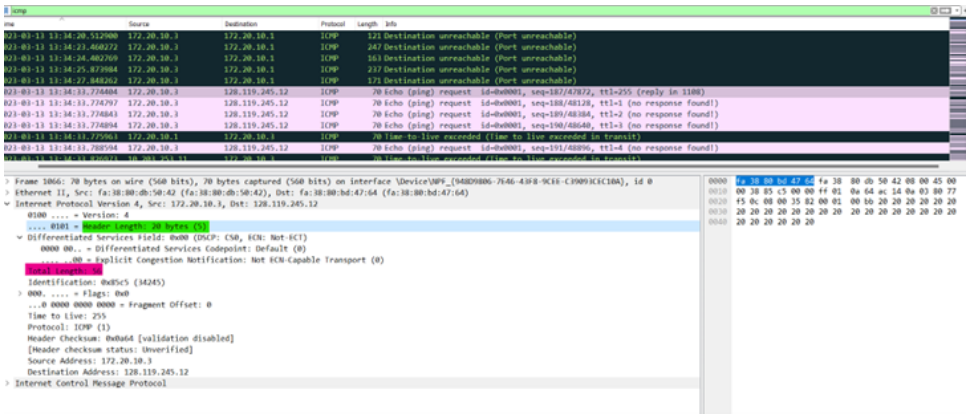

Figure. 2: ICMP Echo Request message

There are 20 bytes in the IP header and 56 bytes in the total of length, so this give 36 bytes in the payload of the IP datagram

4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

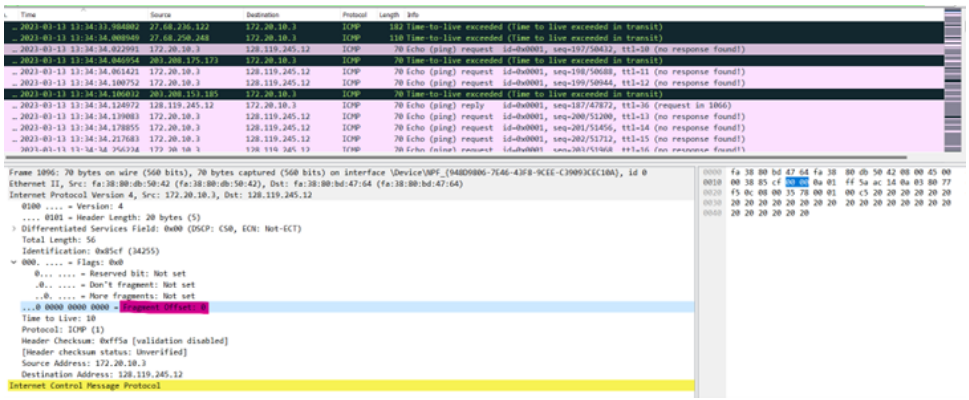

Figure. 3: ICMP Echo Request message

The fragment bits are equal to 0, so the data is not fragmented.

5. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?

   Identification, Header Checksum, and Time to Live always change from one datagram to the next.

6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

   The fields that stay constant across the IP datagrams:

   - Version (we are using IPV4 for all packets)
   - Header length (cause that is ICMP packets)
   - Source IP (we are sending from the same source, in this case, that is my IP address of my computer - 172.20.10.3)
   - Destination IP (we are sending to the same destination, in this case, that is http://gaia.cs.umass.edu)
   - Differentiated Services Field (all the packets are ICMP they use the same Type of Service class)
   - Upper Layer Protocol (cause all of these are ICMP packets)

   The fields must stay constant are the same as the fields they stay constant.

   The fields that must be changed are :

   - Identification (IP packets must have different ids)
   - Time to live (traceroute increments each subsequent packet)
   - Header checksum (since header changes, so must be checksum)

7. Describe the pattern you see in the values in the Identification field of the IP datagram.

   The pattern of the values in the Identification field increament with each ICMP Echo (ping) request.

8. What is the value in the Identification field and the TTL field? Look at *Figure. 4* we have:

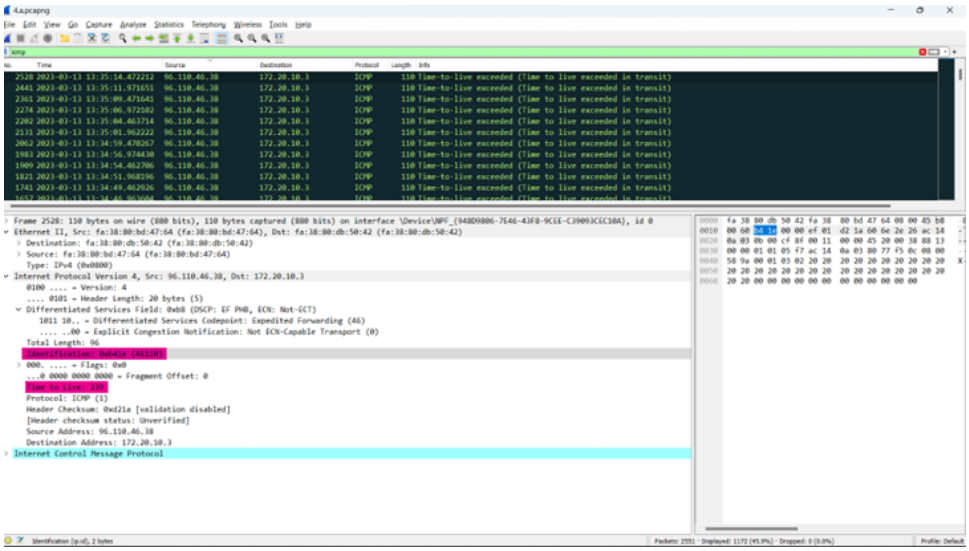

Figure. 4: Capture for Question 8

- The Identification: 46110
- The TTL: 239

9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

The identification field changes for all the ICMP TTL-exceeded replies sent, because the identification field is a unique value. When two or more IP datagrams have the same identification value, then it means that these IP datagrams are fragments of a single large IP datagram.

10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram?

Note: In this question, I had to change my Wifi, so my IP address (source IP) was changed too.

Look at *Figure. 5* Ans: Yes, the message has been fragmented across more than one IP datagram.

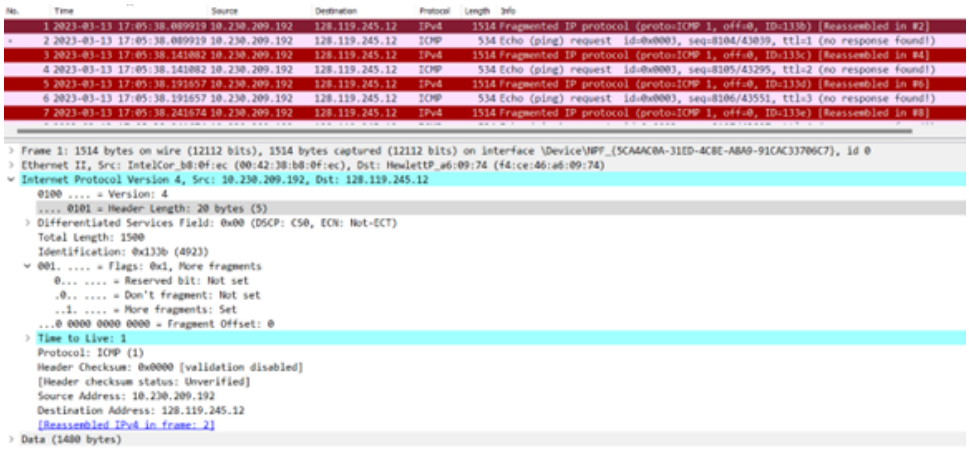

Figure. 5: Packet Size in pingplotter changed to 2000

11. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?

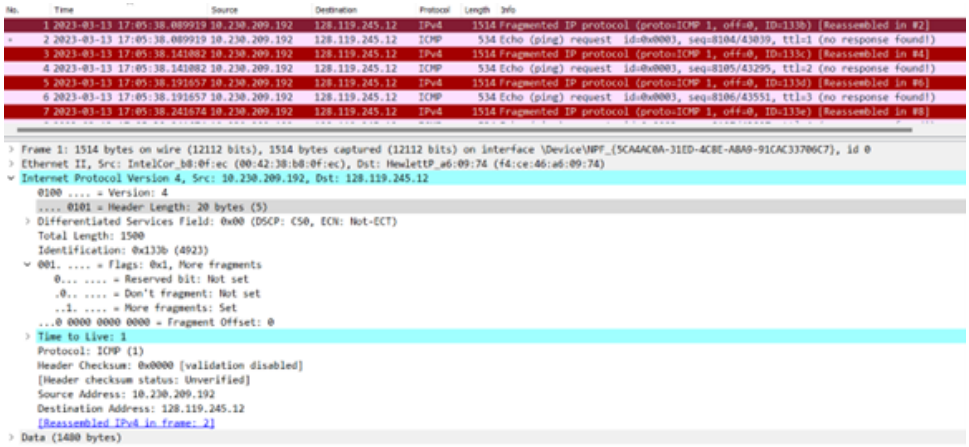

Figure. 6: Packet size 2000 - First fragment - Question 11

This datagram's Identification is 4293.

The Flags bit for "More fragments" is set (highlight by the green), indicating that the datagram has been fragmented.

The "Fragment Offset" is 0 (highlight by the purple), so that indicate this is first fragment.

This first datagram has a total length is 1500 (highlight by the orange), with 20 bytes of Header and 1480 bytes of data.

12. Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?

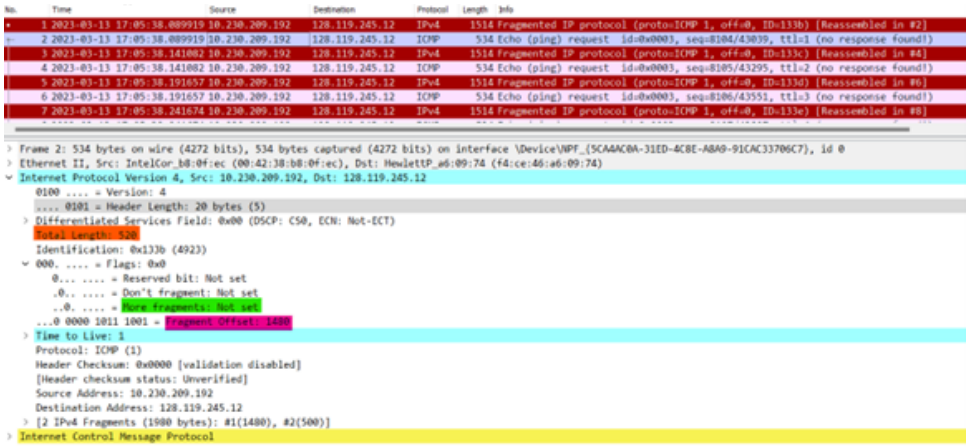

Figure. 7: Packet size 2000 - Second fragment - Question 12

This datagram has the same Identification (4293) as the one in Question 11, so two IP datagrams are fragments of a single large IP datagram.

The Fragment Offset (sign by the purple) is 1480, indicating that this is not the first one. It is the last fragment, since the more fragments flag is not set.

13. What fields change in the IP header between the first and second fragment? Then find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 3500.

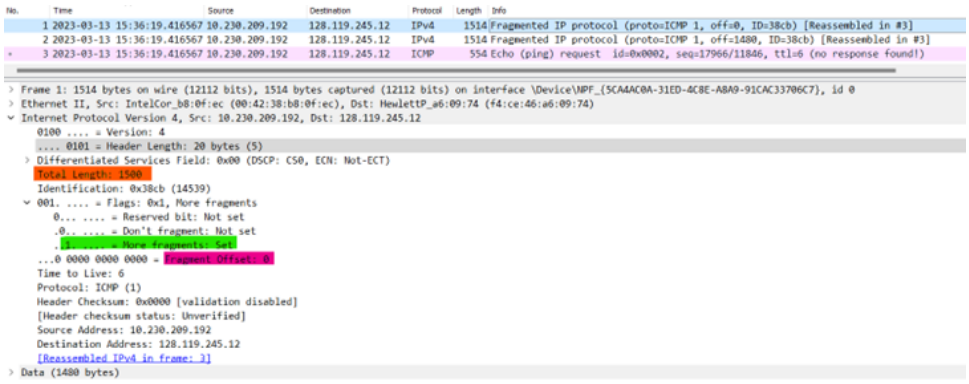

Figure. 8: Packet size 3500 - First fragment

The field changes in the IP header between the first and the second fragment: Flags bit for "Fragment Offset": The first one is 0, and the second is 1480.

14. How many fragments were created from the original datagram?

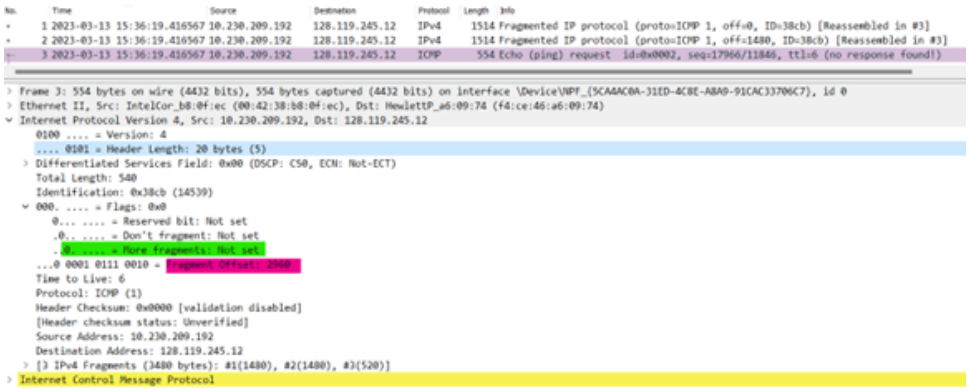

Figure. 9: **Packet size 3500 - Last fragment**

There are 3 fragments were created

15. 15. What fields change in the IP header among the fragments?

We see only one difference between the first and the second because there are three fragments for the large IP datagram. So it's just changed the Fragment Offset. But if we compare the first and the last one. Actually, there are three changes: the Fragment Offset, the Total length, and the flags bit for More fragments.

You can see the difference beetwen Figure 8 in Question 13 and Figure 9 in Question 14 to make it clear.

2 Task 4b

1. Are DHCP messages sent over UDP or TCP? They sent by UDP.

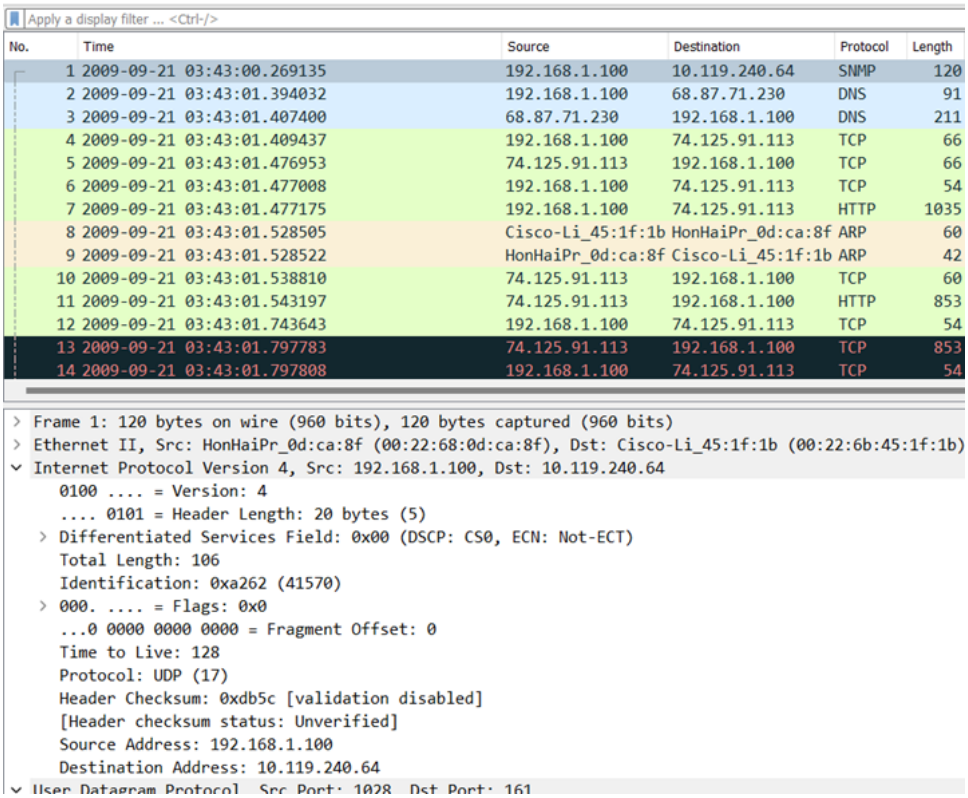

Figure. 10: WireShark Capture DHCP message

2. 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?

   Look at *Figure. 11* we have:

   - The Discover packet has a source port of 68 and a 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

   All of this corresponds to the example given in the lab.

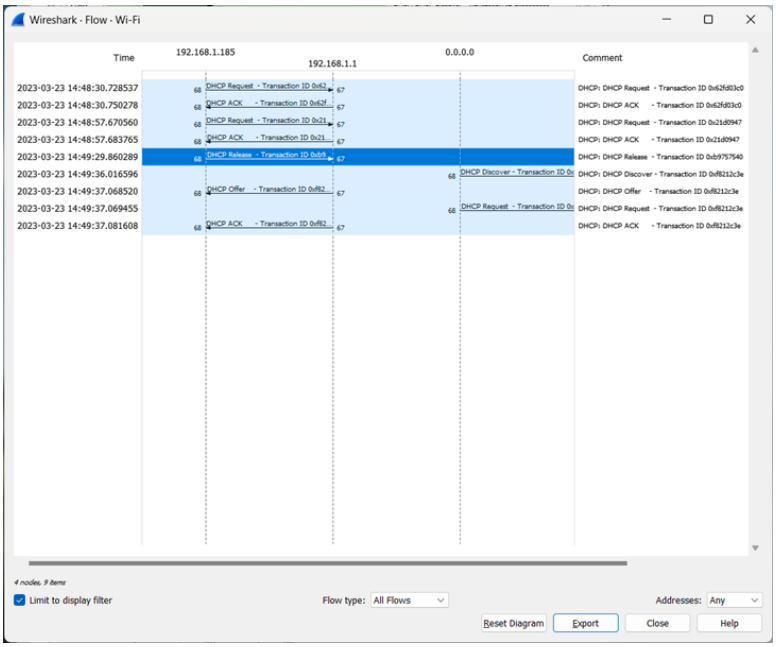

Figure. 11: Timing datagram

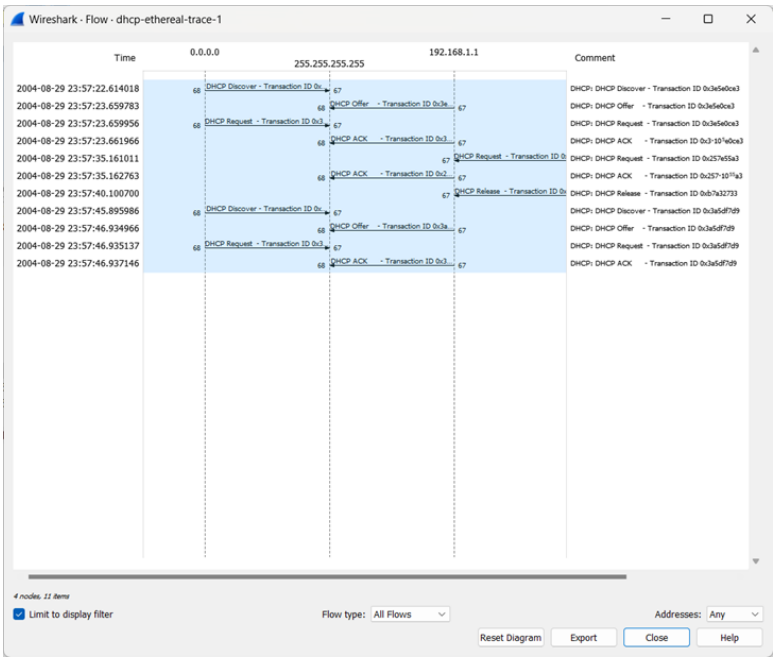

Figure. 12: Timing datagram <example lab>

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

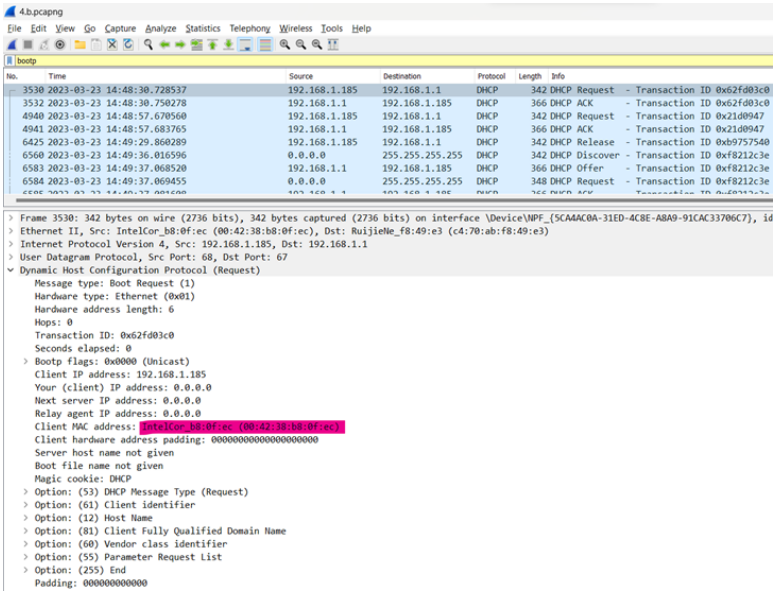

Figure. 13: WireShark Capture 4.b.3

The link-layer (e.g., Ethernet) address of my host is IntelCor_b8:0f:ec (00:42:38:b8:0f:ec)

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

Look at *Figure. 14 and Figure 15*

The discover message has a type value of 1 and the request message has a type value of a 3

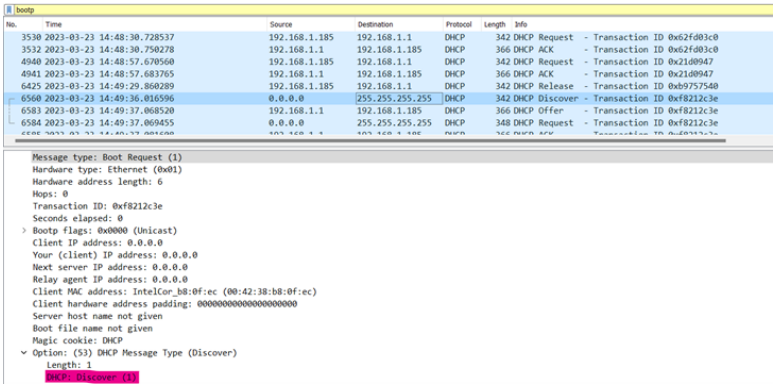

Figure. 14: Discover message

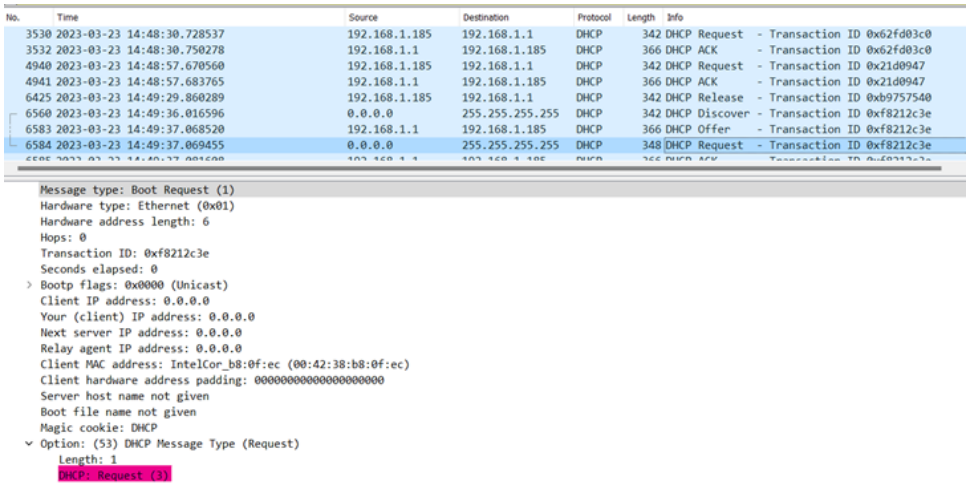

Figure. 15: Request message

5. 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?
The value of the Transaction-ID in each of the first DHCP messages is 0x5cf0dd80

The value of the Transaction-ID in each of the second DHCP messages is 0xeb5ee96b

The transaction ID identifies if a message is part of a set of messages related to one transaction

6. 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. *Note : I use the file dhcp-ethereal-trace-1 to answer this question.*
Look at *Figure 16*

- Discover source 0.0.0.0 Destination 255.255.255.255
- Offer source 192.168.1.1 Destination 255.255.255.255
- Request source 0.0.0.0 Destination 255.255.255.255
- ACK DHCP 192.168.1.1 Destination 255.255.255.255

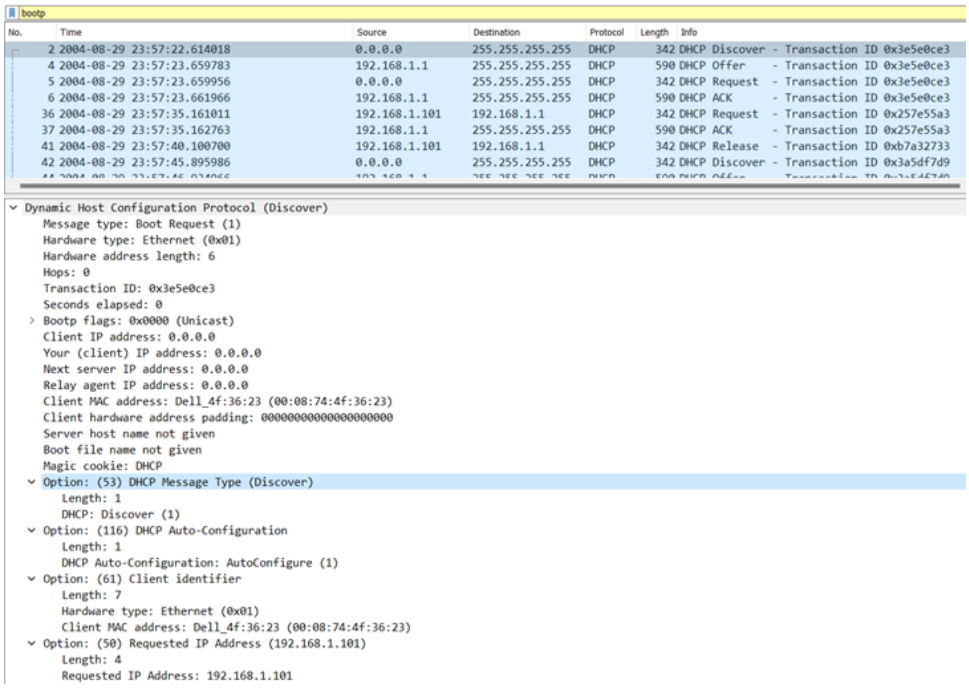

Figure. 16: Wireshark Capture for question 6

7. What is the IP address of your DHCP server?
The IP address of my DHCP server is 192.168.1.185

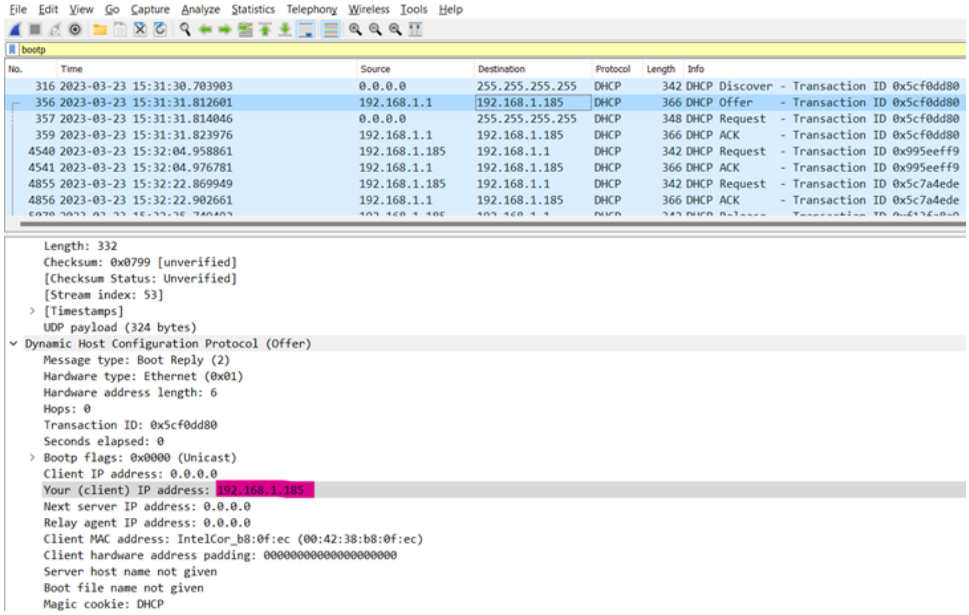

Figure. 17: Wireshark Capture for question 7

8. 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.

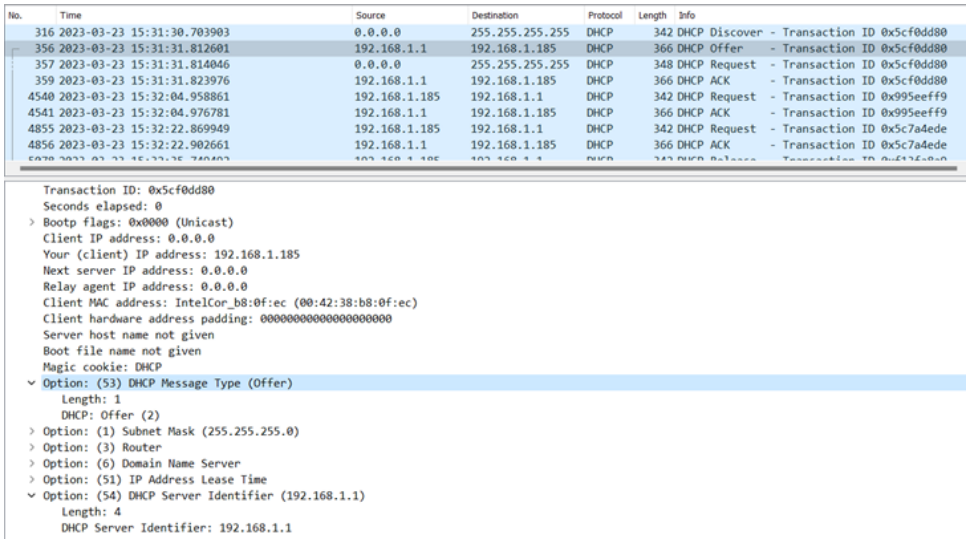

Figure. 18: Offer Message

The DHCP server offers 192.168.1.1 as the ip address in the DHCP offer message.

9. 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?

The IP address being 0.0.0.0 indicates the absence of a relay agent. There is no relay agent in my experiment.

10. Explain the purpose of the router and subnet mask lines in the DHCP offer message.

The IP address for the router identifies the default internet gateway. The subnet mask defines the subnet that is available.

11. 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?

Look at *Figure. 19*
The same thing occurs the host requests the offered IP address.
Option: (50) Requested IP Address (192.168.1.185)

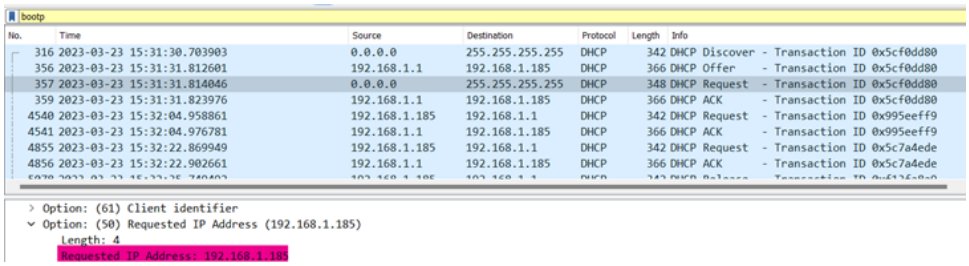

Figure. 19: Offer Message

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

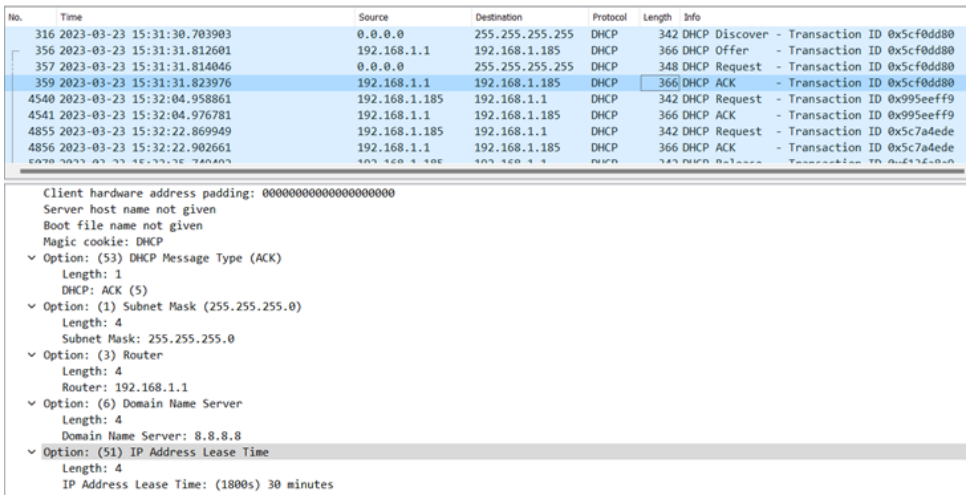

Figure. 20: Offer Message

The lease time is the amount of the time the user is aloud connection to the router

Option: (51) IP Address Lease Time

Length: 4

IP Address Lease Time: (1800s) 30 minutes

13. What is the purpose of the DHCP release message? 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 DHCP release message tells the DHCP server that you want to cancel the IP address offered. The DHCP server will not issue an ack of receipt of the client's DHCP request. If the release message is lost then the DHCP server retains the IP address until the lease time expires.

14. 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, there were arp packets sent and received to map the mac address with the IP address (192.168.1.185)

3 Task 4c

1. What is the IP address of the client?

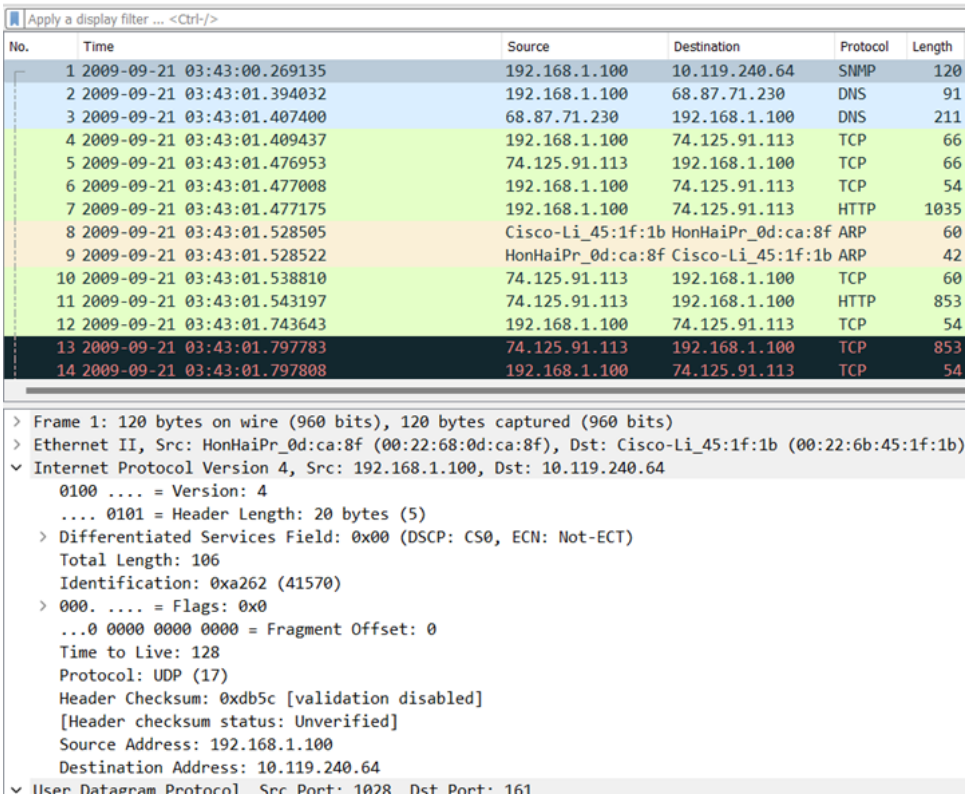

Figure. 21: WireShark Capture 4.a.1

The client's IP address is 192.168.1.100.

2. The client actually communicates with several different Google servers in order to implement "safe browsing." (See extra credit section at the end of this lab). The main Google server that will serve up the main Google web page has IP address 64.233.169.104. In order to display only those frames containing HTTP messages that are sent to/from this Google, server, enter the expression "http && ip.addr == 64.233.169.104" (without quotes) into the Filter: field in Wireshark.

3. Consider now the HTTP GET sent from the client to the Google server (whose IP address is IP address 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?

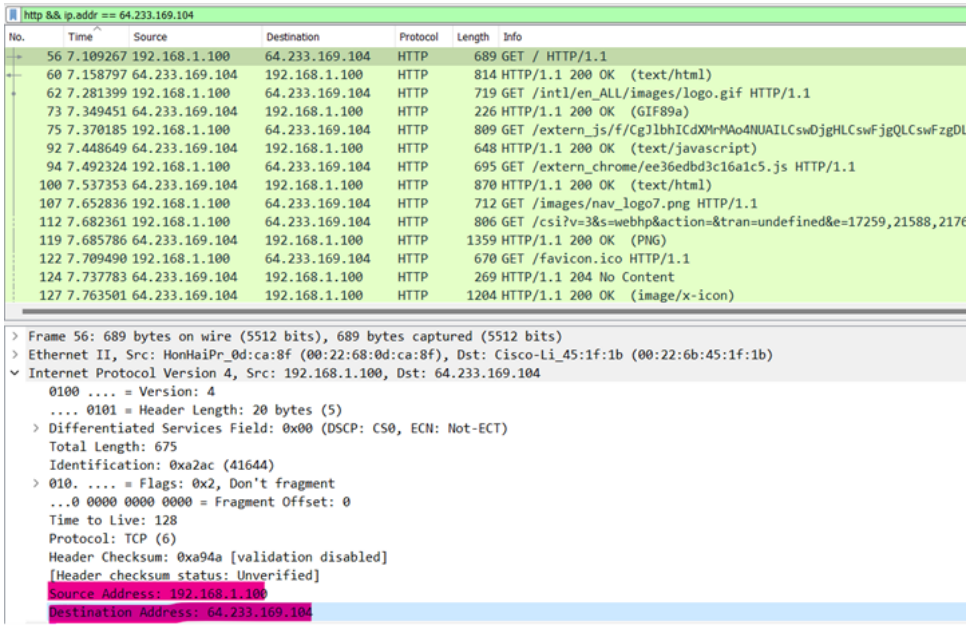

Figure. 22: WireShark Capture 4.a.2

Source Address: 192.168.1.100

Destination Address: 64.233.169.104

4. At what time is the corresponding 200 OK HTTP 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?

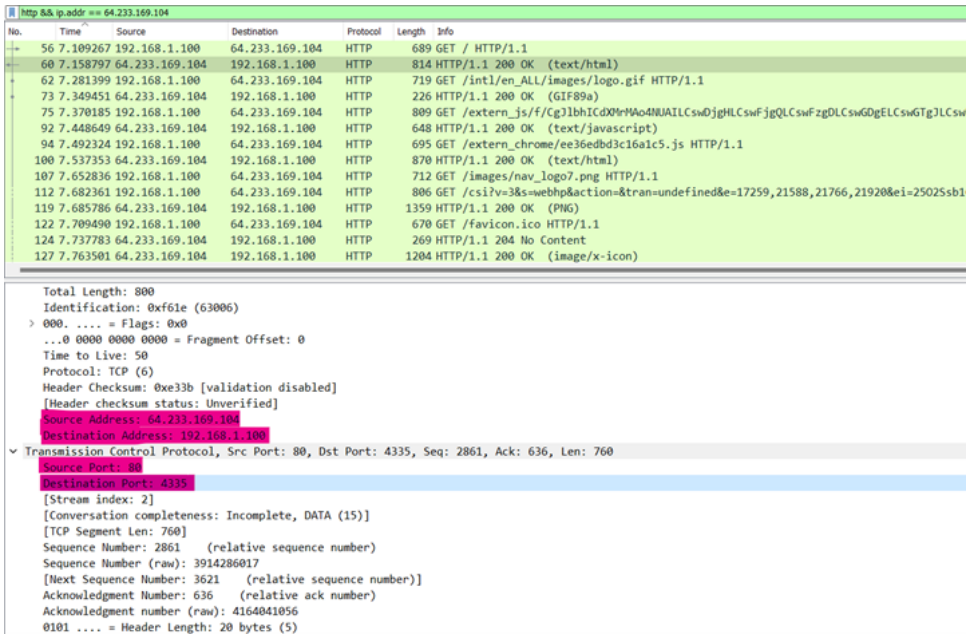

Figure. 23: WireShark Capture 4.a.4

Look at the *Figure. 23*

- At 7.158797 is the corresponding 200 OK HTTP message received from the Google server
- Source Address: 64.233.169.104
- Source Port: 80
- Destination Address: 192.168.1.100
- Destination Port: 4335

5. Recall that before a GET command can be sent to an HTTP server, TCP must first set up a connection using the three-way SYN/ACK handshake. At what time is the client-to-server TCP SYN segment sent that sets up the connection used by the GET sent at time 7.109267? What are the source and destination IP addresses and source and destination ports for the TCP SYN segment? What are the source and destination IP addresses and source and destination ports of the ACK sent in response to the SYN. At what time is this ACK received at the client?

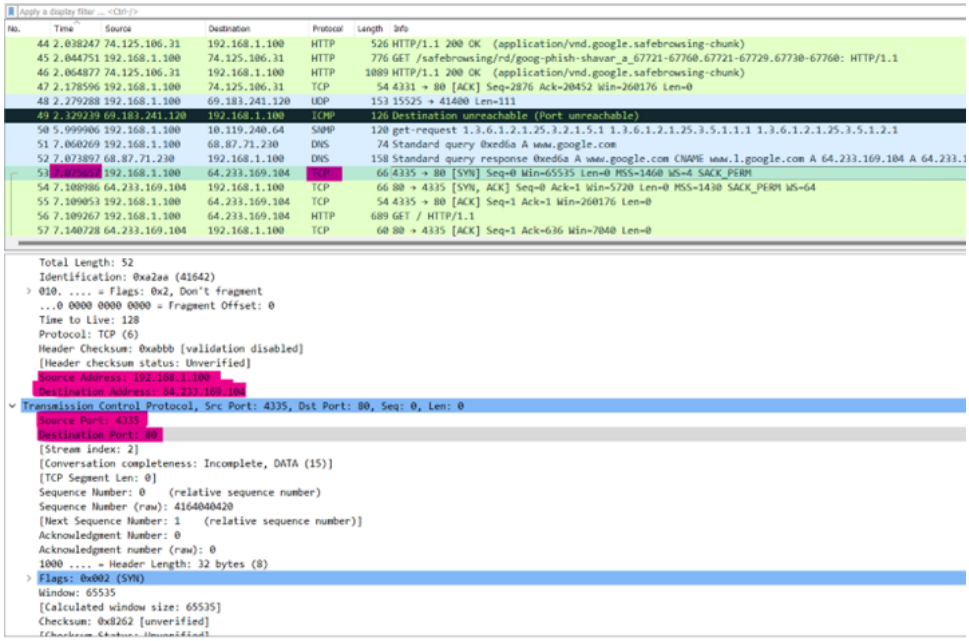

Figure. 24: WireShark Capture 4.a.5

TCP SYN segment. Look at *Figure. 24*

- At 7.075657, the client-to-server TCP SYN segment sent that sets up the connection used by the GET sent at time 7.109267
- Source Address: 192.168.1.100
- Source Port: 4335
- Destination Address: 64.233.169.104
- Destination Port: 80

TCP ACK segment.

- At 7.109053, ACK received at the client
- Source Address: 64.233.169.104
- Source Port: 80
- Destination Address: 192.168.1.100
- Destination Port: 4335

6. In the NAT_ISP_side trace file, find the HTTP GET message was sent from the client to the Google server at time 7.109267 (where t=7.109267 is time at which this was sent as recorded in the NAT_home_side trace file). At what time does this message appear in the NAT_ISP_side trace file? 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 NAT_ISP_side trace file)? Which of these fields are the same, and which are different, than in your answer to question 3 above?

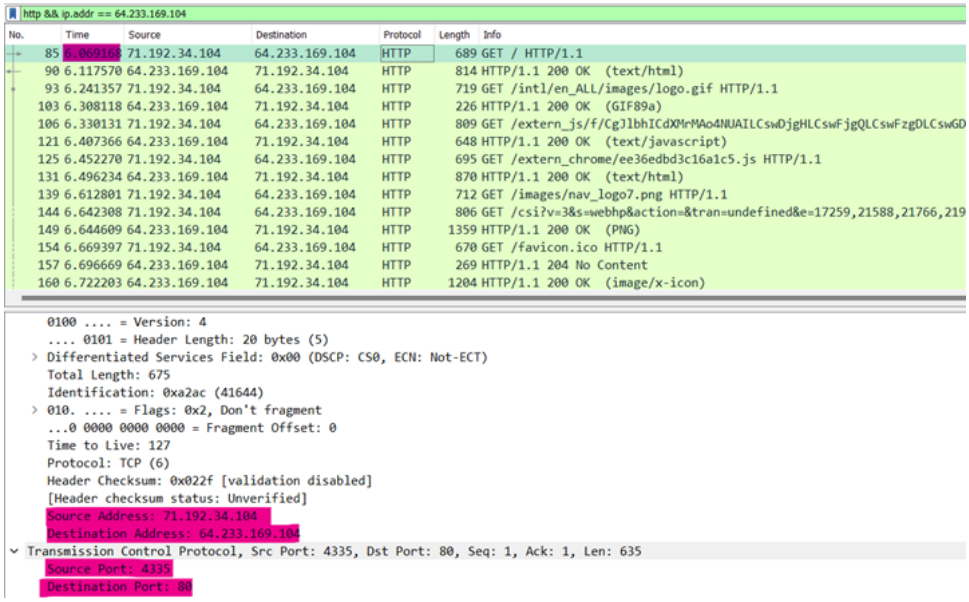

Figure. 25: WireShark Capture 4.a.6

Look at *Figure 25*

- At 6.09168, the GET message was sent from the client to the Google server at time 7.109267 appear in the NAT_ISP_side trace file.
- Source Address: 71.192.34.104
- Source Port: 4335
- Destination Address: 64.233.169.104
- Destination Port: 80

Only the source Address has changed

7. Are any fields in the HTTP GET message changed? Which of the following fields in the IP datagram carrying the HTTP GET are changed: Version, Header Length, Flags, Checksum. If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change.

The HTTP GET message: No changes (*Figure. 26, Figure. 27*)

Look at *Figure. 28 and Figure. 29* we have :

- Version: No changes
- Header Length: No changes
- Flags: No changes
- Checksum: change

Since the IP source address has changed, and the checksum includes the value of the source IP address, the checksum has changed.

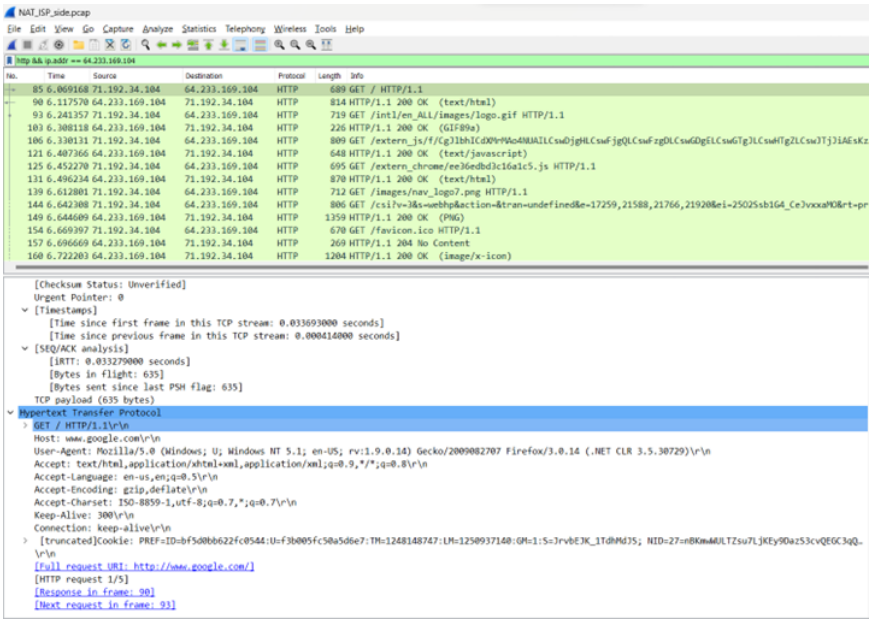

Figure. 26: HTTP GET Message NAT_ISP_side

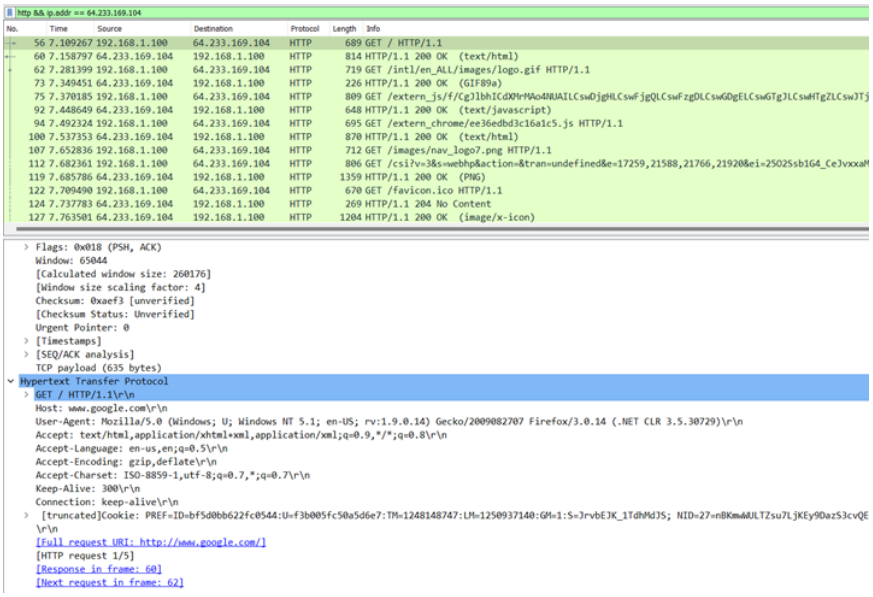

Figure. 27: HTTP GET Message NAT_Home_side

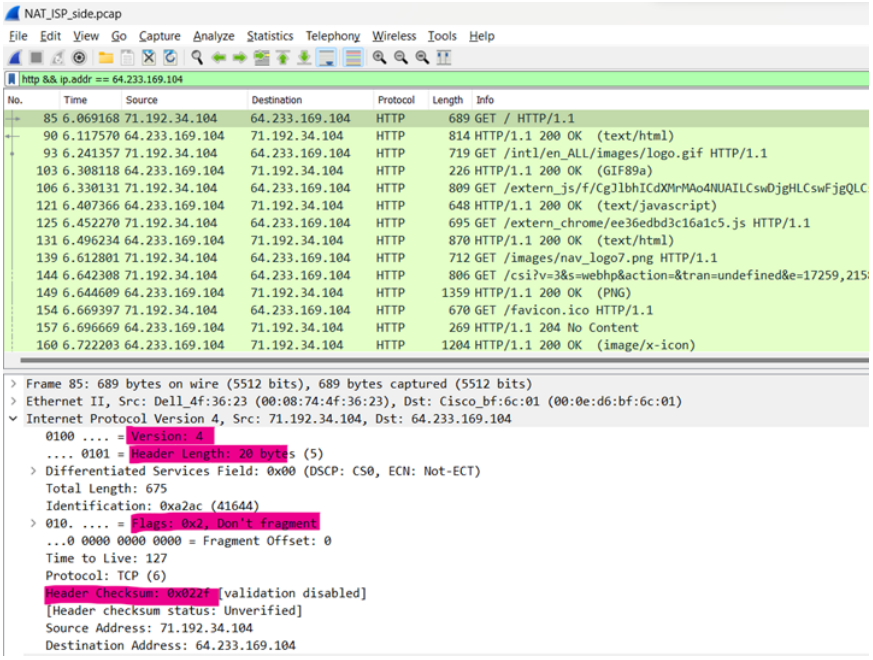

Figure. 28: HTTP GET Message NAT_ISP_side

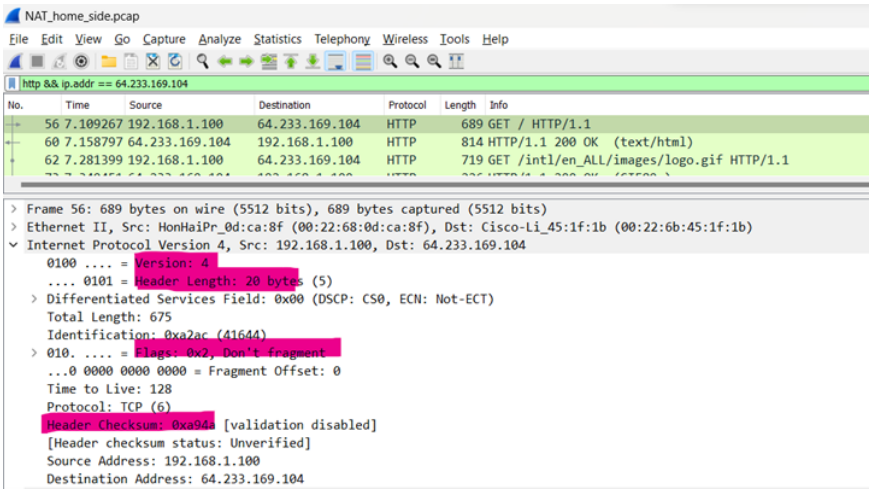

Figure. 29: HTTP GET Message NAT_Home_side

8. In the NAT_ISP_side trace file, at what time is the first 200 OK HTTP 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, and which are different than your answer to question 4 above?

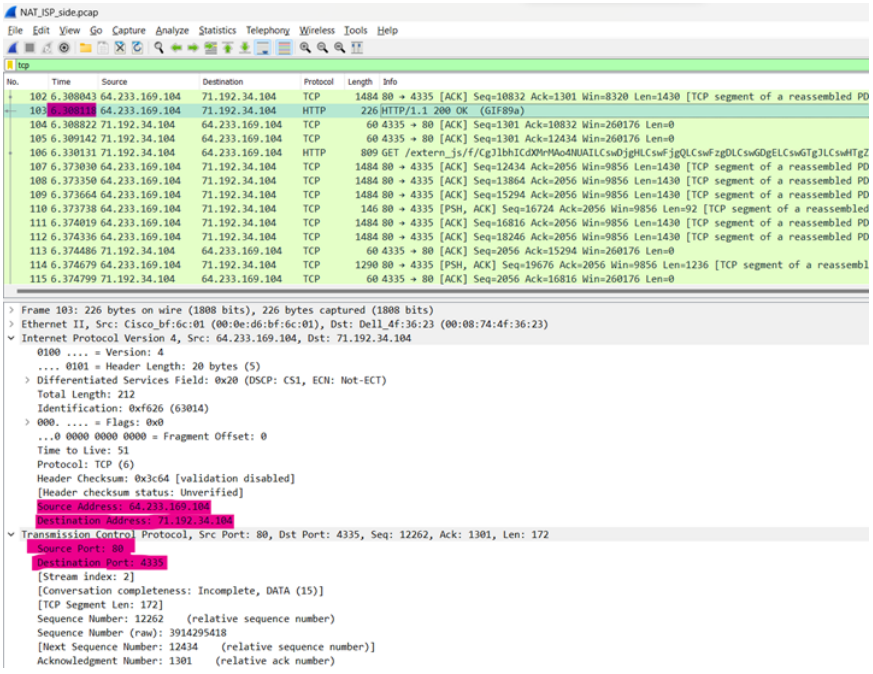

Figure. 30: The first 200 OK HTTP message received from the Google server

Look at *Figure 30*

- Source Address: 64.233.169.104
- Source Port: 80
- Destination Address: 71.192.34.104
- Destination Port: 4335

Only the Destination Address has changed

9. In the NAT_ISP_side trace file, at what time were the client-to-server TCP SYN segment and the server-to-client TCP ACK segment corresponding to the segments in question 5 above captured? What are the source and destination IP addresses and source and destination ports for these two segments? Which of these fields are the same, and which are different than your answer to question 5 above?

Look at *Figure 31* we have:

- Time : 6.03475
- Source Address: 71.192.34.104
- Source Port: 4335
- Destination Address : 64.233.169.104
- Destination Port: 80

Look at *Figure 32* we have:

- Time: 6.067775
- Source Address: 64.233.169.104
- Source Port: 80
- Destination Address : 71.192.34.104
- Destination Port: 4335

For the SYN, the source IP address has changed, For the ACK, the destination IP address has changed. The port numbers are unchanged

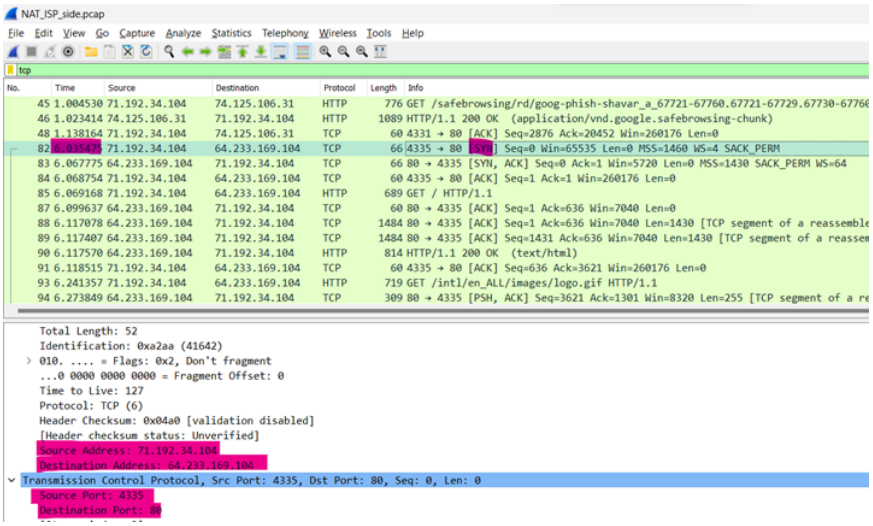

Figure. 31: The SYN

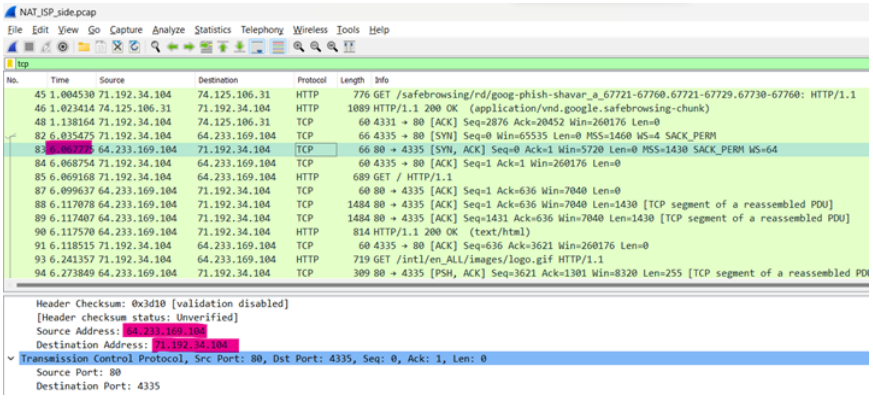

Figure. 32: The ACK

10. Using your answers to 1-8 above, fill in the NAT translation table entries for HTTP connection considered in questions 1-8 above.

Type	WAN side	LAN side
IP Address Port	71.192.34.104	192.168.1.100
Port	4335	14335

Bảng 1: NAT Translate table

4 Task 5

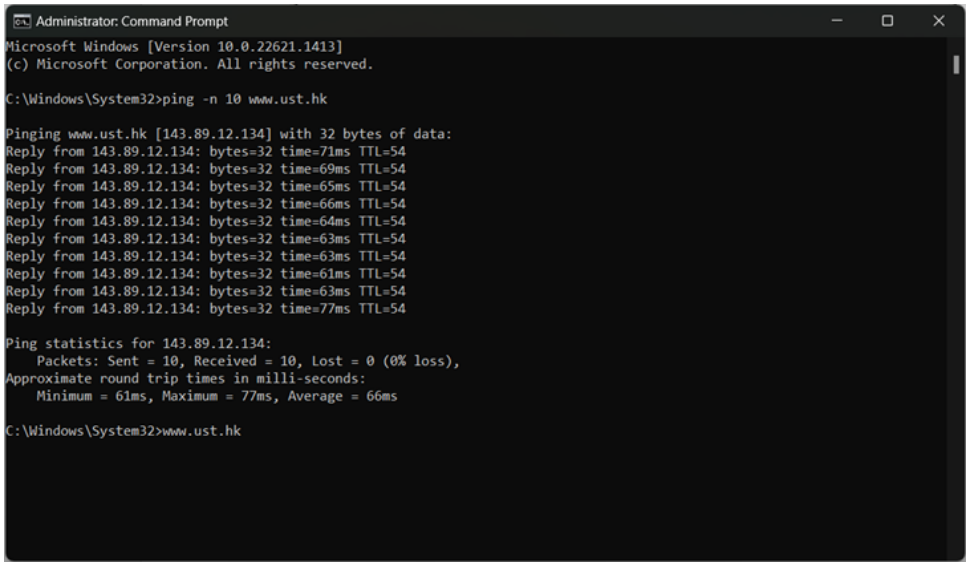

Figure. 33: Command Prompt window after entering Ping command

1. What is the IP address of your host? What is the IP address of the destination host?
   The IP address of my host is 172.17.37.93
   The IP address of the destination host is 143.89.12.134

2. Why is it that an ICMP packet does not have source and destination port numbers?

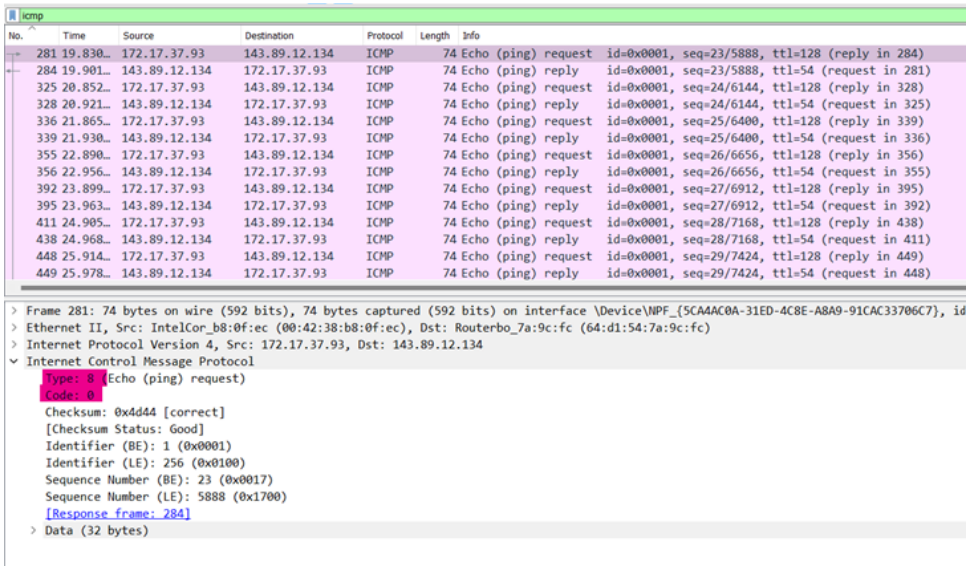

Figure. 34: ICMP packet

The ICMP packet does not have source and destination port numbers because it was designed to communicate network-layer information between application-layer processes. Each ICMP packet has a "Type" and a "Code". The Type/Code combination identifies the specific message being received. Since the network software itself interprets all ICMP messages, no port numbers are needed to direct the ICMP message to an application layer process.

3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and, identifier fields?

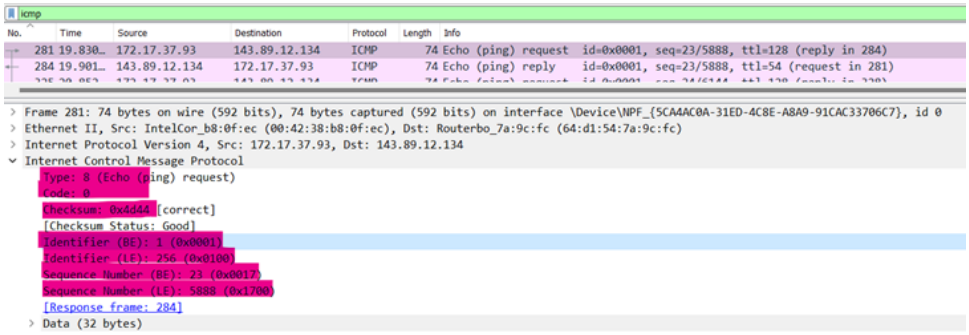

Figure. 35: Command Prompt window after entering Ping command

The ICMP type is 8, and the code number is 0.

4. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and, identifier fields?

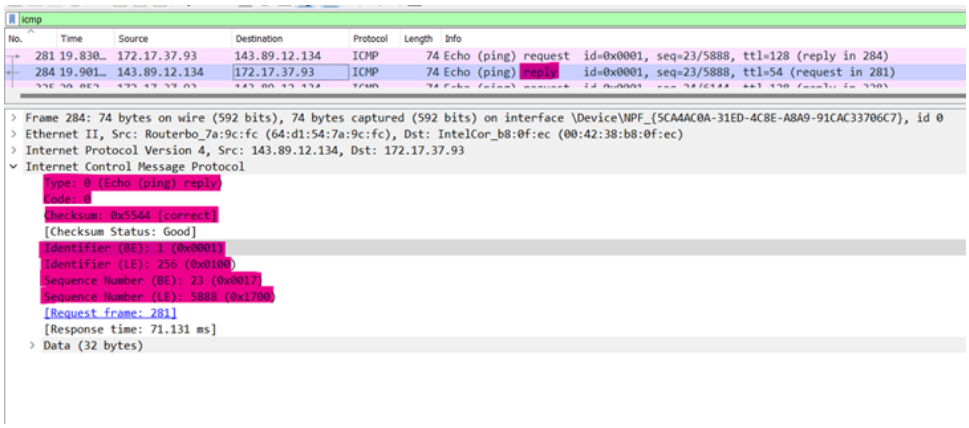

Figure. 36: the corresponding ping reply packet

The ICMP type is 0, and the code number is 0.
The ICMP packet also has a checksum, identifier, sequence number, and data field. The checksum, sequence number ,and identifier fields are two bytes each.

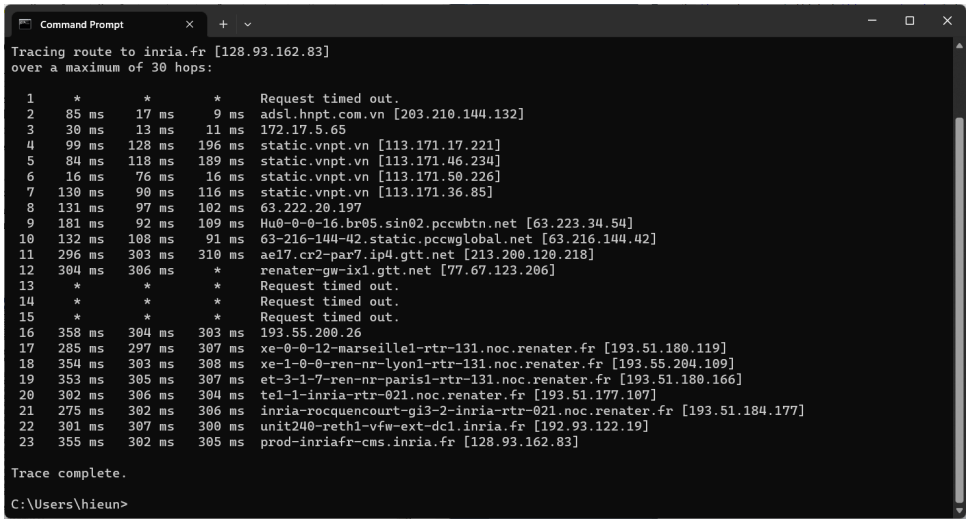

Figure. 37: Command Prompt window displays the results of the Traceroute program

5. What is the IP address of your host? What is the IP address of the target destination host?

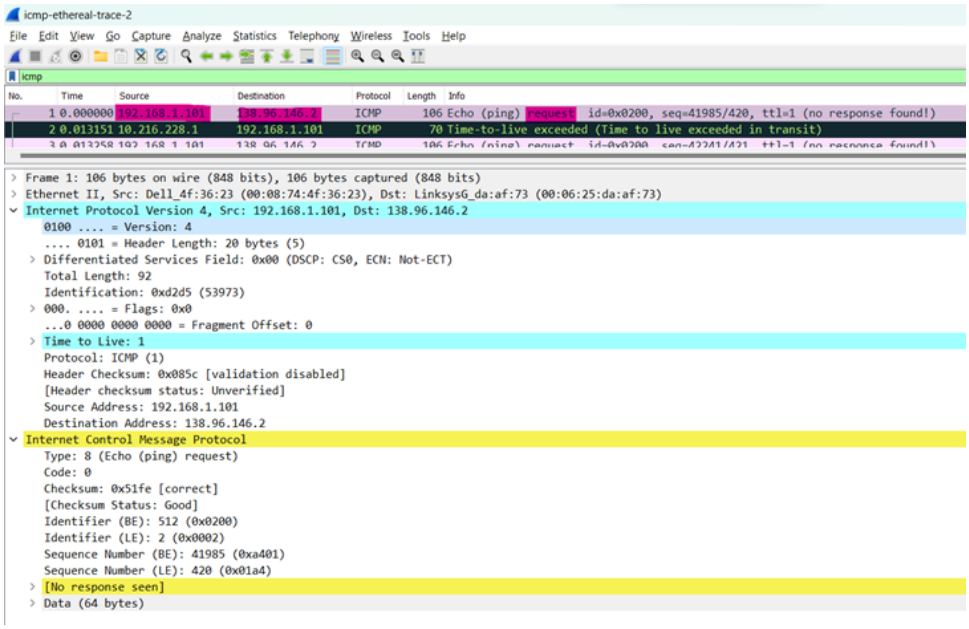

Figure. 38: Capture for Question 5.5

The IP address of my host is 192.168.1.101. The IP address of the destination host is 138.96.146.2

6. If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be?

No. If ICMP sent UDP packets instead, the IP protocol number should be 0x11

7. Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?
The ICMP echo packet has the same fields as the ping query packets.

8. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?

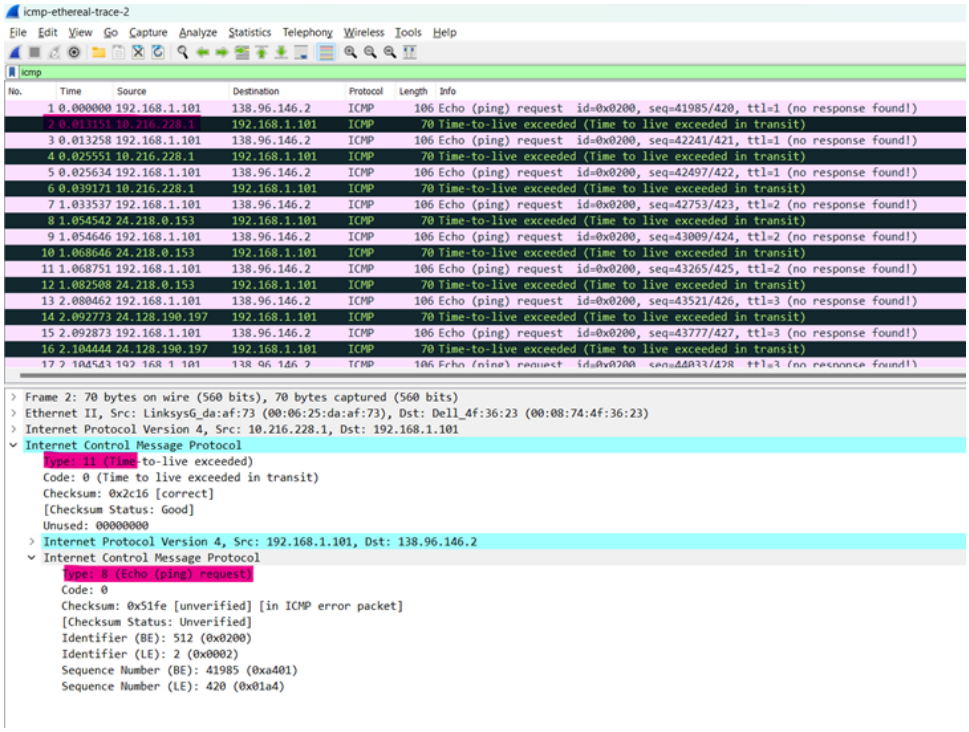

Figure. 39: ICMP error packet

The ICMP error packet is not the same as the ping query packets. It contains both the IP header and the first 8 bytes of the original ICMP packet that the error is for

9. Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?

The last three ICMP packets are message type 0 (echo reply) rather than 11 (TTL expired). They are different because the datagrams have made it all the way to the destination host before the TTL expired.

10. Within the tracert measurements, is there a link whose delay is significantly longer than others? Refer to the screenshot in Figure 4, is there a link whose delay is significantly longer than others? On the basis of the router names, can you guess the location of the two routers on the end of this link?

In *Figure. 41* from the lab, the link is from New York to Pastourelle, France.

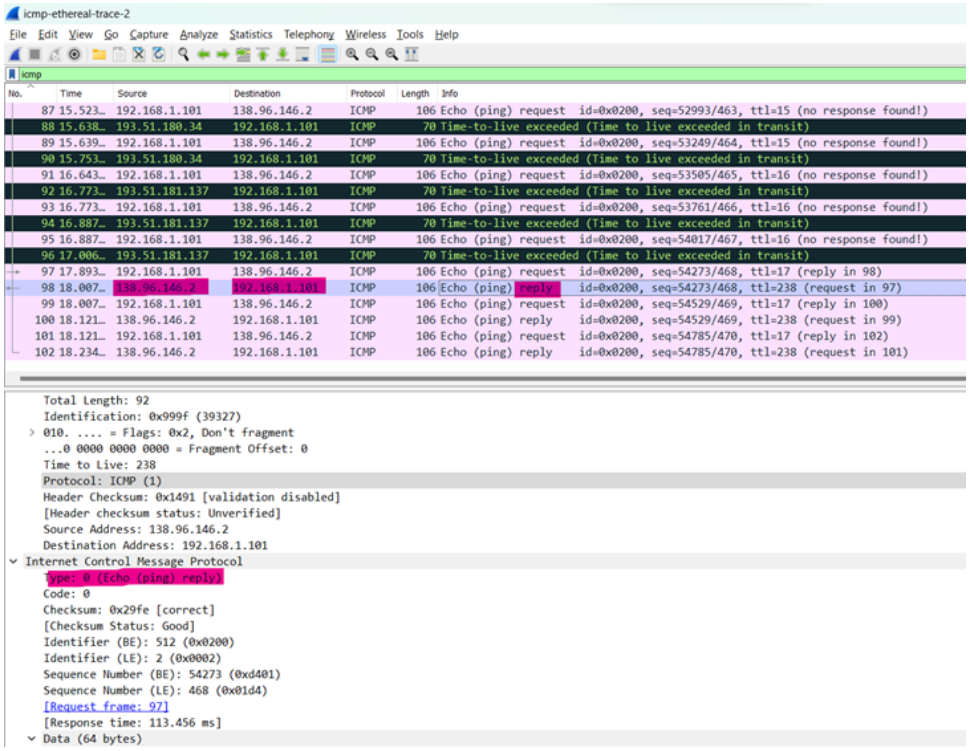

Figure. 40: The last three ICMP packets received

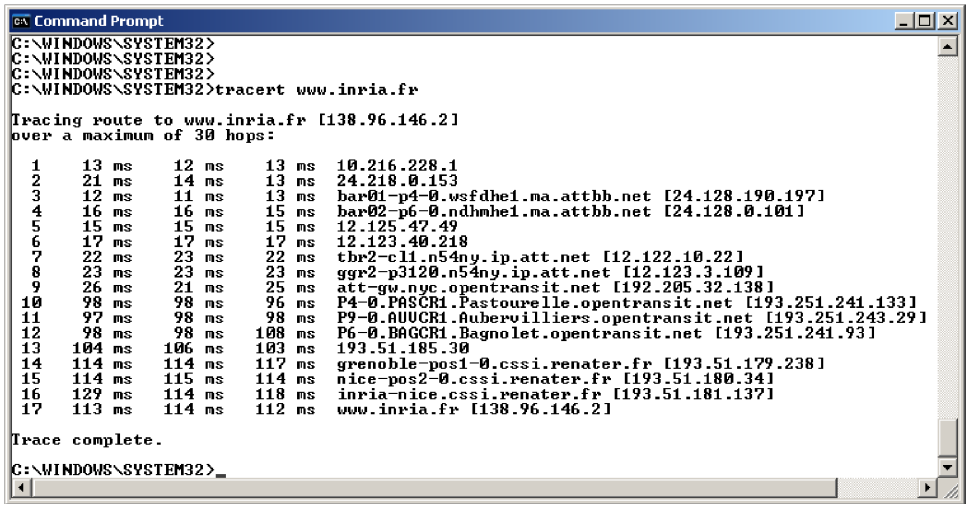

Figure. 41: The last three ICMP packets received

5 Task 6

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

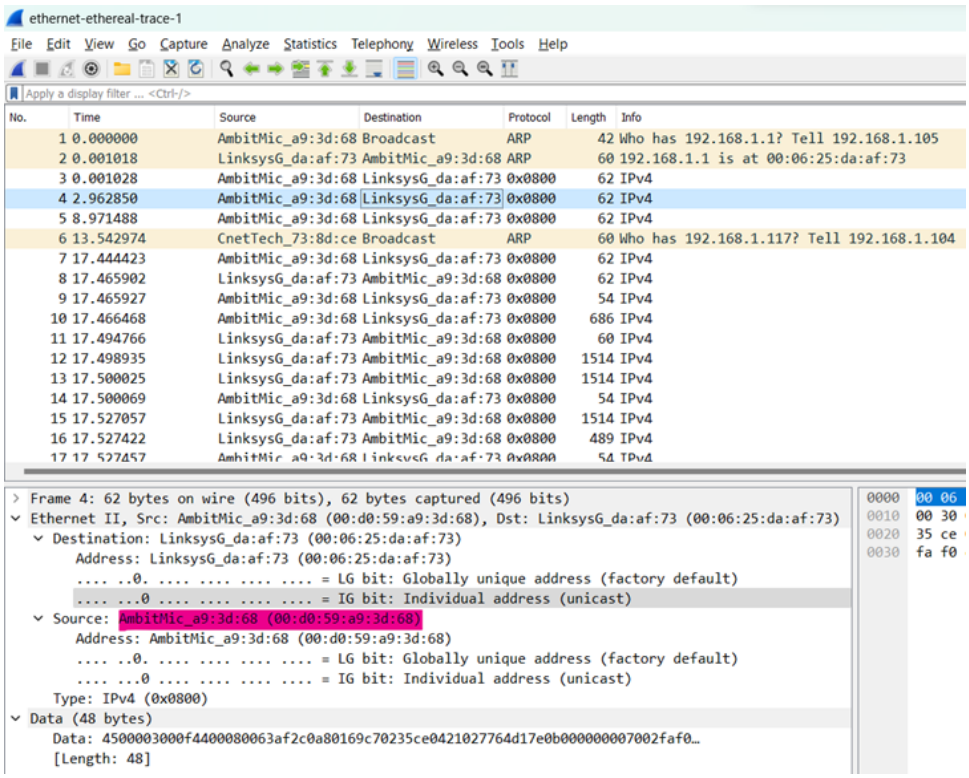

Figure. 42: Capture for Question 6.1

The Ethernet address of my computer is 00:d0:59:a9:3d:68

2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address? [Note: this is an important question and one that students sometimes get wrong. Re-read pages 468-469 in the text and make sure you understand the answer here.]
The destination address 00:06:25:da:af:73 is not the Ethernet address of gaia.cs.umass.edu. It is the address of my Linksys router, which is the link used to get off the subnet.

3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?
The hex value for the Frame type field is 0x0800. this correspond to the IP protocol (the frame type filed indicates that the nest layer above IP – the layer to which the payload of this Ethernet frame will be passed is IP

4. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame?

   Look at *Figure. 43*, it's 54. This is because the data field has to be stuffed to satisfy the 46 bytes minimum. This is later dealt with by comparing this with the length field in the IP datagram header

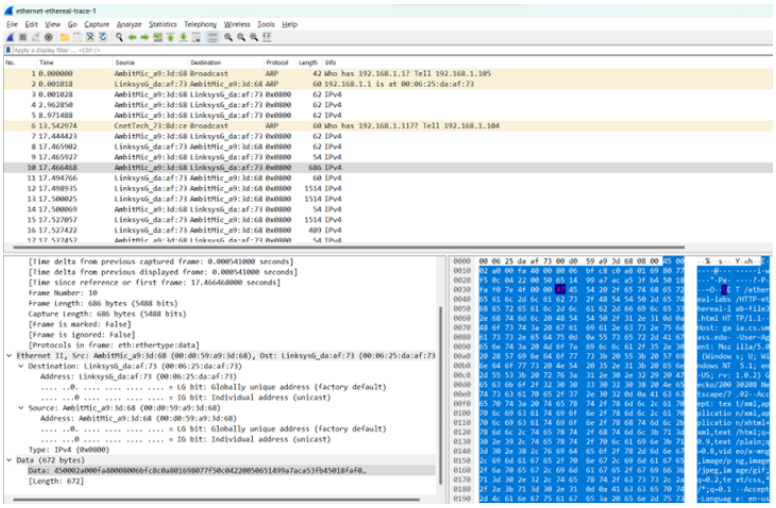

Figure. 43: The GET message

5. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?
   The source address 00:06:25:da:af:73 is neither the Ethernet address of gaia.cs.umass.edu nor the address of my computer. It is the address of my Linksys router, which is the link used to get onto my subnet.

6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?
   The destination address is 00:d0:59:a9:3d:68 and is indeed the Ethernet address of my computer.

7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?
   The hex value for the Frame type field is 0x0800. This value corresponds to the IP protocol (see also answer to 3. above).

8. How many bytes from the very start of the Ethernet frame does the ASCII "O" in "OK" (i.e., the HTTP response code) appear in the Ethernet frame?

   Look at *Figure. 44*, It's 68 bytes.

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

   The left-most column is the Internet Address in A.B.C.D format, the middle column is the Physical Address in varying format and the right-most column is the IP address type, either static or dynamic.

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

    Source address for Request message: 00:d0:59:a9:3d:68

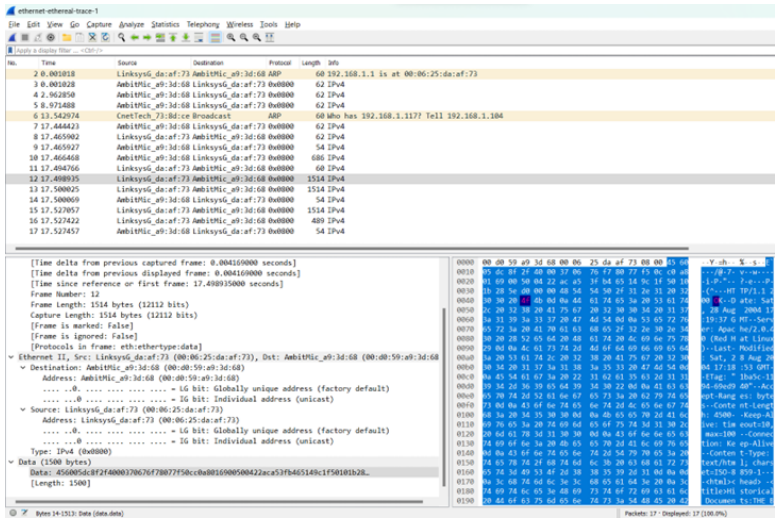

Figure. 44: The OK Message

11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?
0x0806, which it states is ARP.

12. Download the ARP specification from ftp://ftp.rfc-editor.org/in-notes/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? Look at *Figure.* **??**, It's 20 bytes

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?
It's 1
c) Does the ARP message contain the IP address of the sender? Look at *Figure.* **??**. Yes, It's 192.168.1.104

d) Where in the ARP request does the "question" appear – the Ethernet address of the machine whose corresponding IP address is being queried?
In the Target MAC address field (destination) in the form of 00:00:00:00:00:00. Once the MAC address is resolved, this would be populated with the corresponding complete MAC address of the server or its relevant router.

13. Now find the ARP reply that was sent in response to the ARP request.
a) How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin?

Look at *Figure. 49.*It's 20 bytes

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?
It's 2
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?

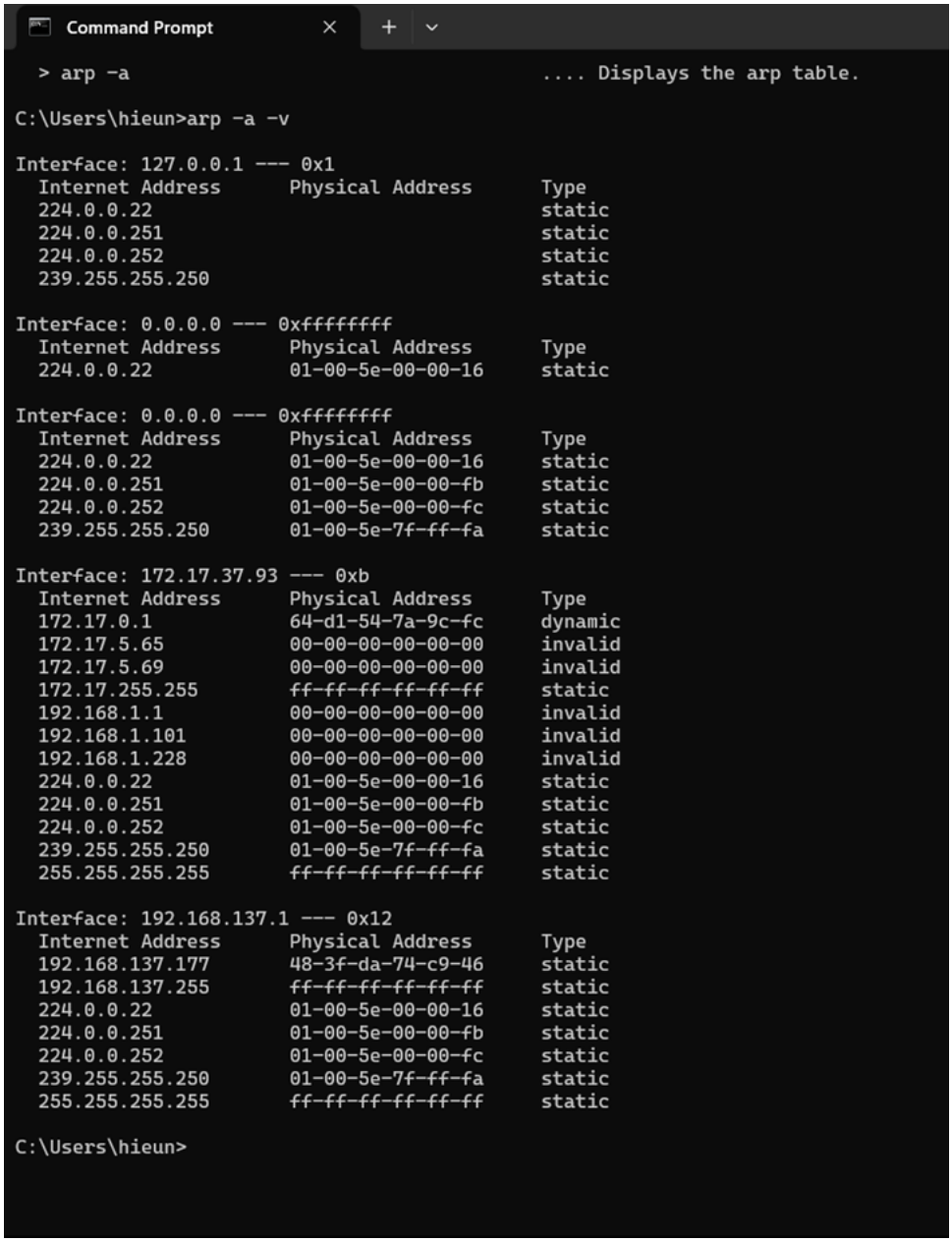

Figure. 45: The *arp* command

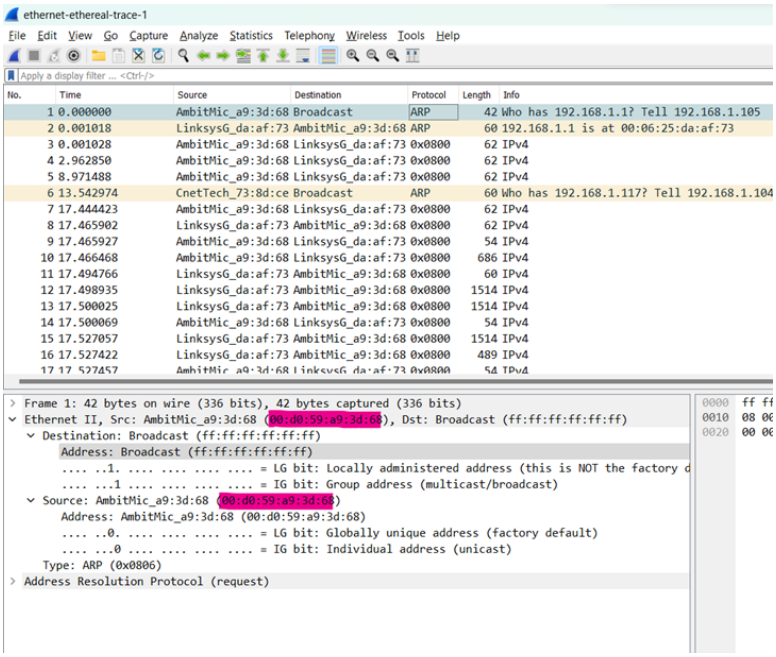

Figure. 46: The Ethernet frame containing the ARP request message

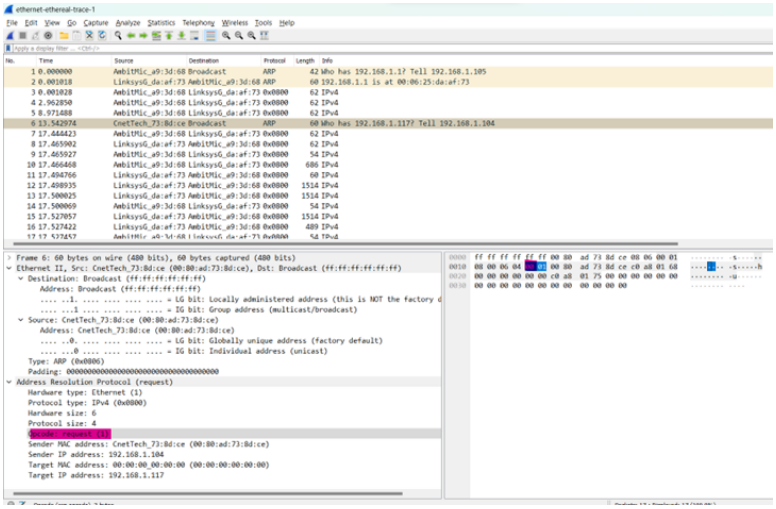

Figure. 47: The ARP request

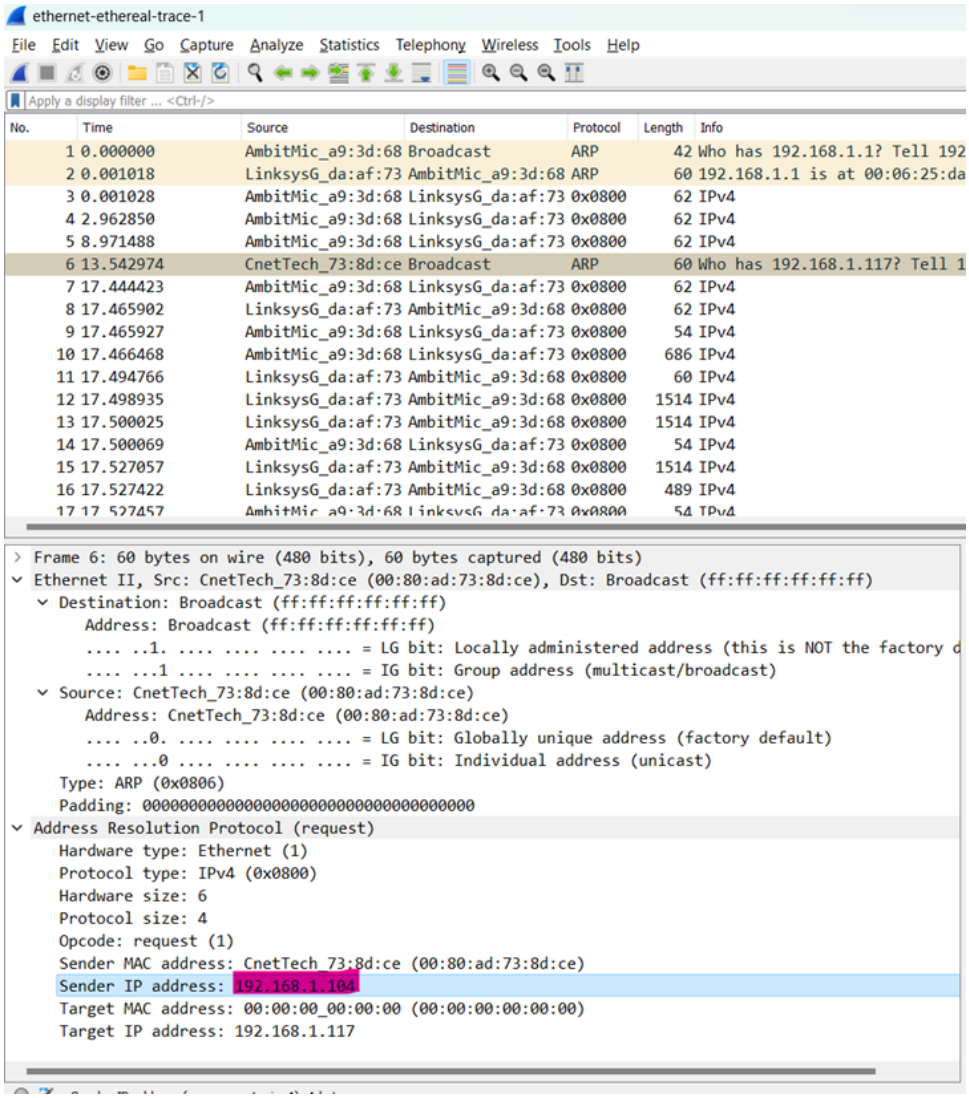

Figure. 48: The ARP request

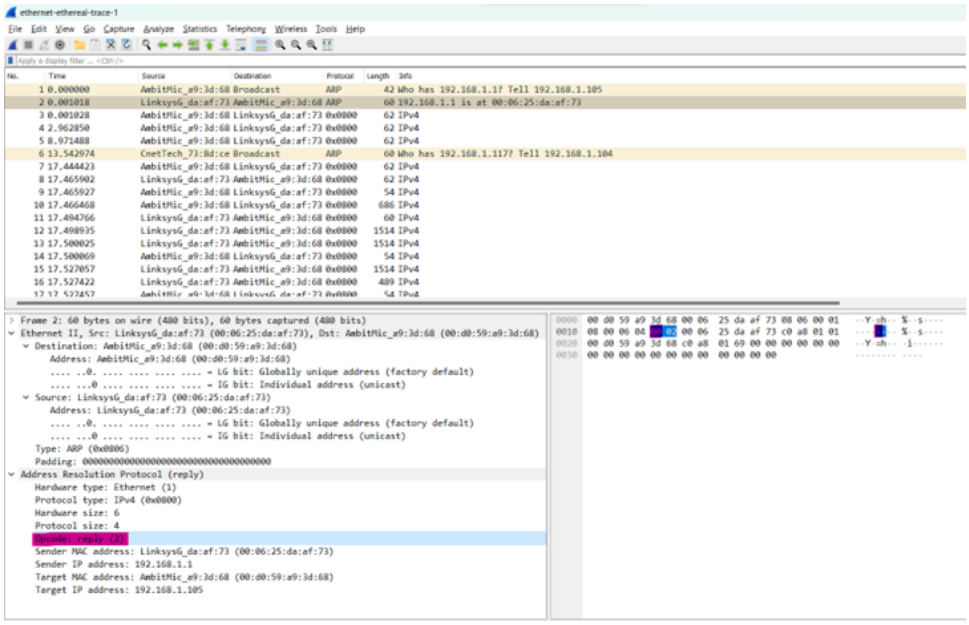

Figure. 49: The ARP reply

The previously "blank" Target MAC Address field, which now would be the Sender's MAC Address since this is a reply to the broadcast request, which is the server's (actually the router's) MAC address, and is 00:06:25:da:af:73

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

Source Address for the Reply Message: 00:06:25:da:af:73
Destination Address for the Reply Message: 00:d0:59:a9:3d:68

15. Open the ethernet-ethereal-trace-1 trace file in http://gaia.cs.umass.edu/wireshark-labs/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 indicated 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?

It is an IP address within the same subnet that the router has already mapped in its ARP table and does not need to be rediscovered and chronicled.

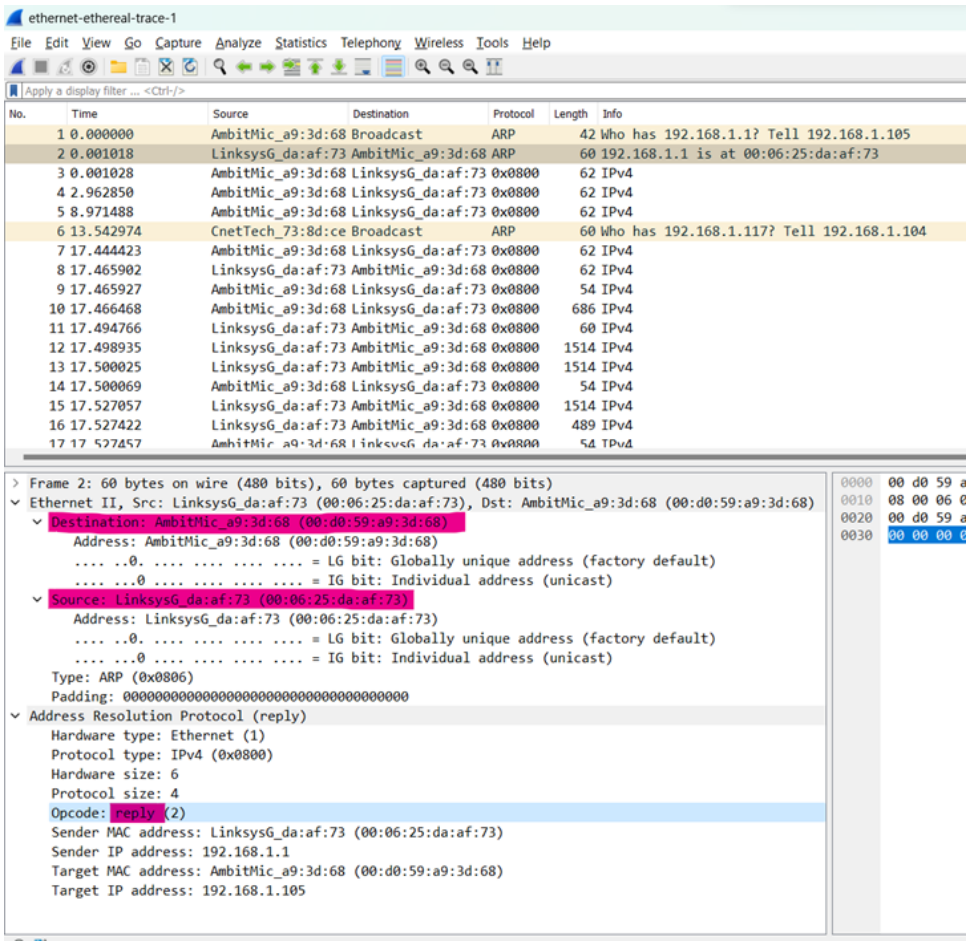

Figure. 50: The ARP reply

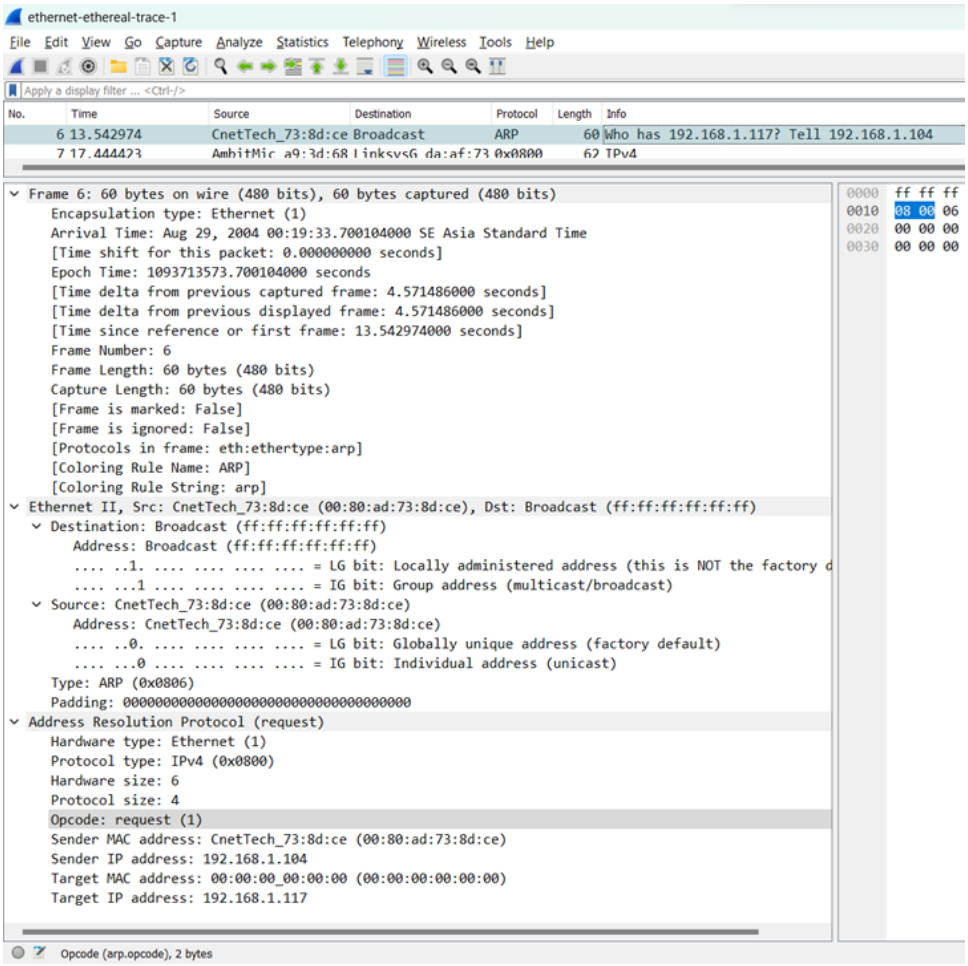

Figure. 51: The ARP reply