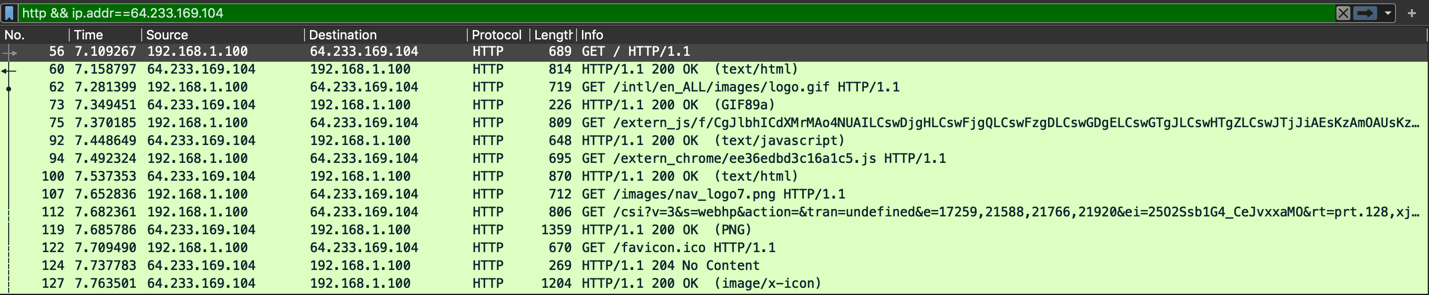
**Name: Nguyen Phi Thong**

**ID: 1814205**

**LAB 4C. NAT**

1. **What is the IP address of the client?**

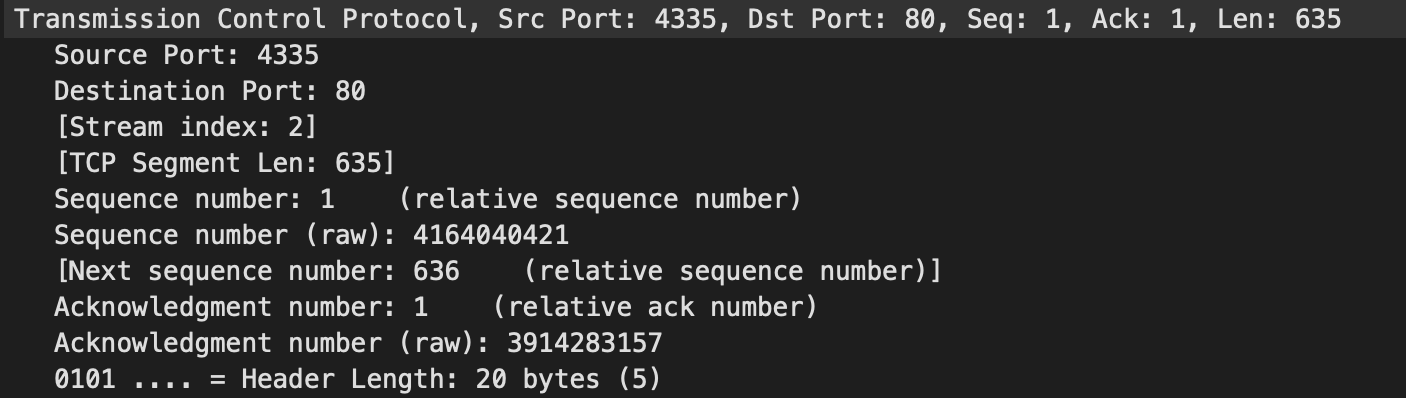
192.168.1.1002.

1. **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**
2. **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?**

Destination IP: 64.233.169.104

Source IP: 192.168.1.100

Source port: 4335

Destination port: 80

1. **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?**

Time: 7.158797

Source IP: 64.233.169.104

Destination IP: 192.168.1.100

Source port: 80

Destination port: 4335

1. **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?**

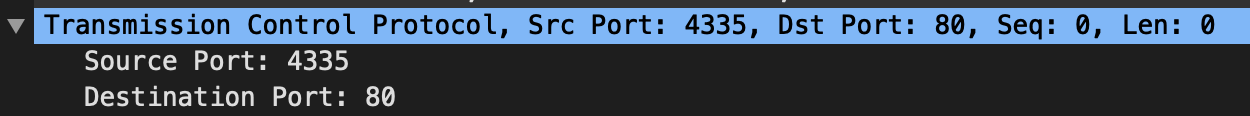
Time: 7.075657

Destination IP: 64.233.169.104

Source IP: 192.168.1.100

Source port: 4335

Destination port: 80



**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? (Note: to find these segments you will need to clear the Filter expression you entered above in step 2. If you enter the filter “tcp”, only TCP segments will be displayed by Wireshark)**

Time: 7.108986

Source IP: 64.233.169.104

Destination IP: 192.168.1.100

Source port: 80

Destination port: 4335



1. **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?**

Time: 6.069168

Source IP: 71.192.34.104

Destination IP: 64.233.169.104

Source port: 4335

Destination port: 80

Only source IP is different (change).

1. **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.**

HTTP GET message not changed.

In IP datagram carrying the HTTP GET: version, header length, flag not changed. Checksum changed because source IP changed.

1. **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?**

Time: 6.117570

Source IP: 64.233.169.104

Destination IP: 71.192.34.104

Source port: 80

Destination port: 4335

Only destination IP is different (change).

1. **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?**

* The client-to-server TCP SYN segment:

Time: 6.035475

Source IP: 71.192.34.104

Destination IP: 64.233.169.104

Source port: 4335

Destination port: 80

Only source IP is different (change).

* The server-to-client TCP ACK segment:

Time: 6.067775

Destination IP: 71.192.34.104

Source IP: 64.233.169.104

Source port: 4335

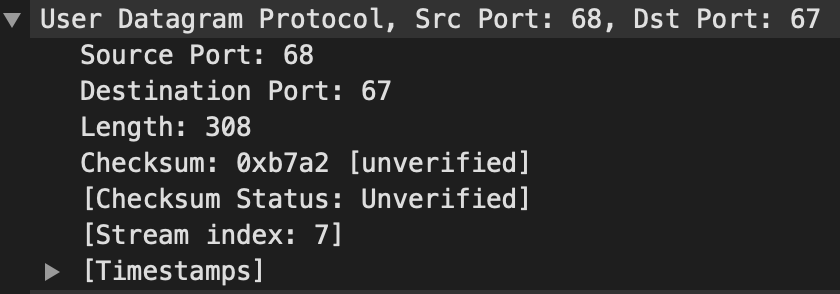
Destination port: 80

Only destination IP is different (change).

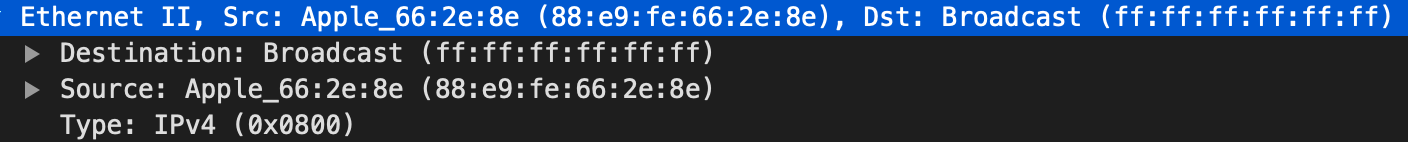
**LAB 4B. DHCP**

*Ghi chú: Em xài MacOS nên không chạy được 2 lệnh ipconfig release/renew. Nên mấy câu hỏi liên quan đến packet Offer và Discover em không trả lời được ạ.*

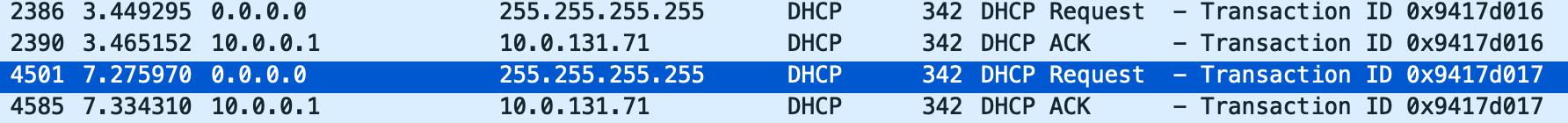
1. **Are DHCP messages sent over UDP or TCP?**

UDP

1. **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?**
2. **What is the link-layer (e.g., Ethernet) address of your host?**

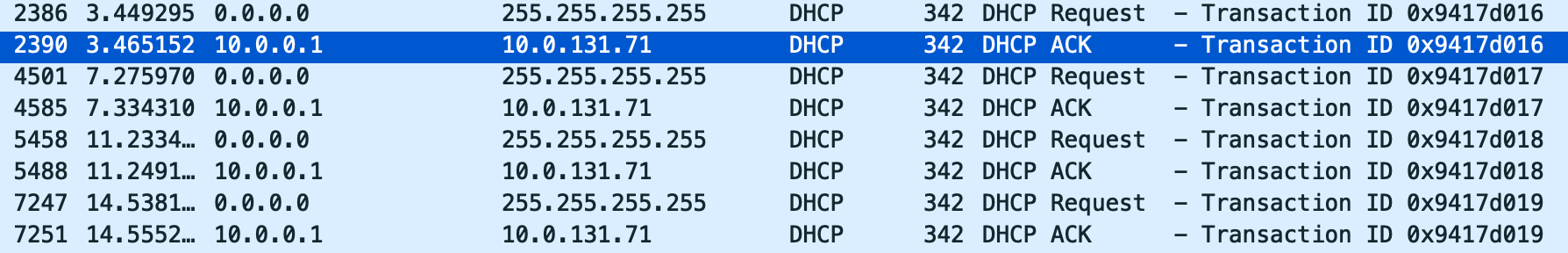
The link-layer address of my host: (88:e9:fe:66:2e:8e)

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

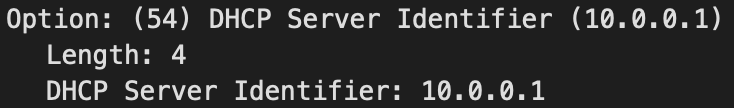
* The first
  + Request: Transaction ID 0x9417d016
  + ACK: Transaction ID 0x9417d016
* The second
  + Request: Transaction ID 0x9417d017
  + ACK: Transaction ID 0x9417d017

Purpose of the Transaction-ID field help the host differentiate between requests made by user.

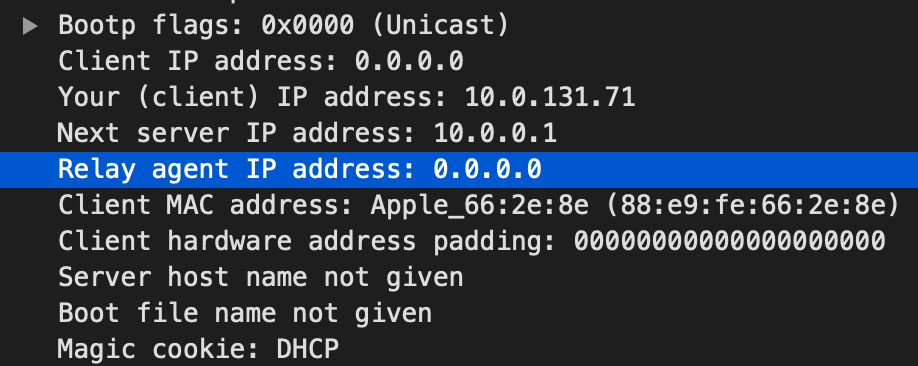
1. **A host uses DHCP to obtain an IP address, among other things. But a host’s IP address is not confirmed until the end of the four-message exchange! If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? 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.**

* Request: src 0.0.0.0 / des 255.255.255.255
* ACK: src 10.0.0.1/ des 10.0.131.71

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

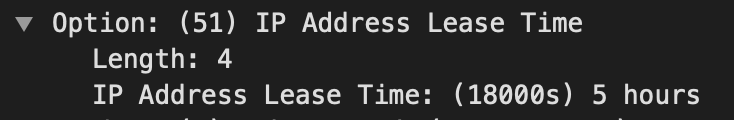
IP: 10.0.0.1

1. **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**
2. **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?**

In your experiment, relay agent IP address: 0.0.0.0

1. **Explain the purpose of the router and subnet mask lines in the DHCP offer message.**
2. **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?**
3. **Explain the purpose of the lease time. How long is the lease time in your experiment?**

**The lease time in my experiment is 5 hours. The purpose of this is the amount of time the DHCP server assigns an IP address to a client.**



1. **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?**

* Purpose of the DHCP release message is to release the IP address back to the server.
* There is no verification that release message is received by server.
* If the release message is lost, the client releases the IP address, but the server will not reassign that address until the clients lease on the address expires.

1. **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.**

Having ARP packets sent/received during the DHCP packet-exchange period.

Purpose: find the hardware address (MAC address) of a device from an IP address.