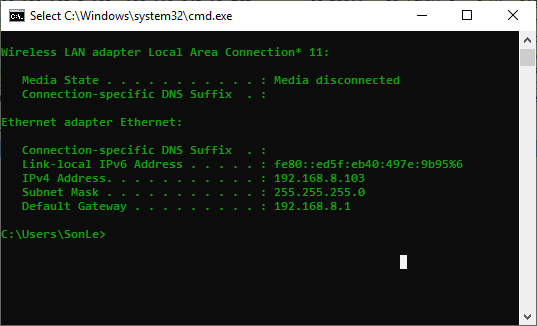
Họ và tên: Lê Trung Sơn

MSSV: 1810482

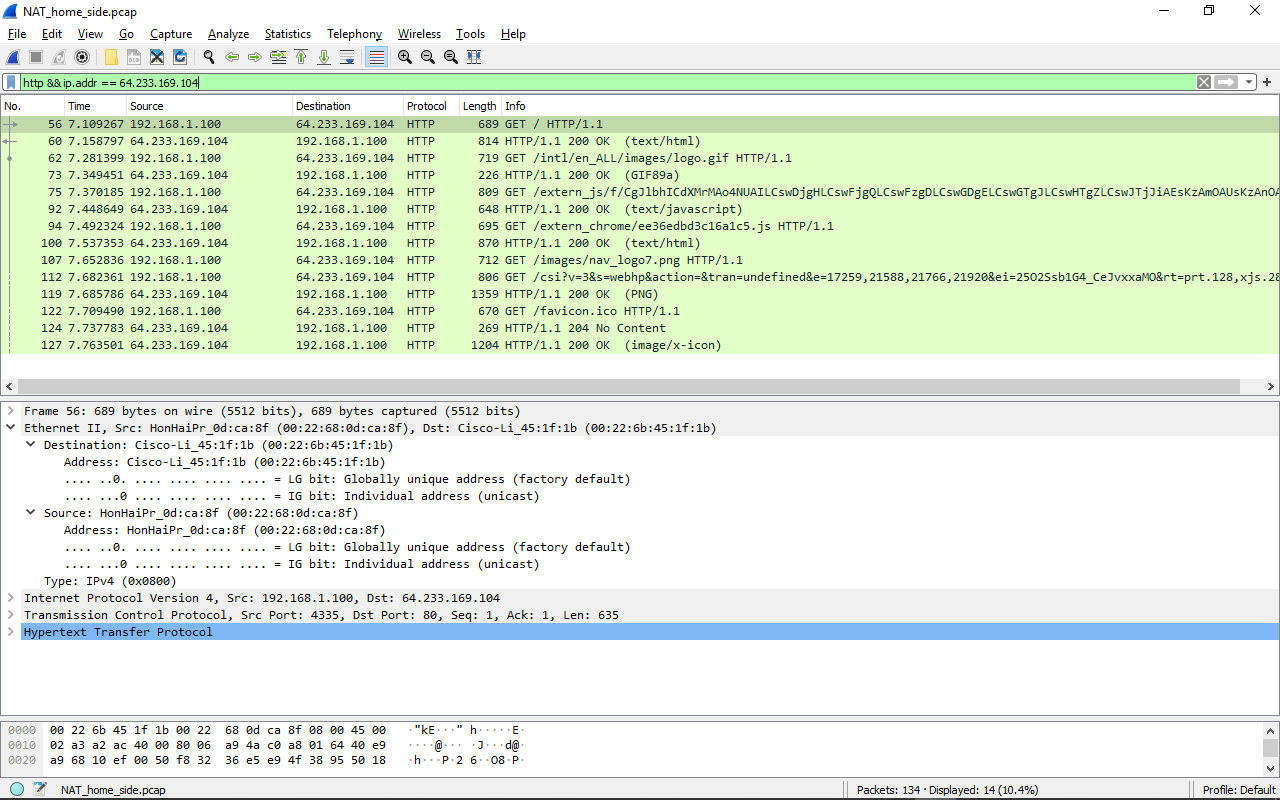
LAB 4C



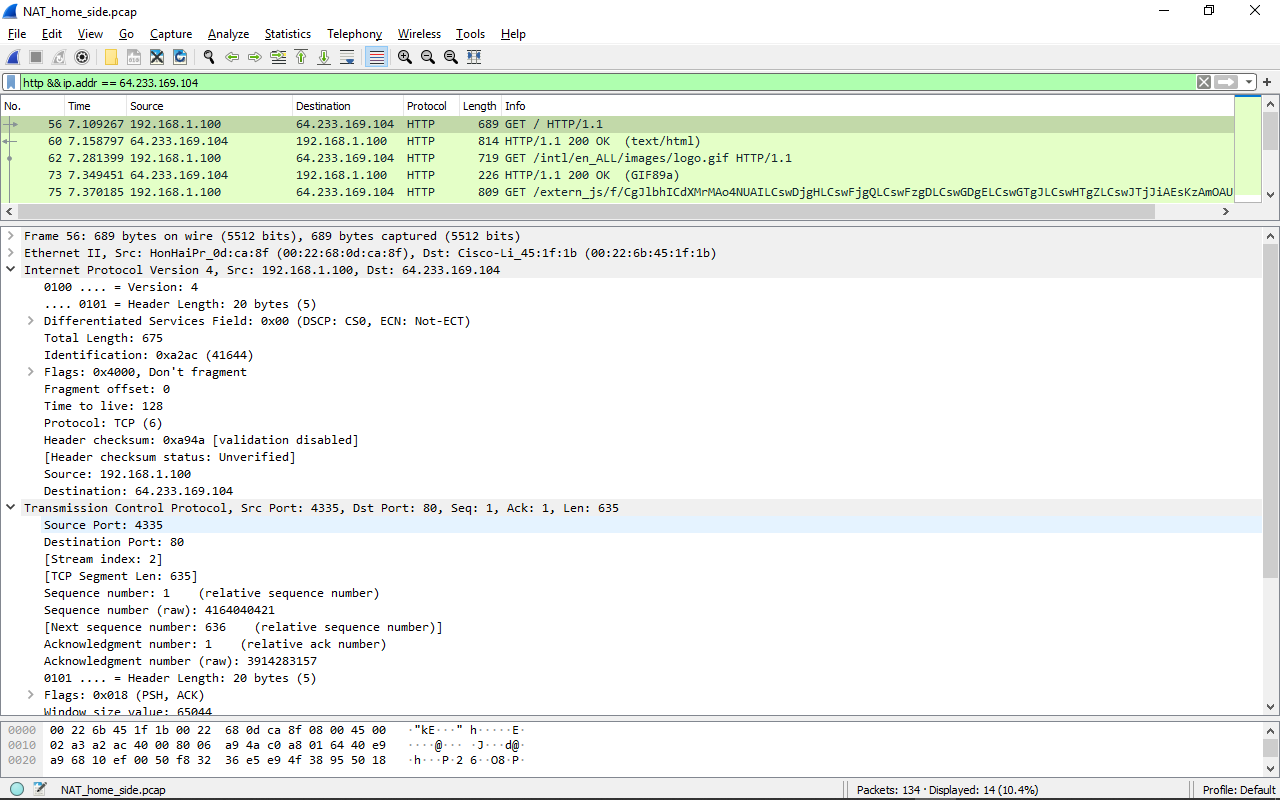
1. What is the IP address of the client?

- IP là 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?



- Source IP Address: 192.168.1.100, Port: 4335

- Destination IP Address: 64.233.169.104, Port: 80

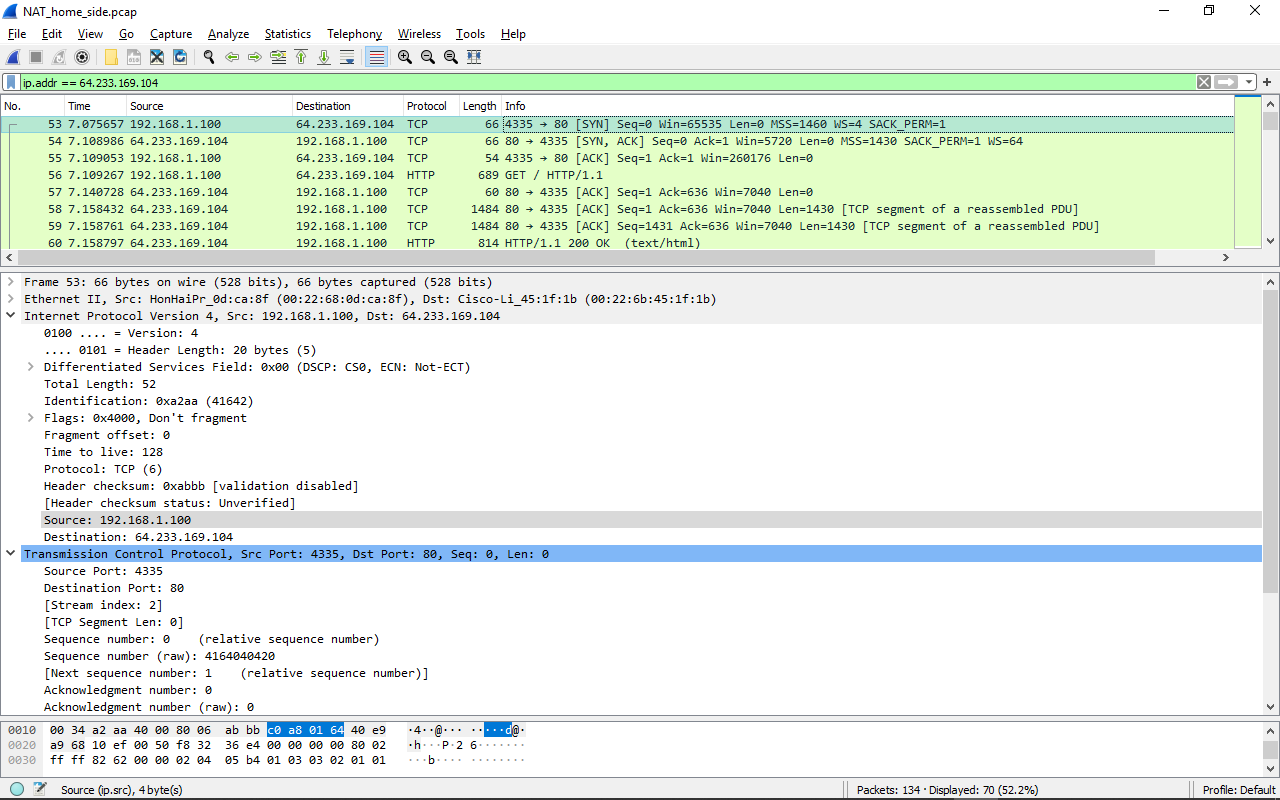
4. At what time is the corresponding 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

- Thời gian khi nhận 200 OK là 7.158797

- Source IP Address: 64.233.169.104, Port: 80

- Destination IP Address: 192.168.1.100, Port: 4335

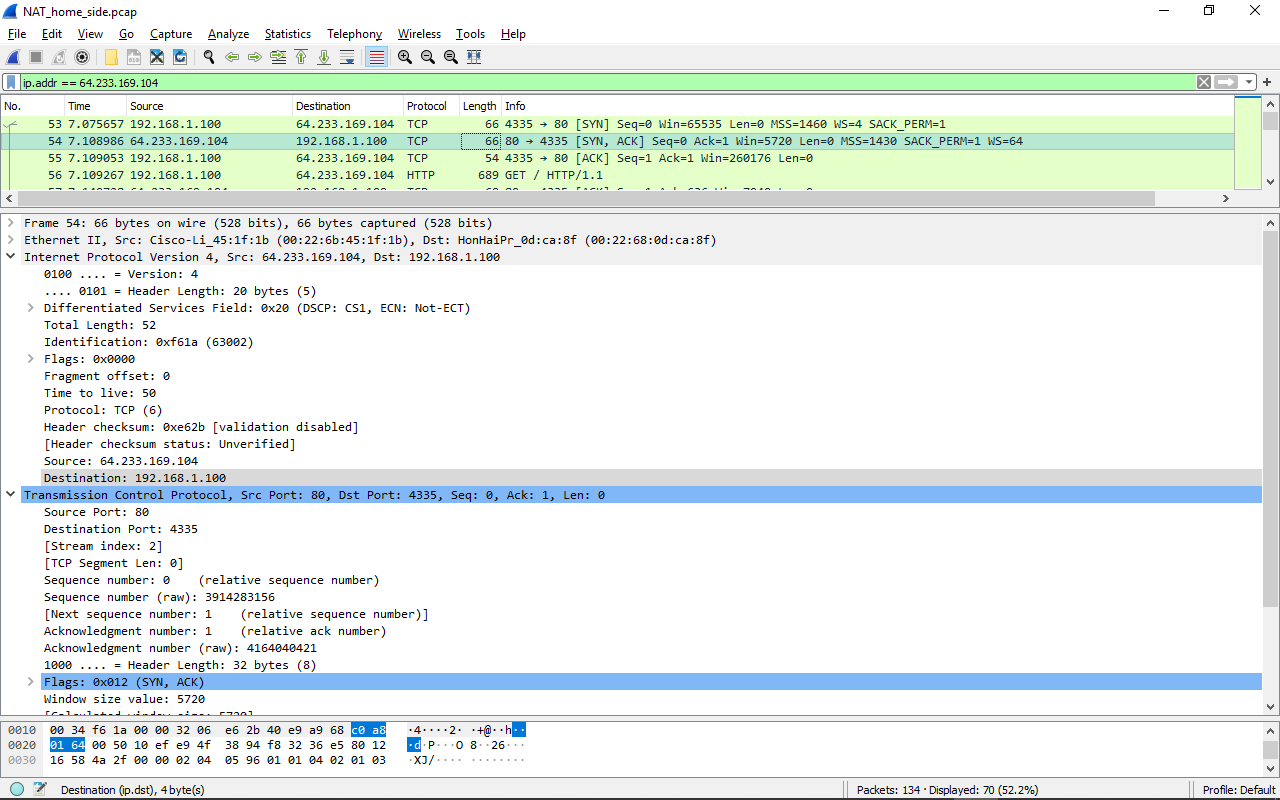
5. Recall that before a GET command can be sent to an HTTP server, TCP must first set up a connection using the three-way SYN/ACK handshake. At what time is the client-to-server TCP SYN segment sent that sets up the connection used by the GET sent at time 7.109267? What are the source and destination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



- Thời gian khi gửi TCP SYN segment là 7.075657

- Source IP Address: 192.168.1.100, Port: 4335

- Destination IP Address: 64.233.169.104, Port: 80

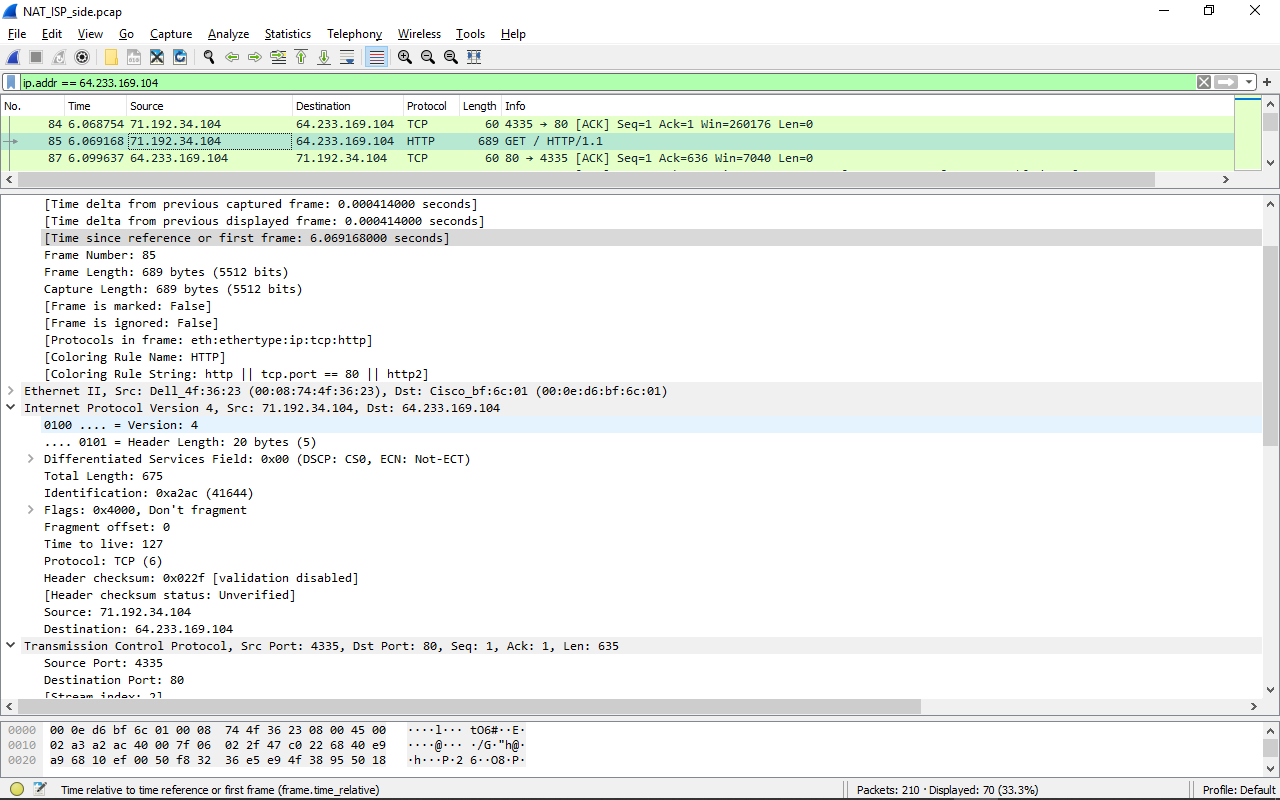


- Thời gian ACK trả về là 7.108986

- Source IP Address: 64.233.169.104, Port: 80

- Destination IP Address: 192.168.1.100, 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?



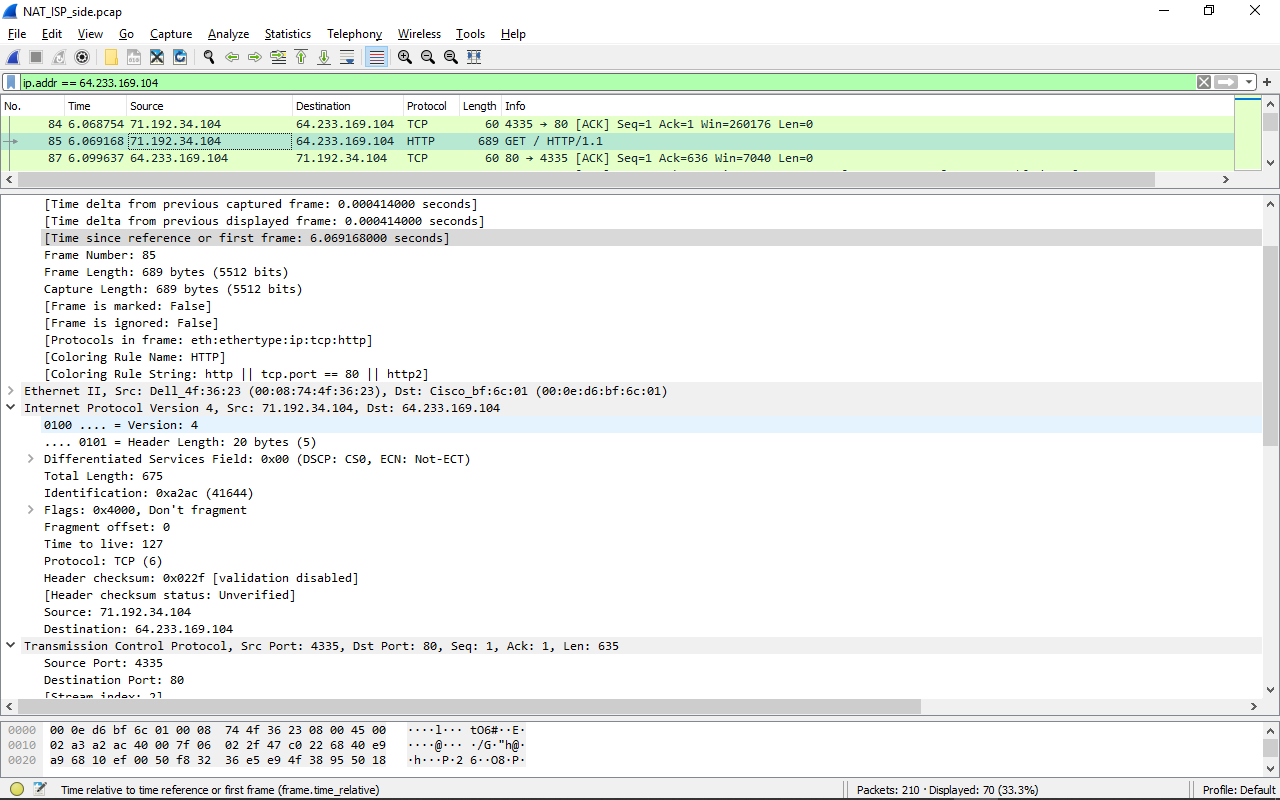
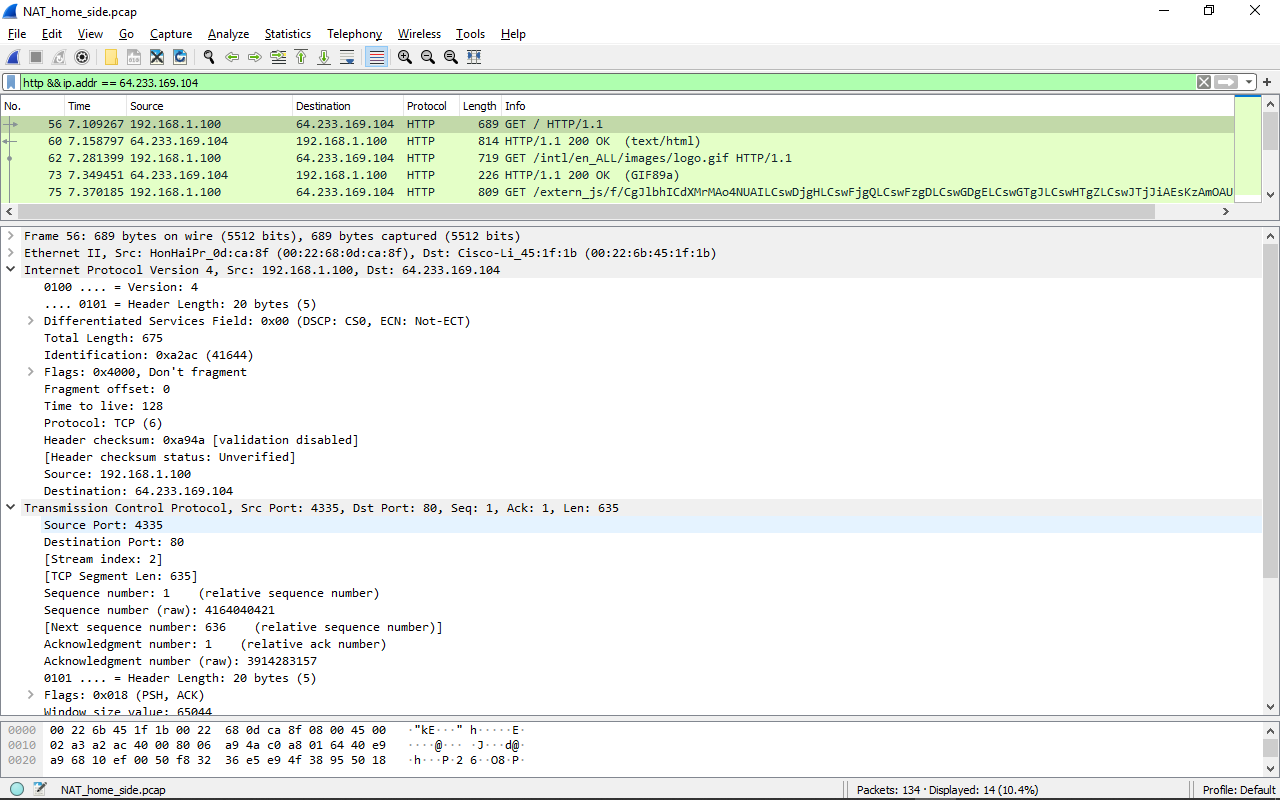
- Thời gian là: 6.069168

- Source IP Address: 71.192.34.104, Port: 4335

- Destination IP Address: 64.233.169.104, Port: 80.

- Destination IP, source IP và các ports đều khác nhau

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.

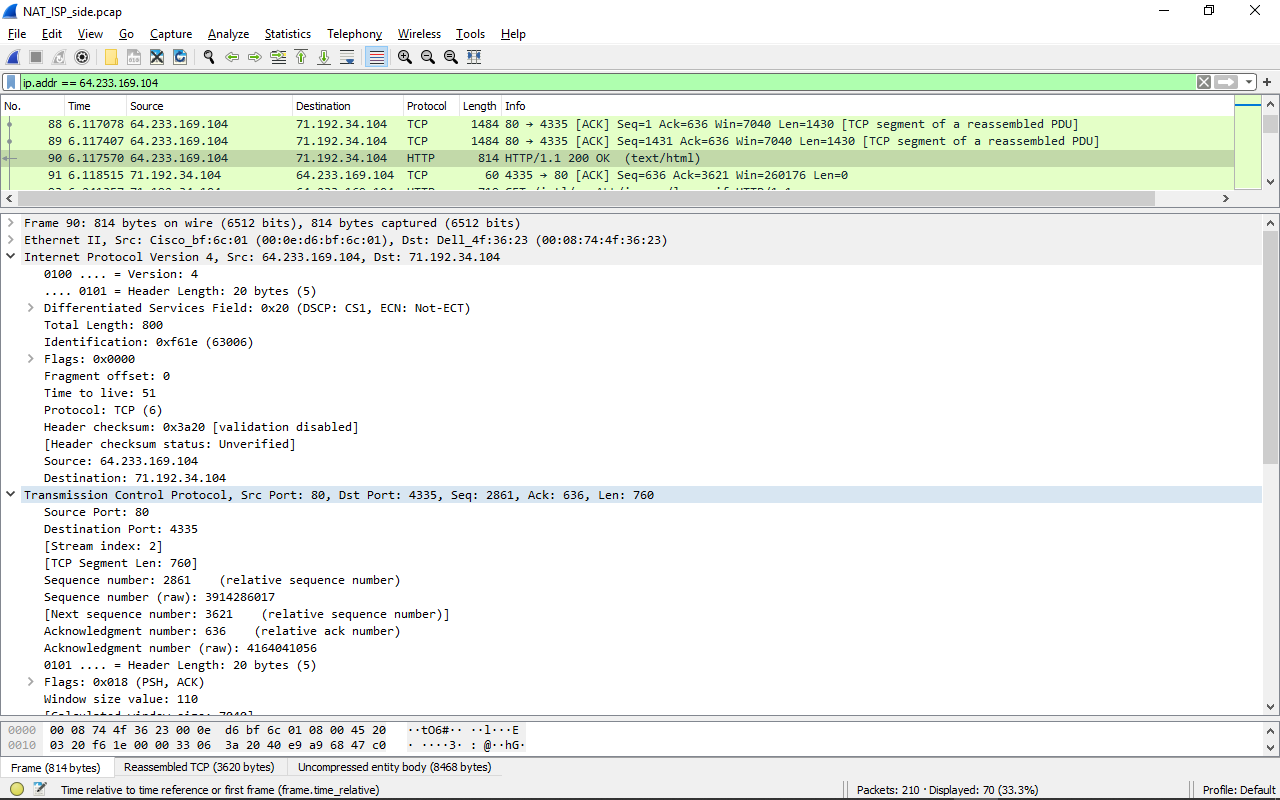


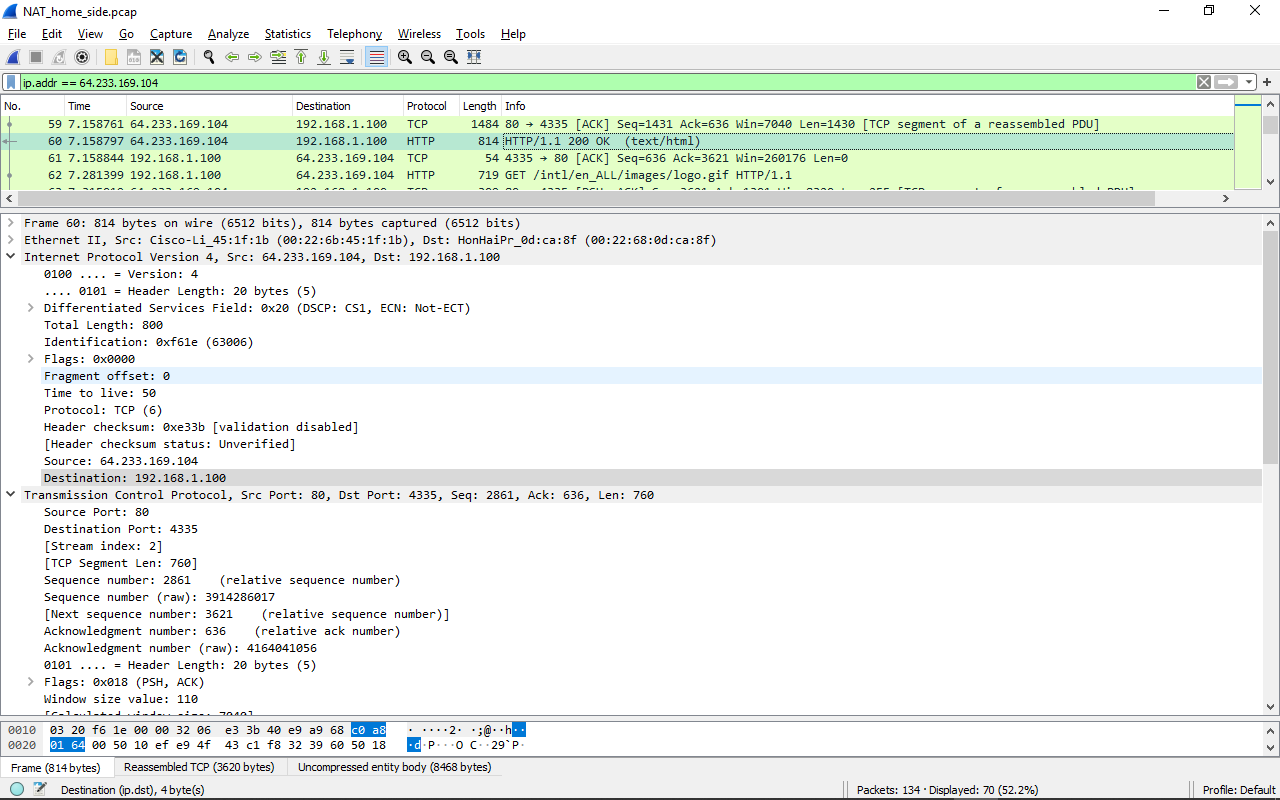
- Trường thay đổi là

+ Time to live: từ 128 (home) thành 127 (ISP)

+ Header checksum: từ 0xa94a (home) thành 0x022f (ISP) do thay đổi địa chỉ IP source từ 192.168.1.100 thành 71.192.34.104

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?





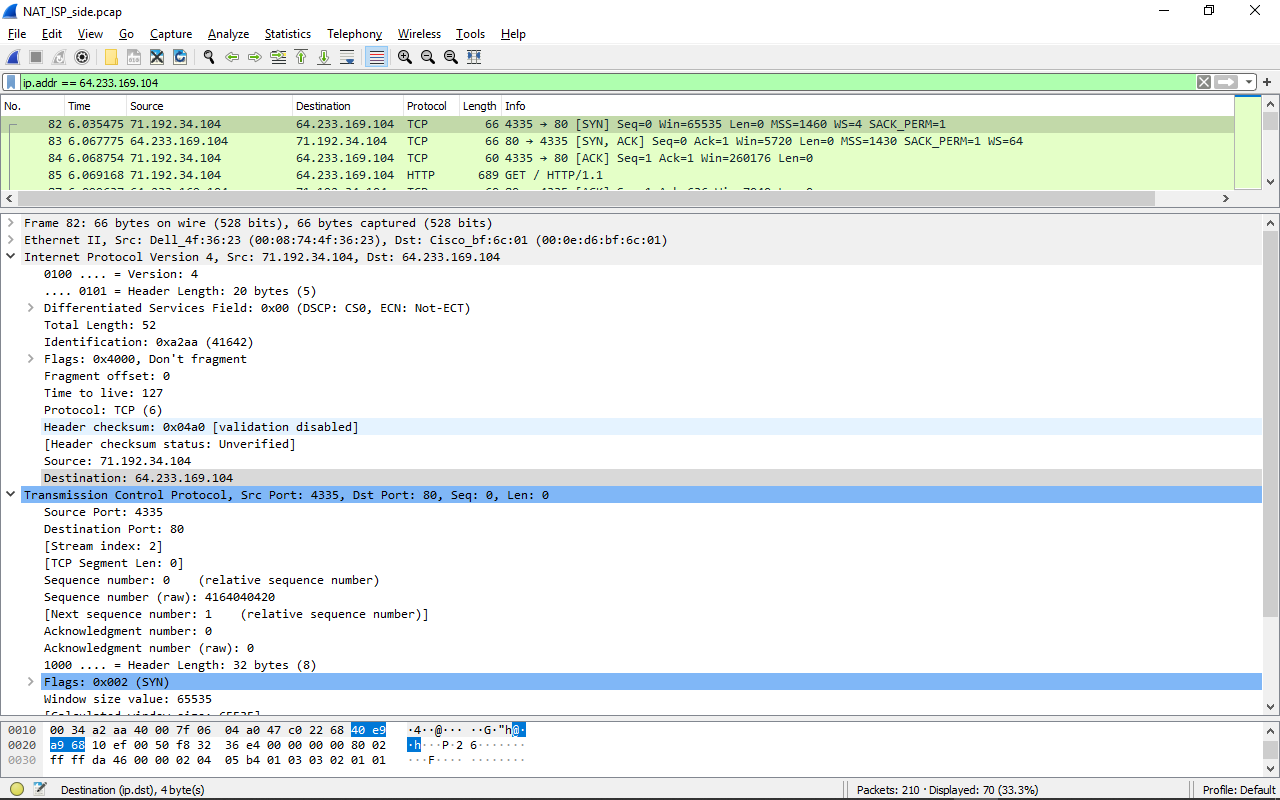
- Thời gian khi nhận 200 OK là 6.117570

- Source IP Address: 64.233.169.104, Port: 80

- Destination IP Address: 71.192.34.104, Port: 4335

- Version và Flag giống nhau. Time to live và Header checksum thay đổi

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?

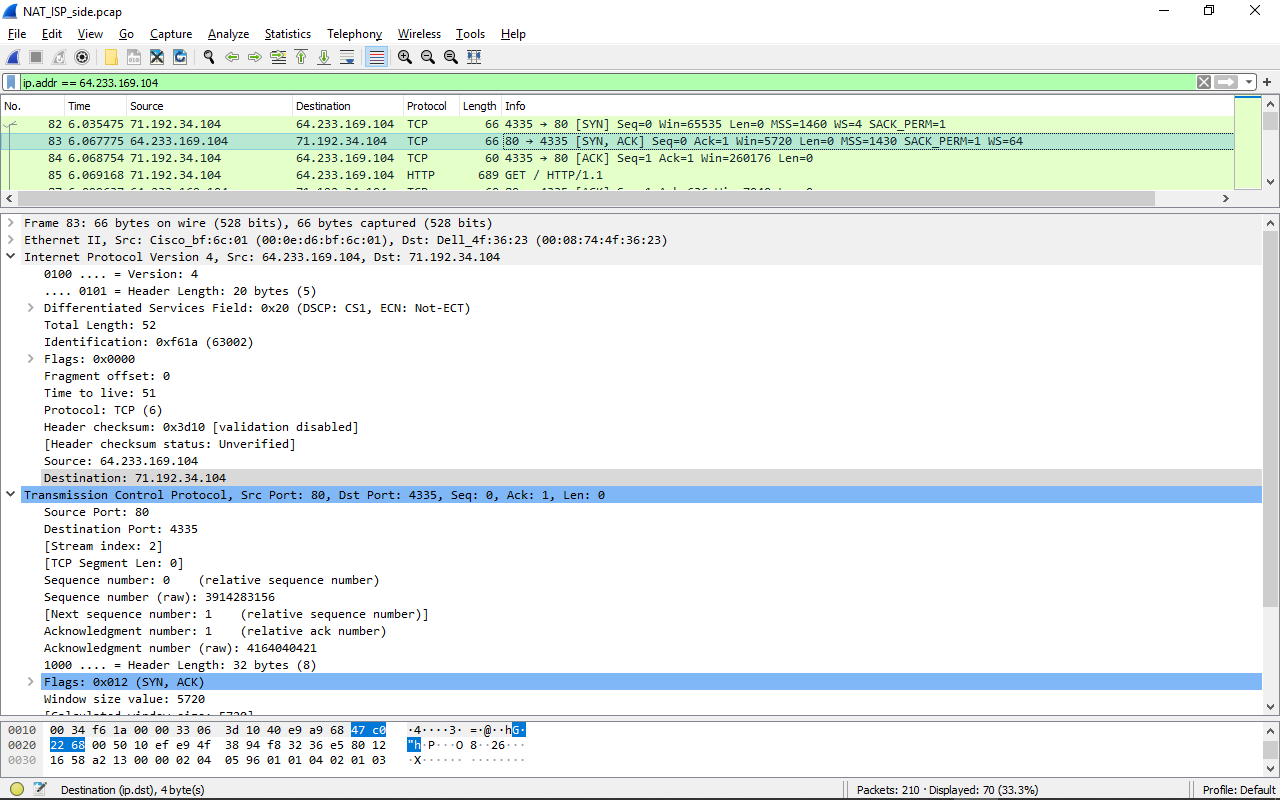


- Thời gian khi gửi TCP SYN segment là 6.035475

- Source IP Address: 71.192.34.104, Port: 4335

- Destination IP Address: 64.233.169.104, Port: 80

- Time to live và Source IP thay đổi



- Thời gian ACK trả về là 7.108986

- Source IP Address: 64.233.169.104, Port: 80

- Destination IP Address: 71.192.34.104, Port: 4335

- Time to live, Destination IP thay đổi

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

|  |  |
| --- | --- |
| NAT translate table | |
| WAN side | LAN side |
| 71.192.34.104:4335 | 192.168.1.100:4335 |