ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH

MẠNG MÁY TÍNH THỰC HÀNH - CO3094

Báo cáo:

Lab4c

Giảng viên hướng dẫn: Vũ Thành Tài

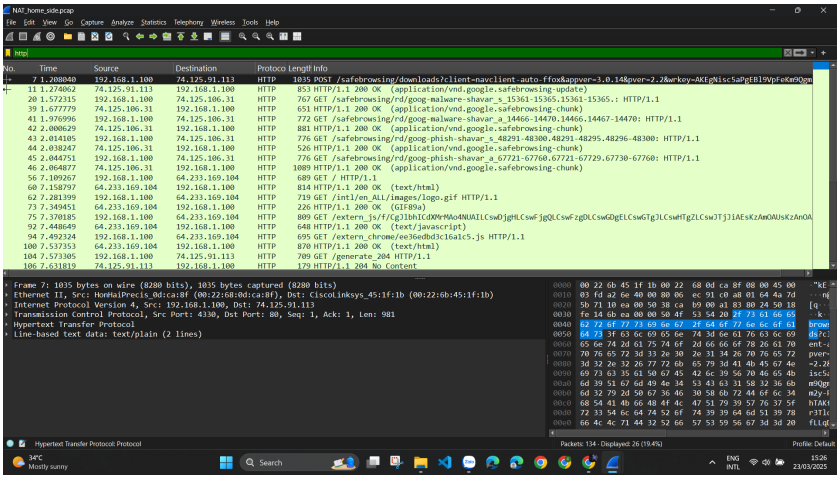
Sinh viên: Lê Đức Cường

Thành phố Hồ Chí Minh, tháng 3 năm 2025

1 Question 1

What is the IP address of the client?

ANS: The IP address of the client in the NAT_home_side trace is 192.168.1.100.

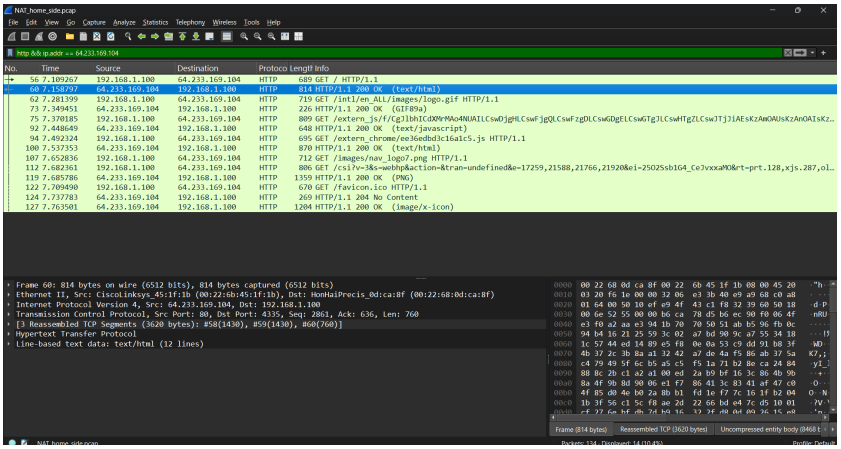


2 Question 2

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 .

ANS:

After applying the filter http && ip.addr == 64.233.169.104, I observed that my client communicates with the Google server at IP 64.233.169.104. The HTTP packets confirm that the client is sending and receiving data from this server, which is responsible for delivering the main Google web page.



3 Question 3

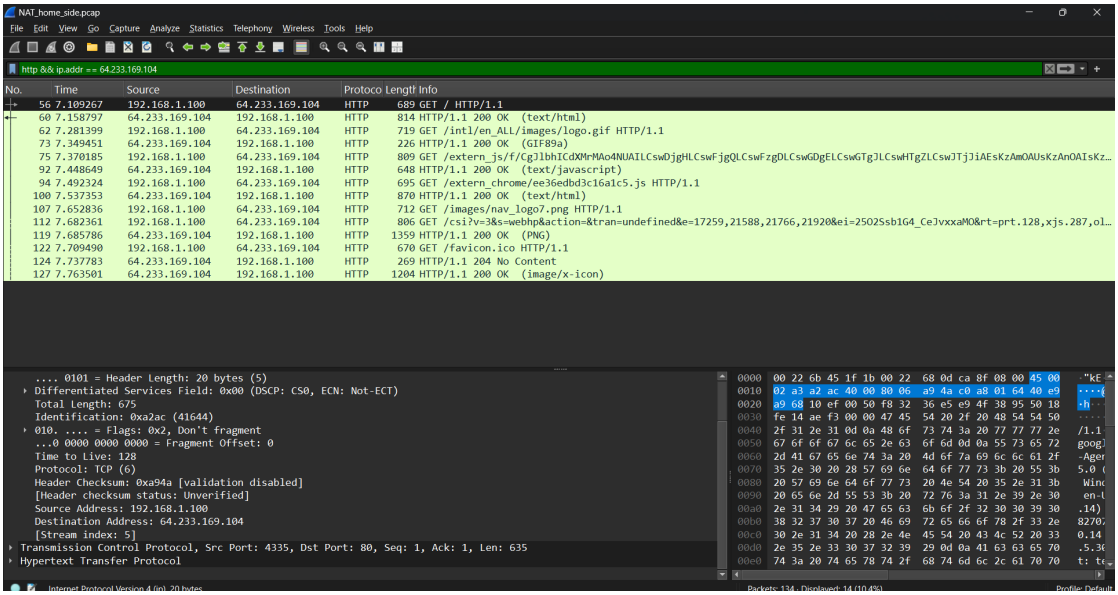
Consider now the HTTP GET sent from the client to the Google server (whose IP address is IP address 64.233.169.104) at time 7.109267. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?

ANS:

The HTTP GET request sent from my client to the Google server at time 7.109267 has the following details:

- Source IP Address: 192.168.1.100
- Destination IP Address: 64.233.169.104
- TCP Source Port: 4335
- TCP Destination Port: 80

These values indicate that my client initiated an HTTP request to the Google server using a dynamically assigned source port.



4 Question 4

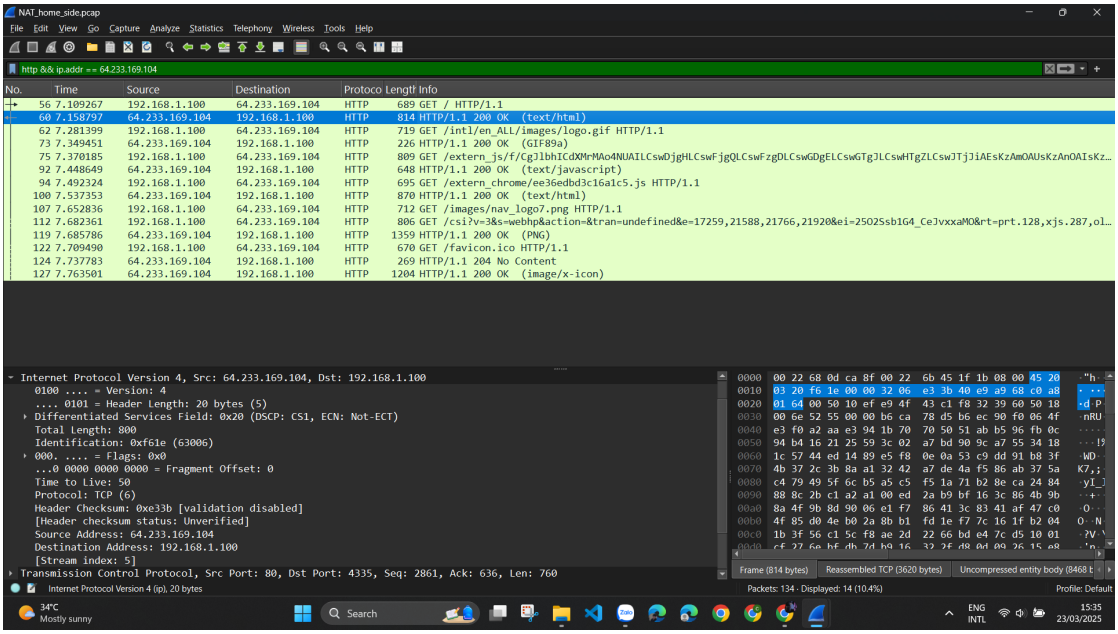
At what time4 is the corresponding 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

ANS:

The HTTP 200 OK response from the Google server was received. The details of the packet are as follows:

- Source IP Address: 64.233.169.104
- Destination IP Address: 192.168.1.100
- TCP Source Port: 80
- TCP Destination Port: 4335

These values confirm that my client successfully received a response from the Google server, completing the HTTP request-response cycle.



5 Question 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).

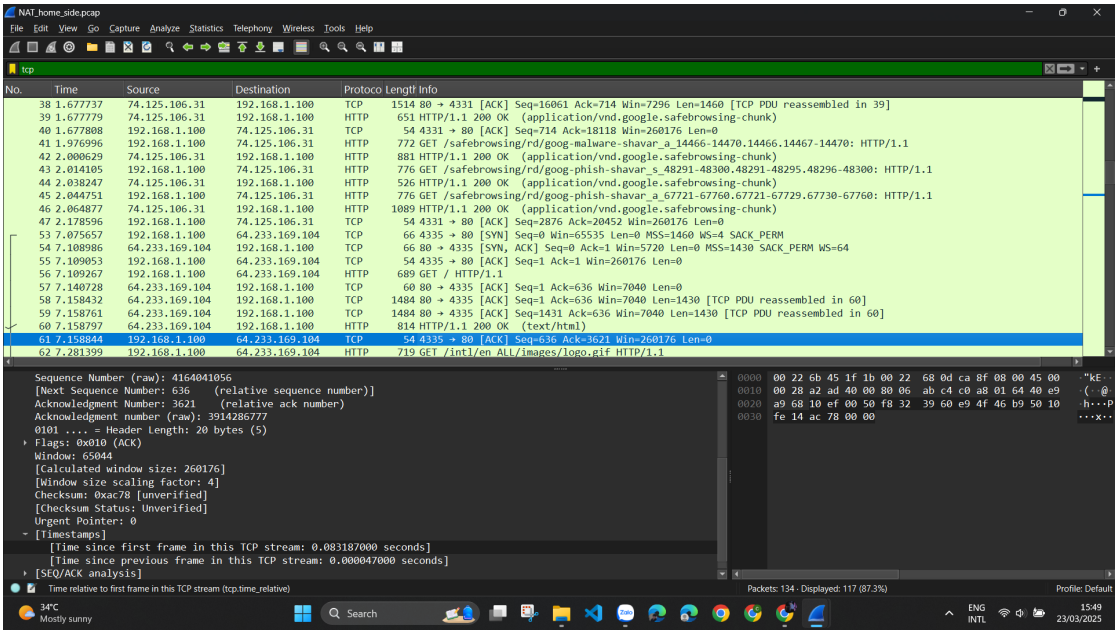
ANS:

The TCP SYN segment that initiates the connection is sent at time 0.083187. The details of the TCP handshake are as follows:

- Source IP Address: 64.233.169.104
- Destination IP Address: 192.168.1.100

- TCP Source Port: 80
- TCP Destination Port: 4335
- Timestamp: 0.083187

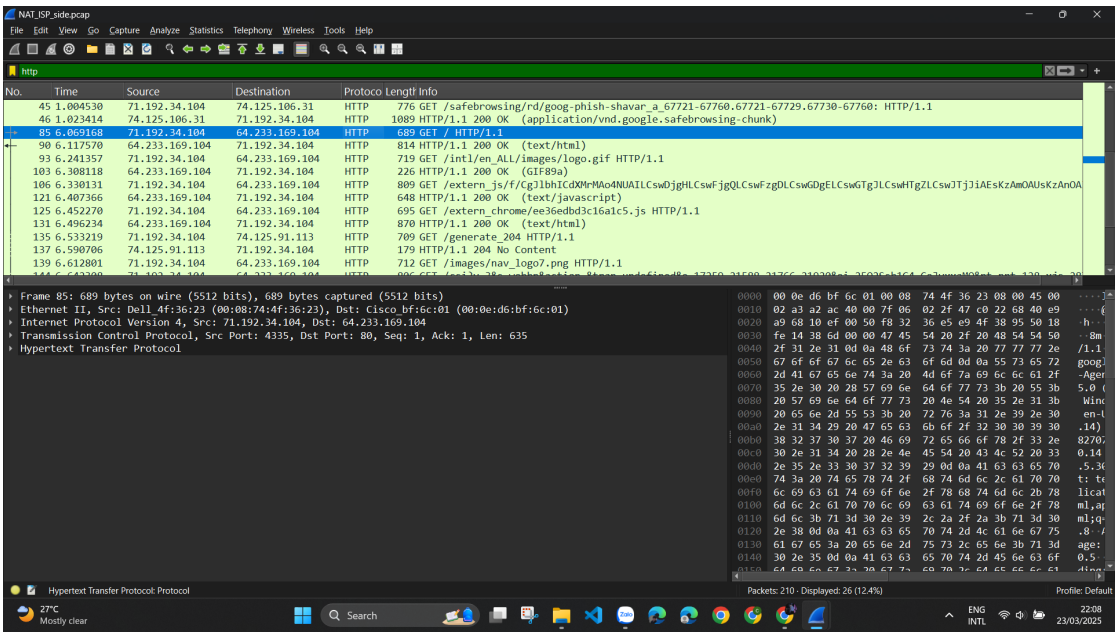
These values confirm that my client successfully received a response from the Google server, completing the HTTP request-response cycle.



6 Question 6

In the NAT_ISP_side trace file, find the HTTP GET message that was sent from the client to the Google server at time $t = 7.109267$ (where $t = 7.109267$ is the 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 recorded in the NAT_ISP_side trace file)? Which of these fields are the same, and which are different, compared to your answer to question 3 above?

ANS:



At 6.069168, the HTTP GET message appears in the NAT_ISP_side trace file.

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

The only difference compared to Question 3 is the source IP address, which has been modified due to NAT translation.

7 Question 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.

ANS:

- Version: Unchanged (IPv4 remains IPv4).
- Header Length: Unchanged (The IP header size is not affected by NAT).
- Flags: Unchanged (Flags in the IP header are mainly used for fragmentation and are not impacted by NAT).
- Checksum: Changed.

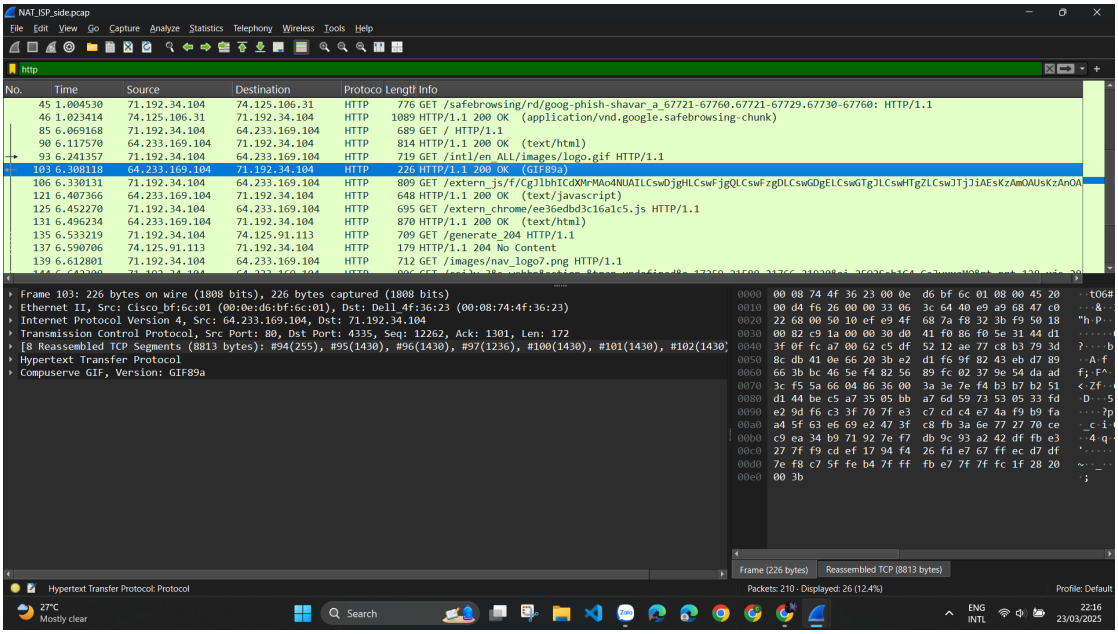
Reason: The checksum is recalculated because NAT modifies the source IP address and possibly the source port, which affects the IP header checksum.

8 Question 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?

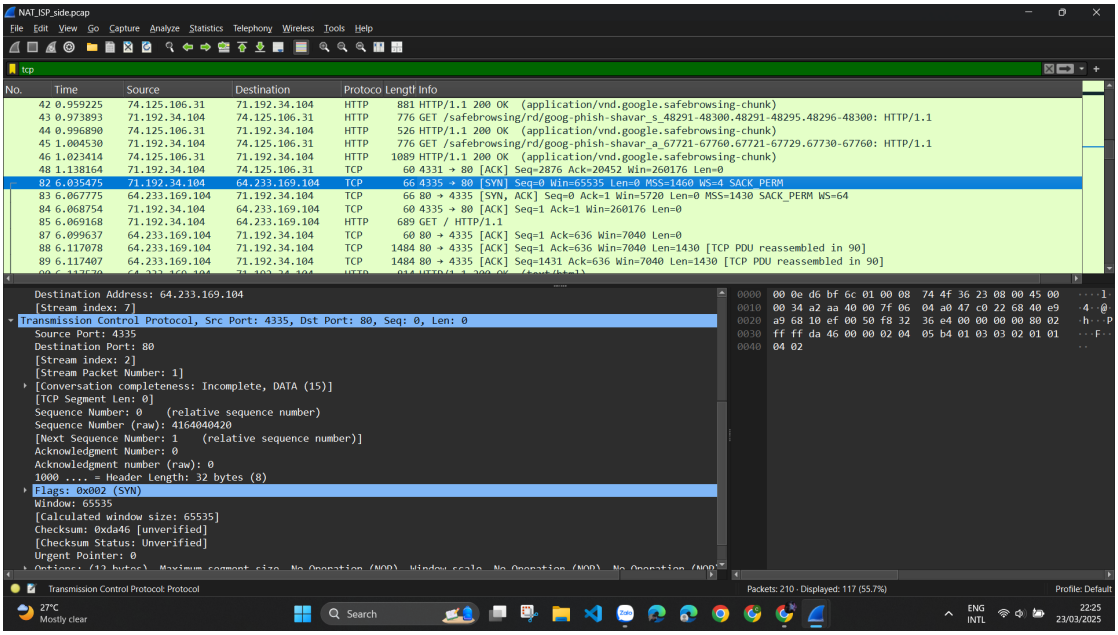
ANS: At 6.308118, the first HTTP 200 OK message is received from the Google server.

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



9 Question 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?



Differences Compared to Question 5:

- The source IP address of the SYN packet has changed due to NAT.
- The destination IP address of the ACK packet has also changed due to NAT mapping.

Packet Details:

TCP SYN:

- Source IP: 71.192.34.104 (modified by NAT)
- Source Port: 4335
- Destination IP: 64.233.169.104 (Google server, unchanged)
- Destination Port: 80

TCP ACK:

- Source IP: 64.233.169.104 (Google server, unchanged)
- Source Port: 80
- Destination IP: 71.192.34.104 (modified by NAT)
- Destination Port: 4335

Due to NAT, the private IP 192.168.1.100 of the client in the home network was translated to the public IP 71.192.34.104 when communicating with external servers on the Internet.

10 Question 10

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

ANS:

NAT translate table

WAN side 71.192.34.104, 4335

LAN side 192.168.1.100, 4335