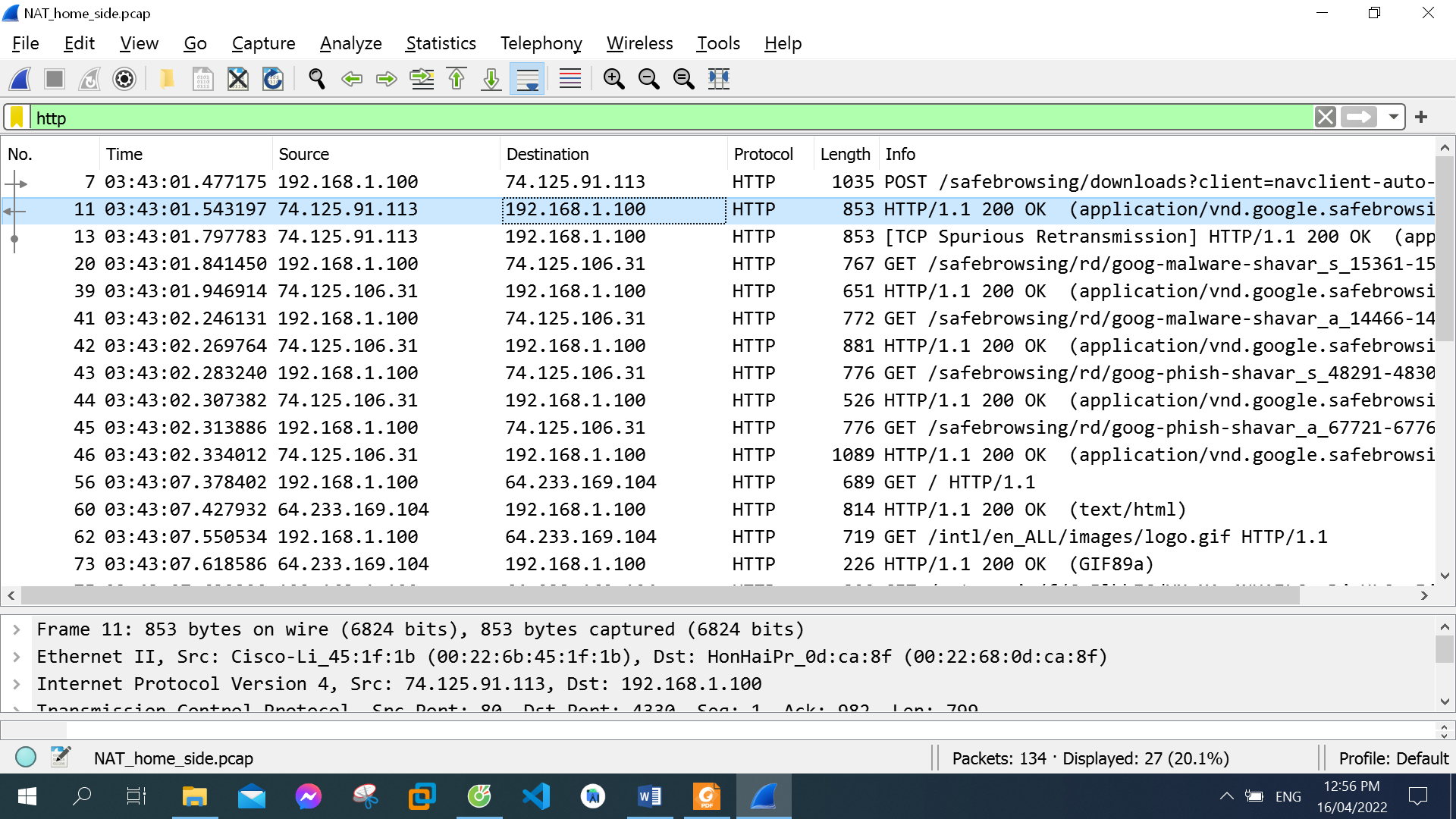
**LAB 4C: NAT v8.0**

**Name: Hồ Đức Trí**

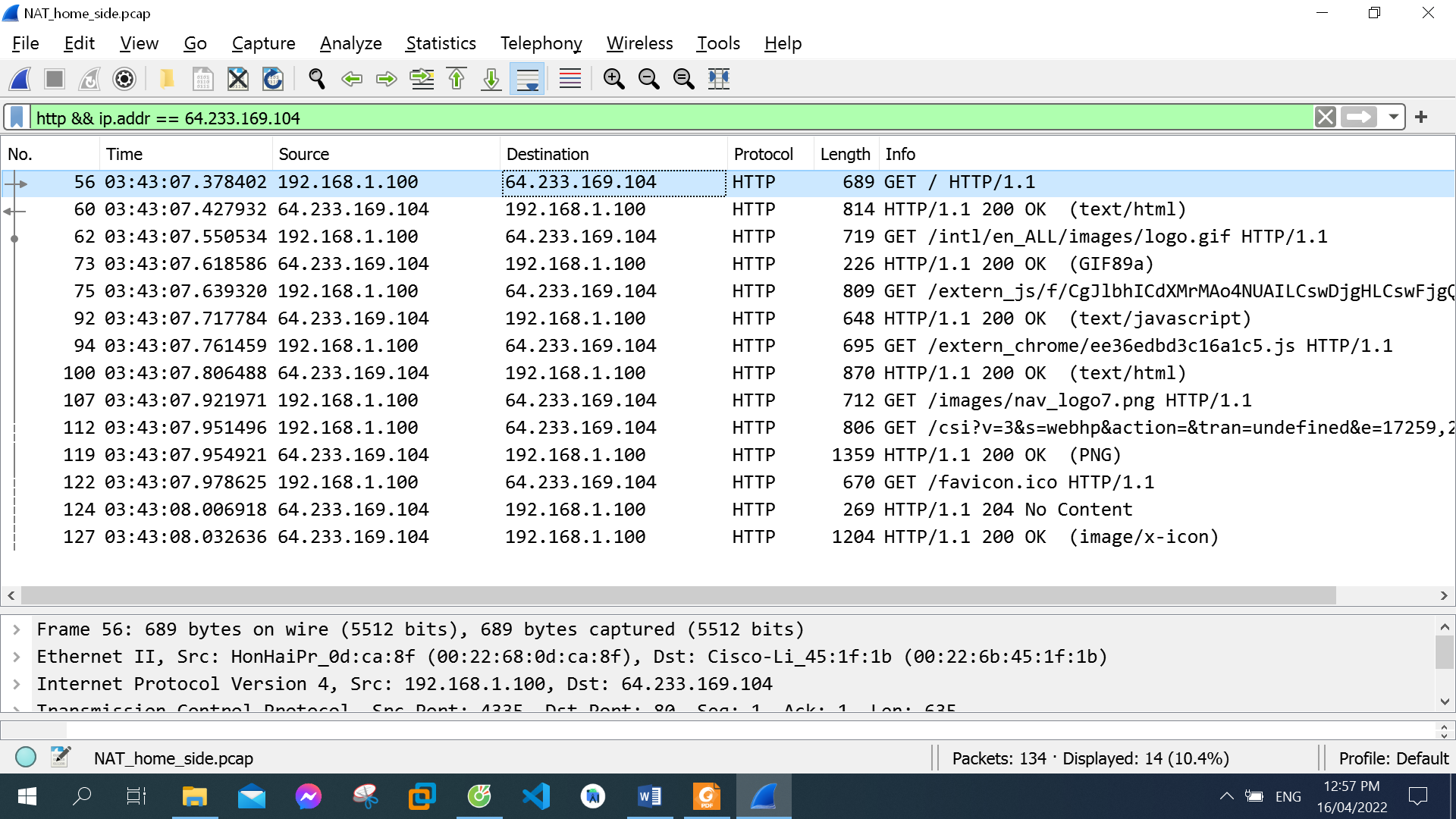
**Student No: 1912288**

1. What is the IP address of the client?

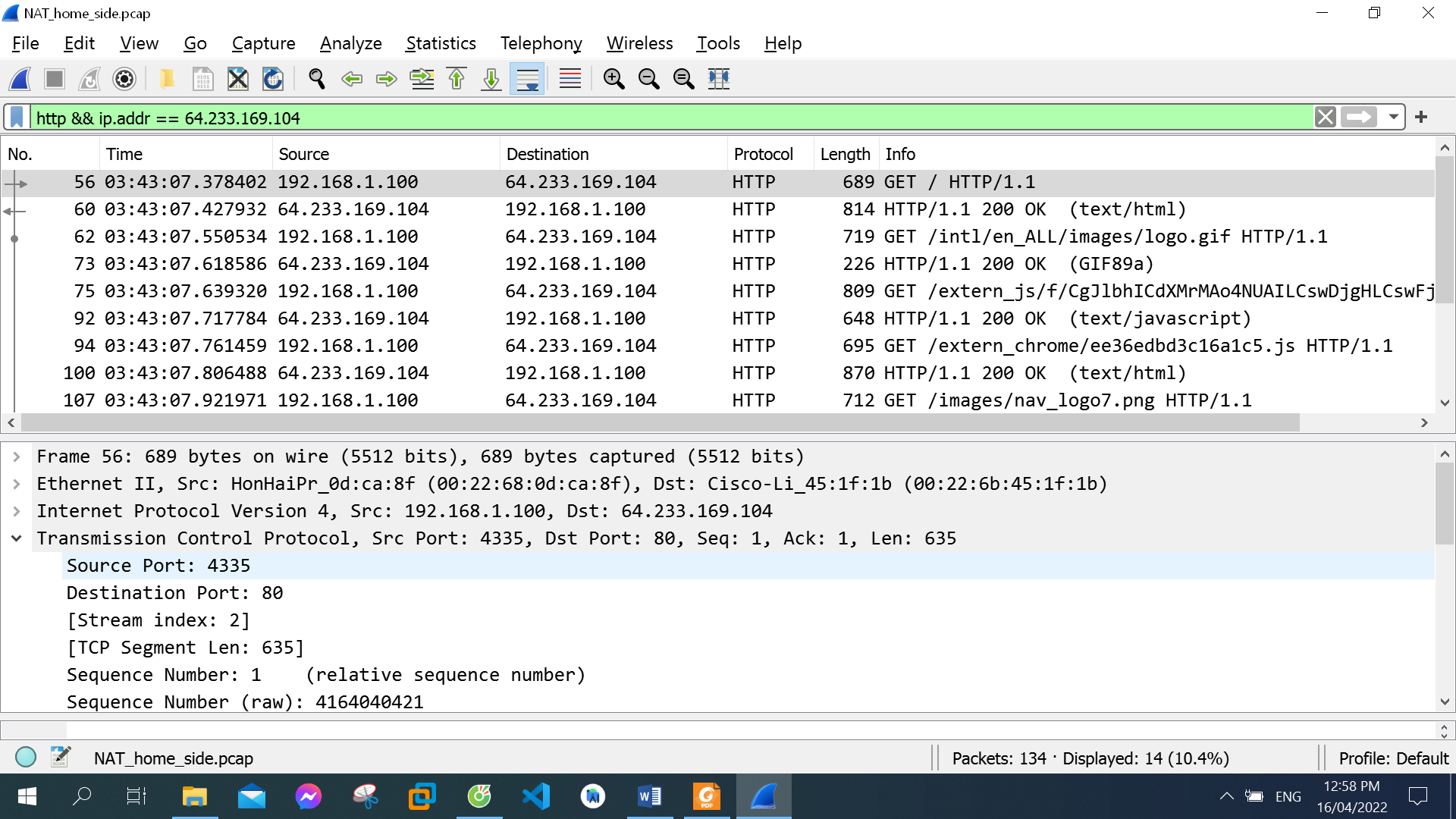


The IP address of the client: 192.168.1.100

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 . .



1. 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 7.378402. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?



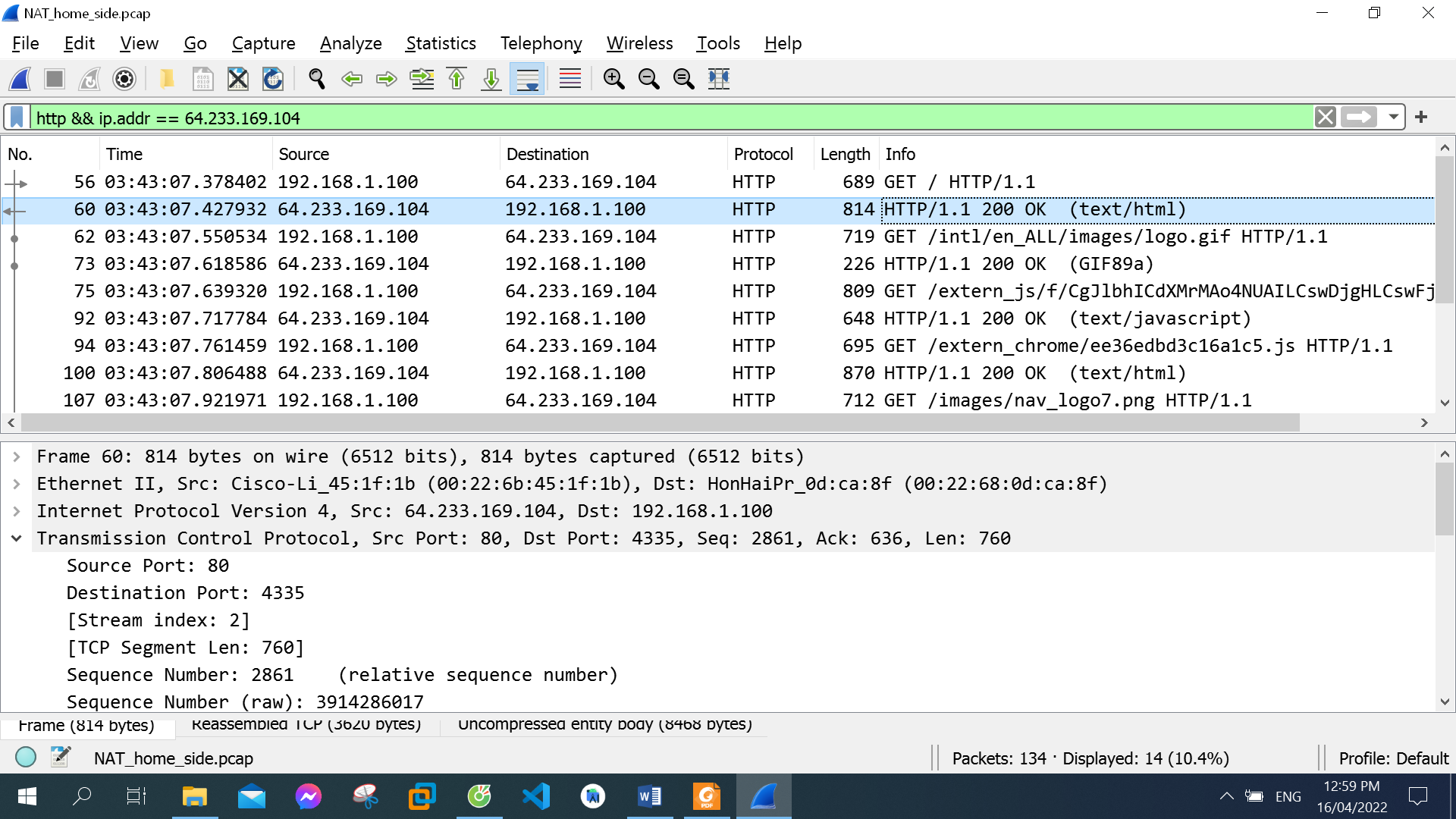
Source IP address: 192.168.1.100

TCP source port: 4335

Destination IP address: 64.233.168.104

TCP 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?



The corresponding 200 OK HTTP message received from the Google server at: 7.427932

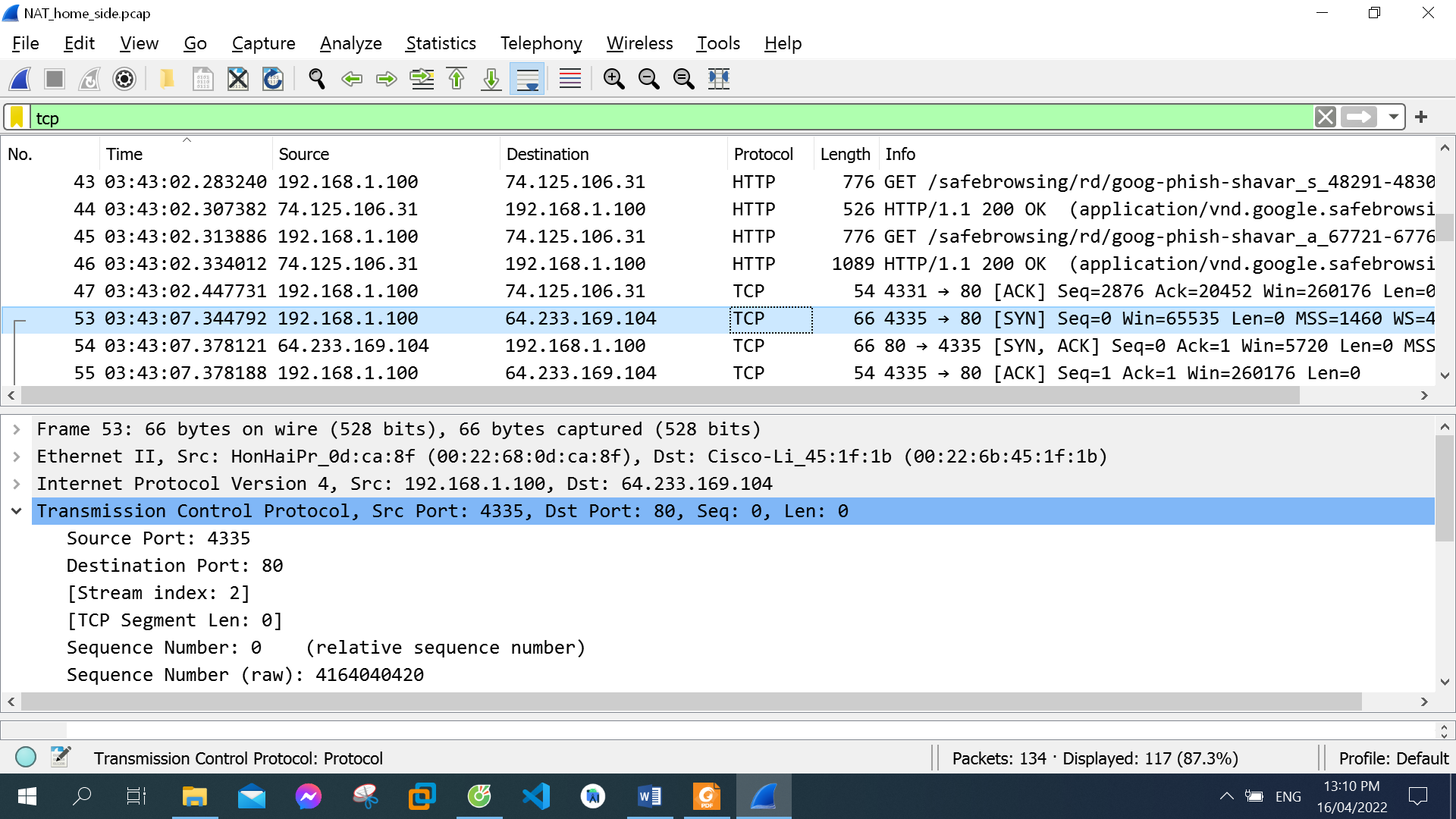
Source IP address: 64.233.168.104

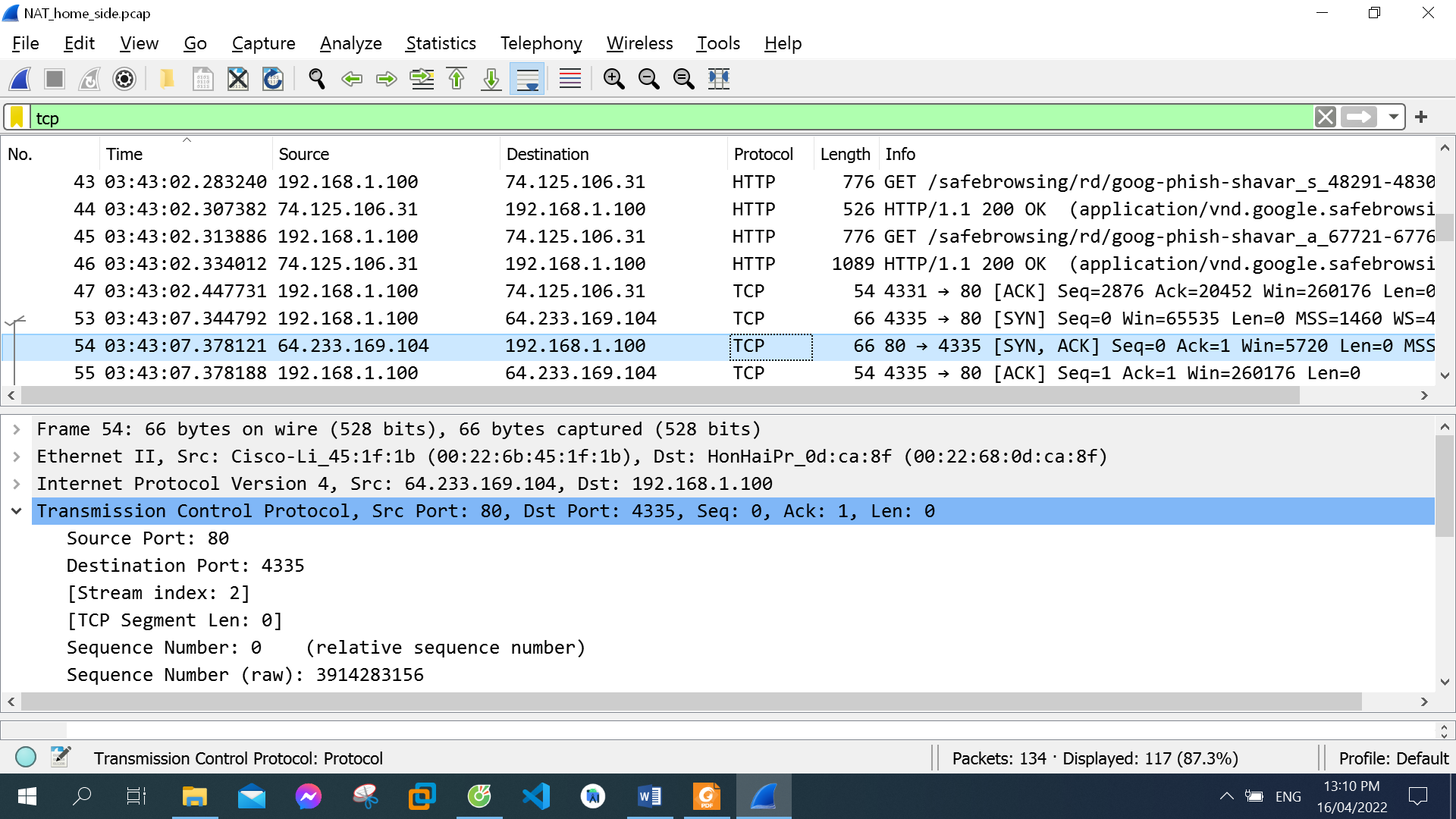
TCP source port: 80

Destination IP address: 192.168.1.100

TCP destination port: 4335

1. 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. 378402? 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?





The client-to-server TCP SYN segment sent that sets up the connection at: 7.344792

TCP segment:

Source IP address: 192.168.1.100

TCP source port: 4335

Destination IP address: 64.233.168.104

TCP destination port: 80

ACK sent in response to the SYN:

Source IP address: 64.233.168.104

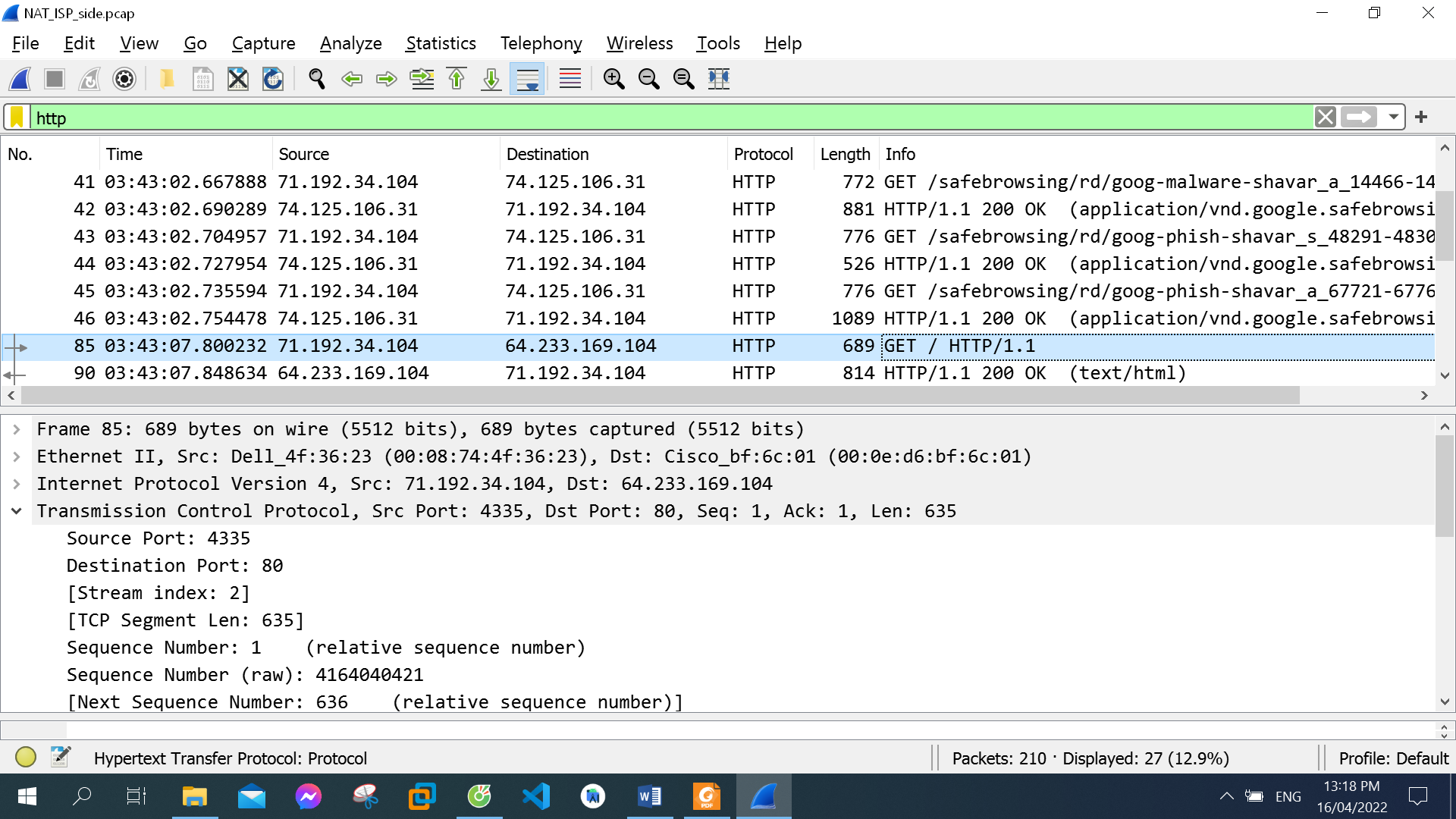
TCP source port: 80

Destination IP address: 192.168.1.100

TCP destination port: 4335

This ACK received at the client at: 7.378121

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? Which of these fields are the same, and which are different, than in your answer to question 3 above?



This message appear in the NAT\_ISP\_side trace file: 7.800232

Source IP address: 71.192.34.104

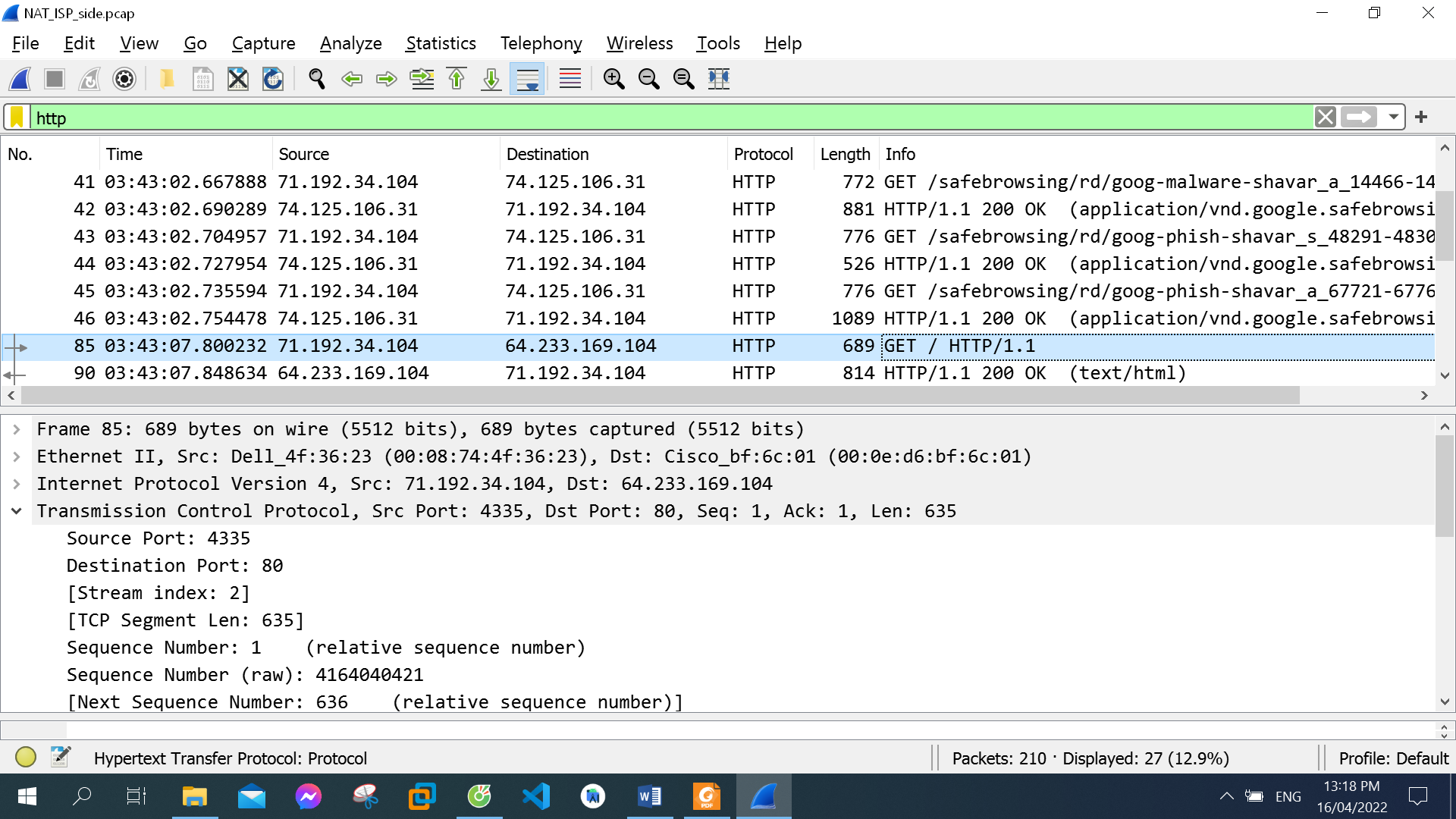
TCP source port: 4335

Destination IP address: 64.233.168.104

TCP destination port: 80

Only Destination IP address is different in my answer to Q4 above

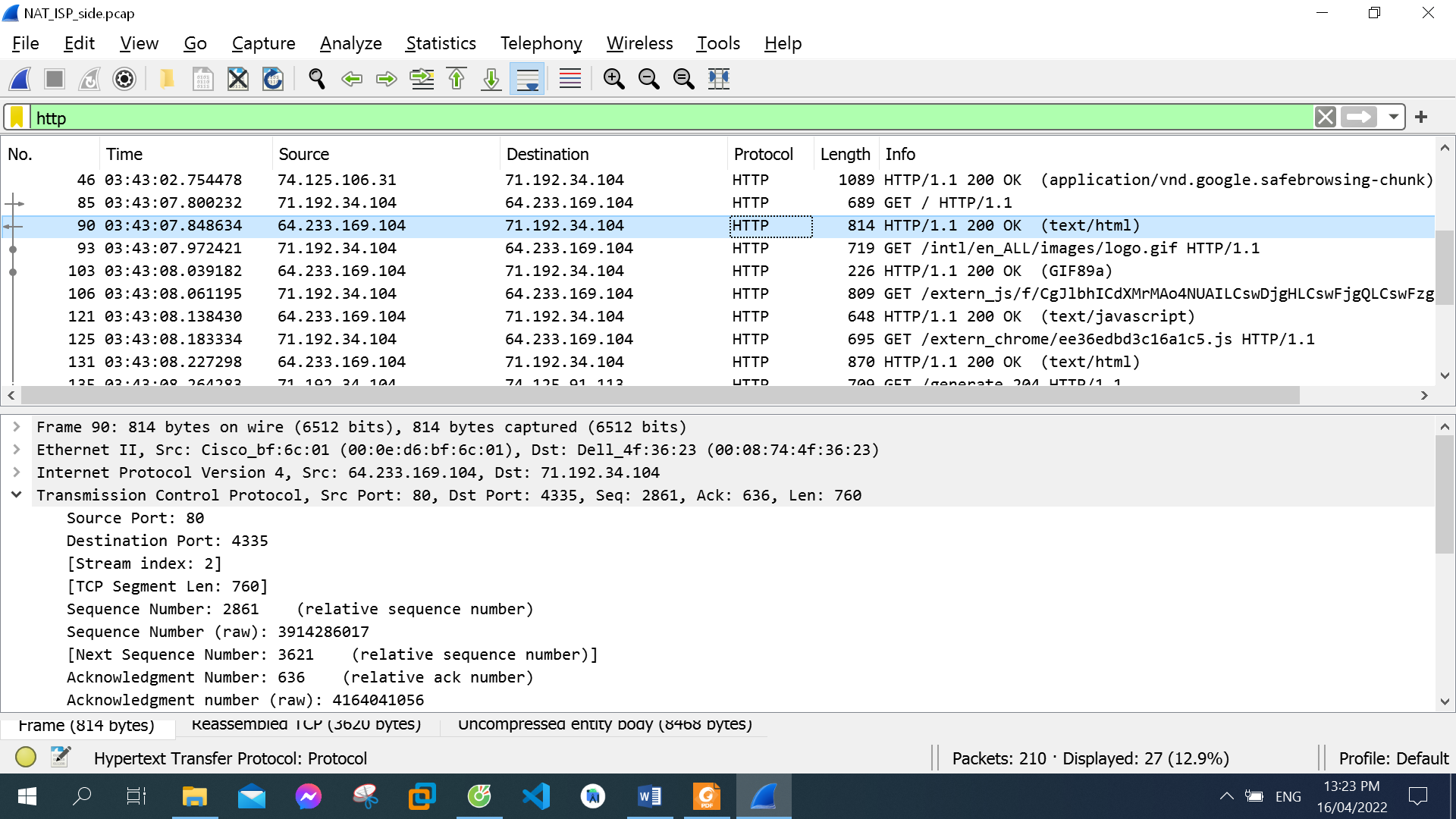
1. Are any fields in the HTTP GET message changed? Which of the following fields in the IP datagram carrying the HTTP GET are changed: Version, Header Length, Flags, Checksum. If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change.



There is no field in the HTTP GET message changed

Only Checksum changed. Because the IP source address changed, checksum include value of IP source address

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?



The first 200 OK HTTP message received from the Google server at: 7.848634

Source IP address: 64.233.168.104

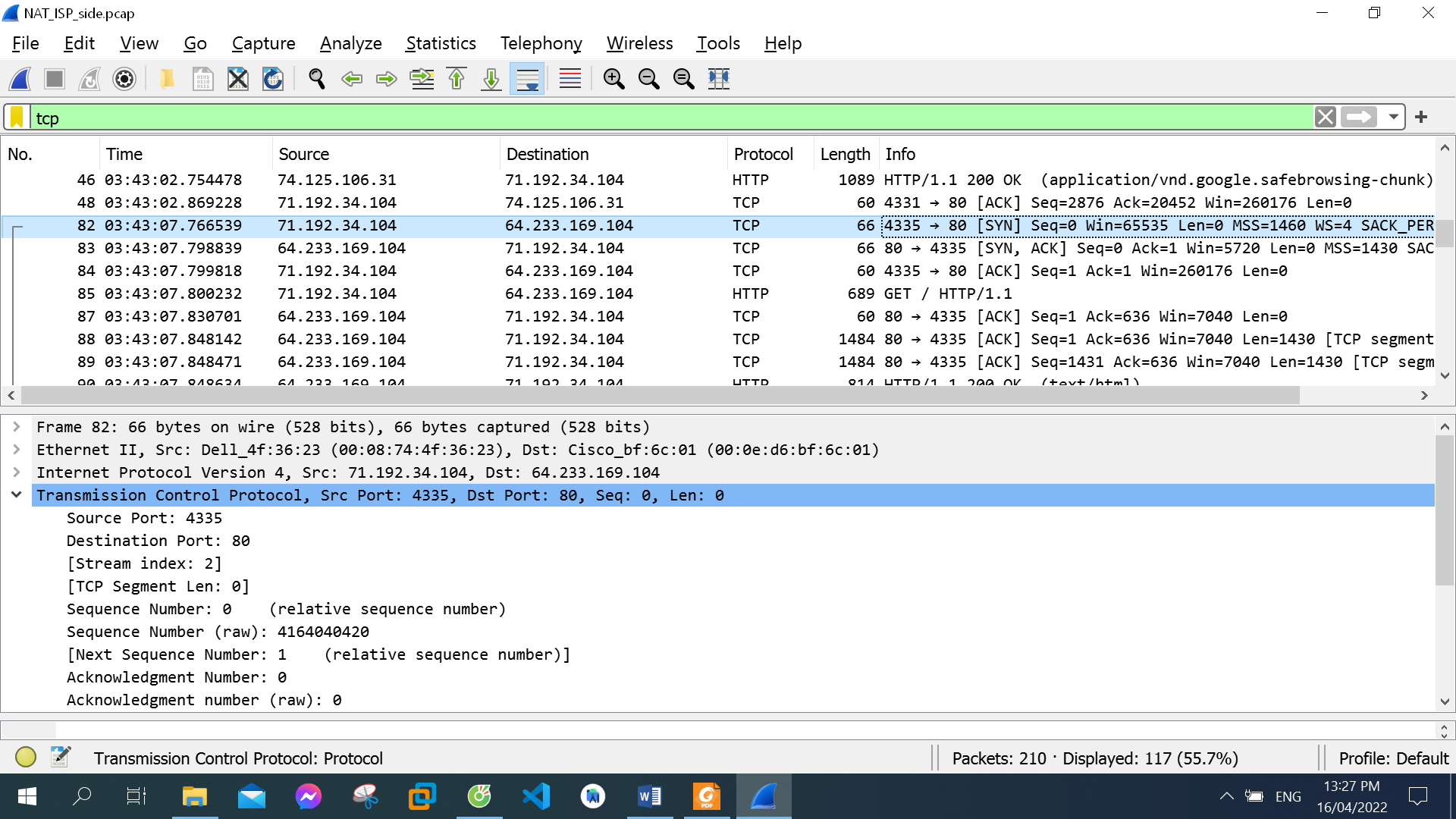
TCP source port: 80

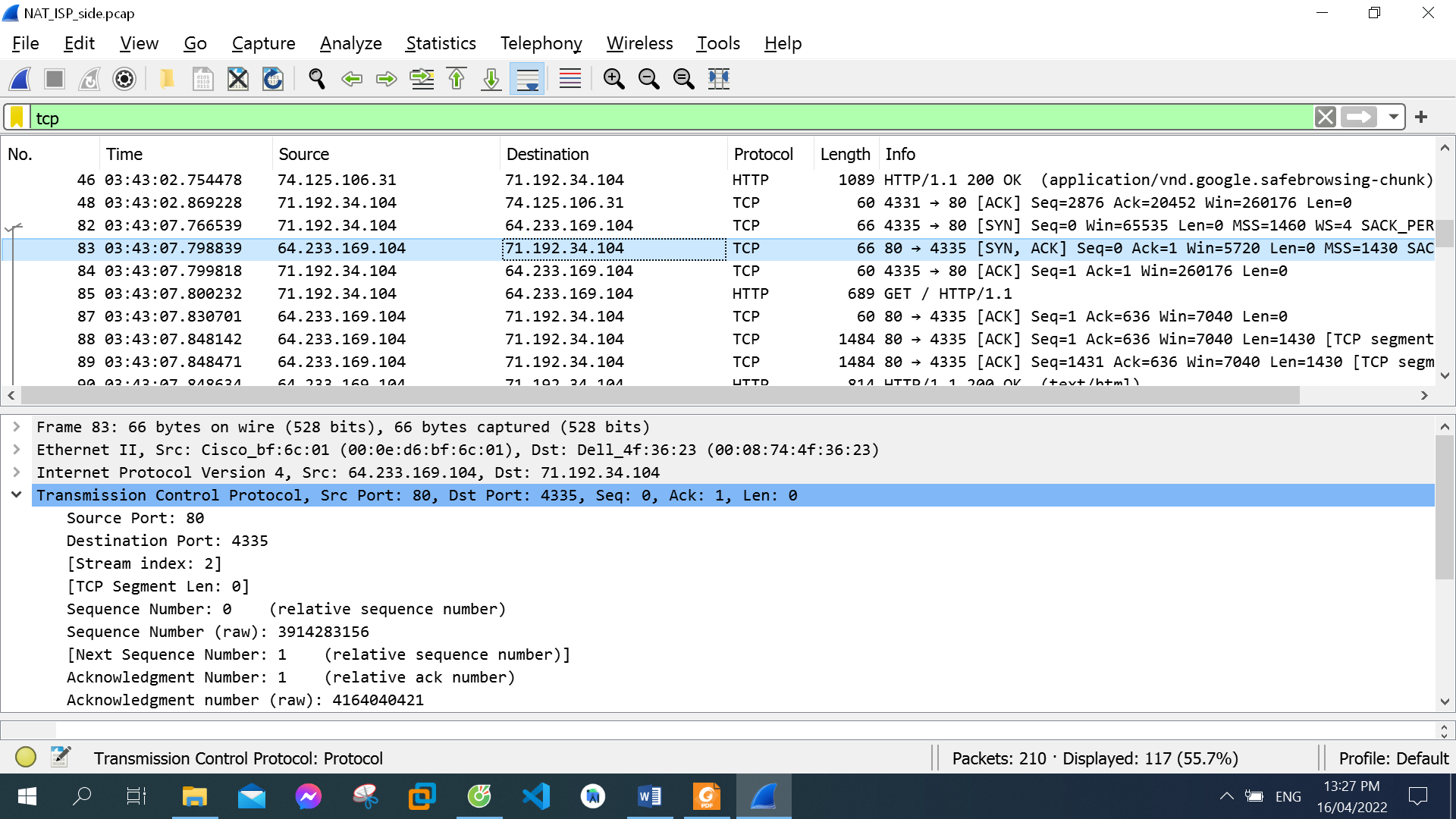
Destination IP address: 71.192.34.104

TCP destination port: 4335

Only Destination IP address is different in my answer to Q4 above

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 corresponding at: 7.766539

The server-to-client TCP ACK segment corresponding at: 7.798839

The client-to-server TCP SYN segment:

Source IP address: 71.192.34.104

TCP source port: 4335

Destination IP address: 64.233.168.104

TCP destination port: 80

The server-to-client TCP ACK segment:

Source IP address: 64.233.168.104

TCP source port: 80

Destination IP address: 71.192.34.104

TCP destination port: 4335

The client-to-server TCP SYN segment: Source IP address changed

The server-to-client TCP ACK segment:: Destination IP address changed

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 translation table entries | | |
|  | WAN side | LAN side |
| IP address | 71.192.34.104 | 192.168.1.100 |
| TCP port | 4335 | 4335 |