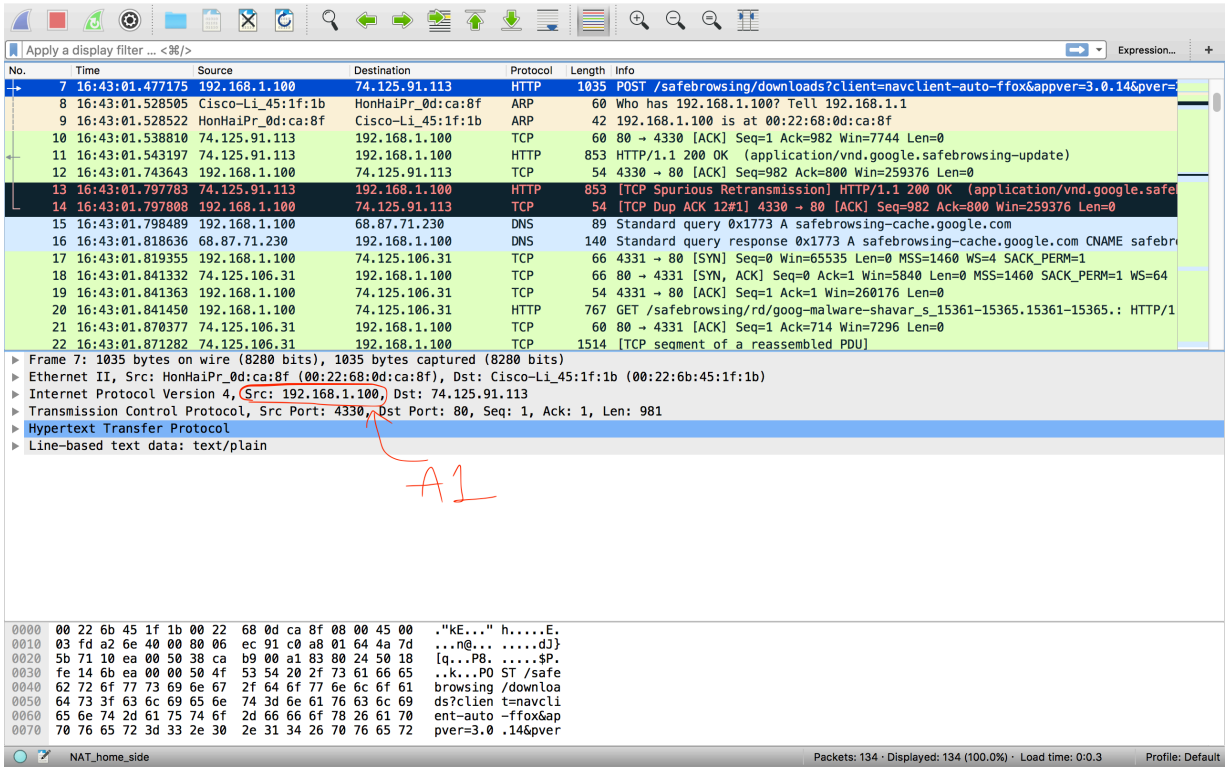
CN Assignment : NAT

BY:
Monil Shah
mds747

1. What is the IP address of the client?

Ans.) The IP address of the client according to the screenshot below is “192.168.1.100”

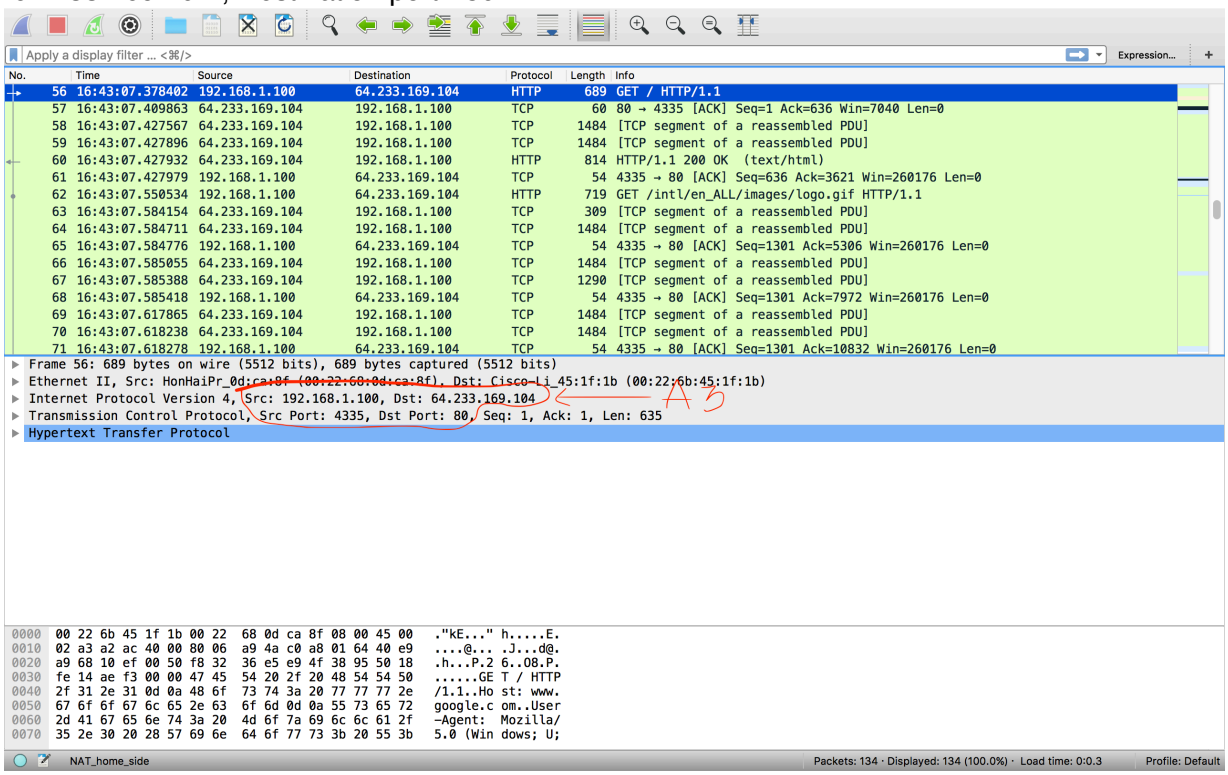


2. The client actually communicates with several different Google servers in order to implement “safe browsing.” (See extra credit section at the end of this lab). The main Google server that will serve up the main Google web page has IP address 64.233.169.104. In order to display only those frames containing 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 .

Ans.) 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 .

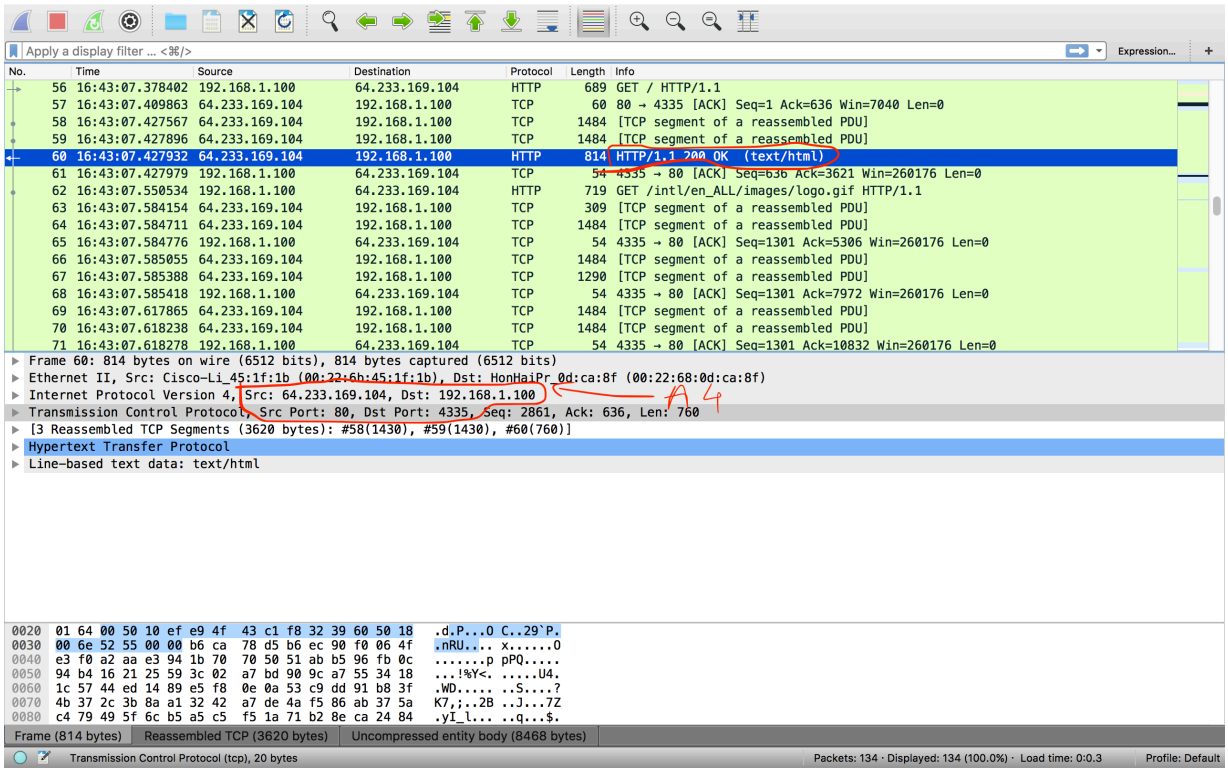
3. Consider now the HTTP GET sent from the client to the Google server (whose IP address is IP address 64.233.169.104) at time 7.109267. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?

Ans.) Source IP address is “192.168.1.100”, Source port: “4335” and Destination IP address: “64.233.169.104”, Destination port: “80”.



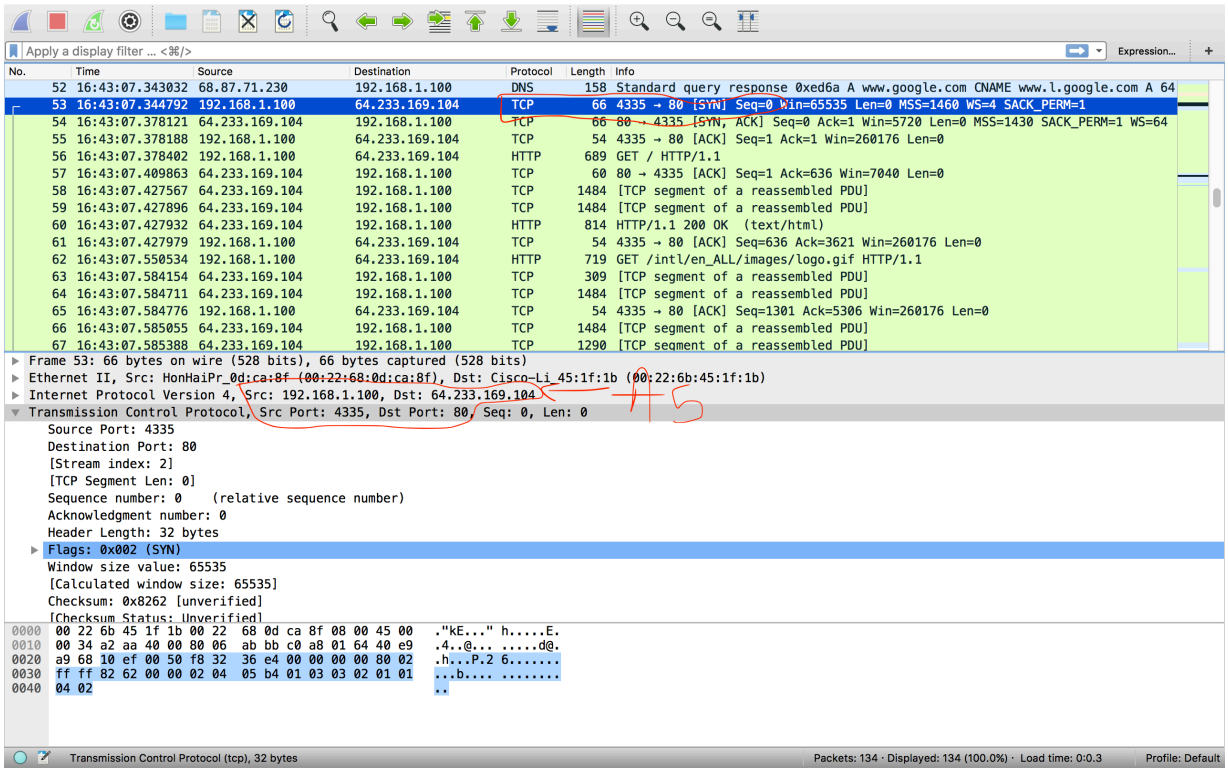
4. At what time4 is the corresponding 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

Ans.) According to the screenshot below the corresponding 200 OK HTTP message received from the Google server at 7.158797 and the Source IP address is “64.233.169.104”, Source port: “80” and Destination IP address: “192.168.1.100”, Destination port: “4335”.



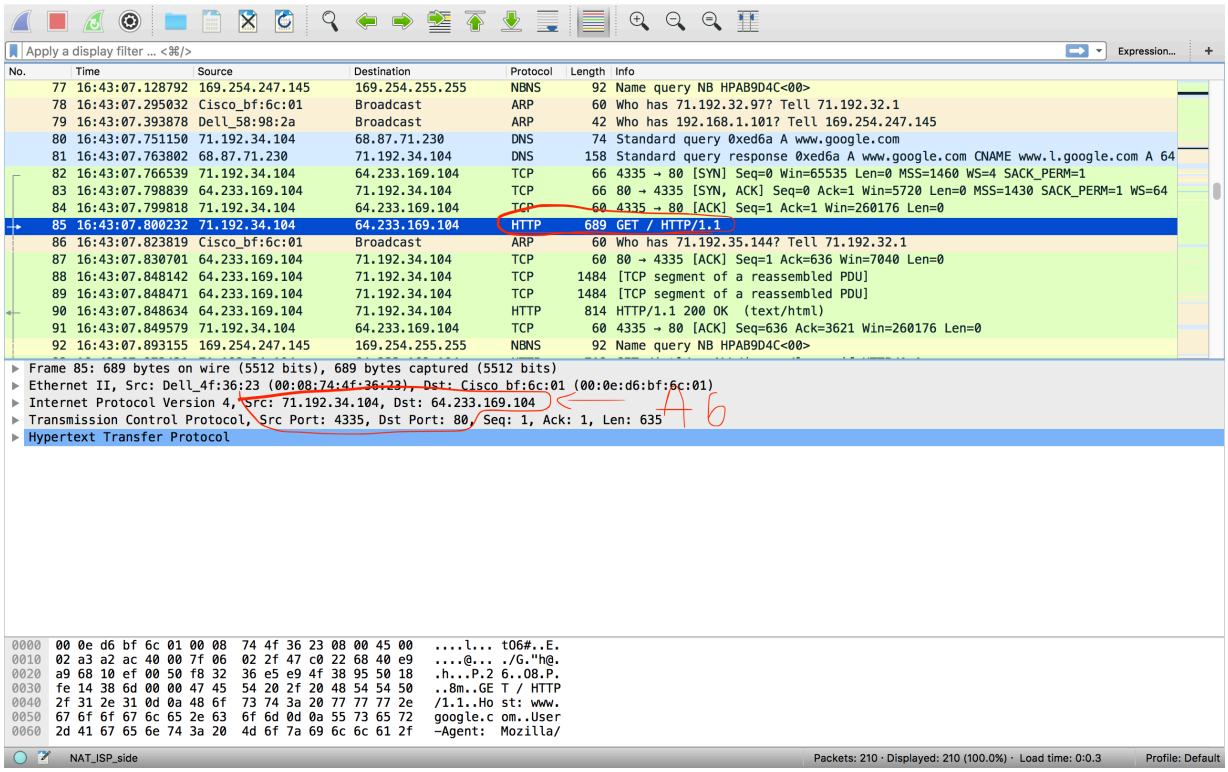
5. Recall that before a GET command can be sent to an HTTP server, TCP must first set up a connection using the three-way SYN/ACK handshake. At what time is the client-to-server TCP SYN segment sent that sets up the connection used by the GET sent at time 7.109267? What are the source and destination 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? (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 client-to-server TCP SYN segment that sets up the connection used by the GET sent at time 7.102967 is sent at 7.075657 and it has the source IP address of “192.168.1.100” with port “4335” and destination IP address of “64.233.169.104” with port “80” according to the screenshot below.



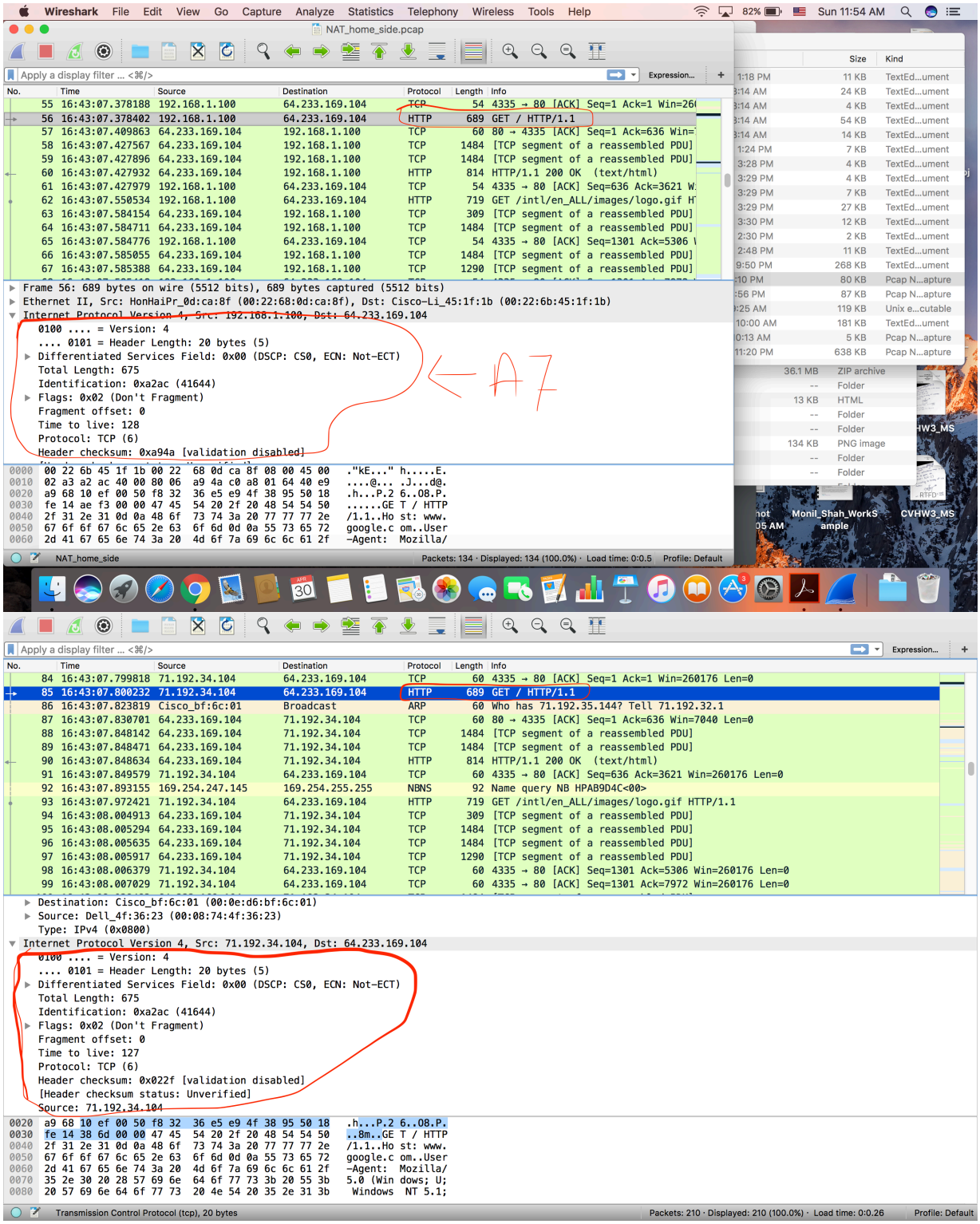
6. In the NAT_ISP_side trace file, find the HTTP GET message was sent from the client to the Google server at time 7.109267 (where t=7.109267 is time at which this was sent as recorded in the NAT_home_side trace file). At what time does this message appear in the NAT_ISP_side trace file? What are the 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?

Ans.) The HTTP GET message in the NAT_ISP_side trace file was sent from the client to the Google server at time 7.102967. This message appear in the NAT_ISP_side trace file at 6.069168 time and the Source IP address is “71.192.34.104” with port “4335” and Destination IP address “64.233.169.106” with port “80” according to the screenshot below. Only the source IP address has changed from the answer to the question 3 above.



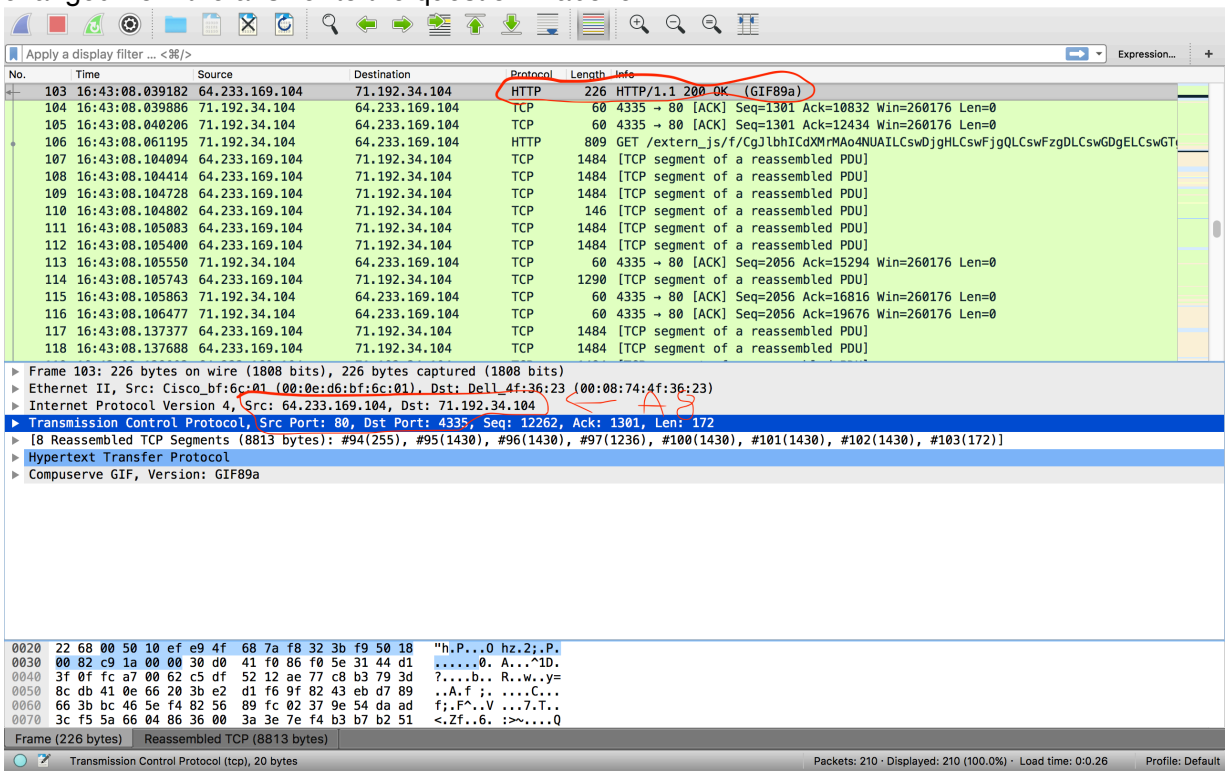
7. Are any fields in the HTTP GET message changed? Which of the following fields in the IP datagram carrying the HTTP GET are changed: Version, Header Length, Flags, Checksum. If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change.

Ans.) None of the HTTP GET message fields are changed. Only the “Checksum” from the given IP datagram fields carrying the HTTP GET is changed, also the source IP address is changed because the checksum includes the value of the source IP address.



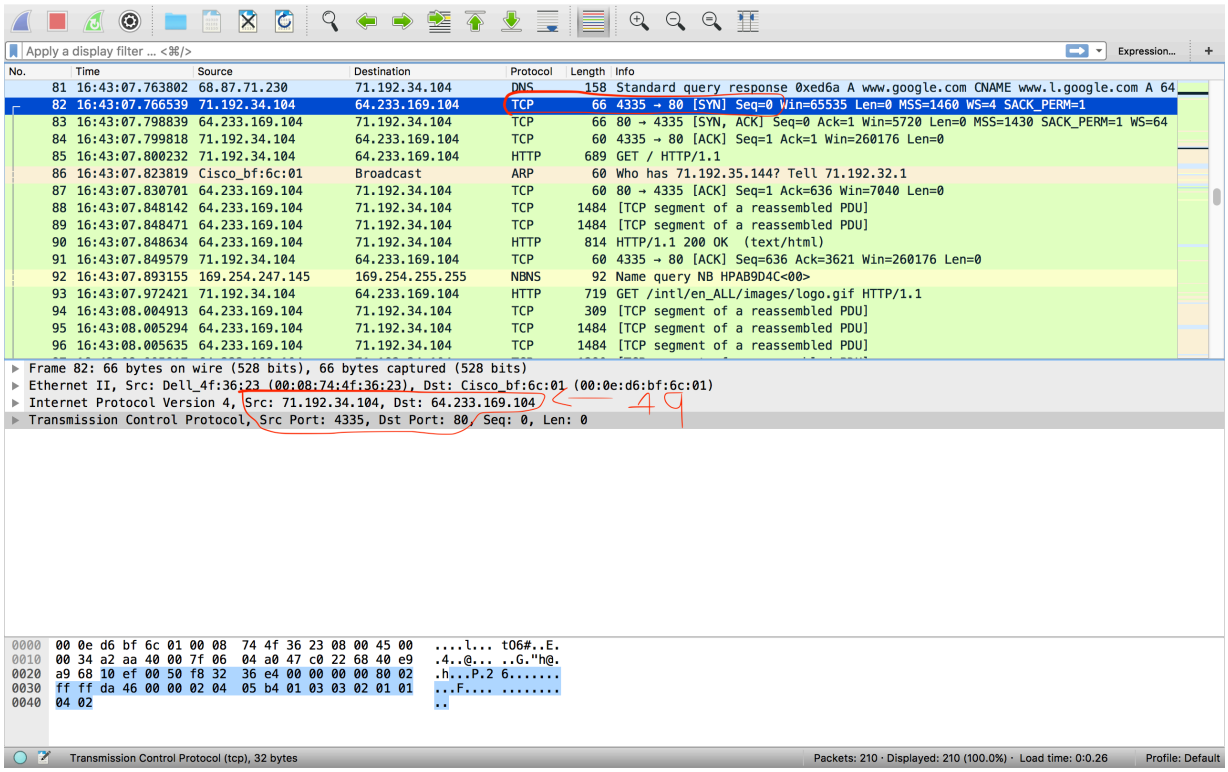
8. In the NAT_ISP_side trace file, at what time is the first 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message? Which of these fields are the same, and which are different than your answer to question 4 above?

Ans.) In the NAT_ISP_side trace file the first 200 OK HTTP message is received from the Google server at 6.308118 time. The source IP address is “64.233.169.106” with port “80” and destination IP address is “71.192.34.104” with port “4335”. Only the destination IP address has changed from the answer to the question 4 above.



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? Figure 4.22 in the text shows the NAT translation table in the NAT router.

Ans.) In the NAT_ISP_side trace file, the client-to-server TCP SYN segment were sent at 6.035475 time and the server-to-client TCP ACK segment were sent at 6.067775 time corresponding to the segments in question 5 above captured. For the SYN the source IP address is “71.192.34.104” and destination IP address is “64.233.169.104” and source port is “4335”and destination port is “80” for these two segments and for the ACK Source IP address is “64.233.169.104” and destination IP address is “71.192.34.104” and source port is “80”and destination port is “4335”. Also for the SYN, the source IP address has changed, and for the ACK, the destination IP address has changed and the port numbers are unchanged.



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 translation table:

WAN side	LAN side
IP address: 71.192.34.104 Port: 4335	IP address: 192.168.1.100 Port: 4335