Wireshark Lab 6

NAT

Suraj Durgesht

(16EC06)

Instructor: Dr. Rajendra Hegadi

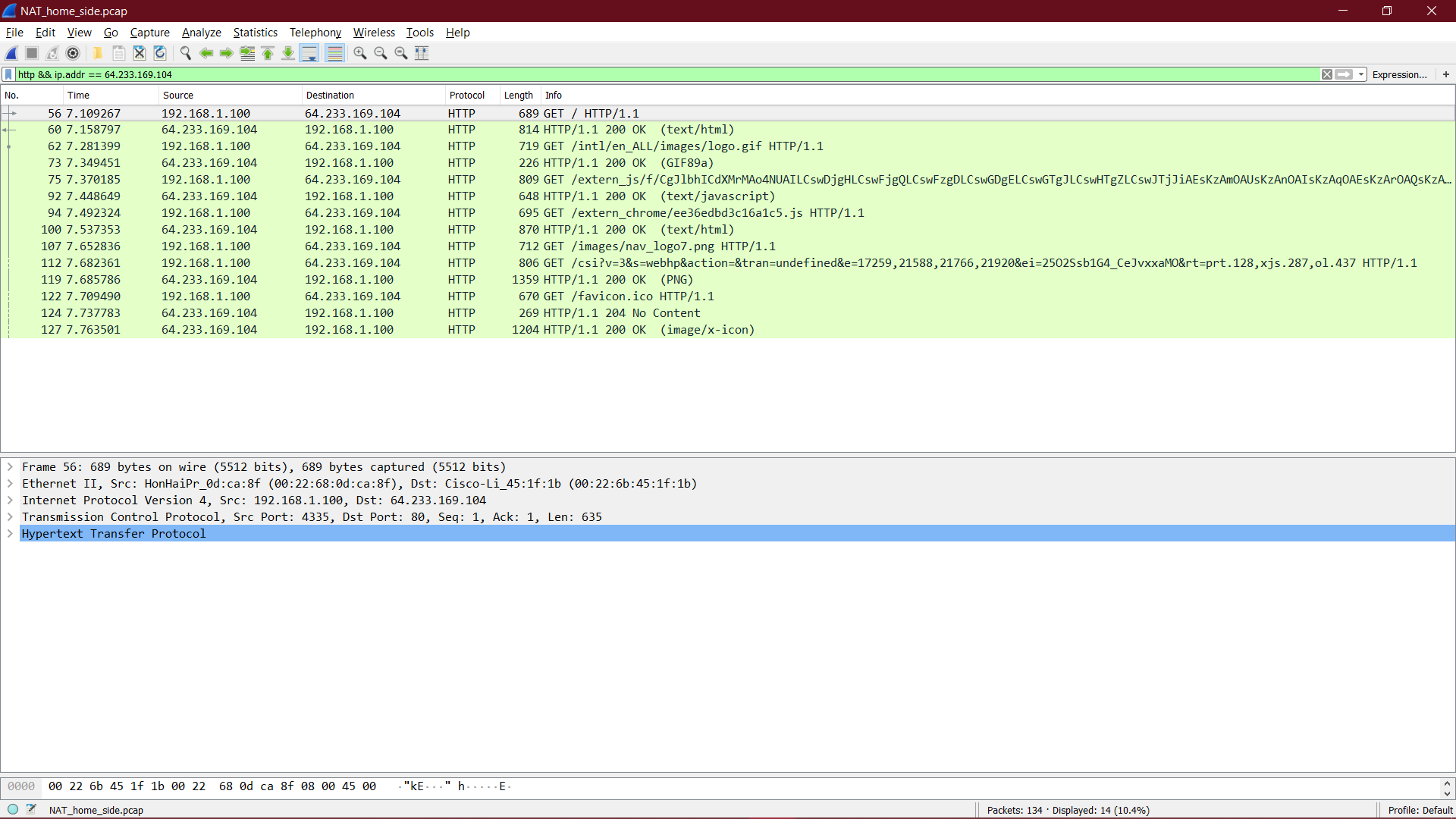
Que1. What is the IP address of the client?

Solution: 192.168.1.100

Que2. The client actually communicates with several different Google servers in order to

implement “safe browsing.”. 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” into the Filter: field in Wireshark.



Que3. 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?

Solution: Source: 192.168.1.100, 4335 Destination: 64.233.169.104, 80

Que4. At what time4 is the corresponding 200 OK HTTP message received from the Google server? What is the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

Solution: 7.158798; Source: 64.233.169.104,80; Destination: 192.168.1.100, 4335

Que5. 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).

Solution: -> 7.075657,

->Source: 192.168.1.100, 4335 Destination: 64.233.169.104, 80,

->Source: 64.233.169.104,80 Destination:192.168.1.100, 4335,

->7.108986.

Que6. 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 appears 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

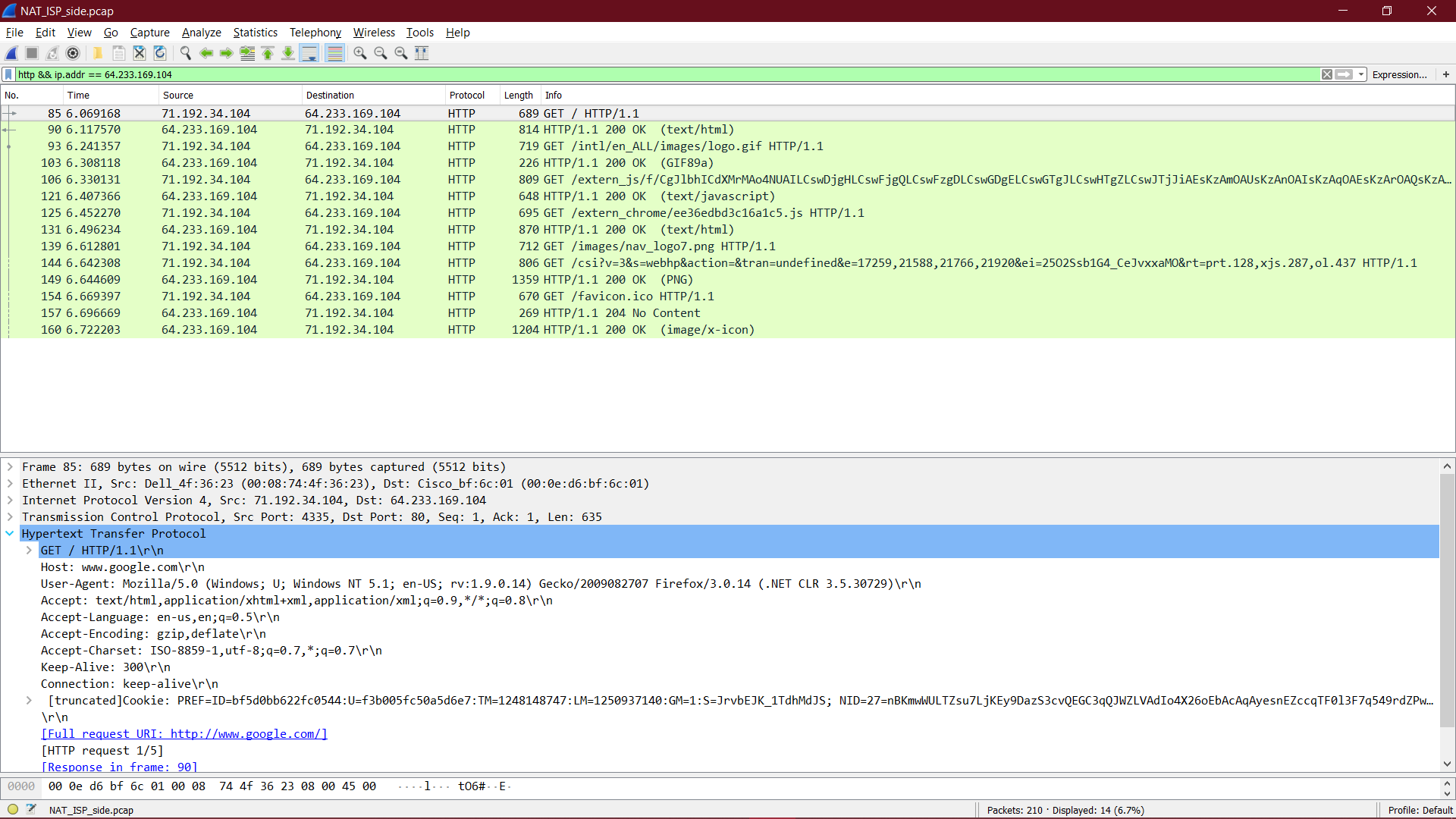
of these fields are the same, and which are different, than in your answer to

question 3 above?

Solution: -> 6.069168,

->Source: 71.192.34.104, 4335 Destination: 64.233.169.104,80,

->only the source IP address has changed.



Que7. Are any fields in the HTTP GET message changed?

sol: No

Which of the following fields in the IP datagram carrying the HTTP GET are changed: Version,

sol: No

Header Length,

sol: No

Flags,

sol: No

Checksum

sol: Yes

If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change.

Solution: Since the IP source address has changed, and the checksum includes the value of the source IP address, the checksum has changed.

Que8. In the NAT\_ISP\_side trace file, at what time is the first 200 OK HTTP message

received from the Google server?

Sol: 6.308118

What is the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

Sol: Source: 64.233.169.104,80; Destination:71.192.34.104, 4335

Which of these fields are the same, and which are different than your answer to question 4 above?

Solution: only the destination IP address has changed.

Que9. 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?

Solution:

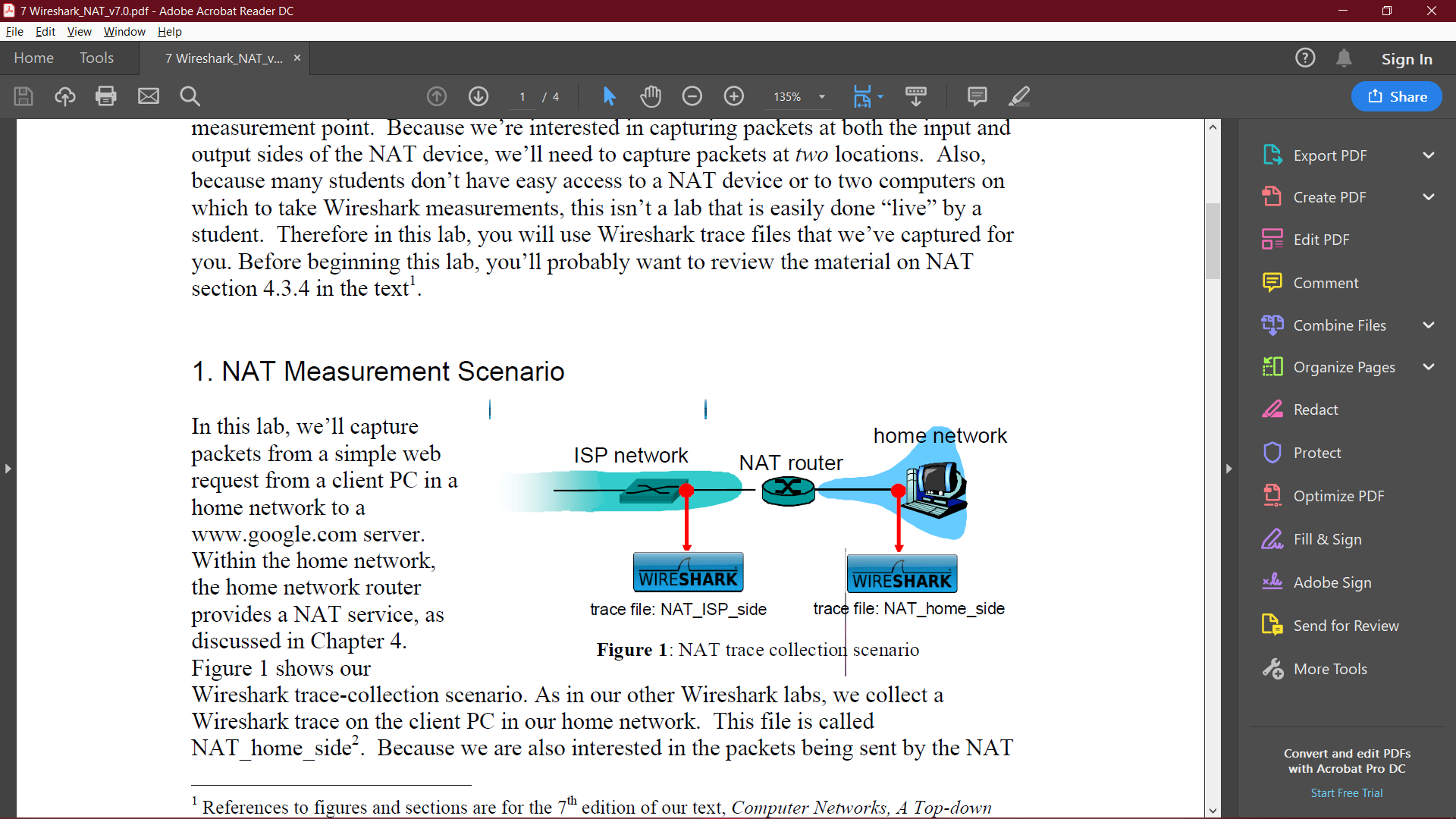
1. .035475, and 6.067775, respectively
2. For the SYN: Source: 71.192.34.104, 4335 Destination: 64.233.169.104, 80. For the ACK: Source: 64.233.169.104, 80 Destination: 71.192.34.104, 4335
3. for the SYN, the source IP address has changed, For the ACK, the destination IP address has changed. The port numbers are unchanged.

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

Que10. Using your answers to 1-8 above, fill in the NAT translation table entries for

HTTP connection considered in questions 1-8 above.

Solution:



NAT translates

Wan Side: 71.192.34.104, 4335

LAN Side: 192.168.1.100, 4335