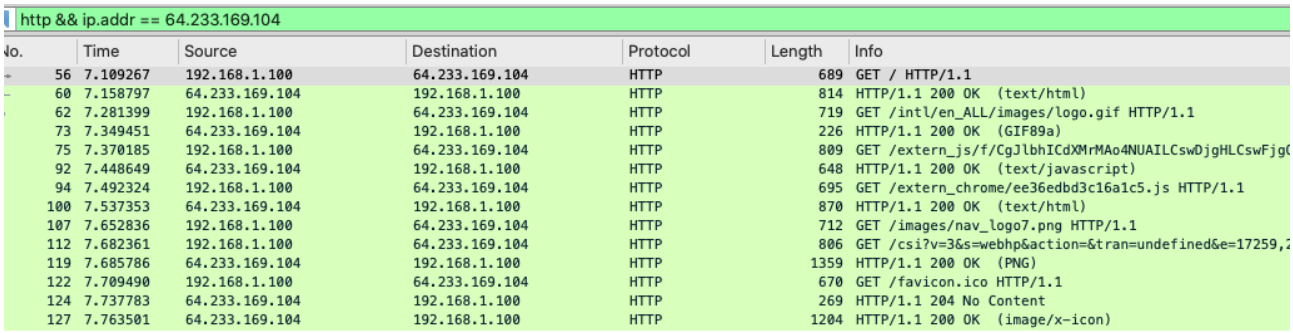
20132927_정재명_HW8_NAT

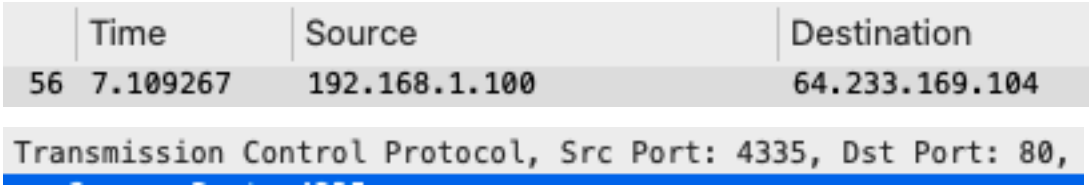
1. What is the IP address of the client?
-> 192.168.1.100

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 : 192.168.1.100. // destination : 64.233.169.104
-> src port : 4335 // Dst port : 80

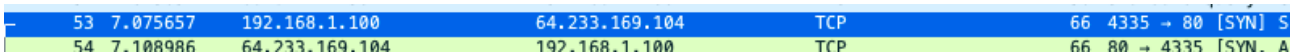


4. At what time is the corresponding 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

-> 7.158797
-> source : 64.233.169.104 // destination : 192.168.1.100.
-> src port : 80 // dest 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?

-> 7.075657

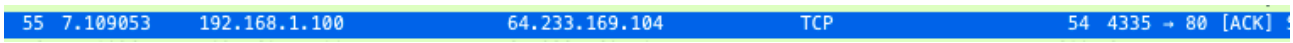


What are the source and destination IP addresses and source and destination ports for the TCP SYN segment?

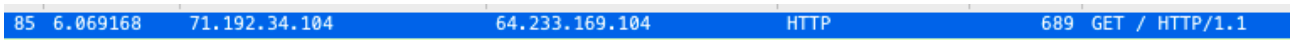
-> source : 192.168.1.100 // destination : 64.233.169.104
-> src port : 4335 // dest port : 80

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).

-> source : 192.168.1.100 // destination : 64.233.169.104
-> src port : 4335 // dest port : 80
-> 7.109053



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?



-> 6.069168

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)?

-> source : 71.192.34.104 // destination : 64.233.169.104
-> src port : 4335 // dest port : 80

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

-> source address가 달라졌다. 나머지는 같다.

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

-> 없다.

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.

-> 체크섬부분만 바뀌었다. 아이피 필드가 바뀌었기 때문에 체크섬도 바뀌어야 한다.

8. In the NAT_ISP_side trace file, at what time is the first 200 OK HTTP message received from the Google server?

-> 6.117570

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

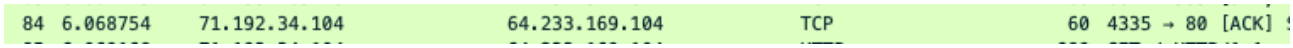
-> source : 64.233.169.104 // destination : 71.192.34.104
-> src port : 80 // dest port : 4335

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

-> destination address 부분만 빼고 나머지는 모두 같다. 4번의 destination address와 달라졌다.

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?

-> the client-to-server TCP SYN segment : 6.035475
-> the server-to-client TCP ACK segment : 6.068754



What are the source and destination IP addresses and source and destination ports for these two segments?

-> source : 71.192.34.104 // destination : 64.233.169.104
-> src port : 4335 // dest port : 80

Which of these fields are the same, and which are different than your answer to question 5 above?

-> source address 부분이 외부 아이피로 바뀌었다.

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	
WAN side	LAN side
71.192.34.104	192.168.1.100