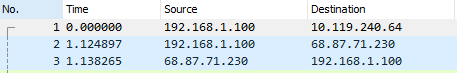
Lab 12 Ques#2

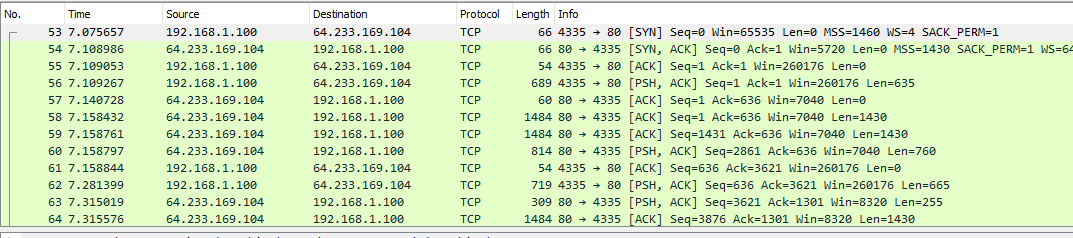
1. What is the IP address of the client?

# The IP address of the client is 192.168.1.100.



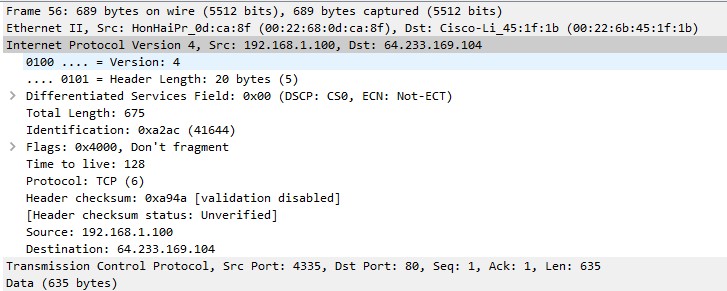
1. The client actually communicates with several different Google servers in order to implement “safe browsing.” (See extra credit section at the end of this lab). The main Google server that will serve up the main Google web page has IP address 64.233.169.104. In order to display only those frames containing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

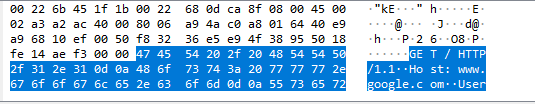
Http && ip.addr == 64.233.169.104 doesn’t return any result but ip.addr == 64.233.169.104 returns result.



1. 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, 4335 Destination: 64.233.169.104, 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?

# Time the corresponding 200 OK HTTP: 7.158432000 seconds Source IP Address: 64.233.169.104, Port: 80 Destination IP Address: 192.168.1.100, Port: 4335



1. 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 Wire shark).

# SYN Time: 7.075657000 seconds SYN Source IP Address: 192.168.1.100, Port: 4335 SYN Destination IP Address: 64.233.169.104, Port: 80

