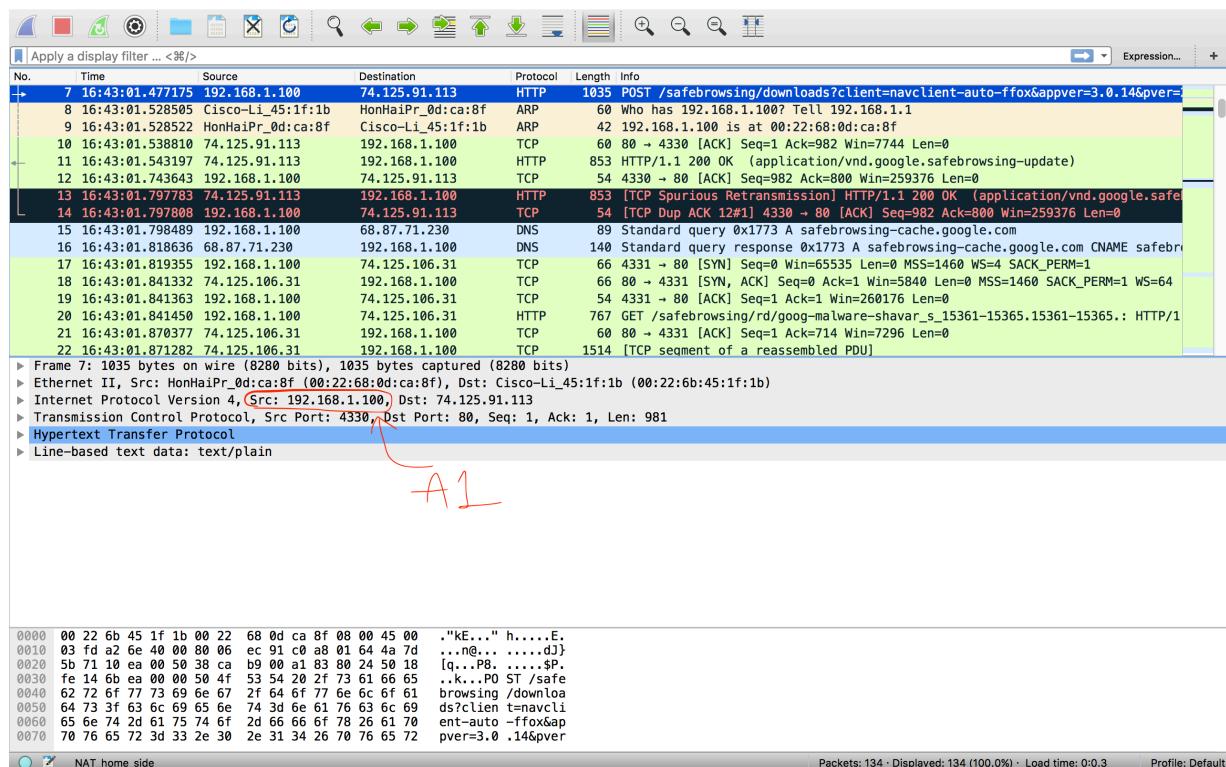


CN Assignment : NAT
BY:
Monil Shah
mds747

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”

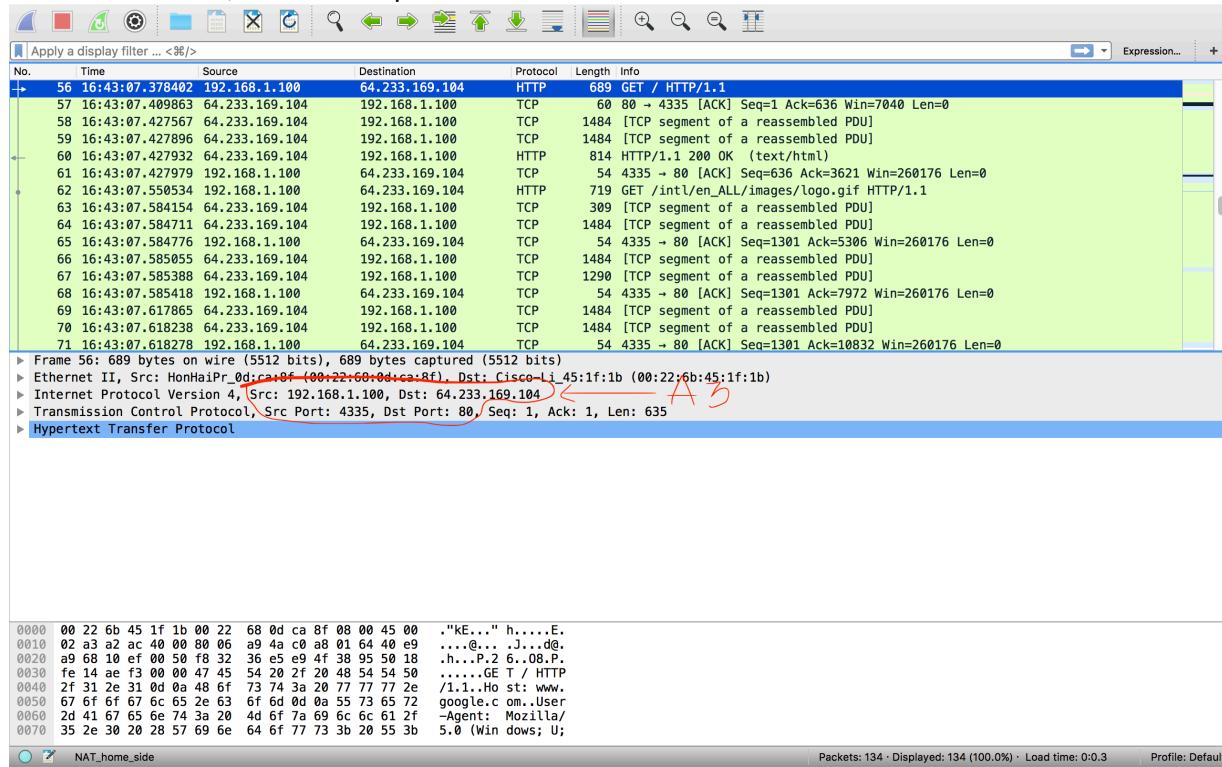


2. The client actually communicates with several different Google servers in order to implement “safe browsing.” (See extra credit section at the end of this lab). The main Google server that will serve up the main Google web page has IP address 64.233.169.104. In order to display only those frames containing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

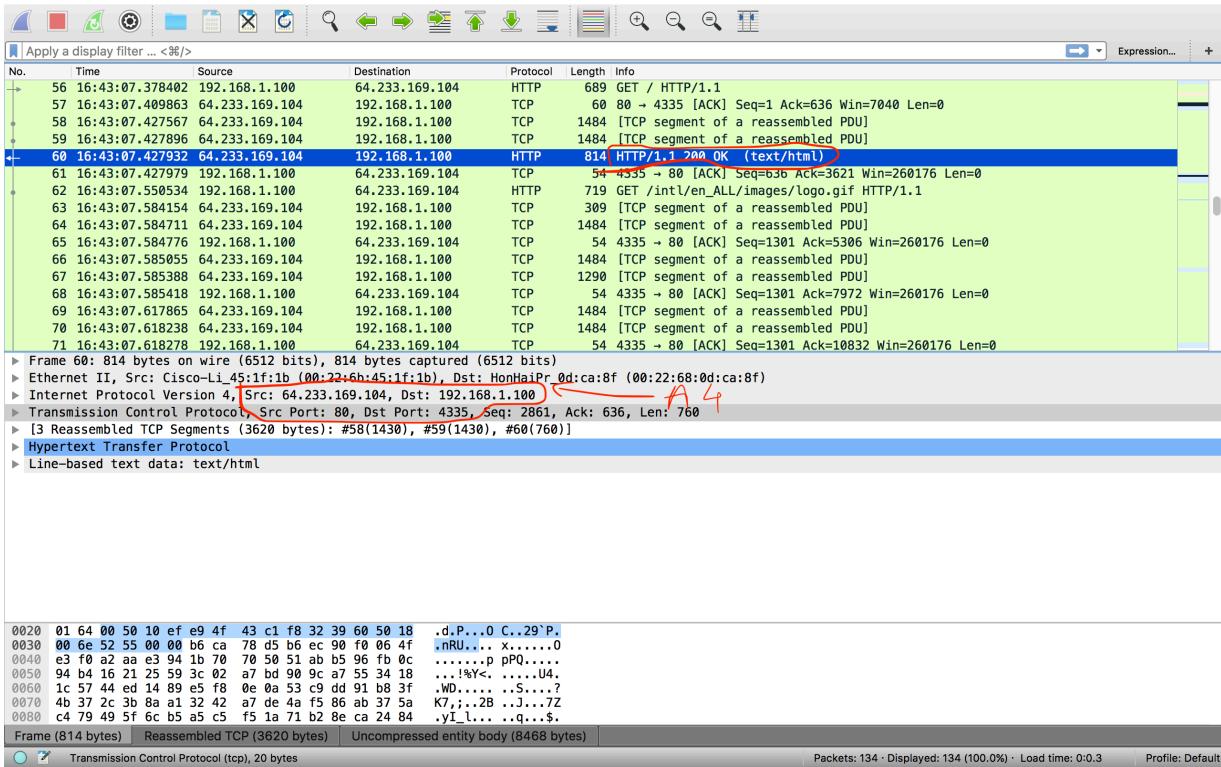
3. Consider now the HTTP GET sent from the client to the Google server (whose IP address is IP address 64.233.169.104) at time 7.109267. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?

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



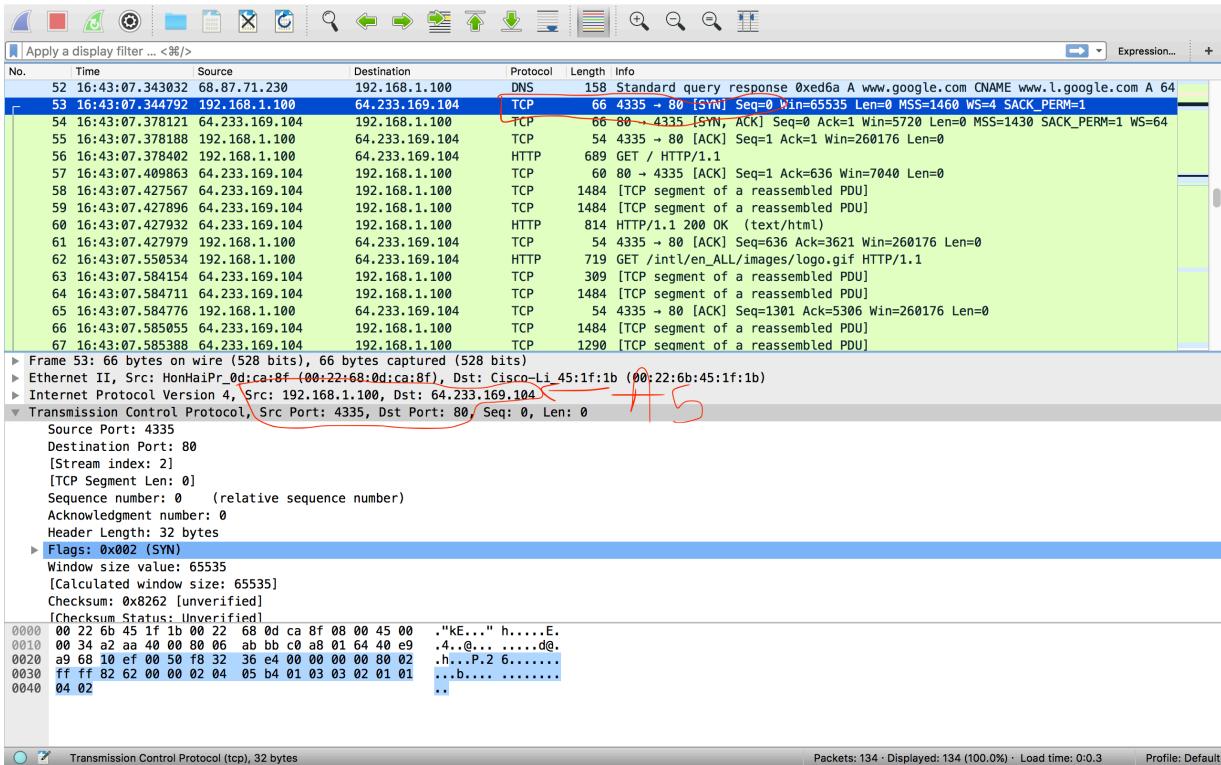
4. At what time is the corresponding 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

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”.



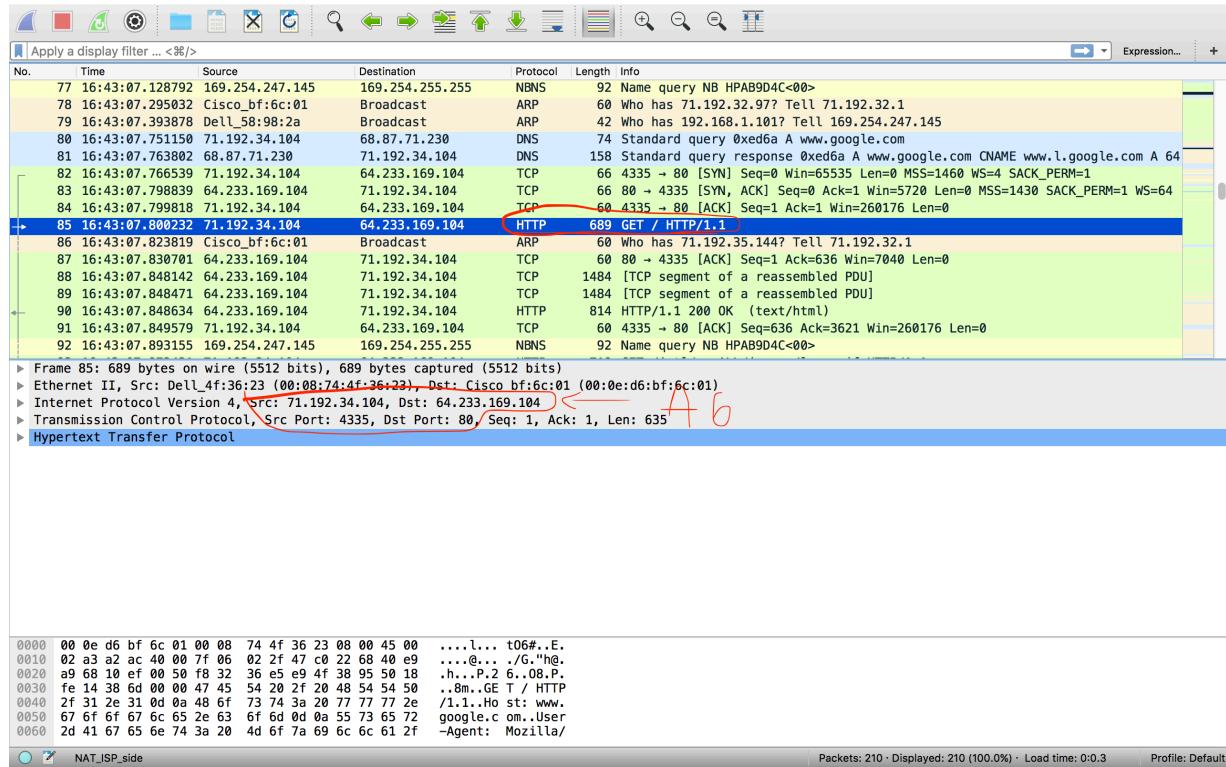
5. Recall that before a GET command can be sent to an HTTP server, TCP must first set up a connection using the three-way SYN/ACK handshake. At what time is the client-to-server TCP SYN segment sent that sets up the connection used by the GET sent at time 7.109267? What are the source and destination 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.

Wireshark Screenshot Analysis:

- Frame 56:** 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)
- Ethernet II, Src: HonHaiPr_0:dca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)**
- Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104**

Packet Details (Frame 56):

- Version:** 4
- Header Length:** 20 bytes (5)
- Differentiated Services Field:** 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length:** 675
- Identification:** 0xa2ac (41644)
- Flags:** 0x02 (Don't Fragment)
- Fragment offset:** 0
- Time to live:** 128
- Protocol:** TCP (6)
- Header checksum:** 0xa94a [validation disabled]

Bytes (Frame 56):

```
0000  00 22 6b 45 1f 1b 00 22 68 0d ca 8f 00 00 45 00 .`K-E... h....E.
0010  02 a3 a2 ac 00 00 80 00 a9 4a c0 a8 01 64 49 e9 .....@... J...@.
0020  a9 68 10 ef 00 50 f8 32 36 e5 e9 4f 38 95 50 18 .h....P2 6...08@.
0030  fe 14 a3 f3 00 00 47 45 54 20 2f 00 48 54 54 50 .....GE T / HTTP
0040  2f 31 2e 31 00 0a 48 6f 73 74 3a 20 77 77 72 ze /1.1.Ho st: www.
0050  67 6f 67 66 65 62 63 6f 6d 0d 0a 55 73 65 72 google.c om.User
0060  2d 41 67 65 66 74 3a 20 4d 6f 7a 69 6c 66 61 2f -Agent: Mozilla/
```

Packets: 134 - Displayed: 134 (100.0%) · Load time: 0:0:0 · Profile: Default

File Statistics:

Size	Kind	
1:18 PM	11 KB	TextEd..ument
3:14 AM	24 KB	TextEd..ument
3:14 AM	4 KB	TextEd..ument
3:14 AM	54 KB	TextEd..ument
3:14 AM	14 KB	TextEd..ument
1:24 PM	7 KB	TextEd..ument
3:28 PM	4 KB	TextEd..ument
3:29 PM	4 KB	TextEd..ument
3:29 PM	7 KB	TextEd..ument
3:29 PM	27 KB	TextEd..ument
3:30 PM	12 KB	TextEd..ument
2:30 PM	2 KB	TextEd..ument
2:48 PM	11 KB	TextEd..ument
9:50 PM	268 KB	TextEd..ument
10:00 PM	80 KB	Pcap N...apture
:56	87 KB	Pcap N...apture
:25 AM	119 KB	Unix e...utable
10:00 AM	181 KB	TextEd..ument
0:13 AM	5 KB	Pcap N...apture
11:20 PM	638 KB	Pcap N...apture
	36.1 MB	ZIP archive
	--	Folder
	13 KB	HTML
	--	Folder
	--	Folder
	134 KB	PNG image
	--	Folder
	--	Folder
	--	Folder
	HW3_MS	Image
	RTFD	Image
	CVHW3_MS	Image
	Moni_Shah_WorkS	Image
	ample	Image

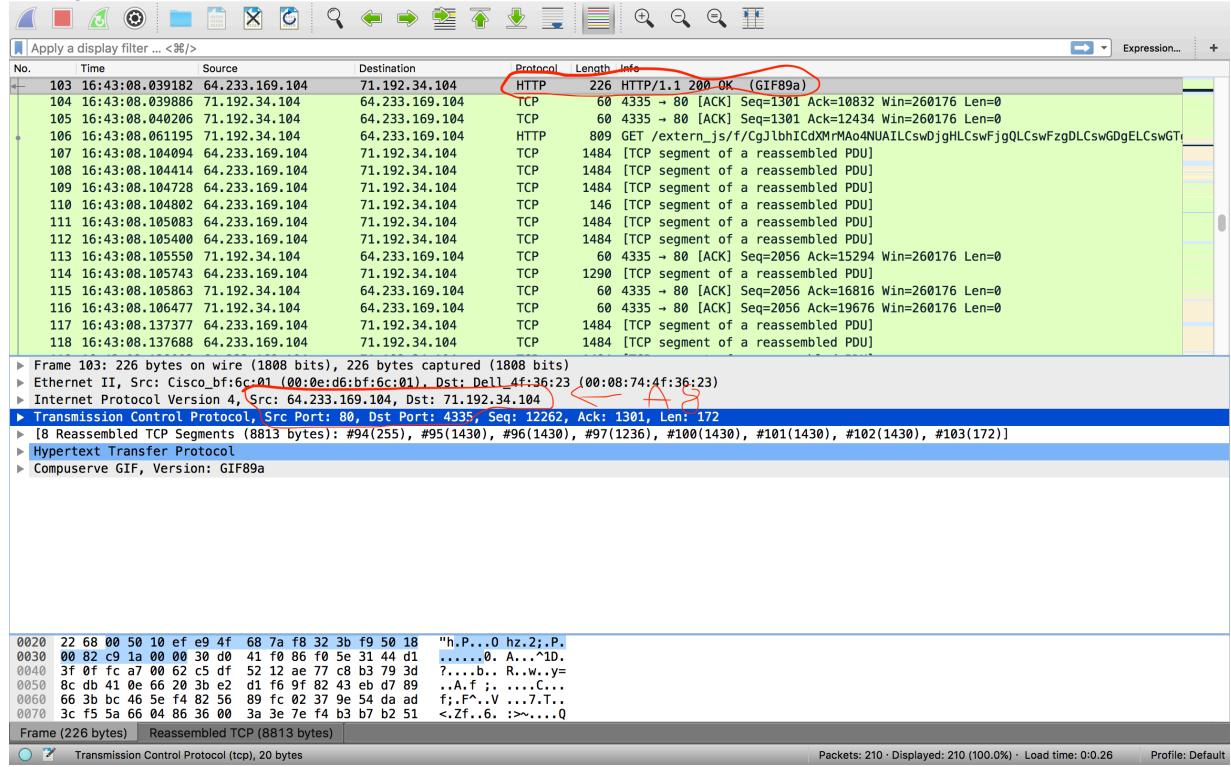
Apply a display filter ... <%>

No.	Time	Source	Destination	Protocol	Length	Info
84	16:43:07.799818	71.192.34.104	64.233.169.104	TCP	60	4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
85	16:43:07.800232	71.192.34.104	64.233.169.104	HTTP	689	GET / HTTP/1.1
86	16:43:07.823819	Cisco_bf:6c:01	Broadcast	ARP	60	Who has 71.192.35.144? Tell 71.192.32.1
87	16:43:07.830701	64.233.169.104	71.192.34.104	TCP	60	80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0
88	16:43:07.848142	64.233.169.104	71.192.34.104	TCP	1484	[TCP segment of a reassembled PDU]
89	16:43:07.848471	64.233.169.104	71.192.34.104	TCP	1484	[TCP segment of a reassembled PDU]
90	16:43:07.848634	64.233.169.104	71.192.34.104	HTTP	814	HTTP/1.1 200 OK (text/html)
91	16:43:07.849579	71.192.34.104	64.233.169.104	TCP	60	4335 → 80 [ACK] Seq=636 Ack=3621 Win=260176 Len=0
92	16:43:07.891535	169.254.247.145	169.254.255.255	NBNS	92	Name query NB HPA89D4C<0>
93	16:43:07.927421	71.192.34.104	64.233.169.104	HTTP	719	GET /int/len_ALL/images/logo.gif HTTP/1.1
94	16:43:08.004913	64.233.169.104	71.192.34.104	TCP	309	[TCP segment of a reassembled PDU]
95	16:43:08.005293	64.233.169.104	71.192.34.104	TCP	1484	[TCP segment of a reassembled PDU]
96	16:43:08.005635	64.233.169.104	71.192.34.104	TCP	1484	[TCP segment of a reassembled PDU]
97	16:43:08.005917	64.233.169.104	71.192.34.104	TCP	1290	[TCP segment of a reassembled PDU]
98	16:43:08.006379	71.192.34.104	64.233.169.104	TCP	60	4335 → 80 [ACK] Seq=1301 Ack=5306 Win=260176 Len=0
99	16:43:08.007029	71.192.34.104	64.233.169.104	TCP	60	4335 → 80 [ACK] Seq=1301 Ack=7972 Win=260176 Len=0
▶	Destination: Cisco_bf:6c:01 (00:0e:0d:b1:6c:01)					
▶	Source: Dell_4f:36:23 (00:08:74:4f:36:23)					
▶	Type: IPv4 (0x0800)					
▼	Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104					
0100 ... = Version: 4						
.... 0010 = Header Length: 20 bytes (5)						
► Differentiated Services Field: 0x00 (DSSCP: CS0, ECN: Not-ECT)						
Total Length: 675						
Identification: 0xa2ac (41644)						
► Flags: 0x02 (Don't Fragment)						
Fragment offset: 0						
Time to live: 127						
Protocol: TCP (6)						
Header checksum: 0x022f [validation disabled]						
[Header checksum status: Unverified]						
Source: 71.192.34.104						
0020 a9 68 10 ef 00 50 f8 32 36 e5 e9 4f 38 95 50 18 .h...P.2 6..08.P.						
0030 fe 14 38 6d 00 47 45 54 20 2f 20 48 54 54 50 ..8m..GE T / HTTP						
0040 2f 31 2c 31 00 48 6f 73 74 3a 20 77 77 72 2e /1.1.Ho st: www.						
0050 67 6f 67 6c 65 6e 63 6f 6d 0d 0a 55 73 65 72 google.c om..User						
0060 2d 41 67 65 66 74 3a 20 4d 6f 7a 69 6c 61 2f ~Agent: Mozilla/						
0070 35 2e 30 28 57 69 6e 64 6f 77 73 3b 20 55 3b 5.0 (Win dows; U;						
0080 28 57 69 6e 64 6f 77 73 20 4e 54 20 35 2e 31 3b Windows NT 5.1;						

Packets: 210 · Displayed: 210 (100.0%) · Load time: 0:0.26 · Profile: Default

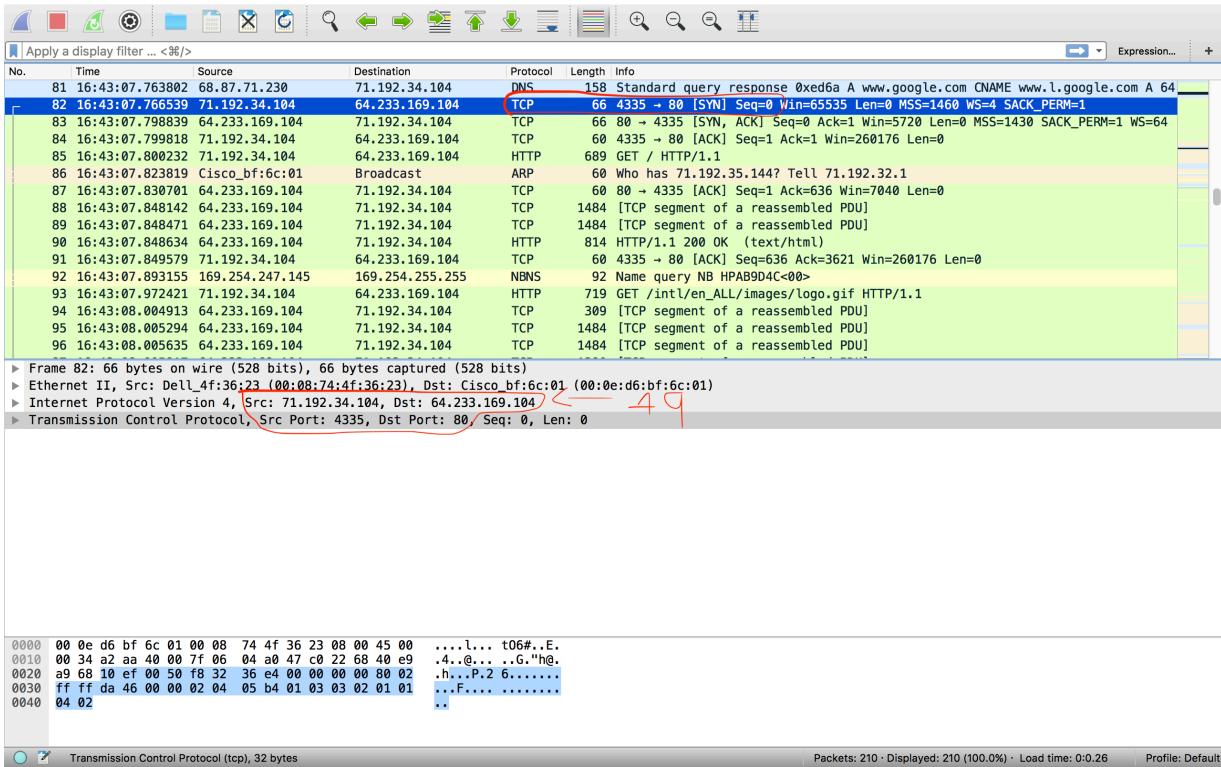
8. In the NAT_ISP_side trace file, at what time is the first 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message? Which of these fields are the same, and which are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

IP address: 71.192.34.104 Port: 4335

LAN side

IP address: 192.168.1.100 Port: 4335