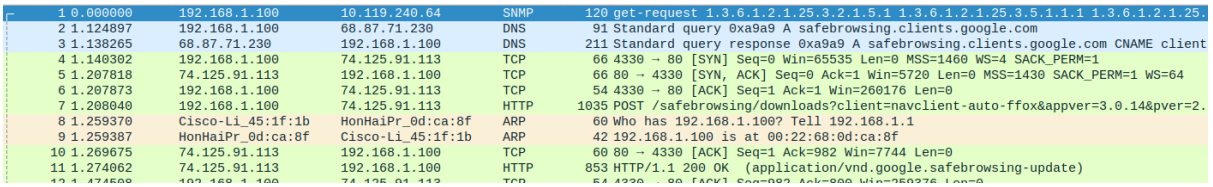
Lab_4c_Wireshark_NAT_v8.0

1. What is the IP address of the client?

Answer:

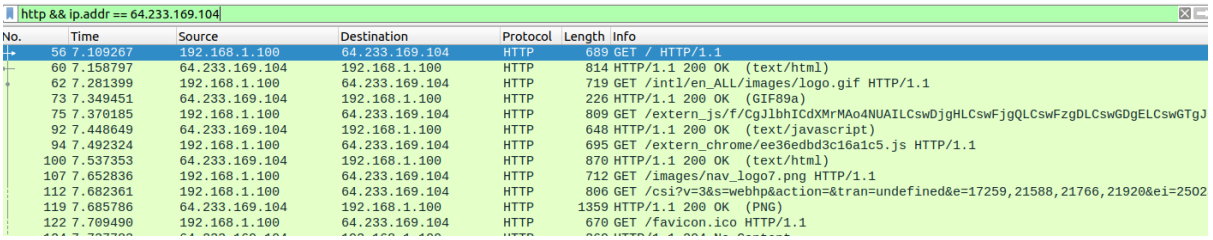


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.100	10.119.240.64	SNMP	120	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.
2	1.124897	192.168.1.100	68.87.71.230	DNS	91	Standard query 0xa9a9 A safebrowsing.clients.google.com
3	1.138265	68.87.71.230	192.168.1.100	DNS	211	Standard query response 0xa9a9 A safebrowsing.clients.google.com CNAME client
4	1.140302	192.168.1.100	74.125.91.113	TCP	66	4330 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
5	1.207818	74.125.91.113	192.168.1.100	TCP	66	80 → 4330 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM=1 WS=64
6	1.207873	192.168.1.100	74.125.91.113	TCP	54	4330 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
7	1.208040	192.168.1.100	74.125.91.113	HTTP	1035	POST /safebrowsing/downloads?client=navclient-auto-ffox&appver=3.0.14&pver=2.
8	1.259370	Cisco-Li_45:1f:1b	HonHaiPr_0d:ca:8f	ARP	60	Who has 192.168.1.100? Tell 192.168.1.1
9	1.259387	HonHaiPr_0d:ca:8f	Cisco-Li_45:1f:1b	ARP	42	192.168.1.100 is at 00:22:68:0d:ca:8f
10	1.269675	74.125.91.113	192.168.1.100	TCP	60	80 → 4330 [ACK] Seq=1 Ack=982 Win=7744 Len=0
11	1.274062	74.125.91.113	192.168.1.100	HTTP	853	HTTP/1.1 200 OK (application/vnd.google.safebrowsing-update)

The IP address of the client 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 .

Answer:

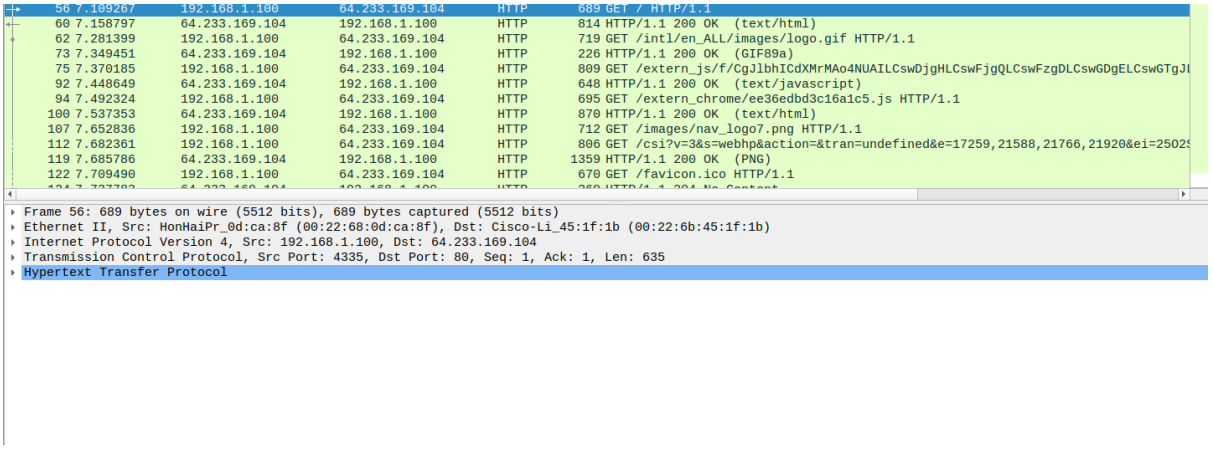


http && ip.addr == 64.233.169.104

No.	Time	Source	Destination	Protocol	Length	Info
56	7.109267	192.168.1.100	64.233.169.104	HTTP	689	GET / HTTP/1.1
60	7.158797	64.233.169.104	192.168.1.100	HTTP	814	HTTP/1.1 200 OK (text/html)
62	7.281399	192.168.1.100	64.233.169.104	HTTP	719	GET /intl/en_ALL/images/logo.gif HTTP/1.1
73	7.349451	64.233.169.104	192.168.1.100	HTTP	226	HTTP/1.1 200 OK (GIF89a)
75	7.370185	192.168.1.100	64.233.169.104	HTTP	809	GET /extern_js/f/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswFzgDLCswGDgELCswGTgJ
92	7.448649	64.233.169.104	192.168.1.100	HTTP	648	HTTP/1.1 200 OK (text/javascript)
94	7.492324	192.168.1.100	64.233.169.104	HTTP	695	GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.1
100	7.537353	64.233.169.104	192.168.1.100	HTTP	870	HTTP/1.1 200 OK (text/html)
107	7.652836	192.168.1.100	64.233.169.104	HTTP	712	GET /images/nav_logo7.png HTTP/1.1
112	7.682361	192.168.1.100	64.233.169.104	HTTP	806	GET /csi?v=3&s=webhp&action=&tran=undefined&e=17259,21588,21766,21920&ei=25O2
119	7.685786	64.233.169.104	192.168.1.100	HTTP	1359	HTTP/1.1 200 OK (PNG)
122	7.709490	192.168.1.100	64.233.169.104	HTTP	670	GET /favicon.ico HTTP/1.1

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?

Answer:



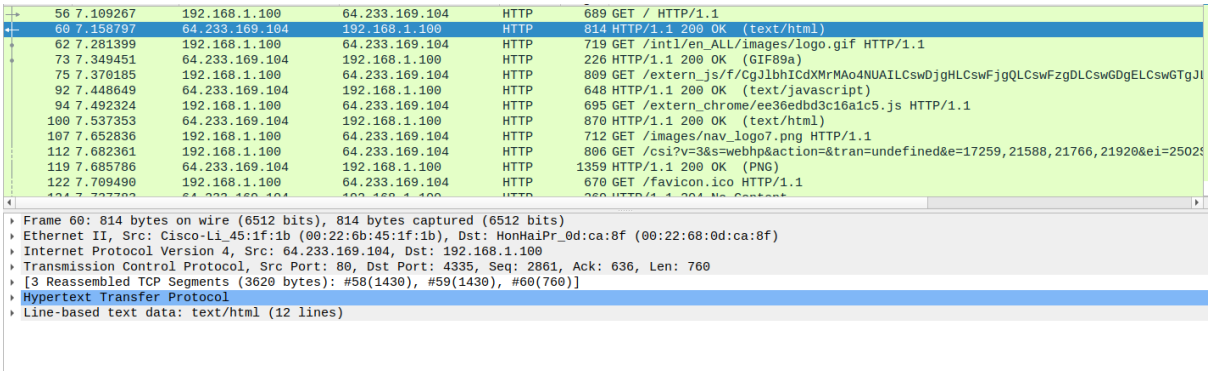
No.	Time	Source	Destination	Protocol	Length	Info
56	7.109267	192.168.1.100	64.233.169.104	HTTP	689	GET / HTTP/1.1
60	7.158797	64.233.169.104	192.168.1.100	HTTP	814	HTTP/1.1 200 OK (text/html)
62	7.281399	192.168.1.100	64.233.169.104	HTTP	719	GET /intl/en_ALL/images/logo.gif HTTP/1.1
73	7.349451	64.233.169.104	192.168.1.100	HTTP	226	HTTP/1.1 200 OK (GIF89a)
75	7.370185	192.168.1.100	64.233.169.104	HTTP	809	GET /extern_js/f/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswFzgDLCswGDgELCswGTgJ
92	7.448649	64.233.169.104	192.168.1.100	HTTP	648	HTTP/1.1 200 OK (text/javascript)
94	7.492324	192.168.1.100	64.233.169.104	HTTP	695	GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.1
100	7.537353	64.233.169.104	192.168.1.100	HTTP	870	HTTP/1.1 200 OK (text/html)
107	7.652836	192.168.1.100	64.233.169.104	HTTP	712	GET /images/nav_logo7.png HTTP/1.1
112	7.682361	192.168.1.100	64.233.169.104	HTTP	806	GET /csi?v=3&s=webhp&action=&tran=undefined&e=17259,21588,21766,21920&ei=25O2
119	7.685786	64.233.169.104	192.168.1.100	HTTP	1359	HTTP/1.1 200 OK (PNG)
122	7.709490	192.168.1.100	64.233.169.104	HTTP	670	GET /favicon.ico HTTP/1.1

```
Frame 56: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)
Ethernet II, Src: HonHaiPr_0d:ca: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
Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
Hypertext Transfer Protocol
```

- Source IP: 192.168.1.100, Source port: 4335
- Destination IP: 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?

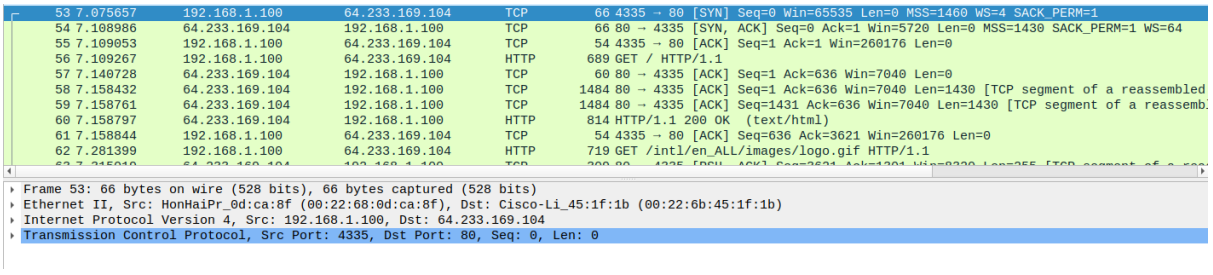
Answer:



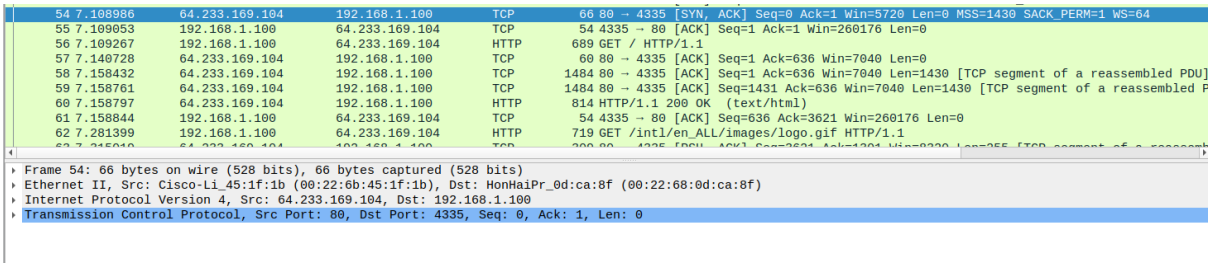
- Time: 7.15797
- Source IP: 64.233.169.104, Source port: 80
- Destination IP: 192.168.1.100, Destination port: 4335

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).

Answer:



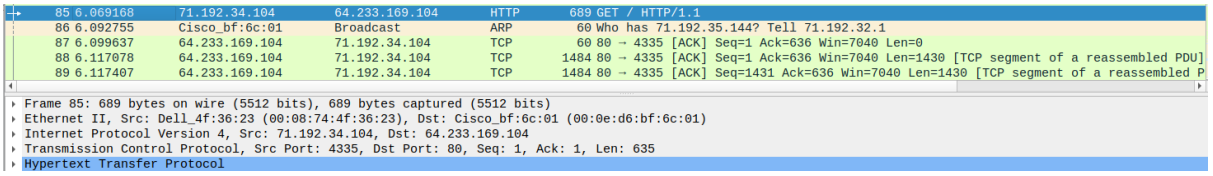
- SYN time: 7.075657
- SYN Source IP: 192.168.1.100, SYN Source port: 4335
- SYN Destination IP: 64.233.169.104, SYN Destination port: 80



- ACK time: 7.108986
- ACK Source IP: 64.233.169.104, ACK Source port:80
- ACK Destination IP: 192.168.1.100, ACK Destination port: 4335

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?

Answer:



- Time: 6.069168
- Source IP: 71.192.34.104, Source port: 4335
- Destination IP: 64.233.169.104, Destination port: 80
- Only source IP address has changed (192.168.1.100 vs 71.192.34.104)

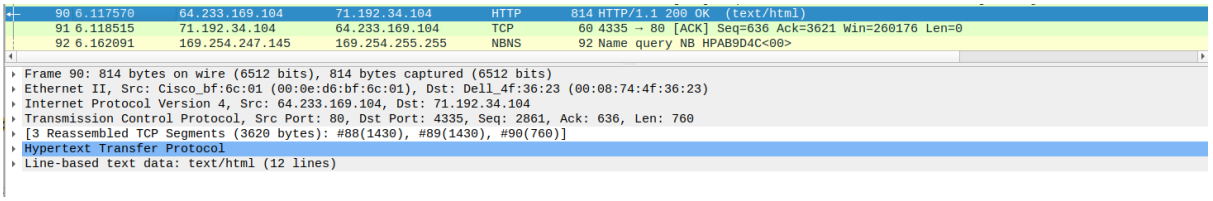
7. Are any fields in the HTTP GET message changed? Which of the following fields in the IP datagram carrying the HTTP GET are changed: Version, Header Length, Flags, Checksum. If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change.

Answer:

- GET message was no changed
- Only the Checksum was changed because the source IP was changed (see the question 6 above)

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?

Answer:

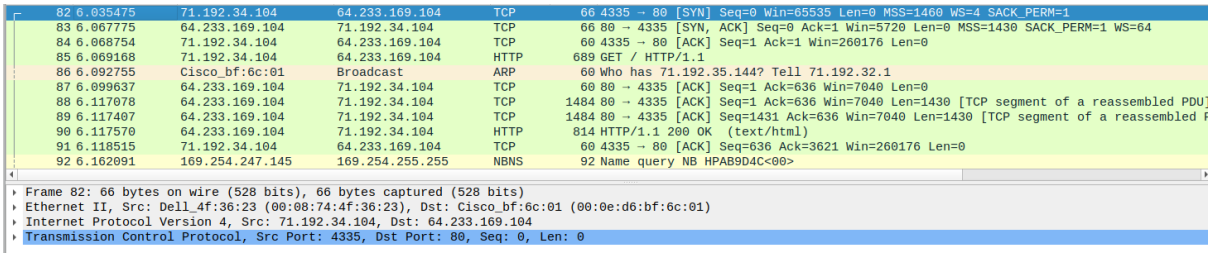


- Time: 6.117570
- Source IP: 64.233.169.104, Source port: 80
- Destination IP: 71.192.34.104, Destination port: 4335
- Only the destination IP address has changed (71.192.34.104 vs 192.168.1.100)

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?

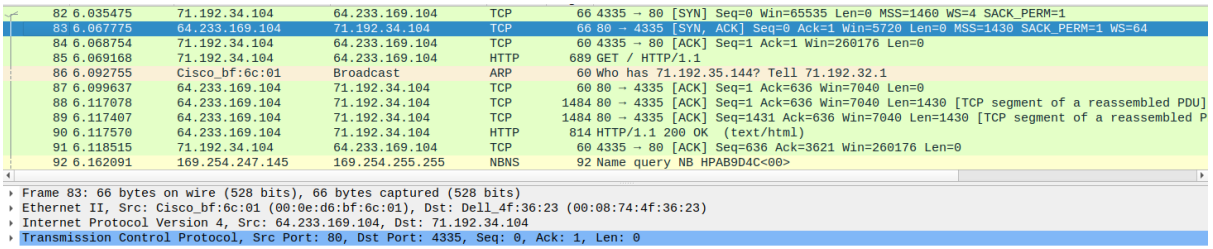
Answer:

TCP SYN:



- Time: 6.03475
- Source IP: 71.192.34.104, Source port:4335
- Destination IP: 64.233.169.104, Destination port: 80

TCP ACK:



- Time: 6.067775
- Source IP: 64.233.169.104, Source port: 80
- Destination IP: 71.192.34.104, Destination port: 4335

Different:

- In TCP SYN: the source IP address has changed (71.192.34.104 vs 192.168.1.100)

- In TCP ACK: the destination IP address has changed (71.192.34.104 vs 192.168.1.100)

10. Using your answers to 1-8 above, fill in the NAT translation table entries for HTTP connection considered in questions 1-8 above

Answer:

	NAT_home_side	NAT_ISP_side
IP	192.168.1.100	71.192.34.104

Only the IP is different.