Computer Networks 1

Lab 4c

Wireshark Lab: NAT v8.0

Student Name: **Nguyễn Quý Hải**

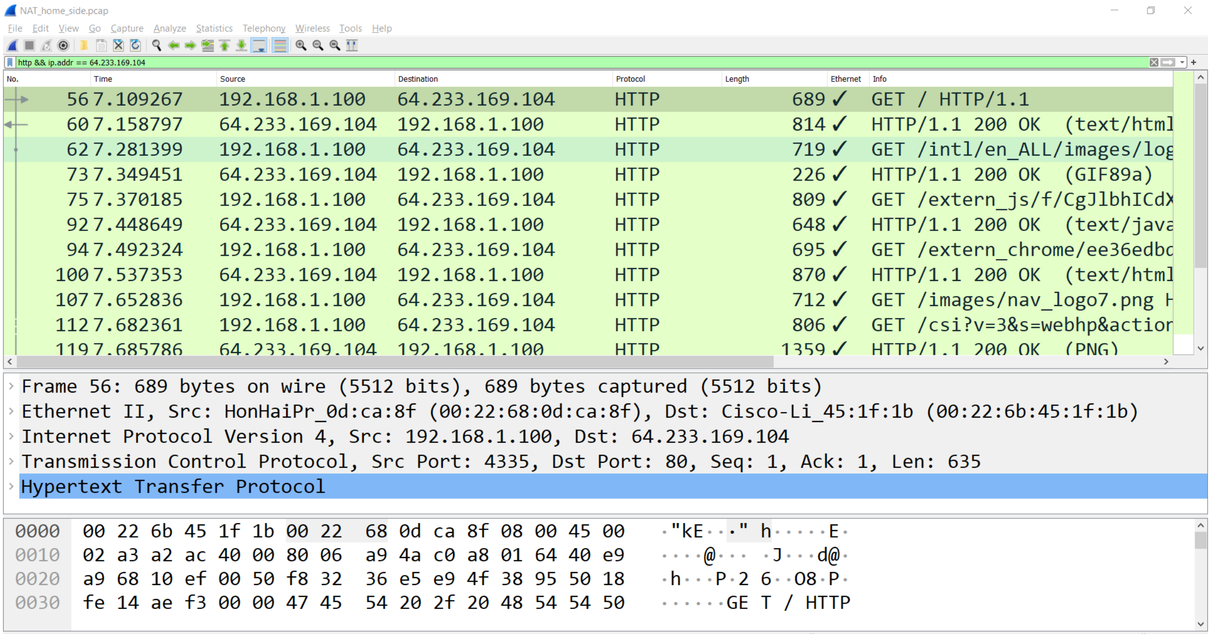
Student No.: **2052974**

- Q1: What is the IP address of the client?

  Answer: 192.168.1.100

- Q2. 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:


NAT_home_side.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http && ip.addr == 64.233.169.104
```

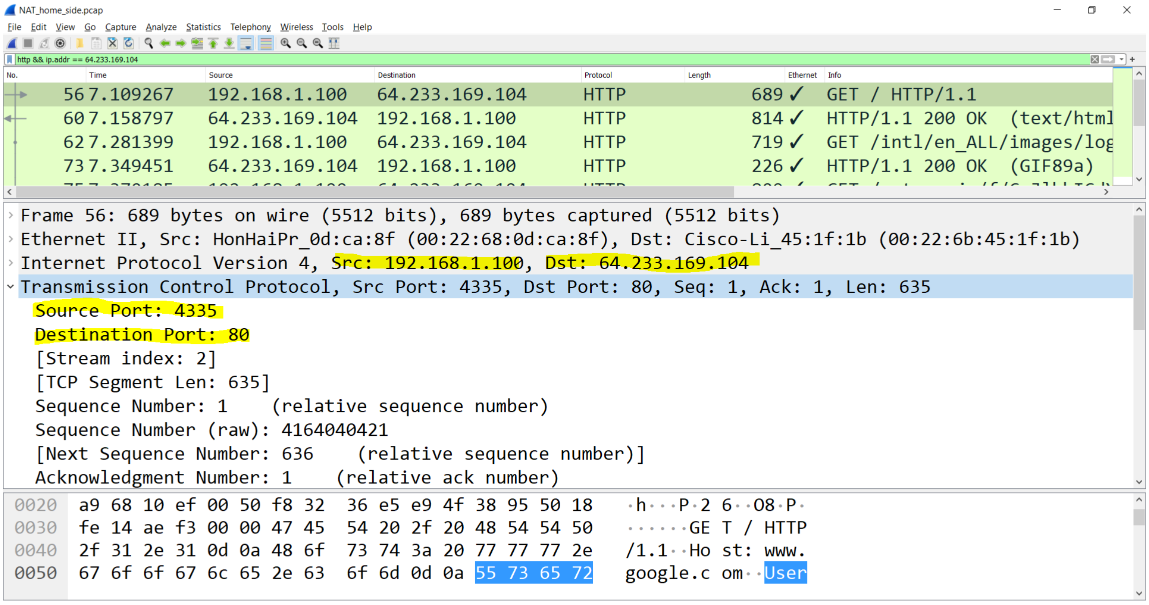
```
No.   Time       Source          Destination     Protocol  Length  Ethernet  Info
 56   7.109267   192.168.1.100   64.233.169.104  HTTP         689  ✓  GET / HTTP/1.1
 60   7.158797   64.233.169.104  192.168.1.100   HTTP         814  ✓  HTTP/1.1 200 OK  (text/html
 62   7.281399   192.168.1.100   64.233.169.104  HTTP         719  ✓  GET /intl/en_ALL/images/log
 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/CgJlbhICdX
 92   7.448649   64.233.169.104  192.168.1.100   HTTP         648  ✓  HTTP/1.1 200 OK  (text/java
 94   7.492324   192.168.1.100   64.233.169.104  HTTP         695  ✓  GET /extern_chrome/ee36edbc
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 H
112   7.682361   192.168.1.100   64.233.169.104  HTTP         806  ✓  GET /csi?v=3&s=webhp&action
119   7.685786   64.233.169.104  192.168.1.100   HTTP        1359  ✓  HTTP/1.1 200 OK  (PNG)
```

```
> 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
```

```
0000  00 22 6b 45 1f 1b 00 22  68 0d ca 8f 08 00 45 00   ·"kE···" h·····E·
0010  02 a3 a2 ac 40 00 80 06  a9 4a c0 a8 01 64 40 e9   ····@···  ·J···d@·
0020  a9 68 10 ef 00 50 f8 32  36 e5 e9 4f 38 95 50 18   ·h···P·2 6··O8·P·
0030  fe 14 ae f3 00 00 47 45  54 20 2f 20 48 54 54 50   ······GE T / HTTP
```

- Q3. 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: Source IP addresses: 192.168.1.100, Destination IP addresses: 64.233.169.104. Source port: 4335, Destination port: 80.


NAT_home_side.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http && ip.addr == 64.233.169.104

No.  Time      Source          Destination     Protocol  Length Ethernet 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/log
73 7.349451   64.233.169.104  192.168.1.100   HTTP        226 ✓  HTTP/1.1 200 OK  (GIF89a)

> 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
v Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
    Source Port: 4335
    Destination Port: 80
    [Stream index: 2]
    [TCP Segment Len: 635]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 4164040421
    [Next Sequence Number: 636    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)

0020  a9 68 10 ef 00 50 f8 32  36 e5 e9 4f 38 95 50 18   ·h···P·2 6··O8·P·
0030  fe 14 ae f3 00 00 47 45  54 20 2f 20 48 54 54 50   ······GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   /1.1··Ho st: www.
0050  67 6f 6f 67 6c 65 2e 63  6f 6d 0d 0a 55 73 65 72   google.c om··User
```

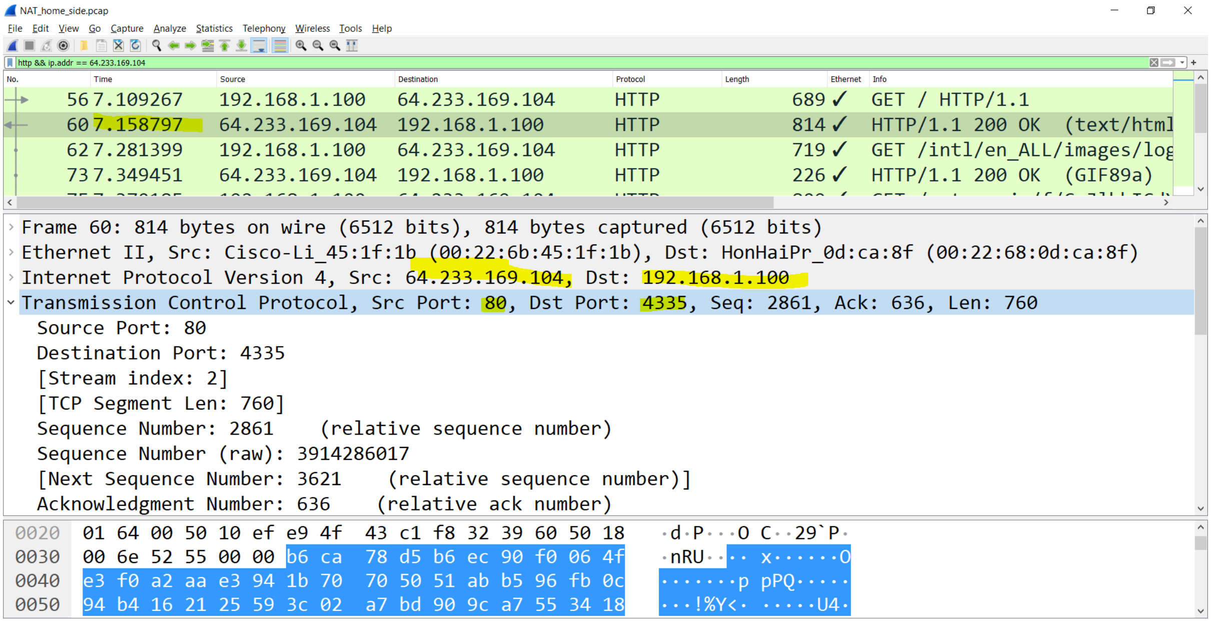
- Q4. At what time is the corresponding 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

Answer:

At the time 7.158798 is the corresponding 200 OK HTTP message received from the Google server.

IP, Src: 64.233.169.104, Dst: 192.168.1.100.

Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 2861, Ack: 636, Len: 760

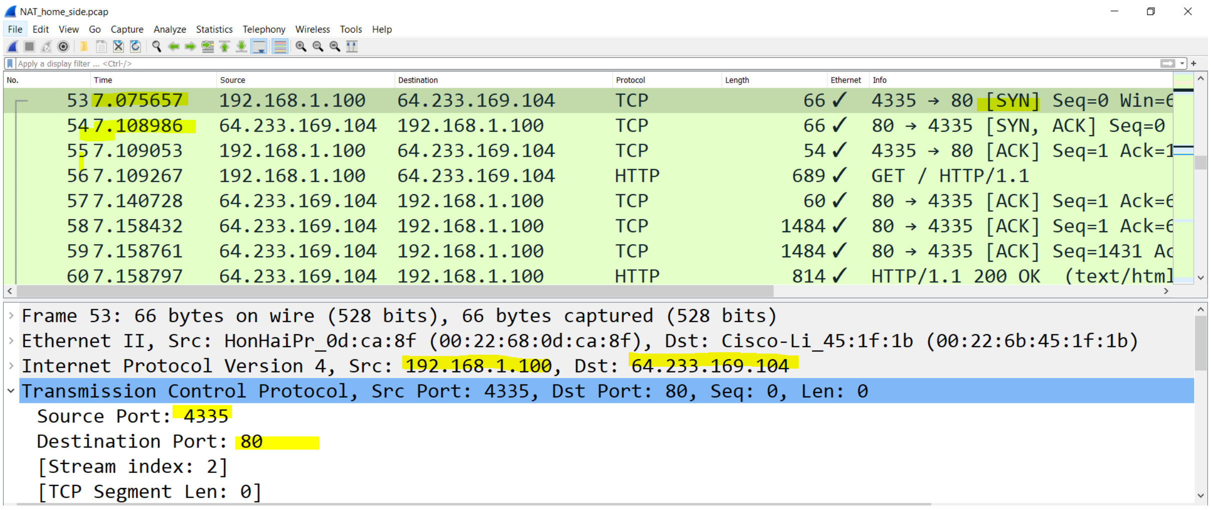

NAT_home_side.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http && ip.addr == 64.233.169.104

No.  Time      Source          Destination     Protocol  Length Ethernet 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/log
73 7.349451   64.233.169.104  192.168.1.100   HTTP        226 ✓  HTTP/1.1 200 OK  (GIF89a)

> Frame 60: 814 bytes on wire (6512 bits), 814 bytes captured (6512 bits)
> Ethernet II, Src: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b), Dst: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f)
> Internet Protocol Version 4, Src: 64.233.169.104, Dst: 192.168.1.100
v Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 2861, Ack: 636, Len: 760
    Source Port: 80
    Destination Port: 4335
    [Stream index: 2]
    [TCP Segment Len: 760]
    Sequence Number: 2861    (relative sequence number)
    Sequence Number (raw): 3914286017
    [Next Sequence Number: 3621    (relative sequence number)]
    Acknowledgment Number: 636    (relative ack number)

0020  01 64 00 50 10 ef e9 4f  43 c1 f8 32 39 60 50 18   ·d·P···O C··29`P·
0030  00 6e 52 55 00 00 b6 ca  78 d5 b6 ec 90 f0 06 4f   ·nRU···· x······O
0040  e3 f0 a2 aa e3 94 1b 70  70 50 51 ab b5 96 fb 0c   ·······p pPQ·····
0050  94 b4 16 21 25 59 3c 02  a7 bd 90 9c a7 55 34 18   ···!%Y<· ·····U4·
```

- Q5. 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:

  - At 7.075657, the client-to-server TCP SYN segment sent that sets up the connection used by the GET sent at time 7.109267.
  - Address: 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
  - At 7.108986, this ACK received at the client

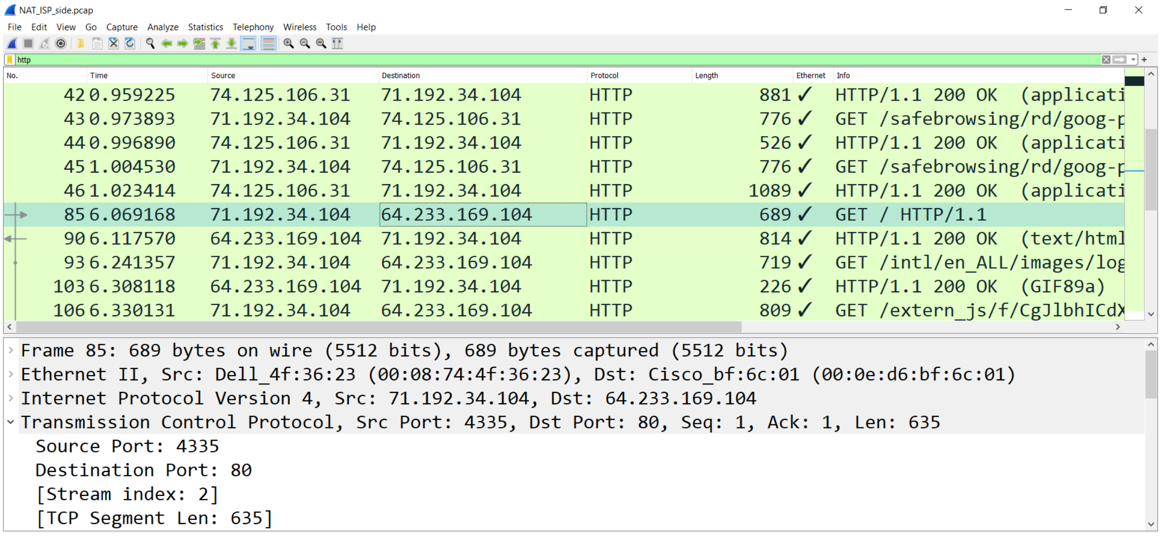

NAT_home_side.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time       Source          Destination     Protocol  Length Ethernet Info
53   7.075657   192.168.1.100   64.233.169.104  TCP           66 ✓  4335 → 80 [SYN] Seq=0 Win=6
54   7.108986   64.233.169.104  192.168.1.100   TCP           66 ✓  80 → 4335 [SYN, ACK] Seq=0
55   7.109053   192.168.1.100   64.233.169.104  TCP           54 ✓  4335 → 80 [ACK] Seq=1 Ack=1
56   7.109267   192.168.1.100   64.233.169.104  HTTP         689 ✓  GET / HTTP/1.1
57   7.140728   64.233.169.104  192.168.1.100   TCP           60 ✓  80 → 4335 [ACK] Seq=1 Ack=6
58   7.158432   64.233.169.104  192.168.1.100   TCP         1484 ✓  80 → 4335 [ACK] Seq=1 Ack=6
59   7.158761   64.233.169.104  192.168.1.100   TCP         1484 ✓  80 → 4335 [ACK] Seq=1431 Ac
60   7.158797   64.233.169.104  192.168.1.100   HTTP         814 ✓  HTTP/1.1 200 OK  (text/html
```

```
> Frame 53: 66 bytes on wire (528 bits), 66 bytes captured (528 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
v Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 4335
    Destination Port: 80
    [Stream index: 2]
    [TCP Segment Len: 0]
```

- Q6: 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: At 6.069168, this message appears in the NAT_ISP_side trace file. Source: 71.192.34.104, 4335 Destination: 64.233.169.104, 80. Only Source IP address has been changed compared to Q3.


NAT_ISP_side.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

No.	Time	Source	Destination	Protocol	Length	Ethernet	Info
42	0.959225	74.125.106.31	71.192.34.104	HTTP	881	✓	HTTP/1.1 200 OK (applicati
43	0.973893	71.192.34.104	74.125.106.31	HTTP	776	✓	GET /safebrowsing/rd/goog-p
44	0.996890	74.125.106.31	71.192.34.104	HTTP	526	✓	HTTP/1.1 200 OK (applicati
45	1.004530	71.192.34.104	74.125.106.31	HTTP	776	✓	GET /safebrowsing/rd/goog-p
46	1.023414	74.125.106.31	71.192.34.104	HTTP	1089	✓	HTTP/1.1 200 OK (applicati
85	6.069168	71.192.34.104	64.233.169.104	HTTP	689	✓	GET / HTTP/1.1
90	6.117570	64.233.169.104	71.192.34.104	HTTP	814	✓	HTTP/1.1 200 OK (text/html
93	6.241357	71.192.34.104	64.233.169.104	HTTP	719	✓	GET /intl/en_ALL/images/log
103	6.308118	64.233.169.104	71.192.34.104	HTTP	226	✓	HTTP/1.1 200 OK (GIF89a)
106	6.330131	71.192.34.104	64.233.169.104	HTTP	809	✓	GET /extern_js/f/CgJlbhICdX

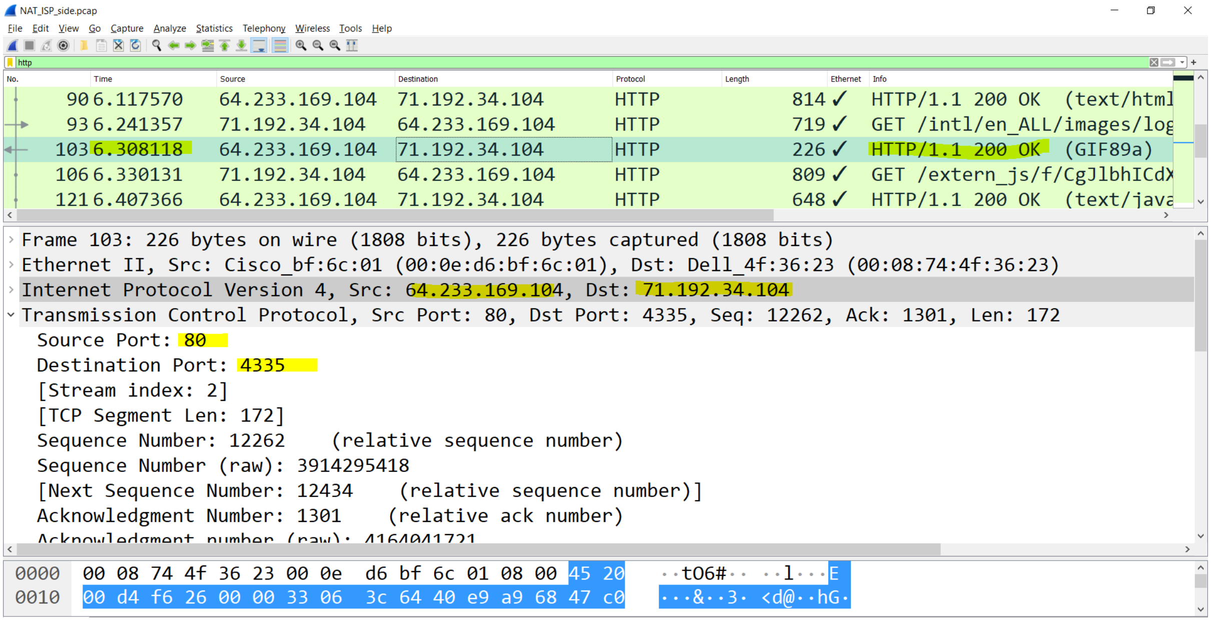
```
› Frame 85: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)
› Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01)
› Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104
˅ Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
    Source Port: 4335
    Destination Port: 80
    [Stream index: 2]
    [TCP Segment Len: 635]
```

- Q7. 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: There are no fields in HTTP GET message changed. Only the Checksum field is changed. The reason for the checksum change is that the IP source address has changed => content changed.

- Q8. 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 from your answer to question 4 above?

  Answer: At 6.308118, the first 200 OK HTTP message received from the Google server. Source: 64.233.169.104, 80. Destination: 71.192.34.104, 4335. Only the destination IP address has changed compared to Q4.



NAT_ISP_side.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time      Source          Destination     Protocol  Length Ethernet Info
   90 6.117570  64.233.169.104  71.192.34.104   HTTP         814 ✓  HTTP/1.1 200 OK  (text/html
   93 6.241357  71.192.34.104   64.233.169.104  HTTP         719 ✓  GET /intl/en_ALL/images/log
  103 6.308118  64.233.169.104  71.192.34.104   HTTP         226 ✓  HTTP/1.1 200 OK  (GIF89a)
  106 6.330131  71.192.34.104   64.233.169.104  HTTP         809 ✓  GET /extern_js/f/CgJlbhICdX
  121 6.407366  64.233.169.104  71.192.34.104   HTTP         648 ✓  HTTP/1.1 200 OK  (text/java
```

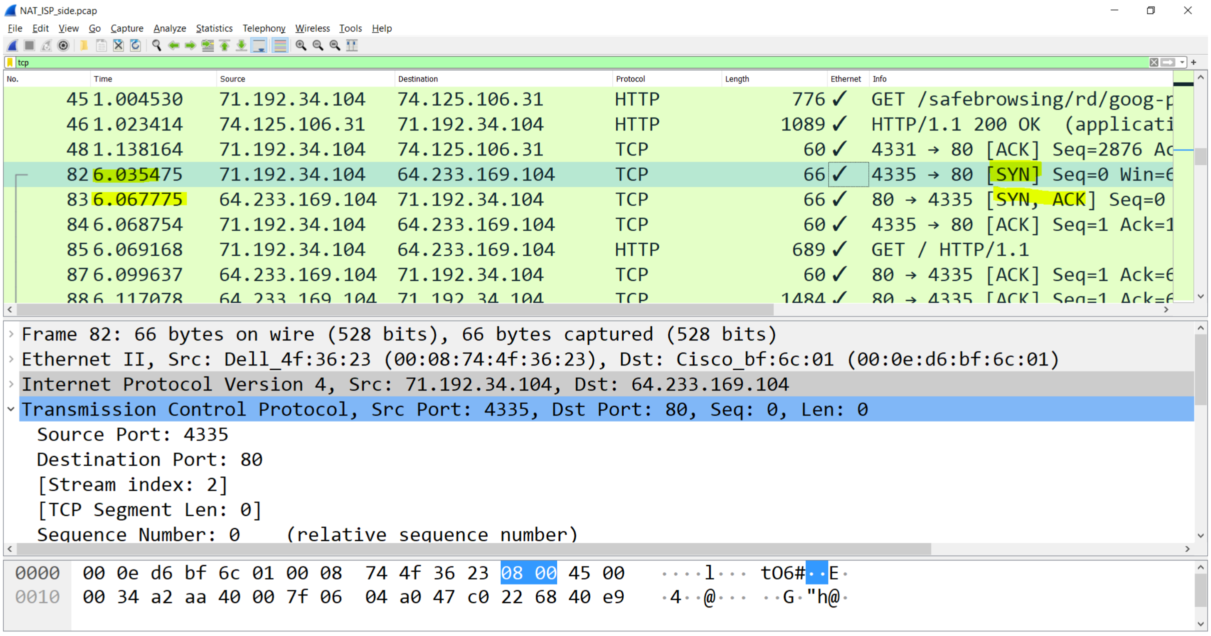
```
> Frame 103: 226 bytes on wire (1808 bits), 226 bytes captured (1808 bits)
> Ethernet II, Src: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
> Internet Protocol Version 4, Src: 64.233.169.104, Dst: 71.192.34.104
v Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 12262, Ack: 1301, Len: 172
    Source Port: 80
    Destination Port: 4335
    [Stream index: 2]
    [TCP Segment Len: 172]
    Sequence Number: 12262    (relative sequence number)
    Sequence Number (raw): 3914295418
    [Next Sequence Number: 12434    (relative sequence number)]
    Acknowledgment Number: 1301    (relative ack number)
    Acknowledgment number (raw): 4164041721
```

```
0000  00 08 74 4f 36 23 00 0e  d6 bf 6c 01 08 00 45 20   ··tO6#··  ··l···E
0010  00 d4 f6 26 00 00 33 06  3c 64 40 e9 a9 68 47 c0   ···&··3·  <d@··hG·
```

- Q9. 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 from your answer to question 5 above?

  Answer: the client-to-server TCP SYN corresponding to the segments in question 5 above were captured at 6.035475, the server-to-client TCP ACK was captured at 6.067775. Compared to question 5, the source IP address for SYN and the destination IP address for ACK have changed.

  - TCP SYN: Source: 71.192.34.104, 4335 . Destination: 64.233.169.104, 80
  - TCP ACK: Source: 64.233.169.104, 80 . Destination: 71.192.34.104, 4335


NAT_ISP_side.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.  Time      Source          Destination     Protocol  Length Ethernet Info
  45 1.004530  71.192.34.104   74.125.106.31   HTTP        776 ✓  GET /safebrowsing/rd/goog-p
  46 1.023414  74.125.106.31   71.192.34.104   HTTP       1089 ✓  HTTP/1.1 200 OK  (applicati
  48 1.138164  71.192.34.104   74.125.106.31   TCP          60 ✓  4331 → 80 [ACK] Seq=2876 Ac
  82 6.035475  71.192.34.104   64.233.169.104  TCP          66 ✓  4335 → 80 [SYN] Seq=0 Win=6
  83 6.067775  64.233.169.104  71.192.34.104   TCP          66 ✓  80 → 4335 [SYN, ACK] Seq=0
  84 6.068754  71.192.34.104   64.233.169.104  TCP          60 ✓  4335 → 80 [ACK] Seq=1 Ack=1
  85 6.069168  71.192.34.104   64.233.169.104  HTTP        689 ✓  GET / HTTP/1.1
  87 6.099637  64.233.169.104  71.192.34.104   TCP          60 ✓  80 → 4335 [ACK] Seq=1 Ack=6
  88 6.117078  64.233.169.104  71.192.34.104   TCP        1484 ✓  80 → 4335 [ACK] Seq=1 Ack=6
```

```
> Frame 82: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01)
> Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104
v Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 4335
    Destination Port: 80
    [Stream index: 2]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
```

```
0000  00 0e d6 bf 6c 01 00 08  74 4f 36 23 08 00 45 00   ····l··· tO6#··E·
0010  00 34 a2 aa 40 00 7f 06  04 a0 47 c0 22 68 40 e9   ·4··@··· ··G·"h@·
```

- Q10: 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 translate table	
WAN side	LAN side
71.192.34.104, 4335	192.168.1.100, 4335