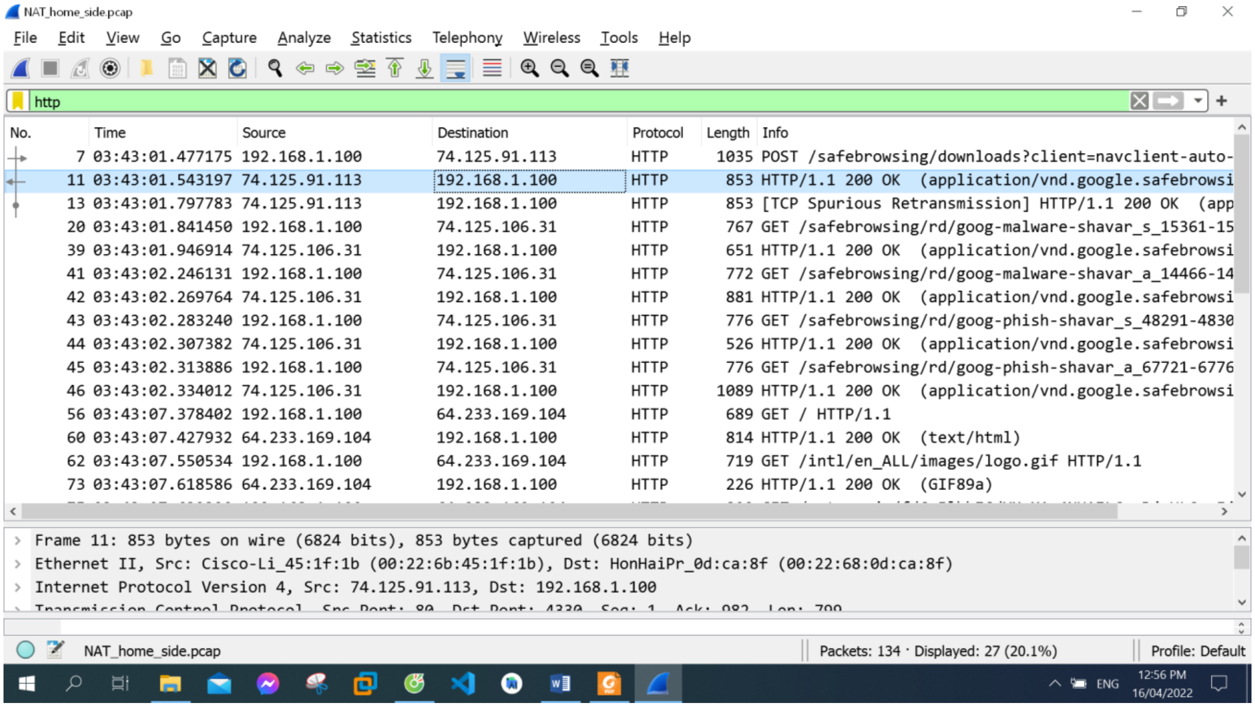
LAB 4C: NAT v8.0

Name: Hồ Đức Trí

Student No: 1912288

1. What is the IP address of the client?



http

No.	Time	Source	Destination	Protocol	Length	Info
7	03:43:01.477175	192.168.1.100	74.125.91.113	HTTP	1035	POST /safebrowsing/downloads?client=navclient-auto-
11	03:43:01.543197	74.125.91.113	192.168.1.100	HTTP	853	HTTP/1.1 200 OK (application/vnd.google.safebrowsi
13	03:43:01.797783	74.125.91.113	192.168.1.100	HTTP	853	[TCP Spurious Retransmission] HTTP/1.1 200 OK (app
20	03:43:01.841450	192.168.1.100	74.125.106.31	HTTP	767	GET /safebrowsing/rd/goog-malware-shavar_s_15361-15
39	03:43:01.946914	74.125.106.31	192.168.1.100	HTTP	651	HTTP/1.1 200 OK (application/vnd.google.safebrowsi
41	03:43:02.246131	192.168.1.100	74.125.106.31	HTTP	772	GET /safebrowsing/rd/goog-malware-shavar_a_14466-14
42	03:43:02.269764	74.125.106.31	192.168.1.100	HTTP	881	HTTP/1.1 200 OK (application/vnd.google.safebrowsi
43	03:43:02.283240	192.168.1.100	74.125.106.31	HTTP	776	GET /safebrowsing/rd/goog-phish-shavar_s_48291-4830
44	03:43:02.307382	74.125.106.31	192.168.1.100	HTTP	526	HTTP/1.1 200 OK (application/vnd.google.safebrowsi
45	03:43:02.313886	192.168.1.100	74.125.106.31	HTTP	776	GET /safebrowsing/rd/goog-phish-shavar_a_67721-6776
46	03:43:02.334012	74.125.106.31	192.168.1.100	HTTP	1089	HTTP/1.1 200 OK (application/vnd.google.safebrowsi
56	03:43:07.378402	192.168.1.100	64.233.169.104	HTTP	689	GET / HTTP/1.1
60	03:43:07.427932	64.233.169.104	192.168.1.100	HTTP	814	HTTP/1.1 200 OK (text/html)
62	03:43:07.550534	192.168.1.100	64.233.169.104	HTTP	719	GET /intl/en_ALL/images/logo.gif HTTP/1.1
73	03:43:07.618586	64.233.169.104	192.168.1.100	HTTP	226	HTTP/1.1 200 OK (GIF89a)

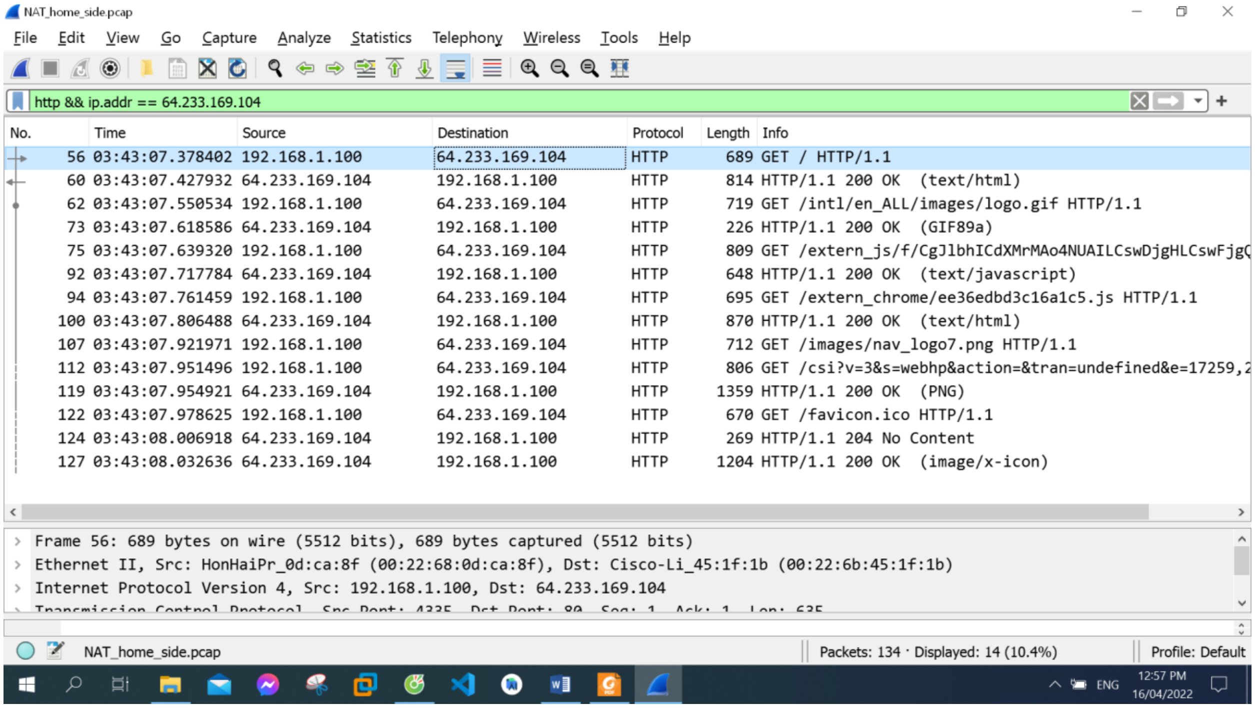
```
> Frame 11: 853 bytes on wire (6824 bits), 853 bytes captured (6824 bits)
> Ethernet II, Src: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b), Dst: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f)
> Internet Protocol Version 4, Src: 74.125.91.113, Dst: 192.168.1.100
> Transmission Control Protocol, Src Port: 80, Dst Port: 4330, Seq: 1, Ack: 982, Len: 799
```

NAT_home_side.pcap | Packets: 134 · Displayed: 27 (20.1%) | Profile: Default

12:56 PM
16/04/2022

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 . .


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

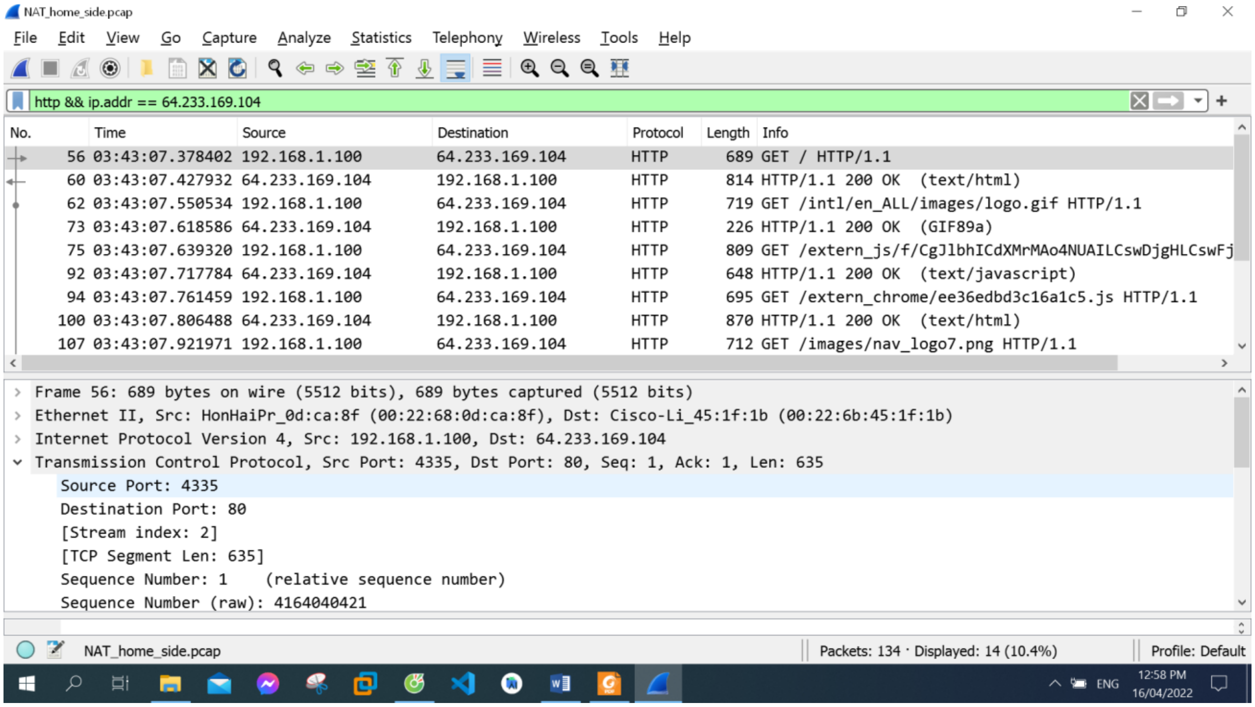
http && ip.addr == 64.233.169.104

```
No.   Time            Source          Destination     Protocol  Length Info
   56 03:43:07.378402 192.168.1.100   64.233.169.104  HTTP        689 GET / HTTP/1.1
   60 03:43:07.427932 64.233.169.104  192.168.1.100   HTTP        814 HTTP/1.1 200 OK  (text/html)
   62 03:43:07.550534 192.168.1.100   64.233.169.104  HTTP        719 GET /intl/en_ALL/images/logo.gif HTTP/1.1
   73 03:43:07.618586 64.233.169.104  192.168.1.100   HTTP        226 HTTP/1.1 200 OK  (GIF89a)
   75 03:43:07.639320 192.168.1.100   64.233.169.104  HTTP        809 GET /extern_js/f/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQ
   92 03:43:07.717784 64.233.169.104  192.168.1.100   HTTP        648 HTTP/1.1 200 OK  (text/javascript)
   94 03:43:07.761459 192.168.1.100   64.233.169.104  HTTP        695 GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.1
  100 03:43:07.806488 64.233.169.104  192.168.1.100   HTTP        870 HTTP/1.1 200 OK  (text/html)
  107 03:43:07.921971 192.168.1.100   64.233.169.104  HTTP        712 GET /images/nav_logo7.png HTTP/1.1
  112 03:43:07.951496 192.168.1.100   64.233.169.104  HTTP        806 GET /csi?v=3&s=webhp&action=&tran=undefined&e=17259,2
  119 03:43:07.954921 64.233.169.104  192.168.1.100   HTTP       1359 HTTP/1.1 200 OK  (PNG)
  122 03:43:07.978625 192.168.1.100   64.233.169.104  HTTP        670 GET /favicon.ico HTTP/1.1
  124 03:43:08.006918 64.233.169.104  192.168.1.100   HTTP        269 HTTP/1.1 204 No Content
  127 03:43:08.032636 64.233.169.104  192.168.1.100   HTTP       1204 HTTP/1.1 200 OK  (image/x-icon)
```

```
> 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
```

NAT_home_side.pcap | Packets: 134 · Displayed: 14 (10.4%) | Profile: Default

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 7.378402. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?


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 Info
   56 03:43:07.378402 192.168.1.100   64.233.169.104  HTTP        689 GET / HTTP/1.1
   60 03:43:07.427932 64.233.169.104  192.168.1.100   HTTP        814 HTTP/1.1 200 OK  (text/html)
   62 03:43:07.550534 192.168.1.100   64.233.169.104  HTTP        719 GET /intl/en_ALL/images/logo.gif HTTP/1.1
   73 03:43:07.618586 64.233.169.104  192.168.1.100   HTTP        226 HTTP/1.1 200 OK  (GIF89a)
   75 03:43:07.639320 192.168.1.100   64.233.169.104  HTTP        809 GET /extern_js/f/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFj
   92 03:43:07.717784 64.233.169.104  192.168.1.100   HTTP        648 HTTP/1.1 200 OK  (text/javascript)
   94 03:43:07.761459 192.168.1.100   64.233.169.104  HTTP        695 GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.1
  100 03:43:07.806488 64.233.169.104  192.168.1.100   HTTP        870 HTTP/1.1 200 OK  (text/html)
  107 03:43:07.921971 192.168.1.100   64.233.169.104  HTTP        712 GET /images/nav_logo7.png 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
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
```

NAT_home_side.pcap | Packets: 134 · Displayed: 14 (10.4%) | Profile: Default

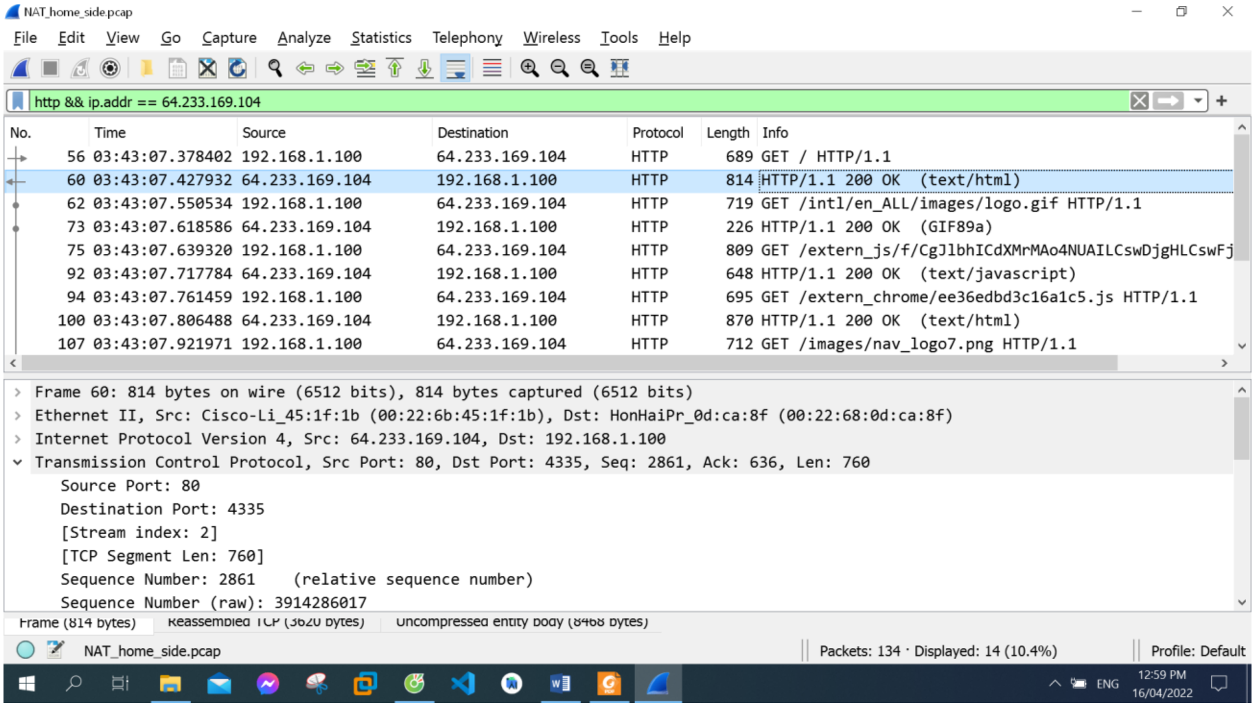
Source IP address: 192.168.1.100

TCP source port: 4335

Destination IP address: 64.233.168.104

TCP 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?


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 Info
 56 03:43:07.378402 192.168.1.100   64.233.169.104  HTTP       689 GET / HTTP/1.1
 60 03:43:07.427932 64.233.169.104  192.168.1.100   HTTP       814 HTTP/1.1 200 OK  (text/html)
 62 03:43:07.550534 192.168.1.100   64.233.169.104  HTTP       719 GET /intl/en_ALL/images/logo.gif HTTP/1.1
 73 03:43:07.618586 64.233.169.104  192.168.1.100   HTTP       226 HTTP/1.1 200 OK  (GIF89a)
 75 03:43:07.639320 192.168.1.100   64.233.169.104  HTTP       809 GET /extern_js/f/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFj
 92 03:43:07.717784 64.233.169.104  192.168.1.100   HTTP       648 HTTP/1.1 200 OK  (text/javascript)
 94 03:43:07.761459 192.168.1.100   64.233.169.104  HTTP       695 GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.1
100 03:43:07.806488 64.233.169.104  192.168.1.100   HTTP       870 HTTP/1.1 200 OK  (text/html)
107 03:43:07.921971 192.168.1.100   64.233.169.104  HTTP       712 GET /images/nav_logo7.png HTTP/1.1

> 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

Frame (814 bytes)   Reassembled TCP (3620 bytes)   Uncompressed entity body (8468 bytes)
NAT_home_side.pcap    Packets: 134 · Displayed: 14 (10.4%)    Profile: Default
```

The corresponding 200 OK HTTP message received from the Google server at: 7.427932

Source IP address: 64.233.168.104

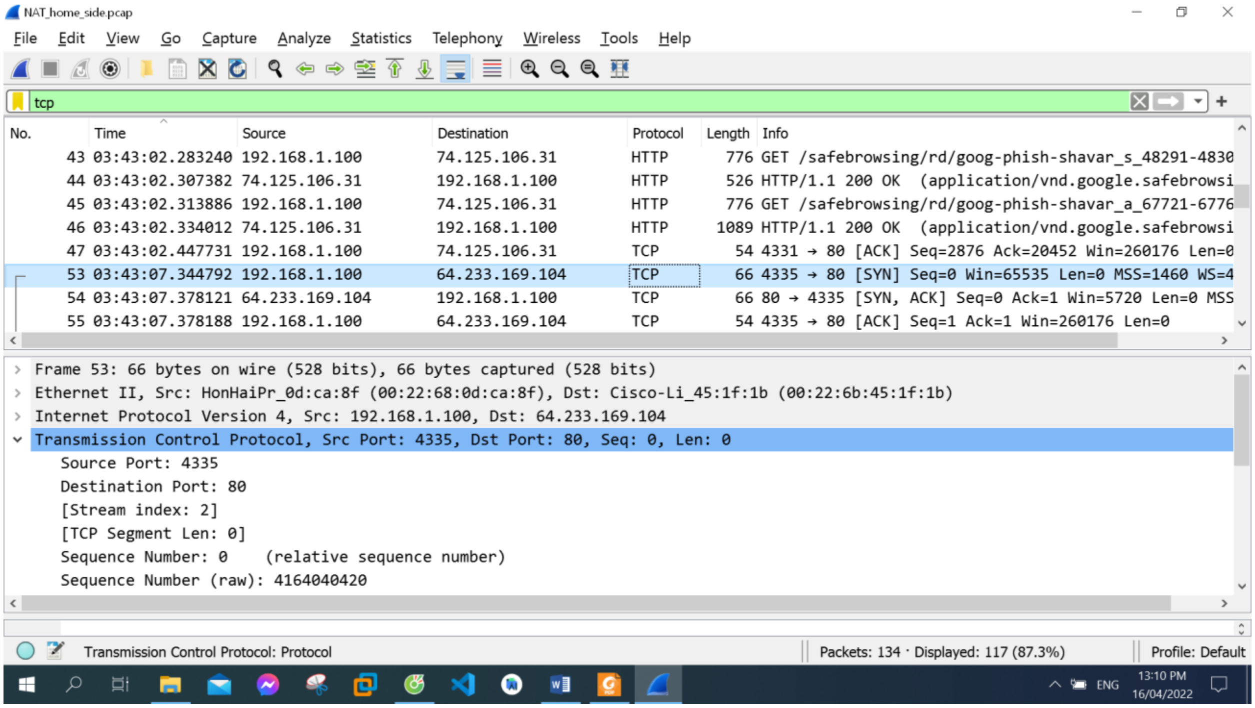
TCP source port: 80

Destination IP address: 192.168.1.100

TCP destination port: 4335

5. 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. 378402? What are the source and destination IP addresses and source and destination ports for the TCP SYN segment? What are the

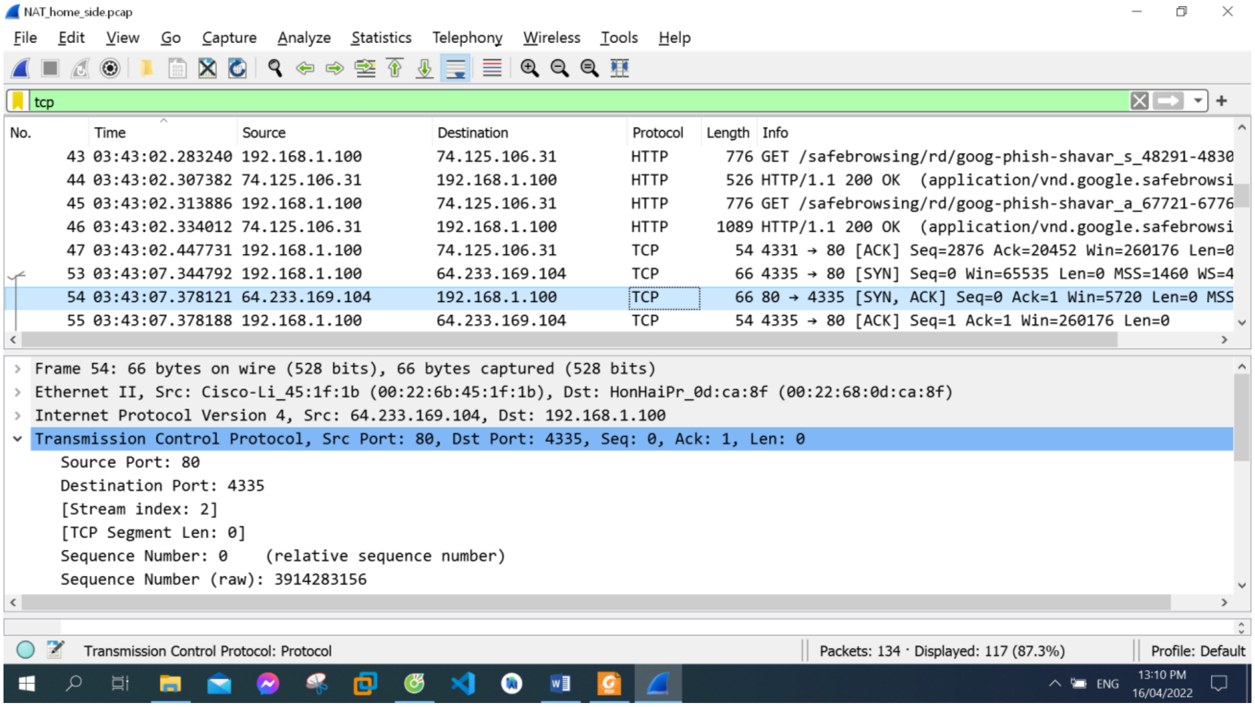
source and destination IP addresses and source and destination ports of the ACK sent in response to the SYN. At what time is this ACK received at the client?


NAT_home_side.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
ENG
13:10 PM
16/04/2022

```
No.   Time             Source          Destination     Protocol Length Info
   43 03:43:02.283240 192.168.1.100   74.125.106.31   HTTP      776 GET /safebrowsing/rd/goog-phish-shavar_s_48291-4830
   44 03:43:02.307382 74.125.106.31   192.168.1.100   HTTP      526 HTTP/1.1 200 OK  (application/vnd.google.safebrowsi
   45 03:43:02.313886 192.168.1.100   74.125.106.31   HTTP      776 GET /safebrowsing/rd/goog-phish-shavar_a_67721-6776
   46 03:43:02.334012 74.125.106.31   192.168.1.100   HTTP     1089 HTTP/1.1 200 OK  (application/vnd.google.safebrowsi
   47 03:43:02.447731 192.168.1.100   74.125.106.31   TCP        54 4331 → 80 [ACK] Seq=2876 Ack=20452 Win=260176 Len=0
   53 03:43:07.344792 192.168.1.100   64.233.169.104  TCP        66 4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4
   54 03:43:07.378121 64.233.169.104  192.168.1.100   TCP        66 80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS
   55 03:43:07.378188 192.168.1.100   64.233.169.104  TCP        54 4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
```

```
> 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]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 4164040420
```

Transmission Control Protocol: Protocol | Packets: 134 · Displayed: 117 (87.3%) | Profile: Default


NAT_home_side.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
ENG
13:10 PM
16/04/2022

```
No.   Time             Source          Destination     Protocol Length Info
   43 03:43:02.283240 192.168.1.100   74.125.106.31   HTTP      776 GET /safebrowsing/rd/goog-phish-shavar_s_48291-4830
   44 03:43:02.307382 74.125.106.31   192.168.1.100   HTTP      526 HTTP/1.1 200 OK  (application/vnd.google.safebrowsi
   45 03:43:02.313886 192.168.1.100   74.125.106.31   HTTP      776 GET /safebrowsing/rd/goog-phish-shavar_a_67721-6776
   46 03:43:02.334012 74.125.106.31   192.168.1.100   HTTP     1089 HTTP/1.1 200 OK  (application/vnd.google.safebrowsi
   47 03:43:02.447731 192.168.1.100   74.125.106.31   TCP        54 4331 → 80 [ACK] Seq=2876 Ack=20452 Win=260176 Len=0
   53 03:43:07.344792 192.168.1.100   64.233.169.104  TCP        66 4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4
   54 03:43:07.378121 64.233.169.104  192.168.1.100   TCP        66 80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS
   55 03:43:07.378188 192.168.1.100   64.233.169.104  TCP        54 4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
```

```
> Frame 54: 66 bytes on wire (528 bits), 66 bytes captured (528 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: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 4335
    [Stream index: 2]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 3914283156
```

Transmission Control Protocol: Protocol | Packets: 134 · Displayed: 117 (87.3%) | Profile: Default

The client-to-server TCP SYN segment sent that sets up the connection at: 7.344792

TCP segment:

Source IP address: 192.168.1.100

TCP source port: 4335

Destination IP address: 64.233.168.104

TCP destination port: 80

ACK sent in response to the SYN:

Source IP address: 64.233.168.104

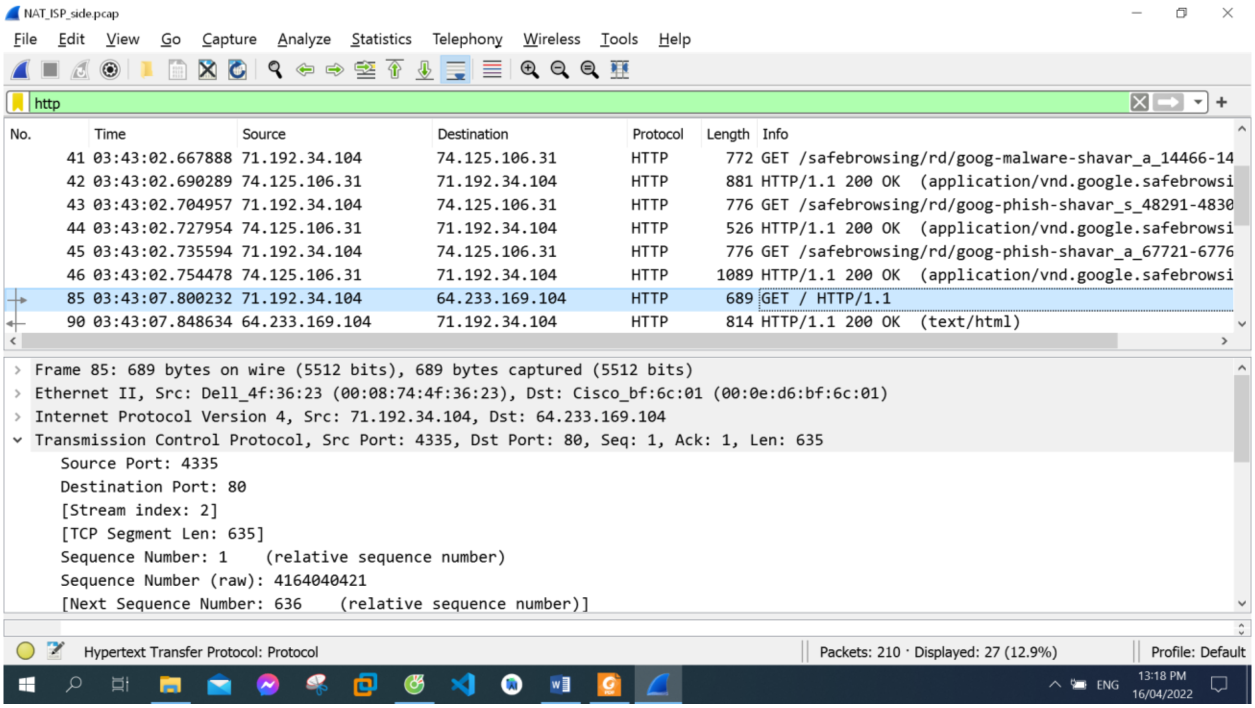
TCP source port: 80

Destination IP address: 192.168.1.100

TCP destination port: 4335

This ACK received at the client at: 7.378121

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


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

```
No.   Time            Source          Destination     Protocol Length Info
   41 03:43:02.667888 71.192.34.104   74.125.106.31   HTTP      772 GET /safebrowsing/rd/goog-malware-shavar_a_14466-14
   42 03:43:02.690289 74.125.106.31   71.192.34.104   HTTP      881 HTTP/1.1 200 OK  (application/vnd.google.safebrowsi
   43 03:43:02.704957 71.192.34.104   74.125.106.31   HTTP      776 GET /safebrowsing/rd/goog-phish-shavar_s_48291-4830
   44 03:43:02.727954 74.125.106.31   71.192.34.104   HTTP      526 HTTP/1.1 200 OK  (application/vnd.google.safebrowsi
   45 03:43:02.735594 71.192.34.104   74.125.106.31   HTTP      776 GET /safebrowsing/rd/goog-phish-shavar_a_67721-6776
   46 03:43:02.754478 74.125.106.31   71.192.34.104   HTTP     1089 HTTP/1.1 200 OK  (application/vnd.google.safebrowsi
   85 03:43:07.800232 71.192.34.104   64.233.169.104  HTTP      689 GET / HTTP/1.1
   90 03:43:07.848634 64.233.169.104  71.192.34.104   HTTP      814 HTTP/1.1 200 OK  (text/html)
```

```
> 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
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)]
```

Hypertext Transfer Protocol: Protocol
Packets: 210 · Displayed: 27 (12.9%)
Profile: Default
ENG
13:18 PM
16/04/2022

This message appear in the NAT_ISP_side trace file: 7.800232

Source IP address: 71.192.34.104

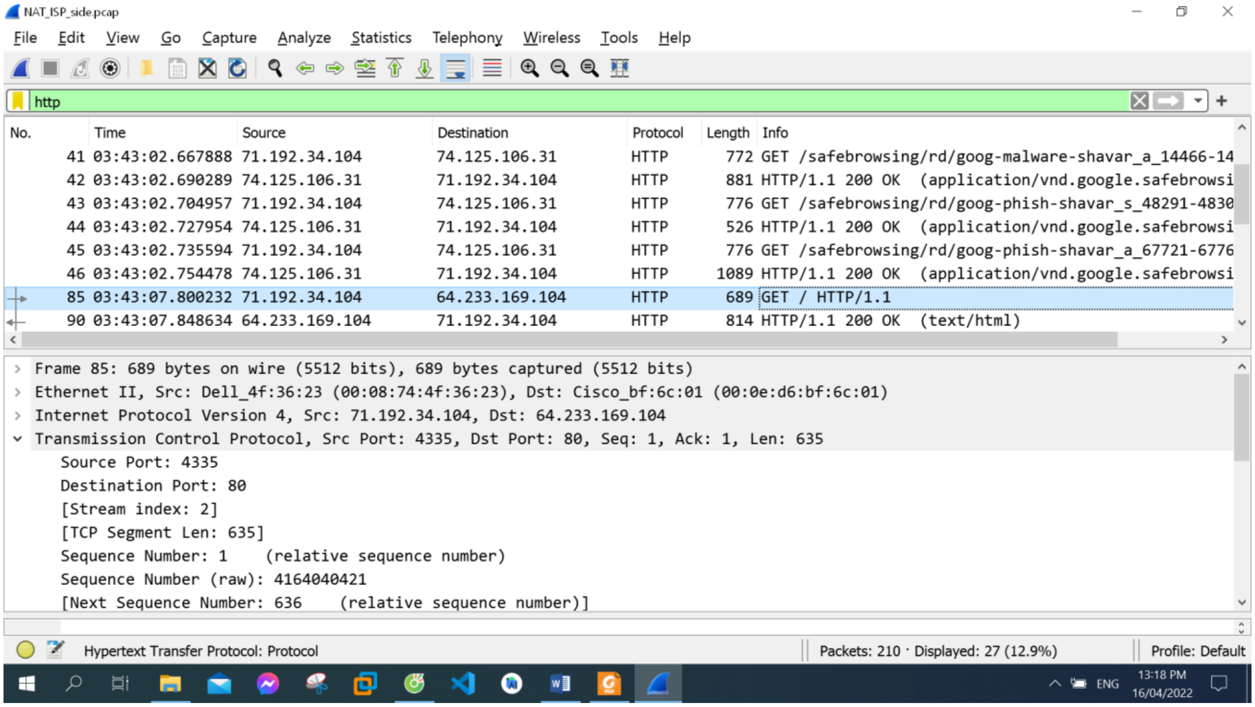
TCP source port: 4335

Destination IP address: 64.233.168.104

TCP destination port: 80

Only Destination IP address is different in my answer to Q4 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.



```
No.      Time            Source          Destination      Protocol  Length Info
      41 03:43:02.667888 71.192.34.104   74.125.106.31    HTTP         772 GET /safebrowsing/rd/goog-malware-shavar_a_14466-14
      42 03:43:02.690289 74.125.106.31   71.192.34.104    HTTP         881 HTTP/1.1 200 OK  (application/vnd.google.safebrowsi
      43 03:43:02.704957 71.192.34.104   74.125.106.31    HTTP         776 GET /safebrowsing/rd/goog-phish-shavar_s_48291-4830
      44 03:43:02.727954 74.125.106.31   71.192.34.104    HTTP         526 HTTP/1.1 200 OK  (application/vnd.google.safebrowsi
      45 03:43:02.735594 71.192.34.104   74.125.106.31    HTTP         776 GET /safebrowsing/rd/goog-phish-shavar_a_67721-6776
      46 03:43:02.754478 74.125.106.31   71.192.34.104    HTTP        1089 HTTP/1.1 200 OK  (application/vnd.google.safebrowsi
      85 03:43:07.800232 71.192.34.104   64.233.169.104   HTTP         689 GET / HTTP/1.1
      90 03:43:07.848634 64.233.169.104  71.192.34.104    HTTP         814 HTTP/1.1 200 OK  (text/html)
```

```
> 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
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)]
```

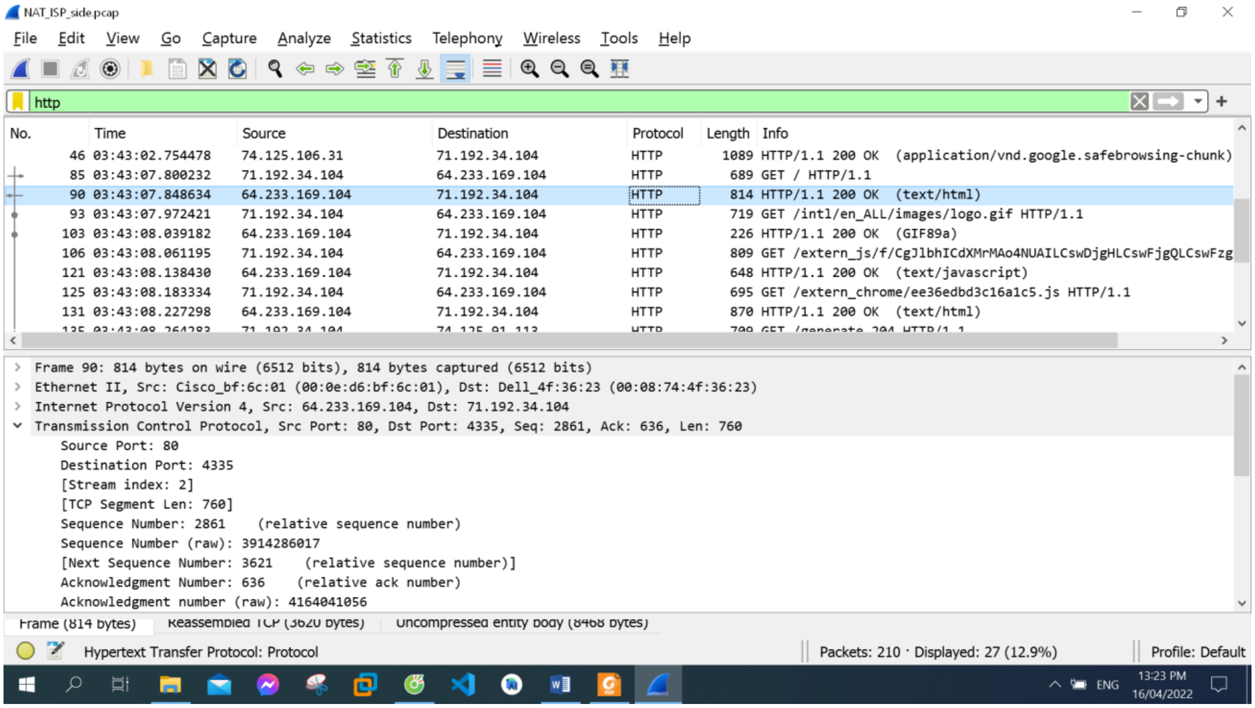
Hypertext Transfer Protocol: Protocol
Packets: 210 · Displayed: 27 (12.9%)
Profile: Default
ENG
13:18 PM
16/04/2022

There is no field in the HTTP GET message changed

Only Checksum changed. Because the IP source address changed, checksum include value of IP source address

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?


NAT_ISP_side.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Frame (814 bytes)
Reassembled TCP (3620 bytes)
Uncompressed entity body (8468 bytes)
Hypertext Transfer Protocol: Protocol
Packets: 210 · Displayed: 27 (12.9%)
Profile: Default
ENG
13:23 PM
16/04/2022

http

```
No.    Time              Source           Destination      Protocol  Length  Info
   46 03:43:02.754478   74.125.106.31    71.192.34.104    HTTP      1089 HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-chunk)
   85 03:43:07.800232   71.192.34.104    64.233.169.104   HTTP       689 GET / HTTP/1.1
   90 03:43:07.848634   64.233.169.104   71.192.34.104    HTTP       814 HTTP/1.1 200 OK  (text/html)
   93 03:43:07.972421   71.192.34.104    64.233.169.104   HTTP       719 GET /intl/en_ALL/images/logo.gif HTTP/1.1
  103 03:43:08.039182   64.233.169.104   71.192.34.104    HTTP       226 HTTP/1.1 200 OK  (GIF89a)
  106 03:43:08.061195   71.192.34.104    64.233.169.104   HTTP       809 GET /extern_js/f/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswFzg
  121 03:43:08.138430   64.233.169.104   71.192.34.104    HTTP       648 HTTP/1.1 200 OK  (text/javascript)
  125 03:43:08.183334   71.192.34.104    64.233.169.104   HTTP       695 GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.1
  131 03:43:08.227298   64.233.169.104   71.192.34.104    HTTP       870 HTTP/1.1 200 OK  (text/html)
  135 03:43:08.264283   71.192.34.104    74.125.91.113    HTTP       709 GET /generate_204 HTTP/1.1
```

```
> Frame 90: 814 bytes on wire (6512 bits), 814 bytes captured (6512 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: 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)
    Acknowledgment number (raw): 4164041056
```

The first 200 OK HTTP message received from the Google server at: 7.848634

Source IP address: 64.233.168.104

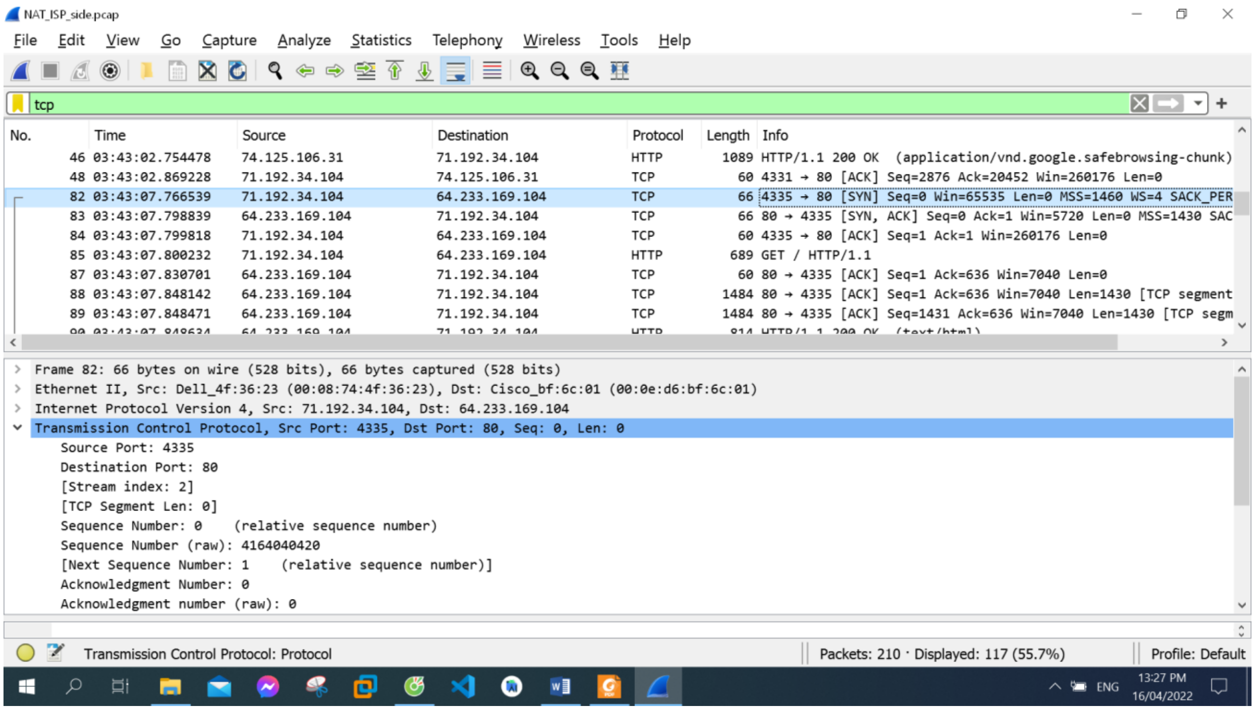
TCP source port: 80

Destination IP address: 71.192.34.104

TCP destination port: 4335

Only Destination IP address is different in my answer to Q4 above

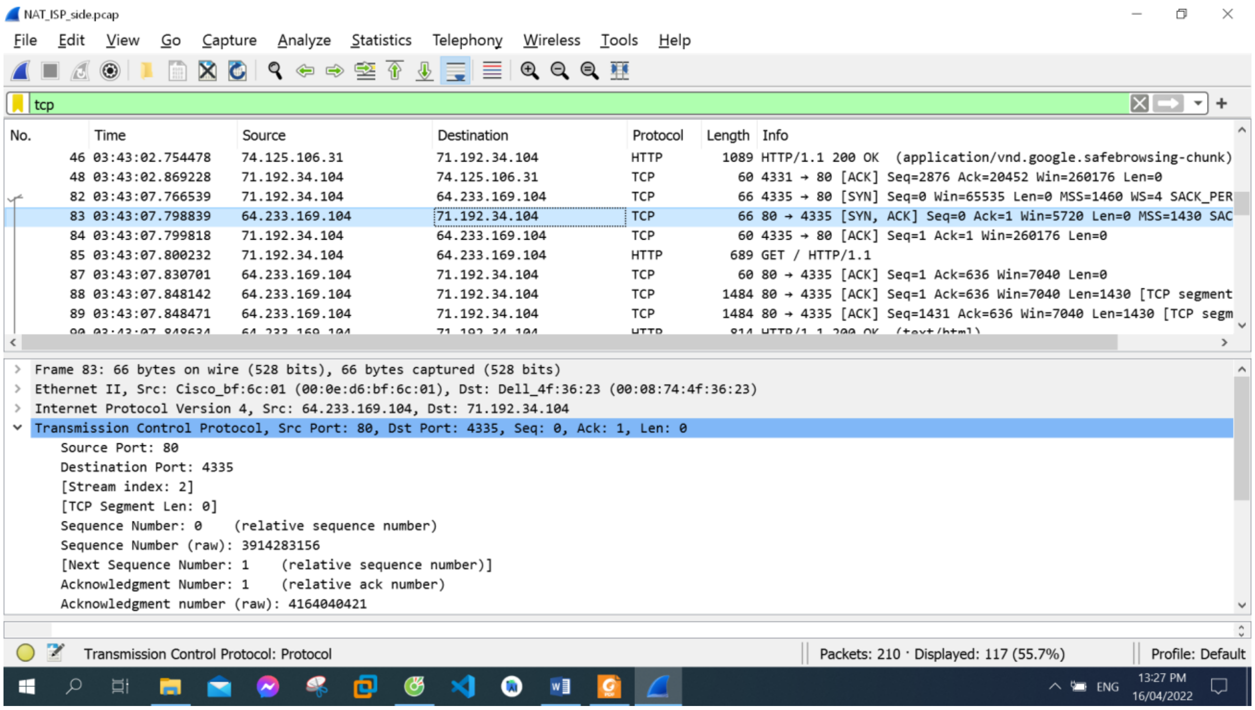
9. In the NAT_ISP_side trace file, at what time were the client-to-server TCP SYN segment and the server-to-client TCP ACK segment corresponding to the segments in question 5 above captured? What are the source and destination IP addresses and source and destination ports for these two segments? Which of these fields are the same, and which are different than your answer to question 5 above?


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

```
No.   Time             Source           Destination      Protocol Length Info
   46 03:43:02.754478  74.125.106.31    71.192.34.104    HTTP     1089 HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-chunk)
   48 03:43:02.869228  71.192.34.104    74.125.106.31    TCP        60 4331 → 80 [ACK] Seq=2876 Ack=20452 Win=260176 Len=0
   82 03:43:07.766539  71.192.34.104    64.233.169.104   TCP        66 4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PER
   83 03:43:07.798839  64.233.169.104   71.192.34.104    TCP        66 80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SAC
   84 03:43:07.799818  71.192.34.104    64.233.169.104   TCP        60 4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
   85 03:43:07.800232  71.192.34.104    64.233.169.104   HTTP      689 GET / HTTP/1.1
   87 03:43:07.830701  64.233.169.104   71.192.34.104    TCP        60 80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0
   88 03:43:07.848142  64.233.169.104   71.192.34.104    TCP      1484 80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=1430 [TCP segment
   89 03:43:07.848471  64.233.169.104   71.192.34.104    TCP      1484 80 → 4335 [ACK] Seq=1431 Ack=636 Win=7040 Len=1430 [TCP segm
   90 03:43:07.849634  64.233.169.104   71.192.34.104    HTTP      814 HTTP/1.1 200 OK  (text/html)
```

```
> 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)
     Sequence Number (raw): 4164040420
     [Next Sequence Number: 1    (relative sequence number)]
     Acknowledgment Number: 0
     Acknowledgment number (raw): 0
```

Transmission Control Protocol: Protocol
Packets: 210 · Displayed: 117 (55.7%)
Profile: Default
ENG
13:27 PM
16/04/2022


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

```
No.   Time             Source           Destination      Protocol Length Info
   46 03:43:02.754478  74.125.106.31    71.192.34.104    HTTP     1089 HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-chunk)
   48 03:43:02.869228  71.192.34.104    74.125.106.31    TCP        60 4331 → 80 [ACK] Seq=2876 Ack=20452 Win=260176 Len=0
   82 03:43:07.766539  71.192.34.104    64.233.169.104   TCP        66 4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PER
   83 03:43:07.798839  64.233.169.104   71.192.34.104    TCP        66 80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SAC
   84 03:43:07.799818  71.192.34.104    64.233.169.104   TCP        60 4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
   85 03:43:07.800232  71.192.34.104    64.233.169.104   HTTP      689 GET / HTTP/1.1
   87 03:43:07.830701  64.233.169.104   71.192.34.104    TCP        60 80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0
   88 03:43:07.848142  64.233.169.104   71.192.34.104    TCP      1484 80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=1430 [TCP segment
   89 03:43:07.848471  64.233.169.104   71.192.34.104    TCP      1484 80 → 4335 [ACK] Seq=1431 Ack=636 Win=7040 Len=1430 [TCP segm
   90 03:43:07.849634  64.233.169.104   71.192.34.104    HTTP      814 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 83: 66 bytes on wire (528 bits), 66 bytes captured (528 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: 0, Ack: 1, Len: 0
     Source Port: 80
     Destination Port: 4335
     [Stream index: 2]
     [TCP Segment Len: 0]
     Sequence Number: 0    (relative sequence number)
     Sequence Number (raw): 3914283156
     [Next Sequence Number: 1    (relative sequence number)]
     Acknowledgment Number: 1    (relative ack number)
     Acknowledgment number (raw): 4164040421
```

Transmission Control Protocol: Protocol
Packets: 210 · Displayed: 117 (55.7%)
Profile: Default
ENG
13:27 PM
16/04/2022

The client-to-server TCP SYN segment corresponding at: 7.766539

The server-to-client TCP ACK segment corresponding at: 7.798839

The client-to-server TCP SYN segment:

Source IP address: 71.192.34.104

TCP source port: 4335

Destination IP address: 64.233.168.104

TCP destination port: 80

The server-to-client TCP ACK segment:

Source IP address: 64.233.168.104

TCP source port: 80

Destination IP address: 71.192.34.104

TCP destination port: 4335

The client-to-server TCP SYN segment: Source IP address changed

The server-to-client TCP ACK segment:: Destination IP address changed

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 entries		
	WAN side	LAN side
IP address	71.192.34.104	192.168.1.100
TCP port	4335	4335