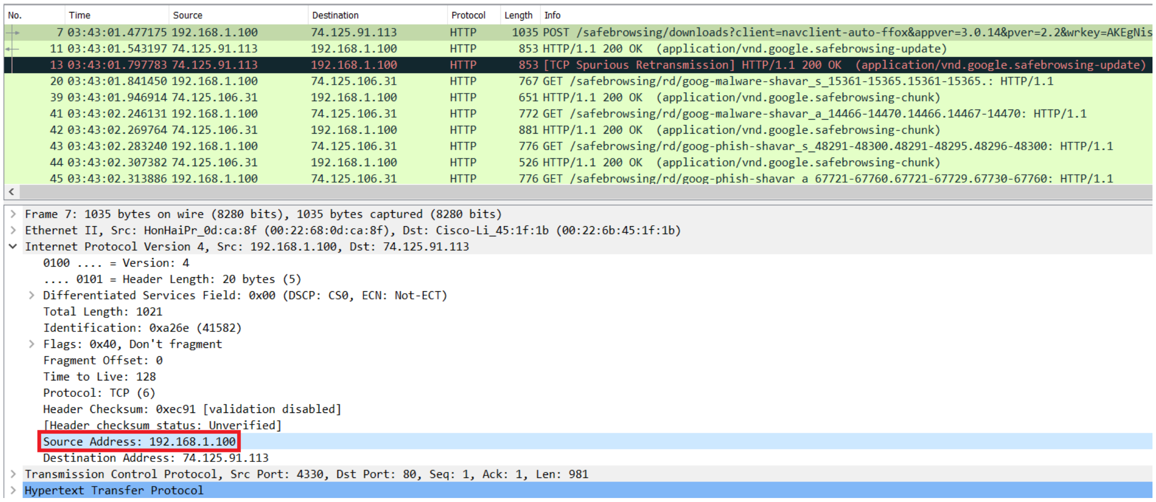
COMPUTER NETWORK
Lab 4c

Student name: Nguyễn Minh Tâm
ID: 1952968

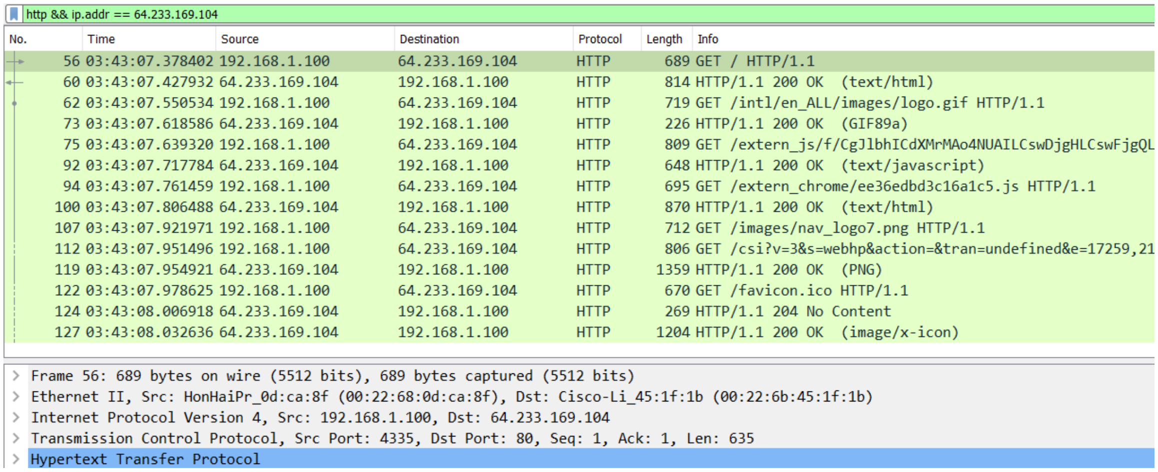
1. What is the IP address of the client?
   Ans: The IP address of the client 192.168.1.100



```
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-ffox&appver=3.0.14&pver=2.2&wrkey=AKEgNis
  11 03:43:01.543197 74.125.91.113   192.168.1.100   HTTP      853 HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-update)
  13 03:43:01.797783 74.125.91.113   192.168.1.100   HTTP      853 [TCP Spurious Retransmission] HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-update)
  20 03:43:01.841450 192.168.1.100   74.125.106.31   HTTP      767 GET /safebrowsing/rd/goog-malware-shavar_s_15361-15365.15361-15365.: HTTP/1.1
  39 03:43:01.946914 74.125.106.31   192.168.1.100   HTTP      651 HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-chunk)
  41 03:43:02.246131 192.168.1.100   74.125.106.31   HTTP      772 GET /safebrowsing/rd/goog-malware-shavar_a_14466-14470.14466.14467-14470: HTTP/1.1
  42 03:43:02.269764 74.125.106.31   192.168.1.100   HTTP      881 HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-chunk)
  43 03:43:02.283240 192.168.1.100   74.125.106.31   HTTP      776 GET /safebrowsing/rd/goog-phish-shavar_s_48291-48300.48291-48295.48296-48300: HTTP/1.1
  44 03:43:02.307382 74.125.106.31   192.168.1.100   HTTP      526 HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-chunk)
  45 03:43:02.313886 192.168.1.100   74.125.106.31   HTTP      776 GET /safebrowsing/rd/goog-phish-shavar_a_67721-67760.67721-67729.67730-67760: HTTP/1.1
```

```
> Frame 7: 1035 bytes on wire (8280 bits), 1035 bytes captured (8280 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)
v Internet Protocol Version 4, Src: 192.168.1.100, Dst: 74.125.91.113
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1021
    Identification: 0xa26e (41582)
  > Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0xec91 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.100
    Destination Address: 74.125.91.113
> Transmission Control Protocol, Src Port: 4330, Dst Port: 80, Seq: 1, Ack: 1, Len: 981
> Hypertext Transfer Protocol
```

2.

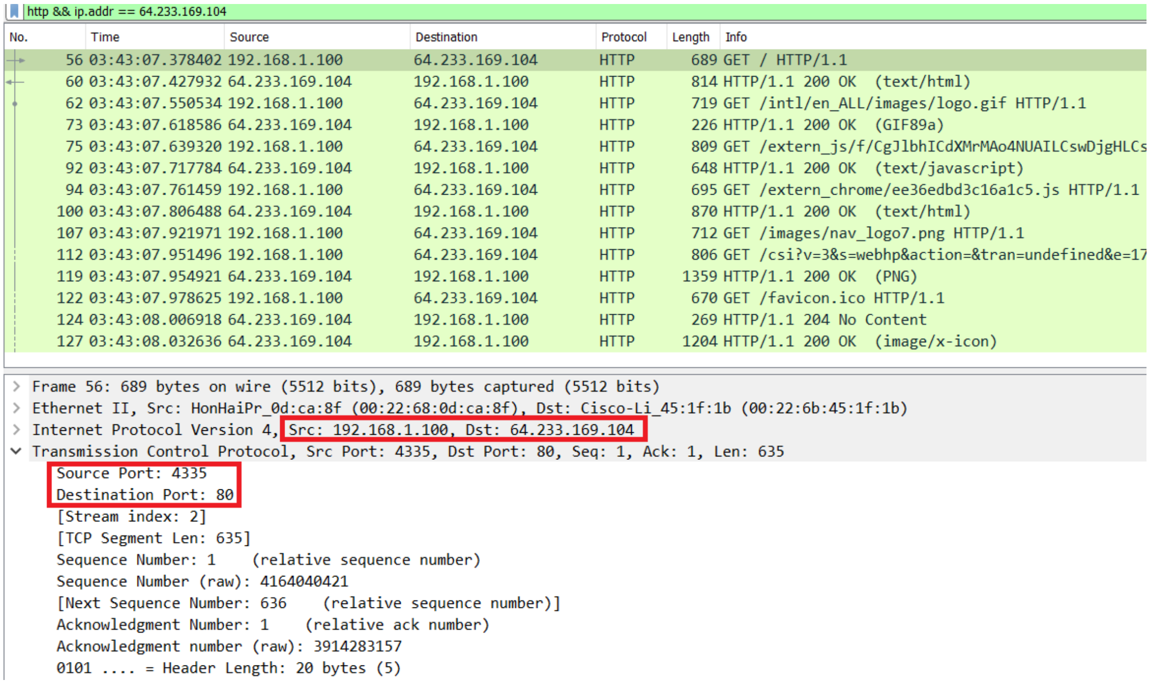


```
http && ip.addr == 64.233.169.104
```

```
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/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQL
  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=17259,21
 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
> Hypertext Transfer Protocol
```

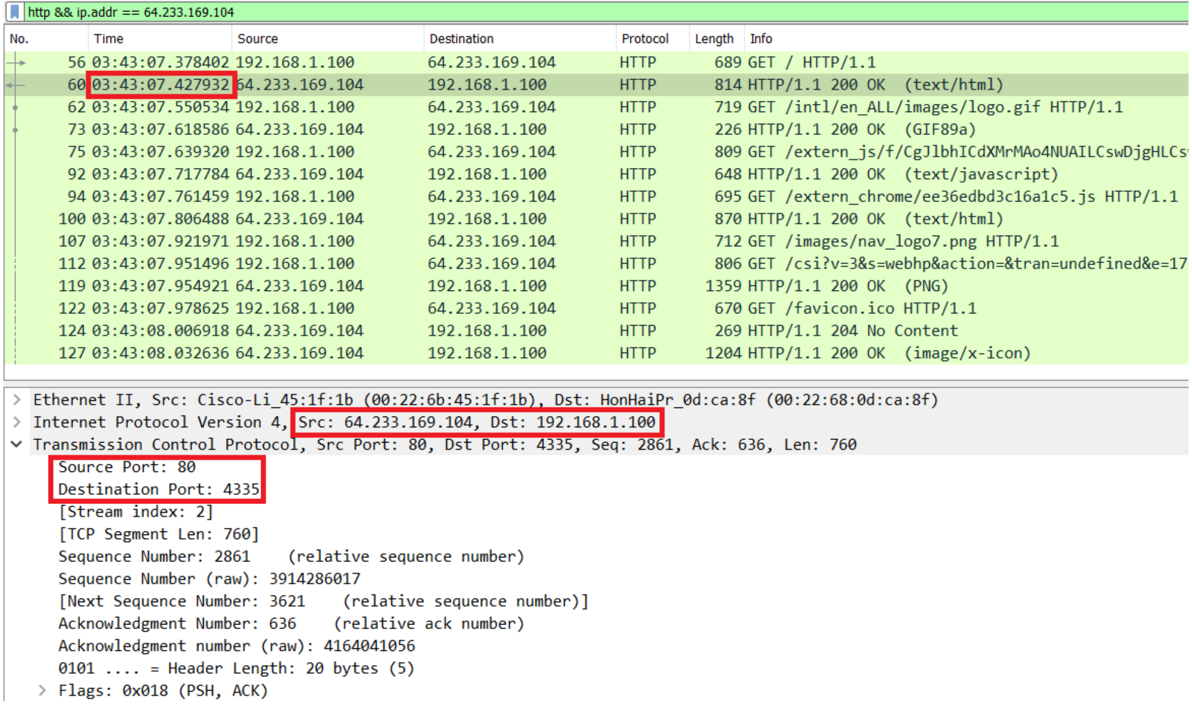
3. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?
   Ans:
   The source IP address: 192.168.1.100
   The destination IP address: 64.233.269.104
   The TCP source port: 4335
   The TCP destination port: 80



```
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/CgJlbhICdXMrMAo4NUAILCswDjgHLCs
   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=17
  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
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)
    Acknowledgment number (raw): 3914283157
    0101 .... = Header Length: 20 bytes (5)
```

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:

   The corresponding 200 OK HTTP message received from the Google server at 03:43:07.427932.
   The source IP address: 64.233.169.104
   The destination IP address: 192.168.1.100
   The TCP source port: 80
   The TCP destination port: 4335



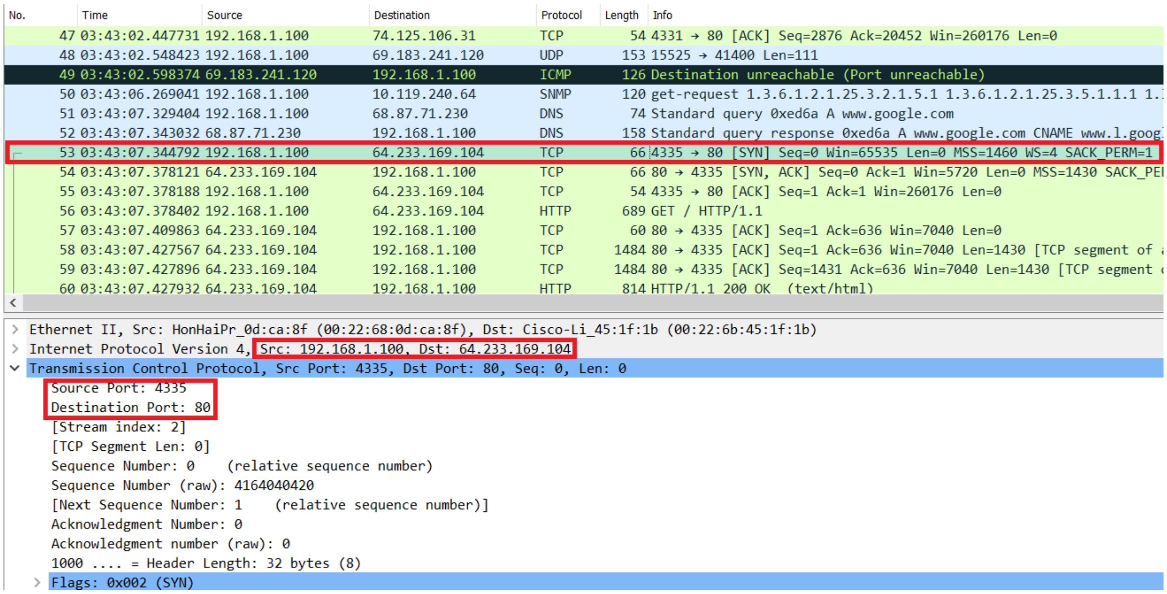
```
http && ip.addr == 64.233.169.104
No.     Time            Source          Destination     Protocol  Length  Info
   56 03:43:07.378402 192.168.1.100   64.233.169.104  HTTP       689 GET / HTTP/1.1
   60 03:43:07.427932 64.233.169.104  192.168.1.100   HTTP       814 HTTP/1.1 200 OK  (text/html)
   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/CgJlbhICdXMrMAo4NUAILCswDjgHLCs
   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=17
  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)

> 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)
    Acknowledgment number (raw): 4164041056
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
```

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 7.109267? 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?

   Ans:

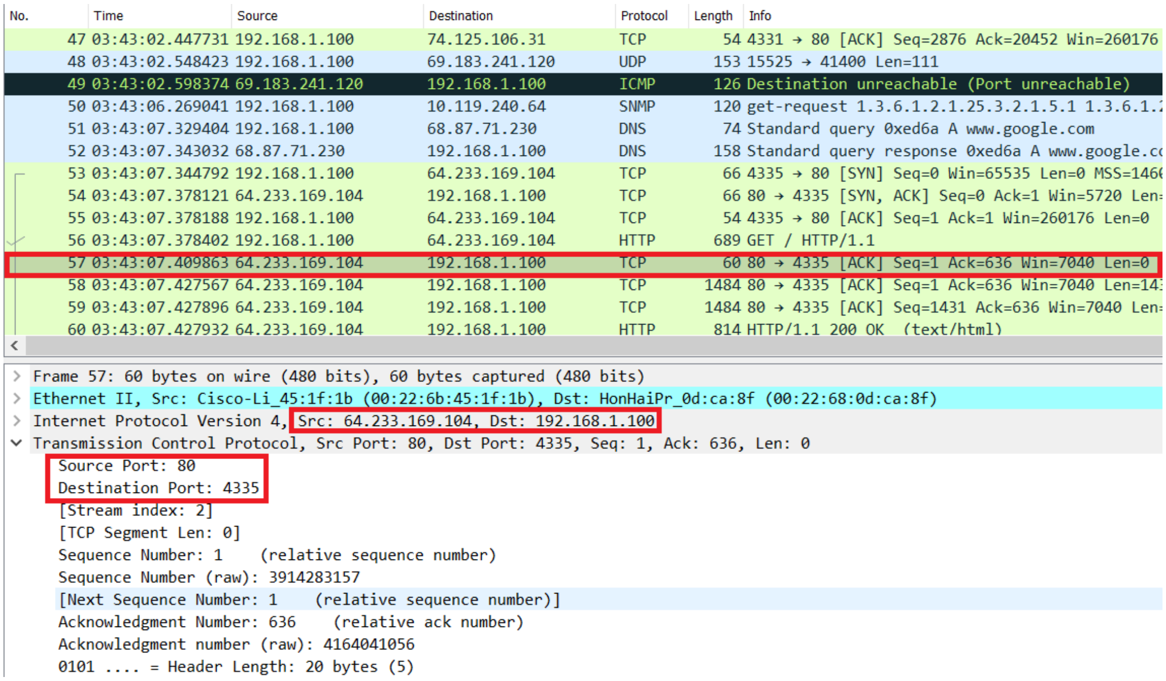
   The client-to-server TCP SYN segment sent that sets up the connection used by the GET at 03:43:07.344792.

   The source IP address: 192.168.1.100
   The destination IP address: 64.233.169.104
   The source port for the TCP SYN segment: 4335
   The destination port for the TCP SYN segment: 80



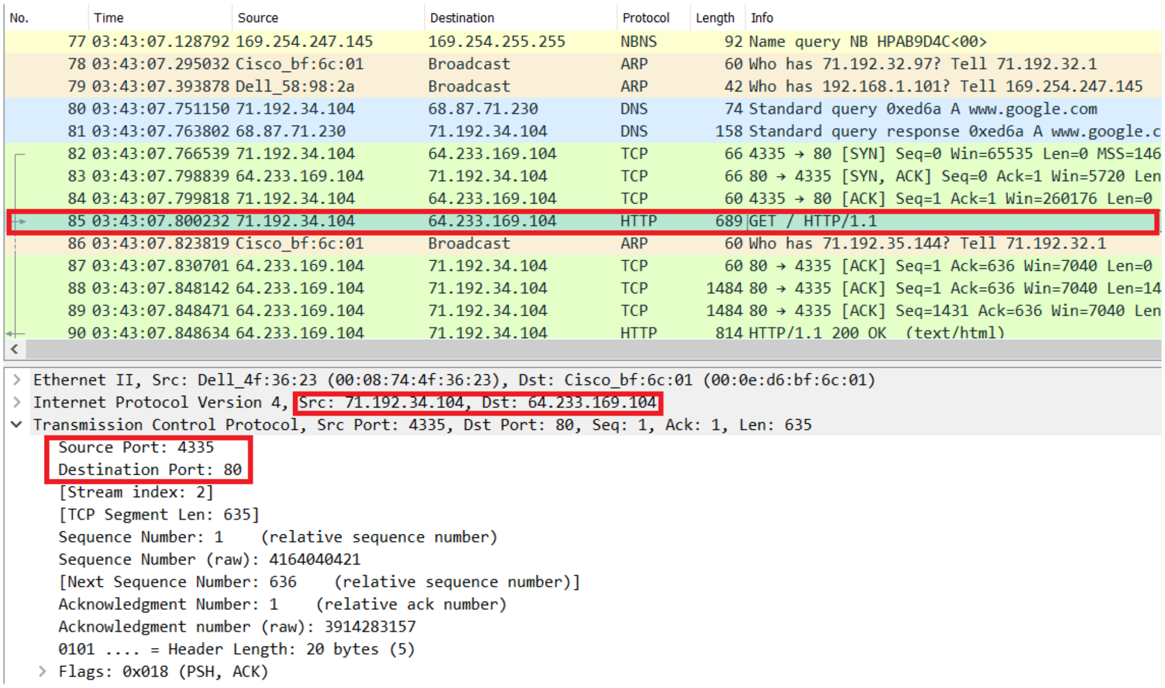
```
No.     Time            Source          Destination     Protocol Length Info
     47 03:43:02.447731 192.168.1.100   74.125.106.31   TCP        54 4331 → 80 [ACK] Seq=2876 Ack=20452 Win=260176 Len=0
     48 03:43:02.548423 192.168.1.100   69.183.241.120  UDP       153 15525 → 41400 Len=111
     49 03:43:02.598374 69.183.241.120  192.168.1.100   ICMP      126 Destination unreachable (Port unreachable)
     50 03:43:06.269041 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.
     51 03:43:07.329404 192.168.1.100   68.87.71.230    DNS        74 Standard query 0xed6a A www.google.com
     52 03:43:07.343032 68.87.71.230    192.168.1.100   DNS       158 Standard query response 0xed6a A www.google.com CNAME www.l.goog
     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 SACK_PERM=1
     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=1430 SACK_PE
     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
     56 03:43:07.378402 192.168.1.100   64.233.169.104  HTTP      689 GET / HTTP/1.1
     57 03:43:07.409863 64.233.169.104  192.168.1.100   TCP        60 80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0
     58 03:43:07.427567 64.233.169.104  192.168.1.100   TCP      1484 80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=1430 [TCP segment of
     59 03:43:07.427896 64.233.169.104  192.168.1.100   TCP      1484 80 → 4335 [ACK] Seq=1431 Ack=636 Win=7040 Len=1430 [TCP segment
     60 03:43:07.427932 64.233.169.104  192.168.1.100   HTTP      814 HTTP/1.1 200 OK  (text/html)

> 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
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
```

The source IP address: 64.233.169.104
The destination IP address: 192.168.1.100
The source port of the ACK: 80
The destination port of the ACK: 4335
The ACK is received at the client at 03:43:07.409863



```
No.   Time             Source          Destination     Protocol Length Info
   47 03:43:02.447731 192.168.1.100   74.125.106.31   TCP        54 4331 → 80 [ACK] Seq=2876 Ack=20452 Win=260176
   48 03:43:02.548423 192.168.1.100   69.183.241.120  UDP       153 15525 → 41400 Len=111
   49 03:43:02.598374 69.183.241.120  192.168.1.100   ICMP      126 Destination unreachable (Port unreachable)
   50 03:43:06.269041 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.
   51 03:43:07.329404 192.168.1.100   68.87.71.230    DNS        74 Standard query 0xed6a A www.google.com
   52 03:43:07.343032 68.87.71.230    192.168.1.100   DNS       158 Standard query response 0xed6a A www.google.co
   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=146
   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=
   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
   56 03:43:07.378402 192.168.1.100   64.233.169.104  HTTP      689 GET / HTTP/1.1
   57 03:43:07.409863 64.233.169.104  192.168.1.100   TCP        60 80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0
   58 03:43:07.427567 64.233.169.104  192.168.1.100   TCP      1484 80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=14
   59 03:43:07.427896 64.233.169.104  192.168.1.100   TCP      1484 80 → 4335 [ACK] Seq=1431 Ack=636 Win=7040 Len=
   60 03:43:07.427932 64.233.169.104  192.168.1.100   HTTP      814 HTTP/1.1 200 OK  (text/html)

> Frame 57: 60 bytes on wire (480 bits), 60 bytes captured (480 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: 1, Ack: 636, Len: 0
    Source Port: 80
    Destination Port: 4335
    [Stream index: 2]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3914283157
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 636    (relative ack number)
    Acknowledgment number (raw): 4164041056
    0101 .... = Header Length: 20 bytes (5)
```

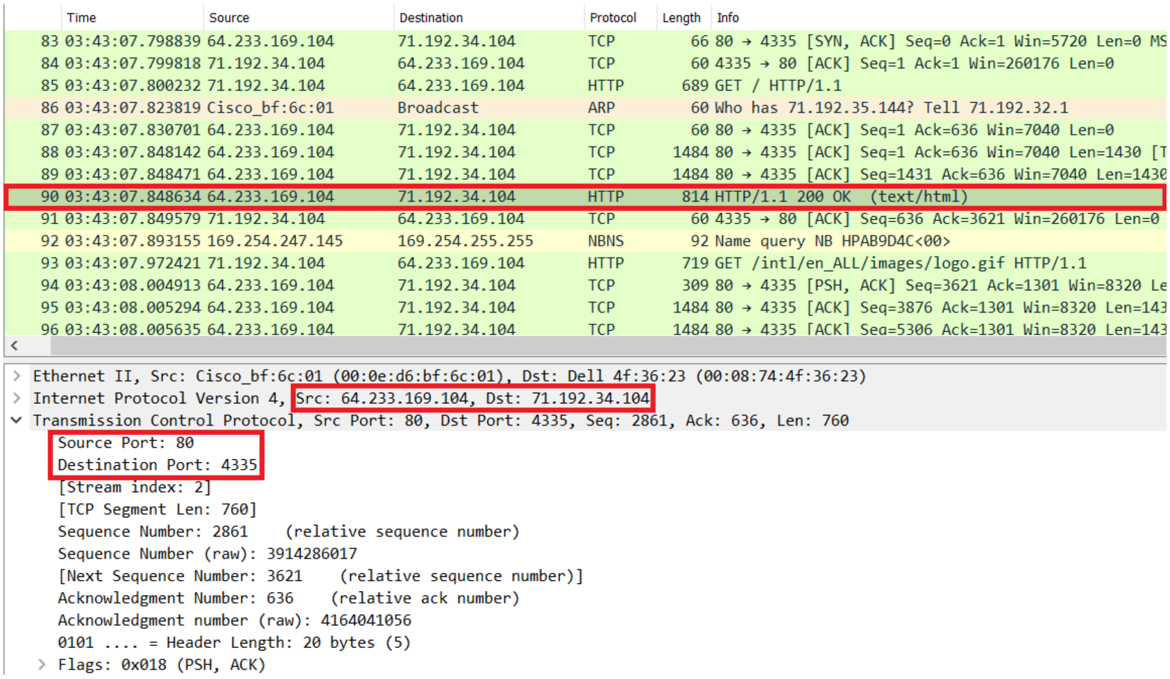
6. At what time does this message appear in the NAT_ISP_side trace file? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET? Which of these fields are the same, and which are different, than in your answer to question 3 above?
   Ans:
   The message appears at 03:43:07.800232.
   The source IP address: 71.192.34.104
   The destination IP address: 64.233.169.104
   The source port: 4335
   The destination port: 80
   Only the time and the source IP address are different from question 3. The others stay the same.



```
No.   Time            Source           Destination      Protocol Length Info
   77 03:43:07.128792 169.254.247.145  169.254.255.255  NBNS       92 Name query NB HPAB9D4C<00>
   78 03:43:07.295032 Cisco_bf:6c:01   Broadcast        ARP        60 Who has 71.192.32.97? Tell 71.192.32.1
   79 03:43:07.393878 Dell_58:98:2a    Broadcast        ARP        42 Who has 192.168.1.101? Tell 169.254.247.145
   80 03:43:07.751150 71.192.34.104    68.87.71.230     DNS        74 Standard query 0xed6a A www.google.com
   81 03:43:07.763802 68.87.71.230     71.192.34.104    DNS       158 Standard query response 0xed6a A www.google.c
   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=146
   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
   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
   86 03:43:07.823819 Cisco_bf:6c:01   Broadcast        ARP        60 Who has 71.192.35.144? Tell 71.192.32.1
   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=14
   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
   90 03:43:07.848634 64.233.169.104   71.192.34.104    HTTP      814 HTTP/1.1 200 OK  (text/html)

> 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)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3914283157
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
```

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: Only the Checksum changes. Since the IP source address has changed, and the checksum includes the value of the source IP address, the checksum has changed.

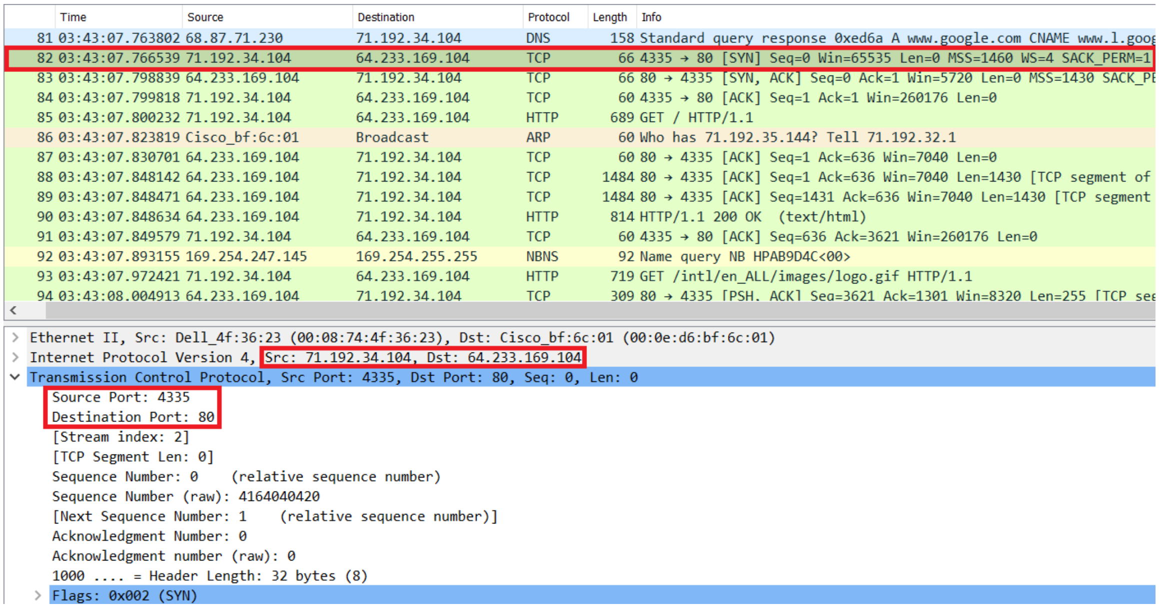
8. In the NAT_ISP_side trace file, at what time is the first 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message? Which of these fields are the same, and which are different than your answer to question 4 above?
   Ans:
   The first 200 OK HTTP message is received from the Google server at 03:43:07.848634.
   The source IP address: 64.233.169.104
   The destination IP address: 71.192.34.104
   The TCP source port: 80
   The TCP destination port: 4335
   Only the destination IP address has changed.



```
   Time              Source           Destination      Protocol Length Info
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 MS
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
86 03:43:07.823819 Cisco_bf:6c:01   Broadcast        ARP        60 Who has 71.192.35.144? Tell 71.192.32.1
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 [T
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
90 03:43:07.848634 64.233.169.104   71.192.34.104    HTTP      814 HTTP/1.1 200 OK  (text/html)
91 03:43:07.849579 71.192.34.104    64.233.169.104   TCP        60 4335 → 80 [ACK] Seq=636 Ack=3621 Win=260176 Len=0
92 03:43:07.893155 169.254.247.145  169.254.255.255  NBNS       92 Name query NB HPAB9D4C<00>
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
94 03:43:08.004913 64.233.169.104   71.192.34.104    TCP       309 80 → 4335 [PSH, ACK] Seq=3621 Ack=1301 Win=8320 Le
95 03:43:08.005294 64.233.169.104   71.192.34.104    TCP      1484 80 → 4335 [ACK] Seq=3876 Ack=1301 Win=8320 Len=143
96 03:43:08.005635 64.233.169.104   71.192.34.104    TCP      1484 80 → 4335 [ACK] Seq=5306 Ack=1301 Win=8320 Len=143
```

```
> 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
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
```

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?
Ans:
The TCP SYN segment was captured at 03:43:07.766539.
The source IP address: 71.192.34.104
The destination IP address: 64.233.169.104
The source port: 4335
The destination port: 80

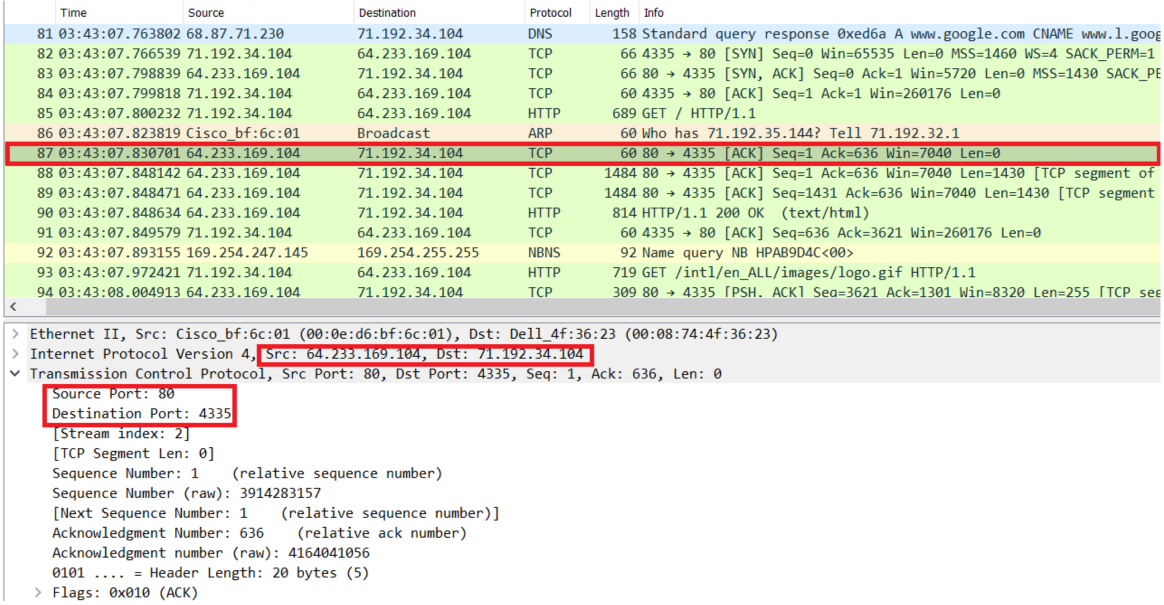


```
   Time              Source           Destination      Protocol Length Info
81 03:43:07.763802 68.87.71.230     71.192.34.104    DNS       158 Standard query response 0xed6a A www.google.com CNAME www.l.goog
82 03:43:07.766539 71.192.34.104    64.233.169.104   TCP        66 4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
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 SACK_PE
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
86 03:43:07.823819 Cisco_bf:6c:01   Broadcast        ARP        60 Who has 71.192.35.144? Tell 71.192.32.1
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 of
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 segment
90 03:43:07.848634 64.233.169.104   71.192.34.104    HTTP      814 HTTP/1.1 200 OK  (text/html)
91 03:43:07.849579 71.192.34.104    64.233.169.104   TCP        60 4335 → 80 [ACK] Seq=636 Ack=3621 Win=260176 Len=0
92 03:43:07.893155 169.254.247.145  169.254.255.255  NBNS       92 Name query NB HPAB9D4C<00>
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
94 03:43:08.004913 64.233.169.104   71.192.34.104    TCP       309 80 → 4335 [PSH, ACK] Seq=3621 Ack=1301 Win=8320 Len=255 [TCP se
```

```
> 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
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
```

The TCP ACK segment was captured at 03:43:07.830701.

The source IP address: 64.233.169.104
The destination IP address: 71.192.34.104
The source port: 80
The destination port: 4335



```
     Time              Source            Destination       Protocol  Length  Info
  81 03:43:07.763802 68.87.71.230      71.192.34.104     DNS        158 Standard query response 0xed6a A www.google.com CNAME www.l.goog
  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_PERM=1
  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 SACK_PE
  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
  86 03:43:07.823819 Cisco_bf:6c:01    Broadcast         ARP         60 Who has 71.192.35.144? Tell 71.192.32.1
  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 of
  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 segment
  90 03:43:07.848634 64.233.169.104    71.192.34.104     HTTP       814 HTTP/1.1 200 OK  (text/html)
  91 03:43:07.849579 71.192.34.104     64.233.169.104    TCP         60 4335 → 80 [ACK] Seq=636 Ack=3621 Win=260176 Len=0
  92 03:43:07.893155 169.254.247.145   169.254.255.255   NBNS        92 Name query NB HPAB9D4C<00>
  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
  94 03:43:08.004913 64.233.169.104    71.192.34.104     TCP        309 80 → 4335 [PSH, ACK] Seq=3621 Ack=1301 Win=8320 Len=255 [TCP seg

> 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: 1, Ack: 636, Len: 0
    Source Port: 80
    Destination Port: 4335
    [Stream index: 2]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3914283157
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 636    (relative ack number)
    Acknowledgment number (raw): 4164041056
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
```

For the SYN, the source IP address has changed. The port numbers are unchanged.
For the ACK, the destination IP address has changed. 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 translate table	
WAN side	LAN side
71.192.34.104, 4335	192.168.1.100, 4335