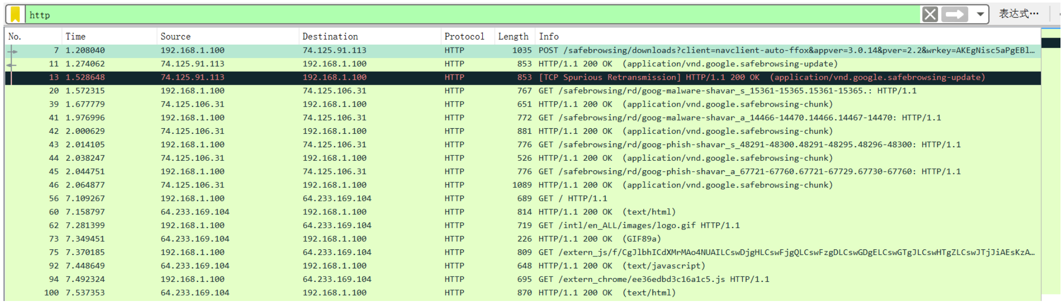
实验四：使用 Wireshark 软件分析 NAT

学号：16307130194，姓名：陈中钰

1 问题 1

What is the IP address of the client?

1.1 客户端 IP 地址



http

No.	Time	Source	Destination	Protocol	Length	Info
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=2.2&wrkey=AKEgNisc5aPgEBl…
11	1.274062	74.125.91.113	192.168.1.100	HTTP	853	HTTP/1.1 200 OK (application/vnd.google.safebrowsing-update)
13	1.528648	74.125.91.113	192.168.1.100	HTTP	853	[TCP Spurious Retransmission] HTTP/1.1 200 OK (application/vnd.google.safebrowsing-update)
20	1.572315	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	1.677779	74.125.106.31	192.168.1.100	HTTP	651	HTTP/1.1 200 OK (application/vnd.google.safebrowsing-chunk)
41	1.976996	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	2.000629	74.125.106.31	192.168.1.100	HTTP	881	HTTP/1.1 200 OK (application/vnd.google.safebrowsing-chunk)
43	2.014105	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	2.038247	74.125.106.31	192.168.1.100	HTTP	526	HTTP/1.1 200 OK (application/vnd.google.safebrowsing-chunk)
45	2.044751	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
46	2.064877	74.125.106.31	192.168.1.100	HTTP	1089	HTTP/1.1 200 OK (application/vnd.google.safebrowsing-chunk)
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/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswFzgDLCswGDgELCswGTgJLCswHTgZLCswJTjJiAEsKzA…
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)

Figure 1: 客户端 IP 地址

打开 NAT_home_side.pcap 文件，设置过滤器为 http，过滤结果如 Figure 1所示。其中，No.7 封包为客户端发送的请求消息，它的 Source 为 192.168.1.100；另外，No.11 封包为服务器回复给客户端的响应消息，它的 Destination 也是 192.168.1.100。因此，可以说明客户端的 IP 地址为 192.168.1.100。

2 问题 2

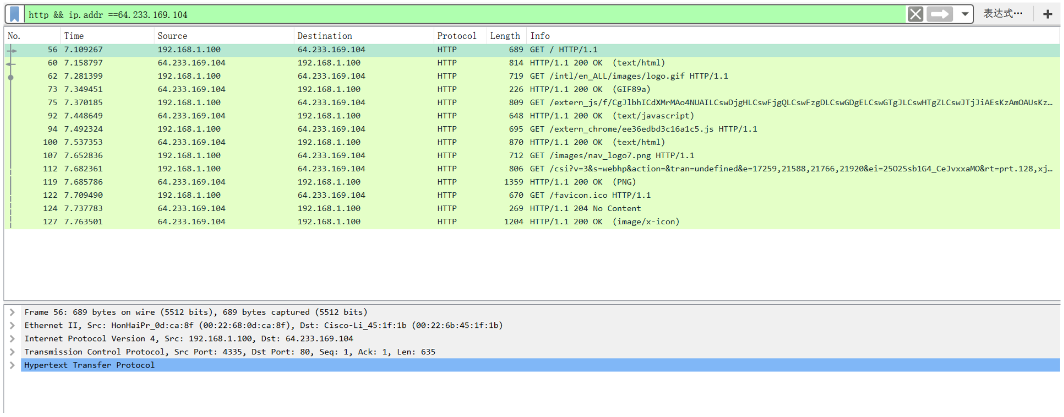
The client actually communicates with several different Google servers in order to implement “safe browsing.” (See extra credit section at the end of this lab). The main Google server that will serve up the main Google web page has IP address 64.233.169.104. In order to display only those frames containing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

2.1 Google 服务器发送或接收的 HTTP 消息

设置过滤器为 http && ip.addr==64.233.169.104，过滤结果如 Figure 2所示。

3 问题 3

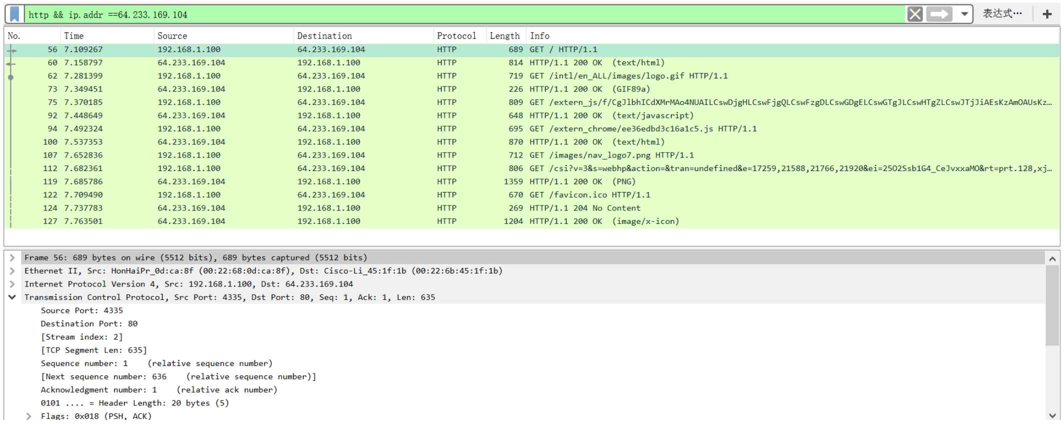
Consider now the HTTP GET sent from the client to the Google server (whose IP address is IP address 64.233.169.104) at time 7.109267. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?



```
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/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswFzgDLCswGDgELCswGTgJLCswHTgZLCswJTjJiAEsKzAmOAUsKz…
     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=25O2Ssb1G4_CeJvxxaMO&rt=prt.128,xj…
    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
    124 7.737783    64.233.169.104    192.168.1.100     HTTP       269  HTTP/1.1 204 No Content
    127 7.763501    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
```

Figure 2: 服务器发送或接收的 HTTP 消息

3.1 客户端在 7.109267 时发送给服务器的 HTTP GET 消息



```
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/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswFzgDLCswGDgELCswGTgJLCswHTgZLCswJTjJiAEsKzAmOAUsKz…
     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=25O2Ssb1G4_CeJvxxaMO&rt=prt.128,xj…
    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
    124 7.737783    64.233.169.104    192.168.1.100     HTTP       269  HTTP/1.1 204 No Content
    127 7.763501    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)
    [Next sequence number: 636    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
```

Figure 3: 客户端在 7.109267 时发送给服务器的 HTTP GET 消息

设置过滤器为 http && ip.addr==64.233.169.104，过滤结果如 Figure 3所示，可以知道，客户端在 7.109267 时发送给服务器的 HTTP GET 消息，就是 No.56 封包。如 Figure 3所示可以看到，IP 源地址为 192.168.1.100，IP 目的地址为 64.233.169.104。查看该封包的封包详细信息中的 TCP 部分，如 Figure 3所示，可以看到 TCP 源端口为 4335，TCP 目的端口为 80。

4 问题 4

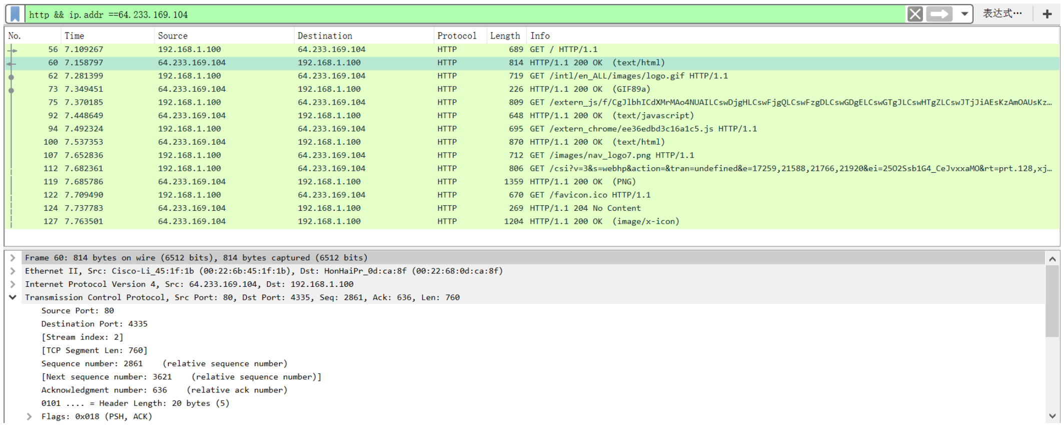
At what time is the corresponding 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

4.1 服务器回复的 HTTP 200 OK 消息

设置过滤器设置不变，服务器回复的 HTTP 200 OK 消息就是 No.60 封包，如 Figure 4所示。可以看到，时间戳是 7.158797，IP 源地址为 64.233.169.104，IP 目的地址为 192.168.1.100，TCP 源端口为 80，TCP 目的端口为 4335。

5 问题 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

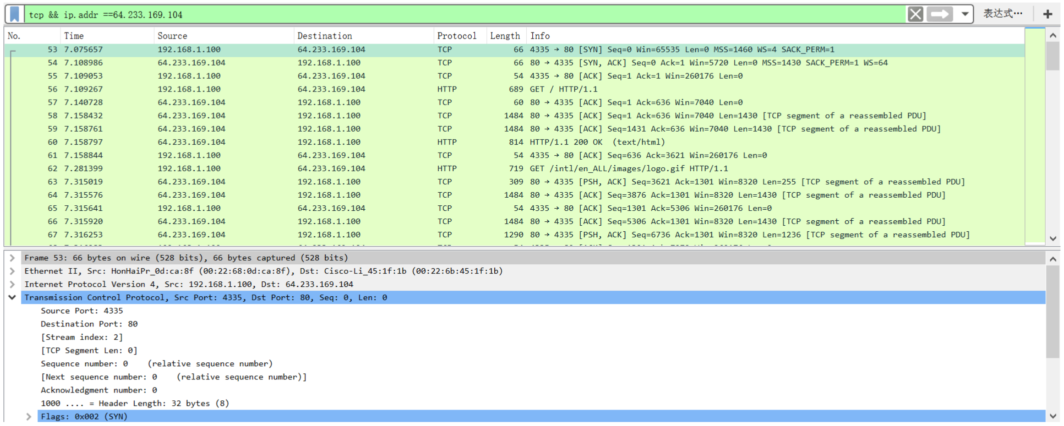


```
http && ip.addr ==64.233.169.104

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/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswFzgDLCswGDgELCswGTgJLCswHTgZLCswJTjJiAEsKzAmOAUsKz…
  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=2502Ssb1G4_CeJvxxaMO&rt=prt.128,xj…
 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
 124 7.737783  64.233.169.104  192.168.1.100   HTTP      269  HTTP/1.1 204 No Content
 127 7.763501  64.233.169.104  192.168.1.100   HTTP     1204  HTTP/1.1 200 OK  (image/x-icon)

> 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)
    [Next sequence number: 3621    (relative sequence number)]
    Acknowledgment number: 636    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
```

Figure 4: 服务器回复的 HTTP 200 OK 消息

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).

5.1 TCP 连接的三次握手过程分析



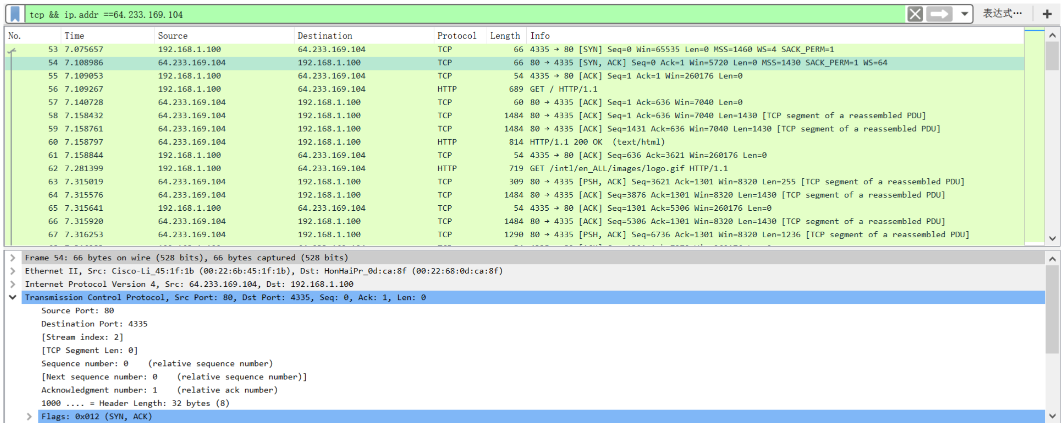
```
tcp && ip.addr ==64.233.169.104

No.  Time      Source          Destination     Protocol Length Info
  53 7.075657  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 7.108986  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_PERM=1 WS=64
  55 7.109053  192.168.1.100   64.233.169.104  TCP        54  4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
  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=636 Win=7040 Len=0
  58 7.158432  64.233.169.104  192.168.1.100   TCP      1484  80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=1430 [TCP segment of a reassembled PDU]
  59 7.158761  64.233.169.104  192.168.1.100   TCP      1484  80 → 4335 [ACK] Seq=1431 Ack=636 Win=7040 Len=1430 [TCP segment of a reassembled PDU]
  60 7.158797  64.233.169.104  192.168.1.100   HTTP      814  HTTP/1.1 200 OK  (text/html)
  61 7.158844  192.168.1.100   64.233.169.104  TCP        54  4335 → 80 [ACK] Seq=636 Ack=3621 Win=260176 Len=0
  62 7.281399  192.168.1.100   64.233.169.104  HTTP      719  GET /intl/en_ALL/images/logo.gif HTTP/1.1
  63 7.315019  64.233.169.104  192.168.1.100   TCP       309  80 → 4335 [PSH, ACK] Seq=3621 Ack=1301 Win=8320 Len=255 [TCP segment of a reassembled PDU]
  64 7.315576  64.233.169.104  192.168.1.100   TCP      1484  80 → 4335 [ACK] Seq=3876 Ack=1301 Win=8320 Len=1430 [TCP segment of a reassembled PDU]
  65 7.315641  192.168.1.100   64.233.169.104  TCP        54  4335 → 80 [ACK] Seq=1301 Ack=5306 Win=260176 Len=0
  66 7.315920  64.233.169.104  192.168.1.100   TCP      1484  80 → 4335 [ACK] Seq=5306 Ack=1301 Win=8320 Len=1430 [TCP segment of a reassembled PDU]
  67 7.316253  64.233.169.104  192.168.1.100   TCP      1290  80 → 4335 [PSH, ACK] Seq=6736 Ack=1301 Win=8320 Len=1236 [TCP segment of a reassembled PDU]

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

Figure 5: 建立 TCP 连接的 SYN 消息

为了找到 TCP 连接过程中传输的 TCP 消息，设置过滤器为 tcp && ip.addr==64.233.169.104，查看时间戳在 7.109267 之前的封包，可以找到建立 TCP 连接的三次握手对应的消息分别为 No.53、No.54、No.55 消息，如 Figure 5所示。

SYN 消息对应 No.53 封包，它的封包详细信息如 Figure 5所示。它的时间戳是 7.075657，IP 源地址为 192.168.1.100，IP 目的地址为 64.233.169.104，TCP 源端口为 4335，TCP 目的端口为 80。

回复上述 SYN 消息的 ACK 消息对应 No.54 封包，它的封包详细信息如 Figure 6所示。它的时间戳是 7.108986，IP 源地址为 64.233.169.104，IP 目的地址为 192.168.1.100，TCP 源端口为 80，TCP 目的端口为 4335。



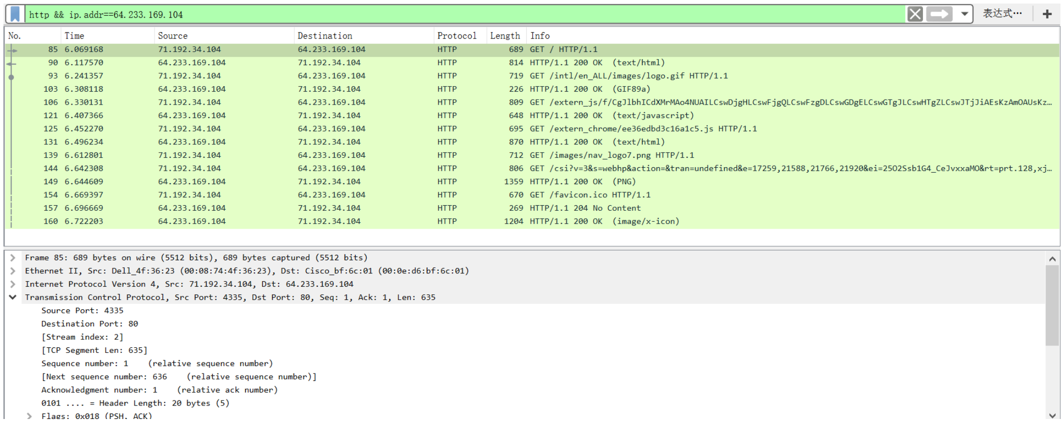
```
tcp && ip.addr ==64.233.169.104

No.   Time        Source           Destination      Protocol  Length  Info
   53 7.075657    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 7.108986    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_PERM=1 WS=64
   55 7.109053    192.168.1.100    64.233.169.104   TCP         54  4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
   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=636 Win=7040 Len=0
   58 7.158432    64.233.169.104   192.168.1.100    TCP       1484  80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=1430 [TCP segment of a reassembled PDU]
   59 7.158761    64.233.169.104   192.168.1.100    TCP       1484  80 → 4335 [ACK] Seq=1431 Ack=636 Win=7040 Len=1430 [TCP segment of a reassembled PDU]
   60 7.158797    64.233.169.104   192.168.1.100    HTTP       814  HTTP/1.1 200 OK  (text/html)
   61 7.158844    192.168.1.100    64.233.169.104   TCP         54  4335 → 80 [ACK] Seq=636 Ack=3621 Win=260176 Len=0
   62 7.281399    192.168.1.100    64.233.169.104   HTTP       719  GET /intl/en_ALL/images/logo.gif HTTP/1.1
   63 7.315019    64.233.169.104   192.168.1.100    TCP        309  80 → 4335 [PSH, ACK] Seq=3621 Ack=1301 Win=8320 Len=255 [TCP segment of a reassembled PDU]
   64 7.315576    64.233.169.104   192.168.1.100    TCP       1484  80 → 4335 [ACK] Seq=3876 Ack=1301 Win=8320 Len=1430 [TCP segment of a reassembled PDU]
   65 7.315641    192.168.1.100    64.233.169.104   TCP         54  4335 → 80 [ACK] Seq=1301 Ack=5306 Win=260176 Len=0
   66 7.315920    64.233.169.104   192.168.1.100    TCP       1484  80 → 4335 [ACK] Seq=5306 Ack=1301 Win=8320 Len=1430 [TCP segment of a reassembled PDU]
   67 7.316253    64.233.169.104   192.168.1.100    TCP       1290  80 → 4335 [PSH, ACK] Seq=6736 Ack=1301 Win=8320 Len=1236 [TCP segment of a reassembled PDU]

> 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)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x012 (SYN, ACK)
```

Figure 6: 回复 SYN 消息的 ACK 消息

6 问题 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?

6.1 客户端在 7.109267 时发送给服务器的 HTTP GET 消息



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

No.   Time        Source           Destination      Protocol  Length  Info
   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/logo.gif HTTP/1.1
  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/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswFzgDLCswGDgELCswGTgJLCswHTgZLCswJTjJiAEsKzAmOAUsKz…
  121 6.407366    64.233.169.104   71.192.34.104    HTTP       648  HTTP/1.1 200 OK  (text/javascript)
  125 6.452270    71.192.34.104    64.233.169.104   HTTP       695  GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.1
  131 6.496234    64.233.169.104   71.192.34.104    HTTP       870  HTTP/1.1 200 OK  (text/html)
  139 6.612801    71.192.34.104    64.233.169.104   HTTP       712  GET /images/nav_logo7.png HTTP/1.1
  144 6.642308    71.192.34.104    64.233.169.104   HTTP       806  GET /csi?v=3&s=webhp&action=&tran=undefined&e=17259,21588,21766,21920&ei=2502Ssb1G4_CeJvxxaMO&rt=prt.128,xj…
  149 6.644609    64.233.169.104   71.192.34.104    HTTP      1359  HTTP/1.1 200 OK  (PNG)
  154 6.669397    71.192.34.104    64.233.169.104   HTTP       670  GET /favicon.ico HTTP/1.1
  157 6.696669    64.233.169.104   71.192.34.104    HTTP       269  HTTP/1.1 204 No Content
  160 6.722203    64.233.169.104   71.192.34.104    HTTP      1204  HTTP/1.1 200 OK  (image/x-icon)

> 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)
    [Next sequence number: 636    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
```

Figure 7: 客户端在 7.109267 时发送给服务器的 HTTP GET 消息

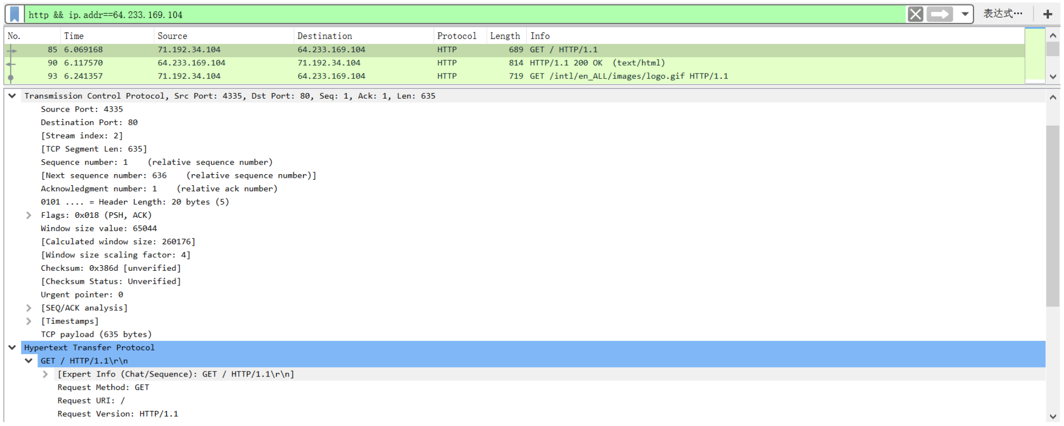
设置过滤器为 http && ip.addr==64.233.169.104，过滤结果如 Figure 7所示，从中寻找发送给服务器的 HTTP GET 消息，可以找到 No.85 封包，也就是客户端在 7.109267 时发送给服务器的 HTTP GET 消息。如 Figure 7所示，时间戳为 6.069168，IP 源地址为 71.192.34.104，IP 目的地址为 64.233.169.104，TCP 源端口为 4335，TCP 目的端口为 80。

和问题3的答案相比，时间戳、IP 源地址是不同的，而 IP 目的地址、TCP 源端口、TCP 目的端口是相同的。

7 问题 7

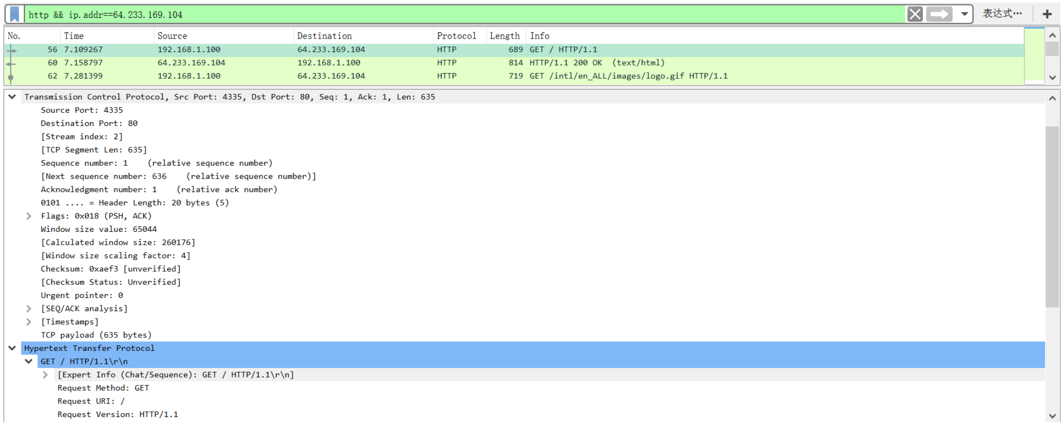
Are any fields in the HTTP GET message changed? Which of the following fields in the IP datagram carrying the HTTP GET are changed: Version, Header Length , Flags , Checksum . If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change.

7.1 NAT 两端的 HTTP GET 消息对比



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

No.   Time      Source          Destination     Protocol Length Info
   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/logo.gif HTTP/1.1

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)
    [Next sequence number: 636    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window size value: 65044
    [Calculated window size: 260176]
    [Window size scaling factor: 4]
    Checksum: 0x386d [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (635 bytes)
v Hypertext Transfer Protocol
  v GET / HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
```

Figure 8: NAT_home_side.pcap 文件的 HTTP GET 消息



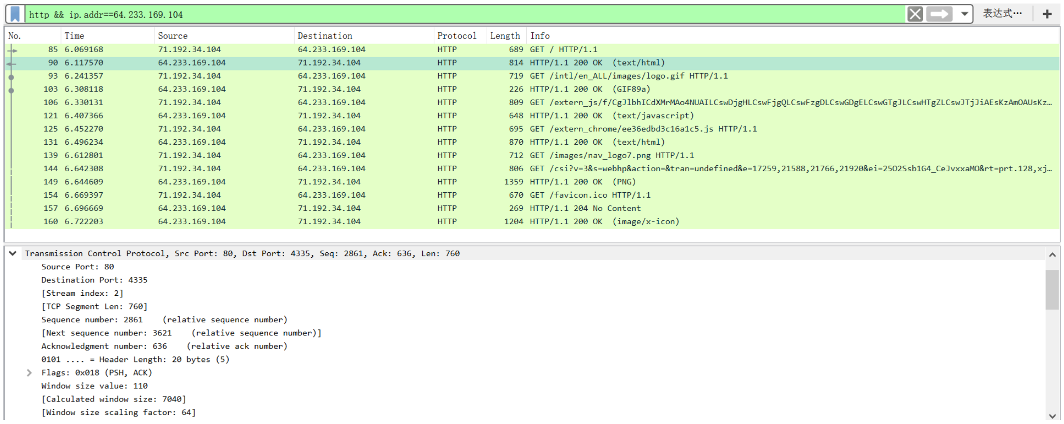
```
http && ip.addr==64.233.169.104

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

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)
    [Next sequence number: 636    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window size value: 65044
    [Calculated window size: 260176]
    [Window size scaling factor: 4]
    Checksum: 0xaef3 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (635 bytes)
v Hypertext Transfer Protocol
  v GET / HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
```

Figure 9: NAT_ISP_side.pcap 文件的 HTTP GET 消息

NAT_home_side.pcap 文件的 HTTP GET 消息如 Figure 8所示，为图中的 No.85 封包，其对应 NAT_ISP_side.pcap 文件中的 HTTP GET 消息如 Figure 9所示，为图中的 No.56 封包。可以看到 Version、Header Length、Flags 都是相同的。不同的只有 Checksum 字段，前者是 0x386d，而后者是 0xaef3，这是因为两者的 IP 源地址不同，因此校验和 Checksum 也会不同。

8 问题 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?



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

No.     Time        Source            Destination       Protocol  Length  Info
     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/logo.gif HTTP/1.1
    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/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswFzgDLCswGDgELCswGTgJLCswHTgZLCswJTjJiAEsKzAmOAUsKz…
    121 6.407366    64.233.169.104    71.192.34.104     HTTP         648  HTTP/1.1 200 OK  (text/javascript)
    125 6.452270    71.192.34.104     64.233.169.104    HTTP         695  GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.1
    131 6.496234    64.233.169.104    71.192.34.104     HTTP         870  HTTP/1.1 200 OK  (text/html)
    139 6.612801    71.192.34.104     64.233.169.104    HTTP         712  GET /images/nav_logo7.png HTTP/1.1
    144 6.642308    71.192.34.104     64.233.169.104    HTTP         806  GET /csi?v=3&s=webhp&action=&tran=undefined&e=17259,21588,21766,21920&ei=25O2Ssb1G4_CeJvxxaMO&rt=prt.128,xj…
    149 6.644609    64.233.169.104    71.192.34.104     HTTP        1359  HTTP/1.1 200 OK  (PNG)
    154 6.669397    71.192.34.104     64.233.169.104    HTTP         670  GET /favicon.ico HTTP/1.1
    157 6.696669    64.233.169.104    71.192.34.104     HTTP         269  HTTP/1.1 204 No Content
    160 6.722203    64.233.169.104    71.192.34.104     HTTP        1204  HTTP/1.1 200 OK  (image/x-icon)

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)
    [Next sequence number: 3621    (relative sequence number)]
    Acknowledgment number: 636    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window size value: 110
    [Calculated window size: 7040]
    [Window size scaling factor: 64]
```

Figure 10: 服务器回复的 HTTP 200 OK 消息

8.1 NAT 两端的 HTTP 200 OK 消息对比

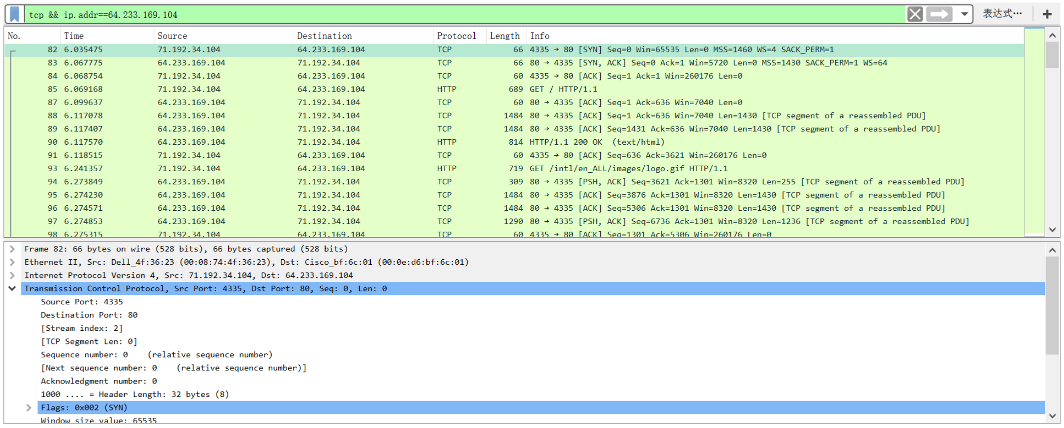
设置过滤器设置不变，服务器回复的 HTTP 200 OK 消息就是 No.90 封包，如 Figure 10所示。可以看到，时间戳是 6.117570，IP 源地址为 64.233.169.104，IP 目的地址为 71.192.34.104，TCP 源端口为 80，TCP 目的端口为 4335。

和问题4的答案相比，时间戳、IP 目的地址是不同的，而 IP 源地址、TCP 源端口、TCP 目的端口是相同的。

9 问题 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?

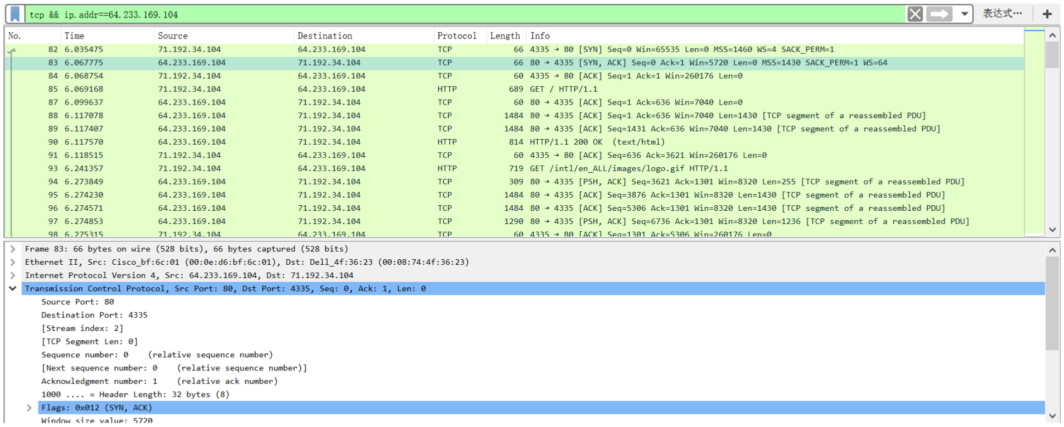
9.1 TCP 连接的三次握手过程分析



```
tcp && ip.addr==64.233.169.104

No.     Time        Source            Destination       Protocol  Length  Info
     82 6.035475    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 6.067775    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_PERM=1 WS=64
     84 6.068754    71.192.34.104     64.233.169.104    TCP           60  4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
     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=636 Win=7040 Len=0
     88 6.117078    64.233.169.104    71.192.34.104     TCP         1484  80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=1430 [TCP segment of a reassembled PDU]
     89 6.117407    64.233.169.104    71.192.34.104     TCP         1484  80 → 4335 [ACK] Seq=1431 Ack=636 Win=7040 Len=1430 [TCP segment of a reassembled PDU]
     90 6.117570    64.233.169.104    71.192.34.104     HTTP         814  HTTP/1.1 200 OK  (text/html)
     91 6.118515    71.192.34.104     64.233.169.104    TCP           60  4335 → 80 [ACK] Seq=636 Ack=3621 Win=260176 Len=0
     93 6.241357    71.192.34.104     64.233.169.104    HTTP         719  GET /intl/en_ALL/images/logo.gif HTTP/1.1
     94 6.273849    64.233.169.104    71.192.34.104     TCP          309  80 → 4335 [PSH, ACK] Seq=3621 Ack=1301 Win=8320 Len=255 [TCP segment of a reassembled PDU]
     95 6.274230    64.233.169.104    71.192.34.104     TCP         1484  80 → 4335 [ACK] Seq=3876 Ack=1301 Win=8320 Len=1430 [TCP segment of a reassembled PDU]
     96 6.274571    64.233.169.104    71.192.34.104     TCP         1484  80 → 4335 [ACK] Seq=5306 Ack=1301 Win=8320 Len=1430 [TCP segment of a reassembled PDU]
     97 6.274853    64.233.169.104    71.192.34.104     TCP         1290  80 → 4335 [PSH, ACK] Seq=6736 Ack=1301 Win=8320 Len=1236 [TCP segment of a reassembled PDU]
     98 6.275315    71.192.34.104     64.233.169.104    TCP           60  4335 → 80 [ACK] Seq=1301 Ack=5306 Win=260176 Len=0

> 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)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 0
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
    Window size value: 65535
```

Figure 11: 建立 TCP 连接的 SYN 消息

为了找到 TCP 连接过程中传输的 TCP 消息，设置过滤器为 tcp && ip.addr==64.233.169.104，查看时间戳在 6.117570 之前的封包，可以找到建立 TCP 连接的三次握手对应的消息分别为 No.82、No.83、No.84 消息，如 Figure 11所示。



```
tcp && ip.addr==64.233.169.104                                                                      表达式…  +
No.   Time        Source            Destination       Protocol  Length  Info
   82 6.035475    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 6.067775    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_PERM=1 WS=64
   84 6.068754    71.192.34.104     64.233.169.104    TCP           60  4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
   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=636 Win=7040 Len=0
   88 6.117078    64.233.169.104    71.192.34.104     TCP         1484  80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=1430 [TCP segment of a reassembled PDU]
   89 6.117407    64.233.169.104    71.192.34.104     TCP         1484  80 → 4335 [ACK] Seq=1431 Ack=636 Win=7040 Len=1430 [TCP segment of a reassembled PDU]
   90 6.117570    64.233.169.104    71.192.34.104     HTTP         814  HTTP/1.1 200 OK  (text/html)
   91 6.118515    71.192.34.104     64.233.169.104    TCP           60  4335 → 80 [ACK] Seq=636 Ack=3621 Win=260176 Len=0
   93 6.241357    71.192.34.104     64.233.169.104    HTTP         719  GET /intl/en_ALL/images/logo.gif HTTP/1.1
   94 6.273849    64.233.169.104    71.192.34.104     TCP          309  80 → 4335 [PSH, ACK] Seq=3621 Ack=1301 Win=8320 Len=255 [TCP segment of a reassembled PDU]
   95 6.274230    64.233.169.104    71.192.34.104     TCP         1484  80 → 4335 [ACK] Seq=3876 Ack=1301 Win=8320 Len=1430 [TCP segment of a reassembled PDU]
   96 6.274571    64.233.169.104    71.192.34.104     TCP         1484  80 → 4335 [ACK] Seq=5306 Ack=1301 Win=8320 Len=1430 [TCP segment of a reassembled PDU]
   97 6.274853    64.233.169.104    71.192.34.104     TCP         1290  80 → 4335 [PSH, ACK] Seq=6736 Ack=1301 Win=8320 Len=1236 [TCP segment of a reassembled PDU]
   98 6.275315    71.192.34.104     64.233.169.104    TCP           60  4335 → 80 [ACK] Seq=1301 Ack=5306 Win=260176 Len=0

> 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)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x012 (SYN, ACK)
    Window size value: 5720
```

Figure 12: 回复 SYN 消息的 ACK 消息

SYN 消息对应 No.82 封包，它的封包详细信息如 Figure 11所示。它的时间戳是 6.035475，IP 源地址为 71.192.34.104，IP 目的地址为 64.233.169.104，TCP 源端口为 4335，TCP 目的端口为 80。

和问题5的答案相比，时间戳、IP 源地址是不同的，而 IP 目的地址、TCP 源端口、TCP 目的端口是相同的。

回复上述 SYN 消息的 ACK 消息对应 No.83 封包，它的封包详细信息如 Figure 12所示。它的时间戳是 6.067775，IP 源地址为 64.233.169.104，IP 目的地址为 71.192.34.104，TCP 源端口为 80，TCP 目的端口为 4335。

和问题5的答案相比，时间戳、IP 目的地址是不同的，而 IP 源地址、TCP 源端口、TCP 目的端口是相同的。