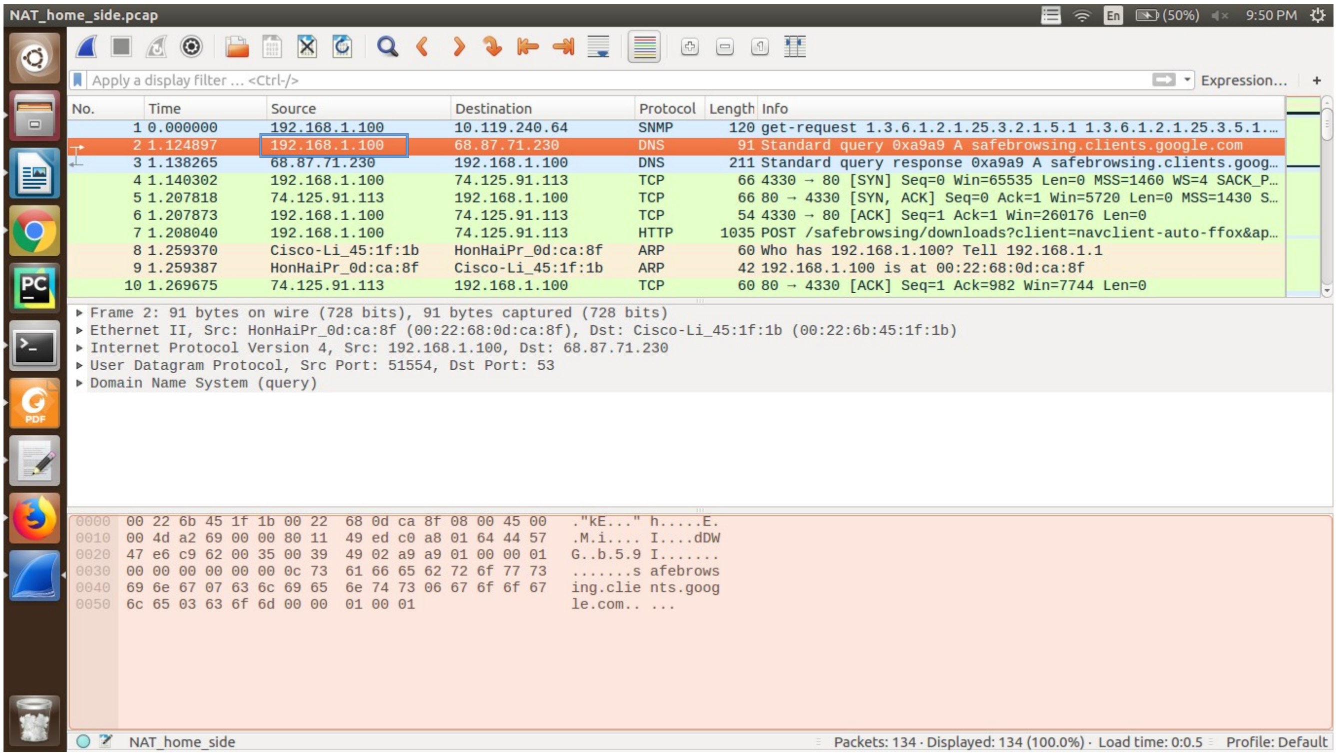
1. What is the IP address of the client?
Ans : IP address of the given client is 192.168.1.100



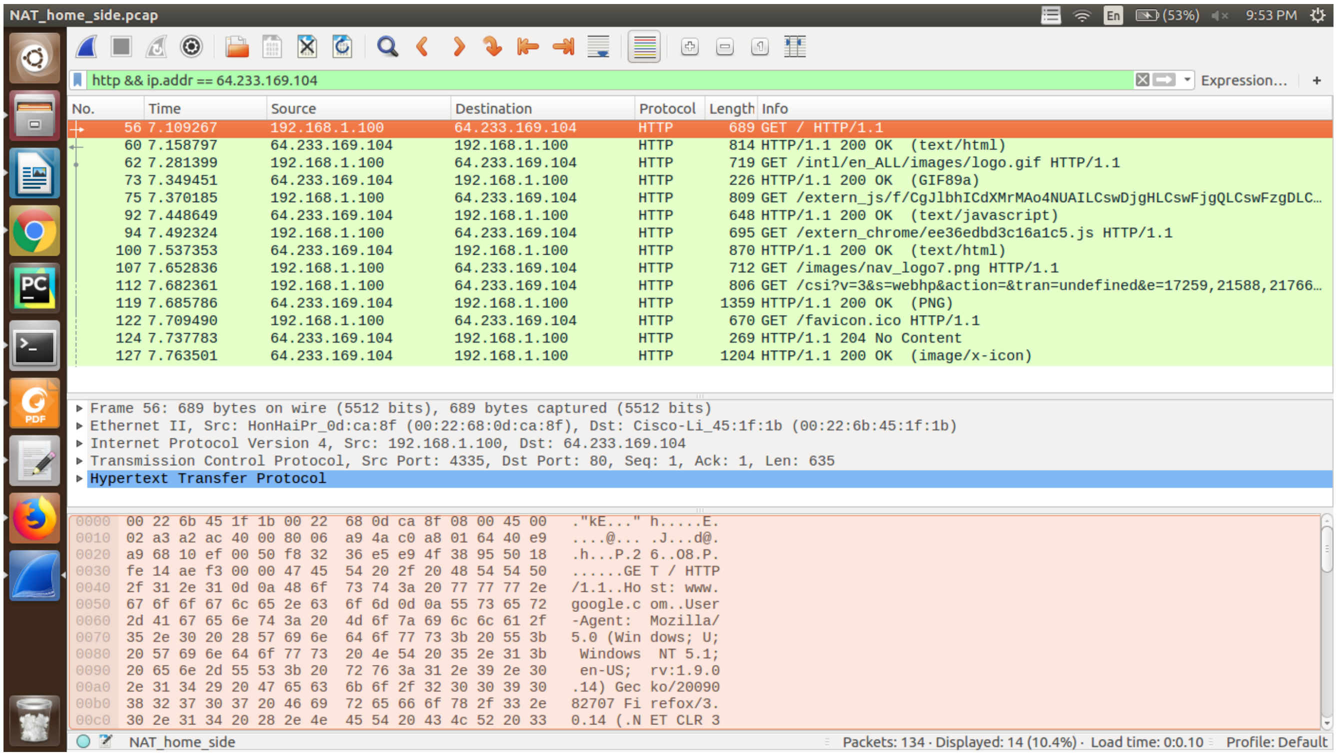
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.100	10.119.240.64	SNMP	120	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.…
2	1.124897	192.168.1.100	68.87.71.230	DNS	91	Standard query 0xa9a9 A safebrowsing.clients.google.com
3	1.138265	68.87.71.230	192.168.1.100	DNS	211	Standard query response 0xa9a9 A safebrowsing.clients.goog…
4	1.140302	192.168.1.100	74.125.91.113	TCP	66	4330 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_P…
5	1.207818	74.125.91.113	192.168.1.100	TCP	66	80 → 4330 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 S…
6	1.207873	192.168.1.100	74.125.91.113	TCP	54	4330 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
7	1.208040	192.168.1.100	74.125.91.113	HTTP	1035	POST /safebrowsing/downloads?client=navclient-auto-ffox&ap…
8	1.259370	Cisco-Li_45:1f:1b	HonHaiPr_0d:ca:8f	ARP	60	Who has 192.168.1.100? Tell 192.168.1.1
9	1.259387	HonHaiPr_0d:ca:8f	Cisco-Li_45:1f:1b	ARP	42	192.168.1.100 is at 00:22:68:0d:ca:8f
10	1.269675	74.125.91.113	192.168.1.100	TCP	60	80 → 4330 [ACK] Seq=1 Ack=982 Win=7744 Len=0

```
▸ Frame 2: 91 bytes on wire (728 bits), 91 bytes captured (728 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: 68.87.71.230
▸ User Datagram Protocol, Src Port: 51554, Dst Port: 53
▸ Domain Name System (query)
```

```
0000  00 22 6b 45 1f 1b 00 22  68 0d ca 8f 08 00 45 00   ."kE..." h.....E.
0010  00 4d a2 69 00 00 80 11  49 ed c0 a8 01 64 44 57   .M.i.... I....dDW
0020  47 e6 c9 62 00 35 00 39  49 02 a9 a9 01 00 00 01   G..b.5.9 I.......
0030  00 00 00 00 00 00 0c 73  61 66 65 62 72 6f 77 73   .......s afebrows
0040  69 6e 67 07 63 6c 69 65  6e 74 73 06 67 6f 6f 67   ing.clie nts.goog
0050  6c 65 03 63 6f 6d 00 00  01 00 01                  le.com.. ...
```

NAT_home_side Packets: 134 · Displayed: 134 (100.0%) · Load time: 0:0.5 Profile: Default

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 .
Ans: The highlighted region represents all the HTTP request sent from client to google server with IP address 64.233.169.104



```
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/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswFzgDLC…
   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…
  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
```

```
0000  00 22 6b 45 1f 1b 00 22  68 0d ca 8f 08 00 45 00   ."kE..." h.....E.
0010  02 a3 a2 ac 40 00 80 06  a9 4a c0 a8 01 64 40 e9   ....@... .J...d@.
0020  a9 68 10 ef 00 50 f8 32  36 e5 e9 4f 38 95 50 18   .h...P.2 6..O8.P.
0030  fe 14 ae f3 00 00 47 45  54 20 2f 20 48 54 54 50   ......GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   /1.1..Ho st: www.
0050  67 6f 6f 67 6c 65 2e 63  6f 6d 0d 0a 55 73 65 72   google.c om..User
0060  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
0070  35 2e 30 20 28 57 69 6e  64 6f 77 73 3b 20 55 3b   5.0 (Win dows; U;
0080  20 57 69 6e 64 6f 77 73  20 4e 54 20 35 2e 31 3b    Windows  NT 5.1;
0090  20 65 6e 2d 55 53 3b 20  72 76 3a 31 2e 39 2e 30    en-US;  rv:1.9.0
00a0  2e 31 34 29 20 47 65 63  6b 6f 2f 32 30 30 39 30   .14) Gec ko/20090
00b0  38 32 37 30 37 20 46 69  72 65 66 6f 78 2f 33 2e   82707 Fi refox/3.
00c0  30 2e 31 34 20 28 2e 4e  45 54 20 43 4c 52 20 33   0.14 (.N ET CLR 3
```

```
Packets: 134 · Displayed: 14 (10.4%) · Load time: 0:0.10    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 7.109267. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?

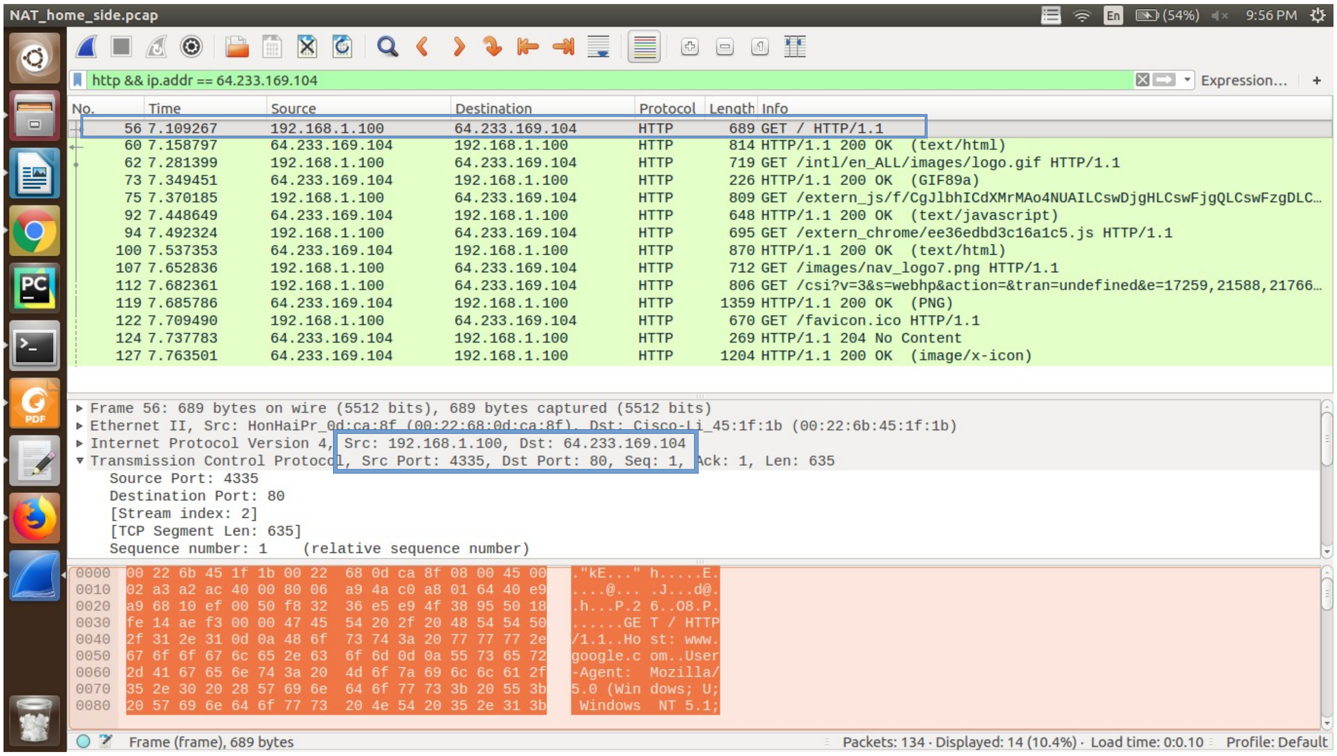
Ans: Answer:

a) Source IP Address: 192.168.1.100

b) Source Port: 4335

c) Destination IP address: 64.233.169.104

d) Destination Port: 80



NAT_home_side.pcap

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/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswFzgDLC…
   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…
  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
    Source Port: 4335
    Destination Port: 80
    [Stream index: 2]
    [TCP Segment Len: 635]
    Sequence number: 1    (relative sequence number)
```

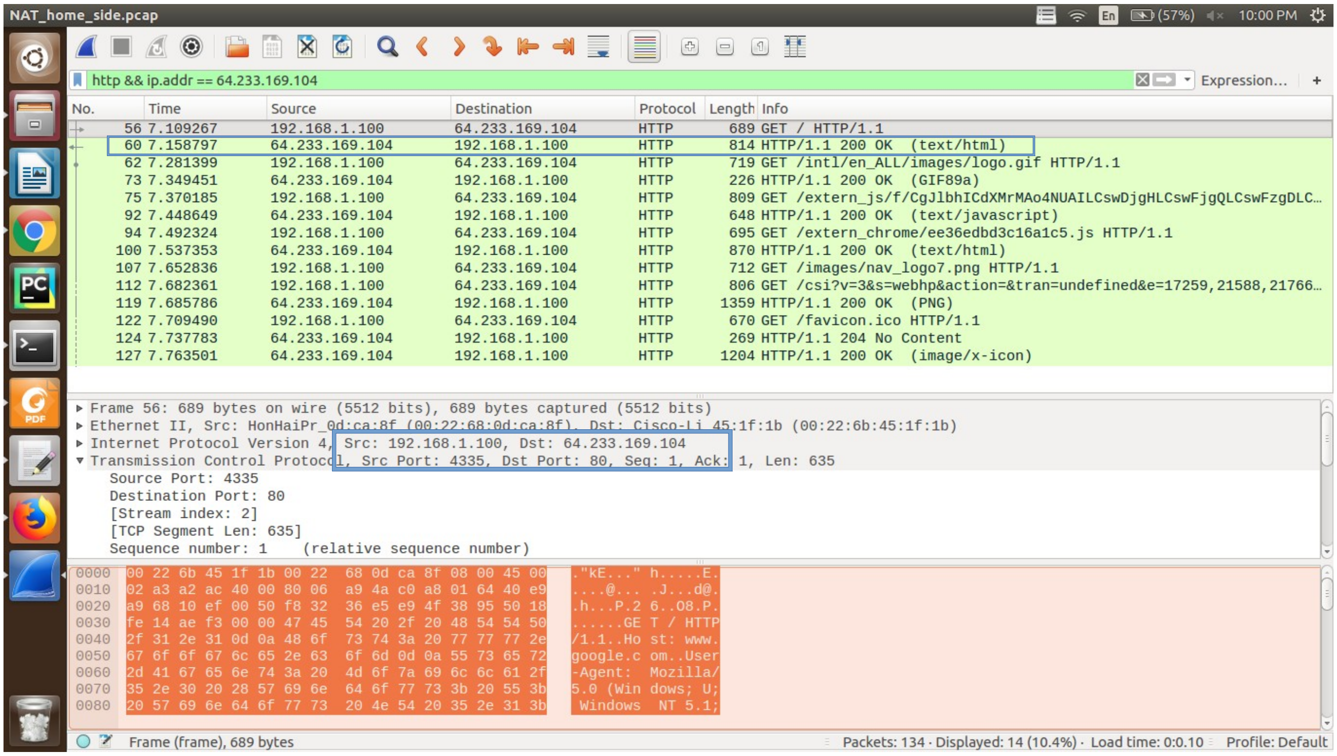
```
0000  00 22 6b 45 1f 1b 00 22  68 0d ca 8f 08 00 45 00   ."kE..." h.....E.
0010  02 a3 a2 ac 40 00 80 06  a9 4a c0 a8 01 64 40 e9   ....@... .J...d@.
0020  a9 68 10 ef 00 50 f8 32  36 e5 e9 4f 38 95 50 18   .h...P.2 6..O8.P.
0030  fe 14 ae f3 00 00 47 45  54 20 2f 20 48 54 54 50   ......GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   /1.1..Ho st: www.
0050  67 6f 6f 67 6c 65 2e 63  6f 6d 0d 0a 55 73 65 72   google.c om..User
0060  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
0070  35 2e 30 20 28 57 69 6e  64 6f 77 73 3b 20 55 3b   5.0 (Win dows; U;
0080  20 57 69 6e 64 6f 77 73  20 4e 54 20 35 2e 31 3b    Windows  NT 5.1;
```

Frame (frame), 689 bytes   Packets: 134 · Displayed: 14 (10.4%) · Load time: 0:0.10   Profile: Default

4. At what time4 is the corresponding 200 OK HTTP message received from theGoogle 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: **Time at which 200 OK was received: 7.158797 seconds**

a) Source IP of the IP datagram: 64.233.169.104
b) Source Port of the IP datagram: 80
c) Destination IP of the IP datagram: 192.168.1.100
d) Destination port of the IP Datagram: 4335



```
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/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswFzgDLC…
   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…
  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
    Source Port: 4335
    Destination Port: 80
    [Stream index: 2]
    [TCP Segment Len: 635]
    Sequence number: 1    (relative sequence number)
```

```
0000  00 22 6b 45 1f 1b 00 22  68 0d ca 8f 08 00 45 00   ."kE..." h.....E.
0010  02 a3 a2 ac 40 00 80 06  a9 4a c0 a8 01 64 40 e9   ....@... .J...d@.
0020  a9 68 10 ef 00 50 f8 32  36 e5 e9 4f 38 95 50 18   .h...P.2 6..O8.P.
0030  fe 14 ae f3 00 00 47 45  54 20 2f 20 48 54 54 50   ......GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   /1.1..Ho st: www.
0050  67 6f 6f 67 6c 65 2e 63  6f 6d 0d 0a 55 73 65 72   google.c om..User
0060  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
0070  35 2e 30 20 28 57 69 6e  64 6f 77 73 3b 20 55 3b   5.0 (Win dows; U;
0080  20 57 69 6e 64 6f 77 73  20 4e 54 20 35 2e 31 3b    Windows  NT 5.1;
```

```
Frame (frame), 689 bytes          Packets: 134 · Displayed: 14 (10.4%) · Load time: 0:0.10     Profile: Default
```

5. Recall that before a GET command can be sent to an HTTP server, TCP must first set up a connection using the three-way SYN/ACK handshake. At what time is the client-to-server TCP SYN segment sent that sets up the connection used by the GET sent at time 7.109267? What are the source and destination IP addresses and source and destination ports for the TCP SYN segment? What are the source and destination IP addresses and source and destination ports of the ACK sent in response to the SYN. At what time is this ACK received at the client?

Ans: Time at which SYN segment was sent from client to server: 7.075657 seconds

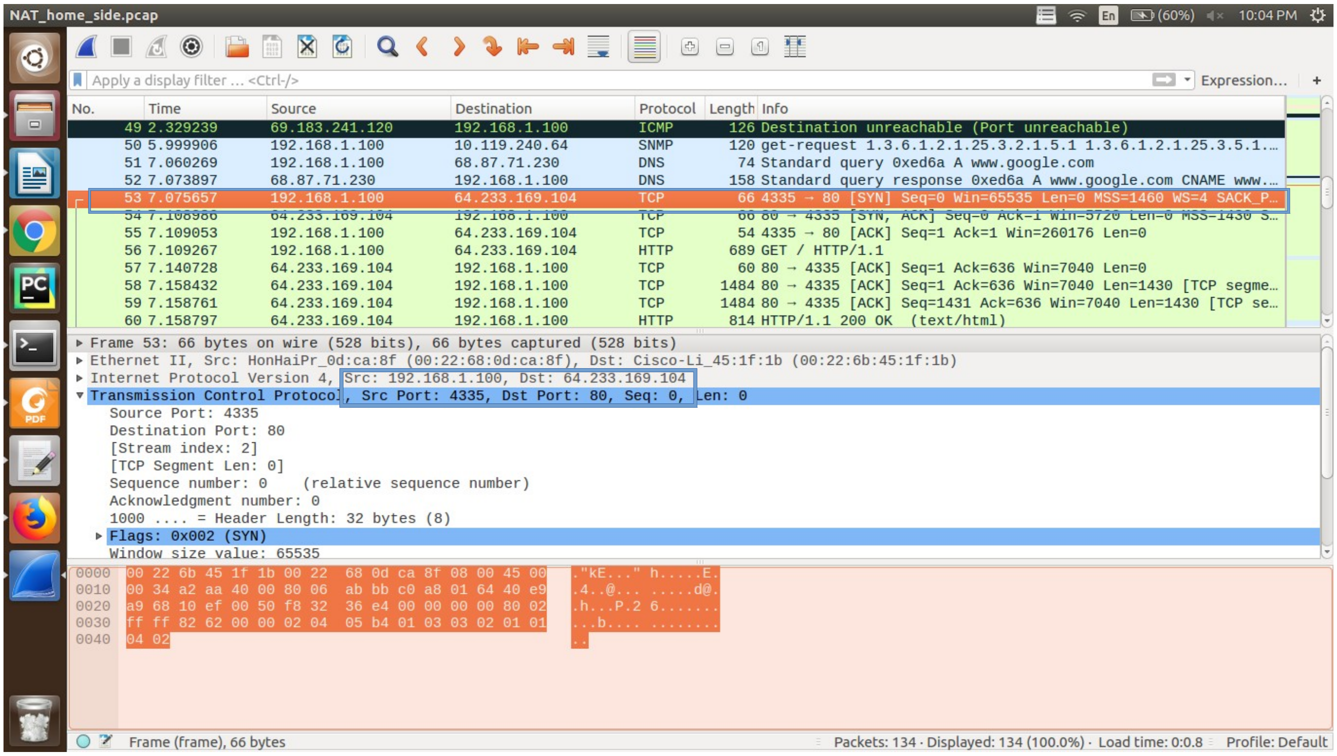
a) Source IP Address: 192.168.1.100
b) Source Port: 4335
c) Destination IP address: 64.233.169.104
d) Destination Port: 80

Time at which ACK segment was received: 7.108986 seconds

a) Source IP of the IP datagram: 64.233.169.104
b) Source Port of the IP datagram: 80
c) Destination IP of the IP datagram: 192.168.1.100

d) Destination port of the IP Datagram: 4335

Below image displays when the SYN segment sent from client to google server and it highlights the source and destination IP and ports



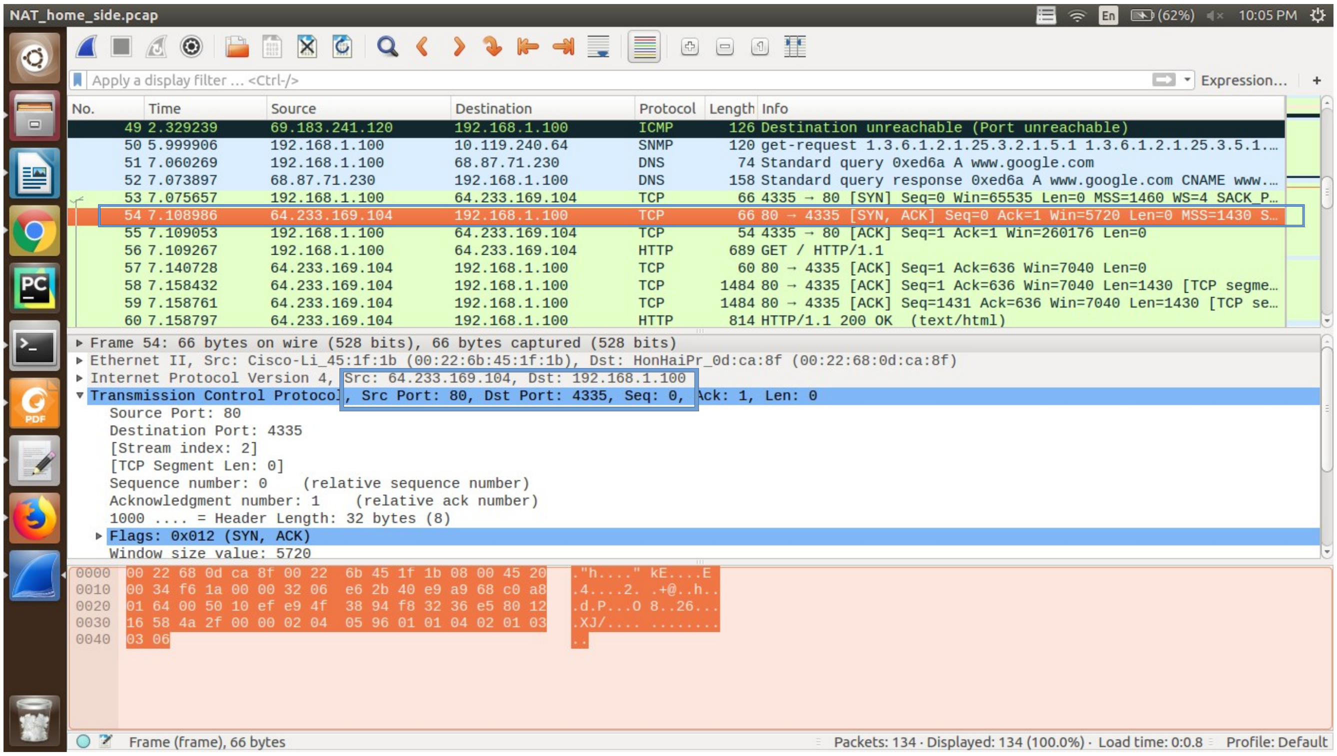
```
No.  Time      Source           Destination      Protocol Length Info
  49 2.329239  69.183.241.120   192.168.1.100    ICMP      126 Destination unreachable (Port unreachable)
  50 5.999906  192.168.1.100    10.119.240.64    SNMP      120 get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.…
  51 7.060269  192.168.1.100    68.87.71.230     DNS        74 Standard query 0xed6a A www.google.com
  52 7.073897  68.87.71.230     192.168.1.100    DNS       158 Standard query response 0xed6a A www.google.com CNAME www.…
  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_P…
  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 S…
  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 segme…
  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 se…
  60 7.158797  64.233.169.104   192.168.1.100    HTTP      814 HTTP/1.1 200 OK  (text/html)
```

```
▸ Frame 53: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▸ Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
▸ Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104
▾ 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)
    Acknowledgment number: 0
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x002 (SYN)
    Window size value: 65535
```

```
0000  00 22 6b 45 1f 1b 00 22  68 0d ca 8f 08 00 45 00   ."kE..." h.....E.
0010  00 34 a2 aa 40 00 80 06  ab bb c0 a8 01 64 40 e9   .4..@... .....d@.
0020  a9 68 10 ef 00 50 f8 32  36 e4 00 00 00 00 80 02   .h...P.2 6.......
0030  ff ff 82 62 00 00 02 04  05 b4 01 03 03 02 01 01   ...b.... ........
0040  04 02                                              ..
```

```
Frame (frame), 66 bytes          Packets: 134 · Displayed: 134 (100.0%) · Load time: 0:0.8   Profile: Default
```

Below image displays when the ACK segment sent from client to google server and it highlights the source and destination IP and ports



```
No.  Time      Source           Destination      Protocol Length Info
  49 2.329239  69.183.241.120   192.168.1.100    ICMP      126 Destination unreachable (Port unreachable)
  50 5.999906  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.…
  51 7.060269  192.168.1.100    68.87.71.230     DNS        74 Standard query 0xed6a A www.google.com
  52 7.073897  68.87.71.230     192.168.1.100    DNS       158 Standard query response 0xed6a A www.google.com CNAME www.…
  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_P…
  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 S…
  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 segme…
  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 se…
  60 7.158797  64.233.169.104   192.168.1.100    HTTP      814 HTTP/1.1 200 OK  (text/html)
```

```
▸ 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
▾ 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)
    Acknowledgment number: 1    (relative ack number)
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x012 (SYN, ACK)
    Window size value: 5720
```

```
0000  00 22 68 0d ca 8f 00 22  6b 45 1f 1b 08 00 45 20   ."h...." kE....E
0010  00 34 f6 1a 00 00 32 06  e6 2b 40 e9 a9 68 c0 a8   .4....2. .+@..h..
0020  01 64 00 50 10 ef e9 4f  38 94 f8 32 36 e5 80 12   .d.P...O 8..26...
0030  16 58 4a 2f 00 00 02 04  05 96 01 01 04 02 01 03   .XJ/.... ........
0040  03 06                                              ..
```

```
Frame (frame), 66 bytes          Packets: 134 · Displayed: 134 (100.0%) · Load time: 0:0.8   Profile: Default
```

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?

Ans: The GET request appear in the NAT_IS_side trace file appear at : 6.069168000 seconds

a) Source IP: 71.192.34.104

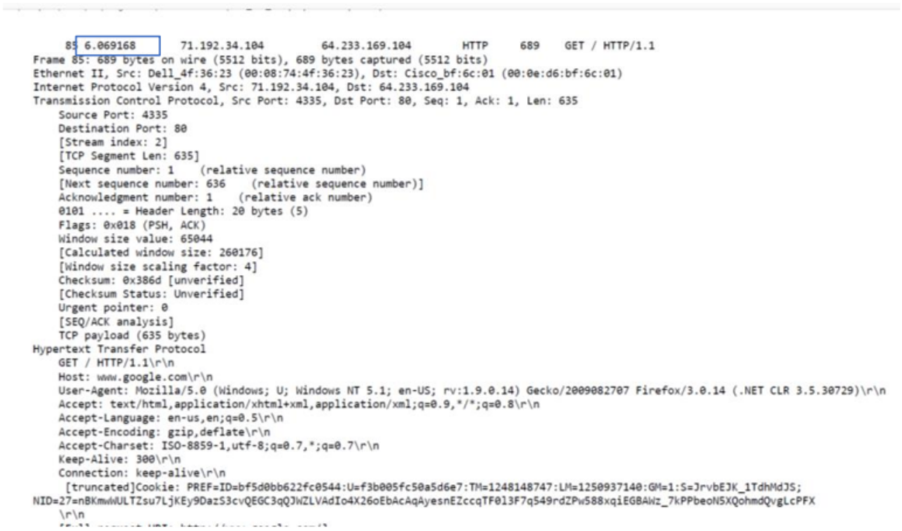
b) Source Port: 4335

c) Destination IP: 64.233.169.104

d) Destination Port: 80

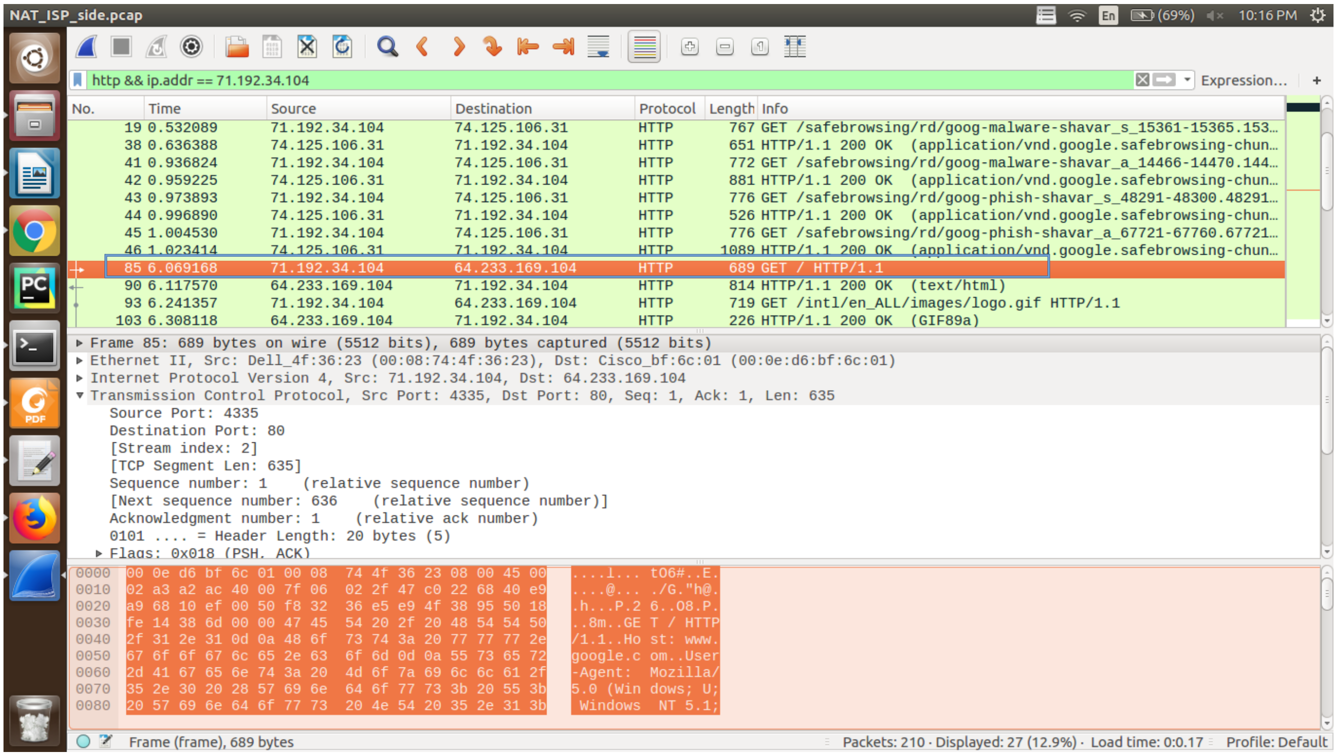
Fields that are same as compared to qns 3 are Source Port, Destination IP, Destination Port.

Fileds that is different as compared to qns 3 is Source IP.



```
     85 6.069168       71.192.34.104        64.233.169.104       HTTP     689    GET / HTTP/1.1
Frame 85: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)
Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01)
Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104
Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
    Source Port: 4335
    Destination Port: 80
    [Stream index: 2]
    [TCP Segment Len: 635]
    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]
    TCP payload (635 bytes)
Hypertext Transfer Protocol
    GET / HTTP/1.1\r\n
    Host: www.google.com\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.14) Gecko/2009082707 Firefox/3.0.14 (.NET CLR 3.5.30729)\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
     [truncated]Cookie: PREF=ID=bf5d0bb622fc0544:U=f3b005fc50a5d6e7:TM=1248148747:LM=1250937140:GM=1:S=JrvbEJK_1TdhMdJS;
NID=27=nBKmwWULTZsu7LjKEy9DazS3cvQEGC3qQJWZLVAdIo4X26oEbAcAqAyesnEZccqTF013F7q549rdZPw588xqiEGBAWz_7kPPbeoN5XQohmdQvgLcPFX
    \r\n
```

Below given images displayed the time at which the message appeared in the ISP side trace file.



```
http && ip.addr == 71.192.34.104
```

```
No.  Time      Source           Destination      Protocol Length Info
  19 0.532089  71.192.34.104    74.125.106.31    HTTP      767 GET /safebrowsing/rd/goog-malware-shavar_s_15361-15365.153…
  38 0.636388  74.125.106.31    71.192.34.104    HTTP      651 HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-chun…
  41 0.936824  71.192.34.104    74.125.106.31    HTTP      772 GET /safebrowsing/rd/goog-malware-shavar_a_14466-14470.144…
  42 0.959225  74.125.106.31    71.192.34.104    HTTP      881 HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-chun…
  43 0.973893  71.192.34.104    74.125.106.31    HTTP      776 GET /safebrowsing/rd/goog-phish-shavar_s_48291-48300.48291…
  44 0.996890  74.125.106.31    71.192.34.104    HTTP      526 HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-chun…
  45 1.004530  71.192.34.104    74.125.106.31    HTTP      776 GET /safebrowsing/rd/goog-phish-shavar_a_67721-67760.67721…
  46 1.023414  74.125.106.31    71.192.34.104    HTTP     1089 HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-chun…
  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)
```

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

```
0000  00 0e d6 bf 6c 01 00 08  74 4f 36 23 08 00 45 00   ....l... tO6#..E.
0010  02 a3 a2 ac 40 00 7f 06  02 2f 47 c0 22 68 40 e9   ....@... ./G."h@.
0020  a9 68 10 ef 00 50 f8 32  36 e5 e9 4f 38 95 50 18   .h...P.2 6..O8.P.
0030  fe 14 38 6d 00 00 47 45  54 20 2f 20 48 54 54 50   ..8m..GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   /1.1..Ho st: www.
0050  67 6f 6f 67 6c 65 2e 63  6f 6d 0d 0a 55 73 65 72   google.c om..User
0060  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
0070  35 2e 30 20 28 57 69 6e  64 6f 77 73 3b 20 55 3b   5.0 (Win dows; U;
0080  20 57 69 6e 64 6f 77 73  20 4e 54 20 35 2e 31 3b    Windows  NT 5.1;
```

Frame (frame), 689 bytes · Packets: 210 · Displayed: 27 (12.9%) · Load time: 0:0.17 · Profile: Default

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.

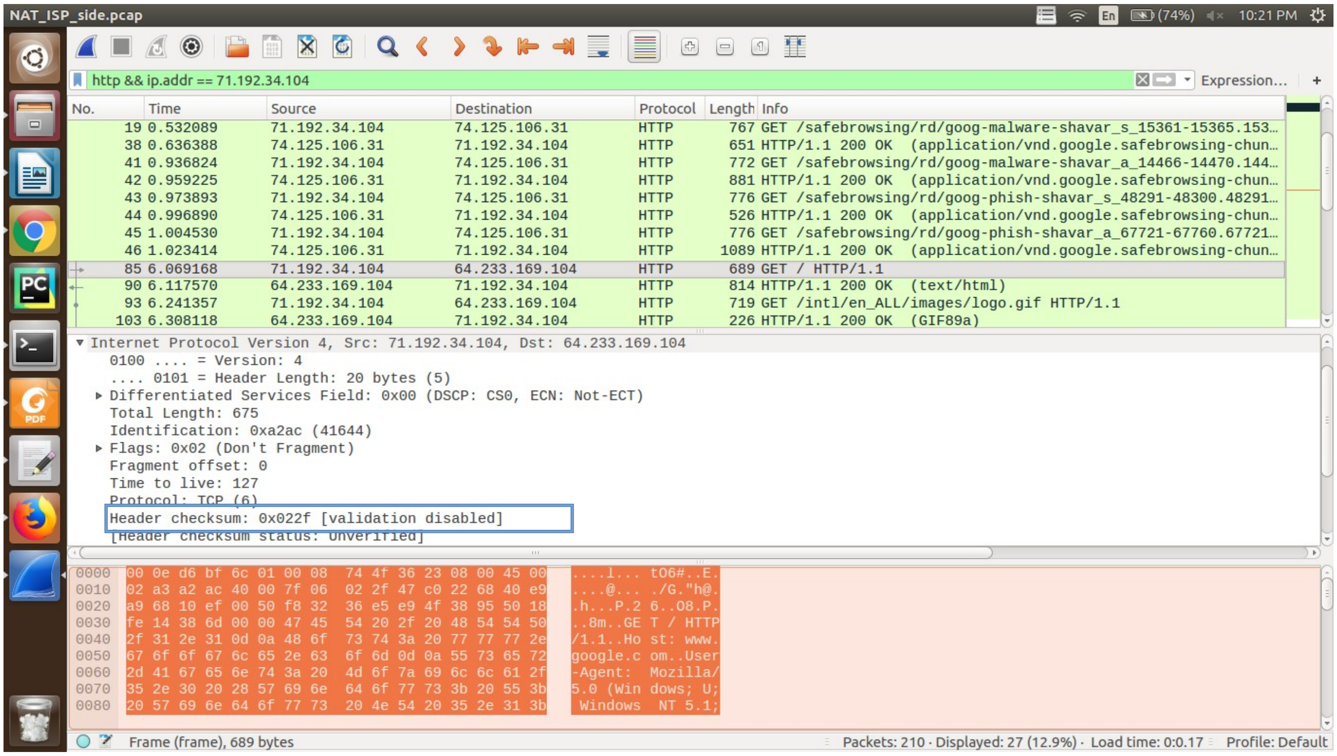
Ans: No, none of the fields changes in the HTTP GET Message

Fields that changed: Checksum

Fields that didn't change: Version, Header Length, Flags.

Since source IP is different between both the IP Datagrams, the calculated checksum will also be different as the change of IP changes datagram content and checksum is calculated for entire Datagram including the header.

Below image displays the GET message sent from the ISP to server.



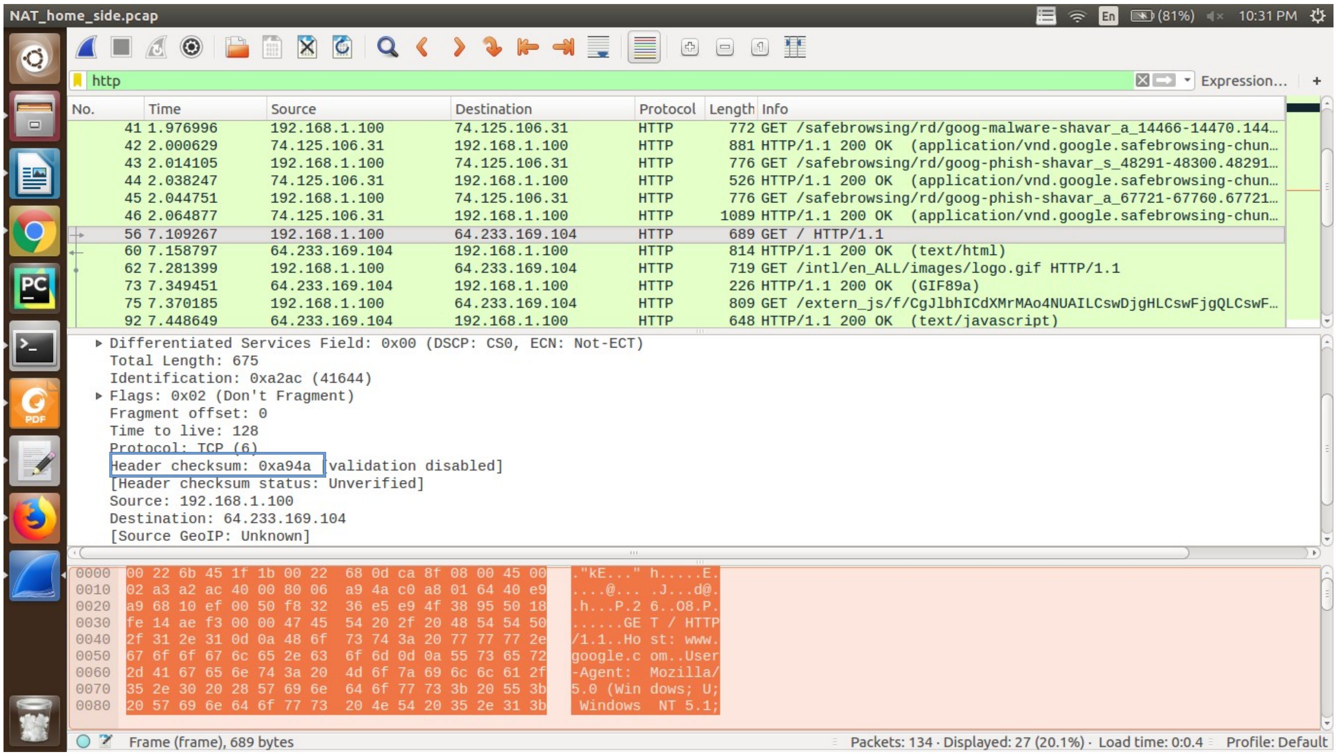
```
http && ip.addr == 71.192.34.104

No.   Time       Source          Destination     Protocol Length Info
   19 0.532089   71.192.34.104   74.125.106.31   HTTP     767 GET /safebrowsing/rd/goog-malware-shavar_s_15361-15365.153…
   38 0.636388   74.125.106.31   71.192.34.104   HTTP     651 HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-chun…
   41 0.936824   71.192.34.104   74.125.106.31   HTTP     772 GET /safebrowsing/rd/goog-malware-shavar_a_14466-14470.144…
   42 0.959225   74.125.106.31   71.192.34.104   HTTP     881 HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-chun…
   43 0.973893   71.192.34.104   74.125.106.31   HTTP     776 GET /safebrowsing/rd/goog-phish-shavar_s_48291-48300.48291…
   44 0.996890   74.125.106.31   71.192.34.104   HTTP     526 HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-chun…
   45 1.004530   71.192.34.104   74.125.106.31   HTTP     776 GET /safebrowsing/rd/goog-phish-shavar_a_67721-67760.67721…
   46 1.023414   74.125.106.31   71.192.34.104   HTTP    1089 HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-chun…
   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)

▼ Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 675
    Identification: 0xa2ac (41644)
  ▸ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 127
    Protocol: TCP (6)
    Header checksum: 0x022f [validation disabled]
    [Header checksum status: Unverified]

0000  00 0e d6 bf 6c 01 00 08  74 4f 36 23 08 00 45 00   ....l... tO6#..E.
0010  02 a3 a2 ac 40 00 7f 06  02 2f 47 c0 22 68 40 e9   ....@... ./G."h@.
0020  a9 68 10 ef 00 50 f8 32  36 e5 e9 4f 38 95 50 18   .h...P.2 6..O8.P.
0030  fe 14 38 6d 00 00 47 45  54 20 2f 20 48 54 54 50   ..8m..GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   /1.1..Ho st: www.
0050  67 6f 6f 67 6c 65 2e 63  6f 6d 0d 0a 55 73 65 72   google.c om..User
0060  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
0070  35 2e 30 20 28 57 69 6e  64 6f 77 73 3b 20 55 3b   5.0 (Win dows; U;
0080  20 57 69 6e 64 6f 77 73  20 4e 54 20 35 2e 31 3b    Windows  NT 5.1;

Frame (frame), 689 bytes     Packets: 210 · Displayed: 27 (12.9%) · Load time: 0:0.17     Profile: Default
```



```
http

No.   Time       Source          Destination     Protocol Length Info
   41 1.976996   192.168.1.100   74.125.106.31   HTTP     772 GET /safebrowsing/rd/goog-malware-shavar_a_14466-14470.144…
   42 2.000629   74.125.106.31   192.168.1.100   HTTP     881 HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-chun…
   43 2.014105   192.168.1.100   74.125.106.31   HTTP     776 GET /safebrowsing/rd/goog-phish-shavar_s_48291-48300.48291…
   44 2.038247   74.125.106.31   192.168.1.100   HTTP     526 HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-chun…
   45 2.044751   192.168.1.100   74.125.106.31   HTTP     776 GET /safebrowsing/rd/goog-phish-shavar_a_67721-67760.67721…
   46 2.064877   74.125.106.31   192.168.1.100   HTTP    1089 HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-chun…
   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/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswF…
   92 7.448649   64.233.169.104  192.168.1.100   HTTP     648 HTTP/1.1 200 OK  (text/javascript)

  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 675
    Identification: 0xa2ac (41644)
  ▸ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0xa94a [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.100
    Destination: 64.233.169.104
    [Source GeoIP: Unknown]

0000  00 22 6b 45 1f 1b 00 22  68 0d ca 8f 08 00 45 00   ."kE..." h.....E.
0010  02 a3 a2 ac 40 00 80 06  a9 4a c0 a8 01 64 40 e9   ....@... .J...d@.
0020  a9 68 10 ef 00 50 f8 32  36 e5 e9 4f 38 95 50 18   .h...P.2 6..O8.P.
0030  fe 14 ae f3 00 00 47 45  54 20 2f 20 48 54 54 50   ......GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   /1.1..Ho st: www.
0050  67 6f 6f 67 6c 65 2e 63  6f 6d 0d 0a 55 73 65 72   google.c om..User
0060  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
0070  35 2e 30 20 28 57 69 6e  64 6f 77 73 3b 20 55 3b   5.0 (Win dows; U;
0080  20 57 69 6e 64 6f 77 73  20 4e 54 20 35 2e 31 3b    Windows  NT 5.1;

Frame (frame), 689 bytes     Packets: 134 · Displayed: 27 (20.1%) · Load time: 0:0.4     Profile: Default
```

The highlighted regions display the change in checksum when the request if sent from client side to server and when request is sent from ISP side to server.

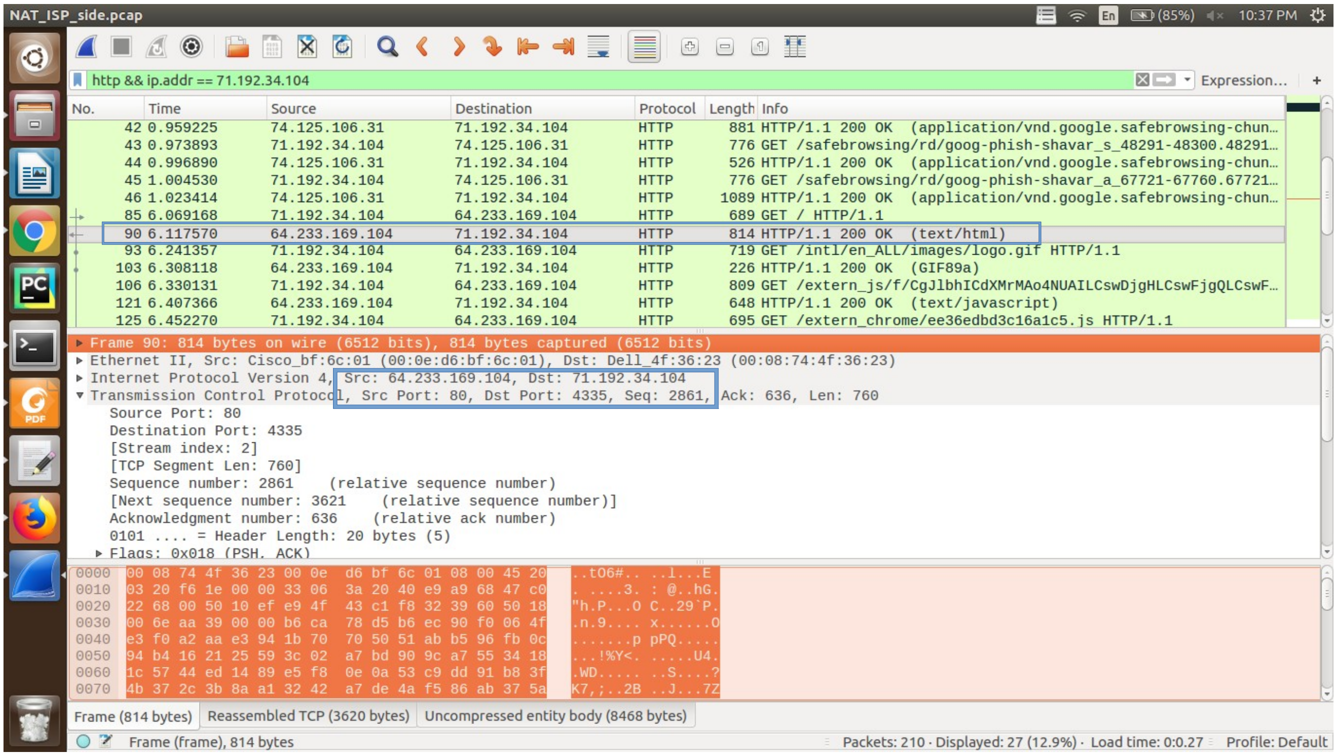
Q8) In the NAT_ISP_side trace file, at what time is the first 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message? Which of these fields are the same, and which are different than your answer to question 4 above?

Ans: Time at which the first HTTP OK Message was received: 6.117570

a) Source IP: 64.233.169.104
b) Source Port: 80
c) Destination IP: 71.192.34.104
d) Destination Port: 4335

The Fields Source IP, Source Port and Destination Port are same and the field Destination IP is different as compared to the fields in question 4.

Below image displays the time at which the HTTP 200 OK reply was received from the server and also the TCP source and desination address and ports of the IP carrying datagram



```
http && ip.addr == 71.192.34.104
```

```
No.   Time      Source          Destination     Protocol Length Info
   42 0.959225  74.125.106.31   71.192.34.104   HTTP      881 HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-chun…
   43 0.973893  71.192.34.104   74.125.106.31   HTTP      776 GET /safebrowsing/rd/goog-phish-shavar_s_48291-48300.48291…
   44 0.996890  74.125.106.31   71.192.34.104   HTTP      526 HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-chun…
   45 1.004530  71.192.34.104   74.125.106.31   HTTP      776 GET /safebrowsing/rd/goog-phish-shavar_a_67721-67760.67721…
   46 1.023414  74.125.106.31   71.192.34.104   HTTP     1089 HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-chun…
   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/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswF…
  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
```

```
▸ 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
▾ 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)
```

```
0000  00 08 74 4f 36 23 00 0e  d6 bf 6c 01 08 00 45 20   ..tO6#.. ..l...E
0010  03 20 f6 1e 00 00 33 06  3a 20 40 e9 a9 68 47 c0   . ....3. : @..hG.
0020  22 68 00 50 10 ef e9 4f  43 c1 f8 32 39 60 50 18   "h.P...O C..29`P.
0030  00 6e aa 39 00 00 b6 ca  78 d5 b6 ec 90 f0 06 4f   .n.9.... x......O
0040  e3 f0 a2 aa e3 94 1b 70  70 50 51 ab b5 96 fb 0c   .......p pPQ.....
0050  94 b4 16 21 25 59 3c 02  a7 bd 90 9c a7 55 34 18   ...!%Y<. .....U4.
0060  1c 57 44 ed 14 89 e5 f8  0e 0a 53 c9 dd 91 b8 3f   .WD..... ..S....?
0070  4b 37 2c 3b 8a a1 32 42  a7 de 4a f5 86 ab 37 5a   K7,;..2B ..J...7Z
```

Frame (814 bytes)
Reassembled TCP (3620 bytes)
Uncompressed entity body (8468 bytes)
Frame (frame), 814 bytes
Packets: 210 · Displayed: 27 (12.9%) · Load time: 0:0.27
Profile: Default

Q9) In the NAT_ISP_side trace file, at what time were the client-to-server TCP SYN segment and the server-to-client TCP ACK segment corresponding to the segments in question 5 above captured? What are the source and destination IP addresses and source and destination ports for these two segments? Which of these fields are the same, and which are different than your answer to question 5 above?

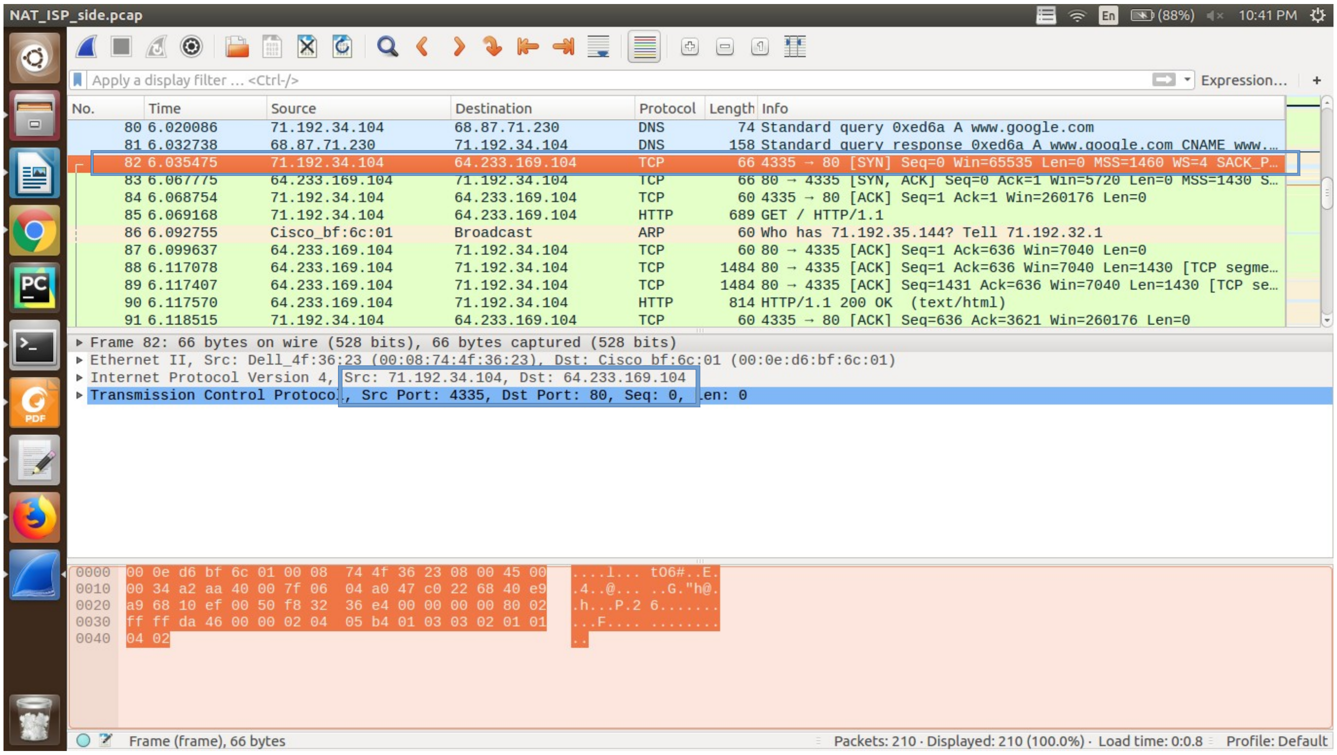
Ans: Time at which SYN was sent from client to server: 6.035475 seconds
a) Source IP Address: 71.192.34.104
b) Source Port: 4335
c) Destination IP address: 64.233.169.104
d) Destination Port: 80

For SYN segment the fields that changed is Source IP and the rest have changed. As compared to Qns. 5

Time at which ACK was sent from server to client: 6.067775 seconds
a) Source IP: 64.233.169.104
b) Source Port: 80
c) Destination IP: 71.192.34.104
d) Destination Port: 4335

For ACK Segment received from the server , the Desination IP value has changed and rest of the values remain same as compared to qns 5

Below image displays the time at which the SYN segment was sent and the src and Ip addresses and port carrying out the TCP segment.



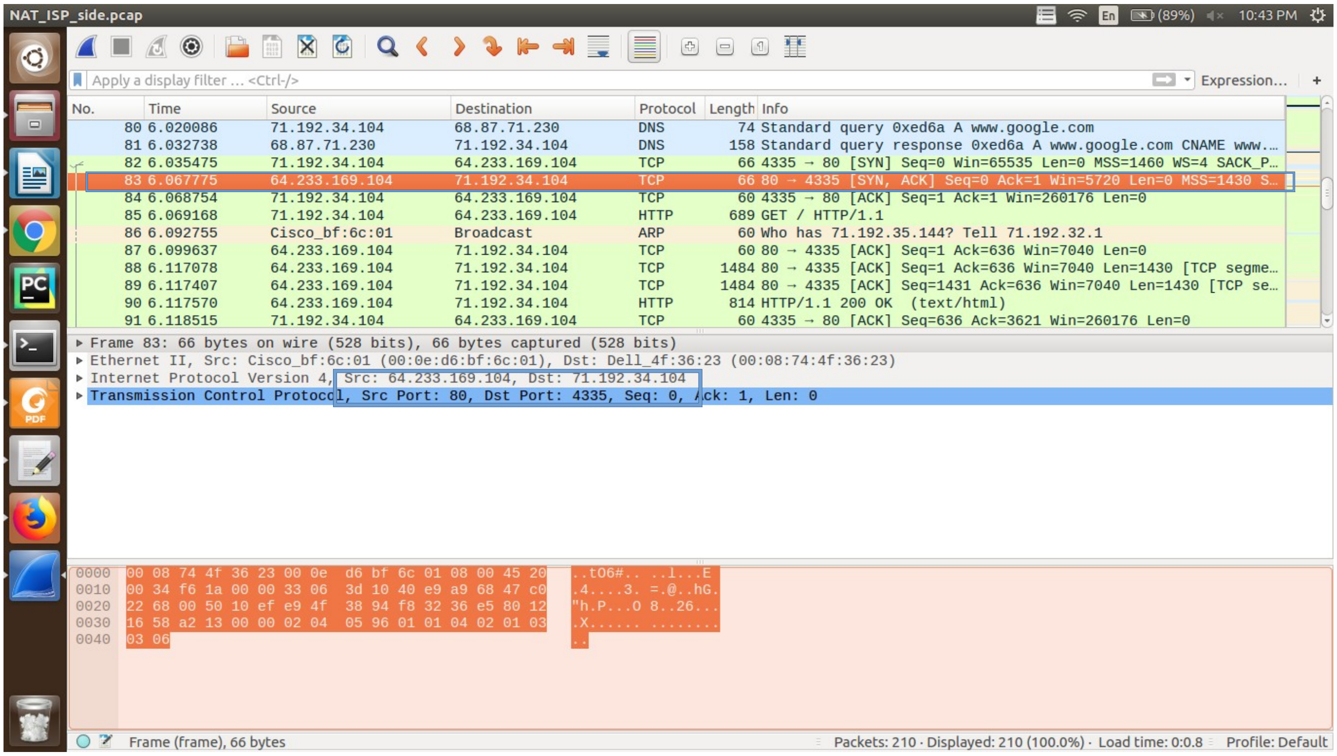
```
No.   Time       Source          Destination     Protocol Length Info
   80 6.020086   71.192.34.104   68.87.71.230    DNS          74 Standard query 0xed6a A www.google.com
   81 6.032738   68.87.71.230    71.192.34.104   DNS         158 Standard query response 0xed6a A www.google.com CNAME www.…
   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_P…
   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 S…
   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
   86 6.092755   Cisco_bf:6c:01  Broadcast       ARP          60 Who has 71.192.35.144? Tell 71.192.32.1
   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 segme…
   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 se…
   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
```

```
▸ 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
▸ Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  00 0e d6 bf 6c 01 00 08  74 4f 36 23 08 00 45 00   ....l... tO6#..E.
0010  00 34 a2 aa 40 00 7f 06  04 a0 47 c0 22 68 40 e9   .4..@... ..G."h@.
0020  a9 68 10 ef 00 50 f8 32  36 e4 00 00 00 00 80 02   .h...P.2 6.......
0030  ff ff da 46 00 00 02 04  05 b4 01 03 03 02 01 01   ...F.... ........
0040  04 02                                              ..
```

Frame (frame), 66 bytes   Packets: 210 · Displayed: 210 (100.0%) · Load time: 0:0.8   Profile: Default

Below image displays the time at which the SYN segment was sent and the src and Ip addresses and port carrying out the TCP segment.



```
No.  Time       Source           Destination      Protocol Length Info
  80 6.020086   71.192.34.104    68.87.71.230     DNS        74 Standard query 0xed6a A www.google.com
  81 6.032738   68.87.71.230     71.192.34.104    DNS       158 Standard query response 0xed6a A www.google.com CNAME www.…
  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_P…
  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 S…
  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
  86 6.092755   Cisco_bf:6c:01   Broadcast        ARP        60 Who has 71.192.35.144? Tell 71.192.32.1
  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 segme…
  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 se…
  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

▸ 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
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 0, Ack: 1, Len: 0

0000  00 08 74 4f 36 23 00 0e  d6 bf 6c 01 08 00 45 20   ..tO6#.. ..l...E
0010  00 34 f6 1a 00 00 33 06  3d 10 40 e9 a9 68 47 c0   .4....3. =.@..hG.
0020  22 68 00 50 10 ef e9 4f  38 94 f8 32 36 e5 80 12   "h.P...O 8..26...
0030  16 58 a2 13 00 00 02 04  05 96 01 01 04 02 01 03   .X...... ........
0040  03 06                                              ..

Frame (frame), 66 bytes        Packets: 210 · Displayed: 210 (100.0%) · Load time: 0:0.8    Profile: Default
```

Q10) 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