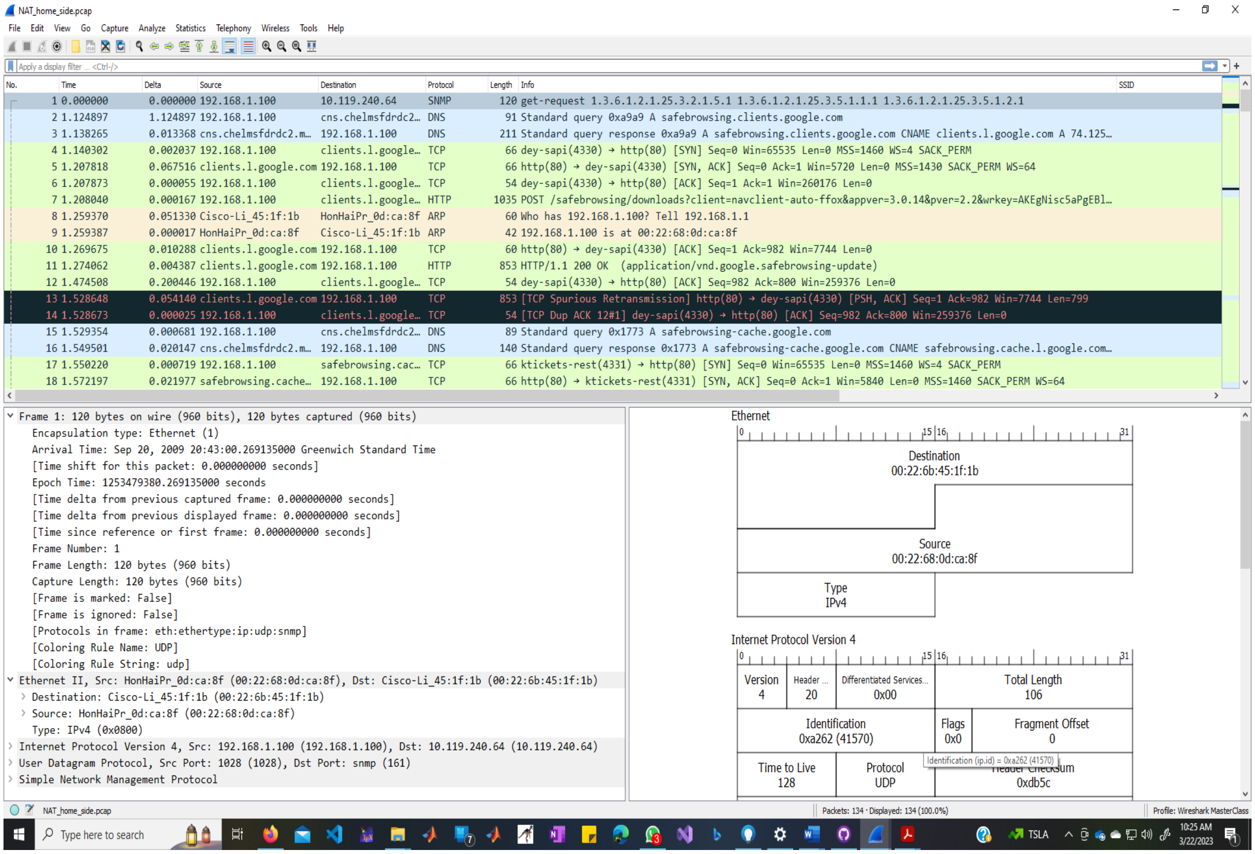
Part B: WIRESHARK

Wireshark NAT trace for Examinations



NAT_home_side.pcap

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

```
No.  Time       Delta    Source                 Destination          Protocol Length Info
   1 0.000000   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 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1.2.1
   2 1.124897   1.124897 192.168.1.100          cns.chelmsfdrdc2…    DNS        91 Standard query 0xa9a9 A safebrowsing.clients.google.com
   3 1.138265   0.013368 cns.chelmsfdrdc2.m…    192.168.1.100        DNS       211 Standard query response 0xa9a9 A safebrowsing.clients.google.com CNAME clients.l.google.com A 74.125…
   4 1.140302   0.002037 192.168.1.100          clients.l.google…    TCP        66 dey-sapi(4330) → http(80) [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM
   5 1.207818   0.067516 clients.l.google.com   192.168.1.100        TCP        66 http(80) → dey-sapi(4330) [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM WS=64
   6 1.207873   0.000055 192.168.1.100          clients.l.google…    TCP        54 dey-sapi(4330) → http(80) [ACK] Seq=1 Ack=1 Win=260176 Len=0
   7 1.208040   0.000167 192.168.1.100          clients.l.google…    HTTP     1035 POST /safebrowsing/downloads?client=navclient-auto-ffox&appver=3.0.14&pver=2.2&wrkey=AKEgNisc5aPgEBl…
   8 1.259370   0.051330 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   0.000017 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   0.010288 clients.l.google.com   192.168.1.100        TCP        60 http(80) → dey-sapi(4330) [ACK] Seq=1 Ack=982 Win=7744 Len=0
  11 1.274062   0.004387 clients.l.google.com   192.168.1.100        HTTP      853 HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-update)
  12 1.474508   0.200446 192.168.1.100          clients.l.google…    TCP        54 dey-sapi(4330) → http(80) [ACK] Seq=982 Ack=800 Win=259376 Len=0
  13 1.528648   0.054140 clients.l.google.com   192.168.1.100        TCP       853 [TCP Spurious Retransmission] http(80) → dey-sapi(4330) [PSH, ACK] Seq=1 Ack=982 Win=7744 Len=799
  14 1.528673   0.000025 192.168.1.100          clients.l.google…    TCP        54 [TCP Dup ACK 12#1] dey-sapi(4330) → http(80) [ACK] Seq=982 Ack=800 Win=259376 Len=0
  15 1.529354   0.000681 192.168.1.100          cns.chelmsfdrdc2…    DNS        89 Standard query 0x1773 A safebrowsing-cache.google.com
  16 1.549501   0.020147 cns.chelmsfdrdc2.m…    192.168.1.100        DNS       140 Standard query response 0x1773 A safebrowsing-cache.google.com CNAME safebrowsing.cache.l.google.com…
  17 1.550220   0.000719 192.168.1.100          safebrowsing.cac…    TCP        66 ktickets-rest(4331) → http(80) [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM
  18 1.572197   0.021977 safebrowsing.cache…    192.168.1.100        TCP        66 http(80) → ktickets-rest(4331) [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM WS=64
```

```
Frame 1: 120 bytes on wire (960 bits), 120 bytes captured (960 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 20, 2009 20:43:00.269135000 Greenwich Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1253479380.269135000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 120 bytes (960 bits)
    Capture Length: 120 bytes (960 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:snmp]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
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)
    Destination: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
    Source: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.100 (192.168.1.100), Dst: 10.119.240.64 (10.119.240.64)
User Datagram Protocol, Src Port: 1028 (1028), Dst Port: snmp (161)
Simple Network Management Protocol
```

NAT_home_side.pcap

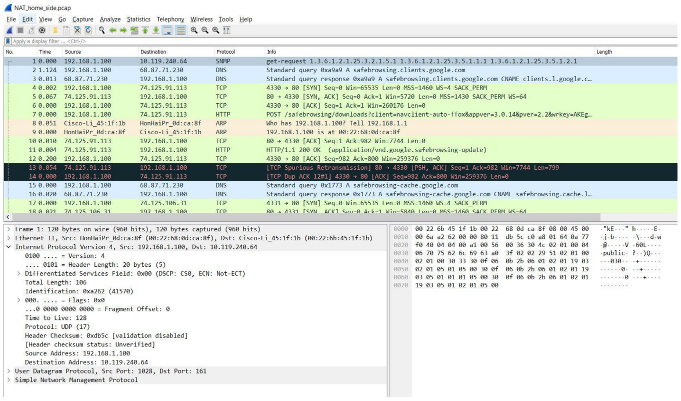
Packets: 134 · Displayed: 134 (100.0%)

Profile: Wireshark MasterClass

Open the NAT_home_side file and answer the following questions. You might find it useful to use a Wireshark filter so that only frames containing HTTP messages are displayed from the trace file.

1. What is the IP address of the client?

***Answer:* IP Address is 192.168.1.100 as shown in the figure below**



NAT_home_side.pcap

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

```
No.  Time   Source             Destination        Protocol  Info                                                                                   Length
   1 0.000  192.168.1.100      10.119.240.64      SNMP      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 1.3.6.1.2.1.25.3.5.1.2.1
   2 1.124  192.168.1.100      68.87.71.230       DNS       Standard query 0xa9a9 A safebrowsing.clients.google.com
   3 0.013  68.87.71.230       192.168.1.100      DNS       Standard query response 0xa9a9 A safebrowsing.clients.google.com CNAME clients.l.google.c…
   4 0.002  192.168.1.100      74.125.91.113      TCP       4330 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM
   5 0.067  74.125.91.113      192.168.1.100      TCP       80 → 4330 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM WS=64
   6 0.000  192.168.1.100      74.125.91.113      TCP       4330 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
   7 0.000  192.168.1.100      74.125.91.113      HTTP      POST /safebrowsing/downloads?client=navclient-auto-ffox&appver=3.0.14&pver=2.2&wrkey=AKEg…
   8 0.051  Cisco-Li_45:1f:1b  HonHaiPr_0d:ca:8f  ARP       Who has 192.168.1.100? Tell 192.168.1.1
   9 0.000  HonHaiPr_0d:ca:8f  Cisco-Li_45:1f:1b  ARP       192.168.1.100 is at 00:22:68:0d:ca:8f
  10 0.010  74.125.91.113      192.168.1.100      TCP       80 → 4330 [ACK] Seq=1 Ack=982 Win=7744 Len=0
  11 0.004  74.125.91.113      192.168.1.100      HTTP      HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-update)
  12 0.200  192.168.1.100      74.125.91.113      TCP       4330 → 80 [ACK] Seq=982 Ack=800 Win=259376 Len=0
  13 0.054  74.125.91.113      192.168.1.100      TCP       [TCP Spurious Retransmission] 80 → 4330 [PSH, ACK] Seq=1 Ack=982 Win=7744 Len=799
  14 0.000  192.168.1.100      74.125.91.113      TCP       [TCP Dup ACK 12#1] 4330 → 80 [ACK] Seq=982 Ack=800 Win=259376 Len=0
  15 0.000  192.168.1.100      68.87.71.230       DNS       Standard query 0x1773 A safebrowsing-cache.google.com
  16 0.020  68.87.71.230       192.168.1.100      DNS       Standard query response 0x1773 A safebrowsing-cache.google.com CNAME safebrowsing.cache.l…
  17 0.000  192.168.1.100      74.125.106.31      TCP       4331 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM
  18 0.021  74.125.106.31      192.168.1.100      TCP       80 → 4331 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM WS=64
```

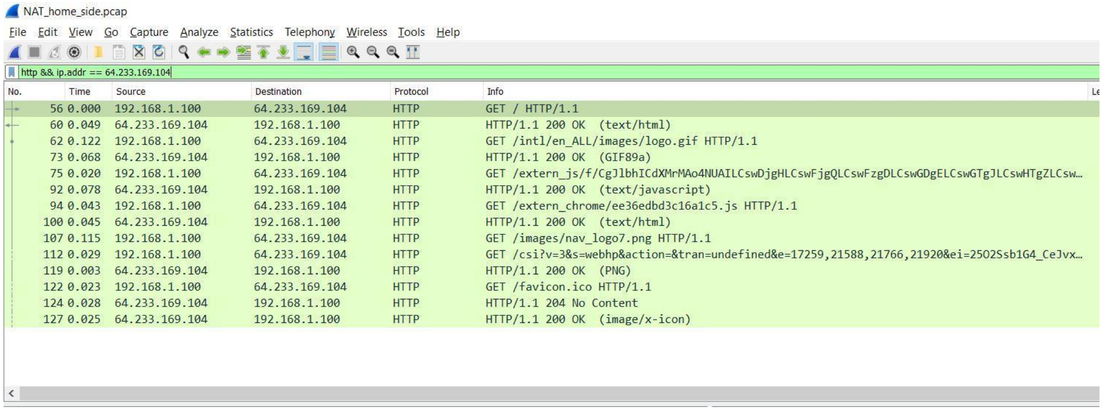
```
Frame 1: 120 bytes on wire (960 bits), 120 bytes captured (960 bits)
Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 10.119.240.64
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 106
    Identification: 0xa262 (41570)
    000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xdb5c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.100
    Destination Address: 10.119.240.64
User Datagram Protocol, Src Port: 1028, Dst Port: 161
Simple Network Management Protocol
```

```
0000  00 22 6b 45 1f 1b 00 22  68 0d ca 8f 08 00 45 00   ·"kE···" h·····E·
0010  00 6a a2 62 00 00 80 11  db 5c c0 a8 01 64 0a 77   ·j·b····  ·\···d·w
0020  f0 40 04 04 00 a1 00 56  00 36 30 4c 02 01 00 04   ·@·····V ·60L····
0030  06 70 75 62 6c 69 63 a0  3f 02 02 29 51 02 01 00   ·public· ?··)Q···
0040  02 01 00 30 33 30 0f 06  0b 2b 06 01 02 01 19 03   ···030·· ·+······
0050  02 01 05 01 05 00 30 0f  06 0b 2b 06 01 02 01 19   ······0· ··+·····
0060  03 05 01 01 01 05 00 30  0f 06 0b 2b 06 01 02 01   ·······0 ···+····
0070  19 03 05 01 02 01 05 00                            ········
```

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.

Answer:

The figure is shown below, the "http && ip.addr == 64.233.169.104" returned the results


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

http && ip.addr == 64.233.169.104

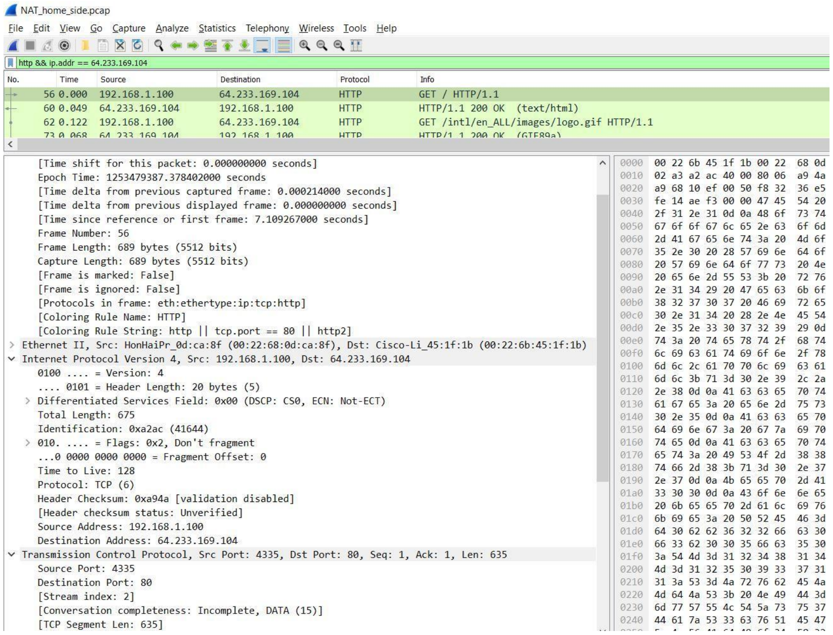
No.	Time	Source	Destination	Protocol	Info
56	0.000	192.168.1.100	64.233.169.104	HTTP	GET / HTTP/1.1
60	0.049	64.233.169.104	192.168.1.100	HTTP	HTTP/1.1 200 OK (text/html)
62	0.122	192.168.1.100	64.233.169.104	HTTP	GET /intl/en_ALL/images/logo.gif HTTP/1.1
73	0.068	64.233.169.104	192.168.1.100	HTTP	HTTP/1.1 200 OK (GIF89a)
75	0.020	192.168.1.100	64.233.169.104	HTTP	GET /extern_js/f/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswFzgDLCswGDgELCswGTgJLCswHTgZLCsw…
92	0.078	64.233.169.104	192.168.1.100	HTTP	HTTP/1.1 200 OK (text/javascript)
94	0.043	192.168.1.100	64.233.169.104	HTTP	GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.1
100	0.045	64.233.169.104	192.168.1.100	HTTP	HTTP/1.1 200 OK (text/html)
107	0.115	192.168.1.100	64.233.169.104	HTTP	GET /images/nav_logo7.png HTTP/1.1
112	0.029	192.168.1.100	64.233.169.104	HTTP	GET /csi?v=3&s=webhp&action=&tran=undefined&e=17259,21588,21766,21920&ei=2502Ssb1G4_CeJvx…
119	0.003	64.233.169.104	192.168.1.100	HTTP	HTTP/1.1 200 OK (PNG)
122	0.023	192.168.1.100	64.233.169.104	HTTP	GET /favicon.ico HTTP/1.1
124	0.028	64.233.169.104	192.168.1.100	HTTP	HTTP/1.1 204 No Content
127	0.025	64.233.169.104	192.168.1.100	HTTP	HTTP/1.1 200 OK (image/x-icon)

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 7.102967. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?

Answer:

Source IP Address is 192.168.1.100, Port: 4335
Destination IP Address is 64.233.169.104, Port: 80

The figure shows it very well


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

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

```
No.    Time   Source           Destination      Protocol  Info
   56 0.000   192.168.1.100    64.233.169.104   HTTP      GET / HTTP/1.1
   60 0.049   64.233.169.104   192.168.1.100    HTTP      HTTP/1.1 200 OK  (text/html)
   62 0.122   192.168.1.100    64.233.169.104   HTTP      GET /intl/en_ALL/images/logo.gif HTTP/1.1
   73 0.068   64.233.169.104   192.168.1.100    HTTP      HTTP/1.1 200 OK  (GIF89a)
```

```
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1253479387.378402000 seconds
    [Time delta from previous captured frame: 0.000214000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 7.109267000 seconds]
    Frame Number: 56
    Frame Length: 689 bytes (5512 bits)
    Capture Length: 689 bytes (5512 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
> 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: 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)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0xa94a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.100
    Destination Address: 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]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 635]
```

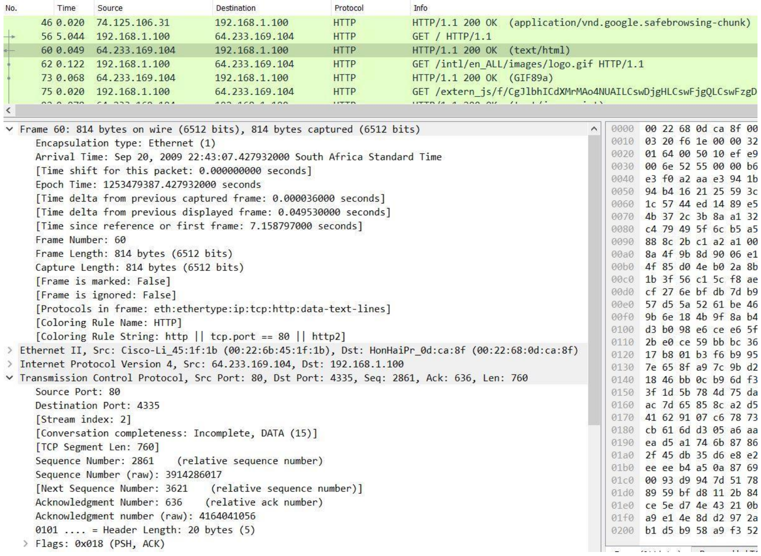
```
0000  00 22 6b 45 1f 1b 00 22  68 0d
0010  02 a3 a2 ac 40 00 80 06  a9 4a
0020  a9 68 10 ef 00 50 f8 32  36 e5
0030  fe 14 ae f3 00 00 47 45  54 20
0040  2f 31 2e 31 0d 0a 48 6f  73 74
0050  67 6f 6f 67 6c 65 2e 63  6f 6d
0060  2d 41 67 65 6e 74 3a 20  4d 6f
0070  35 2e 30 20 28 57 69 6e  64 6f
0080  20 57 69 6e 64 6f 77 73  20 4e
0090  20 65 6e 2d 55 53 3b 20  72 76
00a0  2e 31 34 29 20 47 65 63  6b 6f
00b0  38 32 37 30 37 20 46 69  72 65
00c0  30 2e 31 34 20 28 2e 4e  45 54
00d0  2e 35 2e 33 30 37 32 39  29 0d
00e0  74 3a 20 74 65 78 74 2f  68 74
00f0  6c 69 63 61 74 69 6f 6e  2f 78
0100  6d 6c 2c 61 70 70 6c 69  63 61
0110  6d 6c 3b 71 3d 30 2e 39  2c 2a
0120  2e 38 0d 0a 41 63 63 65  70 74
0130  61 67 65 3a 20 65 6e 2d  75 73
0140  30 2e 35 0d 0a 41 63 63  65 70
0150  64 69 6e 67 3a 20 67 7a  69 70
0160  74 65 0d 0a 41 63 63 65  70 74
0170  65 74 3a 20 49 53 4f 2d  38 38
0180  74 66 2d 38 3b 71 3d 30  2e 37
0190  2e 37 0d 0a 4b 65 65 70  2d 41
01a0  33 30 30 0d 0a 43 6f 6e  6e 65
01b0  20 6b 65 65 70 2d 61 6c  69 76
01c0  6b 69 65 3a 20 50 52 45  46 3d
01d0  64 30 62 62 36 32 32 66  63 30
01e0  66 33 62 30 30 35 66 63  35 30
01f0  3a 54 4d 3d 31 32 34 38  31 34
0200  4d 3d 31 32 35 30 39 33  37 31
0210  31 3a 53 3d 4a 72 76 62  45 4a
0220  4d 64 4a 53 3b 20 4e 49  44 3d
0230  6d 77 57 55 4c 54 5a 73  75 37
0240  44 61 7a 53 33 63 76 51  45 47
```

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?

Answer:

Time the corresponding 200 OK HTTP is 7.15879700 seconds
Source IP Address is 64.233.169.104, Port: 80
Destination IP Address is 192.168.1.100, Port: 4335

The figure is shown below



```
No.    Time   Source           Destination      Protocol  Info
   46 0.020   74.125.106.31    192.168.1.100    HTTP      HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-chunk)
   56 5.044   192.168.1.100    64.233.169.104   HTTP      GET / HTTP/1.1
   60 0.049   64.233.169.104   192.168.1.100    HTTP      HTTP/1.1 200 OK  (text/html)
   62 0.122   192.168.1.100    64.233.169.104   HTTP      GET /intl/en_ALL/images/logo.gif HTTP/1.1
   73 0.068   64.233.169.104   192.168.1.100    HTTP      HTTP/1.1 200 OK  (GIF89a)
   75 0.020   192.168.1.100    64.233.169.104   HTTP      GET /extern_js/f/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswFzgD
```

```
v Frame 60: 814 bytes on wire (6512 bits), 814 bytes captured (6512 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 20, 2009 22:43:07.427932000 South Africa Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1253479387.427932000 seconds
    [Time delta from previous captured frame: 0.000036000 seconds]
    [Time delta from previous displayed frame: 0.049530000 seconds]
    [Time since reference or first frame: 7.158797000 seconds]
    Frame Number: 60
    Frame Length: 814 bytes (6512 bits)
    Capture Length: 814 bytes (6512 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
> 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]
    [Conversation completeness: Incomplete, DATA (15)]
    [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)
```

```
0000  00 22 68 0d ca 8f 00
0010  03 20 f6 1e 00 00 32
0020  01 64 00 50 10 ef e9
0030  00 6e 52 55 00 00 b6
0040  e3 f0 a2 aa e3 94 1b
0050  94 b4 16 21 25 59 3c
0060  1c 57 44 ed 14 89 e5
0070  4b 37 2c 3b 8a a1 32
0080  c4 79 49 5f 6c b5 a5
0090  88 8c 2b c1 a2 a1 00
00a0  8a 4f 9b 8d 90 06 e1
00b0  4f 85 d0 4e b0 2a 8b
00c0  1b 3f 56 c1 5c f8 ae
00d0  cf 27 6e bf db 7d b9
00e0  57 d5 5a 52 61 be 46
00f0  9b 6e 18 4b 9f 8a b4
0100  d3 b0 98 e6 ce e6 5f
0110  2b e0 ce 59 bb bc 36
0120  17 b8 01 b3 f6 b9 95
0130  7e 65 8f a9 7c 9b d2
0140  18 46 bb 0c b9 6d f3
0150  3f 1d 5b 78 4d 75 da
0160  ac 7d 65 85 8c a2 d5
0170  41 62 91 07 c6 78 73
0180  cb 61 6d d3 05 a6 aa
0190  ea d5 a1 74 6b 87 86
01a0  2f 45 db 35 d6 e8 e2
01b0  ee ee b4 a5 0a 87 69
01c0  00 93 d9 94 7d 51 78
01d0  89 59 bf d8 11 2b 84
01e0  ce 5e d7 4e 43 21 0b
01f0  a9 e1 4e 8d d2 97 2a
0200  b1 d5 b9 58 a9 f3 52
```

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 7.102967?

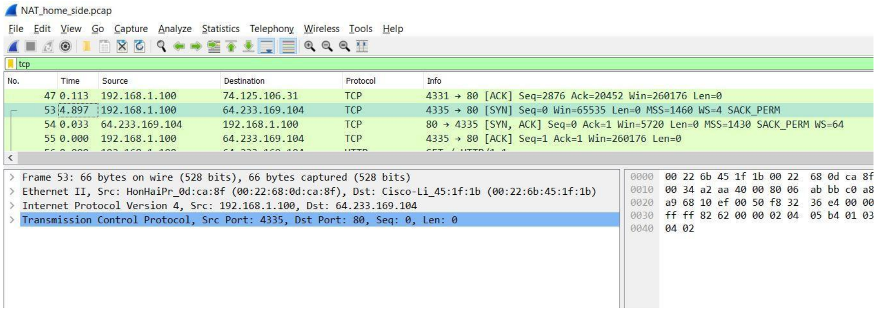
***Answer:* The SYN Time here will be 7.075657000 seconds for the figure below**

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

Answer:

SYN Source IP Address is 192.168.1.100, Port 4335

SYN Destination IP Address is 64.233.169.104, Port: 80


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

```
No.   Time   Source          Destination     Protocol  Info
   47 0.113  192.168.1.100   74.125.106.31   TCP       4331 → 80 [ACK] Seq=2876 Ack=20452 Win=260176 Len=0
   53 4.897  192.168.1.100   64.233.169.104  TCP       4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM
   54 0.033  64.233.169.104  192.168.1.100   TCP       80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM WS=64
   55 0.000  192.168.1.100   64.233.169.104  TCP       4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
```

```
> Frame 53: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
> Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104
> Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 0, Len: 0
```

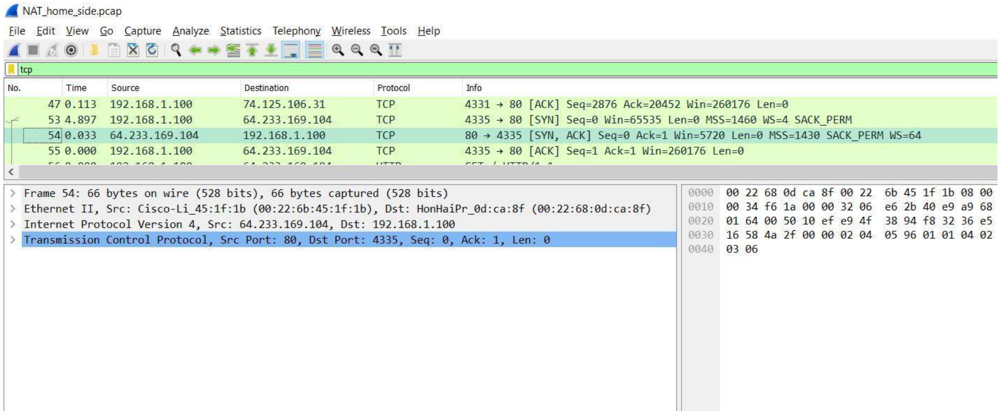
```
0000  00 22 6b 45 1f 1b 00 22  68 0d ca 8f
0010  00 34 a2 aa 40 00 80 06  ab bb c0 a8
0020  a9 68 10 ef 00 50 f8 32  36 e4 00 00
0030  ff ff 82 62 00 00 02 04  05 b4 01 03
0040  04 02
```

What are the source and destination IP addresses and source and destination ports of the ACK sent in response to the SYN.

Answer:

ACK Source IP Address is 64.233.169.104, Port: 80

ACK Destination IP Address is 192.168.1.100, Port: 4335. The figure below shows it clearly.


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

```
No.   Time   Source          Destination     Protocol  Info
   47 0.113  192.168.1.100   74.125.106.31   TCP       4331 → 80 [ACK] Seq=2876 Ack=20452 Win=260176 Len=0
   53 4.897  192.168.1.100   64.233.169.104  TCP       4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM
   54 0.033  64.233.169.104  192.168.1.100   TCP       80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM WS=64
   55 0.000  192.168.1.100   64.233.169.104  TCP       4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
```

```
> Frame 54: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b), Dst: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f)
> Internet Protocol Version 4, Src: 64.233.169.104, Dst: 192.168.1.100
> Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 0, Ack: 1, Len: 0
```

```
0000  00 22 68 0d ca 8f 00 22  6b 45 1f 1b 08 00
0010  00 34 f6 1a 00 00 32 06  e6 2b 40 e9 a9 68
0020  01 64 00 50 10 ef e9 4f  38 94 f8 32 36 e5
0030  16 58 4a 2f 00 00 02 04  05 96 01 01 04 02
0040  03 06
```

At what time is this ACK received at the client? . (Note: to find these segments you will need to clear the Filter expression you entered above in step 2. If you enter the filter "tcp", only TCP segments will be displayed by Wireshark).

***Answer:* The ACK Time will be 7.108986000 seconds from the wireshark results.**

In the following we'll focus on the two HTTP messages (GET and 200 OK) and the TCP SYN and ACK segments identified above. Our goal below will be to locate these two HTTP messages and two TCP segments in the trace file (NAT_ISP_side) captured on the link between the router and the ISP. Because these captured frames will have already been forwarded through the NAT router, some of the IP address and port numbers will have been changed as a result of NAT translation.

Open the NAT_ISP_side. *Note that the time stamps in this file and in NAT_home_side are not synchronized since the packet captures at the two locations shown in Figure 1 were not started simultaneously.* (Indeed, you should discover that the timestamps of a packet captured at the ISP link is actually less that the timestamp of the packet captured at the client PC).

6. In the NAT_ISP_side trace file, find the HTTP GET message was sent from the client to the Google server at time 7.102967 (where t=7.102967 is time at which this was sent as recorded in the NAT_home_side trace file). At what time does this message appear in the NAT_ISP_side trace file? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET (as recording in the NAT_ISP_side trace file)? Which of these fields are the same, and which are different, than in your answer to question 3 above?

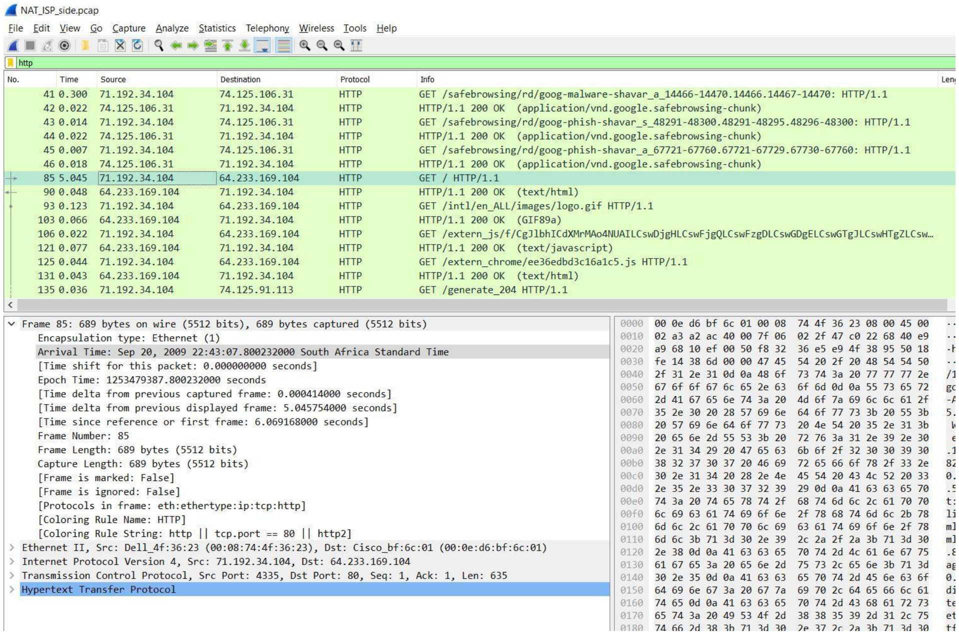
Answer:
The time this message appear in the NAT_ISP_side trace file is 6.069168000 seconds.

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) are:

Source IP Address is 71.192.34.104, Port: 4335
Destination IP Address is 64.233.169.104, Port: 80

Here, by comparing to the question 3 above, only the source IP address has changed, other fields are the same.

The figure below shows it very well as well.


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

```
No.     Time   Source          Destination     Protocol  Info                                                                                    Len
    41 0.300   71.192.34.104   74.125.106.31   HTTP      GET /safebrowsing/rd/goog-malware-shavar_a_14466-14470.14466.14467-14470: HTTP/1.1
    42 0.022   74.125.106.31   71.192.34.104   HTTP      HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-chunk)
    43 0.014   71.192.34.104   74.125.106.31   HTTP      GET /safebrowsing/rd/goog-phish-shavar_s_48291-48300.48291-48295.48296-48300: HTTP/1.1
    44 0.022   74.125.106.31   71.192.34.104   HTTP      HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-chunk)
    45 0.007   71.192.34.104   74.125.106.31   HTTP      GET /safebrowsing/rd/goog-phish-shavar_a_67721-67760.67721-67729.67730-67760: HTTP/1.1
    46 0.018   74.125.106.31   71.192.34.104   HTTP      HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-chunk)
    85 5.045   71.192.34.104   64.233.169.104  HTTP      GET / HTTP/1.1
    90 0.048   64.233.169.104  71.192.34.104   HTTP      HTTP/1.1 200 OK  (text/html)
    93 0.123   71.192.34.104   64.233.169.104  HTTP      GET /intl/en_ALL/images/logo.gif HTTP/1.1
   103 0.066   64.233.169.104  71.192.34.104   HTTP      HTTP/1.1 200 OK  (GIF89a)
   106 0.022   71.192.34.104   64.233.169.104  HTTP      GET /extern_js/f/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswFzgDLCswGDgELCswGTgJLCswHTgZLCsw…
   121 0.077   64.233.169.104  71.192.34.104   HTTP      HTTP/1.1 200 OK  (text/javascript)
   125 0.044   71.192.34.104   64.233.169.104  HTTP      GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.1
   131 0.043   64.233.169.104  71.192.34.104   HTTP      HTTP/1.1 200 OK  (text/html)
   135 0.036   71.192.34.104   74.125.91.113   HTTP      GET /generate_204 HTTP/1.1
```

```
v Frame 85: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 20, 2009 22:43:07.800232000 South Africa Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1253479387.800232000 seconds
    [Time delta from previous captured frame: 0.000414000 seconds]
    [Time delta from previous displayed frame: 5.045754000 seconds]
    [Time since reference or first frame: 6.069168000 seconds]
    Frame Number: 85
    Frame Length: 689 bytes (5512 bits)
    Capture Length: 689 bytes (5512 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
> 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
> Hypertext Transfer Protocol
```

```
0000  00 0e d6 bf 6c 01 00 08  74 4f 36 23 08 00 45 00   ··
0010  02 a3 a2 ac 40 00 7f 06  02 2f 47 c0 22 68 40 e9   ··
0020  a9 68 10 ef 00 50 f8 32  36 e5 e9 4f 38 95 50 18   ·h
0030  fe 14 38 6d 00 00 47 45  54 20 2f 20 48 54 54 50   ··
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   /1
0050  67 6f 6f 67 6c 65 2e 63  6f 6d 0d 0a 55 73 65 72   go
0060  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -A
0070  35 2e 30 20 28 57 69 6e  64 6f 77 73 3b 20 55 3b   5.
0080  20 57 69 6e 64 6f 77 73  20 4e 54 20 35 2e 31 3b    W
0090  20 65 6e 2d 55 53 3b 20  72 76 3a 31 2e 39 2e 30    e
00a0  2e 31 34 29 20 47 65 63  6b 6f 2f 32 30 30 39 30   .1
00b0  38 32 37 30 37 20 46 69  72 65 66 6f 78 2f 33 2e   82
00c0  30 2e 31 34 20 28 2e 4e  45 54 20 43 4c 52 20 33   0.
00d0  2e 35 2e 33 30 37 32 39  29 0d 0a 41 63 63 65 70   .5
00e0  74 3a 20 74 65 78 74 2f  68 74 6d 6c 2c 61 70 70   t:
00f0  6c 69 63 61 74 69 6f 6e  2f 78 68 74 6d 6c 2b 78   li
0100  6d 6c 2c 61 70 70 6c 69  63 61 74 69 6f 6e 2f 78   ml
0110  6d 6c 3b 71 3d 30 2e 39  2c 2a 2f 2a 3b 71 3d 30   ml
0120  2e 38 0d 0a 41 63 63 65  70 74 2d 4c 61 6e 67 75   .8
0130  61 67 65 3a 20 65 6e 2d  75 73 2c 65 6e 3b 71 3d   ag
0140  30 2e 35 0d 0a 41 63 63  65 70 74 2d 45 6e 63 6f   0.
0150  64 69 6e 67 3a 20 67 7a  69 70 2c 64 65 66 6c 61   di
0160  74 65 0d 0a 41 63 63 65  70 74 2d 43 68 61 72 73   te
0170  65 74 3a 20 49 53 4f 2d  38 38 35 39 2d 31 2c 75   et
0180  74 66 2d 38 3b 71 3d 30  2e 37 2c 2a 3b 71 3d 30   tf
```

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.

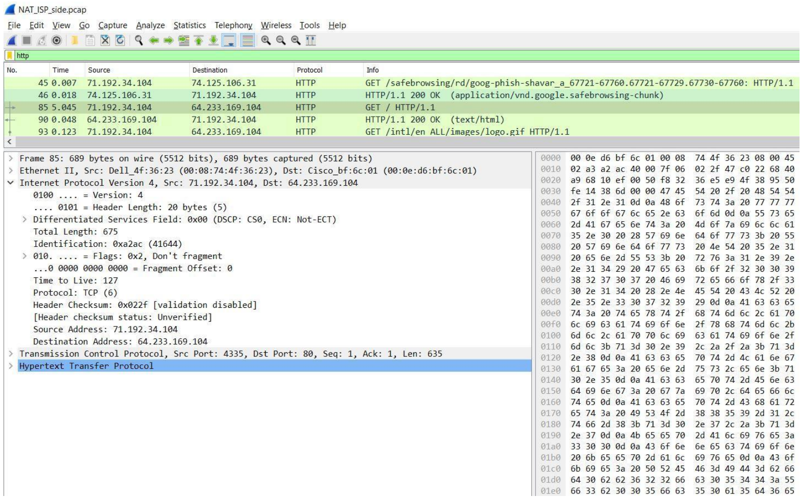
Answer:

GET Message has not changed and the version did change, header length did not change, Flags did not change, But checksum changed.
Source IP changed from 192.168.1.100 to 71.192.34.104 but port is the same.
Header checksum has changed from(Home) 0xa94a to (ISP) 0x022f.
Header checksum was changed because the IP Address changed from 192.168.1.100 to 71.192.34.104.

Here, since the IP source address has changed, and the checksum includes the value of the source IP address, the checksum had to change.

The results are also shown in the figure below.

From NAT_ISP_side trace file


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

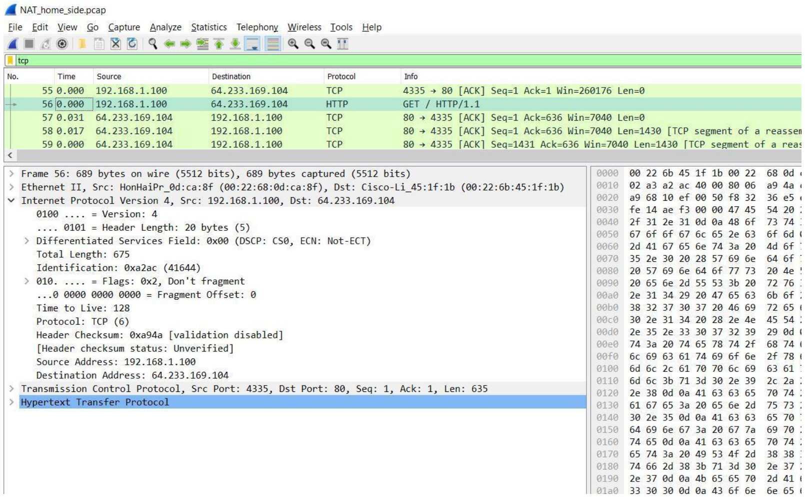
```
http
```

```
No.   Time   Source           Destination      Protocol  Info
   45 0.007  71.192.34.104    74.125.106.31    HTTP      GET /safebrowsing/rd/goog-phish-shavar_a_67721-67760.67721-67729.67730-67760: HTTP/1.1
   46 0.018  74.125.106.31    71.192.34.104    HTTP      HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-chunk)
   85 5.045  71.192.34.104    64.233.169.104   HTTP      GET / HTTP/1.1
   90 0.048  64.233.169.104   71.192.34.104    HTTP      HTTP/1.1 200 OK  (text/html)
   93 0.123  71.192.34.104    64.233.169.104   HTTP      GET /intl/en ALL/images/logo.gif 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)
v 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)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 127
    Protocol: TCP (6)
    Header Checksum: 0x022f [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 71.192.34.104
    Destination Address: 64.233.169.104
> Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
> Hypertext Transfer Protocol
```

```
0000  00 0e d6 bf 6c 01 00 08  74 4f 36 23 08 00 45
0010  02 a3 a2 ac 40 00 7f 06  02 2f 47 c0 22 68 40
0020  a9 68 10 ef 00 50 f8 32  36 e5 e9 4f 38 95 50
0030  fe 14 38 6d 00 00 47 45  54 20 2f 20 48 54 54
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77
0050  67 6f 6f 67 6c 65 2e 63  6f 6d 0d 0a 55 73 65
0060  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61
0070  35 2e 30 20 28 57 69 6e  64 6f 77 73 3b 20 55
0080  20 57 69 6e 64 6f 77 73  20 4e 54 20 35 2e 31
0090  20 65 6e 2d 55 53 3b 20  72 76 3a 31 2e 39 2e
00a0  2e 31 34 29 20 47 65 63  6b 6f 2f 32 30 30 39
00b0  38 32 37 30 37 20 46 69  72 65 66 6f 78 2f 33
00c0  30 2e 31 34 20 28 2e 4e  45 54 20 43 4c 52 20
00d0  2e 35 2e 33 30 37 32 39  29 0d 0a 41 63 63 65
00e0  74 3a 20 74 65 78 74 2f  68 74 6d 6c 2c 61 70
00f0  6c 69 63 61 74 69 6f 6e  2f 78 68 74 6d 6c 2b
0100  6d 6c 2c 61 70 70 6c 69  63 61 74 69 6f 6e 2f
0110  6d 6c 3b 71 3d 30 2e 39  2c 2a 2f 2a 3b 71 3d
0120  2e 38 0d 0a 41 63 63 65  70 74 2d 4c 61 6e 67
0130  61 67 65 3a 20 65 6e 2d  75 73 2c 65 6e 3b 71
0140  30 2e 35 0d 0a 41 63 63  65 70 74 2d 45 6e 63
0150  64 69 6e 67 3a 20 67 7a  69 70 2c 64 65 66 6c
0160  74 65 0d 0a 41 63 63 65  70 74 2d 43 68 61 72
0170  65 74 3a 20 49 53 4f 2d  38 38 35 39 2d 31 2c
0180  74 66 2d 38 3b 71 3d 30  2e 37 2c 2a 3b 71 3d
0190  2e 37 0d 0a 4b 65 65 70  2d 41 6c 69 76 65 3a
01a0  33 30 30 0d 0a 43 6f 6e  6e 65 63 74 69 6f 6e
01b0  20 6b 65 65 70 2d 61 6c  69 76 65 0d 0a 43 6f
01c0  6b 69 65 3a 20 50 52 45  46 3d 49 44 3d 62 66
01d0  64 30 62 62 36 32 32 66  63 30 35 34 34 3a 55
01e0  66 33 62 30 30 35 66 63  35 30 61 35 64 36 65
```

From NAT_home_side trace file


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

```
tcp
```

```
No.   Time   Source           Destination      Protocol  Info
   55 0.000  192.168.1.100    64.233.169.104   TCP       4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
   56 0.000  192.168.1.100    64.233.169.104   HTTP      GET / HTTP/1.1
   57 0.031  64.233.169.104   192.168.1.100    TCP       80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0
   58 0.017  64.233.169.104   192.168.1.100    TCP       80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=1430 [TCP segment of a reassem
   59 0.000  64.233.169.104   192.168.1.100    TCP       80 → 4335 [ACK] Seq=1431 Ack=636 Win=7040 Len=1430 [TCP segment of a reas
```

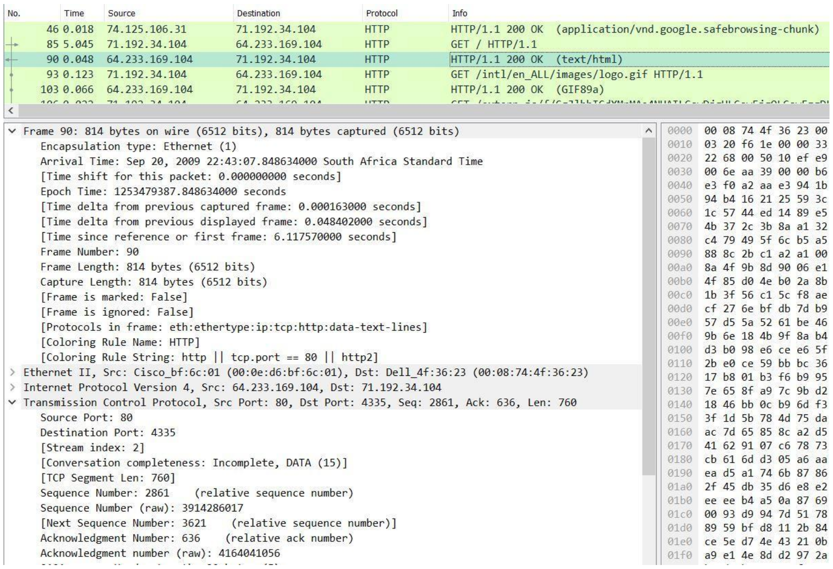
```
> Frame 56: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)
> Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
v Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 675
    Identification: 0xa2ac (41644)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0xa94a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.100
    Destination Address: 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
0010  02 a3 a2 ac 40 00 80 06  a9 4a
0020  a9 68 10 ef 00 50 f8 32  36 e5
0030  fe 14 ae f3 00 00 47 45  54 20
0040  2f 31 2e 31 0d 0a 48 6f  73 74
0050  67 6f 6f 67 6c 65 2e 63  6f 6d
0060  2d 41 67 65 6e 74 3a 20  4d 6f
0070  35 2e 30 20 28 57 69 6e  64 6f
0080  20 57 69 6e 64 6f 77 73  20 4e
0090  20 65 6e 2d 55 53 3b 20  72 76
00a0  2e 31 34 29 20 47 65 63  6b 6f
00b0  38 32 37 30 37 20 46 69  72 65
00c0  30 2e 31 34 20 28 2e 4e  45 54
00d0  2e 35 2e 33 30 37 32 39  29 0d
00e0  74 3a 20 74 65 78 74 2f  68 74
00f0  6c 69 63 61 74 69 6f 6e  2f 78
0100  6d 6c 2c 61 70 70 6c 69  63 61
0110  6d 6c 3b 71 3d 30 2e 39  2c 2a
0120  2e 38 0d 0a 41 63 63 65  70 74
0130  61 67 65 3a 20 65 6e 2d  75 73
0140  30 2e 35 0d 0a 41 63 63  65 70
0150  64 69 6e 67 3a 20 67 7a  69 70
0160  74 65 0d 0a 41 63 63 65  70 74
0170  65 74 3a 20 49 53 4f 2d  38 38
0180  74 66 2d 38 3b 71 3d 30  2e 37
0190  2e 37 0d 0a 4b 65 65 70  2d 41
01a0  33 30 30 0d 0a 43 6f 6e  6e 65
```

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?

Answer:

HTTP 200 OK message first time is 6.117570000 seconds
HTTP 200 OK message source IP is 64.233.169.104, and Port is 80
HTTP 200 OK message Destination IP is 71.192.34.104, and Port is 4335
Version is the same, and Flag does not change.
Time to live change
Header checksum changed
And the other different than the answer to question 4 above is that only the destination IP address has changed



```
No.    Time   Source           Destination      Protocol  Info
   46 0.018   74.125.106.31    71.192.34.104    HTTP      HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-chunk)
   85 5.045   71.192.34.104    64.233.169.104   HTTP      GET / HTTP/1.1
   90 0.048   64.233.169.104   71.192.34.104    HTTP      HTTP/1.1 200 OK  (text/html)
   93 0.123   71.192.34.104    64.233.169.104   HTTP      GET /intl/en_ALL/images/logo.gif HTTP/1.1
  103 0.066   64.233.169.104   71.192.34.104    HTTP      HTTP/1.1 200 OK  (GIF89a)
```

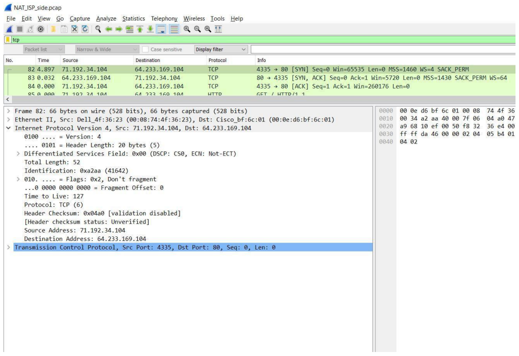
```
Frame 90: 814 bytes on wire (6512 bits), 814 bytes captured (6512 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 20, 2009 22:43:07.848634000 South Africa Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1253479387.848634000 seconds
    [Time delta from previous captured frame: 0.000163000 seconds]
    [Time delta from previous displayed frame: 0.048402000 seconds]
    [Time since reference or first frame: 6.117570000 seconds]
    Frame Number: 90
    Frame Length: 814 bytes (6512 bits)
    Capture Length: 814 bytes (6512 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
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]
    [Conversation completeness: Incomplete, DATA (15)]
    [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
```

```
0000  00 08 74 4f 36 23 00
0010  03 20 f6 1e 00 00 33
0020  22 68 00 50 10 ef e9
0030  00 6e aa 39 00 00 b6
0040  e3 f0 a2 aa e3 94 1b
0050  94 b4 16 21 25 59 3c
0060  1c 57 44 ed 14 89 e5
0070  4b 37 2c 3b 8a a1 32
0080  c4 79 49 5f 6c b5 a5
0090  88 8c 2b c1 a2 a1 00
00a0  8a 4f 9b 8d 90 06 e1
00b0  4f 85 d0 4e b0 2a 8b
00c0  1b 3f 56 c1 5c f8 ae
00d0  cf 27 6e bf db 7d b9
00e0  57 d5 5a 52 61 be 46
00f0  9b 6e 18 4b 9f 8a b4
0100  d3 b0 98 e6 ce e6 5f
0110  2b e0 ce 59 bb bc 36
0120  17 b8 01 b3 f6 b9 95
0130  7e 65 8f a9 7c 9b d2
0140  18 46 bb 0c b9 6d f3
0150  3f 1d 5b 78 4d 75 da
0160  ac 7d 65 85 8c a2 d5
0170  41 62 91 07 c6 78 73
0180  cb 61 6d d3 05 a6 aa
0190  ea d5 a1 74 6b 87 86
01a0  2f 45 db 35 d6 e8 e2
01b0  ee ee b4 a5 0a 87 69
01c0  00 93 d9 94 7d 51 78
01d0  89 59 bf d8 11 2b 84
01e0  ce 5e d7 4e 43 21 0b
01f0  a9 e1 4e 8d d2 97 2a
```

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?

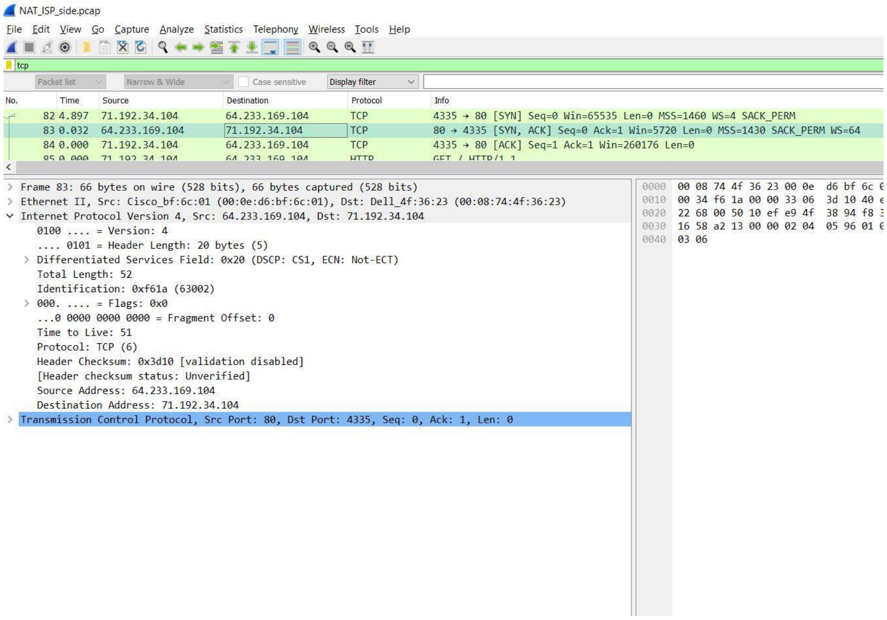
Answer:

For SYN:
The time is 6.035475000 seconds
Source IP Address is 71.192.34.104
Destination IP Address is 64.233.169.104


```
NAT_ISP_side.pcap
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help
tcp
Packet list    Narrow & Wide    Case sensitive    Display filter

No.     Time   Source          Destination     Protocol  Info
    82 4.897   71.192.34.104   64.233.169.104  TCP       4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM
    83 0.032   64.233.169.104  71.192.34.104   TCP       80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM WS=64
    84 0.000   71.192.34.104   64.233.169.104  TCP       4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
    85 0.000   71.192.34.104   64.233.169.104  HTTP      GET / HTTP/1.1

> 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)
v 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: 52
    Identification: 0xa2aa (41642)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 127
    Protocol: TCP (6)
    Header Checksum: 0x04a0 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 71.192.34.104
    Destination Address: 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
0010  00 34 a2 aa 40 00 7f 06  04 a0 47
0020  a9 68 10 ef 00 50 f8 32  36 e4 00
0030  ff ff da 46 00 00 02 04  05 b4 01
0040  04 02
```

For ACK:

Time is 6.067775000 seconds
Source IP Address is 64.233.169.104
Destination IP Address is 71.192.34.104


```
NAT_ISP_side.pcap
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help
tcp
Packet list    Narrow & Wide    Case sensitive    Display filter

No.     Time   Source          Destination     Protocol  Info
    82 4.897   71.192.34.104   64.233.169.104  TCP       4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM
    83 0.032   64.233.169.104  71.192.34.104   TCP       80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM WS=64
    84 0.000   71.192.34.104   64.233.169.104  TCP       4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
    85 0.000   71.192.34.104   64.233.169.104  HTTP      GET / HTTP/1.1

> 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)
v Internet Protocol Version 4, Src: 64.233.169.104, Dst: 71.192.34.104
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
    Total Length: 52
    Identification: 0xf61a (63002)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 51
    Protocol: TCP (6)
    Header Checksum: 0x3d10 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 64.233.169.104
    Destination Address: 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 0
0010  00 34 f6 1a 00 00 33 06  3d 10 40 e
0020  22 68 00 50 10 ef e9 4f  38 94 f8 3
0030  16 58 a2 13 00 00 02 04  05 96 01 0
0040  03 06
```

The different than the answer to question 5 above is that time to live changed, and for the SYN, the source IP address has changed, For the ACK, the destination IP address has changed. The port numbers are unchanged.

In Summar, The time to live, identification, Flags, Source and Destination IP changed

Figure 4.22 in the text shows the NAT translation table in the NAT router.

10. Using your answers to 1-8 above, fill in the NAT translation table entries for HTTP connection considered in questions 1-8 above.

Answer:

NAT translation table	
WAN side	***LAN side***
IP:71.192.34.104 ***and Port:4335***	***IP: 192.168.1.100 and port: 4335***

Extra Credit: The trace files investigated above have additional connections to Google servers above and beyond the HTTP GET, 200OK request/response studied above. For example, in the NAT_home_side trace file, consider the client-to-server GET at time 1.573215, and the GET at time 7.573305. Research the use of these two HTTP messages and write a half page explanation of the purpose of each of these messages.

Answer:

Users are protected from harmful or unwelcome programs by Google Safebrowsing. Safebrowsing runs a website through Google's most recent list of dangerous websites whenever a user clicks on a link in the search results page. If a client visits an insecure website that has questionable software or viruses, a warning screen appears. The HTTP request and response are visible in the NAT_home_side trace file, demonstrating safebrowsing in action.

The request URL "safebrowsing cache.google.com/safebrowsing/rd/googlemalware-shaver_s_15361-15365.15661-15 365" is included in the HTTP GET header at frame 20 at time 1.572315.

In HTTP GET at frame 104, time 7.573305, the request URL "google.com/generate_204" is included in the header. The first URL sends users to the safebrowsing cache site, whereas the second URL sends them to the destination website, which is safe to browse. The two HTTP GET messages that I examined yielded some intriguing findings.

The destination IP changed from 74.125.106.31 to 74.125.91.113 between frames 20 and 104. As a result of the changing destination address and the fact that each one had a separate uniquely allocated number, the header checksums and identification also varied. At frames 52 and 96, the source IP switches from 74.125.106.31 (safebrowsing cache.google.com) to 64.233.169.104 (www.google.com), respectively, before returning to 74.125.106.31 (clients1.google.com) between frames 20 and 104. Both times, DNS requests and requests' responses are present. We might conclude that a Google search was performed in frame 96. recording activities when a webpage is accessed using the Google search engine using WireShark. However, the safebrowsing frame was not to be found.