

# Lab 5 - Network Address Translation

## Computer Networks

Thang Huu Nguyen - 1713239

### 1 What is the IP address of the client?

| No. | Time     | Source         | Destination    | Protocol | Length | Info   |
|-----|----------|----------------|----------------|----------|--------|--|
| 7   | 1.208040 | 192.168.1.100  | 74.125.91.113  | HTTP     | 1035   | POST /safebrowsing/downloads?                  |
| 11  | 1.274062 | 74.125.91.113  | 192.168.1.100  | HTTP     | 853    | HTTP/1.1 200 OK (application...                |
| 13  | 1.528648 | 74.125.91.113  | 192.168.1.100  | HTTP     | 853    | [TCP Spurious Retransmission]                  |
| 20  | 1.572315 | 192.168.1.100  | 74.125.106.31  | HTTP     | 767    | GET /safebrowsing/rd/goog-mall                 |
| 39  | 1.677779 | 74.125.106.31  | 192.168.1.100  | HTTP     | 651    | HTTP/1.1 200 OK (application...                |
| 41  | 1.976996 | 192.168.1.100  | 74.125.106.31  | HTTP     | 772    | GET /safebrowsing/rd/goog-mall                 |
| 42  | 2.000629 | 74.125.106.31  | 192.168.1.100  | HTTP     | 881    | HTTP/1.1 200 OK (application...                |
| 43  | 2.014105 | 192.168.1.100  | 74.125.106.31  | HTTP     | 776    | GET /safebrowsing/rd/goog-phi                  |
| 44  | 2.038247 | 74.125.106.31  | 192.168.1.100  | HTTP     | 526    | HTTP/1.1 200 OK (application...                |
| 45  | 2.044751 | 192.168.1.100  | 74.125.106.31  | HTTP     | 776    | GET /safebrowsing/rd/goog-phi                  |
| 46  | 2.064877 | 74.125.106.31  | 192.168.1.100  | HTTP     | 1089   | HTTP/1.1 200 OK (application...                |
| 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                   |
| 63  | 7.349451 | 64.233.169.104 | 192.168.1.100  | HTTP     | 226    | HTTP/1.1 200 OK (GIF89a)                       |
| 73  | 7.349451 | 64.233.169.104 | 192.168.1.100  | HTTP     | 809    | GET /extern_js/f/CgJlbhIcdXMrMa04NUAIlCswDjgH  |
| 75  | 7.370185 | 192.168.1.100  | 64.233.169.104 | HTTP     | 648    | HTTP/1.1 200 OK (text/javascript)              |
| 92  | 7.448649 | 64.233.169.104 | 192.168.1.100  | HTTP     | 695    | GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1. |
| 94  | 7.492324 | 192.168.1.100  | 64.233.169.104 | HTTP     | 870    | HTTP/1.1 200 OK (text/html)                    |
| 107 | 7.537353 | 64.233.169.104 | 192.168.1.100  | HTTP     | 712    | GET /images/nav_logo7.png HTTP/1.1             |
| 107 | 7.652836 | 192.168.1.100  | 64.233.169.104 | HTTP     | 806    | GET /csi?v=3&s=webhp&action=&tran=undefined&e  |
| 112 | 7.682361 | 192.168.1.100  | 64.233.169.104 | HTTP     | 1359   | HTTP/1.1 200 OK (PNG)                          |
| 119 | 7.685786 | 64.233.169.104 | 192.168.1.100  | HTTP     | 670    | GET /favicon.ico HTTP/1.1                      |
| 122 | 7.709490 | 192.168.1.100  | 64.233.169.104 | HTTP     | 269    | HTTP/1.1 204 No Content                        |
| 124 | 7.737783 | 64.233.169.104 | 192.168.1.100  | HTTP     | 1204   | HTTP/1.1 200 OK (image/x-icon)                 |
| 127 | 7.763501 | 64.233.169.104 | 192.168.1.100  | HTTP     | 1204   | HTTP/1.1 200 OK (image/x-icon)                 |

Answers: The IP address of the client is 192.168.1.100

### 2 The client actually communicates with several different Google servers in order to implement "safe browsing." (See extra credit section at the end of this lab). The main Google server that will serve up the main Google web page has IP address 64.233.169.104. In order to display only those frames containing HTTP messages that are sent to/from this Google, server, enter the expression "http && ip.addr == 64.233.169.104" (without quotes) into the Filter: field in Wireshark .

| 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/CgJlbhIcdXMrMa04NUAIlCswDjgH  |
| 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. |
| 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  |
| 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)                 |

- 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?

| 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 |
| 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/CgJlbhICdXMrMA  |
| 92  | 7.448649 | 64.233.169.104 | 192.168.1.100  | HTTP     | 648    | HTTP/1.1 200 OK (text/javascrip  |
| 94  | 7.492324 | 192.168.1.100  | 64.233.169.104 | HTTP     | 695    | GET /extern_chrome/ee36edbd3c16  |
| 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 |
| 112 | 7.682361 | 192.168.1.100  | 64.233.169.104 | HTTP     | 806    | GET /csi?v=3&s=webhp&action=&tr  |
| 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

```

Answers:

- The source IP address is 192.168.1.100
- The destination IP address is 64.233.169.104
- TCP source port is 4335
- TCP destination port is 80

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

| 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 |
| 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/CgJlbhICdXMrMA  |
| 92  | 7.448649 | 64.233.169.104 | 192.168.1.100  | HTTP     | 648    | HTTP/1.1 200 OK (text/javascrip  |
| 94  | 7.492324 | 192.168.1.100  | 64.233.169.104 | HTTP     | 695    | GET /extern_chrome/ee36edbd3c16  |
| 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 |
| 112 | 7.682361 | 192.168.1.100  | 64.233.169.104 | HTTP     | 806    | GET /csi?v=3&s=webhp&action=&tr  |
| 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
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 2861, Ack: 636, Len: 760
▶ [3 Reassembled TCP Segments (3620 bytes): #58(1430), #59(1430), #60(760)]
▶ Hypertext Transfer Protocol
▶ Line-based text data: text/html (12 lines)

```

Answers:

- 200 OK HTTP message received from the Google server at 7.158797

- The source IP address is 64.233.169.104
- The destination IP address is 192.168.1.100
- TCP source port is 80
- TCP destination port is 4335

5 At what time is the client-to-server TCP SYN segment sent that sets up the connection used by the GET sent at time 7.109267? 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?

| No. | Time     | Source         | Destination    | Protocol | Length | Info                                |
|-----|----------|----------------|----------------|----------|--------|-------------------------------------|
| 46  | 2.064877 | 74.125.106.31  | 192.168.1.100  | HTTP     | 1089   | HTTP/1.1 200 OK (applicatio         |
| 47  | 2.178596 | 192.168.1.100  | 74.125.106.31  | TCP      | 54     | 4331 → 80 [ACK] Seq=2876 Ack        |
| 53  | 7.075657 | 192.168.1.100  | 64.233.169.104 | TCP      | 66     | 4335 → 80 [SYN] Seq=0 Win=65        |
| 54  | 7.108986 | 64.233.169.104 | 192.168.1.100  | TCP      | 66     | 80 → 4335 [SYN, ACK] Seq=0 Win=65   |
| 55  | 7.109053 | 192.168.1.100  | 64.233.169.104 | TCP      | 54     | 4335 → 80 [ACK] Seq=1 Ack=1         |
| 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=63        |
| 58  | 7.158432 | 64.233.169.104 | 192.168.1.100  | TCP      | 1484   | 80 → 4335 [ACK] Seq=1 Ack=63        |
| 59  | 7.158761 | 64.233.169.104 | 192.168.1.100  | TCP      | 1484   | 80 → 4335 [ACK] Seq=1431 Ack=63     |
| 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=63      |
| 62  | 7.281399 | 192.168.1.100  | 64.233.169.104 | HTTP     | 719    | GET /intl/en_ALL/images/logo        |
| 63  | 7.315019 | 64.233.169.104 | 192.168.1.100  | TCP      | 309    | 80 → 4335 [PSH, ACK] Seq=362 Ack=63 |
| 64  | 7.315576 | 64.233.169.104 | 192.168.1.100  | TCP      | 1484   | 80 → 4335 [ACK] Seq=3876 Ack=63     |
| 65  | 7.315576 | 64.233.169.104 | 192.168.1.100  | TCP      | 54     | 4335 → 80 [ACK] Seq=3876 Ack=63     |

▶ 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

Answers:

- The client-to-server TCP SYN segment sent that sets up the connection used by the GET sent at time 7.109267 is segment at 7.075657
- The source IP address is 192.168.1.100
- The destination IP address is 64.233.169.104
- The source port is 4335
- The destination port is 80
- This ACK received at 7.108986

- 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?

| 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  |
| 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/CgJlbhICdXMrMAo4 |
| 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/ee36edbd3c16a1 |
| 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. |
| 144 | 6.642308 | 71.192.34.104  | 64.233.169.104 | HTTP     | 806    | GET /csi?v=3&s=webhp&action=&trar |
| 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)<br>▶ Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01)<br>▶ Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104<br>▶ Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635<br>▶ Hypertext Transfer Protocol |
|---|

Answers:

- This message appear in the NAT\_ISP\_side at 6.069168
- Source: 71.192.34.104:4335
- Destination: 64.233.169.104:80
- Only the source IP address has changed

- 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.

Answers:

- No. Not all have changed
- The fields in the IP datagram carrying the HTTP GET are changed: Checksum
- Because the IP source address has changed, and the checksum includes the value of the source IP address, the checksum has changed

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

| No. | Time     | Source         | Destination    | Protocol | Length | Info  |
|-----|----------|----------------|----------------|----------|--------|---|
| 85  | 6.069168 | 71.192.34.104  | 64.233.169.104 | HTTP     | 689    | GET / HTTP/1.1                                  |
| 93  | 6.241357 | 71.192.34.104  | 64.233.169.104 | HTTP     | 719    | GET /intl/en_ALL/images/logo.gif HTTP/1.1       |
| 106 | 6.330131 | 71.192.34.104  | 64.233.169.104 | HTTP     | 809    | GET /extern_js/f/CgJlbhICdXMrMAo4NUAII HTTP/1.1 |
| 125 | 6.452270 | 71.192.34.104  | 64.233.169.104 | HTTP     | 695    | GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.1 |
| 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=und HTTP/1.1  |
| 154 | 6.669397 | 71.192.34.104  | 64.233.169.104 | HTTP     | 670    | GET /favicon.ico HTTP/1.1                       |
| 90  | 6.117570 | 64.233.169.104 | 71.192.34.104  | HTTP     | 814    | HTTP/1.1 200 OK (text/html)                     |
| 103 | 6.308118 | 64.233.169.104 | 71.192.34.104  | HTTP     | 226    | HTTP/1.1 200 OK (GIF89a)                        |
| 121 | 6.407366 | 64.233.169.104 | 71.192.34.104  | HTTP     | 648    | HTTP/1.1 200 OK (text/javascript)               |
| 131 | 6.496234 | 64.233.169.104 | 71.192.34.104  | HTTP     | 870    | HTTP/1.1 200 OK (text/html)                     |
| 149 | 6.644609 | 64.233.169.104 | 71.192.34.104  | HTTP     | 1359   | HTTP/1.1 200 OK (PNG)                           |
| 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 90: 814 bytes on wire (6512 bits), 814 bytes captured (6512 bits)<br>▶ Ethernet II, Src: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)<br>▶ Internet Protocol Version 4, Src: 64.233.169.104, Dst: 71.192.34.104<br>▶ Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 2861, Ack: 636, Len: 760<br>▶ [3 Reassembled TCP Segments (3620 bytes): #88(1430), #89(1430), #90(760)]<br>▶ Hypertext Transfer Protocol<br>▶ Line-based text data: text/html (12 lines) |
|---|

Answers:

- The first 200 OK HTTP message received at 6.117570
- Source: 64.233.169.104:80
- Destination: 71.192.34.104:4335
- Only the destination IP address has changed

- 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?

Answers:

- The time of client-to-server TCP SYN segment and the server-to-client TCP ACK segment are 6.035475 and 6.067775, respectively
- SYN segment: source(71.192.34.104:4335) and destination(64.233.169.104:80)
- ACK segment: source(64.233.169.104:80) and destination(71.192.34.104:4335)
- For the SYN, the source IP address has changed, For the ACK, the destination IP address has changed. The port numbers are unchanged

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

Answers:

| NAT translate table |                    |
|---------------------|--------------------|
| WAN side            | LAN side           |
| 71.192.34.104:4335  | 192.168.1.100:4335 |