

ASSIGNMENT 2:

NAME: Stuti Parmar

STUDENT ID: 218516625

EECS 3214

Question 2: Understanding NAT

#2-A

Q.3 At time 7.109267, the source address is: 192.168.1.100 and destination IP address is: 64.233.169.104.

- The source port of TCP is: 4335 and destination port of TCP: 80.

| Source IP and port | Destination IP and port |
|------------------------|-------------------------|
| 192.168.1.100 and 4335 | 64.233.169.104 and 80 |

The image shows a Wireshark packet capture of an HTTP GET request. The packet list pane at the top shows a list of packets, with packet 56 selected. The packet details pane on the left shows the structure of the selected packet, and the packet bytes pane on the right shows the raw data in hexadecimal and ASCII.

Packet List:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|---------------|----------------|----------|--------|---|
| 20 | 1.572315 | 192.168.1.100 | 74.125.106.31 | HTTP | 767 | GET /safebrowsing/rd/goog-malware-shavar_s_15361-15365.15361-15365.: HTTP/1.1 |
| 41 | 1.976996 | 192.168.1.100 | 74.125.106.31 | HTTP | 772 | GET /safebrowsing/rd/goog-malware-shavar_a_14466-14470.14466-14470: HTTP/1.1 |
| 43 | 2.014185 | 192.168.1.100 | 74.125.106.31 | HTTP | 776 | GET /safebrowsing/rd/goog-phish-shavar_s_48291-48300.48291-48295.48296-48300: HTTP/1.1 |
| 45 | 2.044751 | 192.168.1.100 | 74.125.106.31 | HTTP | 776 | GET /safebrowsing/rd/goog-phish-shavar_a_67721-67760.67721-67729.67730-67760: HTTP/1.1 |
| 56 | 7.109267 | 192.168.1.100 | 64.233.169.104 | HTTP | 689 | GET / HTTP/1.1 |
| 62 | 7.281399 | 192.168.1.100 | 64.233.169.104 | HTTP | 719 | GET /intl/en_ALL/images/logo.gif HTTP/1.1 |
| 75 | 7.370185 | 192.168.1.100 | 64.233.169.104 | HTTP | 809 | GET /extern_js/f/CgJlbhICdXMmMAo4NUAILCswDjgHLCswFjgQLCswFzgDLCswGDgELCswHTgJLCswJTjJiAEsKzAmO... |
| 94 | 7.492324 | 192.168.1.100 | 64.233.169.104 | HTTP | 695 | GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.1 |
| 104 | 7.573305 | 192.168.1.100 | 74.125.91.113 | HTTP | 709 | GET /generate_204 HTTP/1.1 |
| 107 | 7.652836 | 192.168.1.100 | 64.233.169.104 | HTTP | 712 | GET /images/nav_logo7.png HTTP/1.1 |
| 112 | 7.682361 | 192.168.1.100 | 64.233.169.104 | HTTP | 806 | GET /csi?v=3&s=webhp&action=&tran=undefined&e=17259,21588,21766,21920&ei=2502Ssb1G4_CeJvxxaM0&rt=prt.1... |
| 122 | 7.709490 | 192.168.1.100 | 64.233.169.104 | HTTP | 670 | GET /favicon.ico HTTP/1.1 |

Packet Details:

0010 Identification: 0xa2ac (41644)
0020 > 010. = Flags: 0x2, Don't fragment
0030 ...0 0000 0000 0000 = Fragment Offset: 0
0040 Time to Live: 128
0050 Protocol: TCP (6)
0060 Header Checksum: 0xa94a (validation disabled)
0070 [Header checksum status: Unverified]
0080 Source Address: 192.168.1.100
0090 Destination Address: 64.233.169.104
0100 Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
0110 Source Port: 4335
0120 Destination Port: 80
0130 [Stream index: 2]
0140 [Conversation completeness: Incomplete, DATA (15)]
0150 [TCP Segment Len: 635]
0160 Sequence Number: 1 (relative sequence number)
0170 Sequence Number (raw): 4164040421
0180 [Next Sequence Number: 636 (relative sequence number)]
0190 Source Address (ip.src), 4 bytes

Packet Bytes:

0010 02 a3 a2 ac 40 00 80 06 a9 4a c0 a8 0
0020 a9 68 10 ef 00 50 f8 32 36 e5 e9 4f 3
0030 fe 14 ae f3 00 00 47 45 54 20 2f 20 4
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 7
0050 67 6f 6f 67 6c 65 2e 63 6f 6d 0d 0a 5
0060 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6
0070 35 2e 30 20 28 57 69 6e 64 6f 77 73 3
0080 20 57 69 6e 64 6f 77 73 20 4e 54 20 3
0090 20 65 6e 2d 55 53 3b 20 72 76 3a 31 2
00a0 2e 31 34 29 20 47 65 63 6b 6f 2f 32 3
00b0 38 32 37 30 37 20 46 69 72 65 66 6f 7
00c0 30 2e 31 34 20 28 2e 4e 45 54 20 43 4
00d0 2e 35 2e 33 30 37 32 39 29 0d 0a 41 6
00e0 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2
00f0 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6
0100 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6
0110 6d 6c 3b 71 3d 30 2e 39 2c 2a 2f 2a 3
0120 2e 38 0d 0a 41 63 63 65 70 74 2d 4c 6
0130 61 67 65 3a 20 65 6e 2d 75 73 2c 65 6
0140 30 2e 35 0d 0a 41 63 63 65 70 74 2d 4
0150 64 69 6e 67 3a 20 67 7a 69 70 2c 64 6

#2-B

Q.7 Version: This is 4 for IPv4 and remains the same, doesn't change.

- Header Length: 20 bytes (5)
- Flags: window - 65044
- Checksum: 0x3e2b (unverified)
- The Timestamp changed to 6.612801 but the source port and destination port of TCP remains same.
- Header length has not changed and remains the same. If IP options are added or removed.
- Flags can change if the packet is fragmented.
- Checksum has changed. Must change if any other part of the IP header changes, as it is a checksum for the header itself.

The image shows a Wireshark packet capture of an HTTP GET request. The packet list at the top shows a series of packets, with packet 139 selected. The packet details pane shows the structure of the packet, including the Internet Protocol Version 4 header, the Transmission Control Protocol header, and the Hypertext Transfer Protocol body.

| 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_15361-15365.15361-15365.: HTTP/1.1 |
| 41 | 0.936824 | 71.192.34.104 | 74.125.106.31 | HTTP | 772 | GET /safebrowsing/rd/goog-malware-shavar_a_14466-14470.14466.14467-14470: HTTP/1.1 |
| 43 | 0.973893 | 71.192.34.104 | 74.125.106.31 | HTTP | 776 | GET /safebrowsing/rd/goog-phish-shavar_s_48291-48300.48291-48295.48296-48300: HTTP/1.1 |
| 45 | 1.004530 | 71.192.34.104 | 74.125.106.31 | HTTP | 776 | GET /safebrowsing/rd/goog-phish-shavar_a_67721-67760.67721-67729.67730-67760: HTTP/1.1 |
| 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/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswFzgDLCswGdgELCswGTgJLCswHTgZLCswJTjJiAEsKzAm0... |
| 125 | 6.452270 | 71.192.34.104 | 64.233.169.104 | HTTP | 695 | GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.1 |
| 135 | 6.533219 | 71.192.34.104 | 74.125.91.113 | HTTP | 709 | GET /generate_204 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=undefined&e=17259,21588,21766,21920&ei=2502Ssb1G4_CeJvxxaM0&rt=prt.1... |
| 154 | 6.669397 | 71.192.34.104 | 64.233.169.104 | HTTP | 670 | GET /favicon.ico HTTP/1.1 |

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: 698
- Identification: 0xa2de (41694)
- > 010. = Flags: 0x2, Don't fragment
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 127**
- Protocol: TCP (6)
- Header Checksum: 0x01e6 [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: 2697, Ack: 30902, Len: 658

- Source Port: 4335
- Destination Port: 80
- [Stream index: 2]
- > [Conversation completeness: Incomplete, DATA (15)]
- [TCP Segment Len: 658]
- Sequence Number: 2697 (relative sequence number)

NAT_ISP_side.pcap Packets: 210 - Displayed: 12 (5.7%) Profile: Default

#2-C

Q.10

| WAN side IP and port | LAN side IP and port |
|---|---|
| Source Address: 71.192.34.104 Port: 4335 | Source Address: 192.168.1.100 Port: 4335 |