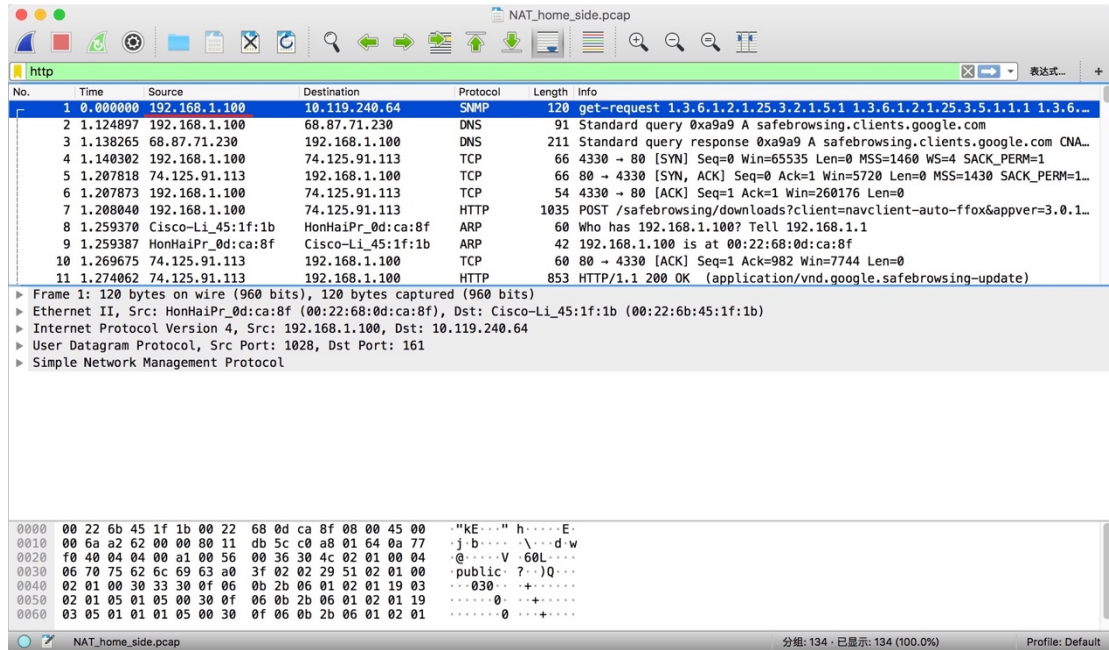


1. IP address of client: 192.168.1.100



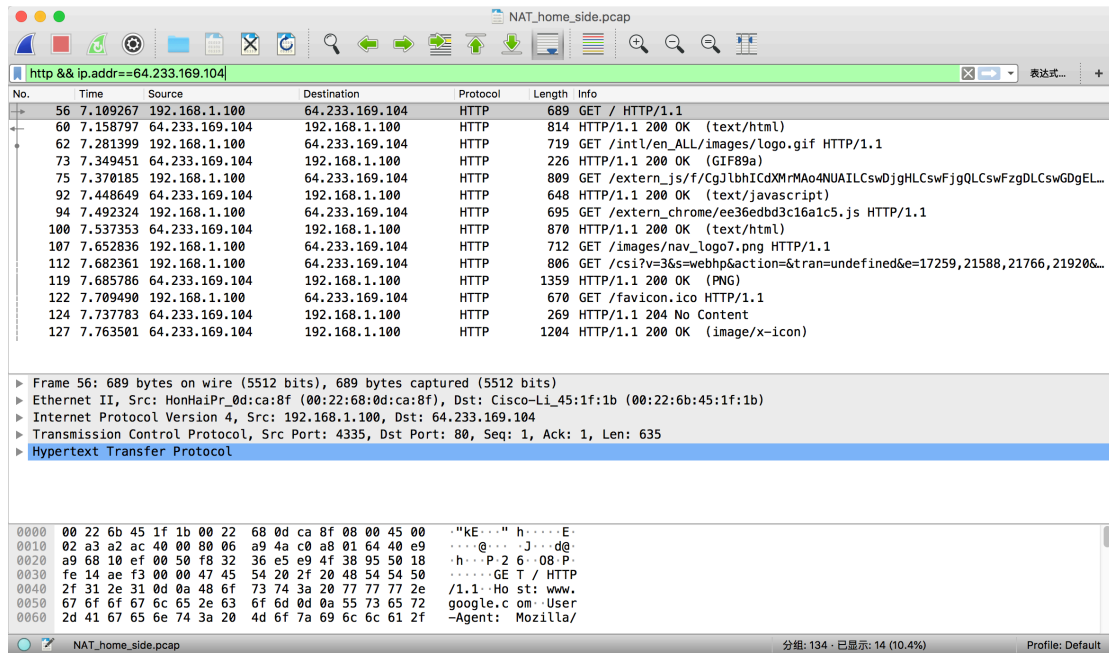
Wireshark packet capture of NAT_home_side.pcap. The filter is set to http. The selected packet is packet 11, an HTTP POST request from 192.168.1.100 to 10.119.240.64. The packet details show the Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Simple Network Management Protocol layers. The packet bytes show the raw data of the HTTP request.

| 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 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1.1.1 |
| 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.google.com CNAME |
| 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_PERM=1 |
| 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 SACK_PERM=1 |
| 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&appver=3.0.1.1 |
| 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 |
| 11 | 1.274062 | 74.125.91.113 | 192.168.1.100 | HTTP | 853 | HTTP/1.1 200 OK (application/vnd.google.safebrowsing-update) |

Frame 11: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) on interface 0
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
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 00 00 45 00 "kE..." h.....E
0010 00 6a a2 62 00 00 00 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 03 ...030...+.....
0050 02 01 05 01 05 00 30 0f 06 0b 2b 06 01 02 01 190...+.....
0060 03 05 01 01 01 05 00 30 0f 06 0b 2b 06 01 02 010...+.....

2.



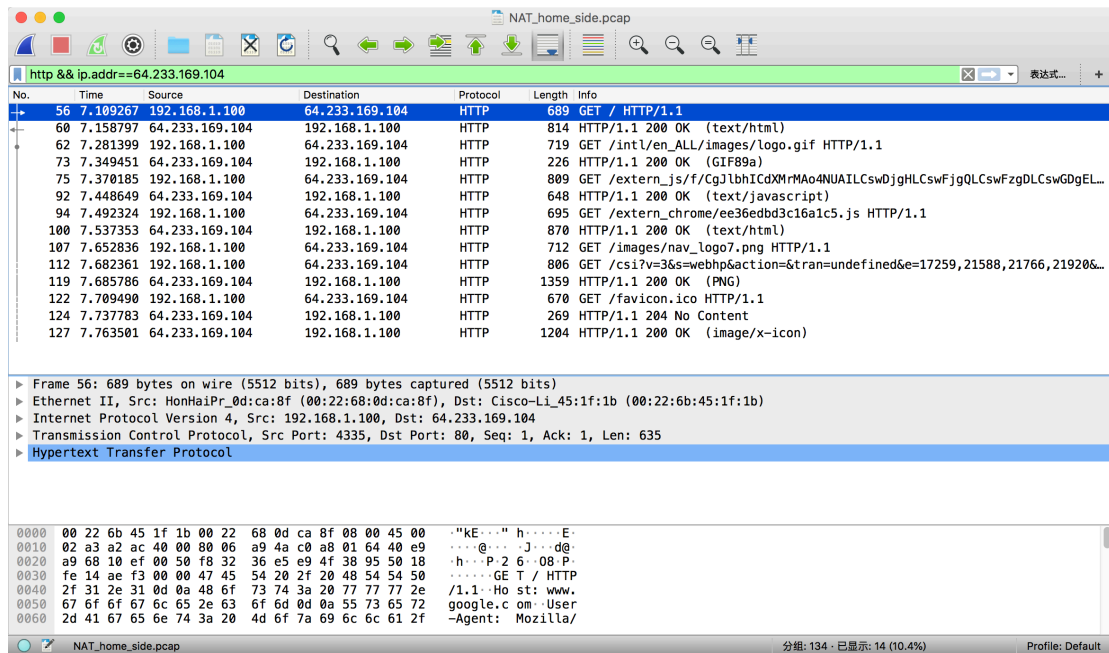
Wireshark packet capture of NAT_home_side.pcap. The filter is set to http && ip.addr==64.233.169.104. The selected packet is packet 56, an HTTP GET request from 192.168.1.100 to 64.233.169.104. The packet details show the Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol layers. The packet bytes show the raw data of the HTTP request.

| 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/CgJlbhICdXMfMAo4NUAILCswDjgHLCswFjgQLCswFzgdLCswGDgEL... |
| 92 | 7.448649 | 64.233.169.104 | 192.168.1.100 | HTTP | 648 | HTTP/1.1 200 OK (text/javascript) |
| 94 | 7.492324 | 192.168.1.100 | 64.233.169.104 | HTTP | 695 | GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.1 |
| 100 | 7.537353 | 64.233.169.104 | 192.168.1.100 | HTTP | 870 | HTTP/1.1 200 OK (text/html) |
| 107 | 7.652836 | 192.168.1.100 | 64.233.169.104 | HTTP | 712 | GET /images/nav_logo7.png HTTP/1.1 |
| 112 | 7.682361 | 192.168.1.100 | 64.233.169.104 | HTTP | 806 | GET /csi?v=3&s=webhp&action=&tran=undefined&e=17259,21588,21766,21920&... |
| 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) on interface 0
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 00 00 45 00 "kE..." h.....E
0010 02 a3 a2 ac 40 00 00 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...08P
0030 fe 14 ae f3 00 00 47 45 54 20 2f 20 48 54 50G.T./ HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 2e /1.1: Ho st: www.
0050 67 6f 6f 6f 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/

3. source: 192.168.1.100,4335 destination: 64.233.169.104,80



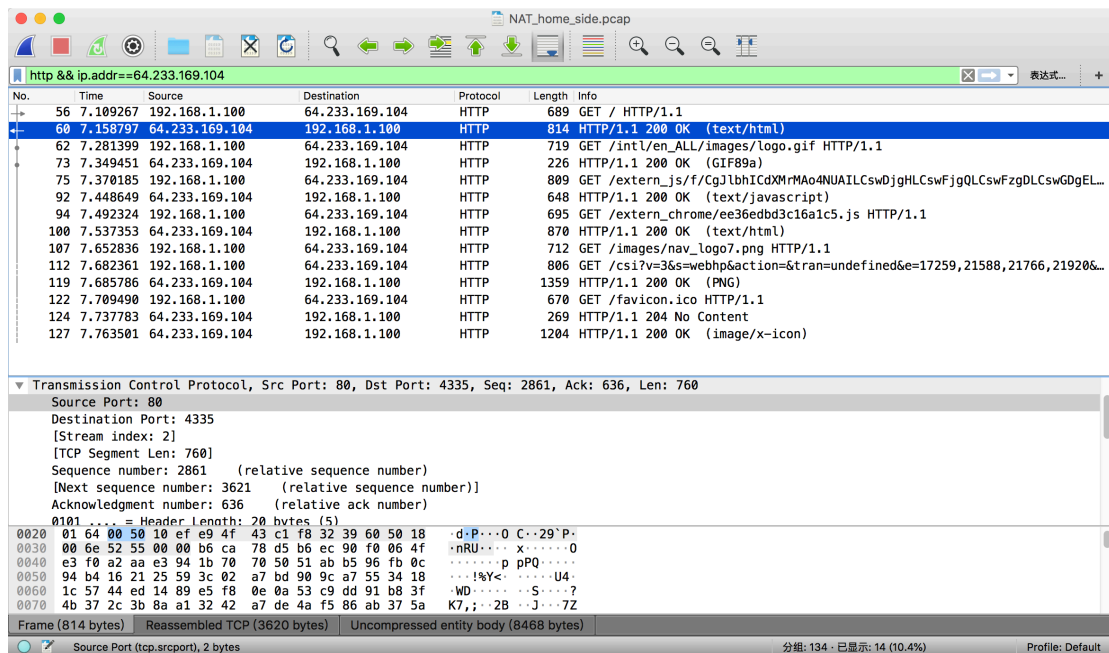
Wireshark packet capture of NAT_home_side.pcap. The filter is 'http && ip.addr==64.233.169.104'. The packet list shows a series of HTTP requests and responses. The selected packet is packet 56, which is a GET request for 'http://64.233.169.104/'.

| 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/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswFzgDLCswGDgEL... |
| 92 | 7.448649 | 64.233.169.104 | 192.168.1.100 | HTTP | 648 | HTTP/1.1 200 OK (text/javascript) |
| 94 | 7.492324 | 192.168.1.100 | 64.233.169.104 | HTTP | 695 | GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.1 |
| 100 | 7.537353 | 64.233.169.104 | 192.168.1.100 | HTTP | 870 | HTTP/1.1 200 OK (text/html) |
| 107 | 7.652836 | 192.168.1.100 | 64.233.169.104 | HTTP | 712 | GET /images/nav_logo7.png HTTP/1.1 |
| 112 | 7.682361 | 192.168.1.100 | 64.233.169.104 | HTTP | 806 | GET /csi?v=3&s=webhp&action=&tran=undefined&e=17259,21588,21766,21920&... |
| 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) on interface 0
Ethernet II, Src: NonHaPr_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 00 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...08 P
0030 fe 14 ae f3 00 00 47 45 54 20 2f 20 48 54 54 50GE T / HTTP
0040 2f 31 2e 31 04 0a 48 6f 73 74 3a 20 77 77 72 e /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/

4. time: 7.158797 source : 64.233.169.104,80 destination : 192.168.1.100,4335



Wireshark packet capture of NAT_home_side.pcap. The filter is 'http && ip.addr==64.233.169.104'. The packet list shows a series of HTTP requests and responses. The selected packet is packet 60, which is a 200 OK response for 'http://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/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswFzgDLCswGDgEL... |
| 92 | 7.448649 | 64.233.169.104 | 192.168.1.100 | HTTP | 648 | HTTP/1.1 200 OK (text/javascript) |
| 94 | 7.492324 | 192.168.1.100 | 64.233.169.104 | HTTP | 695 | GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.1 |
| 100 | 7.537353 | 64.233.169.104 | 192.168.1.100 | HTTP | 870 | HTTP/1.1 200 OK (text/html) |
| 107 | 7.652836 | 192.168.1.100 | 64.233.169.104 | HTTP | 712 | GET /images/nav_logo7.png HTTP/1.1 |
| 112 | 7.682361 | 192.168.1.100 | 64.233.169.104 | HTTP | 806 | GET /csi?v=3&s=webhp&action=&tran=undefined&e=17259,21588,21766,21920&... |
| 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) |

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)
0020 01 64 00 50 10 ef e9 4f 43 c1 f8 32 39 60 50 18 .d.P...0 C...29'P
0030 00 6e 52 55 00 00 b6 ca 78 d5 b6 ec 90 f0 06 4f .nRU...x.....0
0040 e3 f0 a2 aa e3 94 1b 70 70 50 51 ab b5 96 f0 0cp pPQ:...
0050 94 b4 16 21 25 59 3c 02 a7 bd 90 9c a7 55 34 18 ...I&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)

5. time : 7.075657 Source : 192.168.1.100,4335 destination: 64.233.169.104,80

source : 64.233.169.104,80 destination : 192.168.1.100,4335 time: 7.109481

Wireshark packet capture for NAT_home_side.pcap. The filter is 'http && ip.addr==64.233.169.104'. The selected packet is No. 56, a GET request from 192.168.1.100 to 64.233.169.104. The packet details show the Hypertext Transfer Protocol section with a status of 200 OK.

| 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/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswFzgDLCswGDgEL... |
| 92 | 7.448649 | 64.233.169.104 | 192.168.1.100 | HTTP | 648 | HTTP/1.1 200 OK (text/javascript) |
| 94 | 7.492324 | 192.168.1.100 | 64.233.169.104 | HTTP | 695 | GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.1 |
| 100 | 7.537353 | 64.233.169.104 | 192.168.1.100 | HTTP | 870 | HTTP/1.1 200 OK (text/html) |
| 107 | 7.652836 | 192.168.1.100 | 64.233.169.104 | HTTP | 712 | GET /images/nav_logo7.png HTTP/1.1 |
| 112 | 7.682361 | 192.168.1.100 | 64.233.169.104 | HTTP | 806 | GET /csi?v=3&s=webhp&action=&tran=undefined&e=17259,21588,21766,21920&... |
| 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) |

6. time : 6.069168 source : 71.192.34.104,4335 destiantion :64.233.169.104,80

only the source IP address changed.

Wireshark packet capture for NAT_JSP_side.pcap. The filter is 'http'. The selected packet is No. 85, a GET request from 71.192.34.104 to 64.233.169.104. The packet details show the Hypertext Transfer Protocol section with a status of 200 OK.

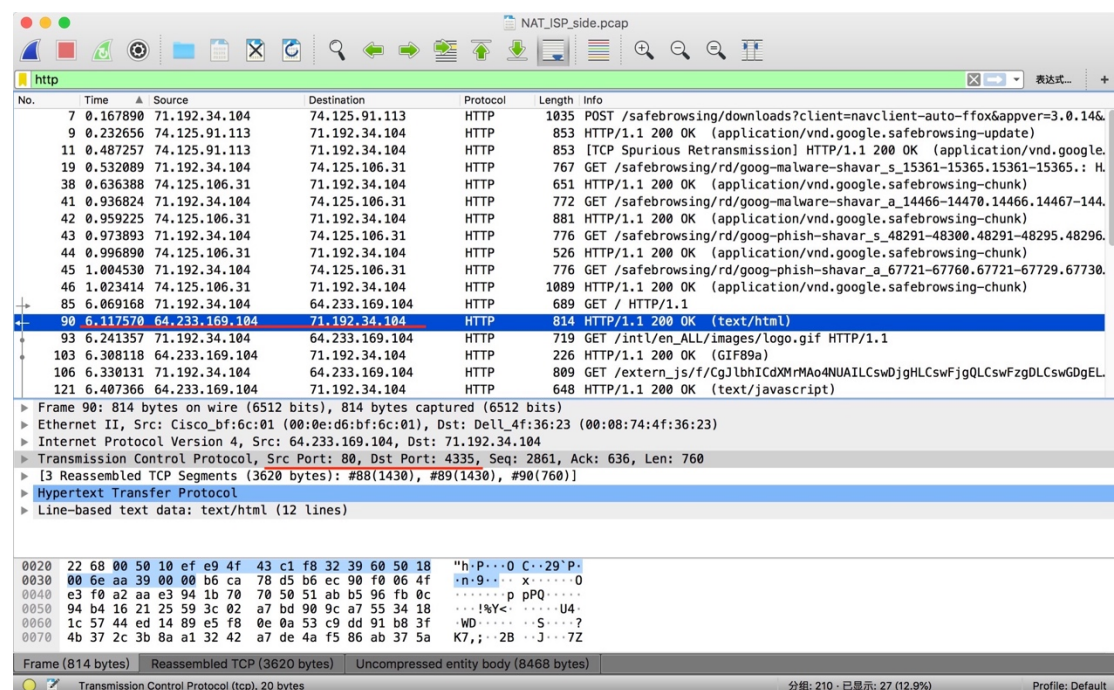
| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|---|
| 46 | 1.023414 | 74.125.106.31 | 71.192.34.104 | HTTP | 1089 | HTTP/1.1 200 OK (application/vnd.google.safebrowsing-chunk) |
| 85 | 6.069168 | 71.192.34.104 | 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/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswFzgDLCswGDgEL... |
| 121 | 6.407366 | 64.233.169.104 | 71.192.34.104 | HTTP | 648 | HTTP/1.1 200 OK (text/javascript) |
| 125 | 6.452270 | 71.192.34.104 | 64.233.169.104 | HTTP | 695 | GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.1 |
| 131 | 6.496234 | 64.233.169.104 | 71.192.34.104 | HTTP | 870 | HTTP/1.1 200 OK (text/html) |
| 135 | 6.533219 | 71.192.34.104 | 74.125.91.113 | HTTP | 709 | GET /generate_204 HTTP/1.1 |
| 137 | 6.590706 | 74.125.91.113 | 71.192.34.104 | HTTP | 179 | HTTP/1.1 204 No Content |
| 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&... |
| 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) |

7. No HTTP GET message chaged. Version:No , Header Length : No , Flags:No

Checksum : Yes Reason : because the IP source address changed,checksum changed too,including the value of source IP.

8. time : 6.117570 source :64.233.169.104,80 destination 71.192.34.104,4335

only the destiantion IP address changed.



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|---|
| 7 | 0.167890 | 71.192.34.104 | 74.125.91.113 | HTTP | 1035 | POST /safebrowsing/downloads?client=navclient-auto-ffox&appver=3.0.146. |
| 9 | 0.232656 | 74.125.91.113 | 71.192.34.104 | HTTP | 853 | HTTP/1.1 200 OK (application/vnd.google.safebrowsing-update) |
| 11 | 0.487257 | 74.125.91.113 | 71.192.34.104 | HTTP | 853 | [TCP Spurious Retransmission] HTTP/1.1 200 OK (application/vnd.google. |
| 19 | 0.532089 | 71.192.34.104 | 74.125.106.31 | HTTP | 767 | GET /safebrowsing/rd/goog-malware-shavar_s_15361-15365.15361-15365.: H. |
| 38 | 0.636388 | 74.125.106.31 | 71.192.34.104 | HTTP | 651 | HTTP/1.1 200 OK (application/vnd.google.safebrowsing-chunk) |
| 41 | 0.936824 | 71.192.34.104 | 74.125.106.31 | HTTP | 772 | GET /safebrowsing/rd/goog-malware-shavar_a_14466-14470.14466.14467-144. |
| 42 | 0.959225 | 74.125.106.31 | 71.192.34.104 | HTTP | 881 | HTTP/1.1 200 OK (application/vnd.google.safebrowsing-chunk) |
| 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. |
| 44 | 0.996890 | 74.125.106.31 | 71.192.34.104 | HTTP | 526 | HTTP/1.1 200 OK (application/vnd.google.safebrowsing-chunk) |
| 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. |
| 46 | 1.023414 | 74.125.106.31 | 71.192.34.104 | HTTP | 1089 | HTTP/1.1 200 OK (application/vnd.google.safebrowsing-chunk) |
| 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/CgJlbhICdXMrmAo4NUAILCswDJghLCswFjgQLCswFzgLcswGDgEL. |
| 121 | 6.407366 | 64.233.169.104 | 71.192.34.104 | HTTP | 648 | HTTP/1.1 200 OK (text/javascript) |

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

[3 Reassembled TCP Segments (3620 bytes): #88(1430), #89(1430), #90(760)]

Hypertext Transfer Protocol

Line-based text data: text/html (12 lines)

0020 22 68 00 50 10 ef e9 4f 43 c1 f8 32 39 60 50 18 "h-P...0 C...29"P-

0030 00 6e aa 39 00 00 b6 ca 78 d5 b6 ec 90 f0 06 4f n:9... x...0

0040 e3 f0 a2 aa e3 94 1b 70 70 50 51 ab b5 96 fb 0cp pQ.....

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)

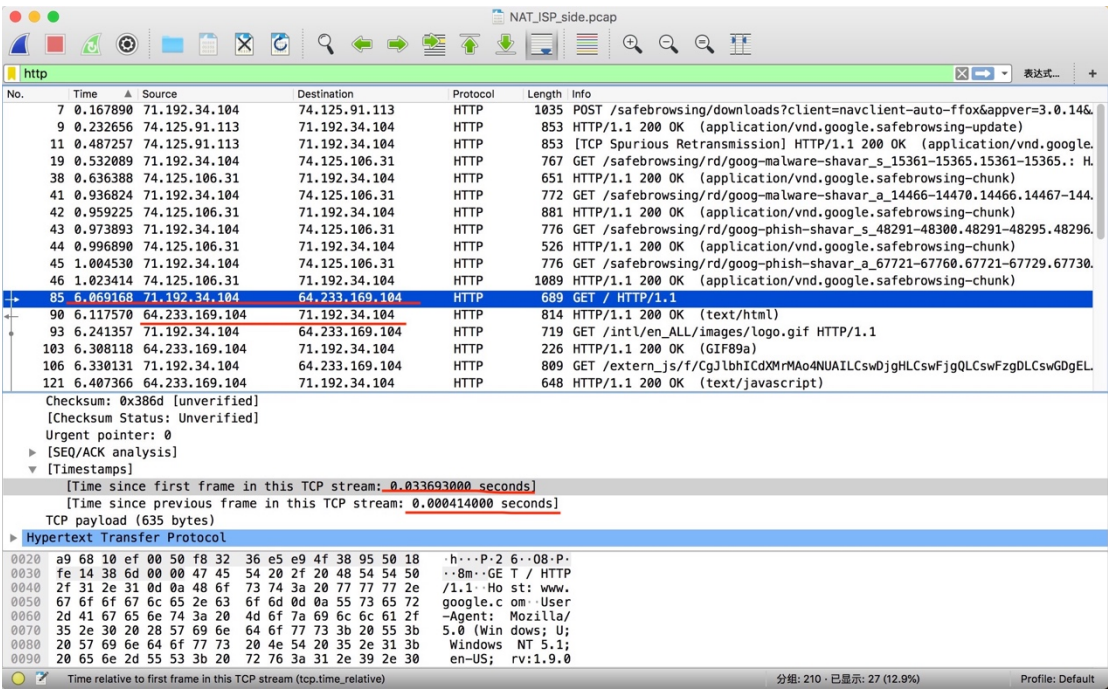
Transmission Control Protocol (tcp), 20 bytes 分组: 210 · 已显示: 27 (12.9%) Profile: Default

9. time: 6.035475 and 6.069582

SYN: source : 71.192.34.104,4335 destination : 54.233.169.104,80

ACK: source : 64.233.169.104,80 destination : 71.192.34.104,4335

SYN source IP address changed. ACK destination IP address changed. The port number are unchanged.



10.NAT translation table

| | WAN side | LAN side |
|-------|---------------|---------------|
| Ip 地址 | 71.192.34.104 | 192.168.1.100 |
| 端口号 | 4335 | 4335 |