

CS425: Assignment 2

Jayant Agrawal

14282

NAT

1. The IP address of client is: 192.168.1.100
2. ---
3.
 - a. Source IP Address: 192.168.1.100
 - b. Destination IP Address: 64.233.169.104
 - c. Source TCP Port: 4335
 - d. Destination TCP Port: 80

http && ip.addr == 64.233.169.104							
No.	Time	Source	Destination	Protocol	Length	Info	
56	7.109267	192.168.1.100	64.233.169.104	HTTP	689	GET / HTTP/1.1	
62	7.281399	192.168.1.100	64.233.169.104	HTTP	719	GET /intl/en_ALL/images/logo	
75	7.370185	192.168.1.100	64.233.169.104	HTTP	809	GET /extern_js/f/CgJlbhICdXM	
94	7.492324	192.168.1.100	64.233.169.104	HTTP	695	GET /extern_chrome/ee36edbd3	
107	7.652836	192.168.1.100	64.233.169.104	HTTP	712	GET /images/nav_logo7.png HT	
112	7.682361	192.168.1.100	64.233.169.104	HTTP	806	GET /csi?v=3&s=webhp&action=	
122	7.709490	192.168.1.100	64.233.169.104	HTTP	670	GET /favicon.ico HTTP/1.1	
▶ 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							
0100 = Version: 4							
.... 0101 = Header Length: 20 bytes (5)							
▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)							
Total Length: 675							
Identification: 0xa2ac (41644)							
▶ Flags: 0x02 (Don't Fragment)							
Fragment offset: 0							
Time to live: 128							
Protocol: TCP (6)							
Header checksum: 0xa94a [validation disabled]							
[Header checksum status: Unverified]							
Source: 192.168.1.100							
Destination: 64.233.169.104							
[Source GeoIP: Unknown]							
▶ [Destination GeoIP: AS15169 Google Inc., Mountain View, CA, United States, 37.419201, -122.057404]							
▶ Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635							
▶ Hypertext Transfer Protocol							

4.
 - a. Time for Corresponding 200 OK HTTP: 7.158797
 - b. Source IP Address: 64.233.169.104
 - c. Destination IP Address: 192.168.1.100
 - d. Source TCP Port: 80

e. Destination TCP Port: 4335

http && ip.addr == 64.233.169.104						
No.	Time	Source	Destination	Protocol	Length	Info
94	7.492324	192.168.1.100	64.233.169.104	HTTP	695	GET /extern_chrome/ee36edbd3c16a1c5.js
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=unde
122	7.789490	192.168.1.100	64.233.169.104	HTTP	670	GET /favicon.ico HTTP/1.1
60	7.158797	64.233.169.104	192.168.1.100	HTTP	814	HTTP/1.1 200 OK (text/html)
73	7.349451	64.233.169.104	192.168.1.100	HTTP	226	HTTP/1.1 200 OK (GIF89a) (GIF89a) (in
92	7.448649	64.233.169.104	192.168.1.100	HTTP	648	HTTP/1.1 200 OK (text/javascript)

▶ 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
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 ▶ Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
 Total Length: 800
 Identification: 0xf61e (63006)
 ▶ Flags: 0x00
 Fragment offset: 0
 Time to live: 50
 Protocol: TCP (6)
 Header checksum: 0xe33b [validation disabled]
 [Header checksum status: Unverified]
 Source: 64.233.169.104
 Destination: 192.168.1.100
 ▶ [Source GeoIP: AS15169 Google, Mountain View, CA, United States, 37.419201, -122.057404]
 [Destination GeoIP: Unknown]
 ▶ 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

5.

a.

- i. TCP SYN TIME: 7.075657
- ii. Source IP Address: 192.168.1.100
- iii. Destination IP Address: 64.233.169.104
- iv. Source TCP Port: 4335
- v. Destination TCP Port: 80

tcp && ip.addr == 64.233.169.104						
No.	Time	Source	Destination	Protocol	Length	Info
5	7.075657	192.168.1.100	64.233.169.104	TCP	66	4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
55	7.109053	192.168.1.100	64.233.169.104	TCP	54	4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
56	7.109267	192.168.1.100	64.233.169.104	HTTP	689	GET / HTTP/1.1
61	7.158844	192.168.1.100	64.233.169.104	TCP	54	4335 → 80 [ACK] Seq=636 Ack=3621 Win=260176 Len=0
62	7.281399	192.168.1.100	64.233.169.104	HTTP	719	GET /intl/en_ALL/images/logo.gif HTTP/1.1
65	7.315641	192.168.1.100	64.233.169.104	TCP	54	4335 → 80 [ACK] Seq=1301 Ack=5306 Win=260176 Len=0
68	7.316283	192.168.1.100	64.233.169.104	TCP	54	4335 → 80 [ACK] Seq=1301 Ack=7972 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
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 52
 Identification: 0xa2aa (41642)
 ▶ Flags: 0x02 (Don't Fragment)
 Fragment offset: 0
 Time to live: 128
 Protocol: TCP (6)
 Header checksum: 0xabbb [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.1.100
 Destination: 64.233.169.104
 [Source GeoIP: Unknown]
 ▶ [Destination GeoIP: AS15169 Google Inc., Mountain View, CA, United States, 37.419201, -122.057404]
 ▶ Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 0, Len: 0

b.

- i. TCP ACK TIME: 7.108986
- ii. Source IP Address: 64.233.169.104
- iii. Destination IP Address: 192.168.1.100

- iv. Source TCP Port:80
- v. Destination TCP Port: 4335

No.	Time	Source	Destination	Protocol	Length	Info
128	7.763537	192.168.1.100	64.233.169.104	TCP	54	4338 → 80 [ACK] Seq=617 Ack=1409 Win=258768 Len=0
130	7.811374	192.168.1.100	64.233.169.104	TCP	54	4335 → 80 [ACK] Seq=3355 Ack=36558 Win=258868 Len=0
131	7.911938	192.168.1.100	64.233.169.104	TCP	54	4337 → 80 [ACK] Seq=753 Ack=216 Win=259960 Len=0
54	7.108986	64.233.169.104	192.168.1.100	TCP	66	80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1460
57	7.140728	64.233.169.104	192.168.1.100	TCP	60	80 → 4335 [ACK] Seq=1 Ack=636 Win=7940 Len=0
58	7.158432	64.233.169.104	192.168.1.100	TCP	1484	[TCP segment of a reassembled PDU]
59	7.158761	64.233.169.104	192.168.1.100	TCP	1484	[TCP segment of a reassembled PDU]

▶ 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
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 ▶ Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
 Total Length: 52
 Identification: 0xf61a (63902)
 ▶ Flags: 0x00
 Fragment offset: 0
 Time to live: 50
 Protocol: TCP (6)
 Header checksum: 0xe62b [validation disabled]
 [Header checksum status: Unverified]
 Source: 64.233.169.104
 Destination: 192.168.1.100
 ▶ [Source GeoIP: AS15169 Google Inc., Mountain View, CA, United States, 37.419201, -122.057404]
 [Destination GeoIP: Unknown]
 ▶ Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 0, Ack: 1, Len: 0

6.

- a. Request Packet: No 51, Time: 7.060269
- b. Response Packet: No 52, Time: 7.073897

No.	Time	Source	Destination	Protocol	Length	Info
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 clients.l.google.com
15	1.529354	192.168.1.100	68.87.71.230	DNS	89	Standard query 0x1773 A safebrowsing-cache.google.com
16	1.549501	68.87.71.230	192.168.1.100	DNS	140	Standard query response 0x1773 A safebrowsing-cache.google.com CNAME safebrowsing.cache.googleusercontent.com
51	7.060269	192.168.1.100	68.87.71.230	DNS	74	Standard query 0xed6a A www.google.com
52	7.073897	68.87.71.230	192.168.1.100	DNS	158	Standard query response 0xed6a A www.google.com CNAME www.l.google.com A 64.233.169.104
95	7.499972	192.168.1.100	68.87.71.230	DNS	79	Standard query 0x0841 A clients1.google.com
96	7.515219	68.87.71.230	192.168.1.100	DNS	199	Standard query response 0x0841 A clients1.google.com CNAME clients.l.google.com A 74.125.195.131
132	12.005621	192.168.1.100	68.87.71.230	DNS	79	Standard query 0xcdc8 A anise.nsn.umass.edu
133	12.022087	68.87.71.230	192.168.1.100	DNS	95	Standard query response 0xcdc8 A anise.nsn.umass.edu A 128.119.47.210

7. The three packets are basically for the three-way handshake required to setup a tcp connection.

- a. 53, TIME: 7.075657, SYN from client to server
- b. 54, TIME: 7.108986, SYN-ACK from server to client
- c. 55, TIME: 7.109053, ACK from client to server

No.	Time	Source	Destination	Protocol	Length	Info
47	2.170596	192.168.1.100	74.125.108.31	TCP	54	4331 → 80 [ACK] Seq=2876 Ack=26452 Win=260176 Len=0
48	2.279208	192.168.1.100	69.183.241.1	UDP	153	15525 → 41400 Len=111
49	2.329239	69.183.241.120	192.168.1.100	ICMP	126	Destination unreachable (Port unreachable)
50	5.999906	192.168.1.100	10.119.240.64	SNMP	120	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1 1.3.6.1.2.1.25.3.5.1.1
51	7.060269	192.168.1.100	68.87.71.230	DNS	74	Standard query 0xed6a A www.google.com
52	7.073897	68.87.71.230	192.168.1.100	DNS	158	Standard query response 0xed6a A www.google.com CNAME www.l.google.com A 64.233.169.104
53	7.075657	192.168.1.100	64.233.169.1	TCP	66	4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
54	7.108986	64.233.169.104	192.168.1.100	TCP	66	80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1460 SACK_PERM=1 WS=64
55	7.109053	192.168.1.100	64.233.169.1	TCP	64	4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
56	7.109267	192.168.1.100	64.233.169.1	HTTP	689	GET / HTTP/1.1
57	7.140728	64.233.169.104	192.168.1.100	TCP	60	80 → 4335 [ACK] Seq=1 Ack=636 Win=7940 Len=0
58	7.158432	64.233.169.104	192.168.1.100	TCP	1484	[TCP segment of a reassembled PDU]
59	7.158761	64.233.169.104	192.168.1.100	TCP	1484	[TCP segment of a reassembled PDU]
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	64.233.169.1	TCP	54	4335 → 80 [ACK] Seq=636 Ack=3621 Win=260176 Len=0

NAT_ISP_SIDE Questions

1.

- a. Time: 6.069168

- b. Source IP Address: 71.192.34.104
- c. Source TCP Port: 4335
- d. Destination IP Address: 64.233.169.104
- e. Destination TCP Port: 80
- f. Source IP Address is different.

http && ip.addr == 64.233.169.104						
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
93	6.241357	71.192.34.104	64.233.169.104	HTTP	719	GET /intl/en_ALL
103	6.308118	64.233.169.104	71.192.34.104	HTTP	226	HTTP/1.1 200 OK
106	6.330131	71.192.34.104	64.233.169.104	HTTP	809	GET /extern_js/f
121	6.407366	64.233.169.104	71.192.34.104	HTTP	648	HTTP/1.1 200 OK
125	6.452270	71.192.34.104	64.233.169.104	HTTP	695	GET /extern_chro
131	6.496234	64.233.169.104	71.192.34.104	HTTP	870	HTTP/1.1 200 OK
139	6.612801	71.192.34.104	64.233.169.104	HTTP	712	GET /images/nav_
144	6.642308	71.192.34.104	64.233.169.104	HTTP	806	GET /csi?v=3&s=w
149	6.644609	64.233.169.104	71.192.34.104	HTTP	1359	HTTP/1.1 200 OK
154	6.669397	71.192.34.104	64.233.169.104	HTTP	670	GET /favicon.ico
157	6.686660	64.233.169.104	71.192.34.104	HTTP	260	HTTP/1.1 204 No

▶ Frame 85: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)
 ▶ Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01)
 ▶ Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104
 ▶ Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
 ▶ Hypertext Transfer Protocol

2. GET Message has not changed. Checksum in the IP datagram has changed because source IP Address has changed.

http && ip.addr == 64.233.169.104							http && ip.addr == 64.233.169.104						
No.	Time	Source	Destination	Protocol	Length	Info	No.	Time	Source	Destination	Protocol	Length	Info
56	7.109267	192.168.1.100	64.233.169.104	HTTP	689	GET / HTTP/1.1	85	6.069168	71.192.34.104	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	90	6.117570	64.233.169.104	71.192.34.104	HTTP	814	HTTP/1.1 200 OK
62	7.281399	192.168.1.100	64.233.169.104	HTTP	719	GET /intl/en_AL	93	6.241357	71.192.34.104	64.233.169.104	HTTP	719	GET /intl/en_AL
73	7.349451	64.233.169.104	192.168.1.100	HTTP	226	HTTP/1.1 200 OK	103	6.308118	64.233.169.104	71.192.34.104	HTTP	226	HTTP/1.1 200 OK
75	7.370185	192.168.1.100	64.233.169.104	HTTP	809	GET /extern_js/	106	6.330131	71.192.34.104	64.233.169.104	HTTP	809	GET /extern_js/
92	7.448649	64.233.169.104	192.168.1.100	HTTP	648	HTTP/1.1 200 OK	121	6.407366	64.233.169.104	71.192.34.104	HTTP	648	HTTP/1.1 200 OK
94	7.492324	192.168.1.100	64.233.169.104	HTTP	695	GET /extern_chr	125	6.452270	71.192.34.104	64.233.169.104	HTTP	695	GET /extern_chr
100	7.537353	64.233.169.104	192.168.1.100	HTTP	870	HTTP/1.1 200 OK	131	6.496234	64.233.169.104	71.192.34.104	HTTP	870	HTTP/1.1 200 OK
107	7.652836	192.168.1.100	64.233.169.104	HTTP	712	GET /images/nav	139	6.612801	71.192.34.104	64.233.169.104	HTTP	712	GET /images/nav
112	7.682361	192.168.1.100	64.233.169.104	HTTP	806	GET /csi?v=3&s=	144	6.642308	71.192.34.104	64.233.169.104	HTTP	806	GET /csi?v=3&s=
119	7.685786	64.233.169.104	192.168.1.100	HTTP	1359	HTTP/1.1 200 OK	149	6.644609	64.233.169.104	71.192.34.104	HTTP	1359	HTTP/1.1 200 OK

▶ Frame 56: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)
 ▶ Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:60:0d:ca:8f), Dst: Cisco-Li_45: (08:0e:d6:bf:6c:01)
 ▶ 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)
 ▶ Flags: 0x02 (Don't Fragment)
 Fragment offset: 0
 Time to live: 128
 Protocol: TCP (6)
 Header checksum: 0xa94a [Validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.1.100
 Destination: 64.233.169.104

NAT_HOME_SIDE

▶ 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 (08:0e:d6:bf:6c:01)
 ▶ Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 675
 Identification: 0xa2ac (41644)
 ▶ Flags: 0x02 (Don't Fragment)
 Fragment offset: 0
 Time to live: 127
 Protocol: TCP (6)
 Header checksum: 0x822f [Validation disabled]
 [Header checksum status: Unverified]
 Source: 71.192.34.104
 Destination: 64.233.169.104

NAT_ISP_SIDE

3.
 - a. Time: 6.117570
 - b. Source IP Address: 64.233.169.104
 - c. Destination IP Address: 71.192.34.104
 - d. Source TCP Port: 80
 - e. Destination TCP Port: 4335

- f. Destination IP Address is different.

http && ip.addr == 64.233.169.104

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) (GIF89
106	6.330131	71.192.34.104	64.233.169.104	HTTP	809	GET /extern_js/f/CgJlbhICdXMrMAo
121	6.407366	64.233.169.104	71.192.34.104	HTTP	648	HTTP/1.1 200 OK (text/javascrip
125	6.452270	71.192.34.104	64.233.169.104	HTTP	695	GET /extern_chrome/ee36edbd3c16a
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=&tra
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	6.686660	64.233.169.104	71.192.34.104	HTTP	260	HTTP/1.1 204 No Content

▶ 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

4.

a.

- TCP SYN TIME: 6.035475
- Source IP Address: 71.192.34.104
- Destination IP Address: 64.233.169.104
- Source TCP Port: 4335
- Destination TCP Port: 80
- Source IP Address has changed due to NAT Translation

tcp && ip.addr == 64.233.169.104

No.	Time	Source	Destination	Protocol	Length	Info
82	6.035475	71.192.34.104	64.233.169.104	TCP	66	4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
83	6.067775	64.233.169.104	71.192.34.104	TCP	66	80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM=1
84	6.068754	71.192.34.104	64.233.169.104	TCP	60	4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
85	6.069168	71.192.34.104	64.233.169.104	HTTP	689	GET / HTTP/1.1
87	6.099637	64.233.169.104	71.192.34.104	TCP	60	80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0
88	6.117078	64.233.169.104	71.192.34.104	TCP	1484	[TCP segment of a reassembled PDU]
89	6.117407	64.233.169.104	71.192.34.104	TCP	1484	[TCP segment of a reassembled PDU]
90	6.117570	64.233.169.104	71.192.34.104	HTTP	814	HTTP/1.1 200 OK (text/html)
91	6.118515	71.192.34.104	64.233.169.104	TCP	60	4335 → 80 [ACK] Seq=636 Ack=3621 Win=260176 Len=0
93	6.241357	71.192.34.104	64.233.169.104	HTTP	719	GET /intl/en_ALL/images/logo.gif HTTP/1.1
94	6.272040	64.233.169.104	71.192.34.104	TCP	200	[TCP segment of a reassembled PDU]

▶ Frame 82: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
 ▶ Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01)
 ▶ Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104
 ▶ Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 0, Len: 0

b.

- TCP ACK TIME: 6.067775
- Source IP Address: 64.233.169.104
- Destination IP Address: 71.192.34.104
- Source TCP Port: 80
- Destination TCP Port: 4335
- Destination IP Address has changed due to NAT Translation

tcp && ip.addr == 64.233.169.104

No.	Time	Source	Destination	Protocol	Length	Info
82	6.035475	71.192.34.104	64.233.169.104	TCP	66	4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
83	6.067775	64.233.169.104	71.192.34.104	TCP	66	80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM=1
84	6.068754	71.192.34.104	64.233.169.104	TCP	60	4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
85	6.069168	71.192.34.104	64.233.169.104	HTTP	689	GET / HTTP/1.1
87	6.099637	64.233.169.104	71.192.34.104	TCP	60	80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0
88	6.117078	64.233.169.104	71.192.34.104	TCP	1484	[TCP segment of a reassembled PDU]
89	6.117407	64.233.169.104	71.192.34.104	TCP	1484	[TCP segment of a reassembled PDU]
90	6.117570	64.233.169.104	71.192.34.104	HTTP	814	HTTP/1.1 200 OK (text/html)
91	6.118515	71.192.34.104	64.233.169.104	TCP	60	4335 → 80 [ACK] Seq=636 Ack=3621 Win=260176 Len=0
93	6.241357	71.192.34.104	64.233.169.104	HTTP	719	GET /intl/en_ALL/images/logo.gif HTTP/1.1
94	6.272040	64.233.169.104	71.192.34.104	TCP	200	[TCP segment of a reassembled PDU]

▶ Frame 83: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
 ▶ Ethernet II, Src: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
 ▶ Internet Protocol Version 4, Src: 64.233.169.104, Dst: 71.192.34.104
 ▶ Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 0, Ack: 1, Len: 0