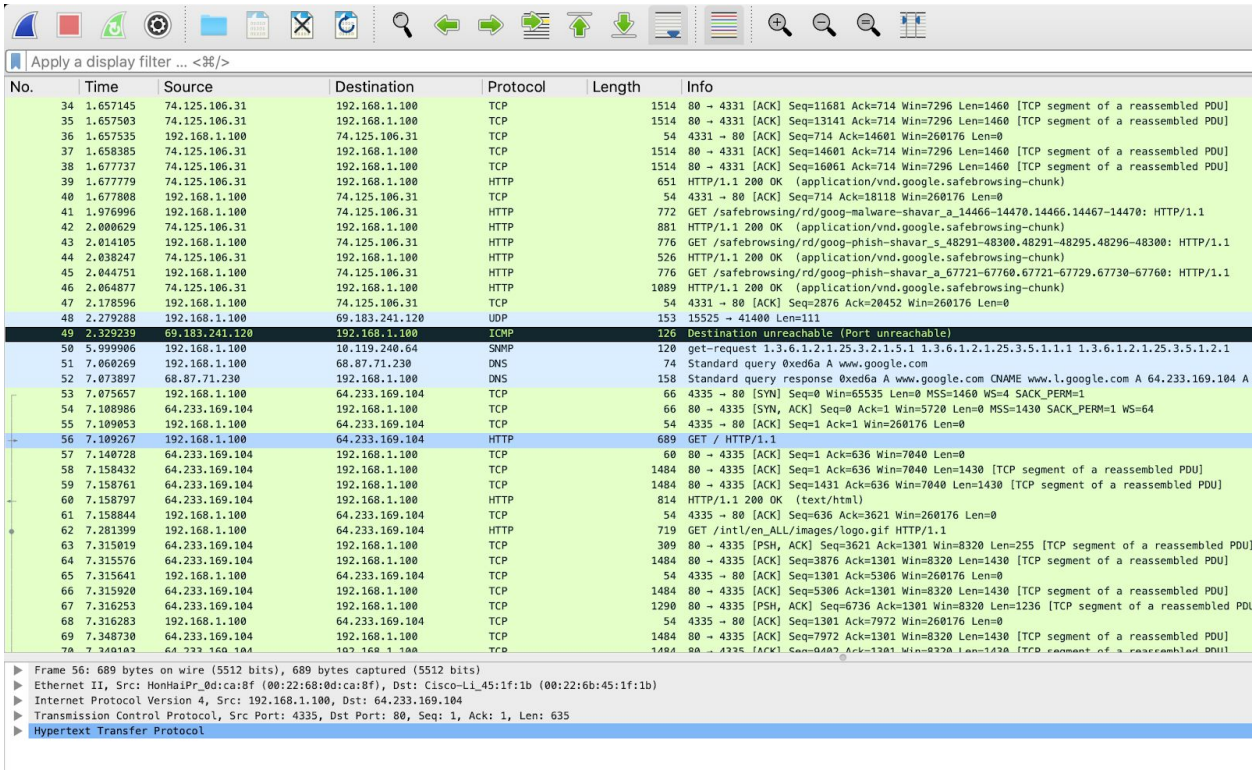
Networks Lab 4

Christina Indudhara, Jiaona Ma, Yi Nian, Jingjing Xiao

1. The client's IP Address is: 192.168.1.100

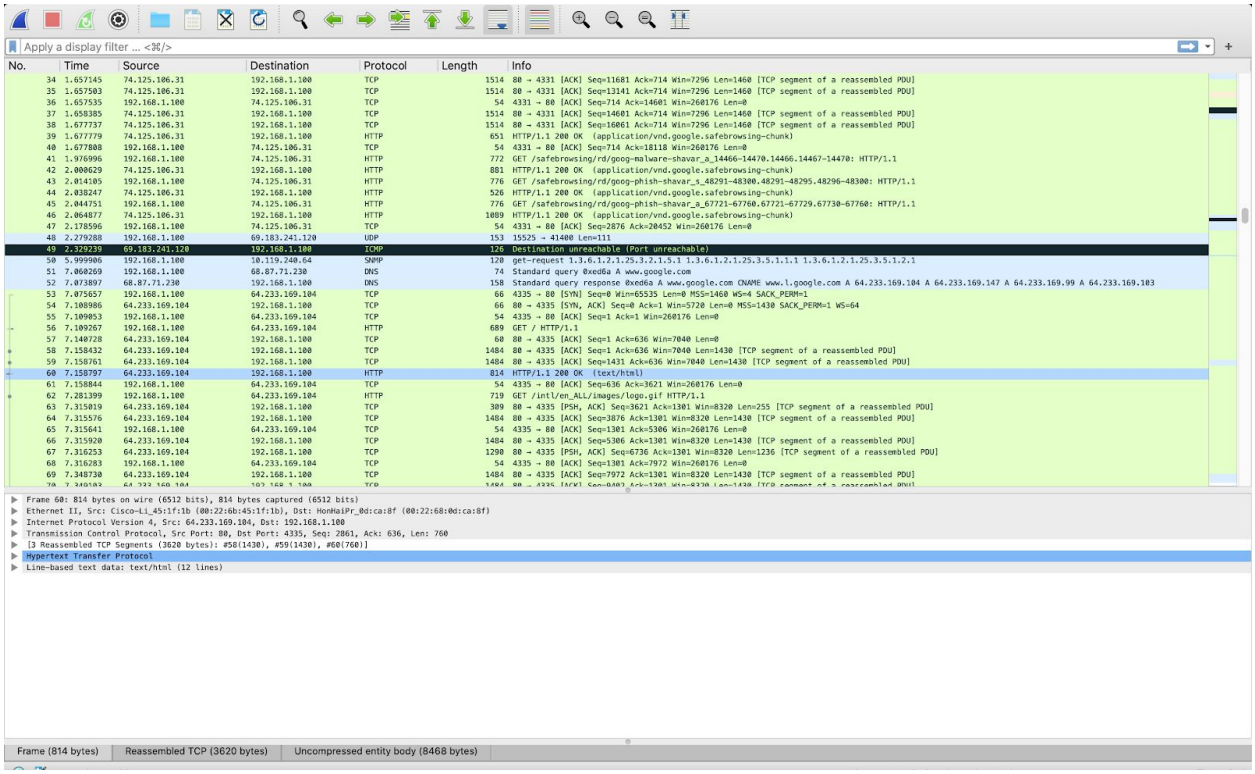


No.	Time	Source	Destination	Protocol	Length	Info
34	1.657145	74.125.106.31	192.168.1.100	TCP	1514	80 → 4331 [ACK] Seq=11681 Ack=714 Win=7296 Len=1460 [TCP segment of a reassembled PDU]
35	1.657503	74.125.106.31	192.168.1.100	TCP	1514	80 → 4331 [ACK] Seq=13141 Ack=714 Win=7296 Len=1460 [TCP segment of a reassembled PDU]
36	1.657535	192.168.1.100	74.125.106.31	TCP	54	4331 → 80 [ACK] Seq=714 Ack=14601 Win=260176 Len=0
37	1.658385	74.125.106.31	192.168.1.100	TCP	1514	80 → 4331 [ACK] Seq=14601 Ack=714 Win=7296 Len=1460 [TCP segment of a reassembled PDU]
38	1.677737	74.125.106.31	192.168.1.100	TCP	1514	80 → 4331 [ACK] Seq=16061 Ack=714 Win=7296 Len=1460 [TCP segment of a reassembled PDU]
39	1.677779	74.125.106.31	192.168.1.100	HTTP	651	HTTP/1.1 200 OK (application/vnd.google.safebrowsing-chunk)
40	1.677808	192.168.1.100	74.125.106.31	TCP	54	4331 → 80 [ACK] Seq=714 Ack=18118 Win=260176 Len=0
41	1.976996	192.168.1.100	74.125.106.31	HTTP	772	GET /safebrowsing/rd/goog-malware-shavar_a_14466-14470.14466.14467-14470: HTTP/1.1
42	2.000629	74.125.106.31	192.168.1.100	HTTP	881	HTTP/1.1 200 OK (application/vnd.google.safebrowsing-chunk)
43	2.014105	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
44	2.038247	74.125.106.31	192.168.1.100	HTTP	526	HTTP/1.1 200 OK (application/vnd.google.safebrowsing-chunk)
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
46	2.064877	74.125.106.31	192.168.1.100	HTTP	1089	HTTP/1.1 200 OK (application/vnd.google.safebrowsing-chunk)
47	2.178596	192.168.1.100	74.125.106.31	TCP	54	4331 → 80 [ACK] Seq=2876 Ack=20452 Win=260176 Len=0
48	2.279288	192.168.1.100	69.183.241.120	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 1.3.6.1.2.1.25.3.5.1.2.1
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 A
53	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
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=1430 SACK_PERM=1 WS=64
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
57	7.140728	64.233.169.104	192.168.1.100	TCP	60	80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0
58	7.158432	64.233.169.104	192.168.1.100	TCP	1484	80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=1430 [TCP segment of a reassembled PDU]
59	7.158761	64.233.169.104	192.168.1.100	TCP	1484	80 → 4335 [ACK] Seq=1431 Ack=636 Win=7040 Len=1430 [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	64.233.169.104	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
63	7.315019	64.233.169.104	192.168.1.100	TCP	309	80 → 4335 [PSH, ACK] Seq=3621 Ack=1301 Win=8320 Len=255 [TCP segment of a reassembled PDU]
64	7.315576	64.233.169.104	192.168.1.100	TCP	1484	80 → 4335 [ACK] Seq=3876 Ack=1301 Win=8320 Len=1430 [TCP segment of a reassembled PDU]
65	7.315641	192.168.1.100	64.233.169.104	TCP	54	4335 → 80 [ACK] Seq=1301 Ack=5306 Win=260176 Len=0
66	7.315920	64.233.169.104	192.168.1.100	TCP	1484	80 → 4335 [ACK] Seq=5306 Ack=1301 Win=8320 Len=1430 [TCP segment of a reassembled PDU]
67	7.316253	64.233.169.104	192.168.1.100	TCP	1290	80 → 4335 [PSH, ACK] Seq=6736 Ack=1301 Win=8320 Len=1236 [TCP segment of a reassembled PDU
68	7.316283	192.168.1.100	64.233.169.104	TCP	54	4335 → 80 [ACK] Seq=1301 Ack=7972 Win=260176 Len=0
69	7.348730	64.233.169.104	192.168.1.100	TCP	1484	80 → 4335 [ACK] Seq=7972 Ack=1301 Win=8320 Len=1430 [TCP segment of a reassembled PDU]

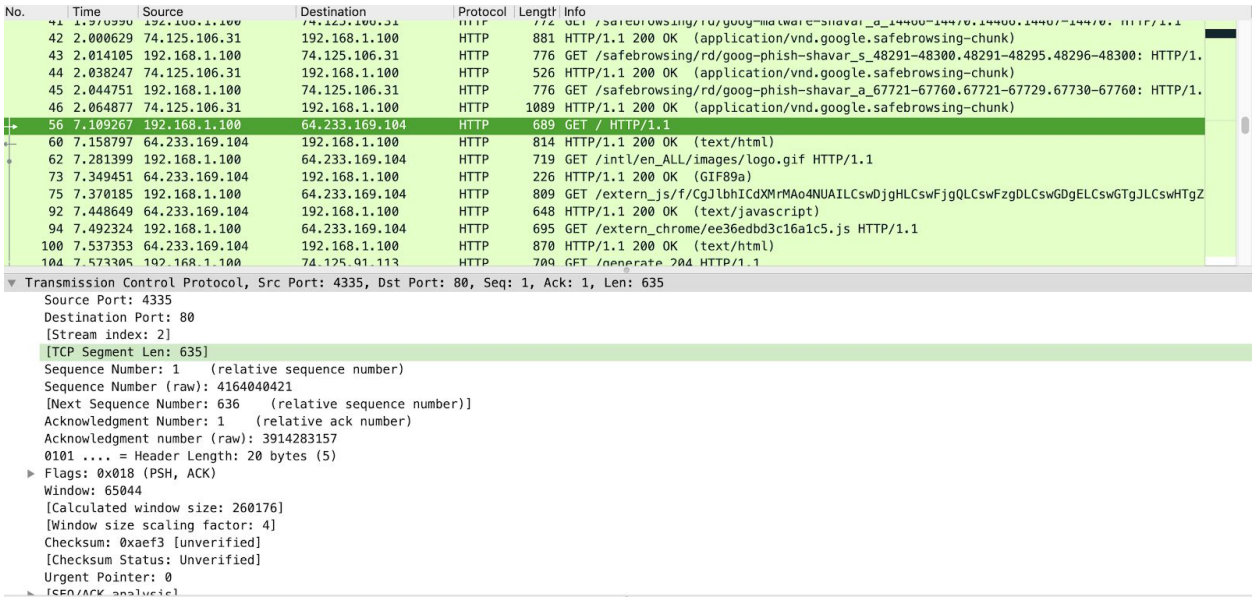
```
Frame 56: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)
Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104
Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
Hypertext Transfer Protocol
```

2.

Source IP: 192.168.1.100
Destination IP: 64.233.169.104
TCP source: 4335
Destination port: 80

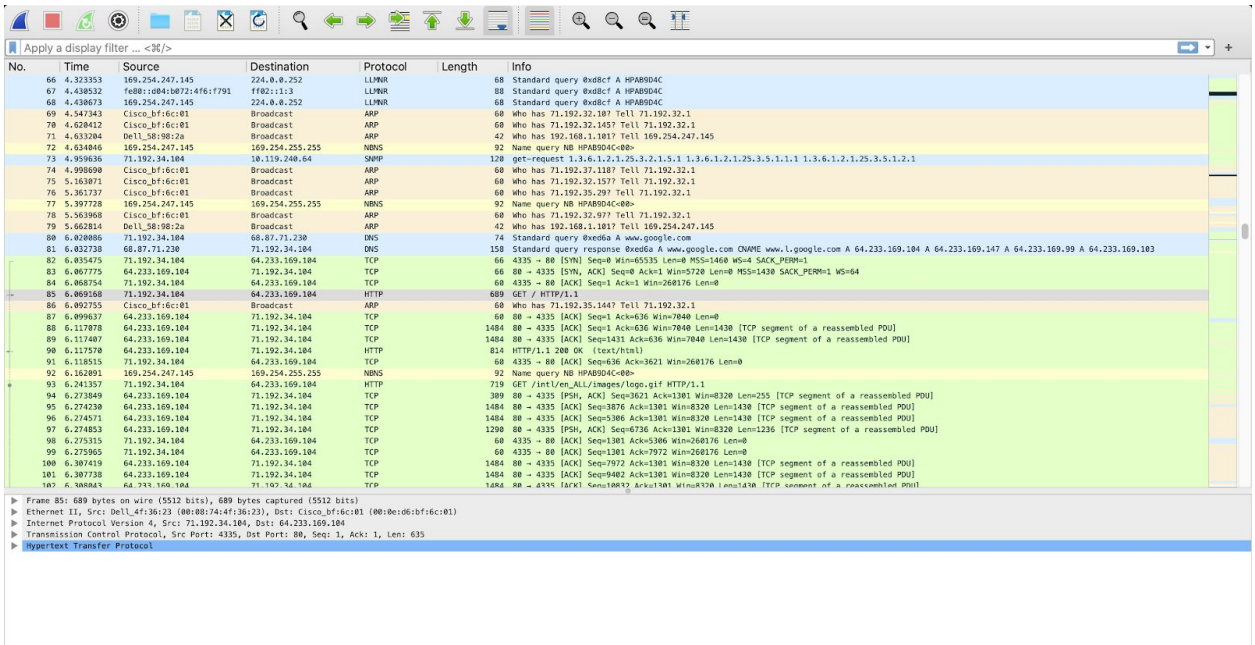
3. 

Time received: 7.158797
Source IP: 192.168.1.100
Destination IP: 64.233.169.104
TCP source: 4335
Destination port:80

4. 

Time client-to-server TCP SYN segment sent (this segment was used by the time 7.109267 GET):

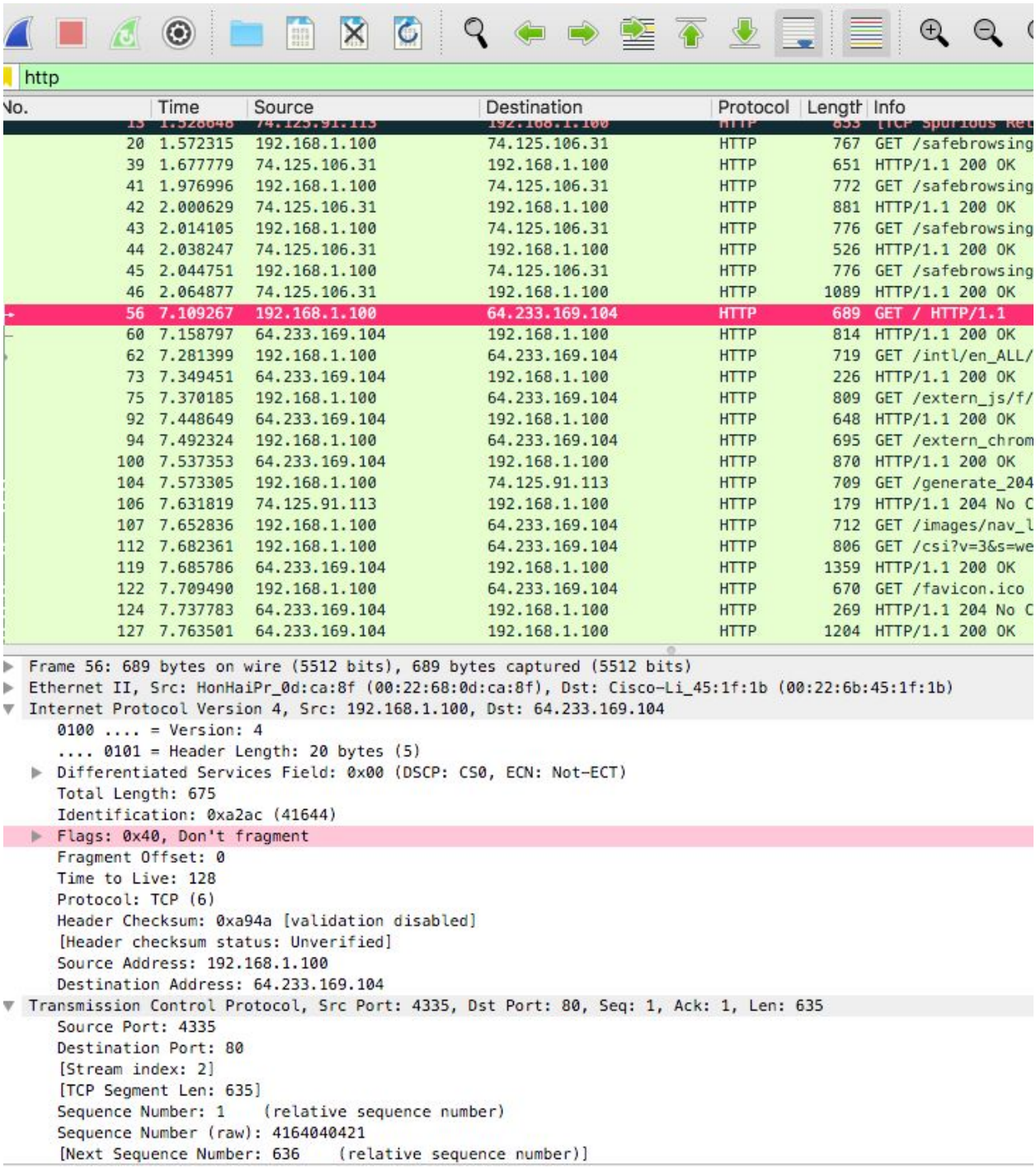
Time the client-to-server the SYN/ACK: 7.0575657
Source for TCP SYN: 192.168.1.100, port 4335
Destination for TCP SYN:64.233.169.104 port 80
ACK Source IP: 64.233.169.104 port 80
ACK Destination IP: 192.168.1.100, port 4335
ACK received time at client: 7.108986



5.

Time HTTP GET appears in NAT_ISP_side trace: 6.069168
Source IP: 71.192.34.104
Destination IP: 64.233.169.104
TCP source port: 4335
Destination port: 80
Which fields are the same than the Q3 answer? Everything is the same except for Source IP Address
Which fields are different than the Q3 answer? Source IP Address, time, destination and source port

6. Home Side:



http

No.	Time	Source	Destination	Protocol	Length	Info
20	1.572315	192.168.1.100	74.125.106.31	HTTP	767	GET /safebrowsing
39	1.677779	74.125.106.31	192.168.1.100	HTTP	651	HTTP/1.1 200 OK
41	1.976996	192.168.1.100	74.125.106.31	HTTP	772	GET /safebrowsing
42	2.000629	74.125.106.31	192.168.1.100	HTTP	881	HTTP/1.1 200 OK
43	2.014105	192.168.1.100	74.125.106.31	HTTP	776	GET /safebrowsing
44	2.038247	74.125.106.31	192.168.1.100	HTTP	526	HTTP/1.1 200 OK
45	2.044751	192.168.1.100	74.125.106.31	HTTP	776	GET /safebrowsing
46	2.064877	74.125.106.31	192.168.1.100	HTTP	1089	HTTP/1.1 200 OK
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
62	7.281399	192.168.1.100	64.233.169.104	HTTP	719	GET /intl/en_ALL/
73	7.349451	64.233.169.104	192.168.1.100	HTTP	226	HTTP/1.1 200 OK
75	7.370185	192.168.1.100	64.233.169.104	HTTP	809	GET /extern_js/f/
92	7.448649	64.233.169.104	192.168.1.100	HTTP	648	HTTP/1.1 200 OK
94	7.492324	192.168.1.100	64.233.169.104	HTTP	695	GET /extern_chrom
100	7.537353	64.233.169.104	192.168.1.100	HTTP	870	HTTP/1.1 200 OK
104	7.573305	192.168.1.100	74.125.91.113	HTTP	709	GET /generate_204
106	7.631819	74.125.91.113	192.168.1.100	HTTP	179	HTTP/1.1 204 No C
107	7.652836	192.168.1.100	64.233.169.104	HTTP	712	GET /images/nav_l
112	7.682361	192.168.1.100	64.233.169.104	HTTP	806	GET /csi?v=3&s=we
119	7.685786	64.233.169.104	192.168.1.100	HTTP	1359	HTTP/1.1 200 OK
122	7.709490	192.168.1.100	64.233.169.104	HTTP	670	GET /favicon.ico
124	7.737783	64.233.169.104	192.168.1.100	HTTP	269	HTTP/1.1 204 No C
127	7.763501	64.233.169.104	192.168.1.100	HTTP	1204	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 (00:22:68:0d: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: 0x40, Don't fragment
    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
    Source Port: 4335
    Destination Port: 80
    [Stream index: 2]
    [TCP Segment Len: 635]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 4164040421
    [Next Sequence Number: 636    (relative sequence number)]
```

ISP side screenshot:

```
▶ 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
    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: 0x40, Don't fragment
    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
```

Fields changed in the HTTP GET message:
- Checksum: Home side is 0xe33b [validation disabled], ISP side is 0x022f [validation disabled]
- Checksum changed because the router changes the IPV4 header on receipt, so a new checksum must be calculated and subsequent devices don't think the packet contains an error; since the source IP address changed, and checksum includes the value of the source IP address.

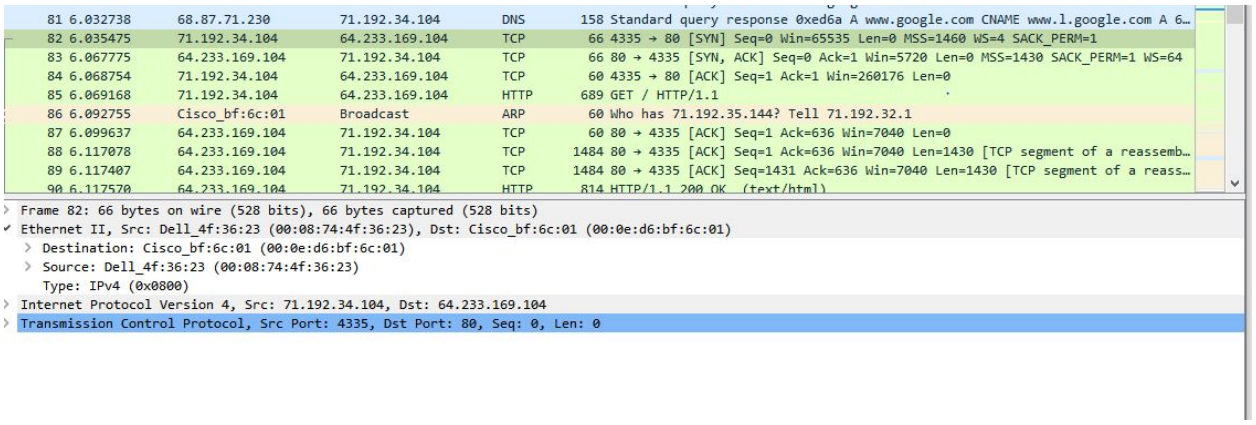
46	1.023414	74.125.106.31	71.192.34.104	HTTP	1089	HTTP/1.1 200 OK (application/vnd.google.safebrowsing-chunk)
85	6.069168	71.192.34.104	64.233.169.104	HTTP	689	GET / HTTP/1.1
90	6.117570	64.233.169.104	71.192.34.104	HTTP	814	HTTP/1.1 200 OK (text/html)
93	6.241357	71.192.34.104	64.233.169.104	HTTP	719	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/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswFzgDLCswGDgELCswG…
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

```
    [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)
  Destination: Dell_4f:36:23 (00:08:74:4f:36:23)
  Source: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01)
  Type: IPv4 (0x0800)
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)
```

7. In NAT_ISP_side trace
   What time is the first 200 OK HTTP message received from the Google server: 6.117570
   Source IP: 64.233.169.104
   Destination IP:71.192.34.104
   TCP source port: 80
   TCP Destination port:4335

Which fields are the same from Q4: Everything except the destination IP
Which fields are different from Q4: The destination IP is different

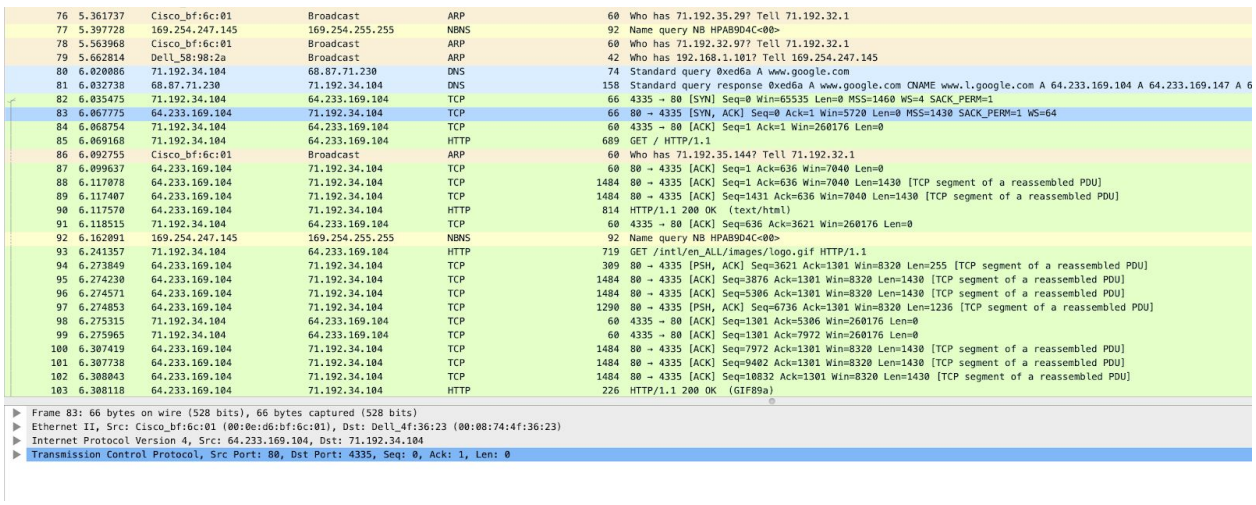
8. TCP SYN Screenshot:



81	6.032738	68.87.71.230	71.192.34.104	DNS	158	Standard query response 0xed6a A www.google.com CNAME www.l.google.com A 6…
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 WS=64
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
86	6.092755	Cisco_bf:6c:01	Broadcast	ARP	60	Who has 71.192.35.144? Tell 71.192.32.1
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	80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=1430 [TCP segment of a reassemb…
89	6.117407	64.233.169.104	71.192.34.104	TCP	1484	80 → 4335 [ACK] Seq=1431 Ack=636 Win=7040 Len=1430 [TCP segment of a reass…
90	6.117570	64.233.169.104	71.192.34.104	HTTP	814	HTTP/1.1 200 OK (text/html)

```
> 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)
  > Destination: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01)
  > Source: Dell_4f:36:23 (00:08:74:4f:36:23)
    Type: IPv4 (0x0800)
> 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
```

SYN ACK Screenshot:



76	5.361737	Cisco_bf:6c:01	Broadcast	ARP	60	Who has 71.192.35.29? Tell 71.192.32.1
77	5.397728	169.254.247.145	169.254.255.255	NBNS	92	Name query NB HPA89D4C<00>
78	5.563968	Cisco_bf:6c:01	Broadcast	ARP	60	Who has 71.192.32.97? Tell 71.192.32.1
79	5.662814	Dell_58:98:2a	Broadcast	ARP	42	Who has 192.168.1.101? Tell 169.254.247.145
80	6.020086	71.192.34.104	68.87.71.230	DNS	74	Standard query 0xed6a A www.google.com
81	6.032738	68.87.71.230	71.192.34.104	DNS	158	Standard query response 0xed6a A www.google.com CNAME www.l.google.com A 64.233.169.104 A 64.233.169.147 A 6
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 WS=64
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
86	6.092755	Cisco_bf:6c:01	Broadcast	ARP	60	Who has 71.192.35.144? Tell 71.192.32.1
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	80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=1430 [TCP segment of a reassembled PDU]
89	6.117407	64.233.169.104	71.192.34.104	TCP	1484	80 → 4335 [ACK] Seq=1431 Ack=636 Win=7040 Len=1430 [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
92	6.162091	169.254.247.145	169.254.255.255	NBNS	92	Name query NB HPA89D4C<00>
93	6.241357	71.192.34.104	64.233.169.104	HTTP	719	GET /intl/en_ALL/images/logo.gif HTTP/1.1
94	6.273849	64.233.169.104	71.192.34.104	TCP	309	80 → 4335 [PSH, ACK] Seq=3621 Ack=1301 Win=8320 Len=255 [TCP segment of a reassembled PDU]
95	6.274230	64.233.169.104	71.192.34.104	TCP	1484	80 → 4335 [ACK] Seq=3876 Ack=1301 Win=8320 Len=1430 [TCP segment of a reassembled PDU]
96	6.274571	64.233.169.104	71.192.34.104	TCP	1484	80 → 4335 [ACK] Seq=5306 Ack=1301 Win=8320 Len=1430 [TCP segment of a reassembled PDU]
97	6.274853	64.233.169.104	71.192.34.104	TCP	1290	80 → 4335 [PSH, ACK] Seq=6736 Ack=1301 Win=8320 Len=1236 [TCP segment of a reassembled PDU]
98	6.275315	71.192.34.104	64.233.169.104	TCP	60	4335 → 80 [ACK] Seq=1301 Ack=5306 Win=260176 Len=0
99	6.275965	71.192.34.104	64.233.169.104	TCP	60	4335 → 80 [ACK] Seq=1301 Ack=7972 Win=260176 Len=0
100	6.307419	64.233.169.104	71.192.34.104	TCP	1484	80 → 4335 [ACK] Seq=7972 Ack=1301 Win=8320 Len=1430 [TCP segment of a reassembled PDU]
101	6.307738	64.233.169.104	71.192.34.104	TCP	1484	80 → 4335 [ACK] Seq=9402 Ack=1301 Win=8320 Len=1430 [TCP segment of a reassembled PDU]
102	6.308043	64.233.169.104	71.192.34.104	TCP	1484	80 → 4335 [ACK] Seq=10832 Ack=1301 Win=8320 Len=1430 [TCP segment of a reassembled PDU]
103	6.308118	64.233.169.104	71.192.34.104	HTTP	226	HTTP/1.1 200 OK (GIF89a)

```
▶ 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
```

In NAT_ISP_side trace:
What time was the client-to-server TCP SYN segment captured:6.035475
What time was the server-to-client ACK segment captured:6.06775
SYN Source IP: 71.192.34.104
SYN Destination IP:64.233.169.104
SYN TCP source port: 4335
SYN TCP Destination port: 80
ACK Source IP:64.233.169.104
ACK Destination IP:71.192.34.104
ACK TCP source port: 80
ACK TCP Destination port: 4335
Which fields are the same from Q5:The source IP address changed for SYN message. The destination IP changed for ACK message.
Which fields are different from Q5: Port number stays the same.

9. Fill in the NAT translation table entries for the HTTP connection considered in Q1-8

NAT translation	
WAN side address	LAN side address
71.192.34.104, port 4335	192.168.1.100, port 4335