CS425: Assignment 2

Jayant Agrawal 14282

NAT

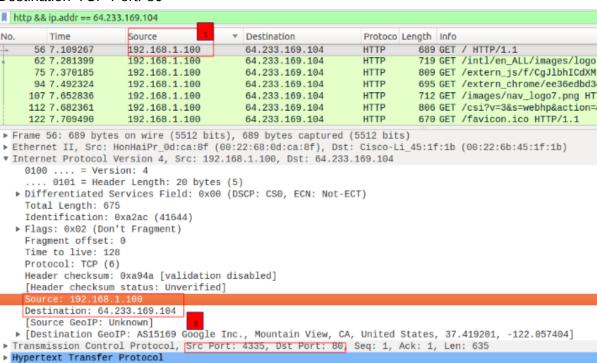
The IP address of client is: 192.168.1.100.

2. ---

3.

a. Source IP Address: 192.168.1.100b. Destination IP Address: 64.233.169.104

c. Source TCP Port: 4335d. Destination TCP Port: 80



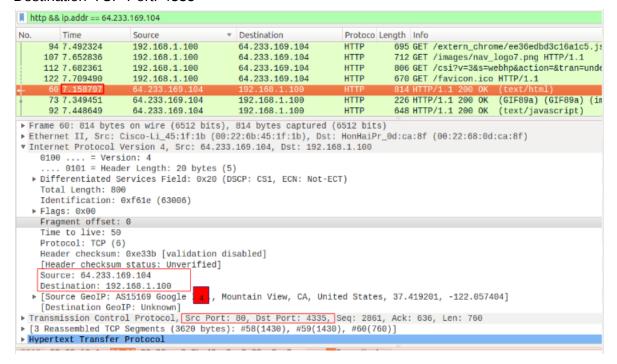
4.

a. Time for Corresponding 200 OK HTTP: 7.158797

b. Source IP Address:64.233.169.104c. Destination IP Address: 192.168.1.100

d. Source TCP Port:80

e. Destination TCP Port: 4335



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: 4335v. Destination TCP Port: 80

Į t	I tcp && ip.addr == 64.233.169.104 ☑ ▼ Expressi										
No.	Time	Source	▼ Destination	Protoco	Length Info						
г	58 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 Ler	=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=26017	'6 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=2601						
	68 7.316283	192.168.1.100	64.233.169.194	TCP	54 4335 → 80 [ACK] Seq=1301 Ack=7972 Win=2601	.76 Len=0					
▶ E	→ Frame 53: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) → Ethernet II, Src: HonHaiPr_6d:ca:8f (90:22:68:0d: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 0109 = 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	6)									
	Header checksum:	0xabbb [validation	disabled]								
	[Header checksum status: Unverified]										
	Source: 192.168.1.100										
	Destination: 64.		_								
	[Source GeoIP: Unknown] sa										
	▶ [Destination GeoIP: AS15169 Google Inc., Mountain View, CA, United States, 37.419201, -122.057404]										
١	Transmission Control Protocol, Src Port: 4335, Ost Port: 80, Seq: 0, Len: 0										

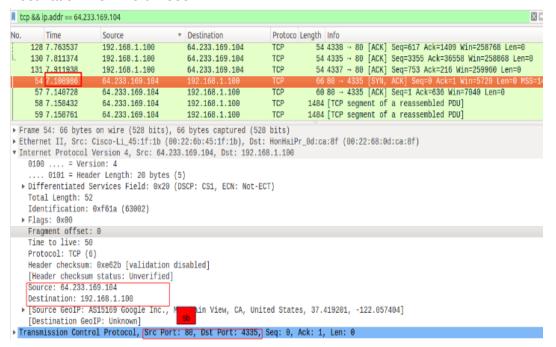
b.

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



6.

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



- 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

```
Destination
                                                                                                   54 4331 - 80 [ACK] Seq=2876 Ack=20452 Win=260176 Len=0
48 2.279288
                         192.168.1.100 69.183.241.1. UDP
                                                                                                 153 15525 - 41400 Len=111
                           69.183.241.120 192.168.1.100 ICM
                                                                                                 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
                          192.168.1.100
                                                     10.119.240.64 SNM
                                                                                                 120 get-request 1.3.0.1.21.25.3.2.1.5.1 1.3.0.1.21.25.3.3.1.1.1 1.3.0.1.21.25.3.3.1.

74 Standard query Oxed6a A www.google.com CNAME www.l.google.com A 64.233.16..

66 4335 + 80 [SYN] Sog=0 win=65935 Len=0 MSS=1460 WS=4 SACK_PERM=1

66 80 + 4335 [SYN, ACK] Sog=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM=1 WS=64

54 4335 + 80 [ACK] Sog=1 Ack=1 Win=260170 Len=0
51.7.868269
                         192,168,1,100 68,87,71,230 DNS
52 7.073897
53 7.075657
                         68,87,71,230
192,168,1,160
                                                    64.233.169.1..
54 7.108986
                         64.233.169.164 192.168.1.166 TCP
                                                                                               58 4335 - 86 [ACK] Seg=1 ACK=1 Win=2001/0 Cen=3
689 GET / HTTP/1.1
66 80 - 4335 [ACK] Seq=1 Ack=636 Win=7646 Len=9
1484 [TCP segment of a reassembled PDU]
814 HTTP/1.1 200 OK (text/html)
                         192.108.1.196 64.233.109.1... HTTP
64.233.169.104 192.168.1.106 TCP
64.233.169.104 192.168.1.106 TCP
64.233.169.104 192.168.1.106 TCP
64.233.169.104 192.168.1.106 HTTP
58 7.158432
59 7, 158761
69 7.158797
                                                                                                  54 4335 - 80 [ACK] Seq=638 Ack=3621 Win=260176 Len=0
61 7.158844
                         192.168.1.166 64.233.169.1.. TCP
```

NAT ISP SIDE Questions

1.

a. Time: 6.069168

b. Source IP Address: 71.192.34.104

c. Source TCP Port: 4335

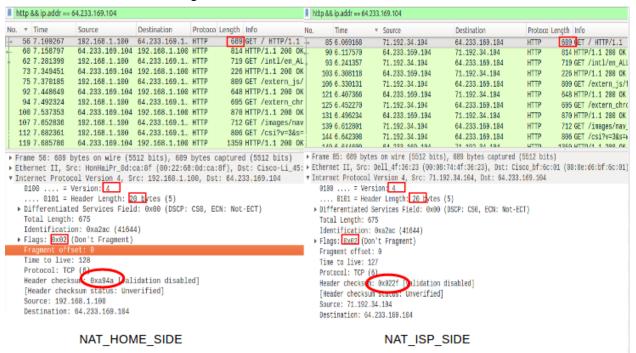
d. Destination IP Address: 64.233.169.104

e. Destination TCP Port: 80

f. Source IP Address is different.

Ā	http && ip.addr == 64.233.169.104									
Ν	0.	Time	₹	Source		Destination		Protoco	Length	Info
+	85	5.069168		71.192.34.104		64.233.169.104		HTTP	689	GET / HTTP/1.1
4	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
ĺ	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
1	467	e enecen		E4 222 4E0 404		74 400 94 404		UTTD	260	UTTD/4 4 204 No.
Þ	Frame 85: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)									
Þ	Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01)									
Þ	Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104									
Þ	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.



3.

a. Time: 6.117570

b. Source IP Address:64.233.169.104c. Destination IP Address: 71.192.34.104

d. Source TCP Port:80

e. Destination TCP Port: 4335

f. Destination IP Address is different.

N I	nttp && ip.addr == 64	.233.	169.104							
No.	Time	w	Source	Destination	Protoco	Length Info				
+	85 6.069168		71.192.34.104	64.233.169.104	HTTP	689 GET / HTTP/1.1				
+	96 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.gi				
+	103 6.308118		64.233.169.104	71.192.34.104	HTTP	226 HTTP/1.1 200 OK (GIF89a) (GIF8				
	106 6.330131		71.192.34.104	64.233.169.104	HTTP	809 GET /extern_js/f/CgJlbhICdXMrMA				
	121 6.407366		64.233.169.104	71.192.34.104	HTTP	648 HTTP/1.1 200 OK (text/javascri				
	125 6.452270		71.192.34.104	64.233.169.104	HTTP	695 GET /extern_chrome/ee36edbd3c16				
	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/				
	144 6.642308		71.192.34.104	64.233.169.104	HTTP	806 GET /csi?v=3&s=webhp&action=&tr				
İ	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				
į	457 £ £0£££0		E4 222 4E0 404	74 402 24 404	HTTD	260 HTTD/4 4 204 No Content				
▶ F	rame 90: 814 by	tes	on wire (6512 bits), 814 bytes captured	(6512 bits	s)				
▶ E	▶ 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, <u>Src: 64.233.169.104</u> , <u>Dst: 71.192.34.104</u>									
	▶ 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)]									
► H	> Hypertext Transfer Protocol									
⊳ I	ine-based text	data	: text/html							

4.

a.

i. TCP SYN TIME: 6.035475

ii. Source IP Address: 71.192.34.104

iii. Destination IP Address: 64.233.169.104

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

vi. Source IP Address has changed due to NAT Translation

tcp	&& ip.addr == 64.23	3.169.104			⊠ ■ Expressi
No.	Time	▼ Source	Destination	Protoco	Length Info
Е	82 6.035475	71.192.34.104	64.233.169.194		56 4335 → 80 [SYN] Seq=8 Win=65535 Len=8 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_PE
	84 6.968754	71.192.34.104	64.233.169.194	TCP	60 4335 - 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
	85 6.069168	71.192.34.184	64.233.169.194	HTTP	689 GET / HTTP/1.1
	87 6.099637	64.233.169.104	71.192.34.194	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	71.192.34.194	TCP	1484 [TCP segment of a reassembled PDU]
	90 6.117570	64.233.169.104	71.192.34.194	HTTP	814 HTTP/1.1 200 OK (text/html)
	91 6.118515	71.192.34.184	64.233.169.184	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
	04.8. 272040	84 222 180 104	71 100 24 104	TCD	200 LTCD commont of a resecombled DBH1
▶ Fra	me 82: 66 bytes	on wire (528 bits),	66 bytes captured (5	28 bits)	
▶ Eth	mernet II, Src:	Dell_4f:36:23 (00:08:	74:4f:36:23), Dst: C	isco bf:5c	:61 (99:8e:d6:bf:6c:91)
		Version 4, Brc: 71.19			
		ol Protocol, Src Port			Len: 0

b.

i. TCP ACK TIME: 6.067775

ii. Source IP Address:64.233.169.104

iii. Destination IP Address: 71.192.34.104

iv. Source TCP Port:80

v. Destination TCP Port: 4335

vi. Destination IP Address has changed due to NAT Translation

No.	Time	▼ Source	Destination	Protoco	ngth Info	
r	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 SA
	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=14
	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 Wi	n=7040 Len=0
	88 6.117078	64.233.169.104	71.192.34.104	TCP	1484 [TCP segment of a reassembled PD	U]
	89 6.117407	64.233.169.104	71.192.34.104	TCP	1484 [TCP segment of a reassembled PD	υj
	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	64.233.169.184	TCP	60 4335 → 80 [ACK] Seq=636 Ack=3621	Win=260176 Len=0
	93 6.241357	71.192.34.104	64.233.169.184	HTTP	719 GET /intl/en_ALL/images/logo.gif	HTTP/1.1
	DA 6 2720AD	EN 222 4ED 4DN	74 402 24 464	TCD	200 ITCD commont of a reasonabled DD	01
► Fran	ne 83: 66 byte	s on wire (528 bits)	, 66 bytes captured (5)	28 bits)		
▶ Ethe	ernet II, Src:	Cisco_bf:6c:81 (80:	0e:d6:bf:6c:01), Dst:	Dell_4f:36	3 (00:08:74:4f:36:23)	
▶ Inte	ernet Protocol	Version 4, Src: 64.	233.169.104, Dst: 71.1	92.34.104		
► Tran	smission Cont	rol Protocol, Src Po	rt: 80, DST PORT: 4335	Seq: 0.	k: 1. Len: θ	