

Assignment – 11

1. The IP address of the client is 192.168.1.100.
- 2.

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/CgJlbhICdXMrMAo4NUAILCswDj...
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...	7.537353	64.233.169.104	192.168.1.100	HTTP	870	HTTP/1.1 200 OK (text/html)
1...	7.652836	192.168.1.100	64.233.169.104	HTTP	712	GET /images/nav_logo7.png HTTP/1.1
1...	7.682361	192.168.1.100	64.233.169.104	HTTP	806	GET /csi?v=3&s=webhp&action=&tran=undefined...
1...	7.685786	64.233.169.104	192.168.1.100	HTTP	1359	HTTP/1.1 200 OK (PNG)
1...	7.709490	192.168.1.100	64.233.169.104	HTTP	670	GET /favicon.ico HTTP/1.1
1...	7.737783	64.233.169.104	192.168.1.100	HTTP	269	HTTP/1.1 204 No Content
1...	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)
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

3. Source address is 192.168.1.100 and the destination address is 64.233.169.104.
4. The corresponding 200 OK HTTP message was received from the Google server at 7.158797. The source (address, port) is (64.233.169.104, 80) and the (destination address, port) is (192.168.1.100, 4335).

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/CgJlbhICdXMrMAo4NUAILCswDj...
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
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
Line-based text data: text/html (12 lines)

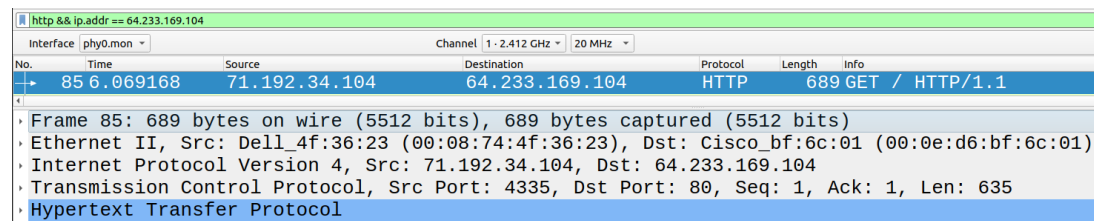
5. The client sent a TCP SYN segment to the server at 7.075657. Source: (192.168.1.100, 4335) and destination: (64.233.169.104, 80). In response to the SYN, the server sent an ACK with source: (64.233.169.104, 80) and destination: (192.168.1.100, 4335). This ACK was received at 7.108986.

No.	Time	Source	Destination	Protocol	Length	Info
53	7.075657	192.168.1.100	64.233.169.104	TCP	66	4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1
54	7.108986	64.233.169.104	192.168.1.100	TCP	66	80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 L
55	7.109053	192.168.1.100	64.233.169.104	TCP	54	4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=

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
Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 0, Len: 0

6. The message appears at 6.069168 in the NAT_ISP_side trace file. Source (address, port): (79.192.34.104, 4335) and destination (address, port):

(64.233.169.104, 80). Only the source IP address has changed and the remaining are the same.

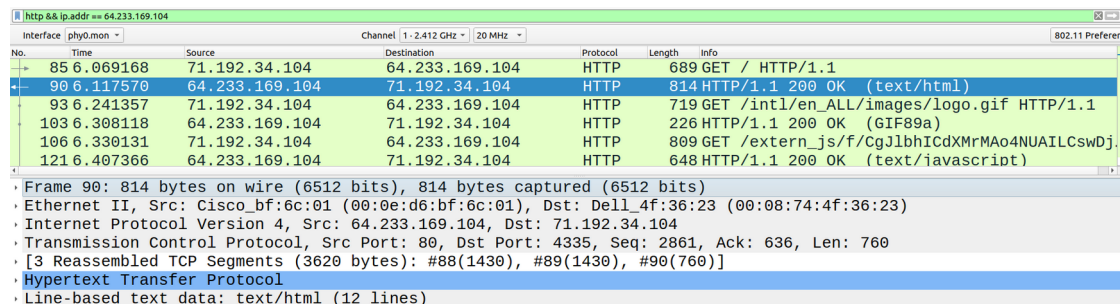


No.	Time	Source	Destination	Protocol	Length	Info
85	6.069168	71.192.34.104	64.233.169.104	HTTP	689	GET / HTTP/1.1

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

7. No, the fields in HTTP GET message have not changed.
 - i. Verison: not changed
 - ii. Header length: not changed
 - iii. Flags: not changed
 - iv. Checksum: changed, since the IP source address has changed, and the checksum includes the value of the source IP address, the checksum has changed
8. The first HTTP 200 OK message was received at 6.117570. Source: (64.233.169.104, 80) and destination: (79.192.34.104, 4335). Only the destination IP address has changed.



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 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/CgJlbhICdXMrMAo4NUAILCswDj HTTP/1.1
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)

9. SYN and ACK at 6.035475, and 6.067775 respectively.
 - i. SYN:
 1. Source: (71.192.34.104, 433)
 2. Destination: (64.233.169.104, 80)
 3. The source IP has changed
 - ii. ACK:
 1. Source: (64.233.169.104, 80)
 2. Destination: (71.192.34.104, 433)
 3. The destination IP has changed

The ports remained unchanged.

tcp && ip.addr == 64.233.169.104						
Interface		Channel		20 MHz		
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
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
84	6.068754	71.192.34.104	64.233.169.104	TCP	60	4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
Frame 83: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 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						

10. NAT translation table

WAN side	LAN side
71.192.34.104, 4335	192.168.1.100, 4335