Assignment-2 CS425A

Saket Jhunjhunwala

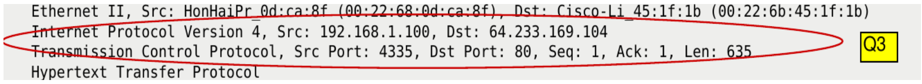
8, September 2017

1 NAT-HOME SIDE

1.1 Problem 1

The IP address of the client is 192.168.1.100.

1.2 Problem 3



```
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
```

The source IP address is 192.168.1.100. The destination IP address is 64.233.169.104. The source port is 4335. The destination port is 80.

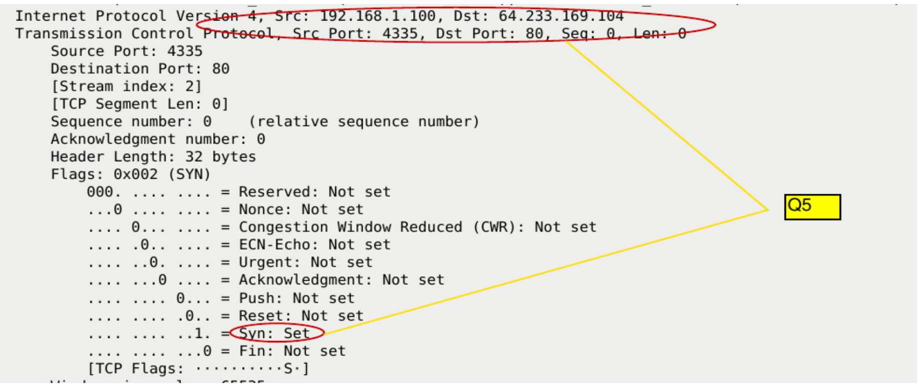
1.3 Problem 4

The response was received at 7.158797. The destination IP address is 192.168.1.100. The source IP address is 64.233.169.104. The destination port is 4335. The source port is 80.

1.4 Problem 5

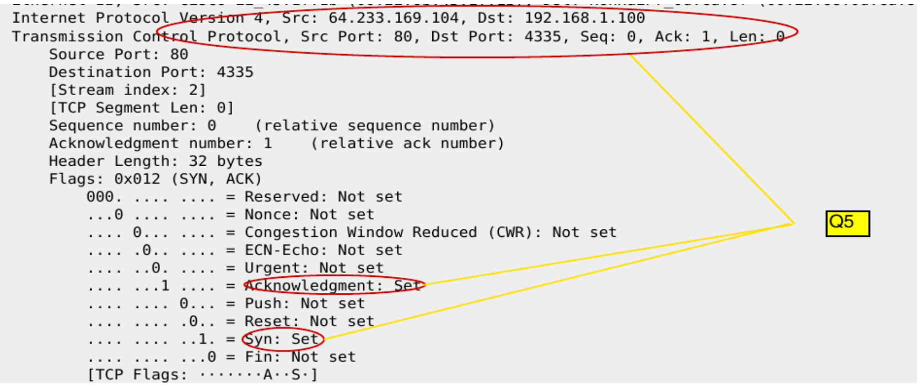
Client-to-server SYN was sent at time 7.075657. The source IP address is 192.168.1.100. The destination IP address is 64.233.169.104. The source port is 4335. The destination port is 80.

Server-to-client SYN ACK was received at 7.108986. The destination IP address is 192.168.1.100. The source IP address is 64.233.169.104. The destination port is 4335. The source port is 80.



```
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
    Source Port: 4335
    Destination Port: 80
    [Stream index: 2]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 0
    Header Length: 32 bytes
    Flags: 0x002 (SYN)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...0 .... = Acknowledgment: Not set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..1. = Syn: Set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ··········S·]
```

Figure 1: SYN

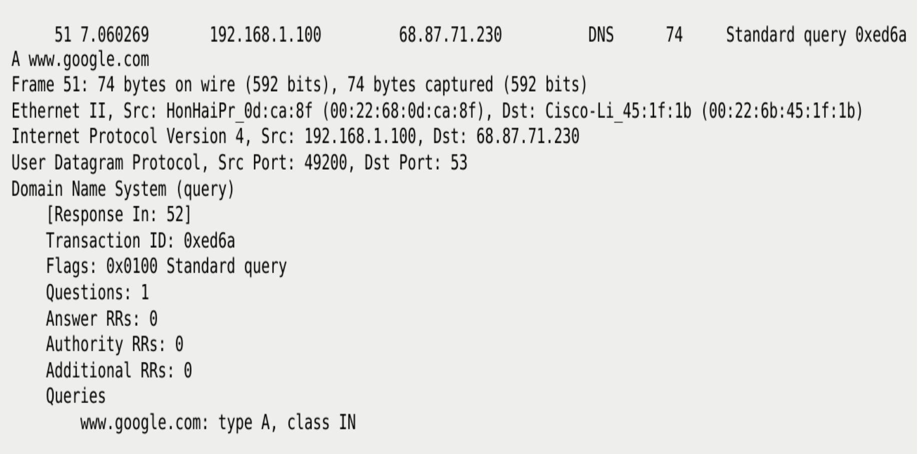


```
Internet Protocol Version 4, Src: 64.233.169.104, Dst: 192.168.1.100
Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 4335
    [Stream index: 2]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 1    (relative ack number)
    Header Length: 32 bytes
    Flags: 0x012 (SYN, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..1. = Syn: Set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·······A··S·]
```

Figure 2: SYN, ACK

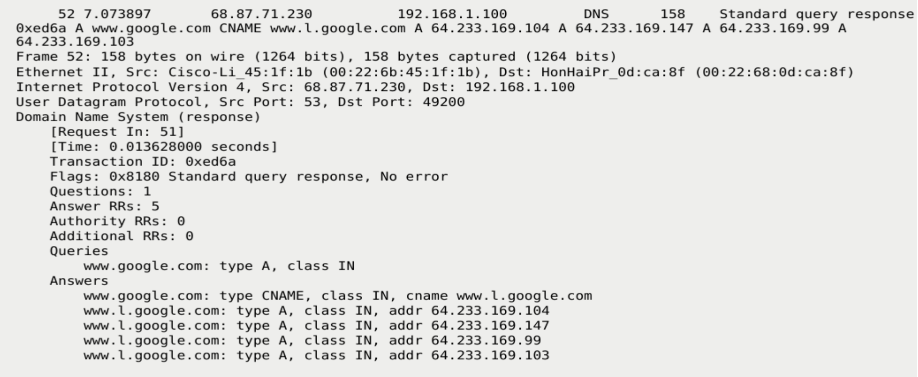
1.5 Problem 6

The following 2 packets were used for finding the IP address of www.google.com:



```
    51 7.060269       192.168.1.100        68.87.71.230         DNS      74     Standard query 0xed6a
A www.google.com
Frame 51: 74 bytes on wire (592 bits), 74 bytes captured (592 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: 68.87.71.230
User Datagram Protocol, Src Port: 49200, Dst Port: 53
Domain Name System (query)
    [Response In: 52]
    Transaction ID: 0xed6a
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        www.google.com: type A, class IN
```

Figure 3: DNS Query

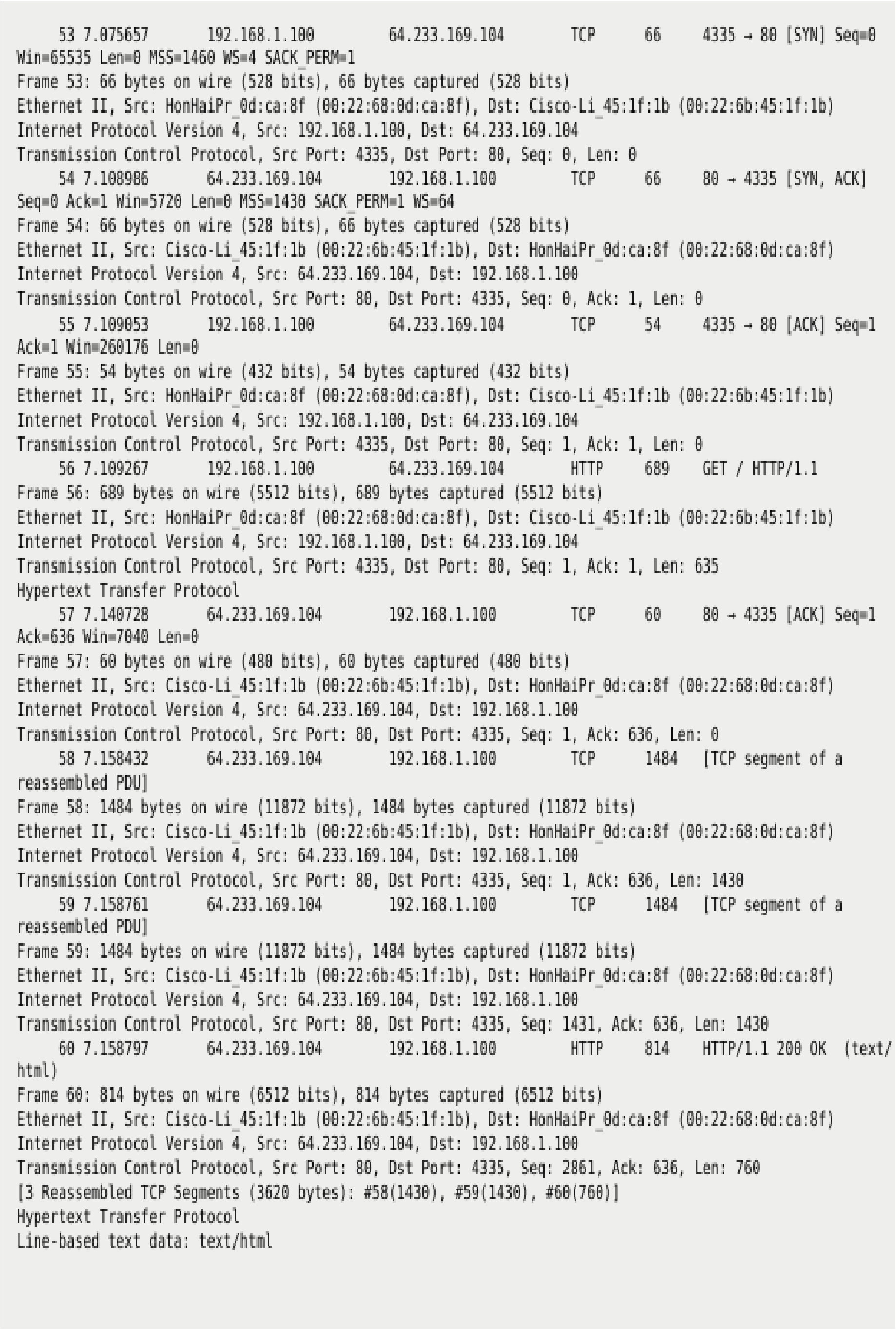


```
     52 7.073897       68.87.71.230          192.168.1.100         DNS      158    Standard query response
0xed6a A www.google.com CNAME www.l.google.com A 64.233.169.104 A 64.233.169.147 A 64.233.169.99 A
64.233.169.103
Frame 52: 158 bytes on wire (1264 bits), 158 bytes captured (1264 bits)
Ethernet 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: 68.87.71.230, Dst: 192.168.1.100
User Datagram Protocol, Src Port: 53, Dst Port: 49200
Domain Name System (response)
    [Request In: 51]
    [Time: 0.013628000 seconds]
    Transaction ID: 0xed6a
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 5
    Authority RRs: 0
    Additional RRs: 0
    Queries
        www.google.com: type A, class IN
    Answers
        www.google.com: type CNAME, class IN, cname www.l.google.com
        www.l.google.com: type A, class IN, addr 64.233.169.104
        www.l.google.com: type A, class IN, addr 64.233.169.147
        www.l.google.com: type A, class IN, addr 64.233.169.99
        www.l.google.com: type A, class IN, addr 64.233.169.103
```

Figure 4: DNS Reply

1.6 Problem 7

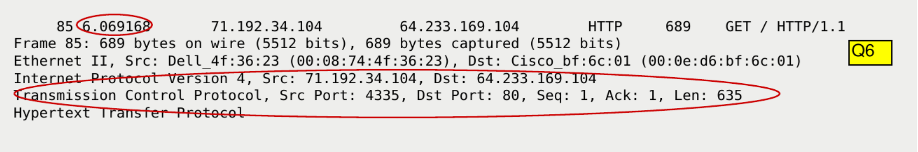
The following packets were sent/received after receiving the IP address. Packets 53,54 and 55 were used for TCP three way handshaking. This is important as TCP is connection oriented protocol. HTTP GET request was sent in packet 56 to www.google.com. Packet 57 is an ack for the HTTP GET sent to the client. HTTP Response was received completely in packet 60.



```
     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
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
     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
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
Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 0, Ack: 1, Len: 0
     55 7.109053       192.168.1.100         64.233.169.104       TCP      54     4335 → 80 [ACK] Seq=1
Ack=1 Win=260176 Len=0
Frame 55: 54 bytes on wire (432 bits), 54 bytes captured (432 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: 0
     56 7.109267       192.168.1.100         64.233.169.104       HTTP     689    GET / 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
Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
Hypertext Transfer Protocol
     57 7.140728       64.233.169.104        192.168.1.100        TCP      60     80 → 4335 [ACK] Seq=1
Ack=636 Win=7040 Len=0
Frame 57: 60 bytes on wire (480 bits), 60 bytes captured (480 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: 1, Ack: 636, Len: 0
     58 7.158432       64.233.169.104        192.168.1.100        TCP      1484   [TCP segment of a
reassembled PDU]
Frame 58: 1484 bytes on wire (11872 bits), 1484 bytes captured (11872 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: 1, Ack: 636, Len: 1430
     59 7.158761       64.233.169.104        192.168.1.100        TCP      1484   [TCP segment of a
reassembled PDU]
Frame 59: 1484 bytes on wire (11872 bits), 1484 bytes captured (11872 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: 1431, Ack: 636, Len: 1430
     60 7.158797       64.233.169.104        192.168.1.100        HTTP     814    HTTP/1.1 200 OK  (text/
html)
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
```

2 NAT-ISP SIDE

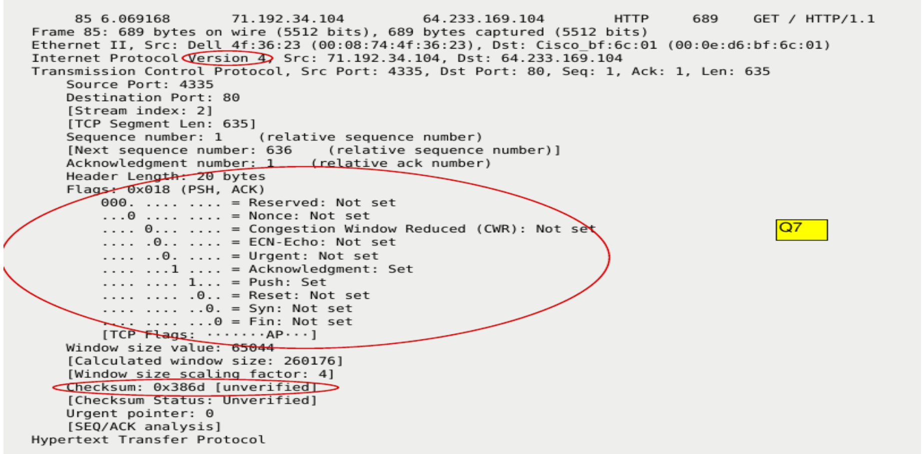
2.1 Problem 6



```
     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
```

It appears at 6.069168 on the ISP side. The destination IP address is 64.233.169.104. The source IP address is 71.192.34.104. The source port is 4335, and the destination port is 80.
The source IP address and time are different than question3.

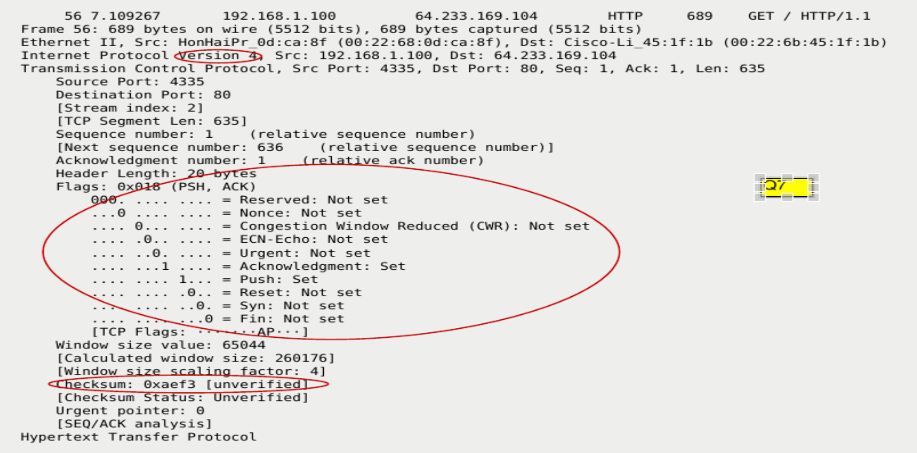
2.2 Problem 7



```
     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
    Source Port: 4335
    Destination Port: 80
    [Stream index: 2]
    [TCP Segment Len: 635]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 636    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Header Length: 20 bytes
    Flags: 0x018 (PSH, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 1... = Push: Set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·······AP···]
    Window size value: 65044
    [Calculated window size: 260176]
    [Window size scaling factor: 4]
    Checksum: 0x386d [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
Hypertext Transfer Protocol
```

Figure 5: ISP Side

The HTTP GET message doesn't change. Headers, Version and flags also doesn't change. Checksum change, as it includes the source IP address, and the source IP address has changed.

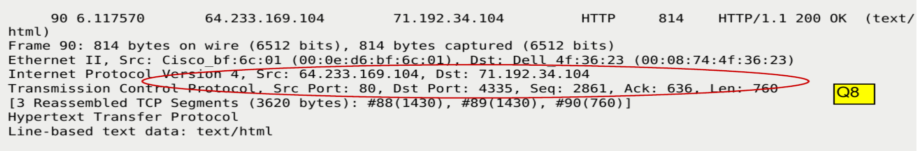


```
     56 7.109267       192.168.1.100         64.233.169.104        HTTP     689    GET / HTTP/1.1
  Frame 56: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)
  Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
  Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104
  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)
      [Next sequence number: 636    (relative sequence number)]
      Acknowledgment number: 1    (relative ack number)
      Header Length: 20 bytes
      Flags: 0x018 (PSH, ACK)
          000. .... .... = Reserved: Not set
          ...0 .... .... = Nonce: Not set
          .... 0... .... = Congestion Window Reduced (CWR): Not set
          .... .0.. .... = ECN-Echo: Not set
          .... ..0. .... = Urgent: Not set
          .... ...1 .... = Acknowledgment: Set
          .... .... 1... = Push: Set
          .... .... .0.. = Reset: Not set
          .... .... ..0. = Syn: Not set
          .... .... ...0 = Fin: Not set
          [TCP Flags: ·······AP···]
      Window size value: 65044
      [Calculated window size: 260176]
      [Window size scaling factor: 4]
      Checksum: 0xaef3 [unverified]
      [Checksum Status: Unverified]
      Urgent pointer: 0
      [SEQ/ACK analysis]
  Hypertext Transfer Protocol
```

Figure 6: Home Side

2.3 Problem 8

The packet received at 6.117570. The destination IP address is 71.192.34.104.



```
     90 6.117570       64.233.169.104        71.192.34.104         HTTP     814    HTTP/1.1 200 OK  (text/
html)
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
```

Figure 7: ISP Side

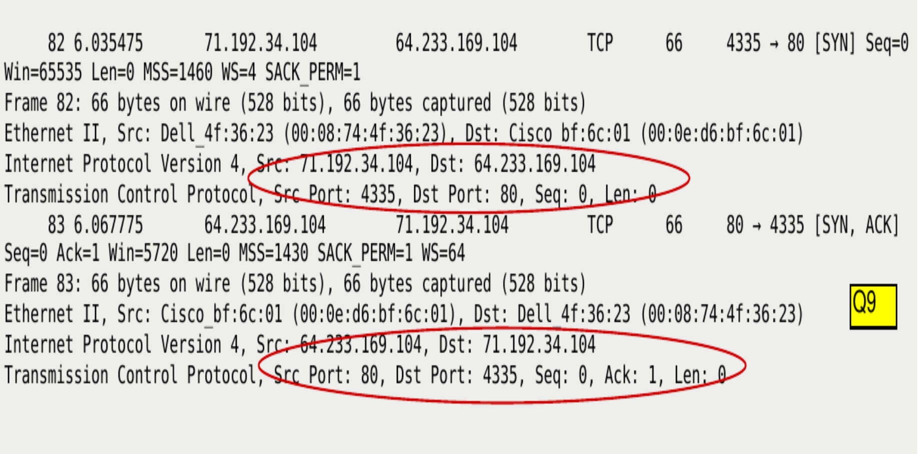
The source IP address is 64.233.169.104. The source port is 80, and destination port is 4335. The destination IP address and time are different than the question4, and rest of the fields are same.

2.4 Problem 9

The client-to-server TCP SYN segment was captured at 6.035475. The server-to-client TCP SYN-ACK segment was captured at 6.067775.

- client-to-server TCP SYN
  - Source IP address:71.192.34.104
  - Source Port: 4335
  - Destination IP address: 64.233.169.104
  - Destination Port: 80

  The source IP address and time changed as compared to question5.



```
    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
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
    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
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
```

Figure 8: ISP Side

- server-to-client TCP SYN-ACK
  - Destination IP address:71.192.34.104
  - Destination Port: 4335
  - Source IP address: 64.233.169.104
  - Source Port: 80

  The destination IP address and time changed as compared to the above question.