

**Izaan Mohtashim**

**P20-0613**

**Sec 5A**

# LAB TASK 9

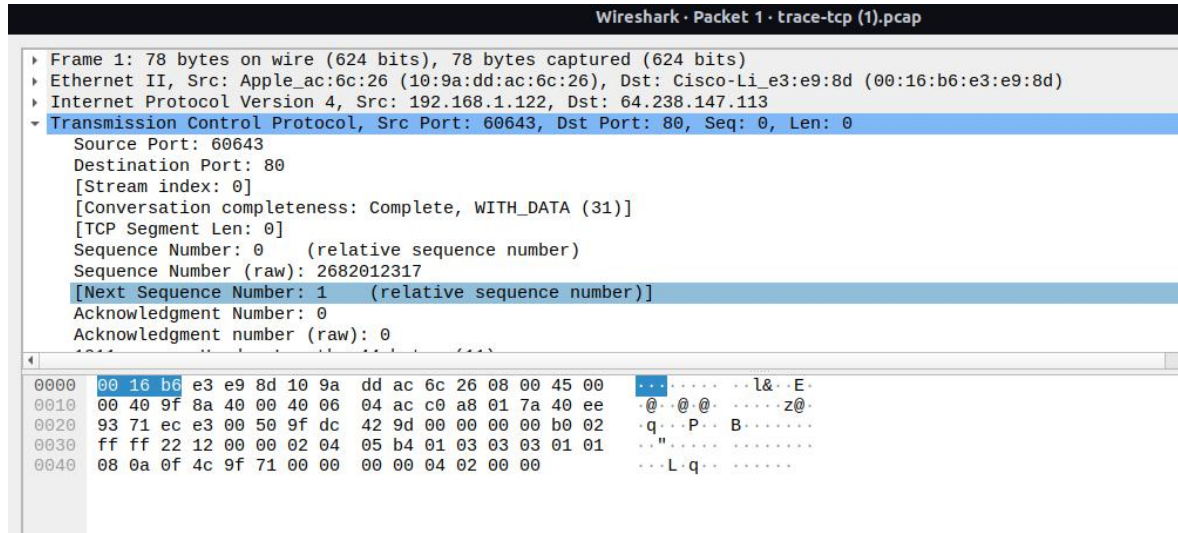


## 1. What is the source and destination port numbers?

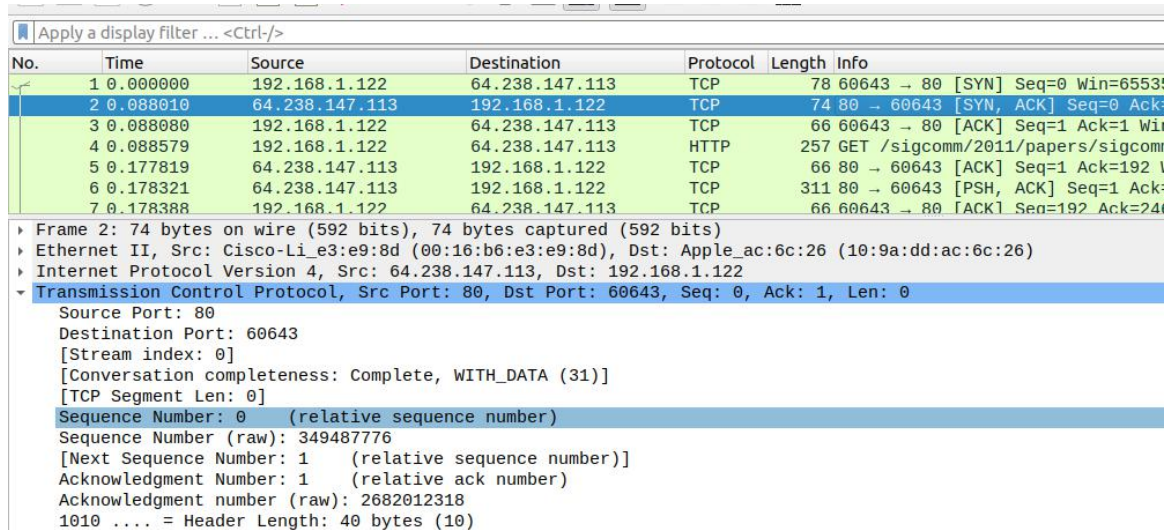
When sending from client to server.

Source-> 60643

Port-> 80



When server send acknowledgment to client that he is available.



When client is confirmed that i have to send data to this server

```

Wireshark · Packet 3 · trace-tcp (1).pcap
└─ Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
  └─ Ethernet II, Src: Apple_ac:6c:26 (10:9a:dd:ac:6c:26), Dst: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d)
    └─ Internet Protocol Version 4, Src: 192.168.1.122, Dst: 64.238.147.113
      └─ Transmission Control Protocol, Src Port: 60643, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
        Source Port: 60643
        Destination Port: 80
        [Stream index: 0]
        [Conversation completeness: Complete, WITH_DATA (31)]
        [TCP Segment Len: 0]
        Sequence Number: 1 (relative sequence number)
        Sequence Number (raw): 2682012318
        [Next Sequence Number: 1 (relative sequence number)]
        Acknowledgment Number: 1 (relative ack number)
        Acknowledgment number (raw): 349487777
        1000 .... = Header Length: 32 bytes (8)
0000  00 16 b6 e3 e9 8d 10 9a dd ac 6c 26 08 00 45 00  ....l&..E.
0010  00 34 e7 a0 40 00 40 06 bc a1 c0 a8 01 7a 40 ee  -4..@.@.....z@.
0020  93 71 ec e3 00 50 9f dc 42 9e 14 d4 c2 a1 80 10  -q..P..B.....
0030  ff ff ac 96 00 00 01 01 08 0a 0f 4c 9f c9 ef 6c  ....L...l
0040  ed fd

```

2. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection? What is it in the segment that identifies the segment as a SYN segment?

```

[... Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2682012317
[Next Sequence Number: 1 (relative sequence number)]

```

The segment that identifies the segment as a SYN segment is the flag ,as the flag is set to 1 that means tcp connection is esblished.

```

└─ Flags: 0x0002 (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

```

3. What is the sequence number of the SYNACK segment sent by the server to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did server determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

sequence number of the SYNACK segment-> 0

Acknowledgement field in the SYNACK segment->1

The value is determined by the initial sequence number +1.

```
Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d), Dst: Apple_ac:6c:26 (10:9a:dd:ac:6c:26)
Internet Protocol Version 4, Src: 64.238.147.113, Dst: 192.168.1.122
Transmission Control Protocol, Src Port: 80, Dst Port: 60643, Seq: 0, Ack: 1, Len: 0
  Source Port: 80
  Destination Port: 60643
  [Stream index: 0]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 349487776
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 2682012318
  1010 .... = Header Length: 40 bytes (10)
```

Acknowledgment flag is set to 1 and SYN flag is also set to 1 so that we identifies the segment as SYNACK segment.

```
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.]
Window: 5792
[Calculated window size: 5792]
Checksum: 0x67d7 [unverified]
```



## 4. What is the length of each of the first six TCP segments?

### 1<sup>st</sup> Tcp segment lenght -> 0

No.	Time	Source	Destination	Protocol	Length	Info
3	0.088080	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [ACK] Seq=1 Ack=1 Win=524280 Len=0 TSval=25
4	0.088579	192.168.1.122	64.238.147.113	HTTP	257	GET /sigcomm/2011/papers/sigcomm/p2.pdf HTTP/1.1
5	0.177819	64.238.147.113	192.168.1.122	TCP	66	80 → 60643 [ACK] Seq=1 Ack=192 Win=6864 Len=0 TSval=48
6	0.178321	64.238.147.113	192.168.1.122	TCP	311	80 → 60643 [PSH, ACK] Seq=1 Ack=192 Win=6864 Len=245 T
7	0.178388	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [ACK] Seq=192 Ack=246 Win=524280 Len=0 TSva

Frame 5: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)  
Ethernet II, Src: Cisco-Li\_e3:e9:8d (00:16:b6:e3:e9:8d), Dst: Apple\_ac:6c:26 (10:9a:dd:ac:6c:26)  
Internet Protocol Version 4, Src: 64.238.147.113, Dst: 192.168.1.122  
Transmission Control Protocol, Src Port: 80, Dst Port: 60643, Seq: 1, Ack: 192, Len: 0  
Source Port: 80  
Destination Port: 60643  
[Stream index: 0]  
[Conversation completeness: Complete, WITH\_DATA (31)]  
[TCP Segment Len: 0]  
Sequence Number: 1 (relative sequence number)

### 2<sup>nd</sup> Tcp segment lenght -> 245

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.122	64.238.147.113	TCP	78	60643 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
2	0.088010	64.238.147.113	192.168.1.122	TCP	74	80 → 60643 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
3	0.088080	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [ACK] Seq=1 Ack=1 Win=524280 Len=0 T
4	0.088579	192.168.1.122	64.238.147.113	HTTP	257	GET /sigcomm/2011/papers/sigcomm/p2.pdf HTTP/1.
5	0.177819	64.238.147.113	192.168.1.122	TCP	66	80 → 60643 [ACK] Seq=1 Ack=192 Win=6864 Len=0 T
6	0.178321	64.238.147.113	192.168.1.122	TCP	311	80 → 60643 [PSH, ACK] Seq=1 Ack=192 Win=6864 Le
7	0.178388	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [ACK] Seq=192 Ack=246 Win=524280 Len

Frame 6: 311 bytes on wire (2488 bits), 311 bytes captured (2488 bits)  
Ethernet II, Src: Cisco-Li\_e3:e9:8d (00:16:b6:e3:e9:8d), Dst: Apple\_ac:6c:26 (10:9a:dd:ac:6c:26)  
Internet Protocol Version 4, Src: 64.238.147.113, Dst: 192.168.1.122  
Transmission Control Protocol, Src Port: 80, Dst Port: 60643, Seq: 1, Ack: 192, Len: 245  
Source Port: 80  
Destination Port: 60643  
[Stream index: 0]  
[Conversation completeness: Complete, WITH\_DATA (31)]  
[TCP Segment Len: 245]

### 3<sup>rd</sup> Tcp segment lenght -> 0

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.122	64.238.147.113	TCP	78	60643 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
2	0.088010	64.238.147.113	192.168.1.122	TCP	74	80 → 60643 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
3	0.088080	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [ACK] Seq=1 Ack=1 Win=524280 Len=0 T
4	0.088579	192.168.1.122	64.238.147.113	HTTP	257	GET /sigcomm/2011/papers/sigcomm/p2.pdf HTTP/1.
5	0.177819	64.238.147.113	192.168.1.122	TCP	66	80 → 60643 [ACK] Seq=1 Ack=192 Win=6864 Len=0 T
6	0.178321	64.238.147.113	192.168.1.122	TCP	311	80 → 60643 [PSH, ACK] Seq=1 Ack=192 Win=6864 Le
7	0.178388	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [ACK] Seq=192 Ack=246 Win=524280 Len

Frame 7: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)  
Ethernet II, Src: Apple\_ac:6c:26 (10:9a:dd:ac:6c:26), Dst: Cisco-Li\_e3:e9:8d (00:16:b6:e3:e9:8d)  
Internet Protocol Version 4, Src: 192.168.1.122, Dst: 64.238.147.113  
Transmission Control Protocol, Src Port: 60643, Dst Port: 80, Seq: 192, Ack: 246, Len: 0  
Source Port: 60643  
Destination Port: 80  
[Stream index: 0]  
[Conversation completeness: Complete, WITH\_DATA (31)]  
[TCP Segment Len: 0]

### 4<sup>th</sup> Tcp segment lenght -> 1368

No.	Time	Source	Destination	Protocol	Length	Info
4	0.088579	192.168.1.122	64.238.147.113	HTTP	257	GET /sigcomm/2011/papers/sigcomm/p2.pdf HTTP/1.
5	0.177819	64.238.147.113	192.168.1.122	TCP	66	80 → 60643 [ACK] Seq=1 Ack=192 Win=6864 Len=0 T
6	0.178321	64.238.147.113	192.168.1.122	TCP	311	80 → 60643 [PSH, ACK] Seq=1 Ack=192 Win=6864 Len
7	0.178388	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [ACK] Seq=192 Ack=246 Win=524280 Len
8	0.189114	64.238.147.113	192.168.1.122	TCP	1434	80 → 60643 [ACK] Seq=246 Ack=192 Win=6864 Len=1
9	0.266705	64.238.147.113	192.168.1.122	TCP	1434	80 → 60643 [ACK] Seq=1614 Ack=192 Win=6864 Len=
10	0.266787	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [ACK] Seq=192 Ack=2982 Win=523944 Le

Frame 8: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits)  
Ethernet II, Src: Cisco-Li\_e3:e9:8d (00:16:b6:e3:e9:8d), Dst: Apple\_ac:6c:26 (10:9a:dd:ac:6c:26)  
Internet Protocol Version 4, Src: 64.238.147.113, Dst: 192.168.1.122  
Transmission Control Protocol, Src Port: 80, Dst Port: 60643, Seq: 246, Ack: 192, Len: 1368  
Source Port: 80  
Destination Port: 60643  
[Stream index: 0]  
[Conversation completeness: Complete, WITH\_DATA (31)]  
[TCP Segment Len: 1368]

## 5<sup>th</sup> Tcp segment lenght -> 1368

No.	Time	Source	Destination	Protocol	Length	Info
4	0.088579	192.168.1.122	64.238.147.113	HTTP	257	GET /sigcomm/2011/papers/sigcomm/p2.pdf HTTP/1.1
5	0.177819	64.238.147.113	192.168.1.122	TCP	66	80 → 60643 [ACK] Seq=1 Ack=192 Win=6864 Len=0
6	0.178321	64.238.147.113	192.168.1.122	TCP	311	80 → 60643 [PSH, ACK] Seq=1 Ack=192 Win=6864 Len=0
7	0.178388	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [ACK] Seq=192 Ack=246 Win=524280 Len=0
8	0.189114	64.238.147.113	192.168.1.122	TCP	1434	80 → 60643 [ACK] Seq=246 Ack=192 Win=6864 Len=1
9	0.266705	64.238.147.113	192.168.1.122	TCP	1434	80 → 60643 [ACK] Seq=1614 Ack=192 Win=6864 Len=1
10	0.266787	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [ACK] Seq=192 Ack=2982 Win=523944 Len=0

▶ Frame 9: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits)  
 ▶ Ethernet II, Src: Cisco-Li\_e3:e9:8d (00:16:b6:e3:e9:8d), Dst: Apple\_ac:6c:26 (10:9a:dd:ac:6c:26)  
 ▶ Internet Protocol Version 4, Src: 64.238.147.113, Dst: 192.168.1.122  
 ▶ Transmission Control Protocol, Src Port: 80, Dst Port: 60643, Seq: 1614, Ack: 192, Len: 1368  
 Source Port: 80  
 Destination Port: 60643  
 [Stream index: 0]  
 [Conversation completeness: Complete, WITH\_DATA (31)]  
 [TCP Segment Len: 1368]

## 6<sup>th</sup> Tcp segment lenght -> 0

No.	Time	Source	Destination	Protocol	Length	Info
4	0.088579	192.168.1.122	64.238.147.113	HTTP	257	GET /sigcomm/2011/papers/sigcomm/p2.pdf HTTP/1.1
5	0.177819	64.238.147.113	192.168.1.122	TCP	66	80 → 60643 [ACK] Seq=1 Ack=192 Win=6864 Len=0
6	0.178321	64.238.147.113	192.168.1.122	TCP	311	80 → 60643 [PSH, ACK] Seq=1 Ack=192 Win=6864 Len=0
7	0.178388	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [ACK] Seq=192 Ack=246 Win=524280 Len=0
8	0.189114	64.238.147.113	192.168.1.122	TCP	1434	80 → 60643 [ACK] Seq=246 Ack=192 Win=6864 Len=1
9	0.266705	64.238.147.113	192.168.1.122	TCP	1434	80 → 60643 [ACK] Seq=1614 Ack=192 Win=6864 Len=1
10	0.266787	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [ACK] Seq=192 Ack=2982 Win=523944 Len=0

▶ Frame 10: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)  
 ▶ Ethernet II, Src: Apple\_ac:6c:26 (10:9a:dd:ac:6c:26), Dst: Cisco-Li\_e3:e9:8d (00:16:b6:e3:e9:8d)  
 ▶ Internet Protocol Version 4, Src: 192.168.1.122, Dst: 64.238.147.113  
 ▶ Transmission Control Protocol, Src Port: 60643, Dst Port: 80, Seq: 192, Ack: 2982, Len: 0  
 Source Port: 60643  
 Destination Port: 80  
 [Stream index: 0]  
 [Conversation completeness: Complete, WITH\_DATA (31)]  
 [TCP Segment Len: 0]

5. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?

From client side it is retransmitting but from the server it is not. when we use source ip it will be retransmitted but when we use destination ip there will be no retransmitted segment in trace.



No.	Time	Source	Destination	Protocol	Length	Info
10	0.266787	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [ACK] Seq=192 Ack=2982 Win=523944 Len=0 TSval=256680057 TSecr=401
13	0.354647	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [ACK] Seq=192 Ack=5718 Win=523944 Len=0 TSval=256680144 TSecr=401
16	0.355579	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [ACK] Seq=192 Ack=8454 Win=523944 Len=0 TSval=256680144 TSecr=401
19	0.442003	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [ACK] Seq=192 Ack=11190 Win=523944 Len=0 TSval=256680230 TSecr=401
21	0.442716	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [ACK] Seq=192 Ack=12558 Win=523944 Len=0 TSval=256680230 TSecr=401
24	0.446405	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [ACK] Seq=192 Ack=15294 Win=523944 Len=0 TSval=256680233 TSecr=401
27	0.536678	192.168.1.122	64.238.147.113	TCP	66	60643 → 80 [ACK] Seq=192 Ack=18030 Win=523944 Len=0 TSval=256680322 TSecr=401

```

> Frame 19: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: Apple_ac:6c:26 (10:9a:dd:ac:6c:26), Dst: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d)
> Internet Protocol Version 4, Src: 192.168.1.122, Dst: 64.238.147.113
< Transmission Control Protocol, Src Port: 60643, Dst Port: 80, Seq: 192, Ack: 11190, Len: 0
    Source Port: 60643
    Destination Port: 80
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 192 (relative sequence number)
    Sequence Number (raw): 2682012509
    [Next Sequence Number: 192 (relative sequence number)]
    Acknowledgment Number: 11190 (relative ack number)
    Acknowledgment number (raw): 349498966
    1000 .... = Header Length: 32 bytes (8)
    > Flags: 0x010 (ACK)
    Window: 65493
    [Calculated window size: 523944]
    [Window size scaling factor: 8]
    Checksum: 0x7d8f [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    < [Timestamps]
        [Time since first frame in this TCP stream: 0.442003000 seconds]
        [Time since previous frame in this TCP stream: 0.000030000 seconds]
  
```