Name : Waqar Ahmed

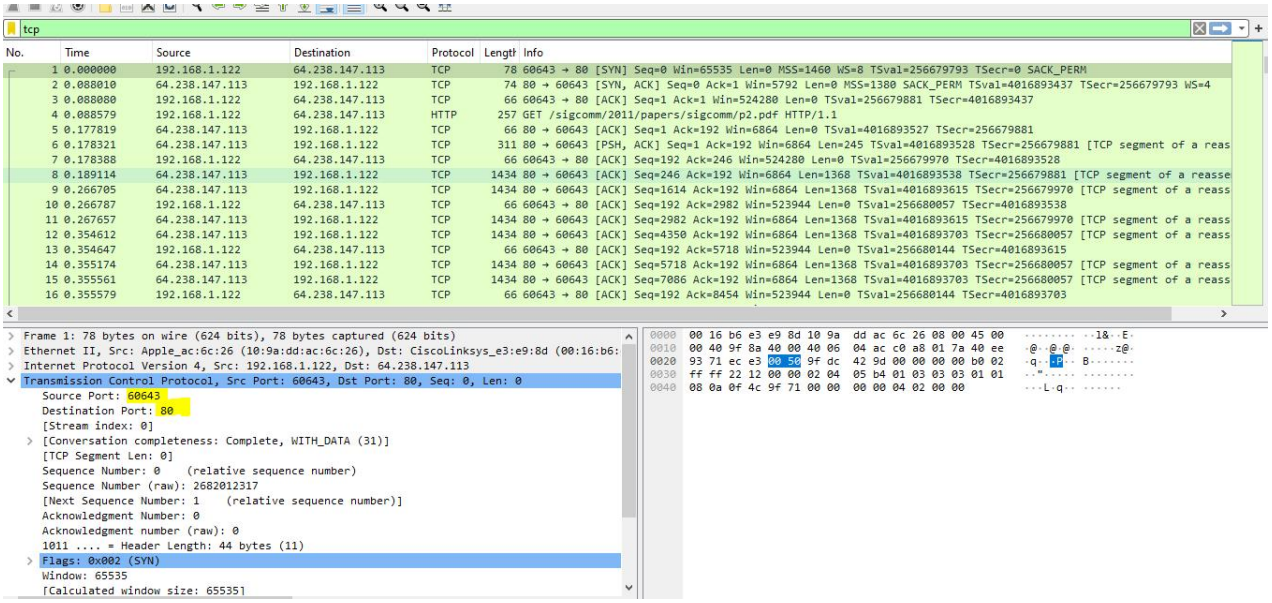
Roll No : P200750

LabTask : 10

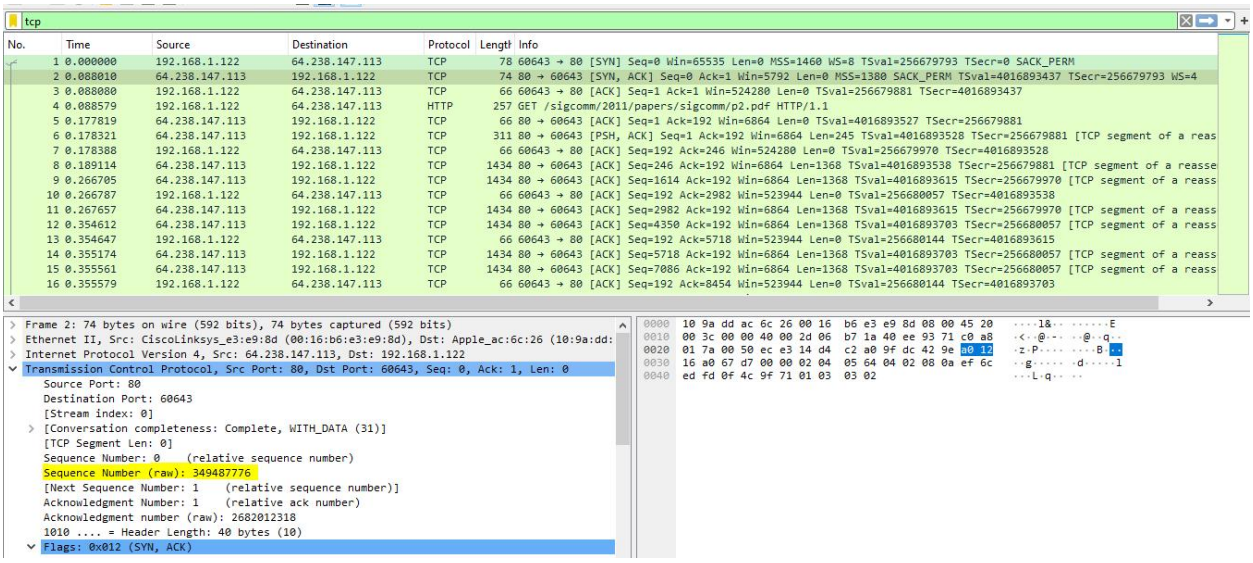
Instructor : Maa’m Hurmat

Task : Inspect the three-way handshake and answer the following questions:

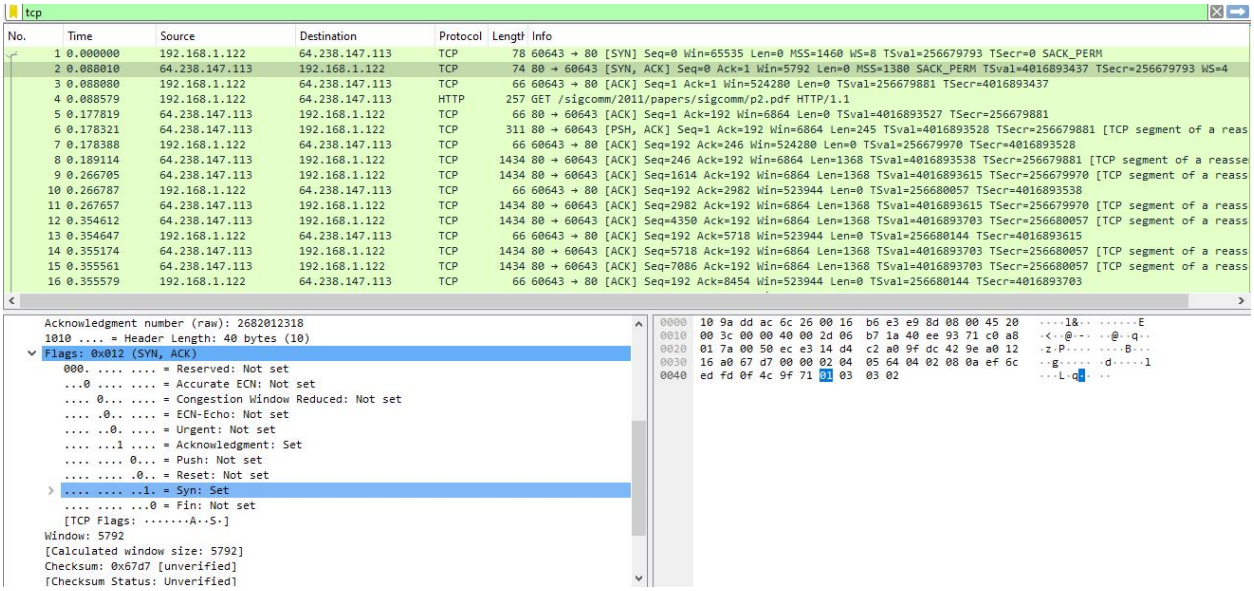
1. What is the source and destination port numbers?



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?

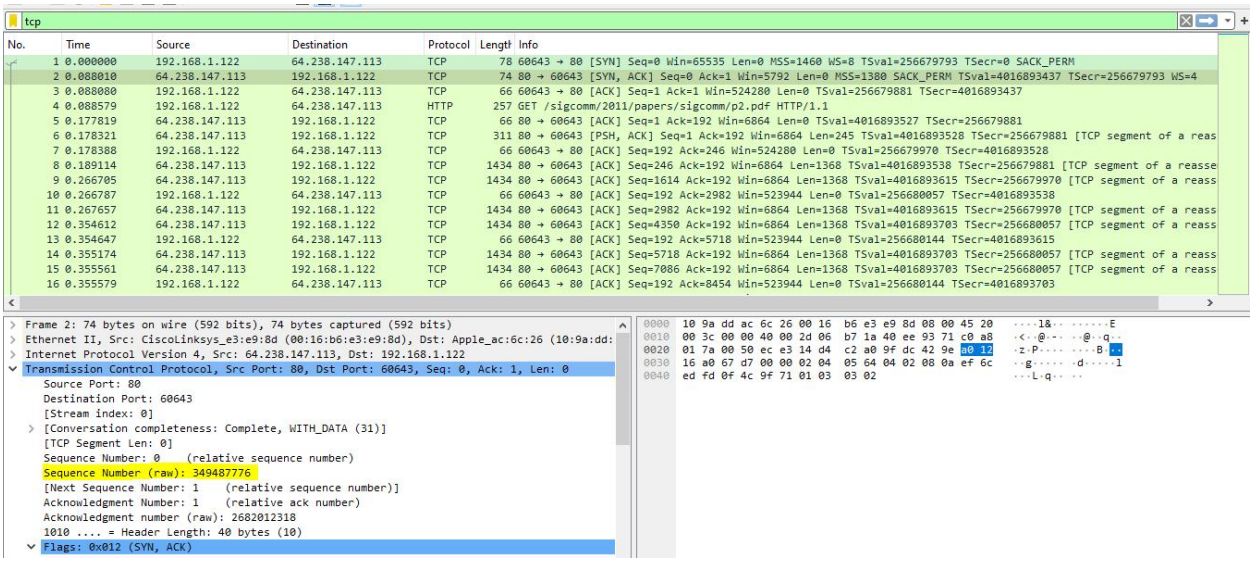


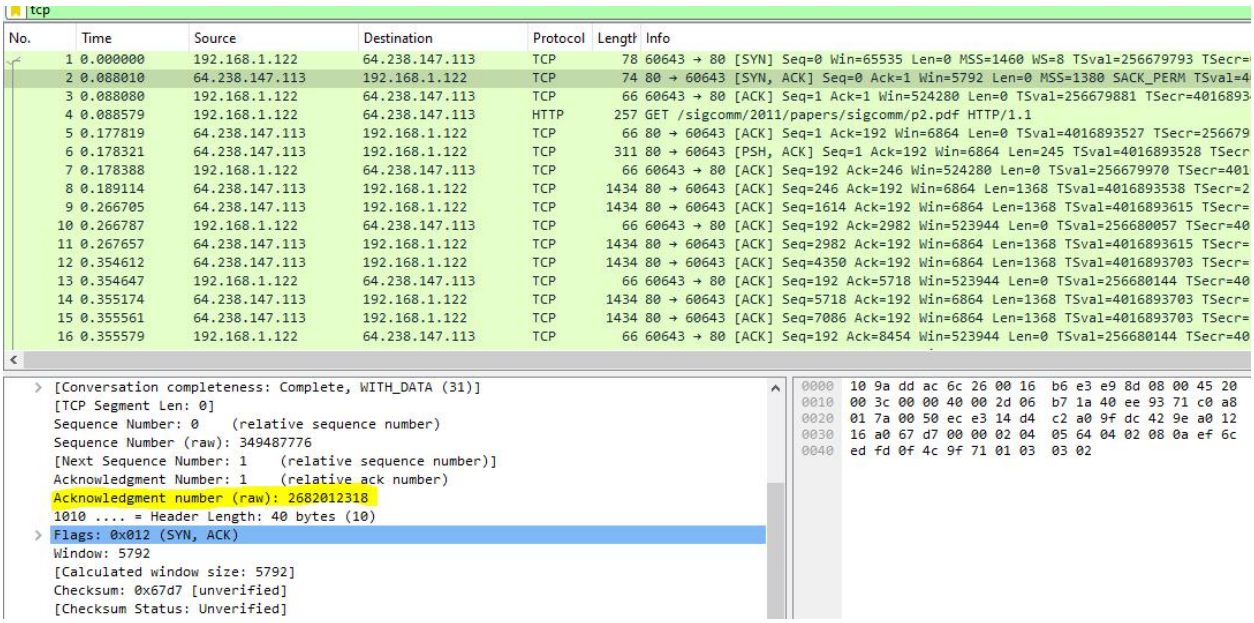
To Identify the segment that is it a SYN Segment check it SYN bit is set to 1 or not. If the SYN bit is set to 1 that means it is a SYN Segment. The segment I am inspecting is SYN because SYN bit is 1.



3. What is the sequence number of the SYNACK segment sent by the server to

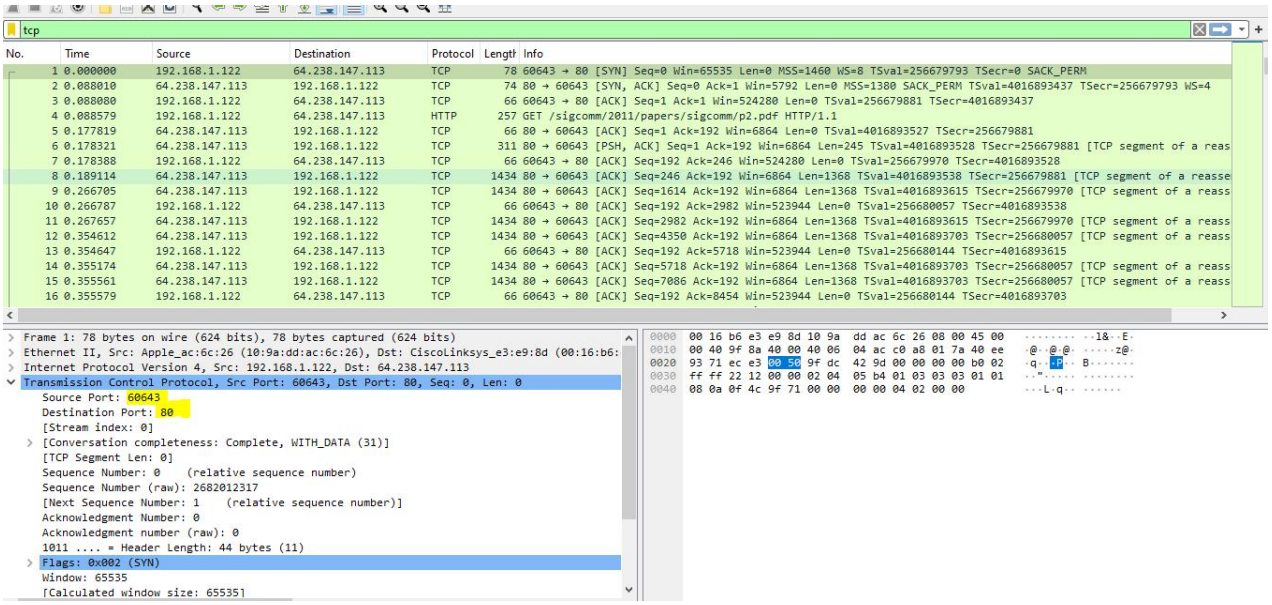
the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did server determine that value? What is it in the segment that identifies the segment as a SYNACK segment?



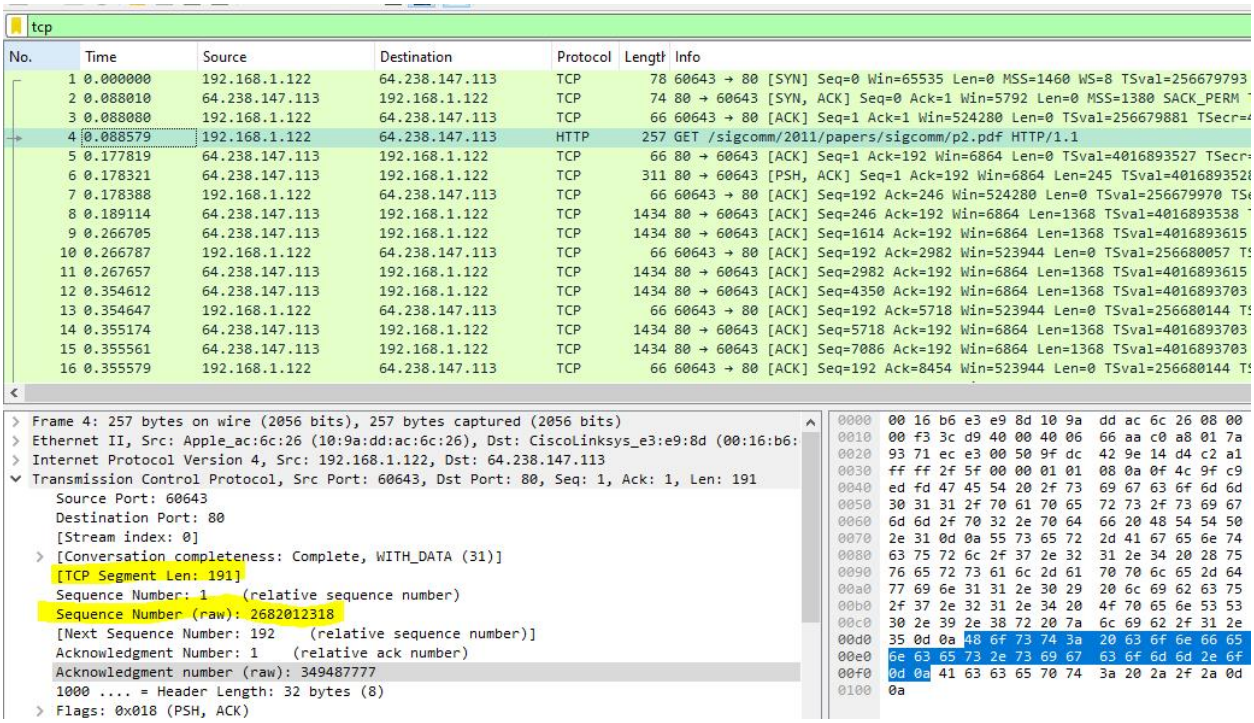


Server determines the value of Acknowledgement field by adding 1 in the previous segment sequence number.

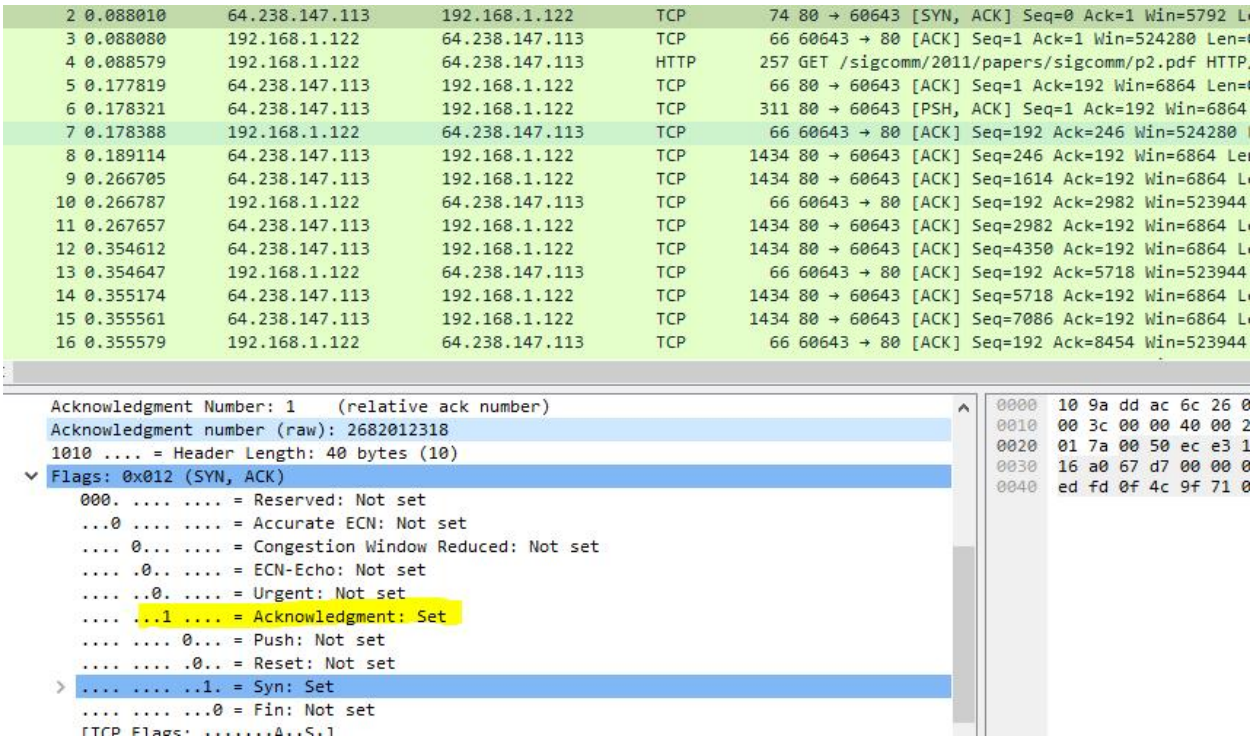
Previous segment sequence number:



Acknowledgement number of the second Segment

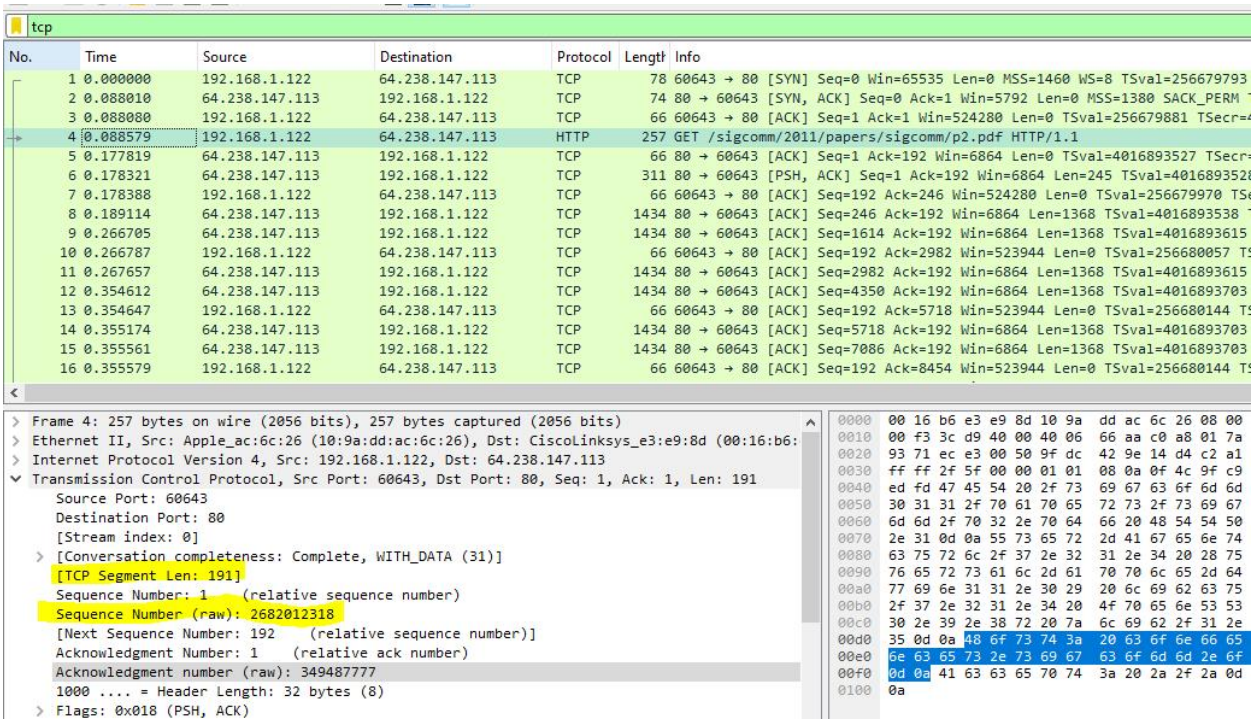


The **SYN** and **ACK** bit is set to 1. This identify the segment as **SYNACK** segment.

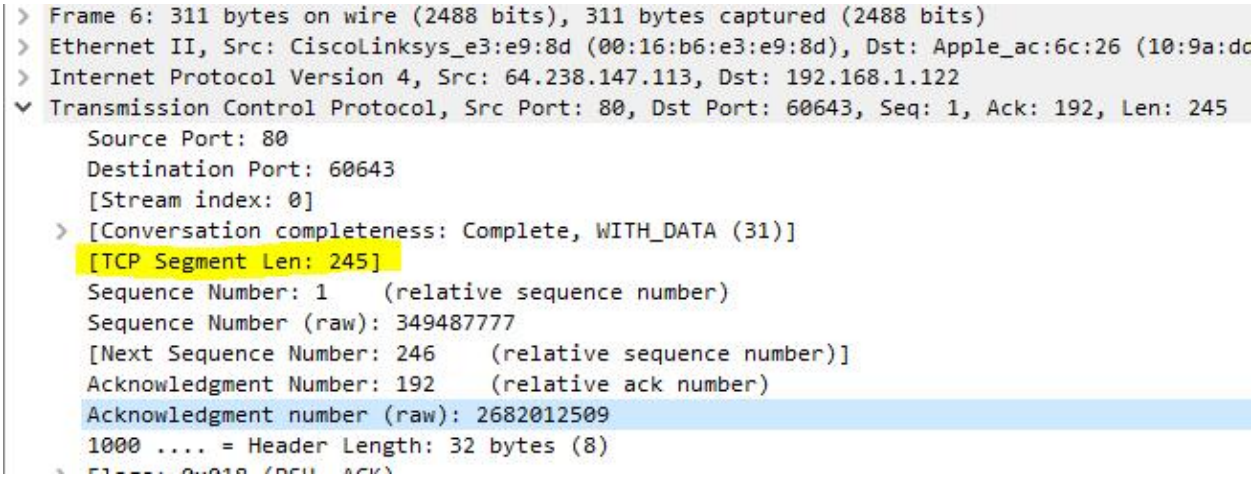


What is the length of each of the first six TCP segments?

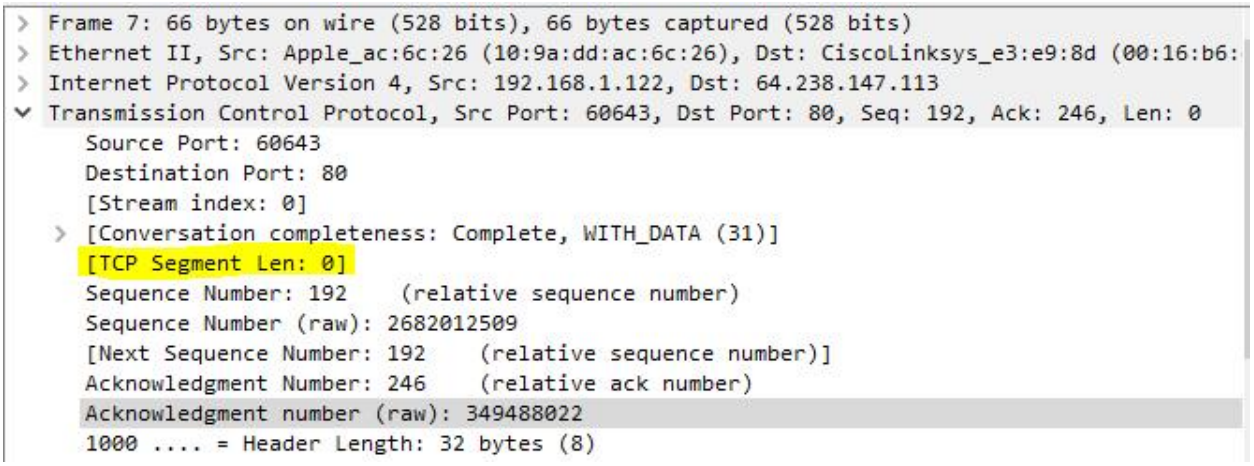
After Handshaking first http length:



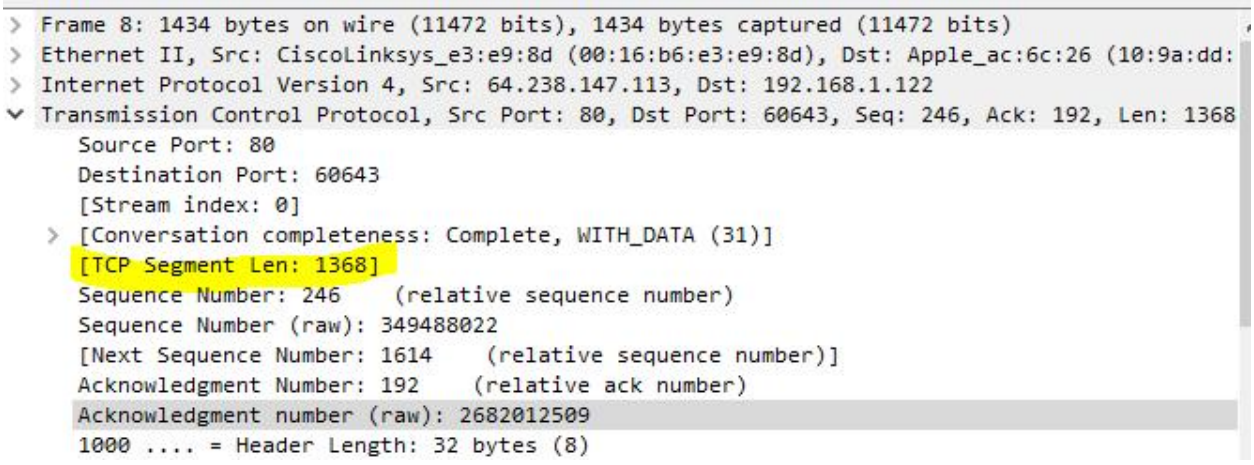
Second Tcp Segment Length :



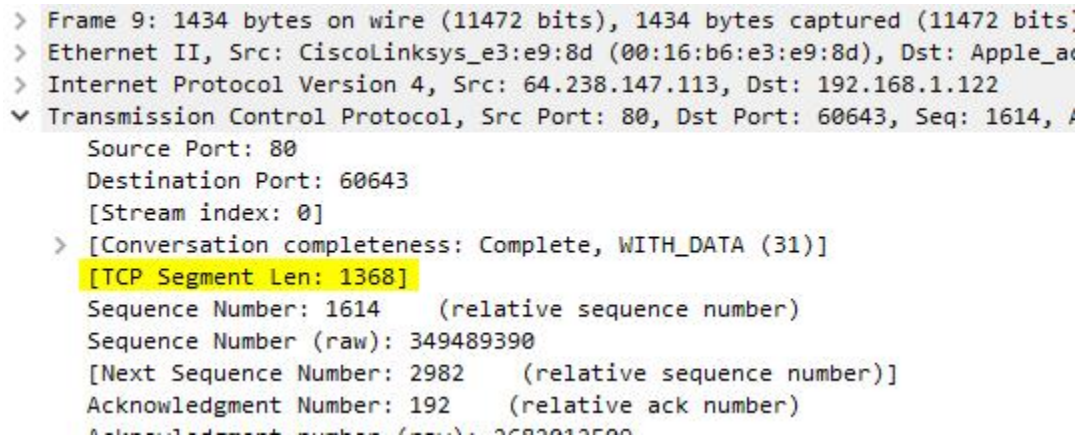
Third TCP Segment Length :



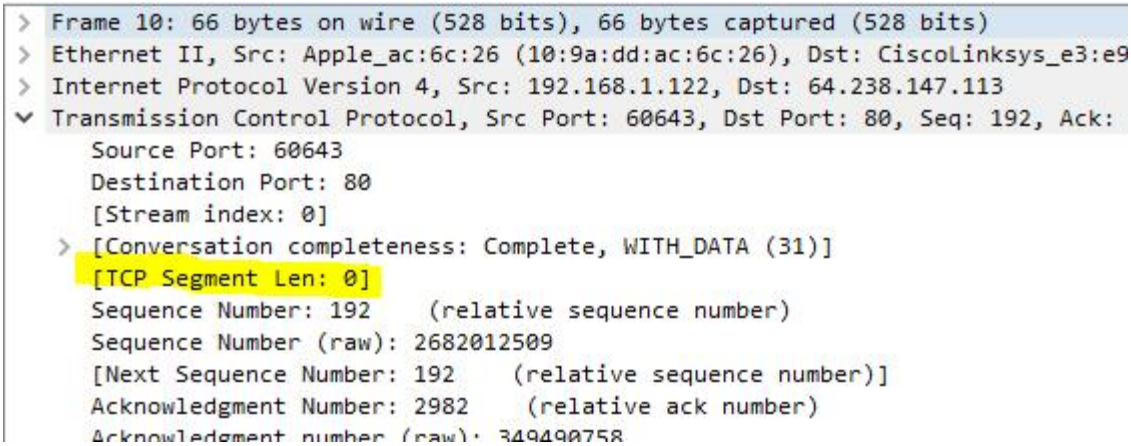
4th TCP Segment Length:



5th TCP Segment Length:



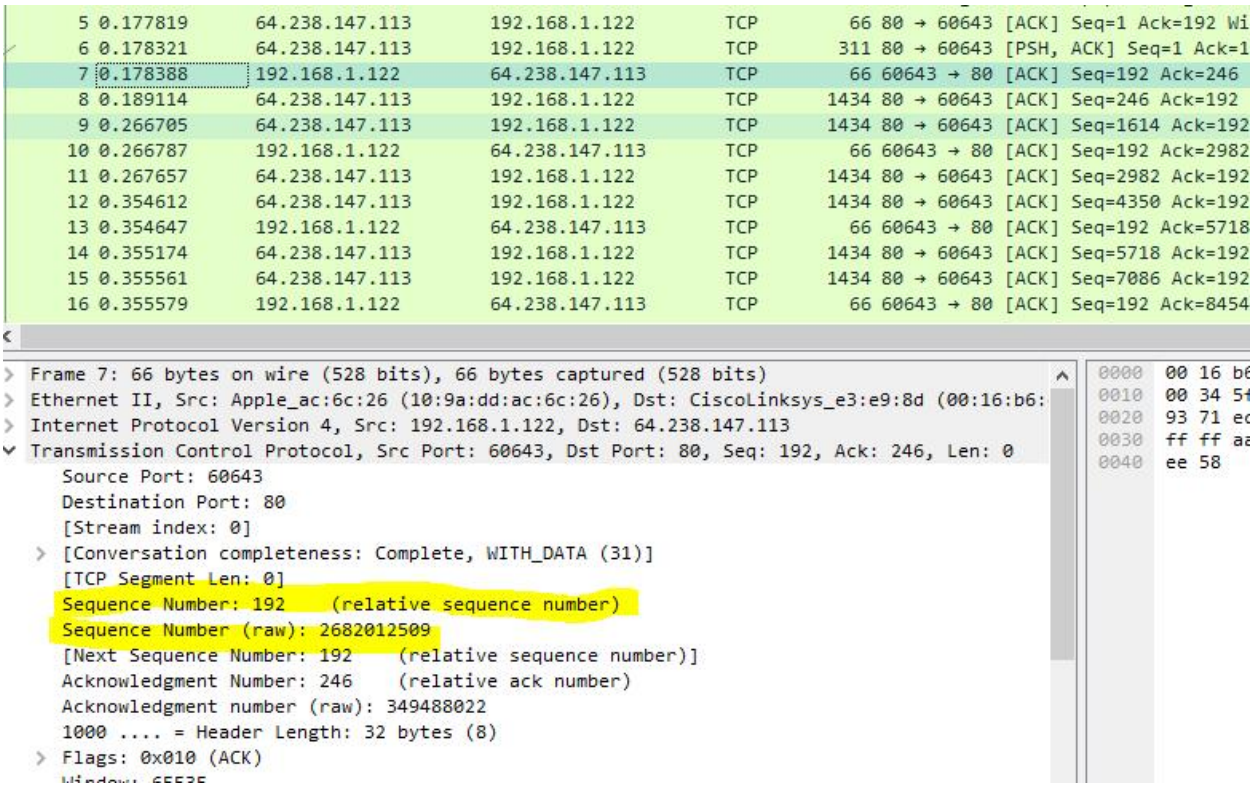
6th TCP Segment Length:



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

Ans: Yes, there are re-transmitted segments in the trace file.

• Segment 7 has the sequence number = **192** (relative sequence number) and it has raw sequence number = **2682012509** source and destination are also same. ACK is also 1.



```
    5 0.177819    64.238.147.113    192.168.1.122     TCP      66 80 → 60643 [ACK] Seq=1 Ack=192 Wi
    6 0.178321    64.238.147.113    192.168.1.122     TCP     311 80 → 60643 [PSH, ACK] Seq=1 Ack=1
    7 0.178388    192.168.1.122     64.238.147.113    TCP      66 60643 → 80 [ACK] Seq=192 Ack=246
    8 0.189114    64.238.147.113    192.168.1.122     TCP    1434 80 → 60643 [ACK] Seq=246 Ack=192
    9 0.266705    64.238.147.113    192.168.1.122     TCP    1434 80 → 60643 [ACK] Seq=1614 Ack=192
   10 0.266787    192.168.1.122     64.238.147.113    TCP      66 60643 → 80 [ACK] Seq=192 Ack=2982
   11 0.267657    64.238.147.113    192.168.1.122     TCP    1434 80 → 60643 [ACK] Seq=2982 Ack=192
   12 0.354612    64.238.147.113    192.168.1.122     TCP    1434 80 → 60643 [ACK] Seq=4350 Ack=192
   13 0.354647    192.168.1.122     64.238.147.113    TCP      66 60643 → 80 [ACK] Seq=192 Ack=5718
   14 0.355174    64.238.147.113    192.168.1.122     TCP    1434 80 → 60643 [ACK] Seq=5718 Ack=192
   15 0.355561    64.238.147.113    192.168.1.122     TCP    1434 80 → 60643 [ACK] Seq=7086 Ack=192
   16 0.355579    192.168.1.122     64.238.147.113    TCP      66 60643 → 80 [ACK] Seq=192 Ack=8454

> 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: CiscoLinksys_e3:e9:8d (00:16:b6:
> Internet Protocol Version 4, Src: 192.168.1.122, Dst: 64.238.147.113
v 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]
    Sequence Number: 192    (relative sequence number)
    Sequence Number (raw): 2682012509
    [Next Sequence Number: 192    (relative sequence number)]
    Acknowledgment Number: 246    (relative ack number)
    Acknowledgment number (raw): 349488022
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x010 (ACK)
    Window: 65535

0000  00 16 b6
0010  00 34 5f
0020  93 71 ec
0030  ff ff aa
0040  ee 58
```

The packet is retransmitted due to these reasons.