Name Nolan Anderson

Wireshark Project 3
Answers

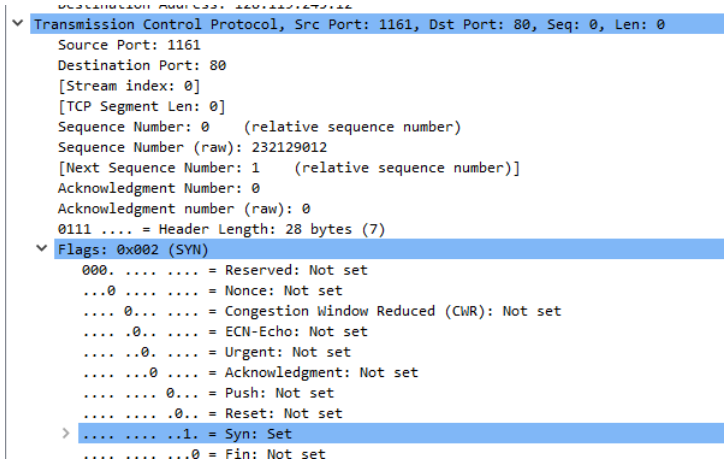
1. What is the IP address and TCP port number used by the client (source)?
   IP: 192.168.1.102
   PORT: 1161

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1

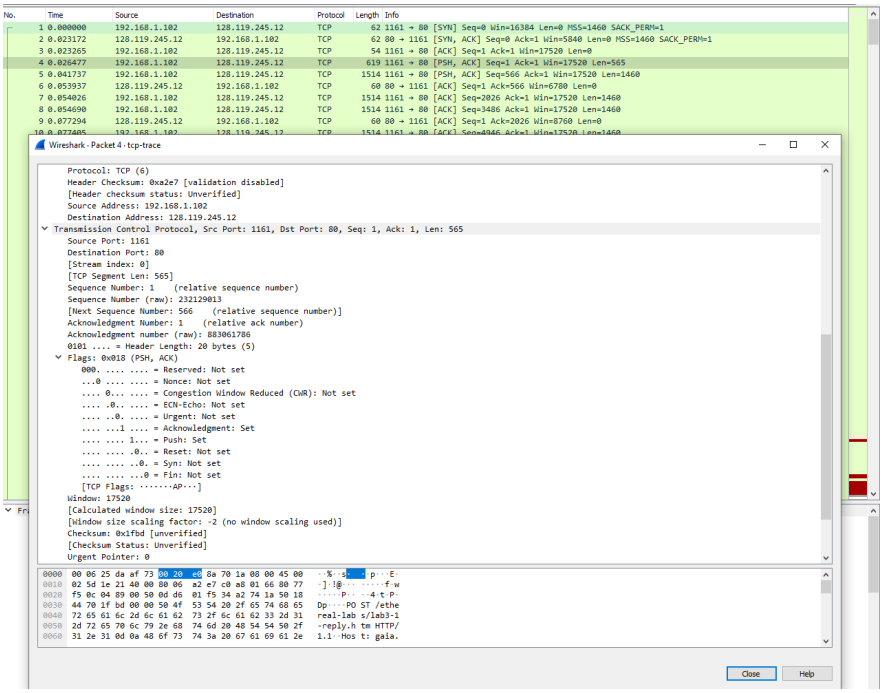
2. What is the IP address and TCP port number of the server (destination)?
   IP: 128.119.245.12
   PORT: 80

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1

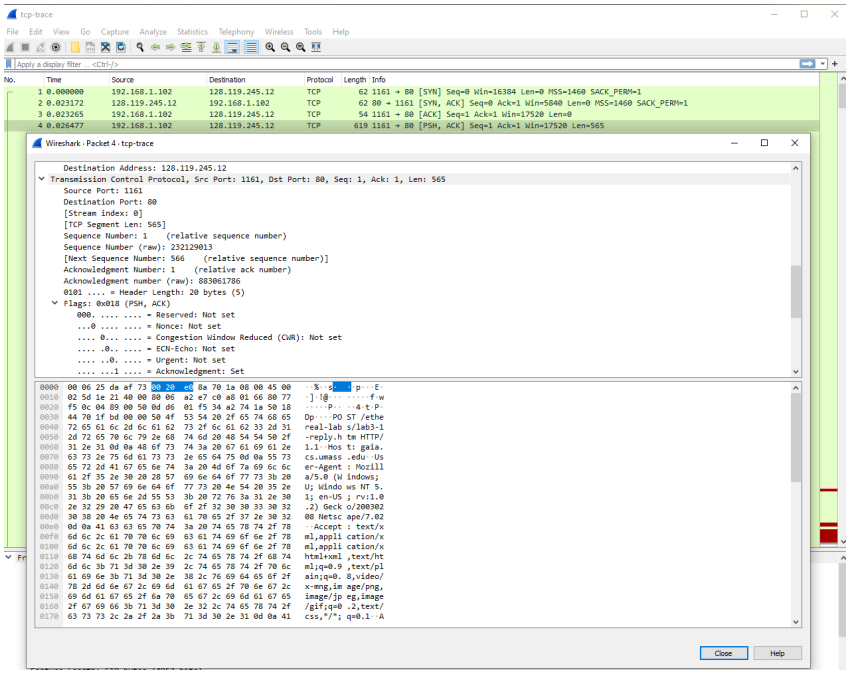
3. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client and server?
   When looking at the flags section, the SYN flag is set to 1. This indicates that the segment is a SYN segment.



4. What is the sequence number of the SYNACK segment sent by sever to the client in reply to the SYN?
   The sequence number provided is 0 and the acknowledgement segment is set to 1. The initial sequence number of SYN segment from the client is 0 which means that the ACKnowledgement field will be set to 1.



5. What is the sequence number of the TCP segment containing the HTTP POST command? *Hint: you need to dig into the packet content field looking for a segment with a "POST" within its DATA field.*



Segment number 4 contains the post command. The sequence number provided is 1.

6. What is the length of each of the first six TCP segments? Note that the first segment of these six segments starts from the one after completion of TCP handshake.

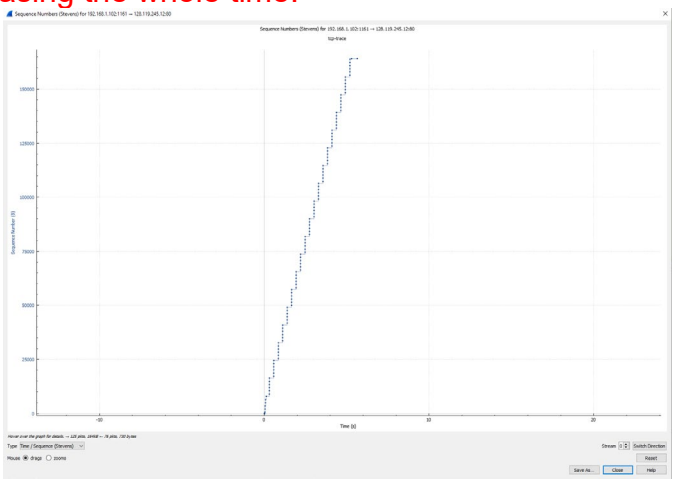
   First six segments are 4, 5, 7, 8, 10, 11
   Lengths are 565 for 4 and the rest are 1460.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
2	0.023172	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
3	0.023265	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	0.026477	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565
5	0.041737	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460
6	0.053937	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
7	0.054026	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460
8	0.054690	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460
9	0.077294	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10	0.077405	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460

7. What is the minimum advertised window size at the receiver for the entire trace? Does this flow control condition ever throttle the sender?
   Shown below, the buffer space advertised is 5840 bytes. The sender is never throttled as it never reaches the receiver buffer size.

```
Destination Address: 192.168.1.102
Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 1161
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 883061785
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 232129013
    0111 .... = Header Length: 28 bytes (7)
  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: 5840
```

8. Are there any retransmitted segments in the trace file? If there are any, indicate their sequence number(s).
   As shown in the figure below, it does not look like and of the packets are resent. They are continually increasing the whole time.



9. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What is the RTT value for each of the six segments? *(Hint: Use the difference in time of sending data and receiving ACK.)*

   What is the `EstimatedRTT` value after the receipt of each ACK? Use the original algorithm with alpha = 0.125. *(refer to my lecture slides for the right formula)*

   Note: Wireshark has the feature to plot the RTT. Select a TCP segment in the "listing of captured packets" window that is being sent from the client to the server. Then select: *Statistics->TCP Stream Graph->Round Trip Time Graph.*

Segment	SeqNum	ACK	Sent Time	ACK time	RTT	ERTT
4	1	6	0.0265	0.054	0.0275	0.0275
5	566	9	0.0417	0.0773	0.03556	0.028507
7	2026	12	0.054	0.1241	0.07006	0.033701
8	3486	14	0.0547	0.1691	0.11443	0.043792
10	4946	15	0.0774	0.2173	0.13989	0.055805
11	6406	16	0.0782	0.2678	0.18965	0.072535