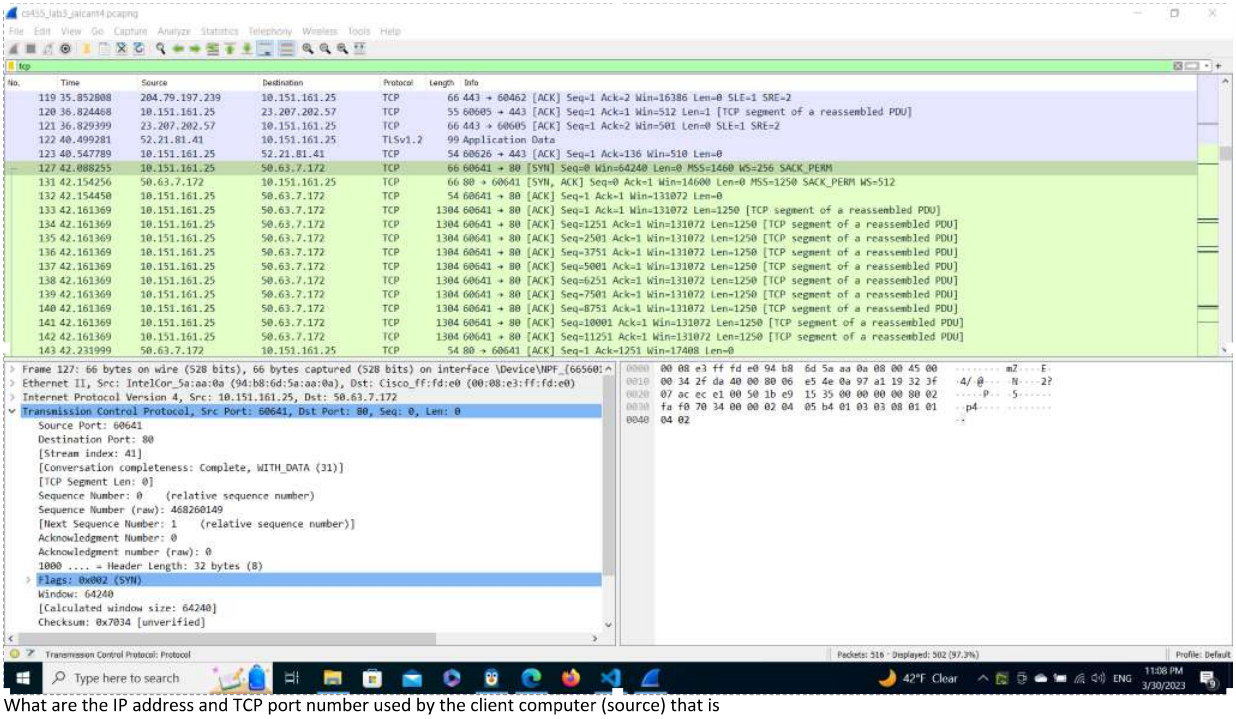
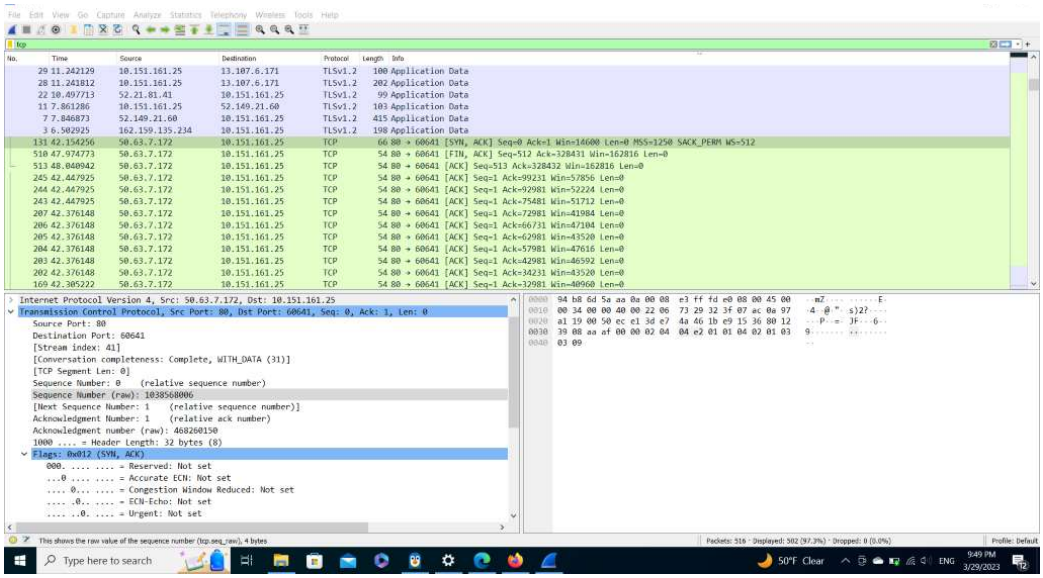
L3: Jed Alcantara

Wednesday, March 29, 2023 7:54 PM



1. What are the IP address and TCP port number used by the client computer (source) that is transferring the file to phpathak.com? To answer this question, it's probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the "details of the selected packet header window".
   a. The IP address is 10.151.161.25
   b. The source port is 60465
2. What is the IP address of phpathak.com? On what port number is it sending and receiving TCP segments for this connection?
   a. The IP address is 50.63.7.172
   b. The destination port is 80
3. What are the IP address and TCP port number used by your client computer (source) to transfer the file to phpathak.com?
   a. The IP address is 10.151.161.25
   b. The source port is 60465
4. What is the sequence number (raw and relative) of the TCP SYN segment that is used to initiate the TCP connection between the client computer and phpathak.com? What is it in the segment that identifies the segment as a SYN segment? Include a screenshot of the corresponding packet.
   a. The raw and relative seq number is 468260150 and 1 respectively.
   b.
```
Source Port: 60641
Destination Port: 80
[Stream index: 41]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 1    (relative sequence number)
Sequence Number (raw): 468260150
[Next Sequence Number: 1    (relative sequence number)]
Acknowledgment Number: 1    (relative ack number)
Acknowledgment number (raw): 1038568007
```
   c. The SYN is 0.
   d.
```
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
000. .... .... = Reserved: Not set
...0 .... .... = Accurate ECN: Not set
.... 0... .... = Congestion Window Reduced: Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
.... ...1 .... = Acknowledgment: Set
.... .... 0... = Push: Not set
.... .... .0.. = Reset: Not set
.... .... ..0. = Syn: Not set
.... .... ...0 = Fin: Not set
[TCP Flags: ·····A····]
```
5. What is the sequence number (raw and relative) of the SYNACK segment sent by phpathak.com to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? What is it in the segment that identifies the segment as a SYNACK segment? Include a screenshot of the corresponding packet.



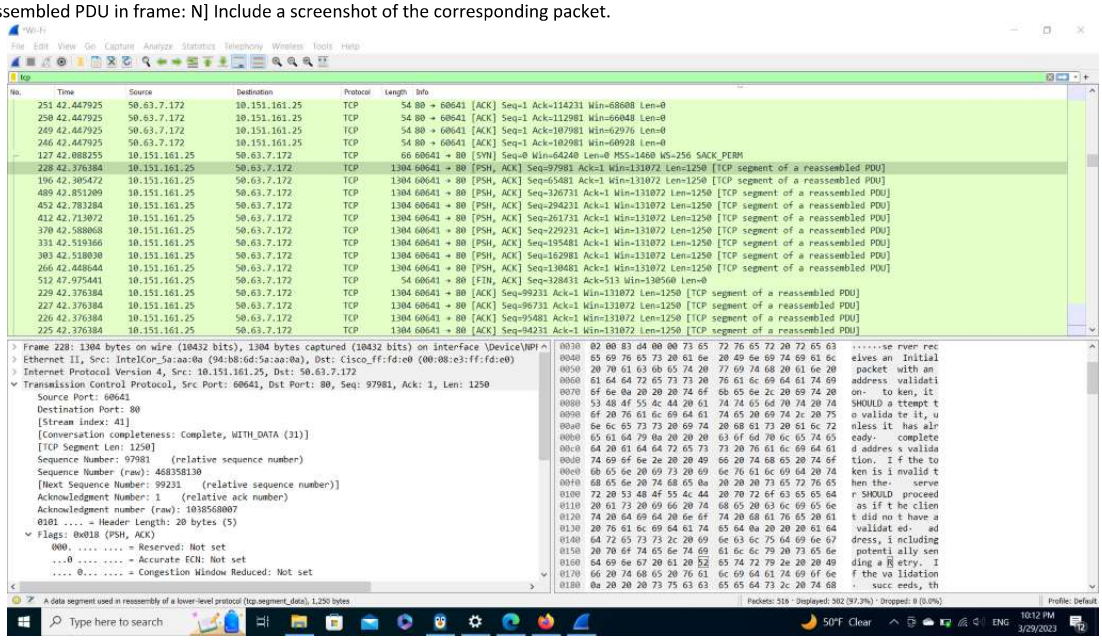
a. The raw and relative sequence number is 1038568006 and 0.

b.
```
1000 .... = Header Length: 32 bytes (8)
Flags: 0x012 (SYN, ACK)
   000. .... .... = Reserved: Not set
   ...0 .... .... = Accurate ECN: Not set
   .... 0... .... = Congestion Window Reduced: 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: 14600
```

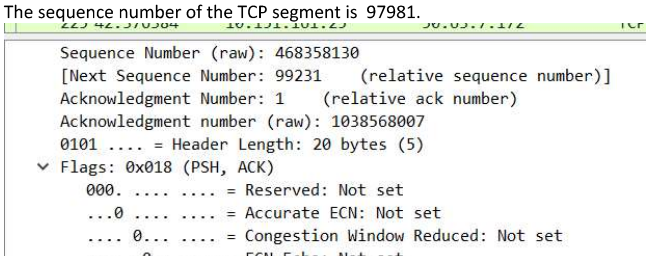
c. The ACK is 1.

d. The segment that identifies the segment as a SYNACK is if both the ACK and SYN are 1.

6. What is the sequence number of the TCP segment containing the HTTP POST command? The file is uploaded first with many data-ack chunks of packets, followed by the POST command (i.e., the POST command might be later in the capture). Also, keep an eye on [Reassembled PDU in frame: N] Include a screenshot of the corresponding packet.



a. The sequence number of the TCP segment is 97981.

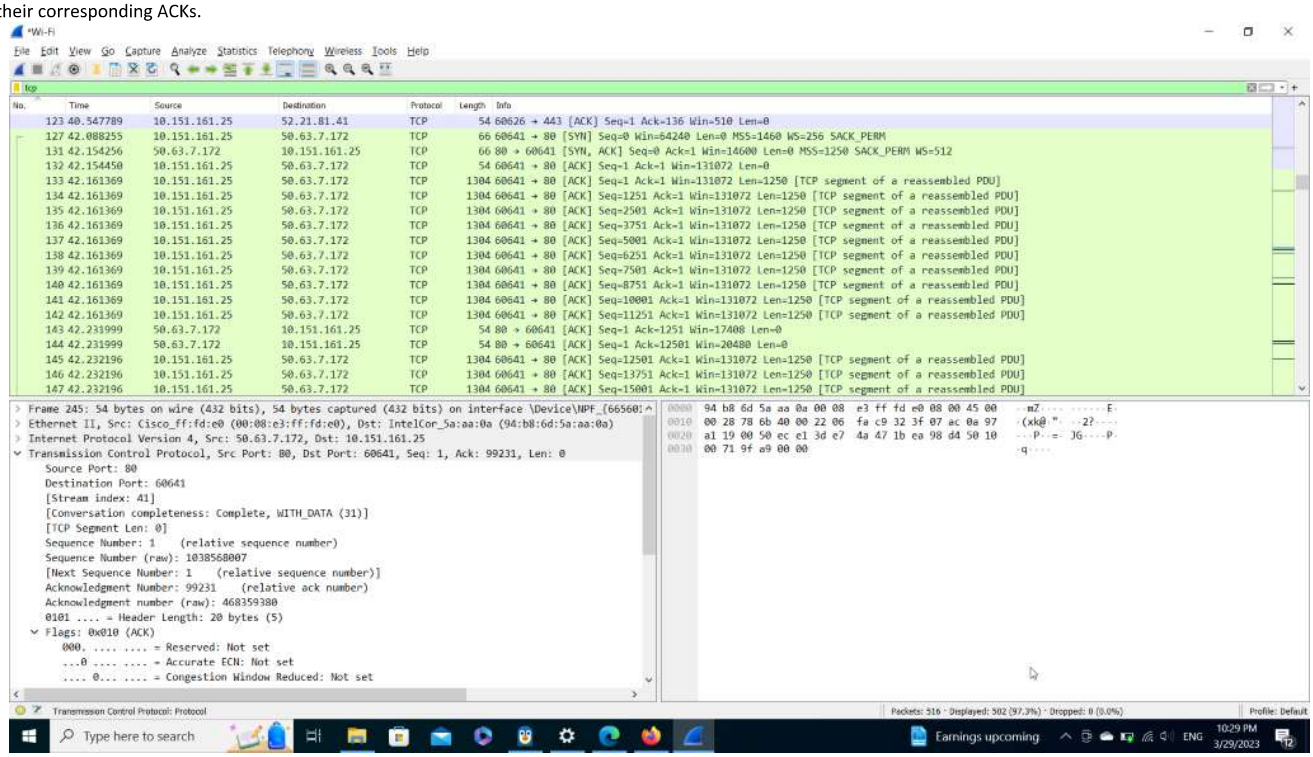


```
Sequence Number (raw): 468358130
[Next Sequence Number: 99231    (relative sequence number)]
Acknowledgment Number: 1    (relative ack number)
Acknowledgment number (raw): 1038568007
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
   000. .... .... = Reserved: Not set
   ...0 .... .... = Accurate ECN: Not set
   .... 0... .... = Congestion Window Reduced: Not set
```

b.
```
        .... .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: 512
    [Calculated window size: 131072]
```

c. The segment containing POST is set to 1. It is Push.

7. Consider the first 10 TCP segments part of uploading the file (No. 249 onwards in the example screenshot of Fig. 1 given above). At what time was each segment sent? When was the ACK for each segment received? Given the difference between when each TCP segment was sent, and when its acknowledgment was received, what is the RTT value for each of the ten segments? Include a screenshot like Fig. 1 above showing the 10 segments and their corresponding ACKs.



a. The segments are 133-142. The ACK segments are 144

Segment	Seg no.	Sent	ACK	RTT
133	1	42.16	42.23	0.07
134	1251	42.16	42.23	0.07
135	2501	42.16	42.23	0.07
136	3751	42.16	42.23	0.07
137	5001	42.16	42.23	0.07
138	6251	42.16	42.23	0.07
139	7501	42.16	42.23	0.07
140	8751	42.16	42.23	0.07
141	10001	42.16	42.23	0.07
142	12501	42.16	42.23	0.07

8. What is the length of each of the first 10 TCP segments? What is the length of their corresponding ACK segments?
   a. The length of the first ten segments is 1304.
   b. The length of the ACKs are 54.
9. Do you observe any TCP DUP ACKs or retransmitted TCP segments in your capture? Note that this is different for every trace, so it is possible that you might or might not see them. If you do, include a screenshot of such a packet.

a. No. 143 and no. 144 were ACKs for 1251 and 12501 respectively at the same time. According to the protocol, that means the receiver was expecting the next window of packets. Due to the previous packets and the next packets sent, no. 143 is possibly a dup packet.