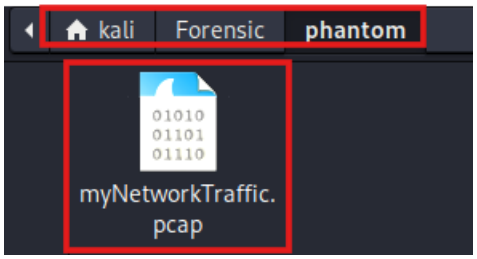
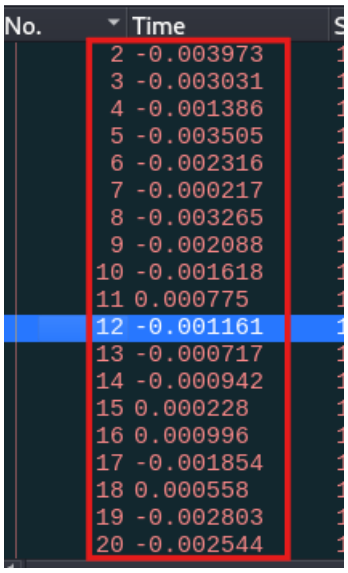
Forensic CTF: Ph4nt0m 1ntrud3r

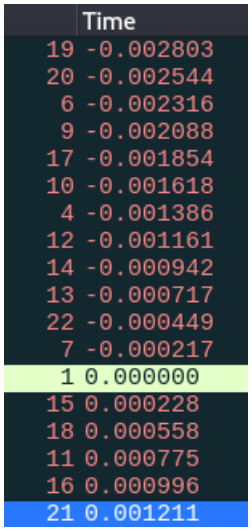
Student Name: John Bless Santos

1. We download the pcap file provided by the CTF
   a. 

2. We use Wireshark to open the file
3. The following hints given were:
   a. Filter your packets to narrow down your search
   b. Attacks were done in a timely matter
   c. Time is essential
4. From these hints, we can determine that we would need to use time to find the flag. Since the attacks were done in a timely matter, the flag could be segmented into different packets.
5. We noticed the packet order had different transmission times
   a. 

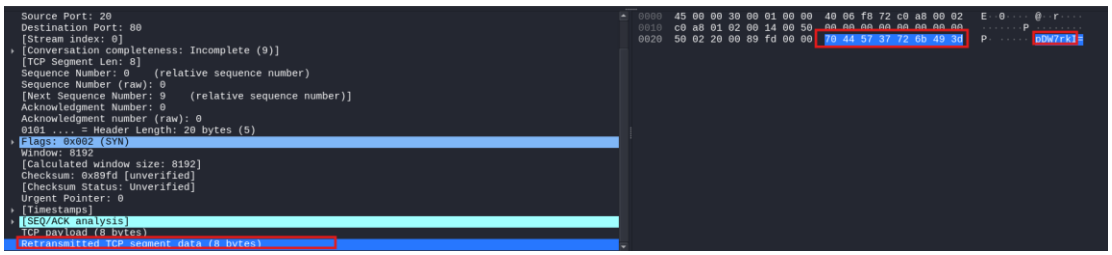
No.	Time
2	-0.003973
3	-0.003031
4	-0.001386
5	-0.003505
6	-0.002316
7	-0.000217
8	-0.003265
9	-0.002088
10	-0.001618
11	0.000775
12	-0.001161
13	-0.000717
14	-0.000942
15	0.000228
16	0.000996
17	-0.001854
18	0.000558
19	-0.002803
20	-0.002544

6. We organize the time

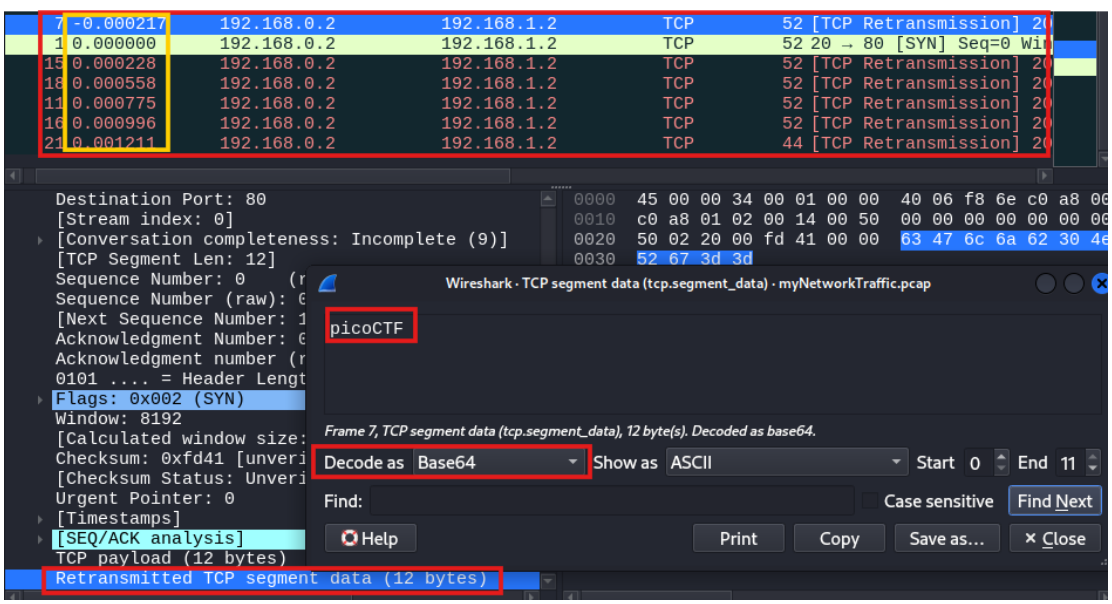
a. 

	Time
19	-0.002803
20	-0.002544
6	-0.002316
9	-0.002088
17	-0.001854
10	-0.001618
4	-0.001386
12	-0.001161
14	-0.000942
13	-0.000717
22	-0.000449
7	-0.000217
1	0.000000
15	0.000228
18	0.000558
11	0.000775
16	0.000996
21	0.001211

7. When we look at the ASCII data from the packets, we can retransmit TCP segment data. When we further look, we can see that the data shown is not readable.

a. 

8. We can assume the data might be encrypted. We chose base64 to decode since it is commonly used.
9. When we analyze the packets, the packets with a positive time have a frame length of 12 bytes. We analyze this first. We choose the packet, go to “Retransmitted TCP segment data (12 bytes)”, then show packet bytes and then decode as Base64.

a. 

b. We decode the rest of the packets after and combine all the flag segments
c. picoCTF{1t_w4snt_th4t_34sy_tbh_4r_d1065384}
d.