Computer Networks Laboratory

NAME: PREM SAGAR J S	SRN: PES1UG20CS825	SEC: 'H'

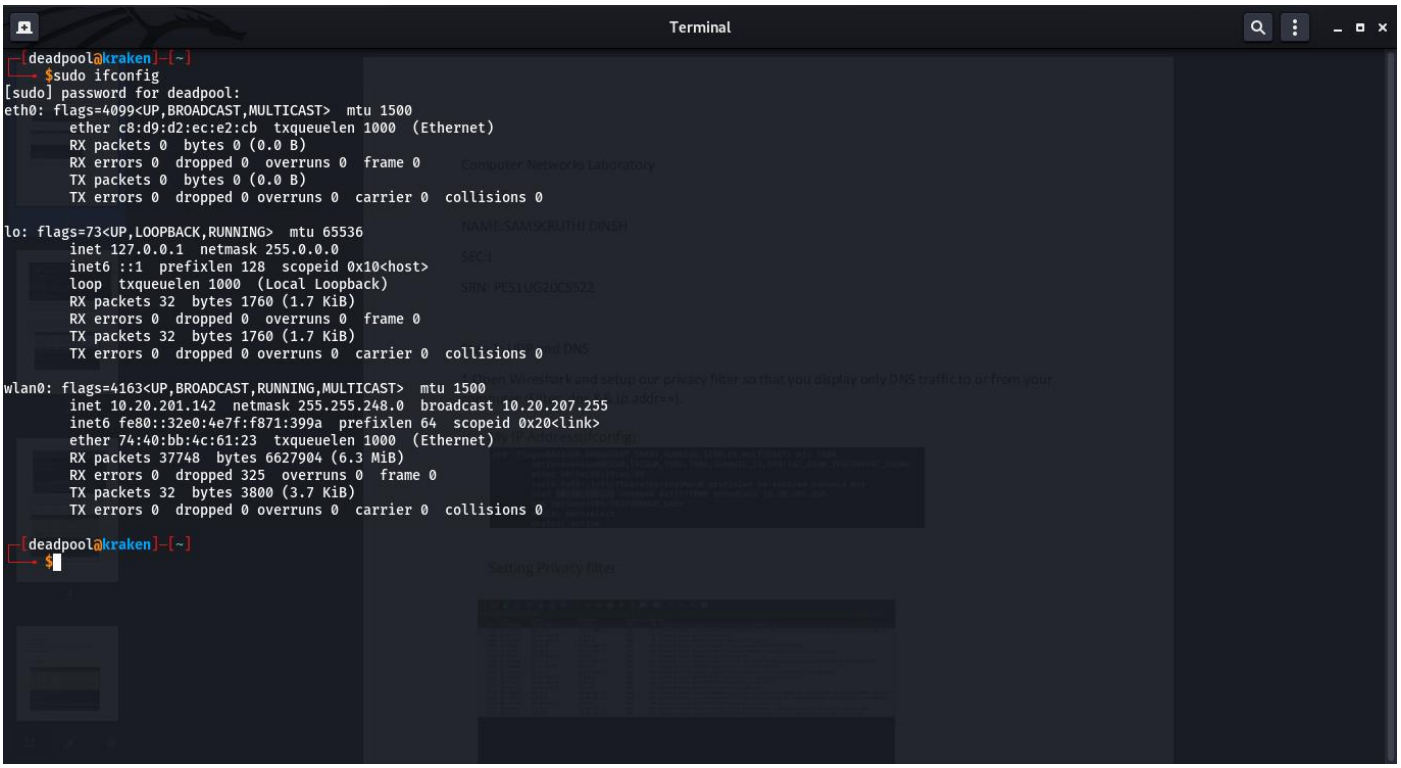
Lab #5

Understanding Transport and Network Layer using Wireshark

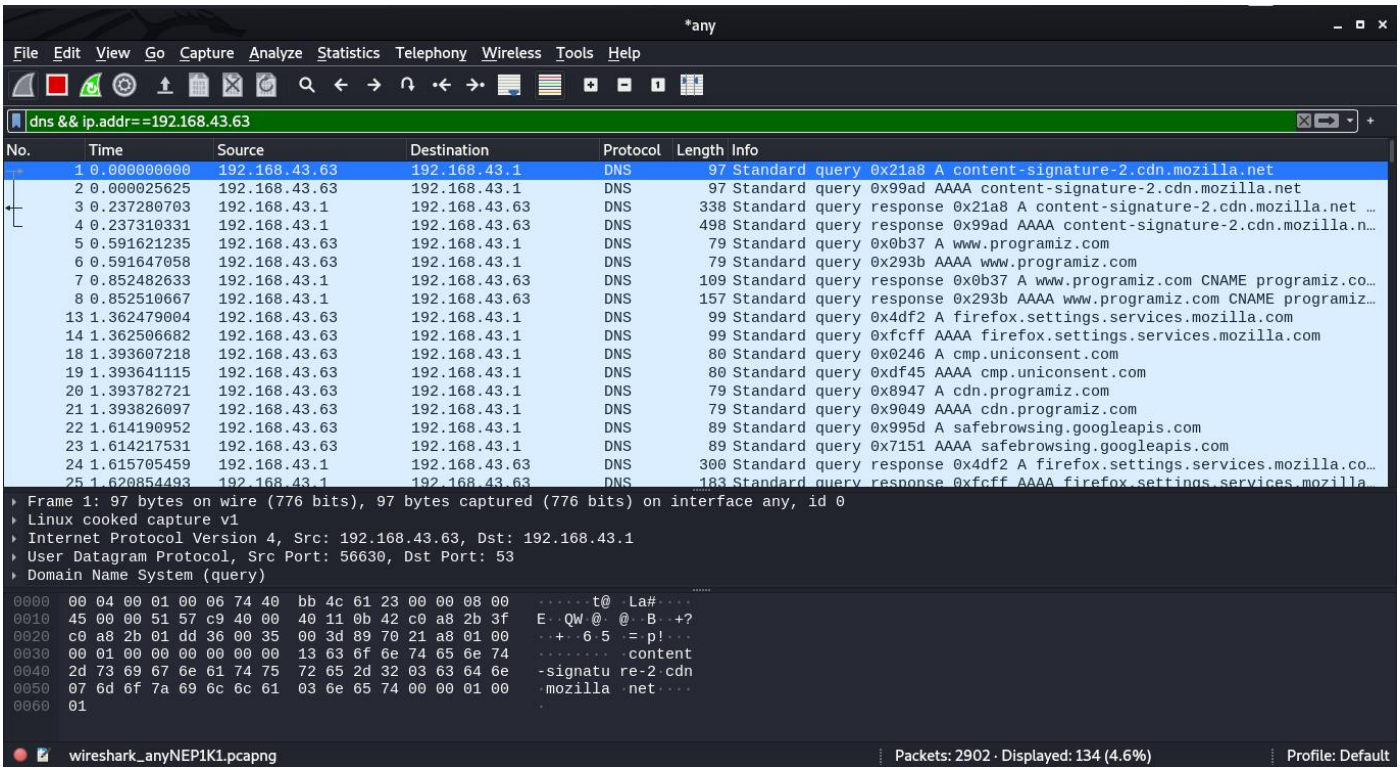
Step 1: UDP and DNS

1) Open Wireshark and set up our privacy filter so that you display only DNS traffic to or from your computer (Filter: **dns && ip.addr==<your IP address>**).

Ifconfig :



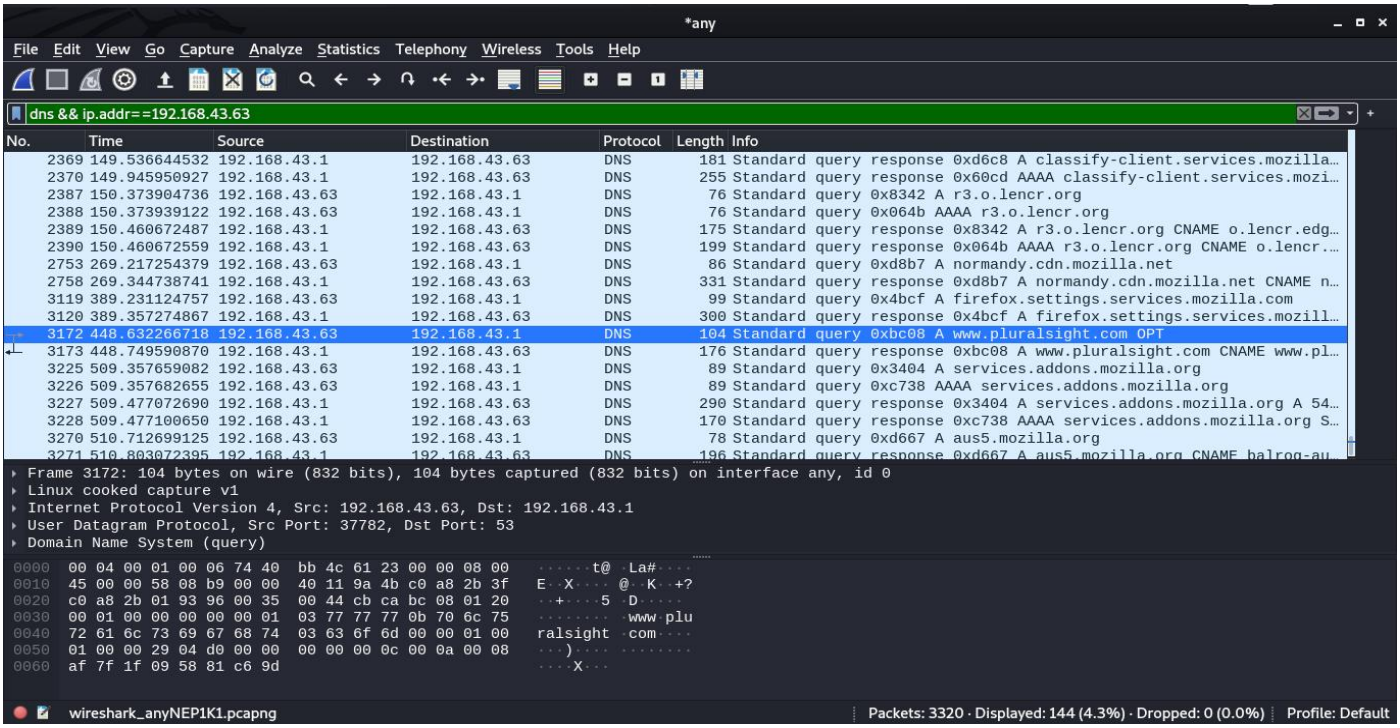
filter (**dns && ip.addr==<your IP address>**):

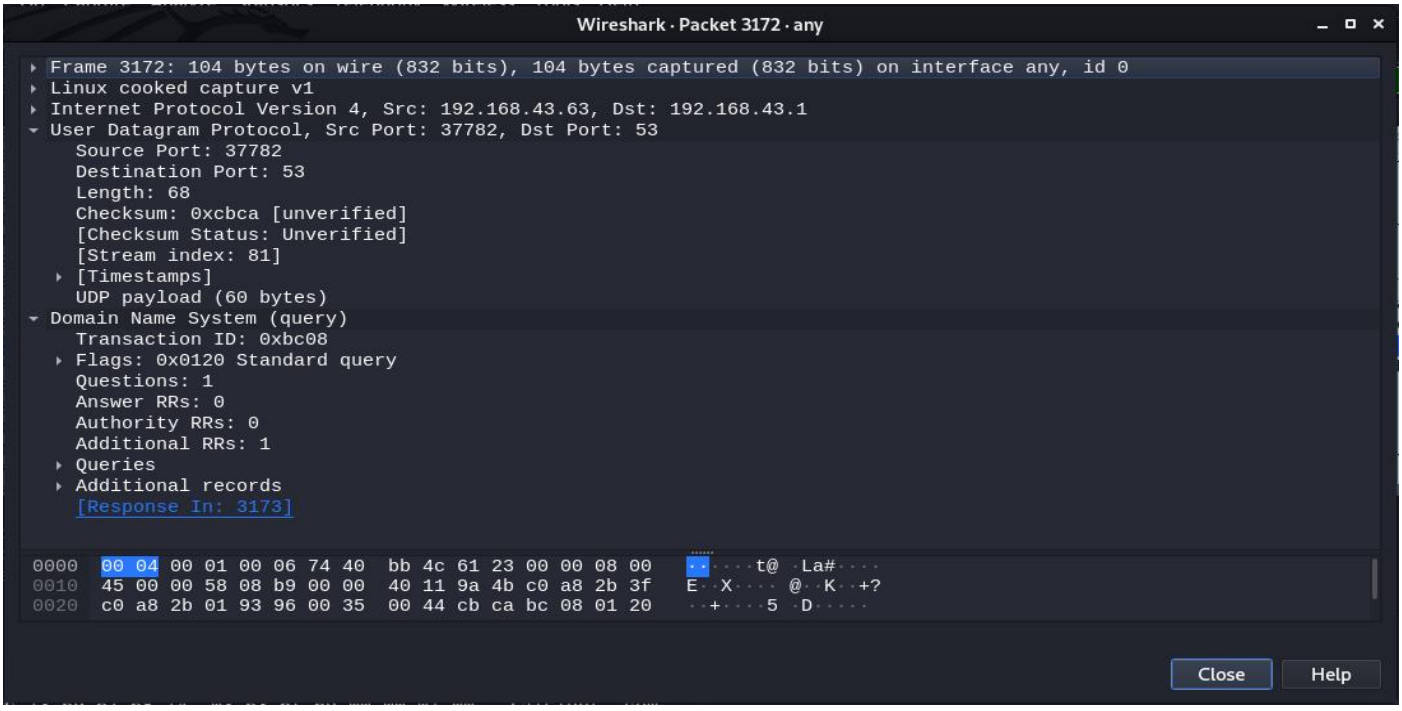


2) Use dig to generate a DNS query to lookup the domain name “www.pluralsight.com”. Then, stop the capture.

3) Before you look at the packets in Wireshark, think for a minute about what you expect to see as the UDP segment headers. What can you reasonably predict, and what could you figure out if you had some time and a calculator handy? Use your knowledge of UDP to inform your predictions. I expect to see Source-port and Destination-port numbers ,Length ,Check-sum and Application data.

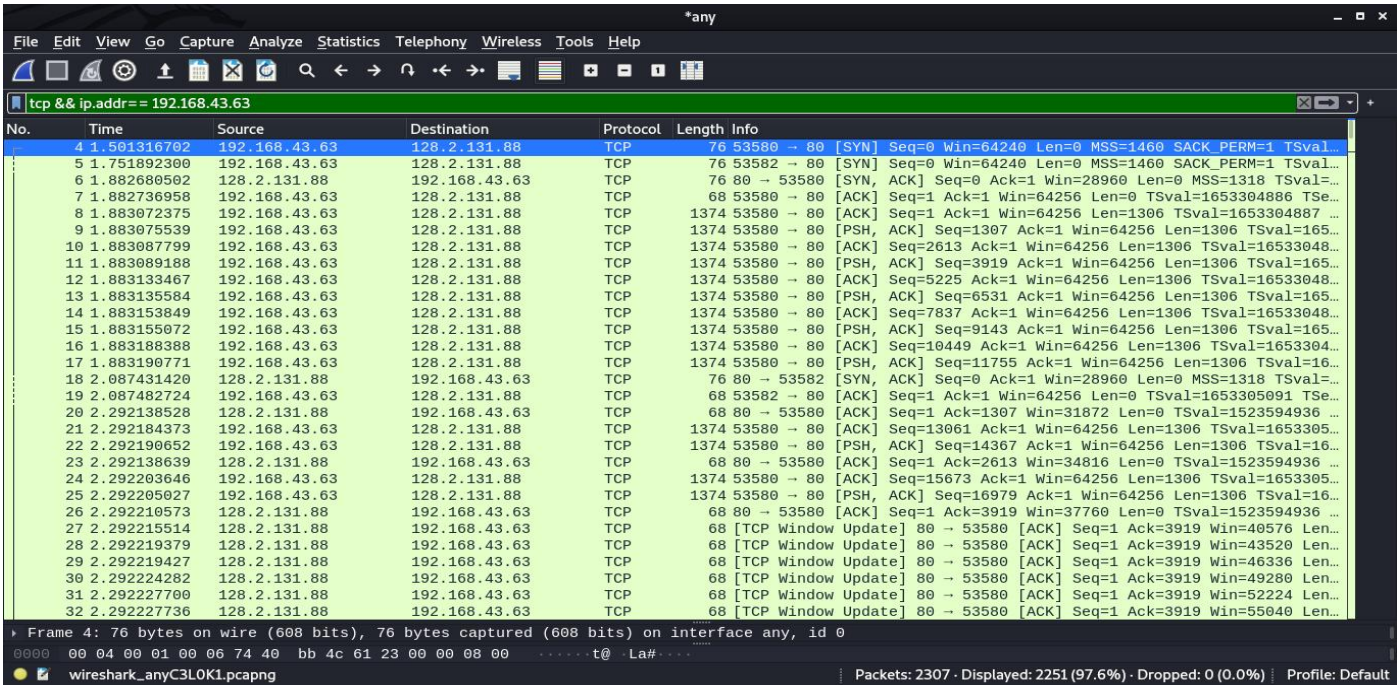
4) Take a look at the query packet on Wireshark. You'll see a bunch of bytes (70-75 bytes) listed as the actual packet contents in the bottom Wireshark window. The bytes at offsets up to number 33-34 are generated by the lower-level protocols .You will also see Wireshark interpret the header contents. Matchup the bytes int he packet contents window with each field of the UDP header. Were your predictions correct?





5) Continue to examine the DNS request packet. Which fields does the UDP checksum cover? Wireshark probably shows the UDP checksum as "Validation Disabled". Why is that? Due to the prevalence of offloading in modern hardware and operating systems.

Step 2: TCP



12) What is the IP address and TCP port number used by your computer (client) to transfer the file?

- TCP port number : 53589

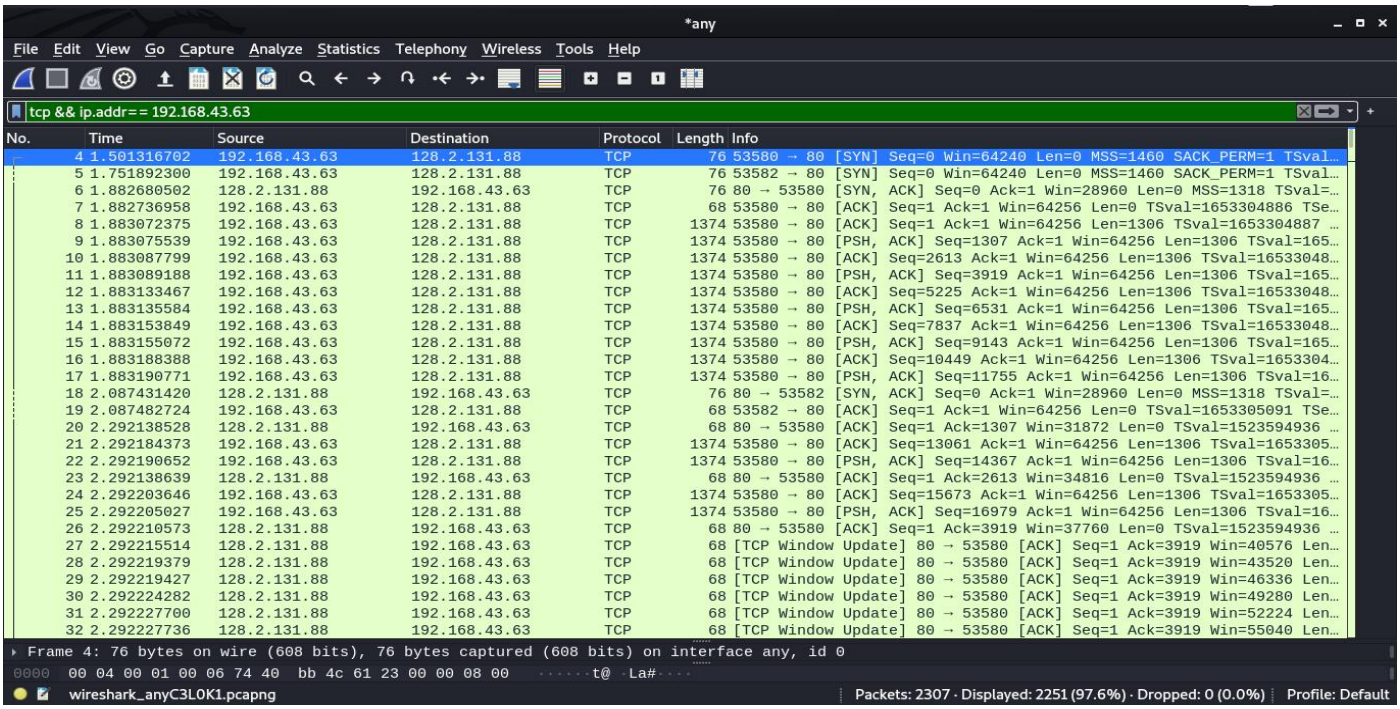
What is the IP address of the server?

- 128.2.131.88

On what port number is it
sending and receiving TCP segments for this transfer of the file?

- 80

After Disabling HTTP:



Step 2b: TCP Basics

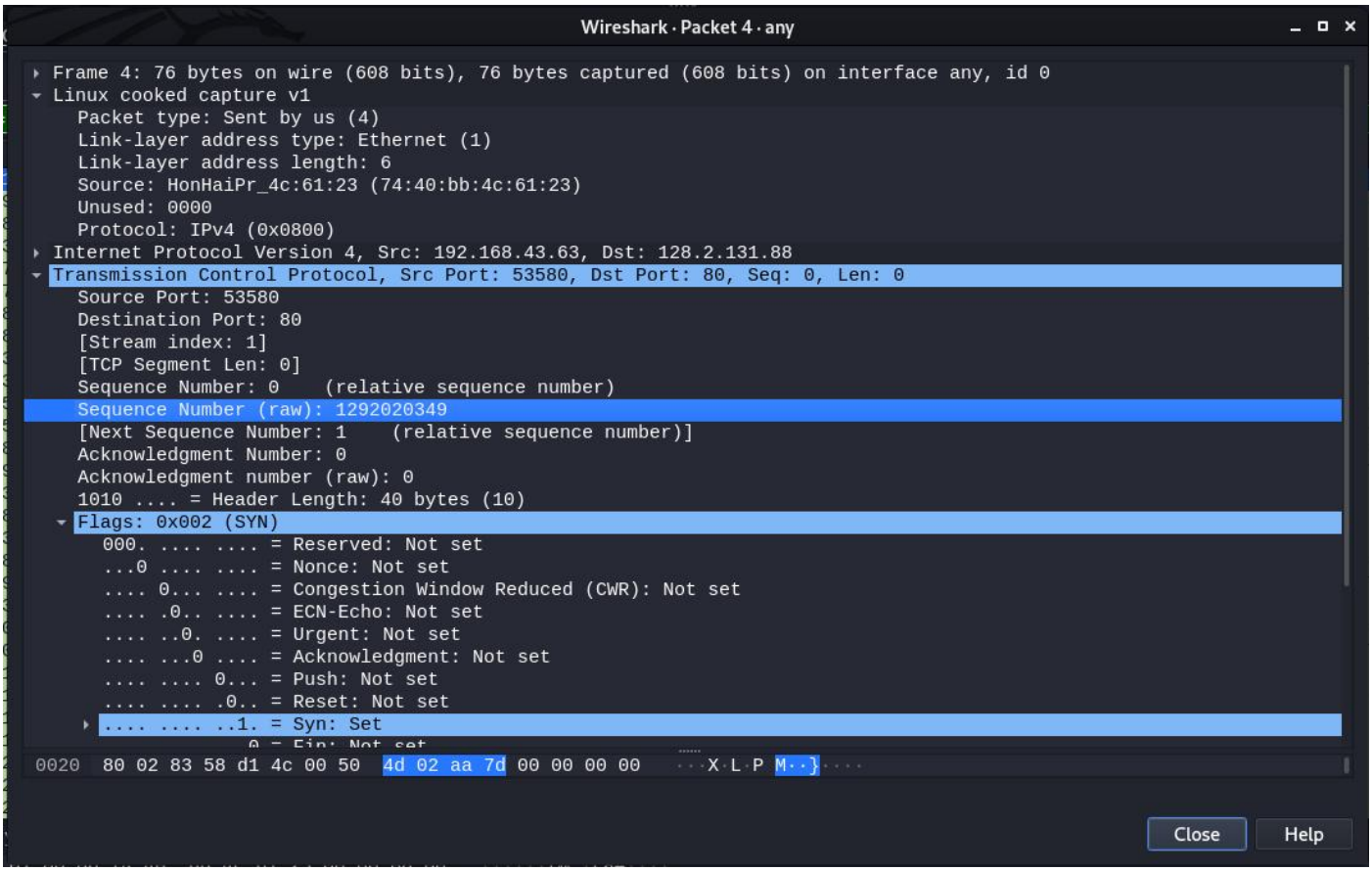
What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection?

○ Relative Sequence Number:0

○ Raw Sequence number:1292020349

What element of the segment identifies it as a SYN segment?

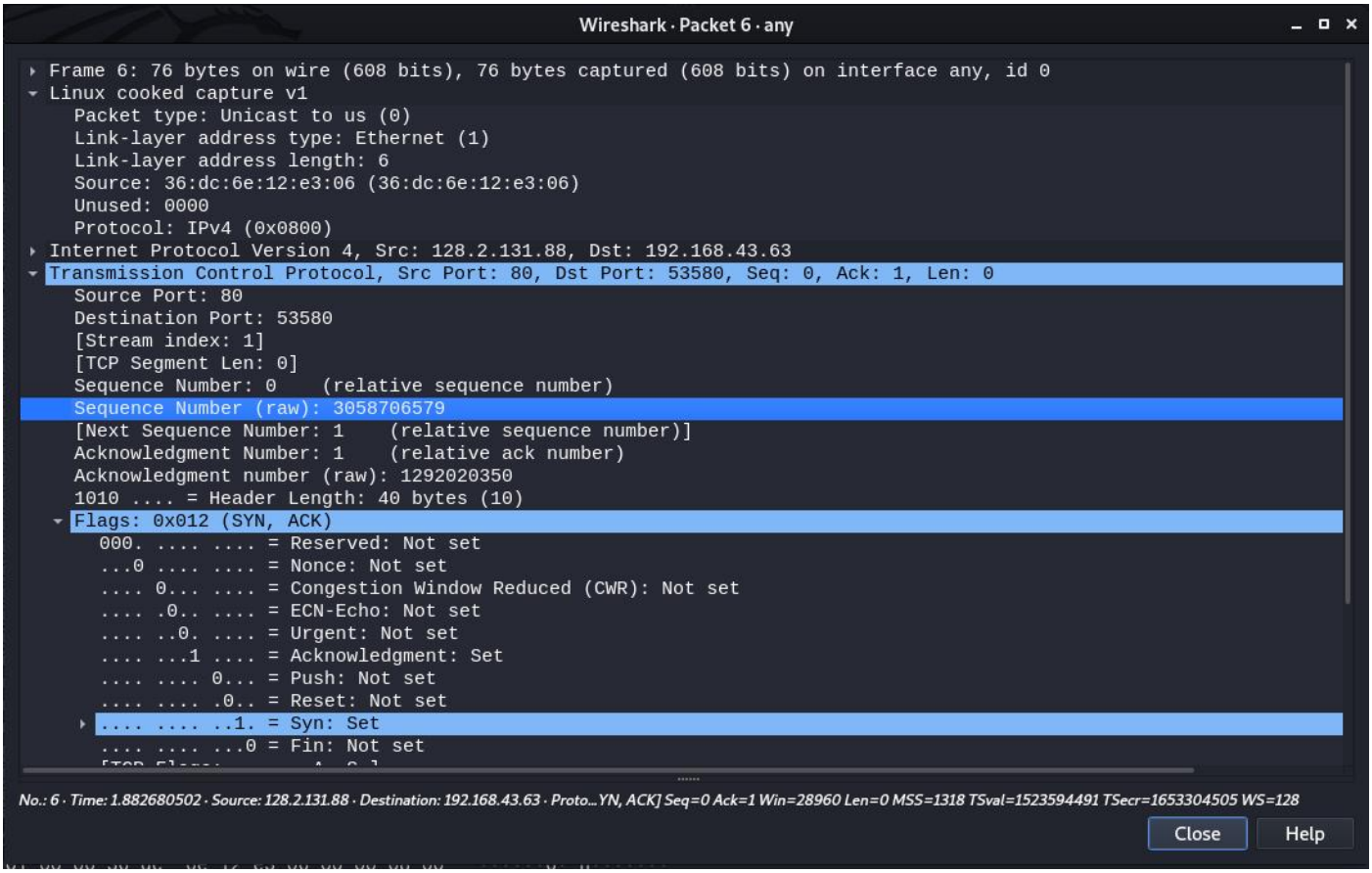
○ Here the SYN bit is set to 1 in the flags section in below figure. So, It can be identified as a SYN segment.



Wireshark uses relative sequence numbers by default. Can you obtain absolute sequence numbers instead? How?

○ Absolute Sequence number=Relative Sequence Number+offset

What is the sequence number of the SYNACK segment sent by the server in reply to the SYN?



○ the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN is 0.

What is the value of the Acknowledgement field in the SYNACK segment?

○ The value of the acknowledgement field in the SYNACK segment is 1 How did the server determine that value?

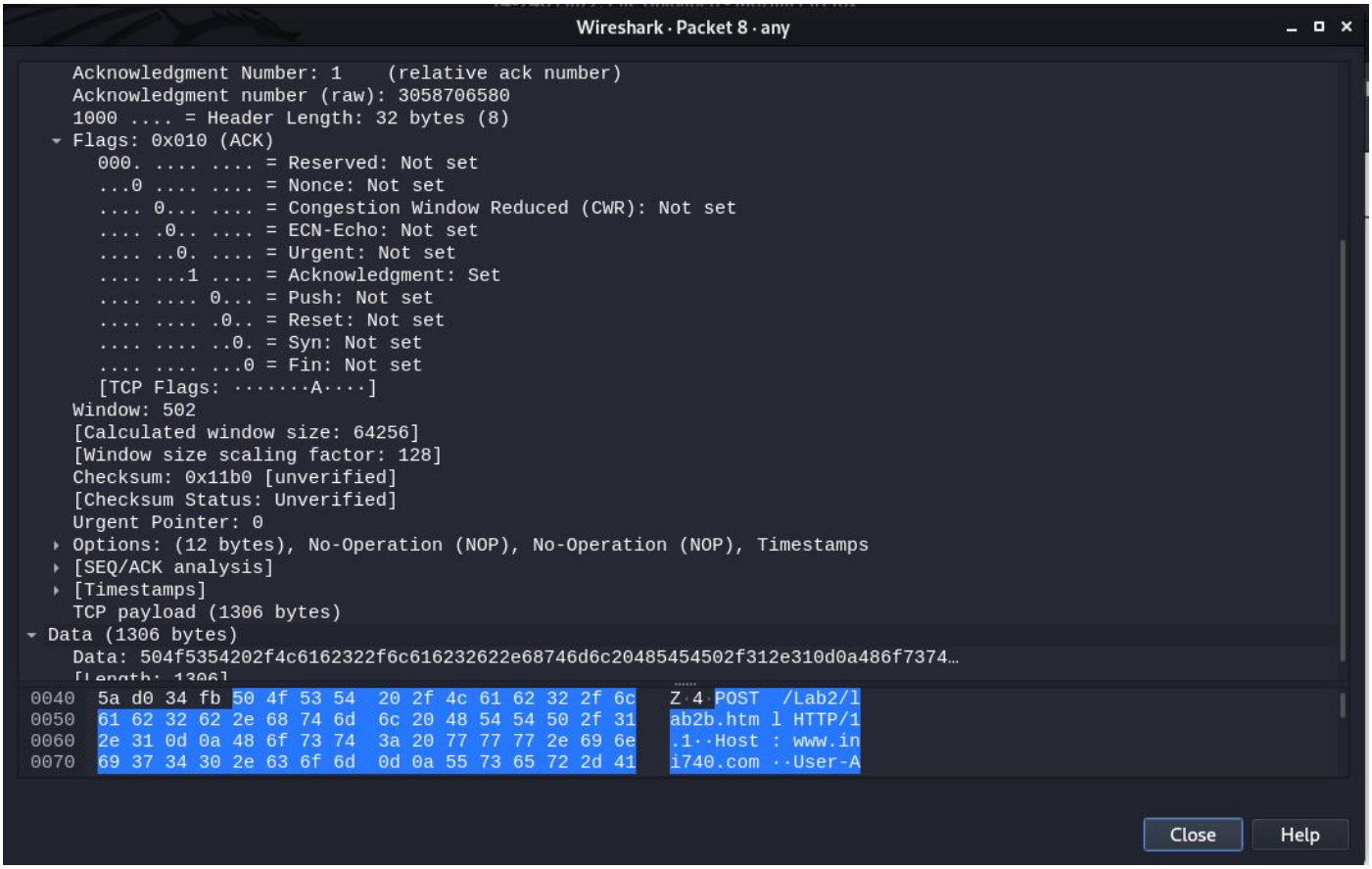
○ The server adds 1 to the initial sequence number of SYN segment form the client computer. For this case, the initial sequence number of SYN segment from the client computer is 0, thus the value

of the ACKnowledgement field in the SYNACK segment is

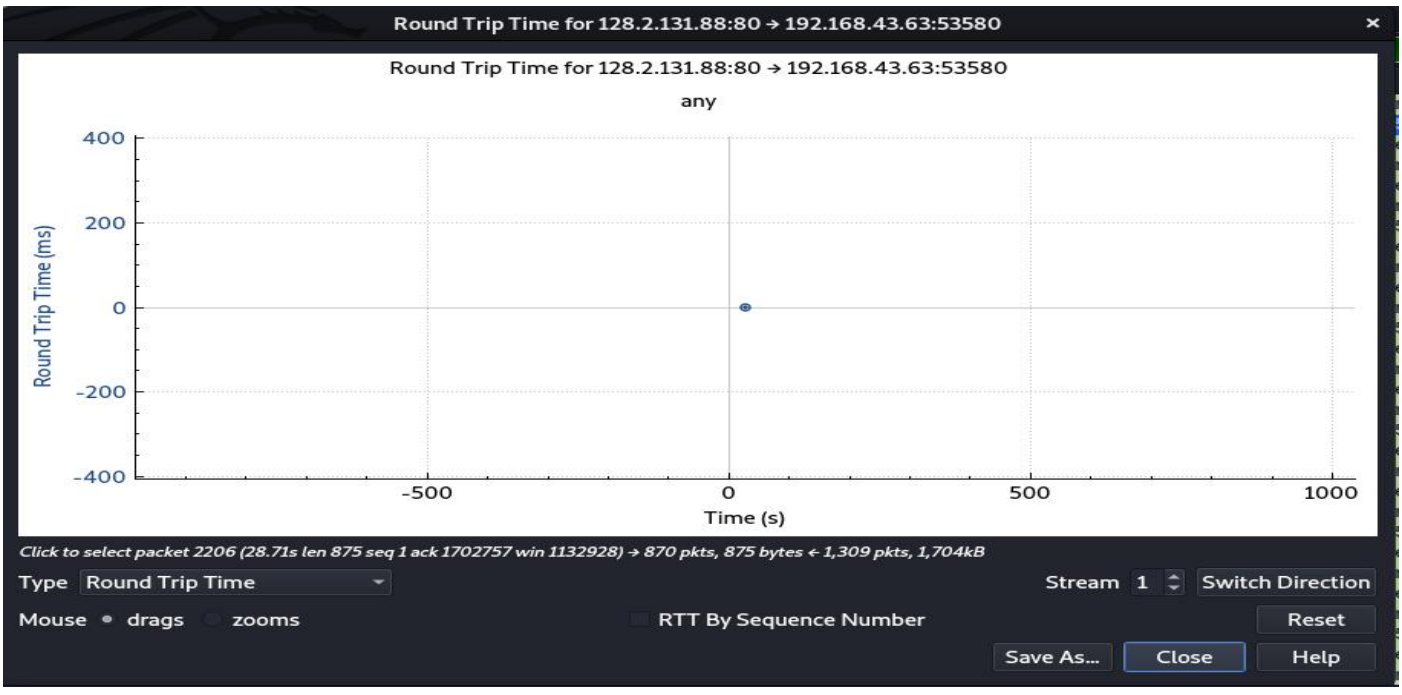
1. What element in the segment identifies it as a SYNACK segment?

○ A segment will be identified as a SYNACK segment if both SYN flag and Acknowledgement in the segment are set to 1.

What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" with in its DATA field.



According to the above figure, segment 379 contains the POST command. It's sequence number is 1. Consider the TCP segment containing the HTTP POST as the first segment in the non-overhead part of the TCP connection. For the segments which follow, put together a table with one row per segment (and columns for whatever data you think is useful)until you have enough segments to calculate four SampleRTT values according to the RTT estimation techniques discussed in class. Calculate what those SampleRTT values are, as well as the EstimatedRTT after each Sample is collected. Discuss this calculation, including what your initial EstimatedRTT was, your choice of parameters, and any segments that weren't used in the calculation. Note: Wireshark has a nice feature that allows you to plot the RTT for each of the TCP segments sent. 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.



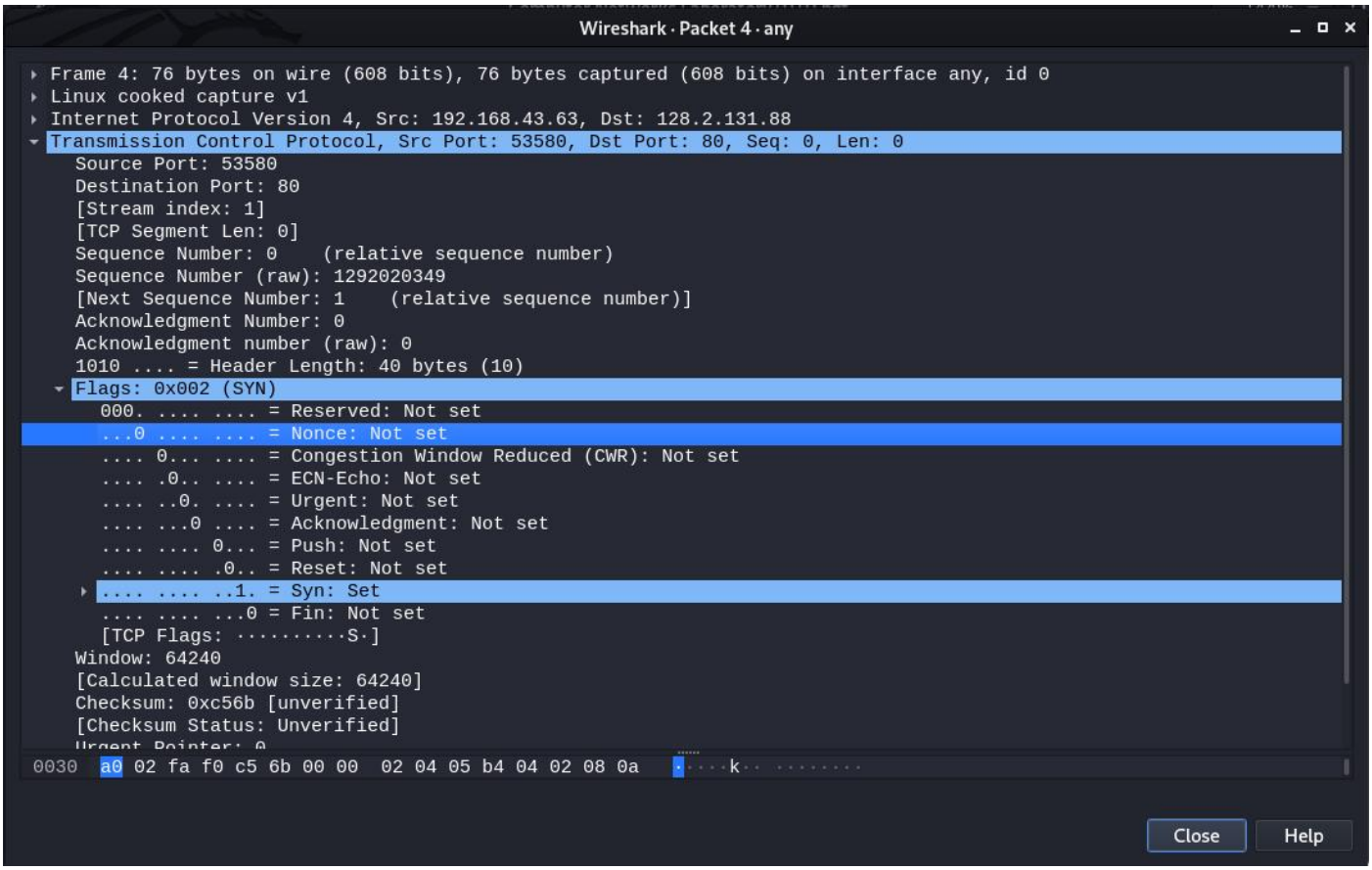
○ As we can see in the above figure, the first 6 segments are numbered as 379,380,381,382,383,384
○ Sequence number of segment 1:1
Sequence number of segment 2:580
Sequence number of segment 3:718
Sequence number of segment 4:2158
Sequence number of segment 5:3598
Sequence number of segment 6:5038

Segment	Sent Time	ACK received time	RTT
1	48.441203	48.844942	6.458
2	48.442227	48.844942	6.457
3	48.444505	48.844943	6.456
4	48.444512	48.844943	6.455
5	48.444516	48.844943	6.455
6	48.444520	48.844944	6.455

EstimatedRTT = 0.875 * EstimatedRTT + 0.125 *sampleRTT

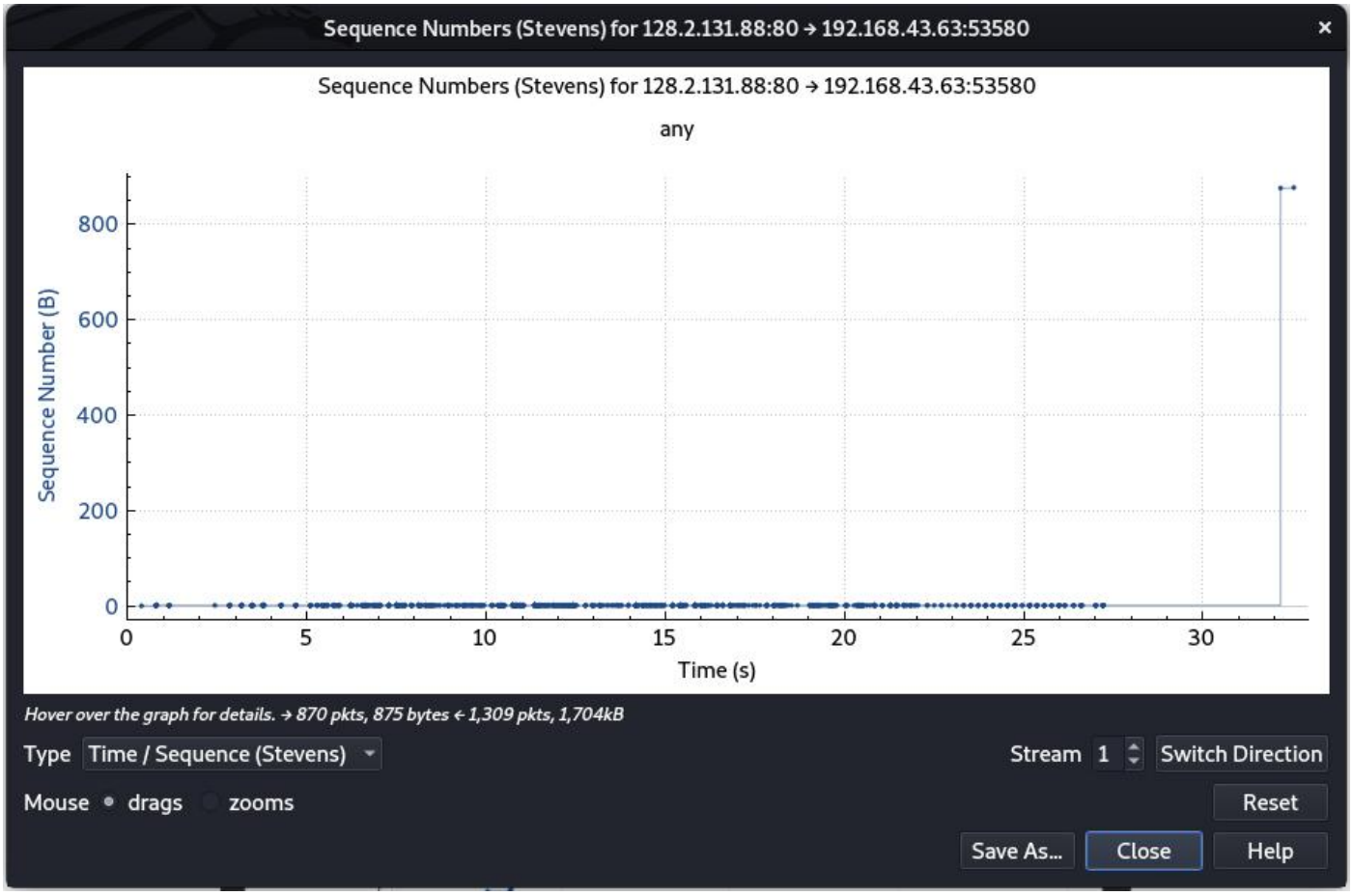
S1: 0.875*0.403739 +0.125*48.844942=6.458889
S2: 0.875*0.402715 +0.125*48.844942=6.457993
S3: 0.875* 0.400438+0.125*48.844943=6.456001
S4: 0.875*0.400431 +0.125*48.844943=6.455995
S5: 0.875*0.400427 +0.125*48.844943=6.455991
S6: 0.875*0.400424 +0.125*48.844944=6.455989

What is the minimum amount of available buffer space advertised at the receiver for the entire trace? Does the lack of receiver buffer space ever throttle the sender?



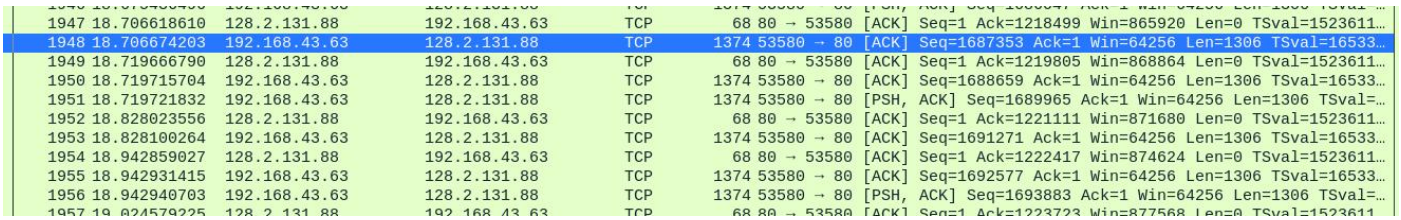
○ The minimum amount of available buffer space advertised at the received for the entire trace is indicated first ACK from the server, its value is 64240 bytes (shown in above figure).

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



As the sequence number-time graph is monotonically increasing from the above graph,we can conclude that no packet is retransmitted How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is delayed ACKing segments?Explain how or why not.

The difference between the acknowledged sequence numbers of two consecutive ACKs indicates the data received by the server between these two ACKs. The receiver is ACKing every other segment. For example, segment of Number. 390 acknowledged data with 718-580=38 bytes.

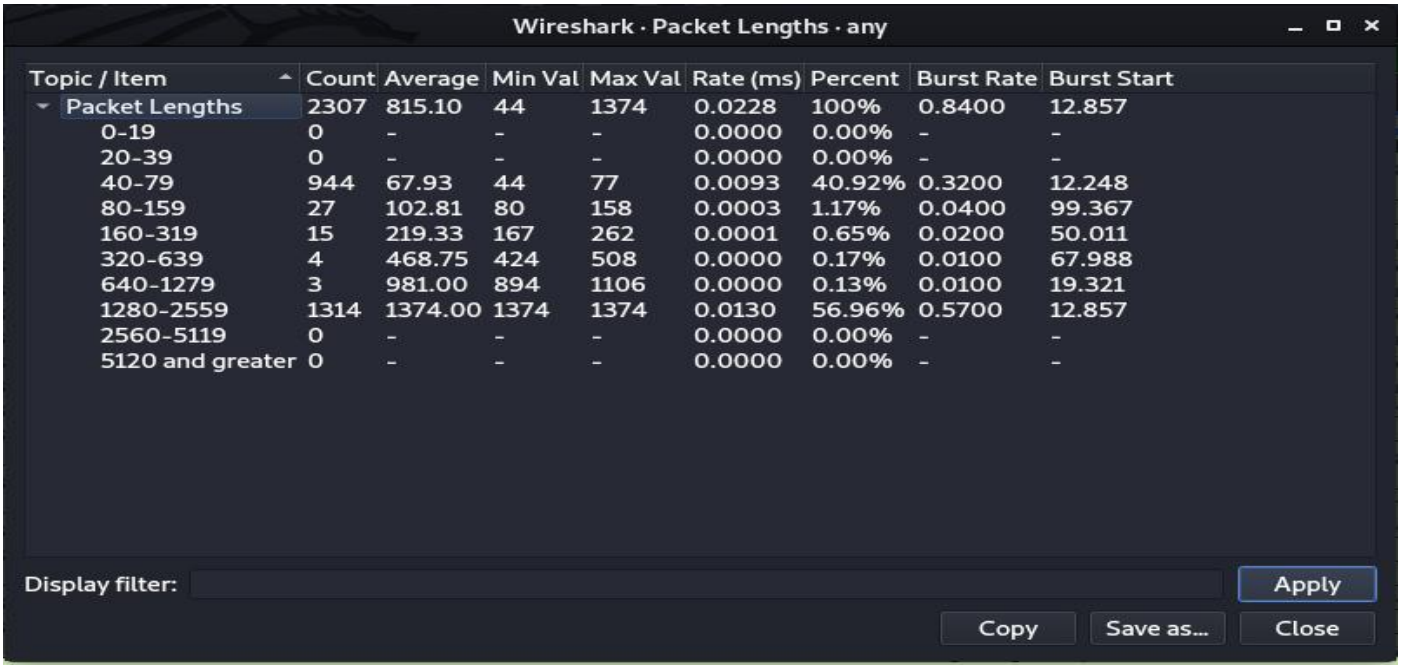


What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

The file on the hard drive is 17,01,981 bytes, and the download time is 51.057952 (last TCP segment) - 48.441203 (last ACK) = 2.616749 second. Therefore, the throughput for the TCP connection is computed as 17,01,981/2.616749=650418.133340 bytes/second.

Step 2c: Statistics

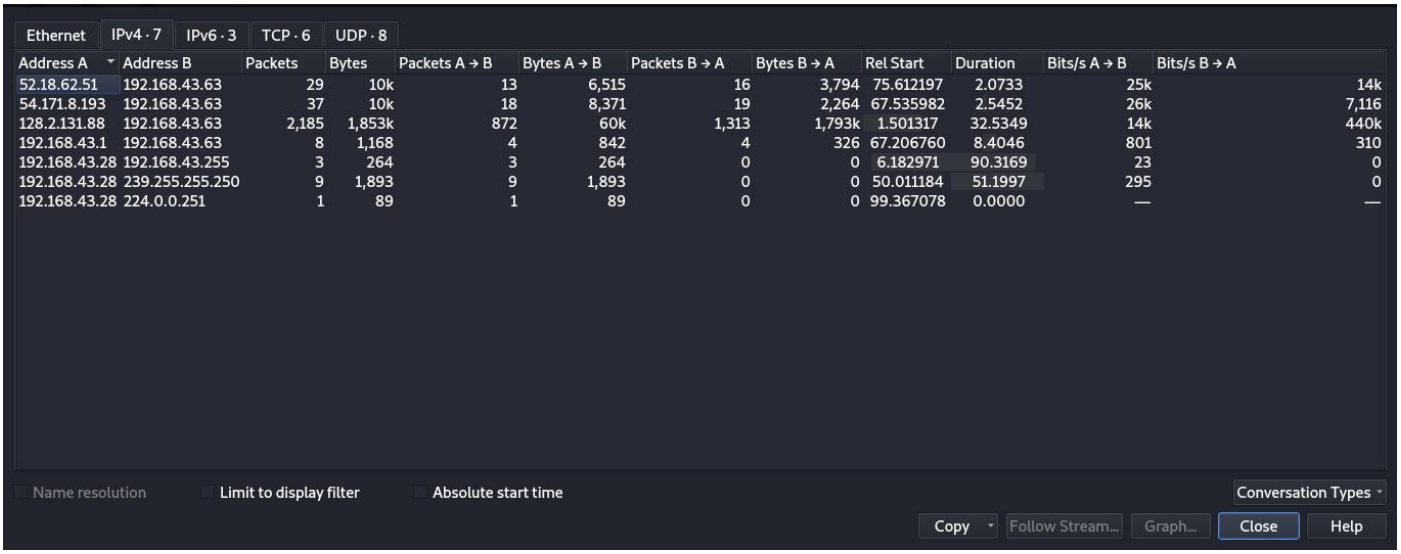
What is the most common TCP packet length range? What is the second most common TCP packet length range? Why is the ratio of TCP packets of length< 40 bytes equal to zero? Describe what actions you took to get answers to these questions from Wireshark.



Most common TCP Packet range is 40-79 (has 1428 packets) Second Most common TCP Packet range is 1280-2559 (has 1185 packets) The header length is 40 bytes in handshaking stage as it consists of 10 headers so as the minimum packet length is 40 bytes without any data in it, the ratio of tcp packets of length <40 is 0.

This information can be obtained by navigating to ‘statistics <packet lenths’ in wireshark menu.

What average throughput did you use in Mbps? How many packets were captured in the packet capture session? How many bytes in total? Explain your methods. Average Throughput=1986545/154.938=12821.547974 Bps=0.102572383792 Mbps 3052 packets have been captured in the packet capture session. 1986545 bytes in total are captured.

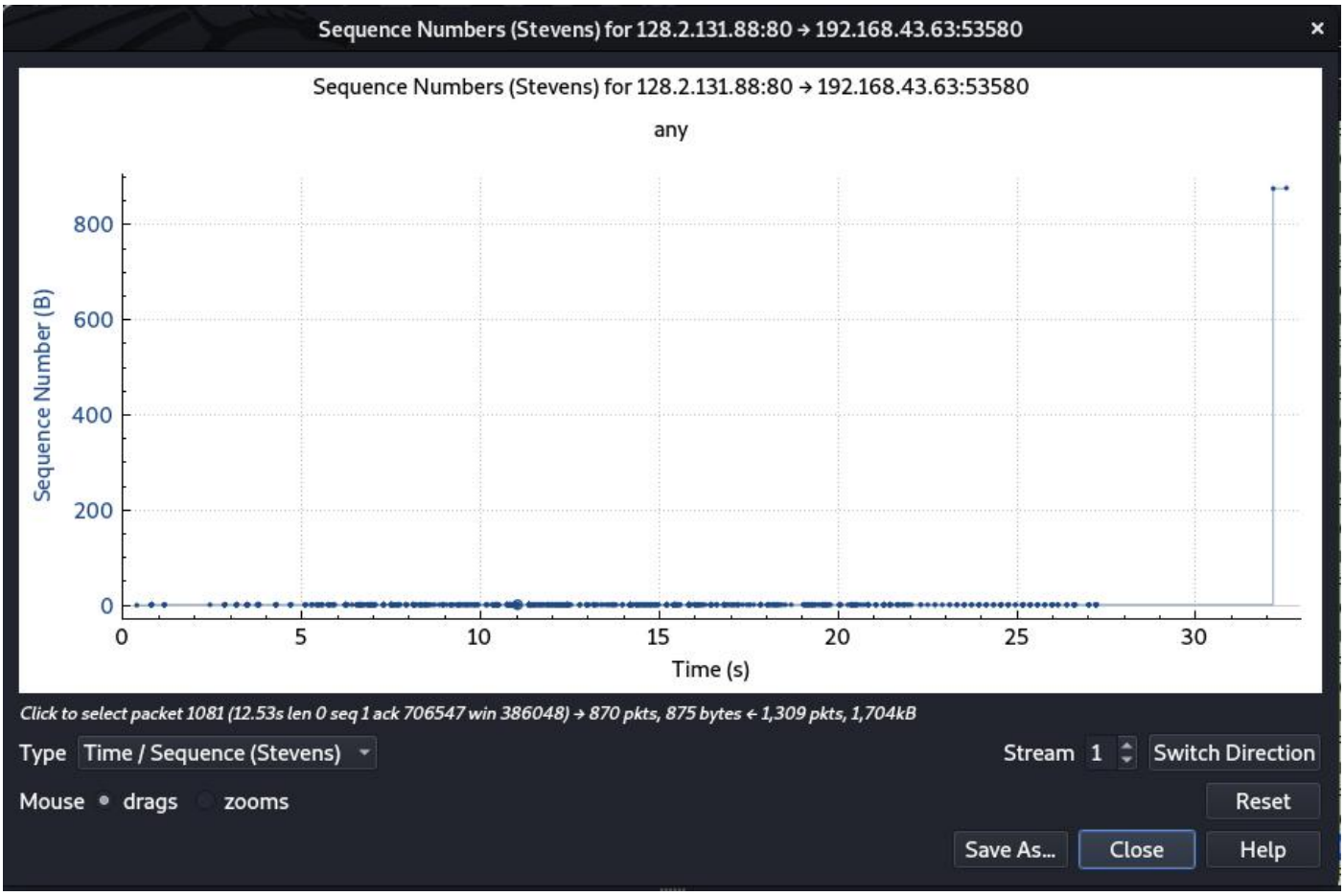


A conversation represents a traffic between two hosts. With which remote host did your localhost converse the most (in bytes)? How many packets were sent from your host? How many packets

were sent from the remote host? With 128.2.131.88 my local host conversed the most(1840k) 1200 packets were sent from my host
872 packets received from remote host.

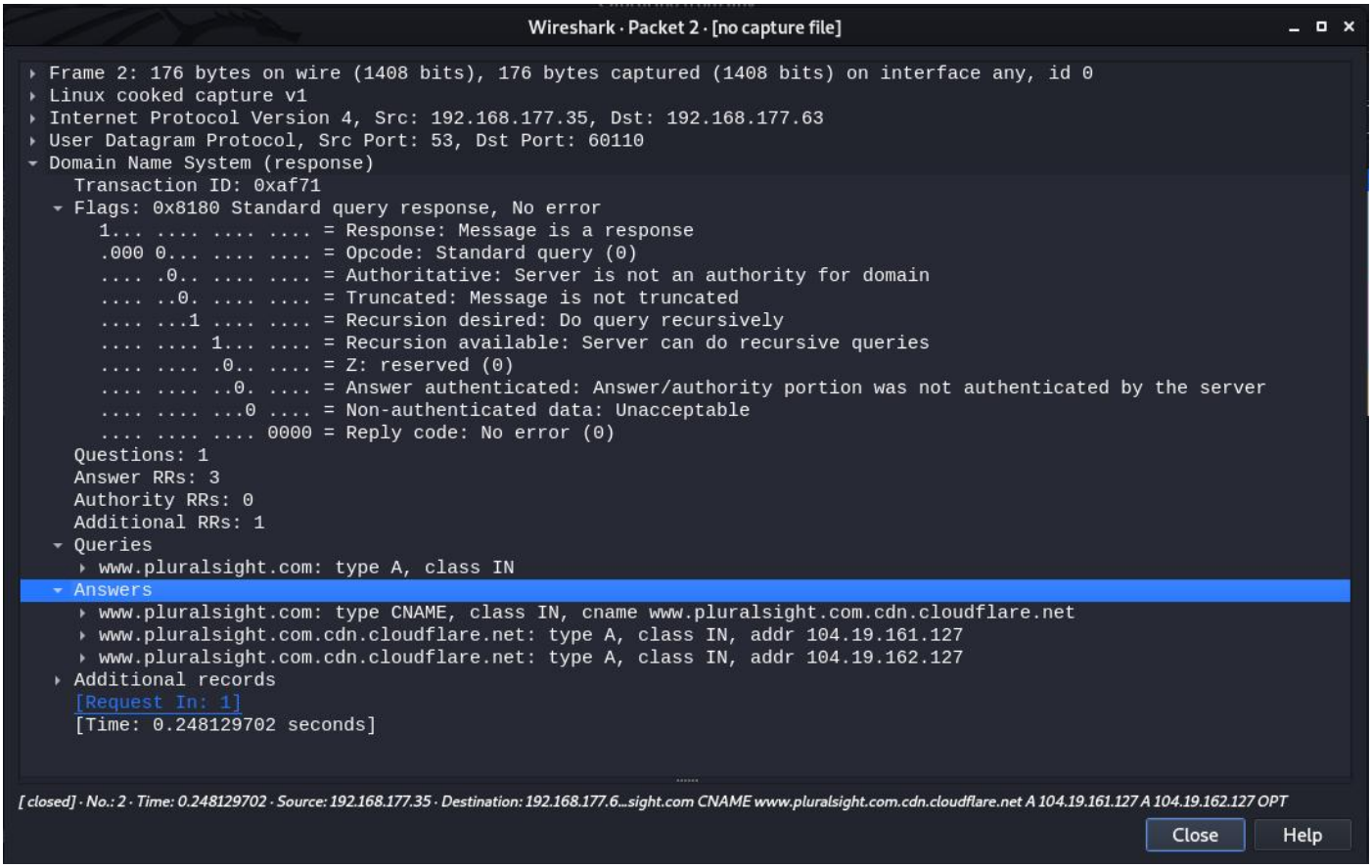
Step 3: Congestion Control

Use the Time-Sequence-Graph(Stevens) plotting tool to view the sequence number versus time plot of segments being sent. Can you identify where TCP's slow start phase begins and ends, and where congestion avoidance takes over? Comment on ways in which the measured data differs from the idealized behavior of TCP that we've studied int he text. Make sure to include a copy of the plot in your report.



Step 4: The Network Layer

Take a look at the IP section of the DNS query (the packet that was generated when you used dig to request the address of www.pluralsight.com). Match up the header fields with the format we discussed in class (don't just look through Wireshark's display -- instead, match the raw bytes with the pictures we saw in lecture, which I've copied on the right).



Most of the fields should matchup and make perfect sense. Verify the Datagram Length, Upper-layer protocol and the IP address fields. Are there any interesting features of the data in the identifier/flags/offset fields?

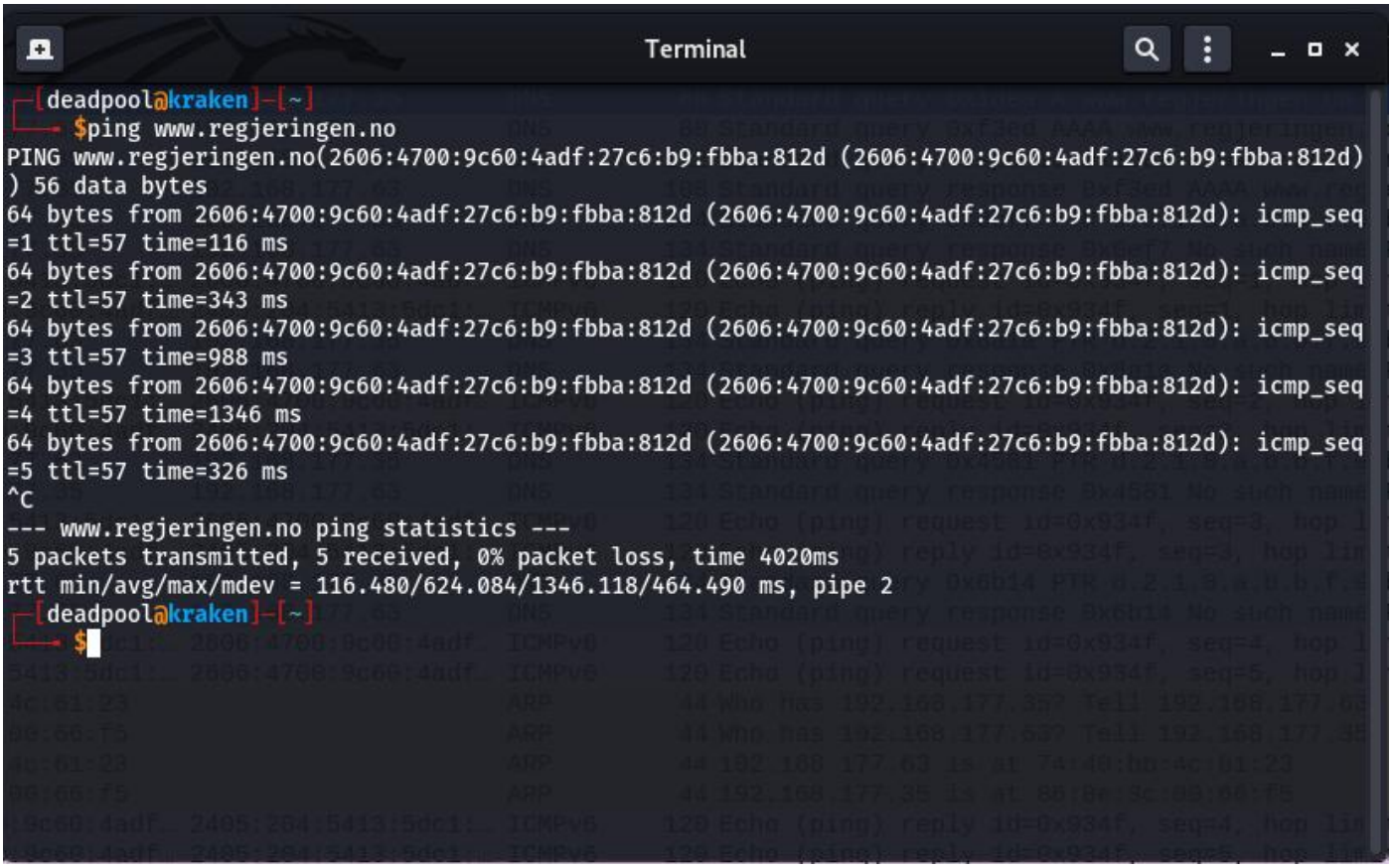
○ Datagram Length=56
○ Upper-Layer protocol-IP
○ IP ADDRESS fields: source-10.20.204.75 destination-8.8.8.8

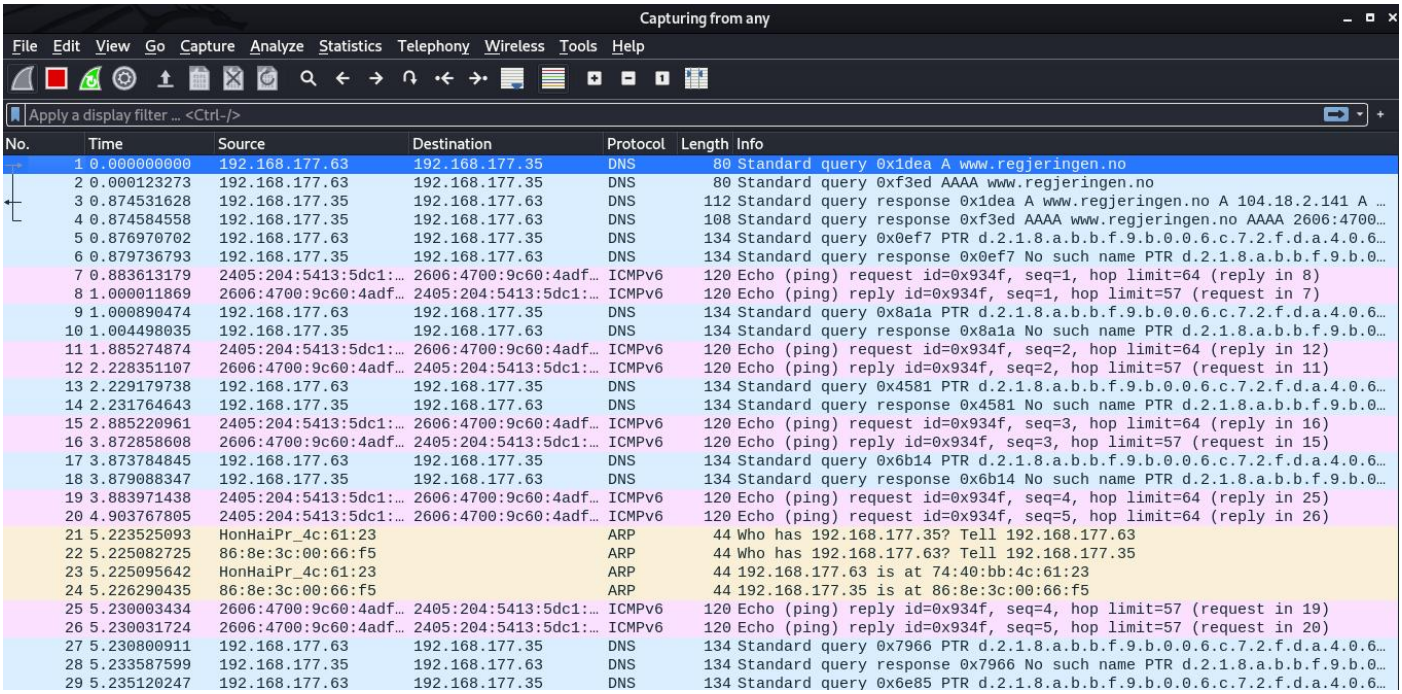
In class, we discussed the TTL field and determined that we didn't know a good way to set this. What does your OS set this field to? ○ 54 ○ OS:MAC OS Monterey ○ OS VERSION:12.2(21D49)

Step 5: ICMP

33) Ina terminal window, execute the traceroute utility to trace from your computer to www.cmuj.jpor www.regjeringen.no or some other far-away destination(like we did in our class). If you are having trouble with the weird traceroutes, try this from anon-campus location(your home, a restaurant, etc).

Do whatever you can to get a traceroute consisting of about a dozen steps.





Used ping as traceroute im my system is not working for some reason

35) What are the transmitted
segments like? Describe the important features of the segments you observe. In particular, examine the destination port field. What characteristics do you observe about this port number and why would it be chosen so?
○ Ping doesn't use a port number as traceroute uses port number 33434
○ For every hop port number increases by 1 36)
What about the return packets? What are the values of the various header fields?

○ Code:0
○ Type:0
○ Identifier:44969 (BE)
○ Identifier:43439 (LE)
○ Sequence number:1 (BE)
○ Sequence Number:256 (LE)

37) The ICMP packets carry some interesting data. What is it? Can you show the relationship to the sent packets?

○ It contains timestamp

38) Lab1 asserted that ping operates in a similar fashion to traceroute. Use Wireshark to show the degree to which this is true. What differences and similarities are there between the network traffic of ping versus traceroute?

○ Did for ping