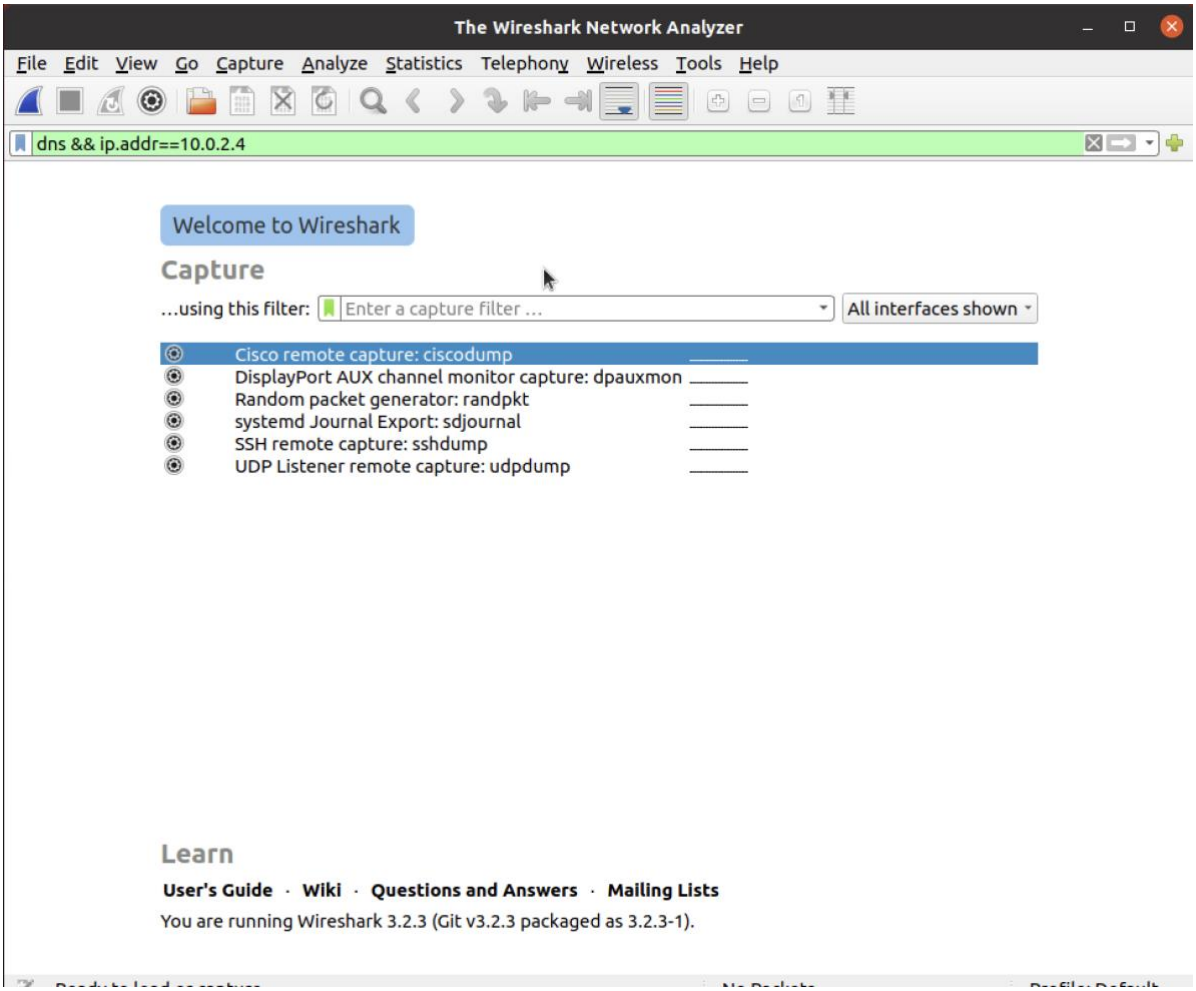
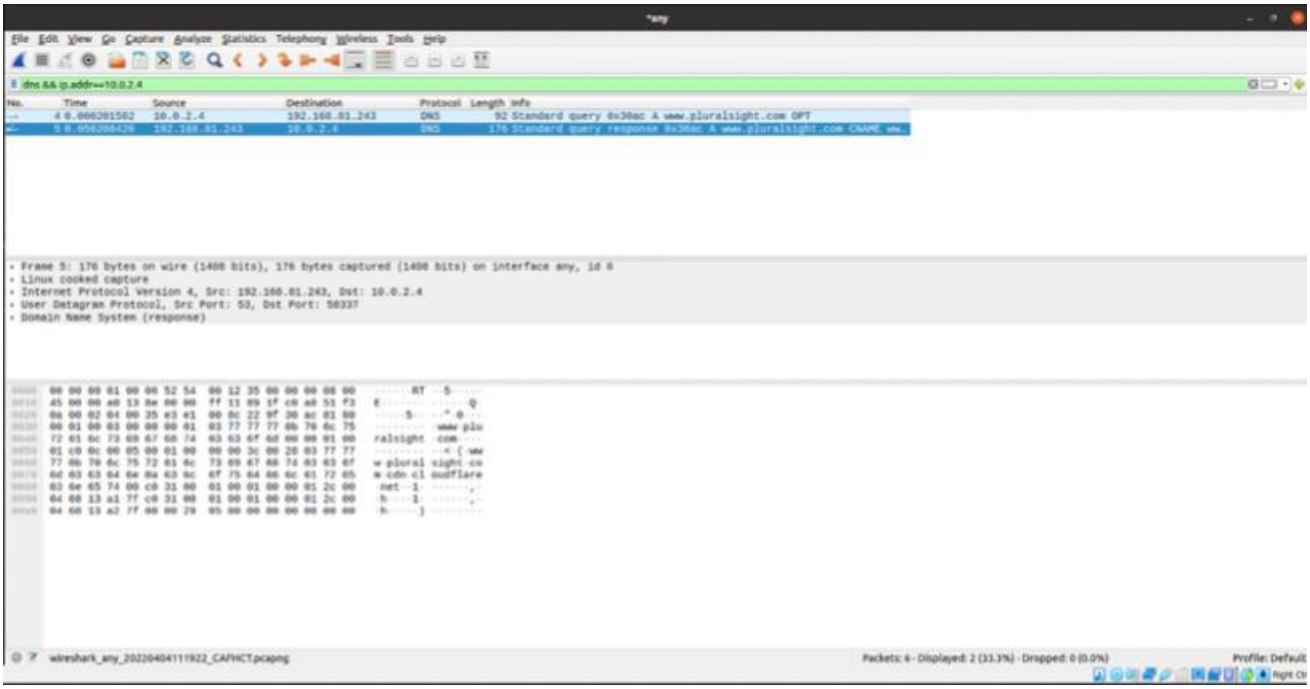
Lab 5 – Understanding Transport and Network Layer using Wireshark

Name: Vanshika Goel	SRN: PES1UG20CS484	Section: H	Roll No: 40

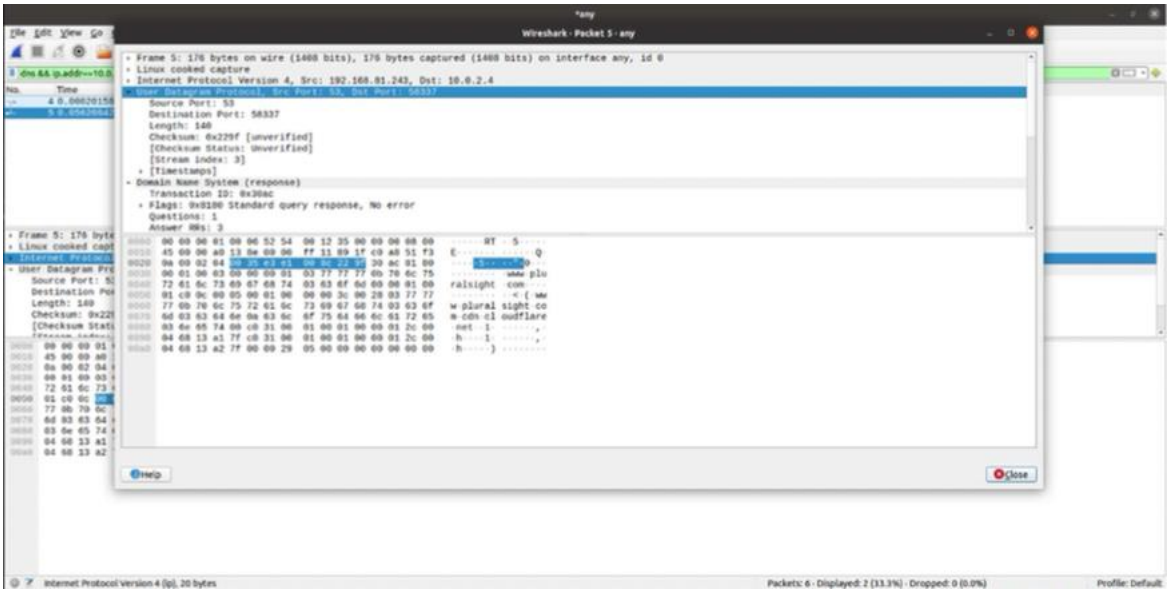
Step 1: UDP and DNS





Q) 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.

A) Checksum can be calculated.



Q) Were your predictions correct?

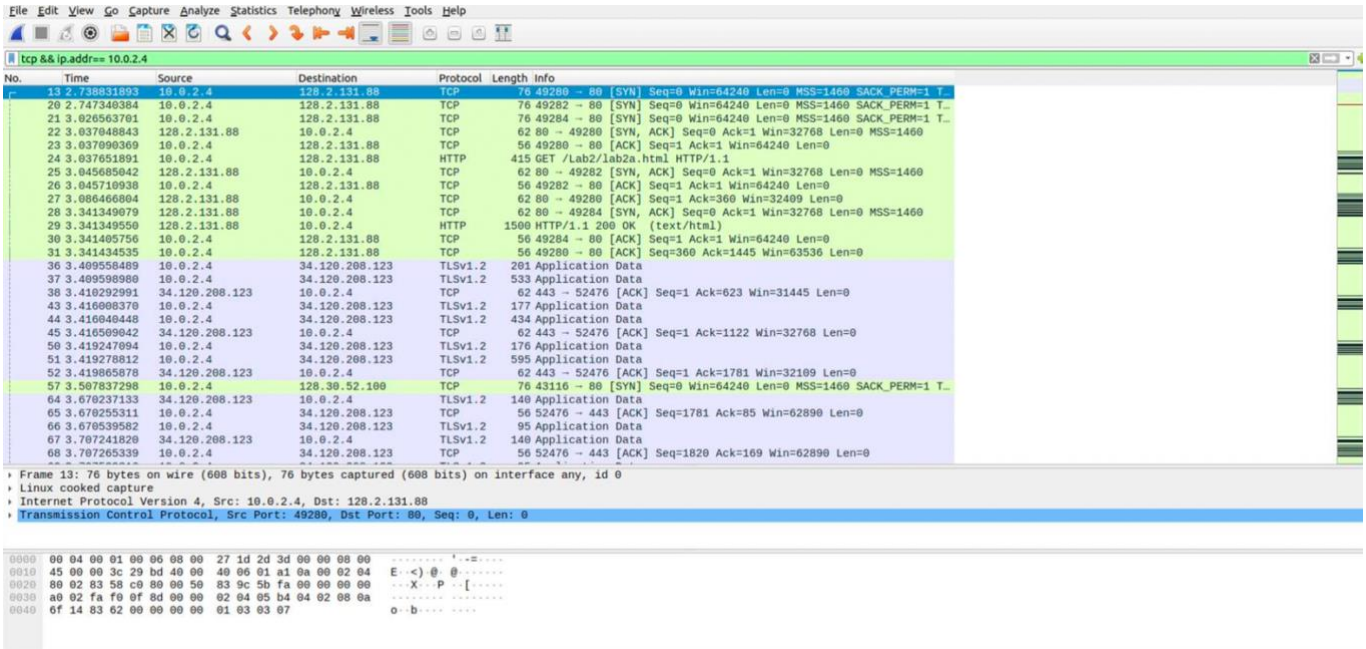
A)Yes, They were correct.

Q) 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?

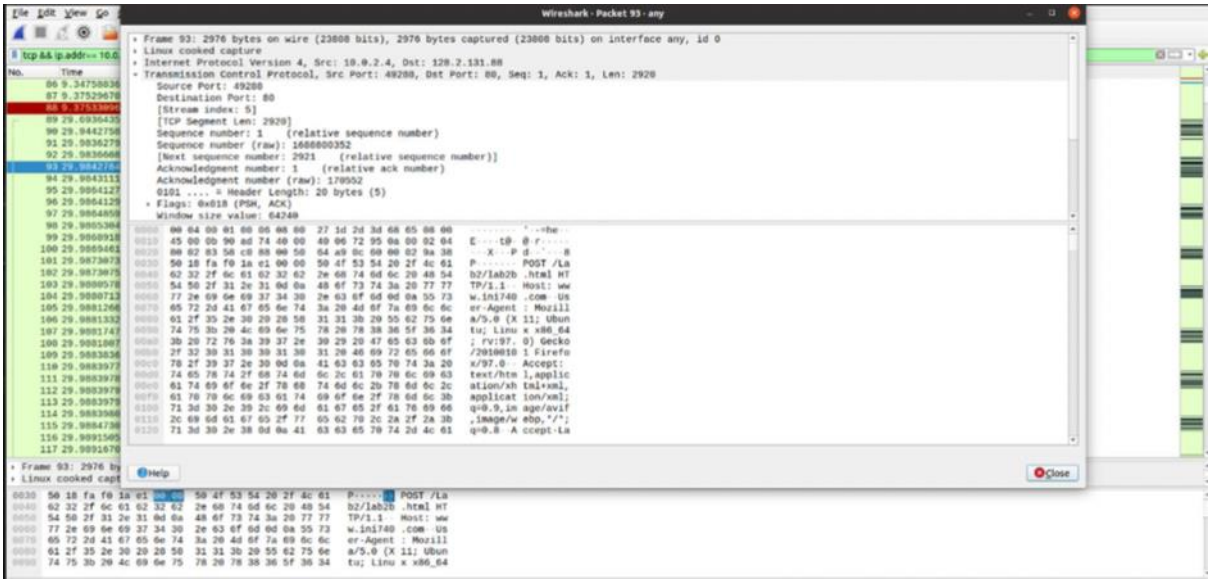
A)Checksum: 0x229f [unverified]

Yes, the reason is that Wireshark is very often used to capture the network frames of the same PC that is running Wireshark. This usually results in the checksums of outgoing frames being incorrect since they are only calculated for transmission by the network card after they were already recorded by Wireshark. To avoid constant "checksum error" messages it was decided to have the checksum validation disabled by default.

Step 2: TCP



Q) What is the IP address and TCP port number used by your computer (client) to transfer the file? What is the IP address of the server? On what port number is it sending and receiving TCP segments for this transfer of the file?

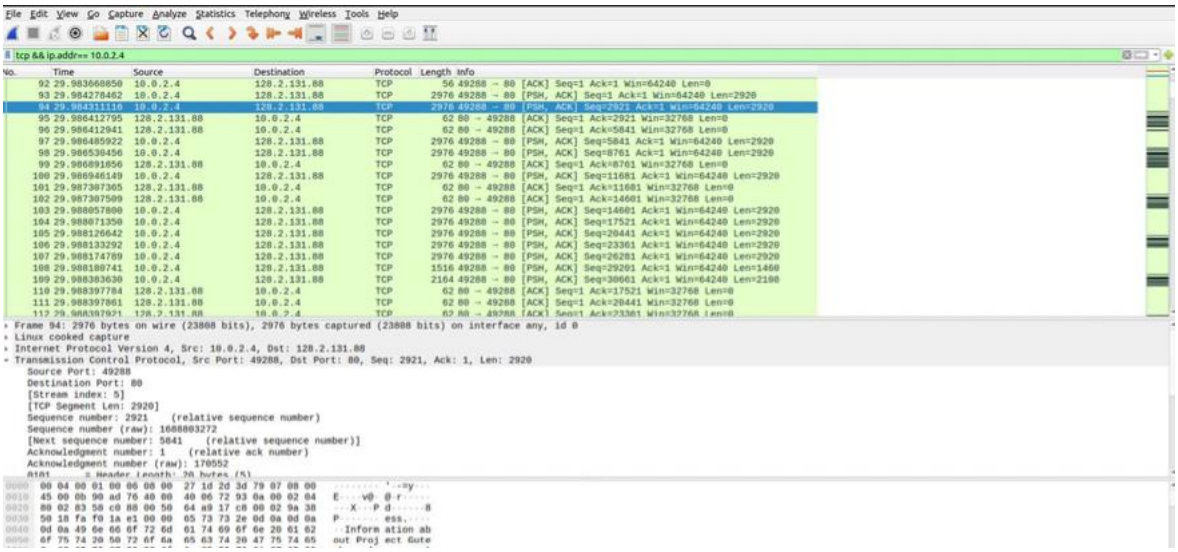


Source:

IP: 10.0.2.4 Port: 49288

Destination:

IP:
Port: 80

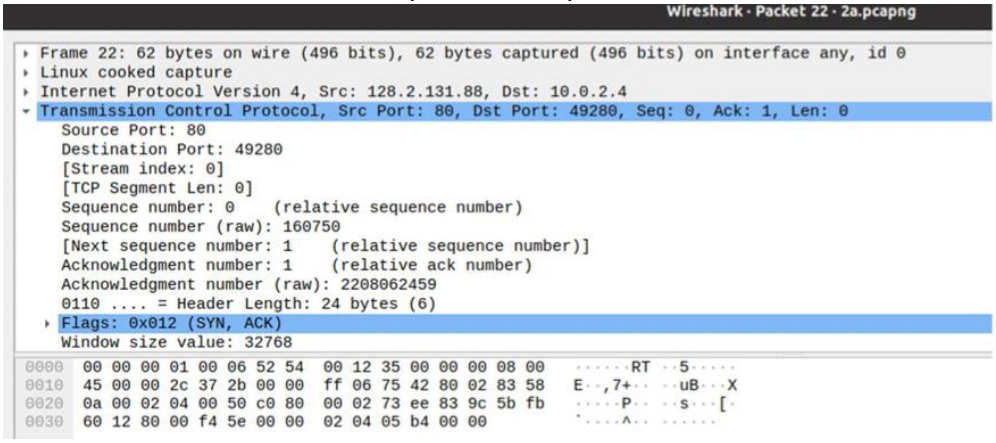


Step 2b: TCP Basics

Answer the following questions for the TCP segments:
Q) What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection? What element of the segment identifies it as a SYN segment? Wireshark uses relative sequence numbers by default. Can you obtain absolute sequence numbers instead? How? You can use relative sequence numbers to answer the remaining questions.

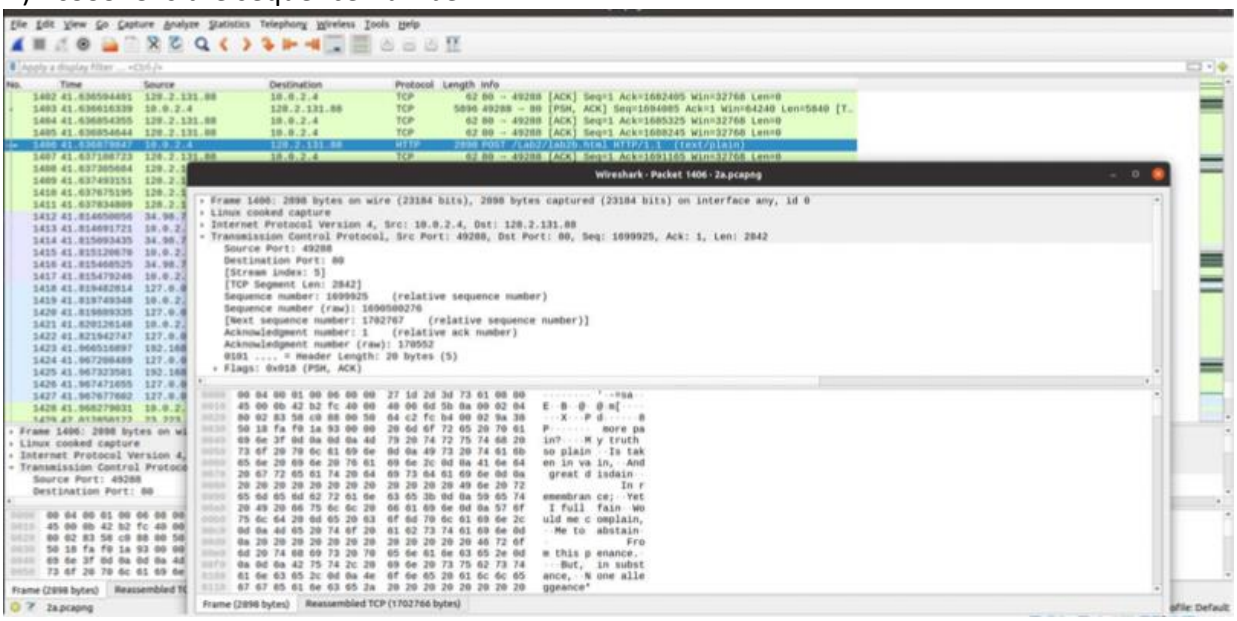
A)The sequence number is 0 to initiate the TCP connection.

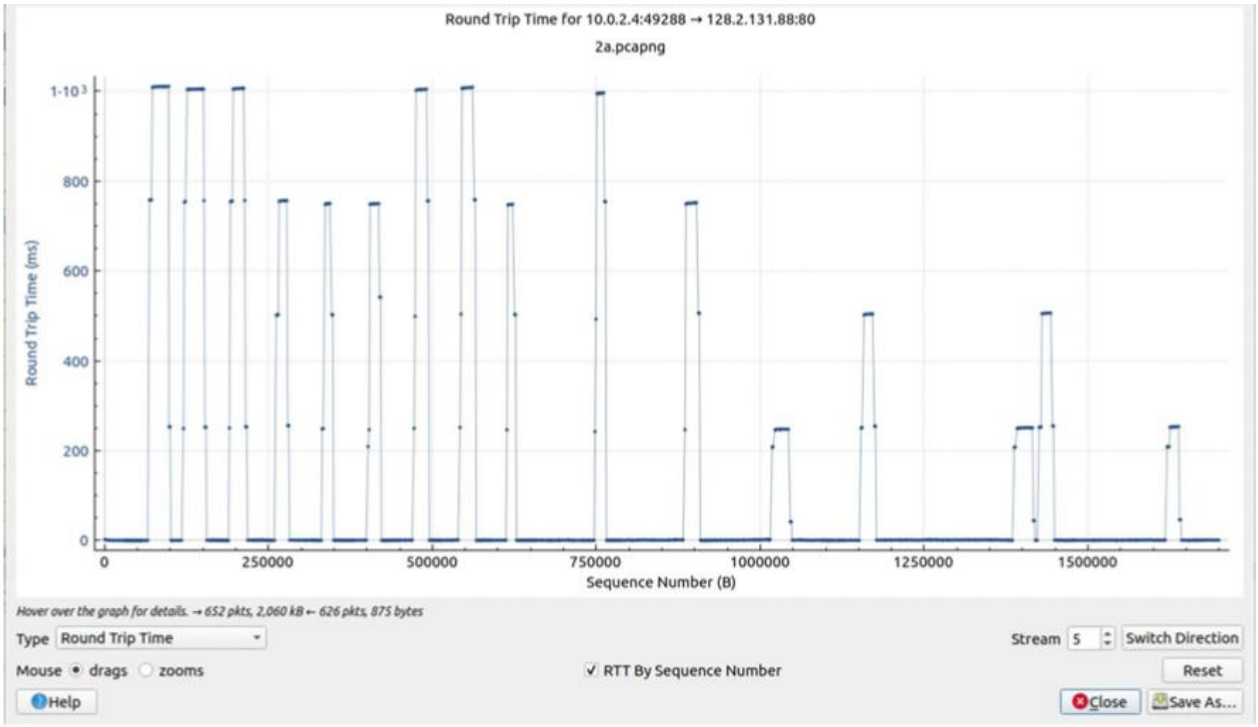
Q)What is the sequence number of the SYNACK segment sent by the server in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did the server determine that value? What element in the segment identifies it as a SYNACK segment?
A) The sequence number is still 0. The value of the acknowledgement field in SYNACK segment is 1. This value is determined based on the previous sequence number received.



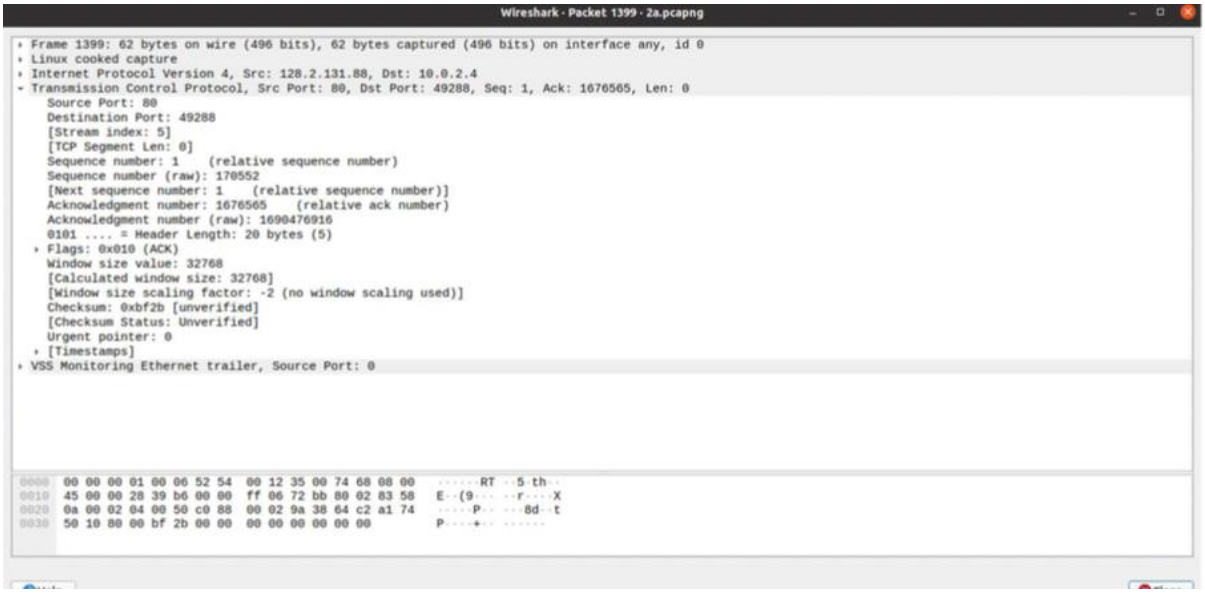
Q) What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.

A) 1699925 is the sequence number.



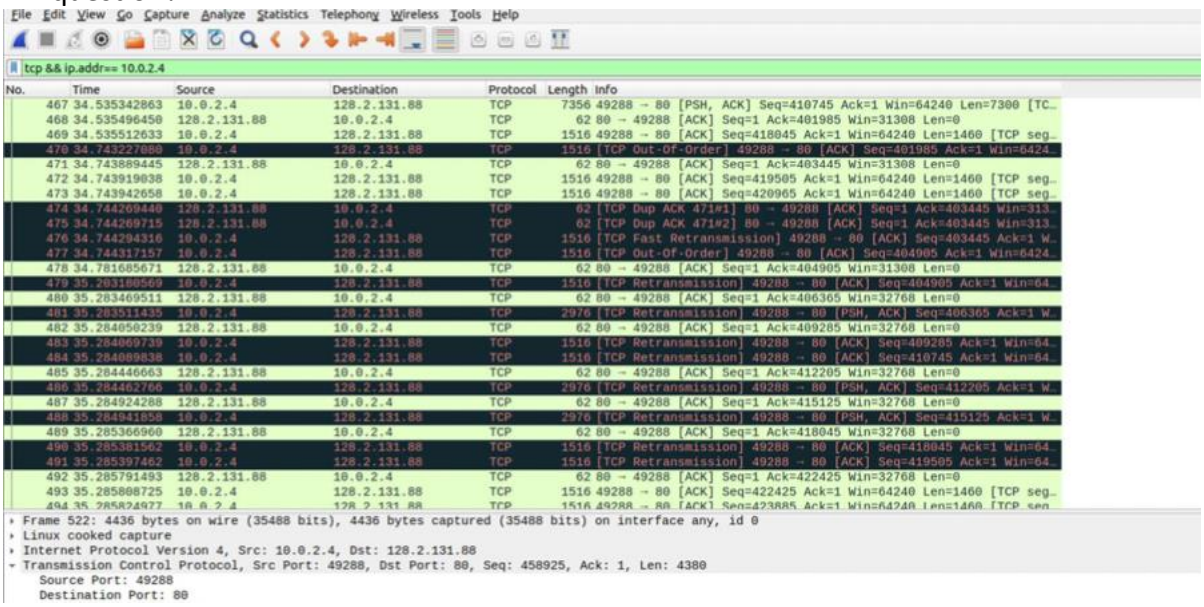


Q) What is the minimum amount of available buffer space advertised at the receiver for the entire trace? Does the lack of receiver buffer space ever throttle the sender?



A)Buffer space available: 32768 Yes, it does throttle the sender.

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

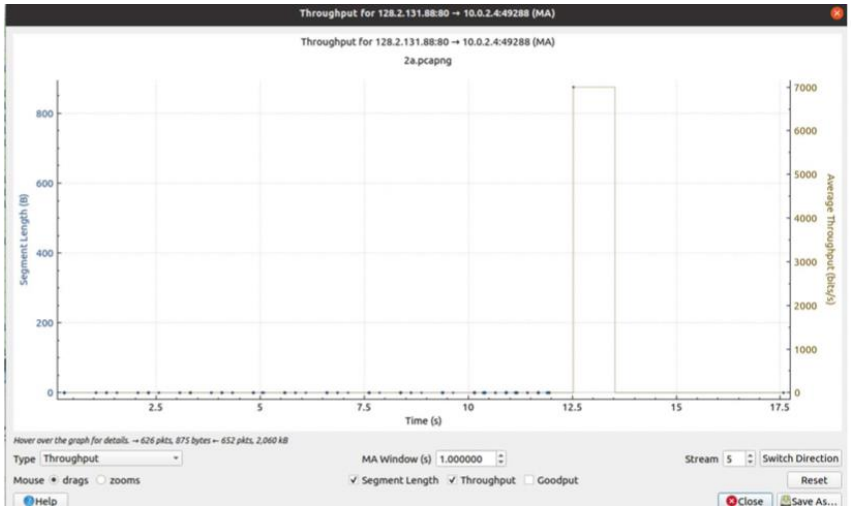


There is a Fast TCP re-transmisson and TCP Dup ACK.

Q)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.

A) There is a TCP payload of 4380 bytes and window size is 64240.
The ‘keep-alive’ status helps identify delayed ACKing segments.

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



Step 2c: Statistics

Q)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.

A) Average packet length is 1467.09

Q)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.

Details

File

Name:	/home/vk27/Desktop/PES1UG20CS500/2a.pcapng
Length:	2,239 kB
Hash (SHA256):	aad3e6b5dc85e959a9c18d0d56908b3e9b91a3f2730ddefc752fa55d64df5a92
Hash (RIPEMD160):	5f35b19caf1a34f2bcc29461a8eb320120e91490
Hash (SHA1):	5fae27d1bb444daf6bda4b84facf37d2d15baee9
Format:	Wireshark/... - pcapng
Encapsulation:	Linux cooked-mode capture

Time

First packet:	2022-04-04 11:42:04
Last packet:	2022-04-04 11:42:56
Elapsed:	00:00:52

Capture

Hardware:	11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz (with SSE4.2)
OS:	Linux 5.13.0-30-generic
Application:	Dumpcap (Wireshark) 3.2.3 (Git v3.2.3 packaged as 3.2.3-1)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit
any	0 (0.0%)	none	Linux cooked-mode capture	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	1493	1419 (95.0%)	—
Time span, s	52.228	49.489	—
Average pps	28.6	28.7	—
Average packet size, B	1467	1536	—
Bytes	2190372	2180037 (99.5%)	0
Average bytes/s	41 k	44 k	—
Average bits/s	335 k	352 k	—

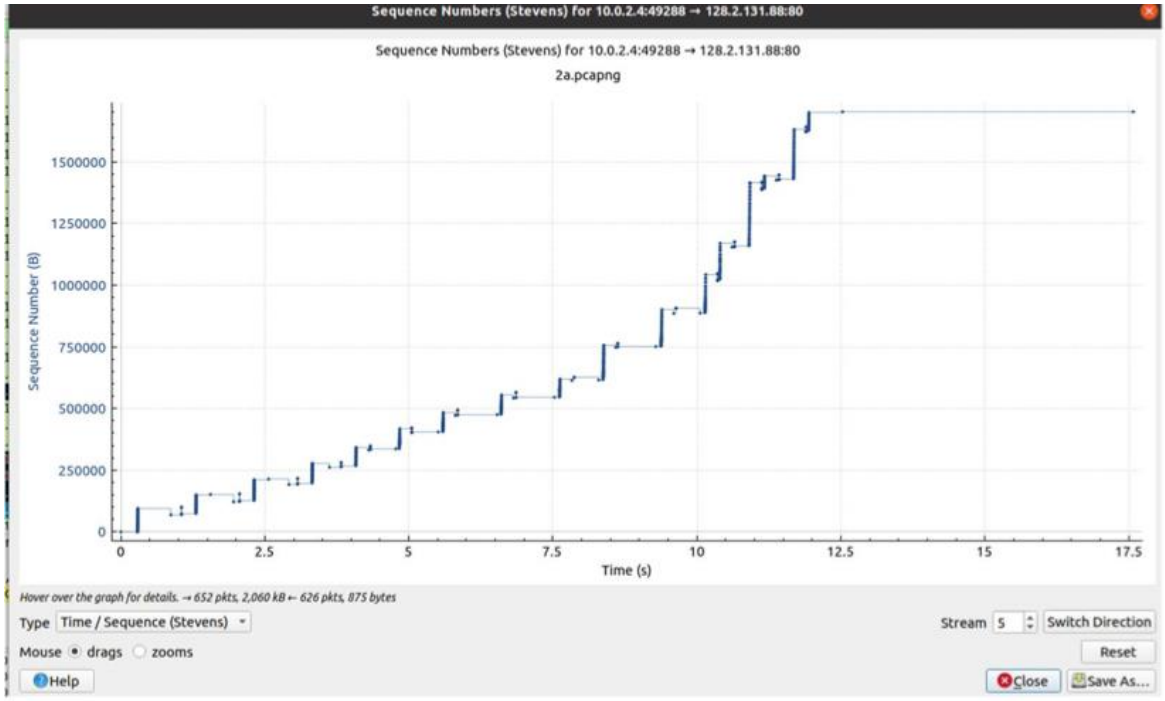
Capture file comments

Help Refresh Copy To Clipboard Close Save Comments

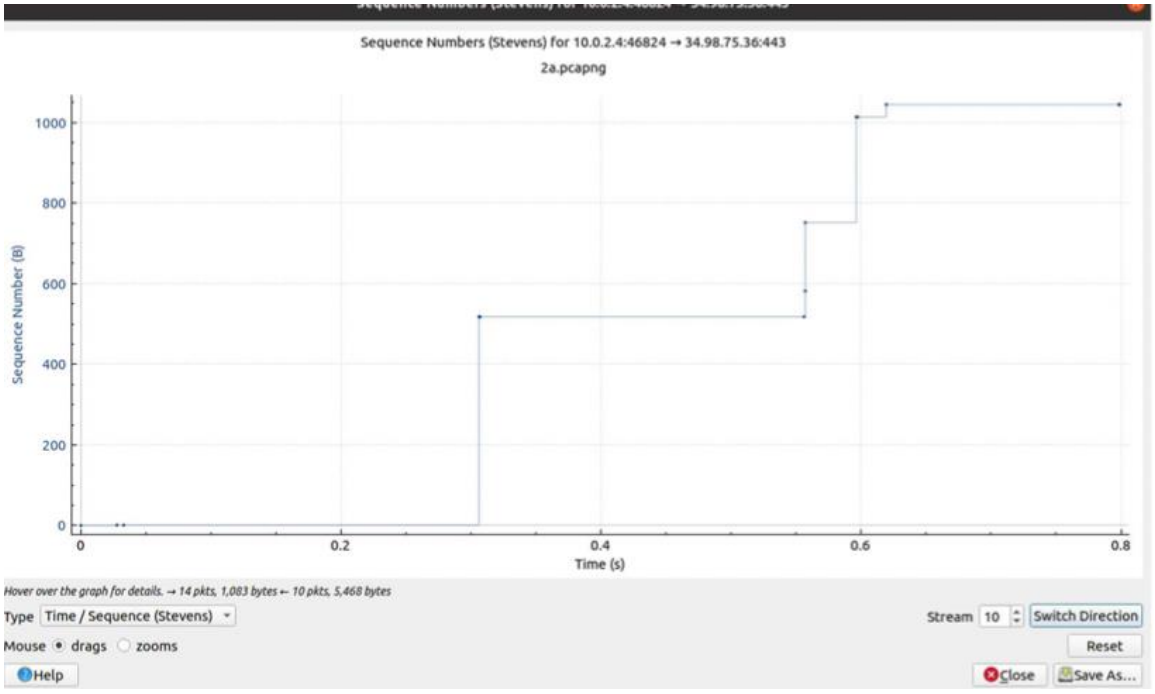
Q) A conversation represents a traffic between two hosts. With which remote host did your local host converse the most (in bytes)? How many packets were sent from your host? How many packets were sent from the remote host?

We converse the most with port 443 of server with IP: 128.2.131.88 (1309 packets = 2140K bytes)

Step 3: Congestion Control



Client -> Server

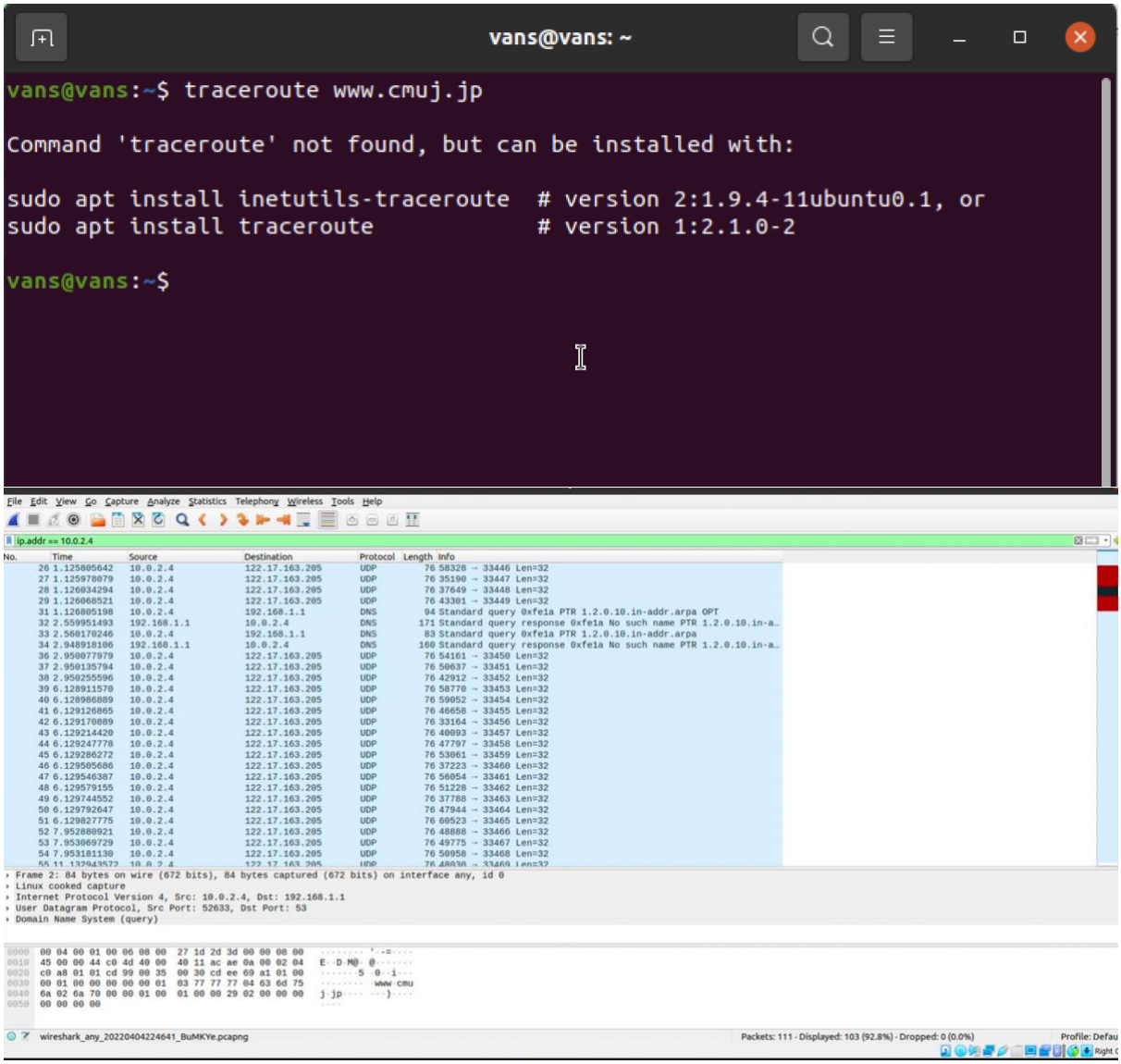


Server -> Client

Step 4: The Network Layer

TTL is set to 64 by OS (default).

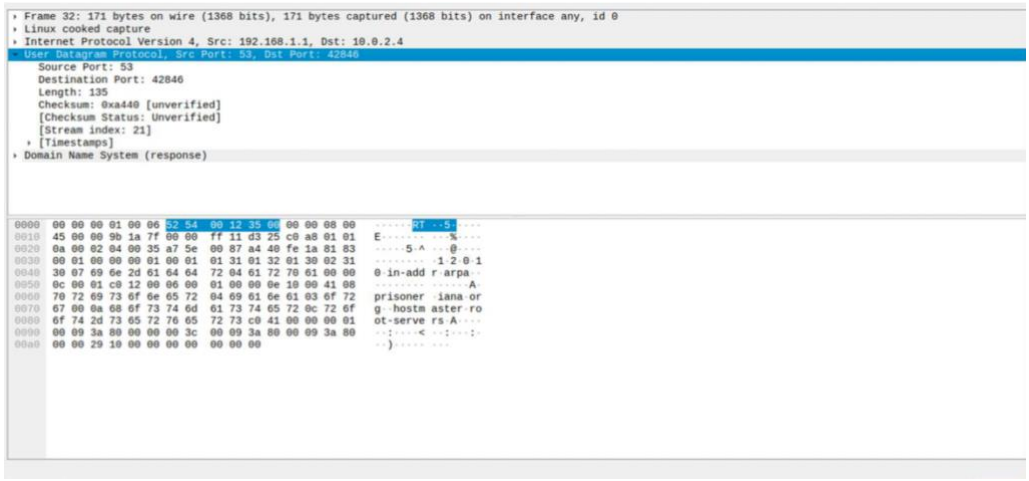
Step 5: ICMP



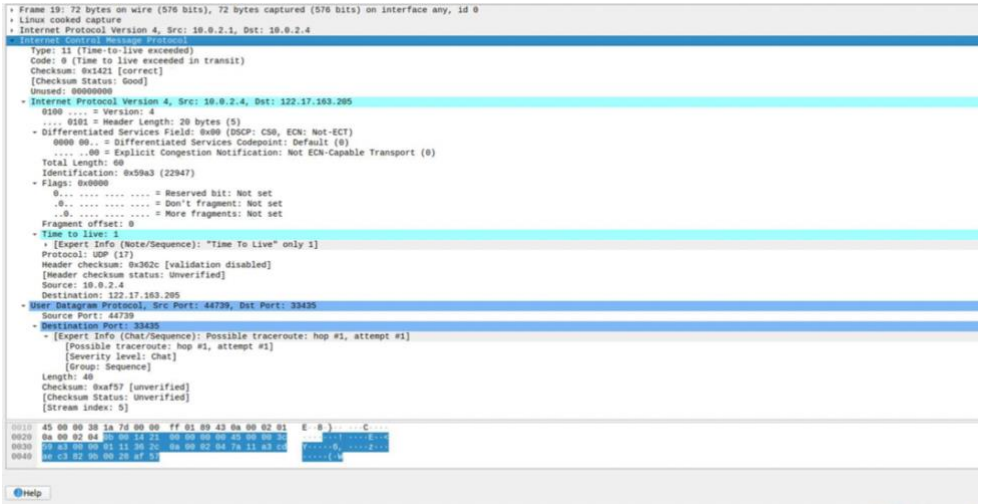
Q)What are the transmitted segments like? Describe the important features of the segments you observe. In particular, examine the destination port field. What characteristics do you observe about this port number and why would it be chosen so?

A) The destination port number chosen is 53, as it can transmit DNS queries in UDP segment.

Q)What about the return packets? What are the values of the various header fields?



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



R)

S) 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?

A) Both ‘ping’ & ‘traceroute’ are used to check the network connectivity issues.