PES2UG20CS389_Vishwa Mehul Mehta_Week6

by Vishwa Mehta

Submission date: 11-Apr-2022 09:02AM (UTC+0530)
Submission ID: 1807349856
File name: PES2UG20CS389_Vishwa_Mehul_Mehta_Week6.pdf (3.95M)
Word count: 677
Character count: 3194

COMPUTER NETWORKS LAB

Understanding Transport and Network Layer using Wireshark
WEEK 6

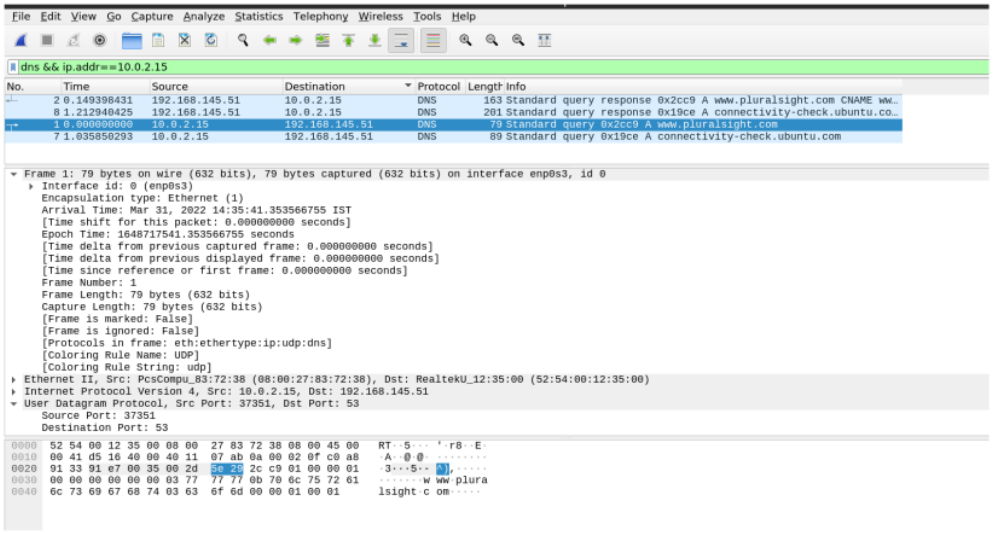
NAME: VISHWA MEHUL MEHTA
SRN: PES2UG20CS389
SECTION: F
DATE: 09/04/2022

I. UDP and DNS:

1.

```
vishwa@vishwa-VirtualBox:~/Documents$ dig www.pluralsight.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.pluralsight.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58981
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.pluralsight.com.           IN      A

;; ANSWER SECTION:
www.pluralsight.com.    60      IN      CNAME   www.pluralsight.com.cdn.cloudflare.ne
t.
www.pluralsight.com.cdn.cloudflare.net. 299 IN A 104.19.162.127
www.pluralsight.com.cdn.cloudflare.net. 299 IN A 104.19.161.127

;; Query time: 43 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sun Apr 03 16:12:14 IST 2022
;; MSG SIZE  rcvd: 132
```

2.



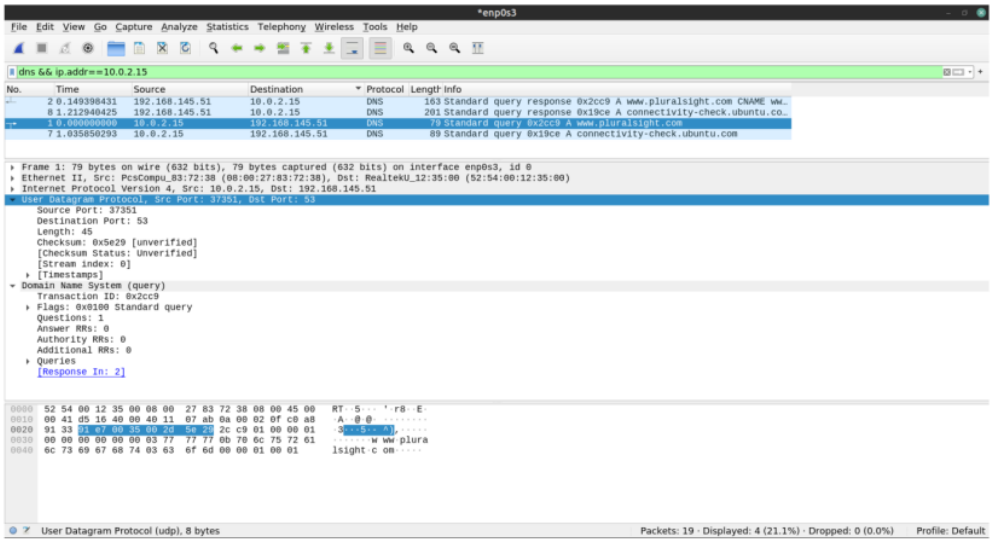
3.

The UDP segment headers expected are:

Source Port Number – 2 bytes, Destination Port Number – 2 bytes, Length – 2 bytes, Checksum – 2 bytes and rest are payload.

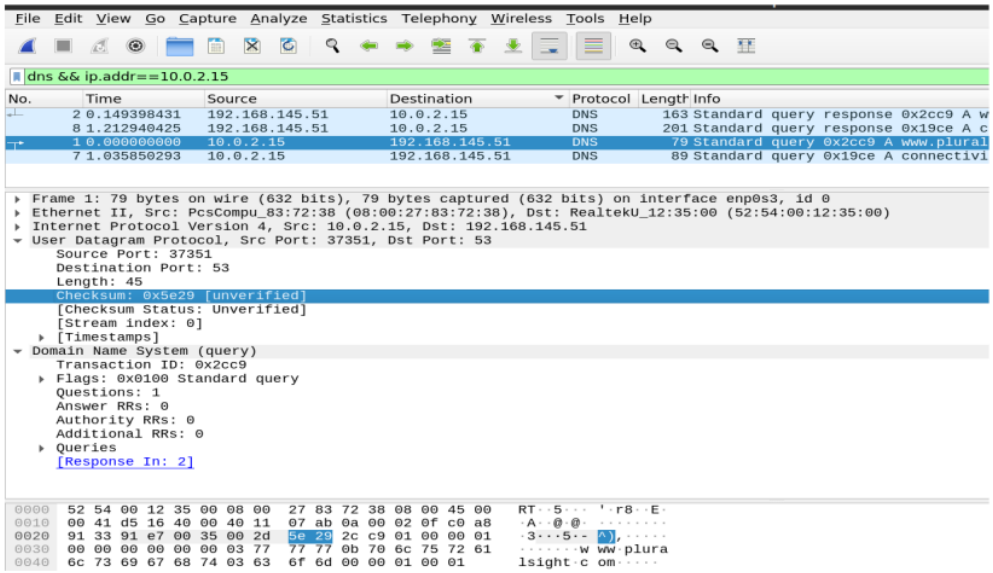
4.

As per the above mentioned predictions the headers in the UDP segment are as shown:



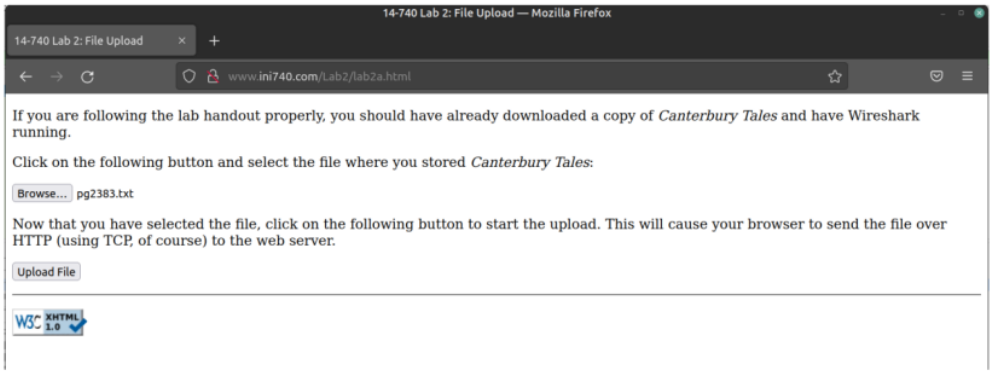
5.

The UDP checksum covers UDP header and the UDP data.



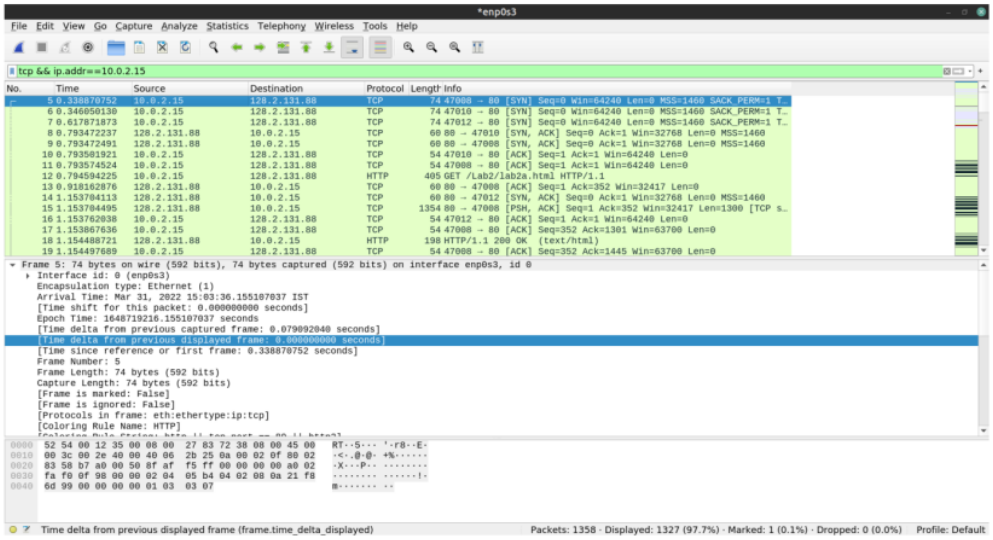
II. TCP:

9.

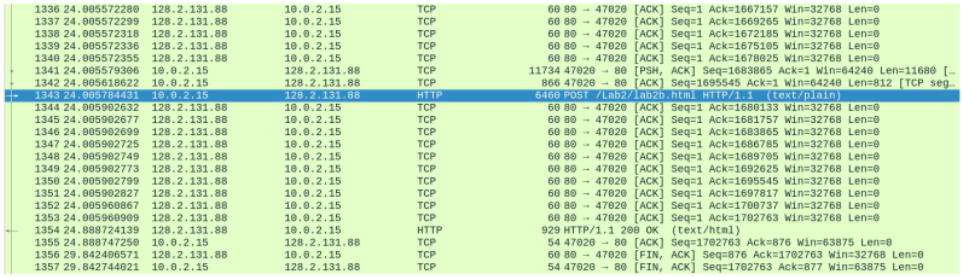


11.

3-Way Handshake:



HTTP POST:



12.

Client:-

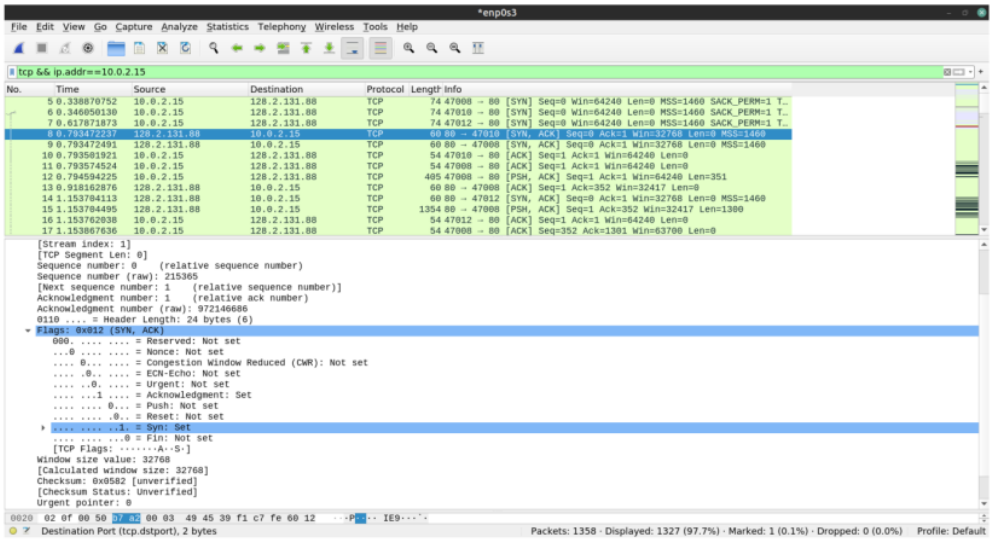
IP Address: 10.0.2.15

Port: 47008

Server IP Address: 128.2.131.88

Server Port number: 80

13.



A. TCP Basics:

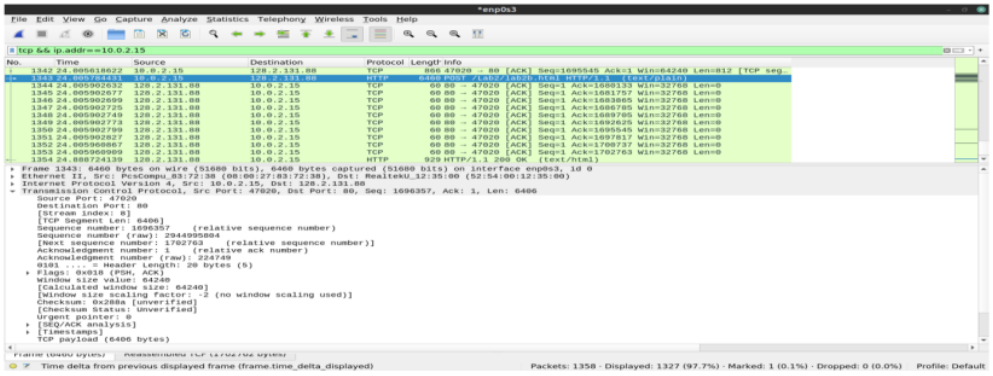
14.

Sequence Number of TCP SYN:

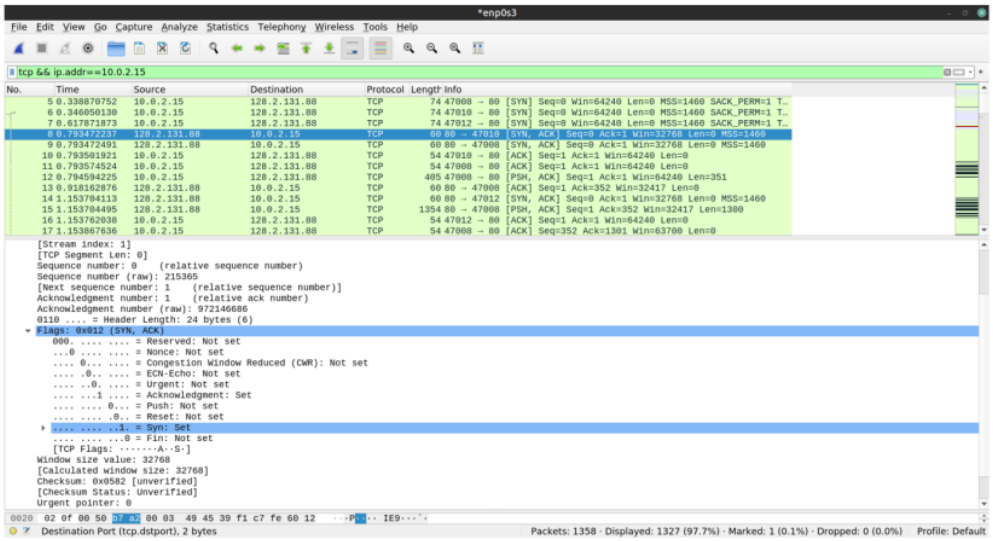
Relative: 0

Raw: 2410673663

The absolute sequence number is the raw sequence number given in the packet info.



15.



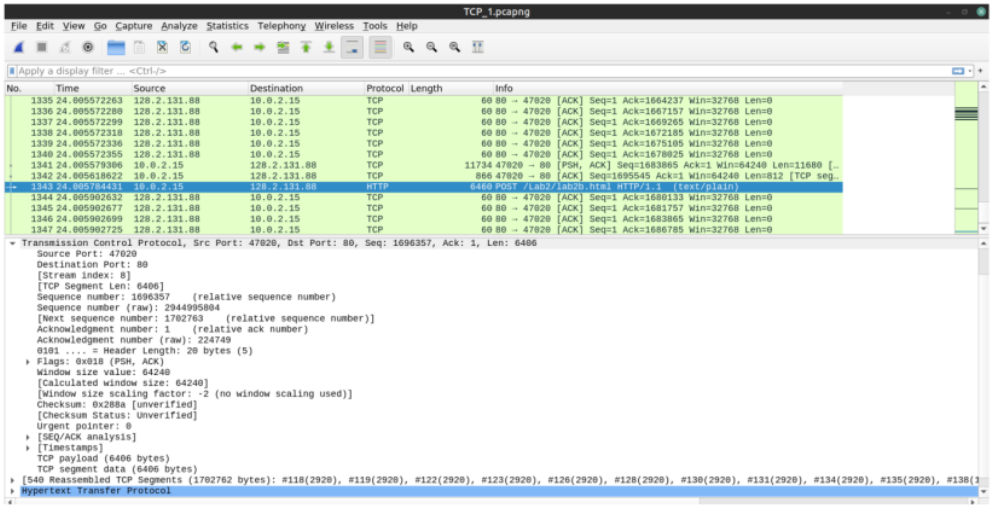
Sequence Number of the SYNACK segment: 0

Acknowledgement field in SYNACK: 1

The server determines the acknowledgement using the sequence number of the next expected packet.

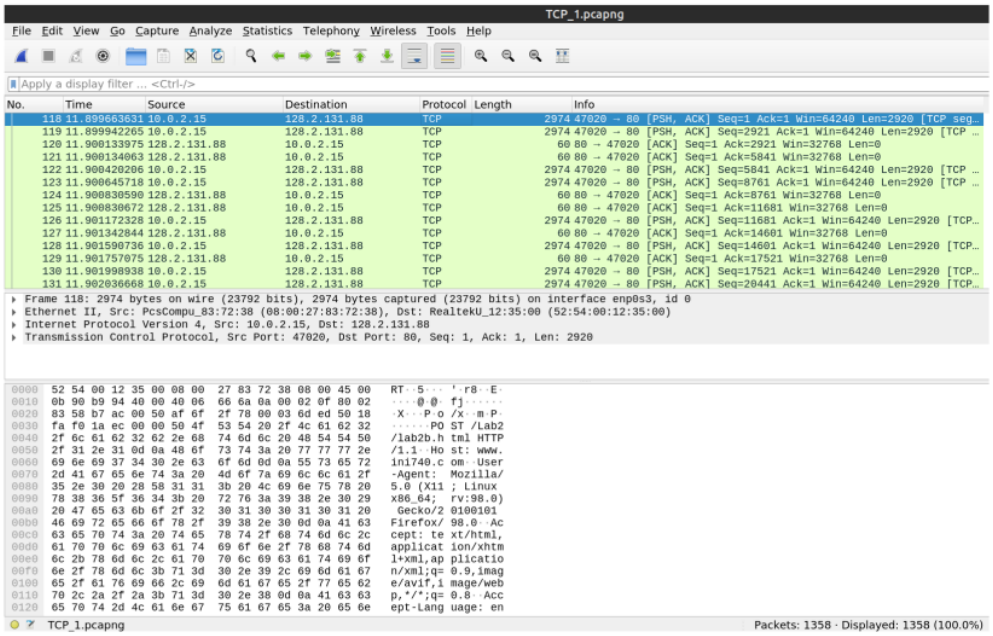
The acknowledgement and the syn bits are set to 1 which determines that it is a SYNACK segment.

16.



Sequence Number of HTTP POST TCP segment: 1696357

17.



Segments: 118, 119, 122, 123, 126, 128

Segment sequence numbers: 1, 2921, 5841, 8761, 11681, 14601

Segment Acknowledgements: 120, 121, 124, 125, 127, 129

1

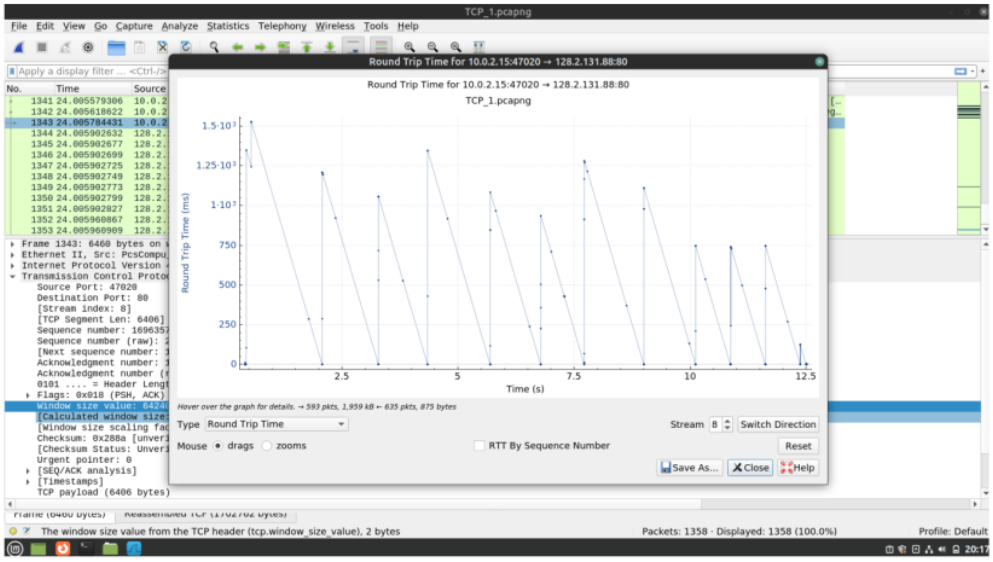
Round Trip Time (RTT) is the measure of how long it takes for a very small packet to travel across the network and for an acknowledgement of that packet to be returned.

Using the formula,

$$EstimatedRTT = (1 - \alpha) \cdot EstimatedRTT + \alpha \cdot SampleRTT$$

Where, $\alpha = 0.125$

Segment Number	Sample RTT	Estimated RTT
118	0.00047034	0.00047034
119	0.00019179	0.00043552
122	0.00041038	0.00043237
123	0.00018495	0.00040144
126	0.00017051	0.00037257
128	0.00016633	0.00034679

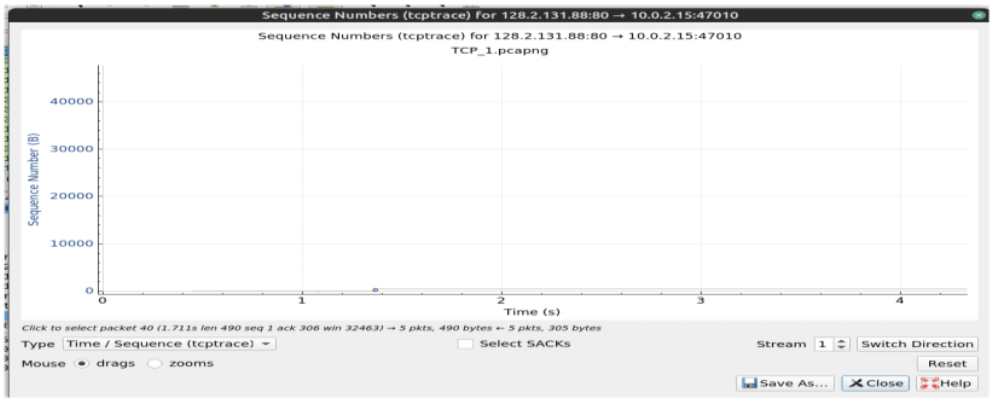


18.

```
    0110 .... = Header Length: 24 bytes (6)
  ▸ Flags: 0x012 (SYN, ACK)
    Window size value: 32768
    [Calculated window size: 32768]
    Checksum: 0x0582 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ Options: (4 bytes), Maximum segment size
  ▸ [SEQ/ACK analysis]
  ▸ [Timestamps]
```

Minimum buffer space available is 32768. The lack of buffer does not throttle the sender due to effective congestion avoidance.

19.



No segments have been retransmitted.

20.

The receiver acknowledges about 2920 packets after every 2 segments sent. There were no delayed ACKs found as there was no congestion in the network.

21.

Total file size = 17,82,579.2 bytes

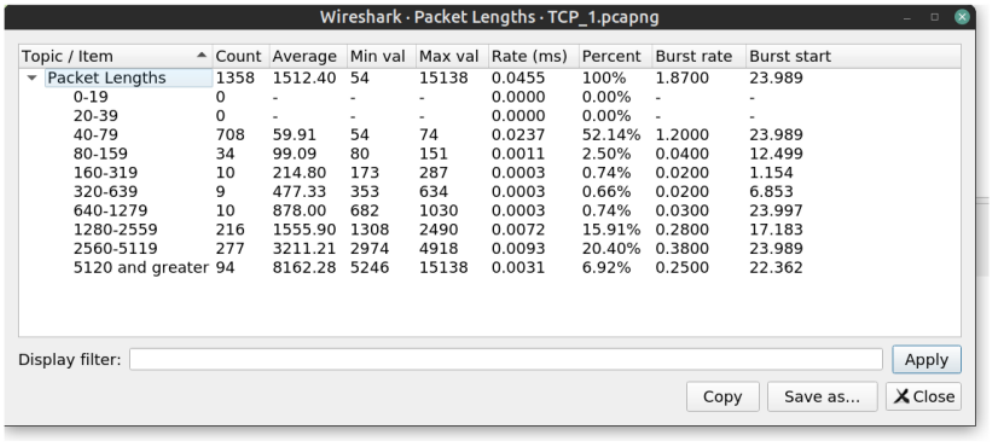
Total download time = (29.842 - 24.888)s = 4.954s

Throughput = 17,82,579.2 / 4.954 = 3,59,826.24 bytes/s

= 351.39 KBps

B. TCP Statistics:

22.



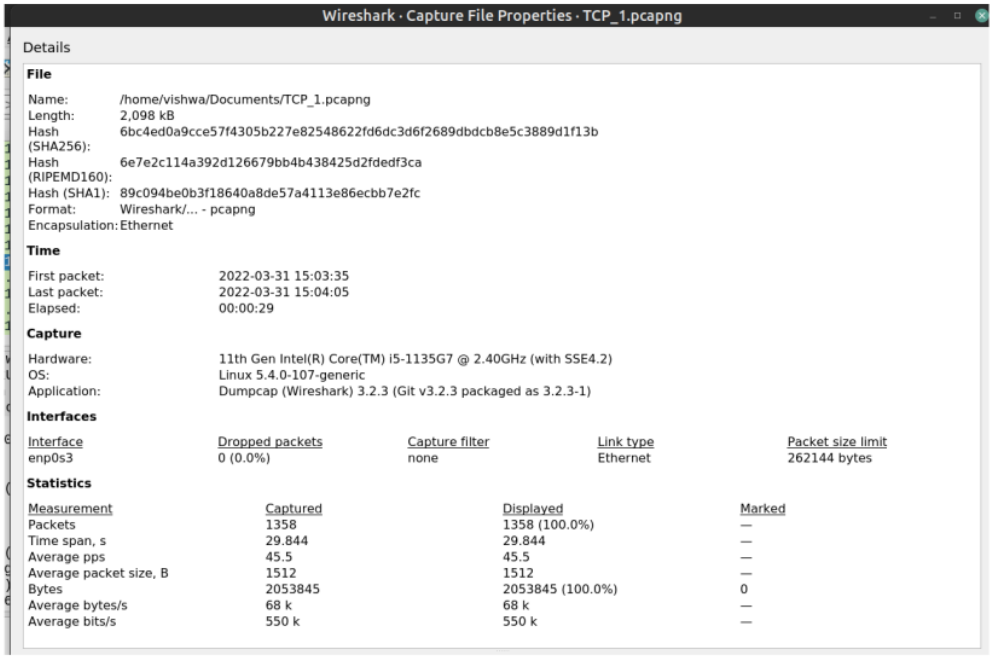
The most common packet length is in the range of 40-79 bytes.

The second-most common packet length range is 2560-5119 bytes.

The length of packets <40 bytes is 0 as the minimum header length is 40 bytes and any packet with <40 bytes contains no data.

Navigate to “Statistics -> Packet Lengths” to get the information.

23.



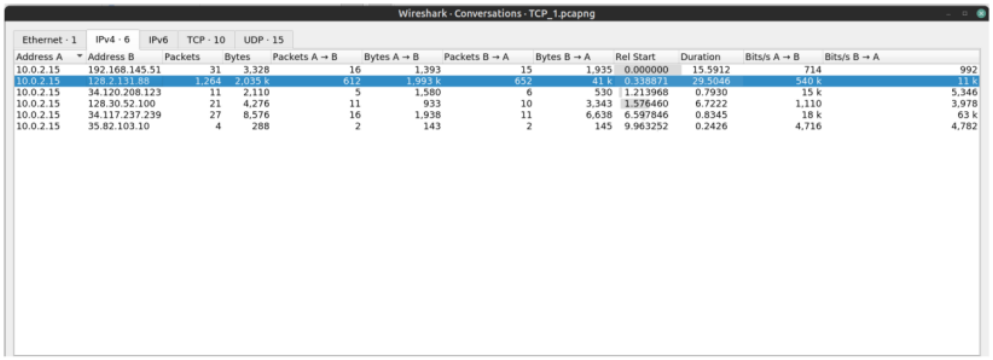
Average Throughput = 2053845/29.844 = 68819.36 bytes/s= 0.065 MBps

Packets captured in the session = 1358

Total bytes = 2053845

Go to “Statistics -> Capture File Properties” to find the above observations.

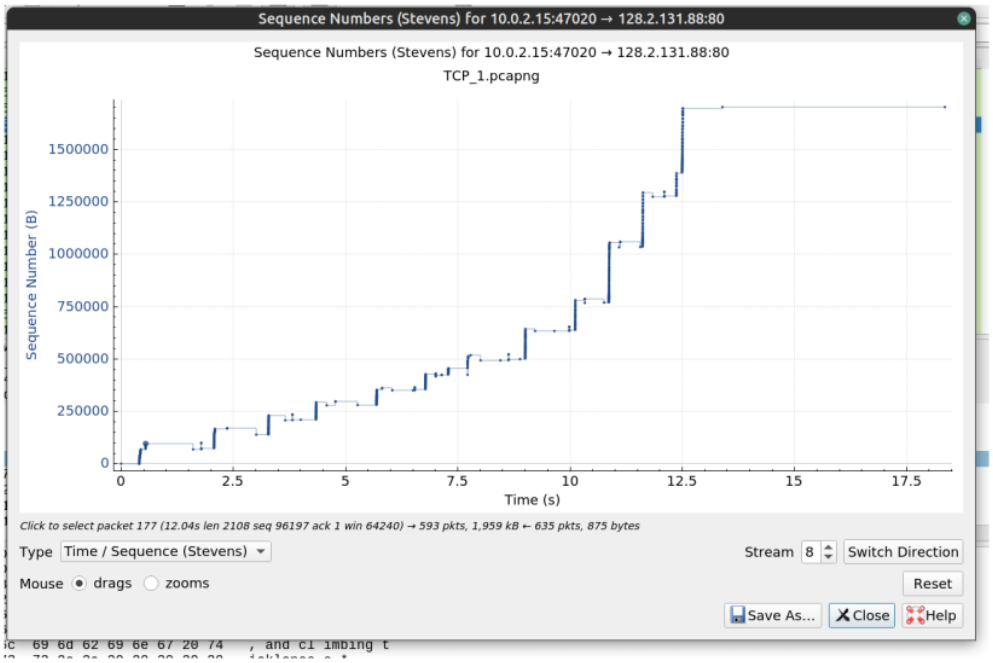
24.



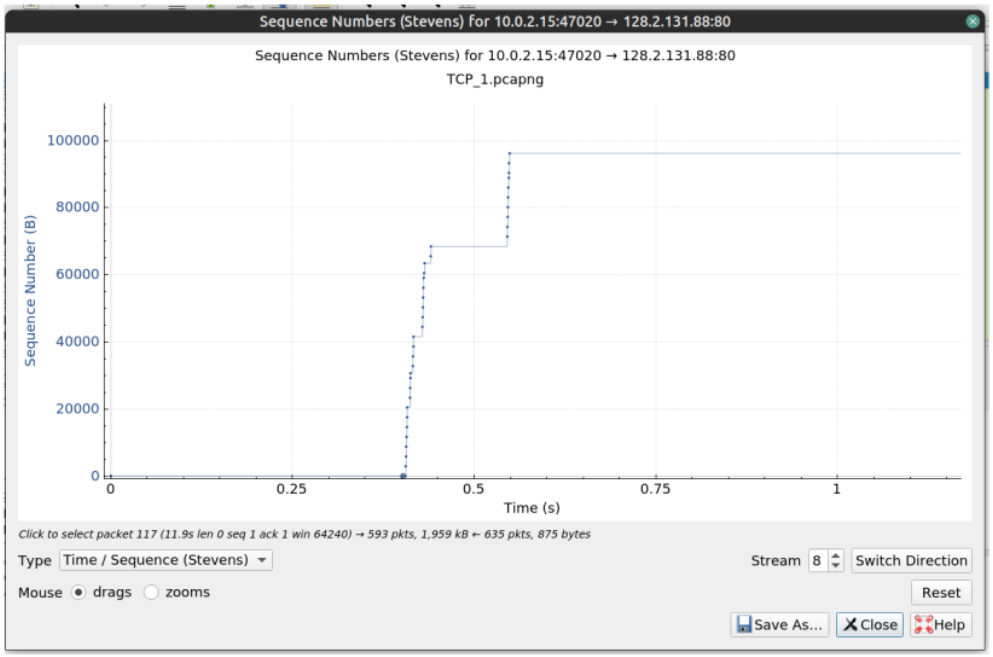
The local host conversed with the remote host with IP address 128.2.131.88 the most. 612 packets were sent to the remote host and 652 packets were sent from the remote host.

III. Congestion Control:

25.



26.

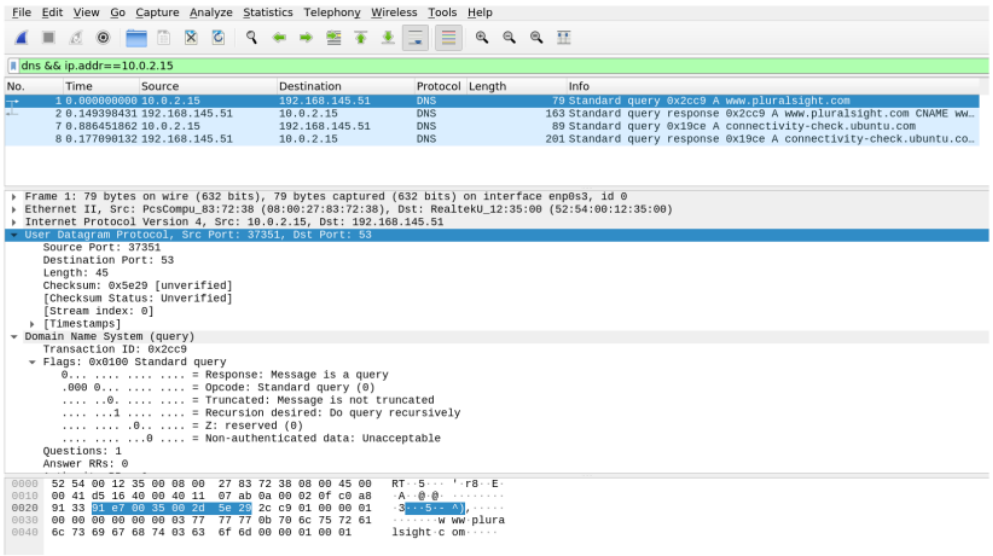


Slow start phase begins: 0.402s

Slow start phase ends: 0.440s

IV. The Network Layer:

27.



29.

Datagram Length: 45 bytes

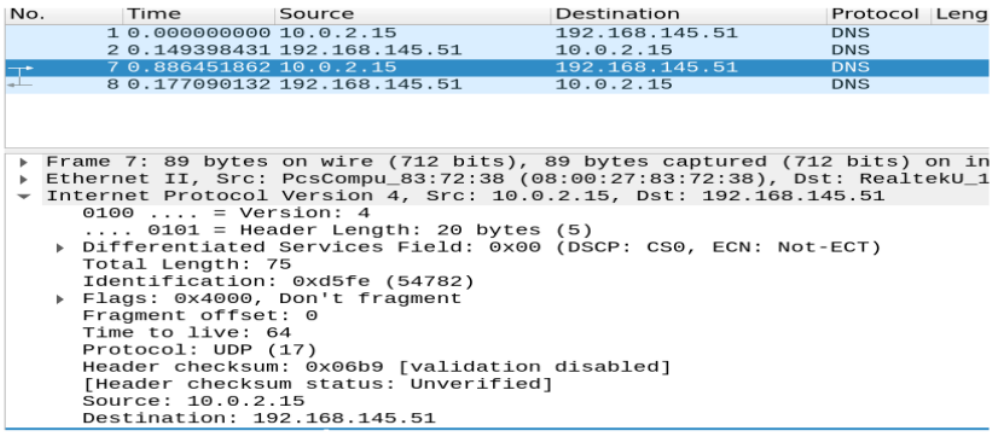
Upper Layer Protocol: IPv4

IP Address Fields:-

Src: 10.0.2.15

Dest: 192.168.145.51

31.



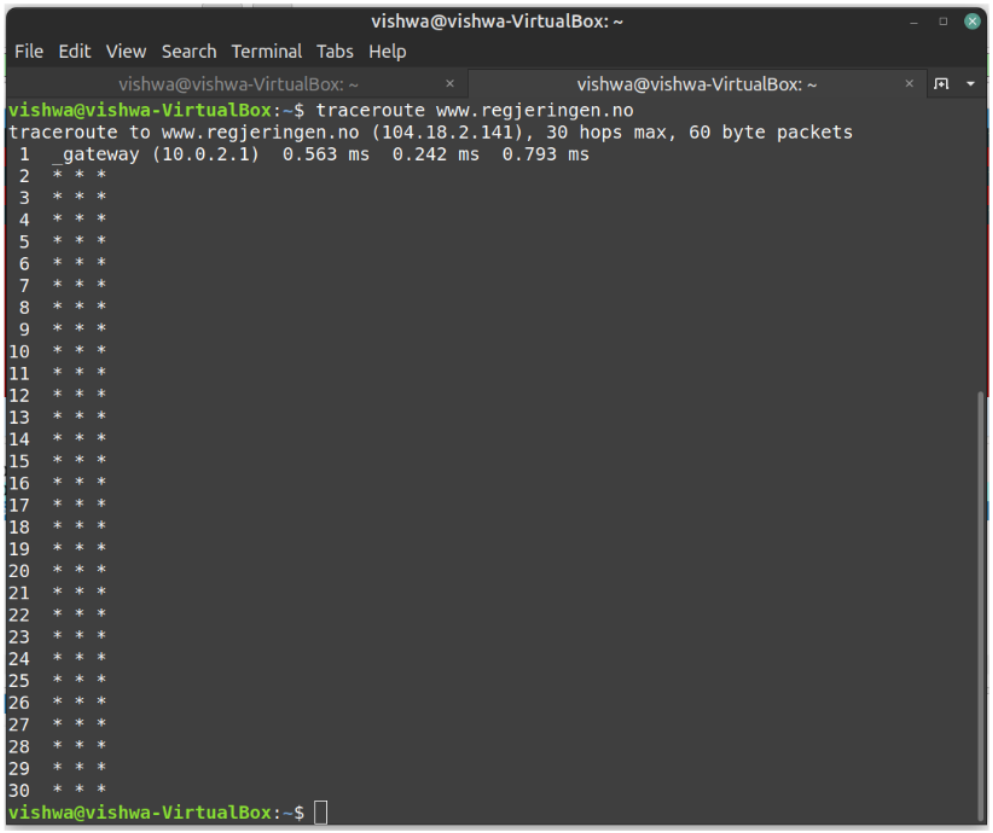
TTL: 64

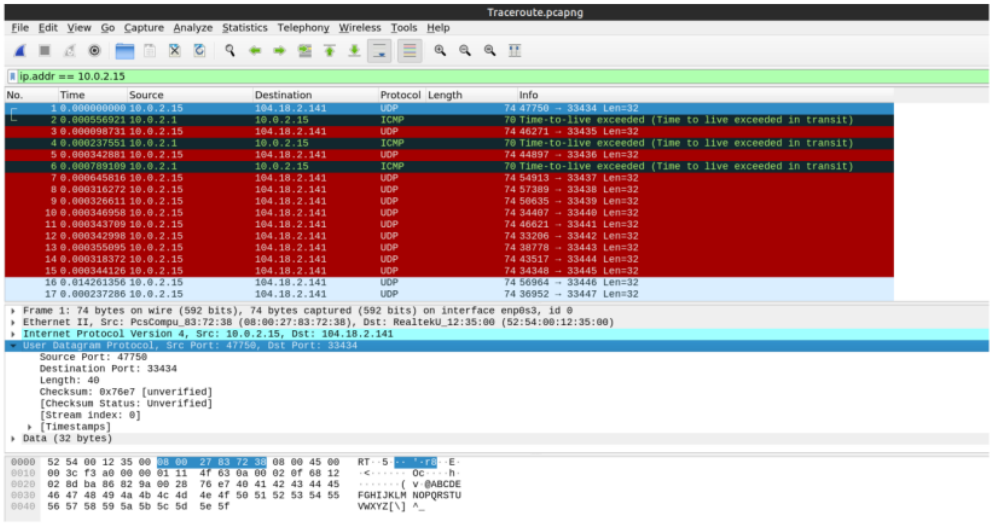
OS: Linux Mint 20.3 Cinnamon

OS Version: 5.2.7

V. ICMP:

32.





35.

When traceroute was used:-

First Destination Port: 33434

Second Destination Port: 33435

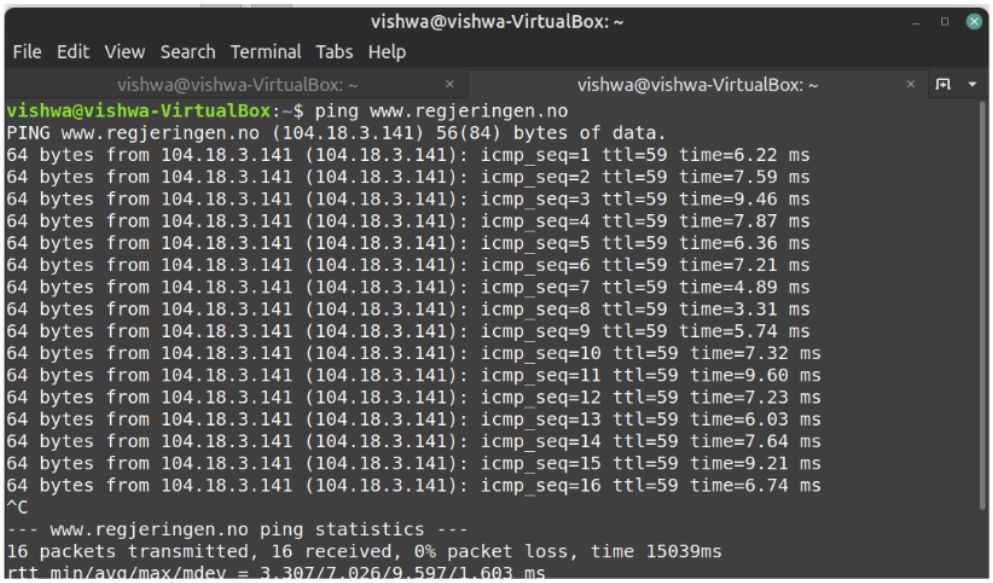
Third Destination Port: 33436

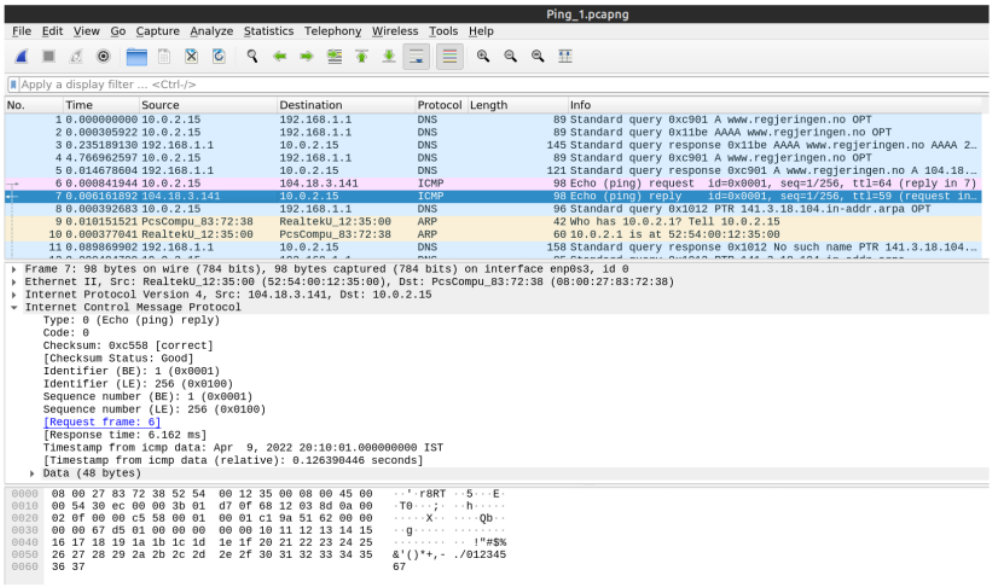
And so on…

Destination Port number increases by 1 every hop.

36.

To inspect the ICMP reply packet ping was used instead of traceroute as the traceroute was not showing any proper routes to be examined.





ICMP Type: 0

ICMP Code: 0

Identifiers: 1(BE), 256(LE)

Sequence numbers: 1(BE), 256(LE)

37.

Timestamp from icmp data is mentioned to relate to the sent packets.

38.

Both ping and traceroute screenshots are pasted above for reference.

Ping does not show the port numbers for every hop unlike traceroute.

PES2UG20CS389_Vishwa Mehul Mehta_Week6

ORIGINALITY REPORT

7%	7%	2%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	manuals.gfi.com Internet Source	5%
2	"Chapter 9 Network Traffic Analysis", Springer Science and Business Media LLC, 2005 Publication	2%

Exclude quotes	On	Exclude matches	< 3 words
Exclude bibliography	On		