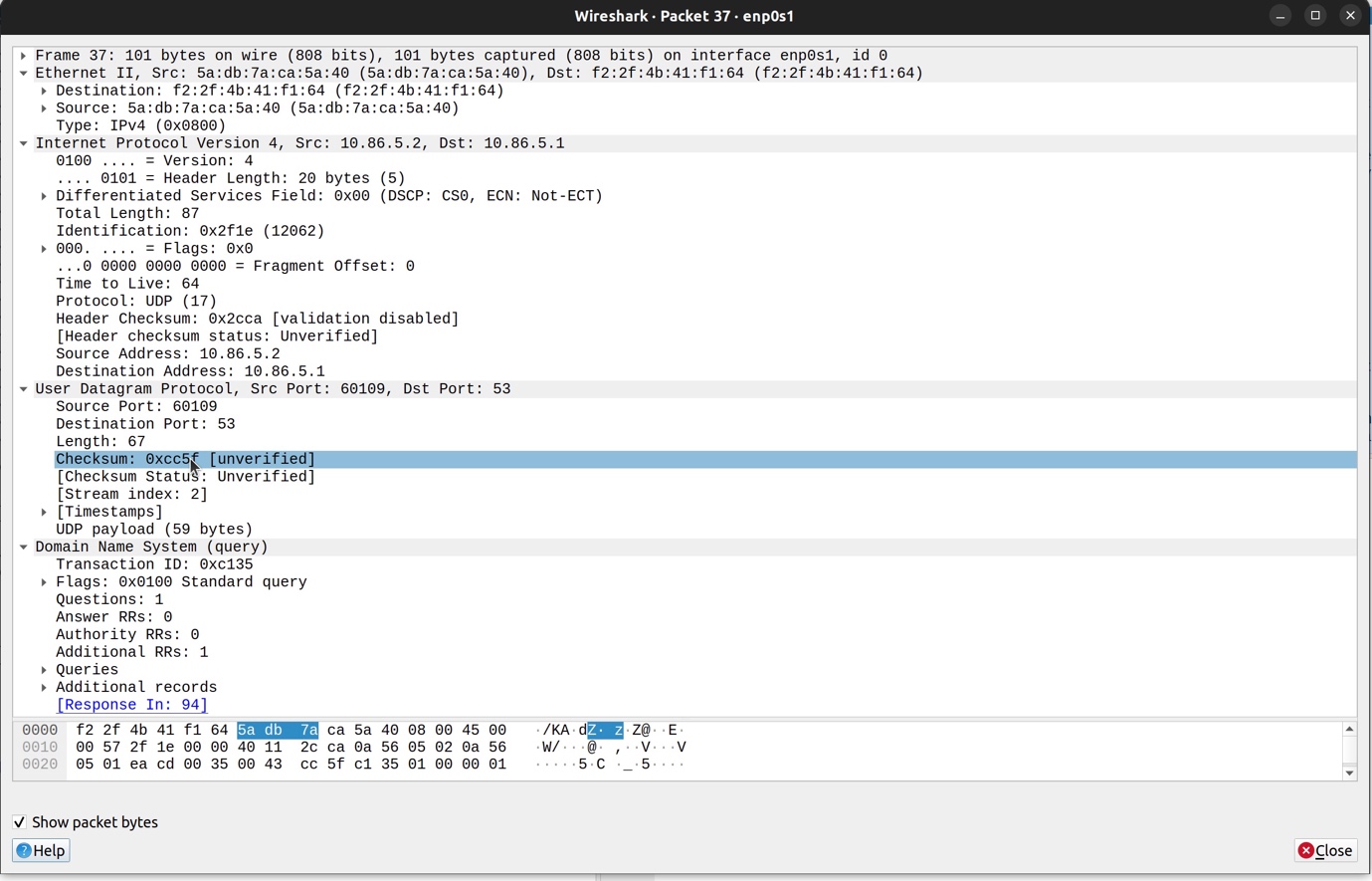
LAB-03. ( Network Monitoring And Analysis With Wireshark)  
(COMPUTER NETWORKS)

-KUBER LAMBA(210905070)

2A.



a)the source port number :-60109

b)the destination port number :-53

c)the total length of the user datagram :-87

d)the length of the data :-67

e)wether the packet is directed from a client to a server or vica versa :- client to server

f)the application-layer protocol : UDP

g)wether a checksum is calculated for this packet or not : - Unverified 0xcc5f

2B



Source IP address: 10.86.5.2

Destination IP address: 10.86.5.1

In the response, the addresses are exactly inverted(the source becomes the destination and destination is source)

2C

Source and destionation port numbers in query : 60109 , 53

Source and destionation port numbers in response : 53 , 60109

The standard port for DNS :- 53

2D

Total length of the query is :-87

UDP Payload is 59 Bytes

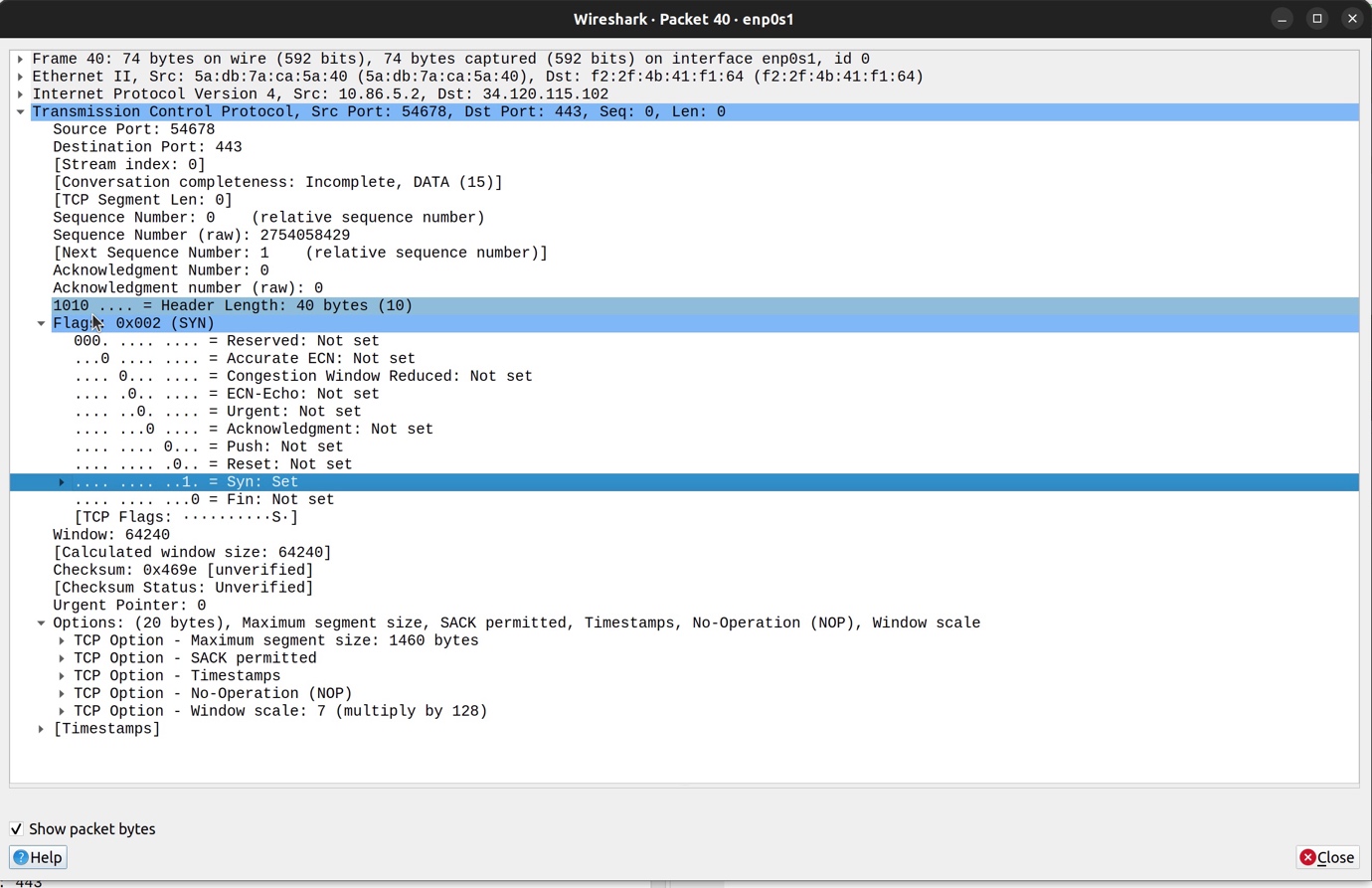
3A

PART-1 : Connection Establishment Phase

A TCP connection establishment consists of 3 way handshake.

(SYN , SYN-ACK , ACK)

SYN :



SYN-ACK :

A screenshot of a computer

Description automatically generated

ACK :

A screenshot of a computer

Description automatically generated

1. What are the addresses for each packet?

Ans) SYN : Source : 10.86.5.2

Destination : 34.120.115.102

SYN-ACK : Source : 34.120.115.102

Destination : 10.86.5.2

ACK : Source : 34.120.115.102

Destination : 10.86.5.2

1. What flags are set in each packet?

* SYN: 0x002 (SYN) (SYN flag is set)
* SYN-ACK: 0x012 (SYN-ACK) (SYN and ACK flags are set)
* ACK: 0x010 (ACK) (ACK flag is set)

3. What are the sequence number and acknowledgment number of each packet?

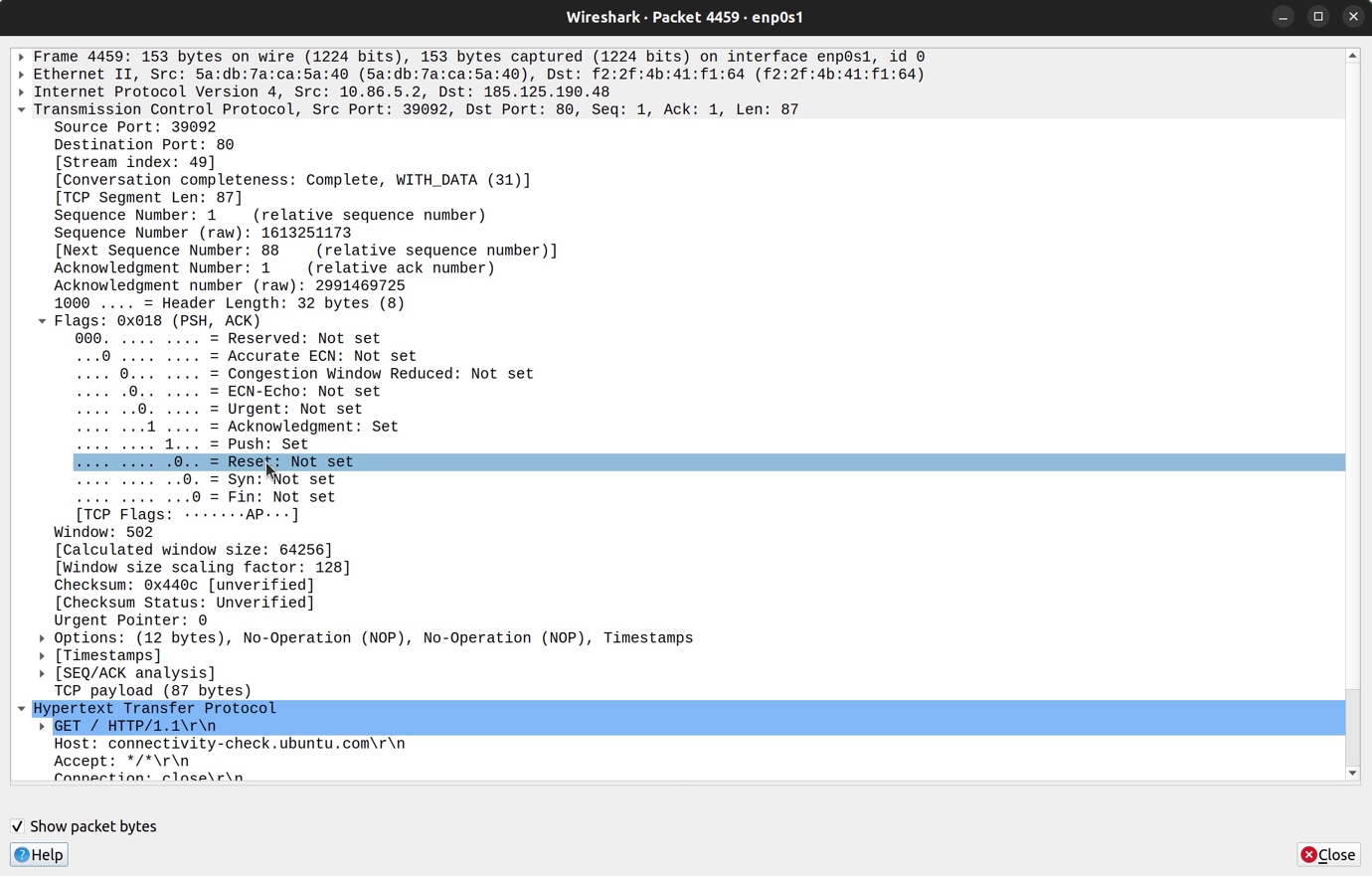
* SYN: Seq Number: 2754058429, Ack Number: 0
* SYN-ACK: Seq Number: 3488253684, Ack Number: 2754058430
* ACK: Seq Number: 3488253685, Ack Number: 2754059100

4. What are the window size of each packet?

* SYN: 64240
* SYN-ACK: 65535
* ACK: 67072

Part 2: Data Transfer Phase

GET request:



OK Response :

A screenshot of a computer

Description automatically generated

1. What TCP flags are set in the first data-transfer packet (HTTP GET message)?

Ans) ACK and PUSH flags are set

1. How many bytes are transmitted in this packet?

Ans) 87 bytes

1. How often does the receiver generate an acknowledgment?

Ans) 0.003 seconds

1. How many bytes are transmitted in each packet? How are the sequence and acknowledgment numbers related to number of bytes transmitted?

* Ans) 87 bytes are transmitted in the GET request, and 189 bytes are received in the OK response. The sequence number increases by the number of bytes transmitted, and the acknowledgment number increases by the number of bytes received.

1. What are the original window sizes that are set by the client and the server? Are these numbers expected? How do they change as more segments are received by the client?

Ans) The window size when sending request to the server was set at 64256. The window size when receiving response was 98304. The window size will increase till a certain capacity (limited by hardware) to prevent congestion.

1. Explain how the window size is used in flow control?

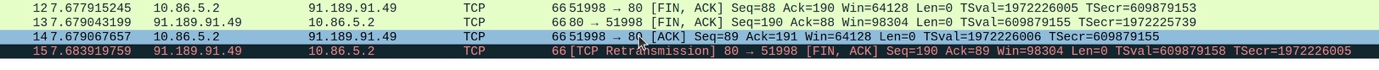
* In a sliding window system in TCP, the size of the window is governed by 2 things:
  + The size of the send buffer on the sending system
  + The size and available space in the receive buffer on the receiving system

To avoid congestion, the sender cannot send more bytes than the space available in the receive buffer of the receiver. The sender must wait till the bytes in the receiving buffer have been acknowledged. This prevents congestion, and helps in flow control.

1. What is the purpose of the HTTP OK message in the data transfer phase?

The HTTP OK message is a feedback about the request that was previously sent. An OK response means that the request has succeeded.

PART-3 Connection Termination Phase



1. How many TCP segments are exchanged for this phase?

Ans) 4 segments are exchanged in the connection termination phase. (FIN, ACK, FIN, ACK)

1. Which end point started the connection termination phase?

* The client started the connection termination phase.

1. What flags are set in each of segments used for connection termination?

Ans) First the client sends a segment with FIN, and ACK flags set. Then the server responds with a segment with FIN, and ACK flags set. Then the client sends a segment with ACK flag set, and finally the server sends a segment with FIN, and ACK flags set.