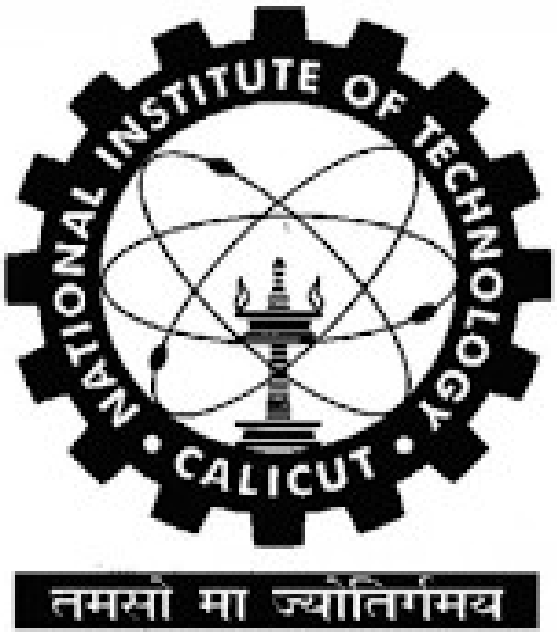
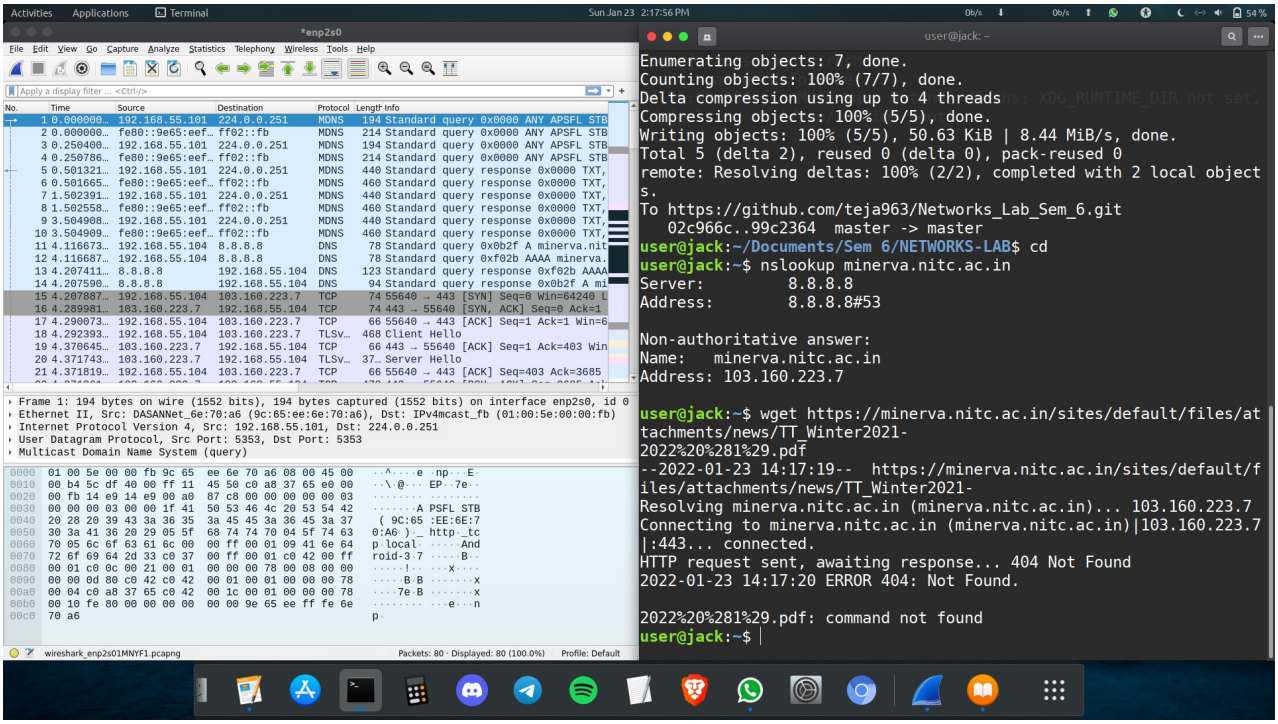
CS3009D: NETWORKS LABORATORY
(EXPERIMENT 2)



Name : Panasa Teja
ROLL : B191143CS
BATCH : B

1. Host Ip address = 192.168.55.104
   Destination Ip address = 103.160.223.7(minerva.nitc.ac.in)
   Transport Layer Protocol = TCP, to get reliable performance
   Internet Protocol Version 4(IPv4)
   Source Port: 55640
   Destination Port: 443(https)



First It used a DNS QUERY to find IP address of Server

It used TCP Protocol for Transferring Data. It established a connection through **Three Way HandShake:**

1. SYN(Synchronize sequence Number):

Ethernet II:

Src: Dell_23:d5:c2(Mac Address)

Dst: DASANNet_5b:5f:0f(Mac Address)

Sequence Number (raw): 3829789170.

Each Sequence Number contains (2^32 bits = 4GB Sequence Numbers can be sent)

Flags: SYN

Window size: 64240

2. SYN/ACK(Acknowledgment):

Ethernet II:

Src: DASANNet_5b:5f:0f

Dst: Dell_23:d5:c2

Sequence Number (raw): 3249011488

Acknowledgment Number: 3829789171

Flags: (SYN/ACK)

Window size: 65160
RTT(Round Trip Time) to ACK: 0.082s

3. ACK:

Ethernet II:

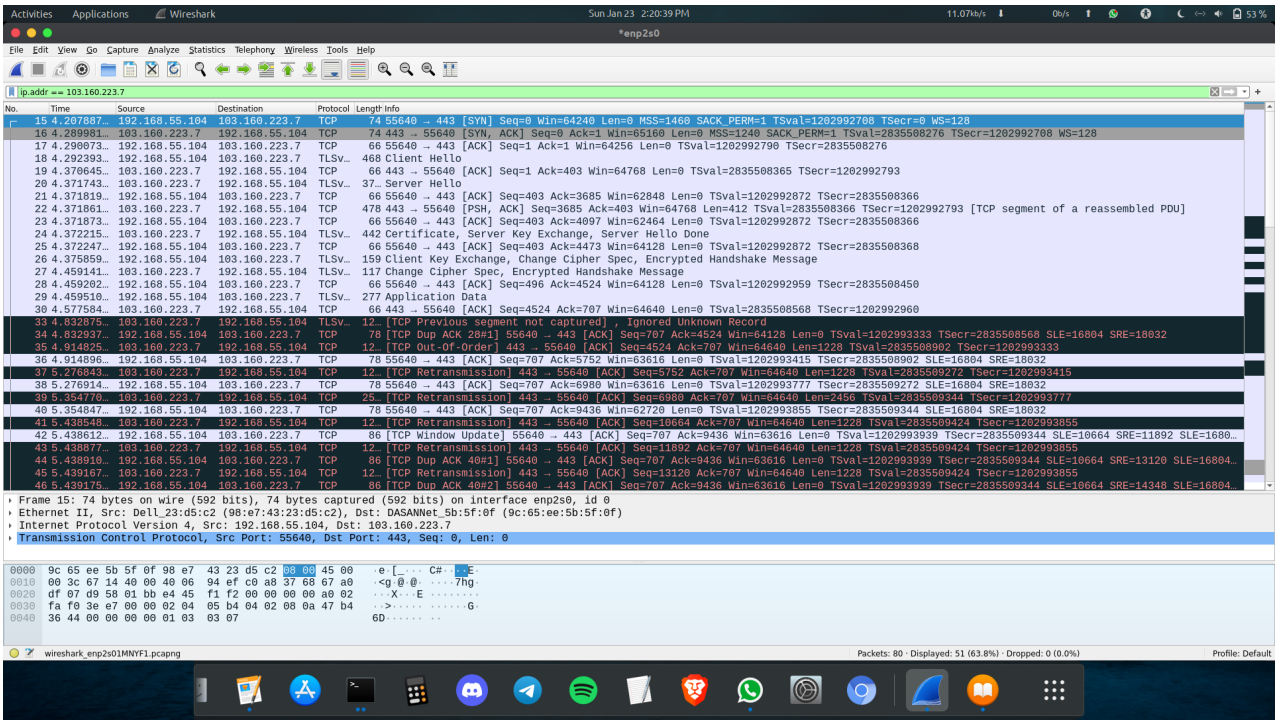
Src: Dell_23:d5:c2(Mac Address)

Dst: DASANNet_5b:5f:0f(Mac Address)

Sequence Number(raw): 3829789171

Acknowledgment Number: 3249011489

Flags: ACK



After this step TCP connection is established for Data Exchange, It will check the host windows size for transferring the data to host.

Now the data is transferred in the Transport Layer by Handshake Protocol: Client Hello and Server Hello

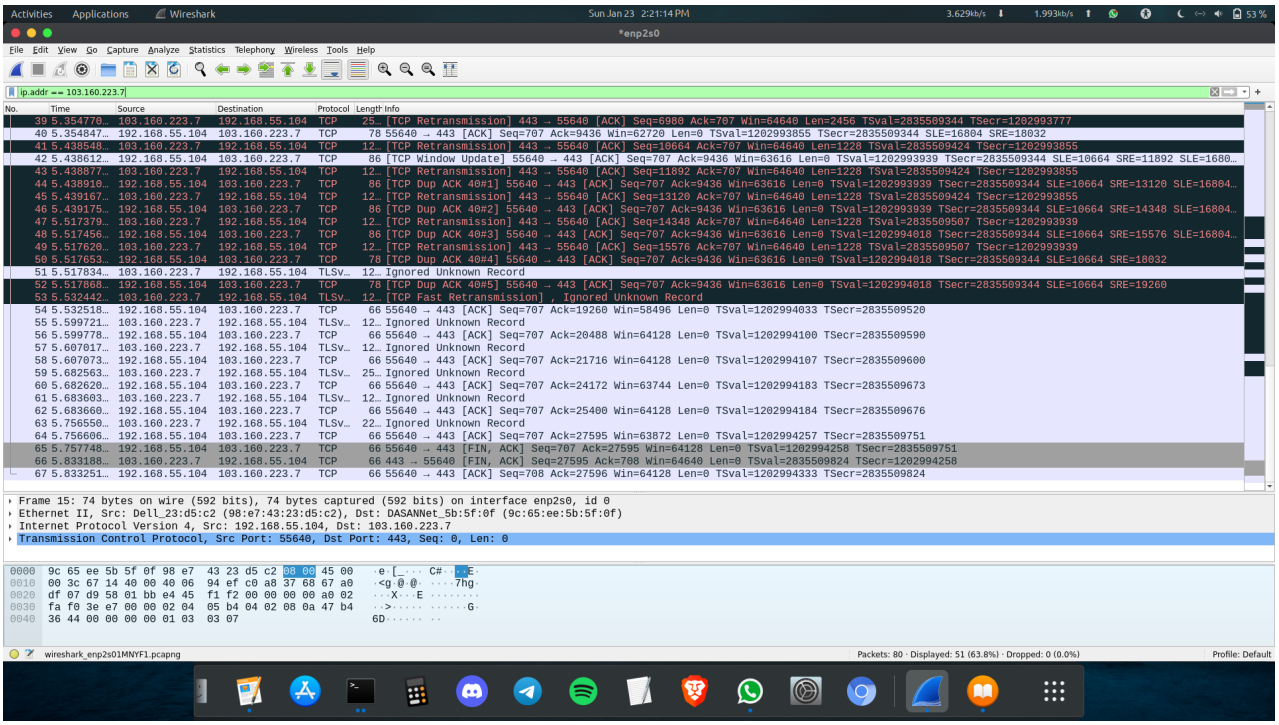
Data transfer started flowing in tcp connection through a stream of packets and they are monitored using fields like sequence number etc .At sometimes 3 dup ack's came may be due to packet loss in the internet and the server retransmitted them from buffer. Client key exchange happened using TLS inorder to encrypt/decrypt the data because http secure protocol is used for this download.

Due to some unkown error in the network the web server sent a reset request to my laptop to terminate the tcp connection temporarily.Again 3-way handshake and client key exchange happened as usual.

To remove a connection of TCP, We can use these packets

1. FIN

2. [FIN,ACK]
3. [ACK]



2. We need to filter HTTP Protocol because of unsecured host systems

(a) IP ADDRESS:(IPv4)
SOURCE: 192.168.44.53
DESTINATION: 192.168.44.1

(b) It is **POST /HTTP Protocol Version 1..1** used in Application Layer
It used **TCP protocol** in Transport Layer with
Source Port: 53810
Destination Port: 1000

(c) **Username:** vasudevanar
Password: vasu

3.

TCP HEADER DEATILS FOR PACKET 27:

0	**15**	**16**	**31**
00000001 10111011(443)		11100111 00000010 (59138)	
10110110 00110100 00011110 01111010(3056868986)			
01000000 10100101 01100010 01110001(1084580465)			
0101(5) | 000000 |010001 (ACK FIN**)** |		00000000 00111100 (60)	
01010100 01000010 (0x5442)		00000000 00000000 (0)	
Options			
Data			

TCP HEADER DEATILS FOR PACKET 32:

0	**15**	**16**	**31**
11100111 00000011 (59139)		00000001 10111011 (443)	
01100011 00000000 00101101 10100010 (1660956066)			
11100110 00100101 00111000 10100010 (3861199010)			
0101 (5) | 000000 | 010100 (ACK RST) |		00000000 00000000(0)	
11111010 11101100 (0xfaec)		00000000 00000000(0)	
Options			
Data			