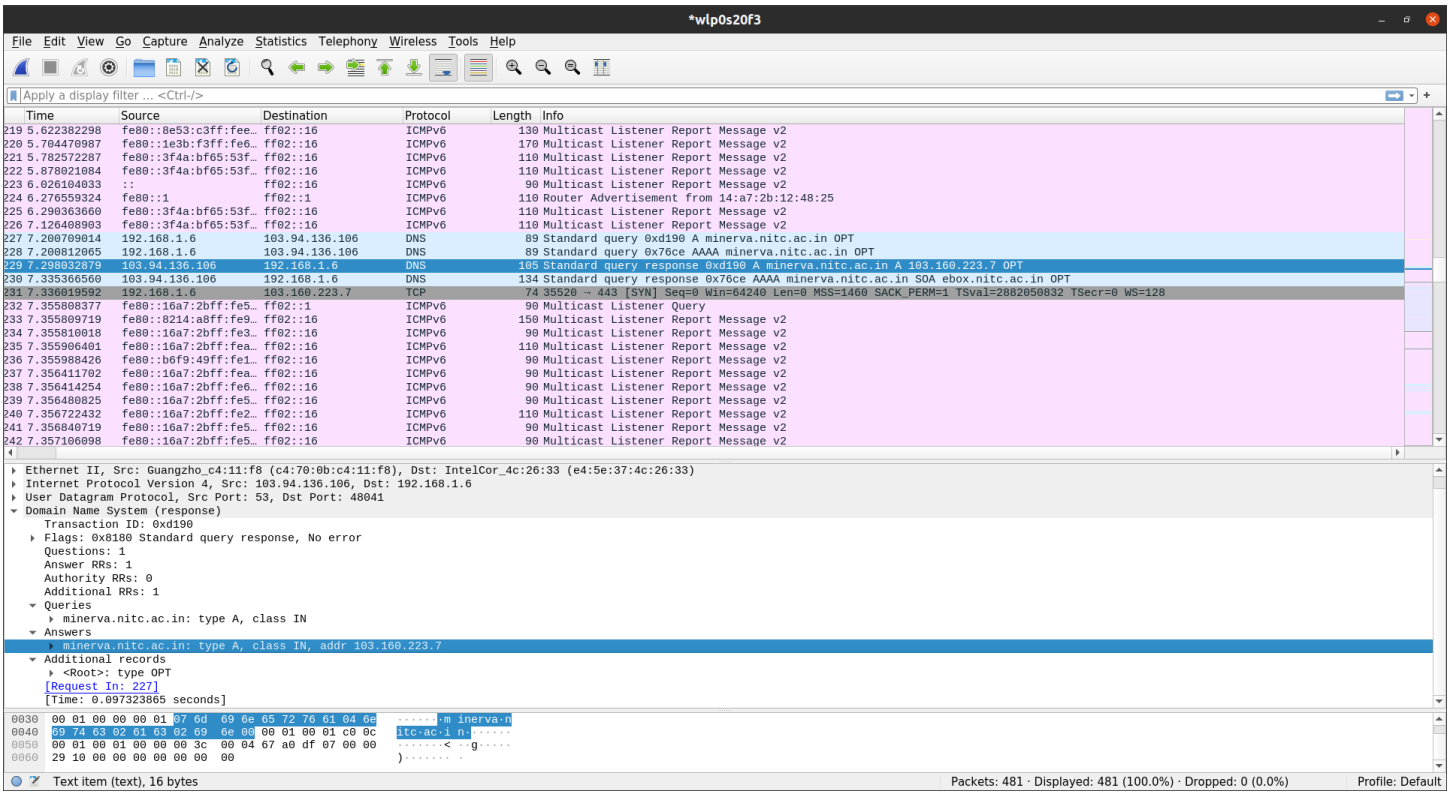
CS3093D: Networks Lab Assignment – II

Hanna Nechikkadan
B190420CS
NIT Calicut
22/01/2022

CONTENTS

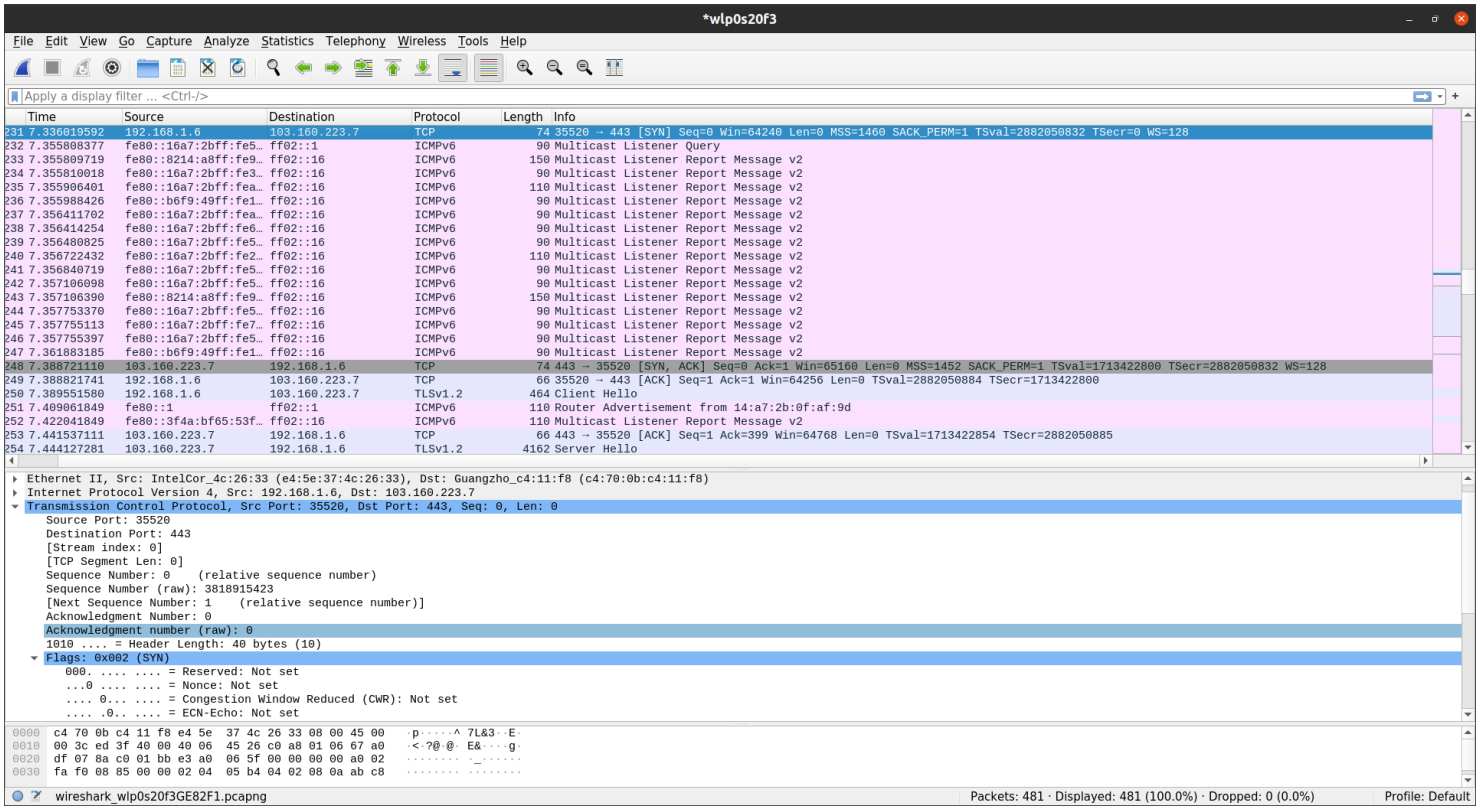
1. Execute the following command in the terminal,
   wget
   https://minerva.nitc.ac.in/sites/default/files/attachments/news/TT_Winter2021- 2022%20%281%29.pdf
   Parallely run the wireshark tool. Note down your network analysis of the command.



- IP address of my device : 192.168.1.6
- IP address of DNS server : 103.94.136.106

My device sends DNS queries over UDP to the DNS servers to resolve the domain minerva.nitc.ac in frames 227 and 228 and receives responses with the IP addresses of minerva.nitc.ac.in in frames 229 and 230.

- IP address of minerva.nitc.ac.in : 103.160.223.7



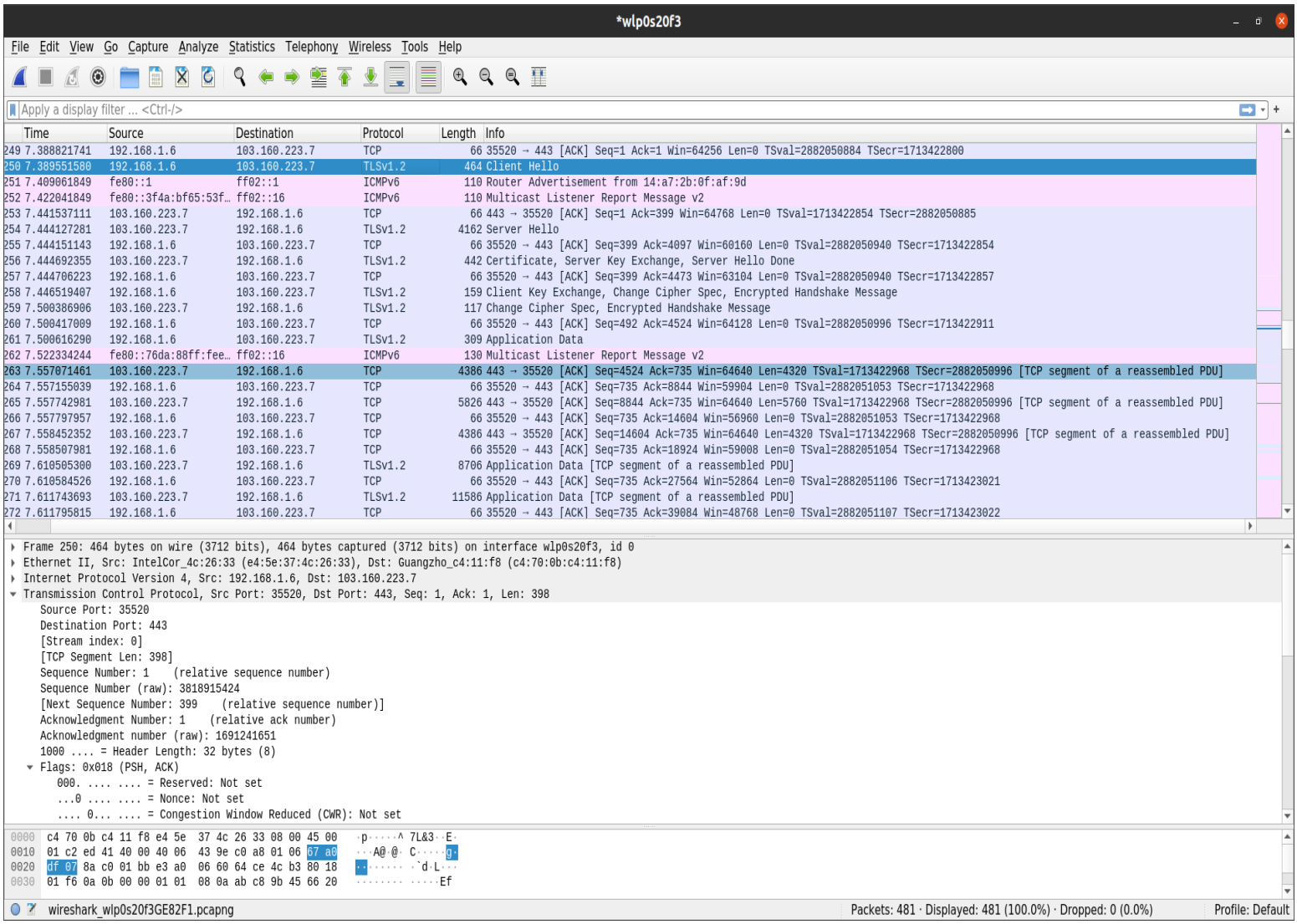
- Then a TCP connection is set up between my device and the minerva.nitc.ac.in server through a 3-way handshake over TCP.
    1. 192.168.1.6 (my device) sent a packet with SYN flag set with source port 35520 to 103.160.223.7 (minerva.nitc server) with destination port 443 in frame 231.
    2. Then 103.160.223.7 sent a packet with SYN and ACK flags set in frame 24.
    3. And then the handshake is completed and a TCP connection is set up when 192.168.1.6 sent a packet with ACK flag set in frame 249.

The communication between my device and minerva.nitc.ac.in happens through :

- Port no. at my end : 35520

- Port no. at minerva.nitc.ac.in : 443

- The connection is secured with TLSv1.2 protocol.

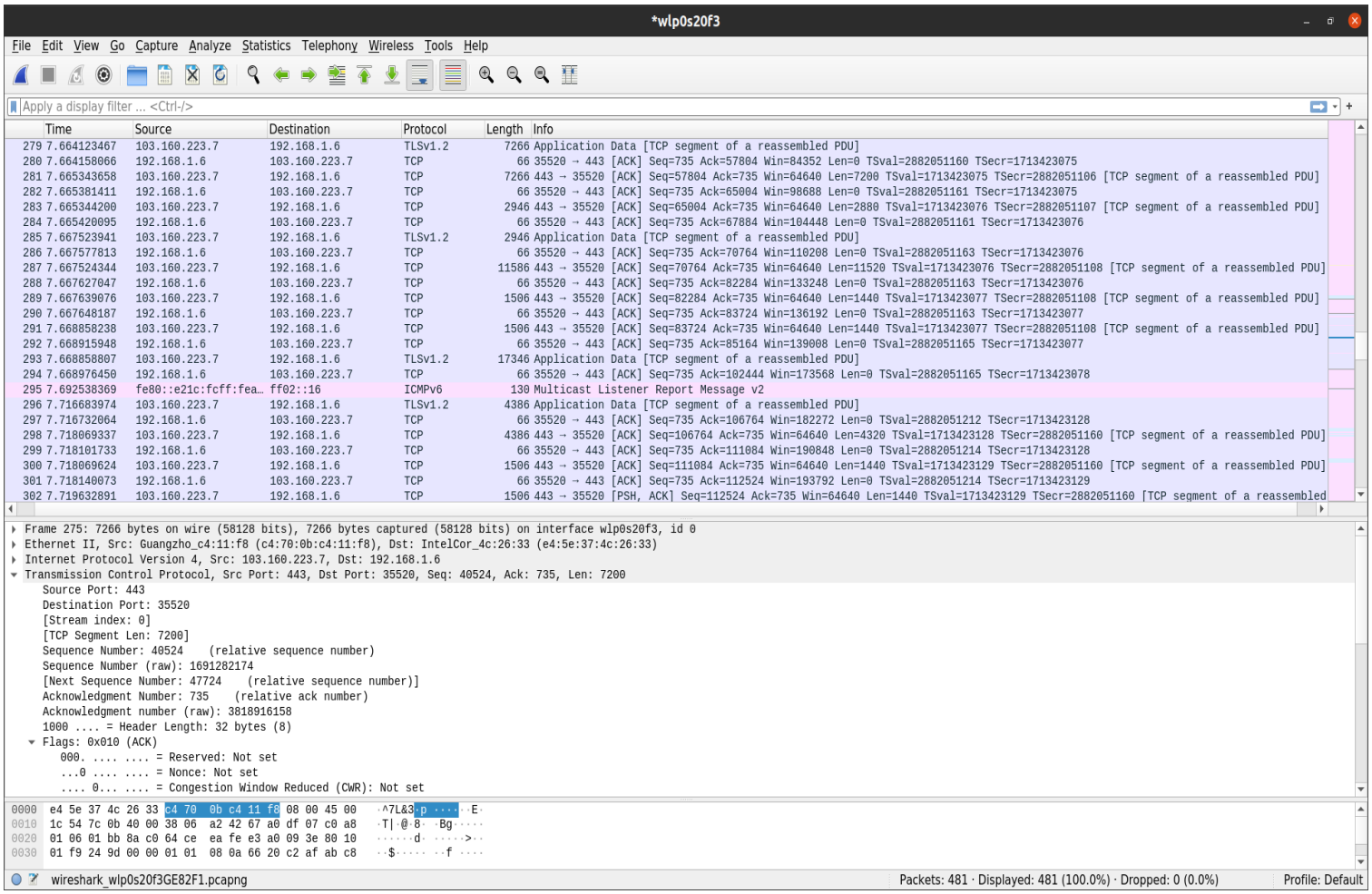


- The frames 250, 254, 256, 258, 259 show the TLS handshake which initiates the TLS connection.

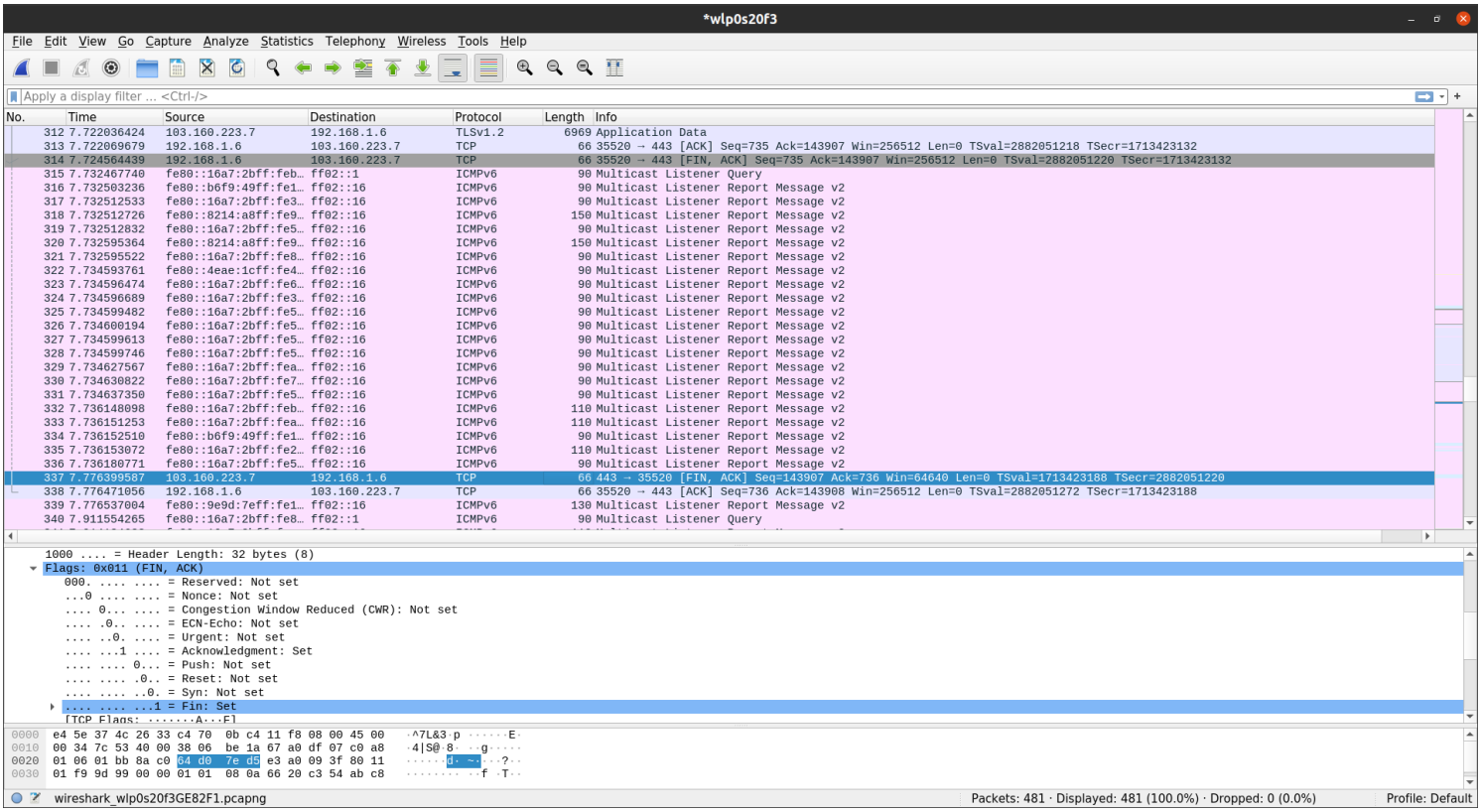
During the TLS handshake, my device and the server:

1. Specify which version of TLS (TLS 1.2) they will use
2. Decide on which cipher suites they will use
3. Authenticate the identity of the server using the server's TLS certificate

4. Generate session keys for encrypting messages between them after the handshake is completed.

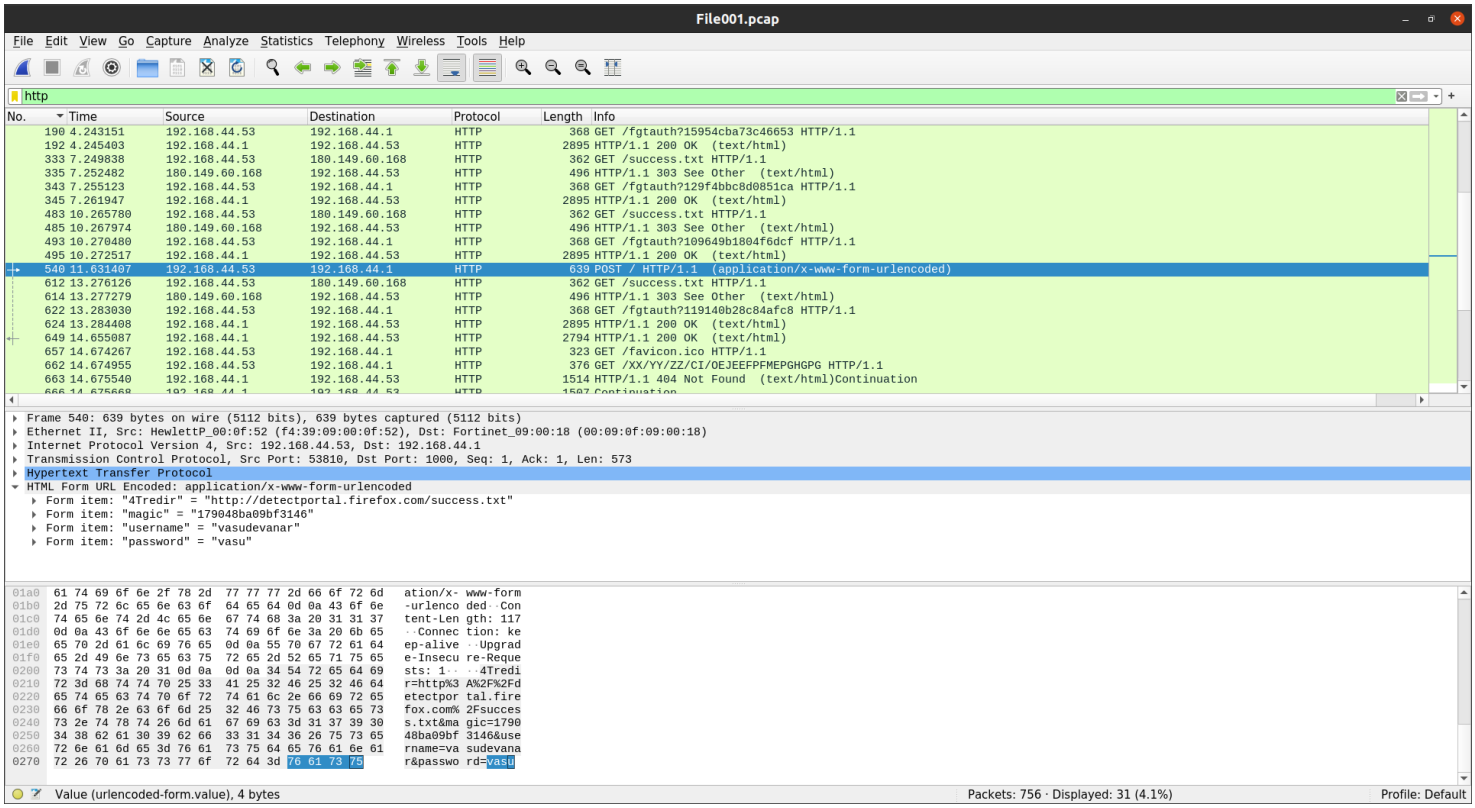


- Then we can see that the client (my device) and server (minerva.nitc.ac.in) communicates through a TCP connection where the server sends data through the packet and my device sends a packet to acknowledge with the ACK flag set in each packet.



- Here in frames 314 and 337, we can see the ACK and FIN flags have been set. This indicates that the connection is being terminated and both ends acknowledge the termination and the connection is ended gracefully.

2. Consider the pcap file, File001.pcap. The file contains captured packets sent over the network. It is noticed the system has made a connection to an unsecured host system and the user has sent his credentials over plaintext. Investigate File001.pcap to unearth the login credentials.



a. Indicate the IP addresses, Source and Destination, of the communicating end systems in which the login credentials are found.

Ans. Source IP Address : 192.168.44.53
Destination IP Address : 192.168.44.1

Internet Protocol Version 4(IPv4) is used.

b. Determine the protocol over which the user credentials are sent.

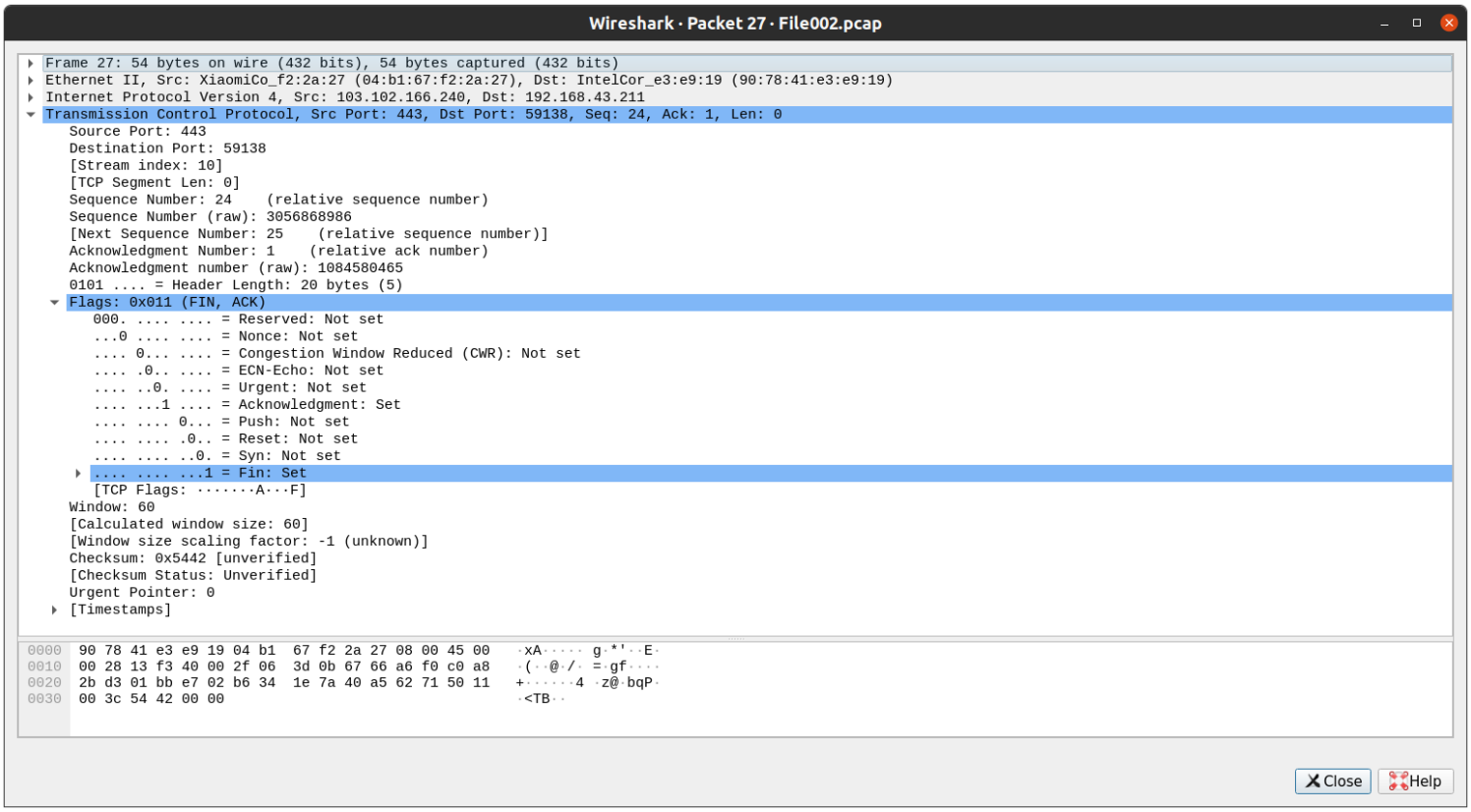
Ans. The protocol used to send the user credentials is HTTP (HyperText Transfer Protocol) as application layer protocol and is sent over TCP (Transmission Control Protocol) in the transport layer.

c. What are the login credentials?

Ans. Username = vasudevanar
Password = vasu

3. Consider the pcap file, File002.pcap. The file contains captured packets. Consider the packets numbered 27 and 32. Fill up the header details for the packets 27 and 32. The header details are provided in Figure 1.

Packet 27



443								59138
3056868986								
1084580465								
0101		0	1	0	0	0	1	60
0x5442								0

The values in each field of the tcp header of packet 27 are as follows :

Source Port (16 bits) : 443

Destination Port (16 bits) : 59138

Sequence Number (32 bits) : 24 (raw : 3056868986)

Acknowledgement Number (32 bits) : 1 (raw : 1084580465)

Data Offset (4 bits) : 5 (5 words = 5*4 bytes = 20 bytes)

Reserved (6 bits) : Reserved for future use and are set to 0

Flags (6 bits) :

URG : 0

ACK : 1 (indicates that the Acknowledgment field is significant. All packets after the initial SYN packet sent by the client should have this flag set.)

PSH : 0

RST : 0

SYN : 0

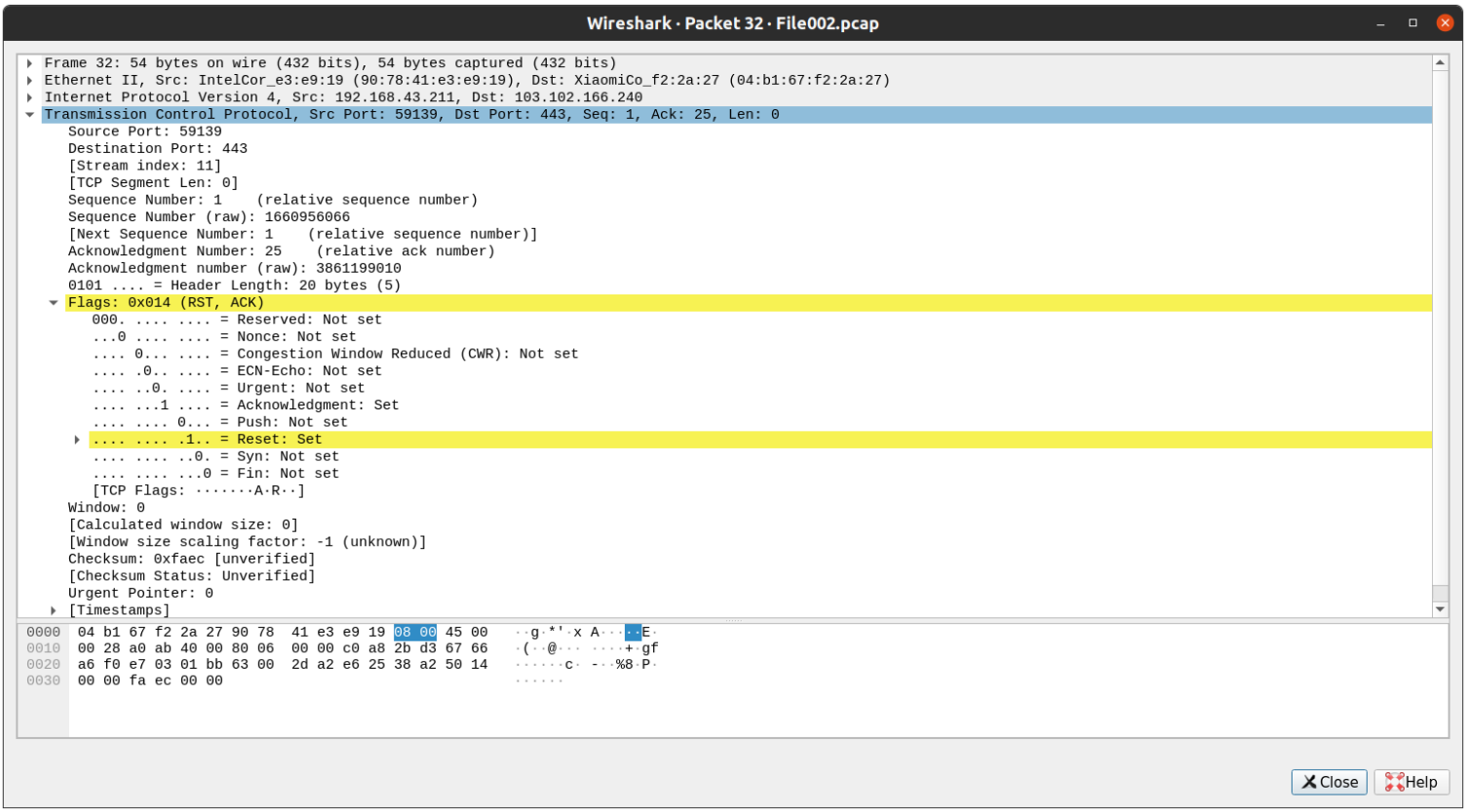
FIN : 1 (indicates that no more data is sent from the sender)

Window Size (16 bits) : 60

Checksum (16 bits) : 21570 (hex: 0x5442)

Urgent Pointer (16 bits) : 0

Packet 32



59139								443
1660956066								
3861199010								
0101		0	1	0	1	0	0	0
0xfaec								0

The values in each field of the tcp header of packet 32 are as follows :

Source Port (16 bits) : 59139

Destination Port (16 bits) : 443

Sequence Number (32 bits) : 1 (raw : 1660956066)

Acknowledgement Number (32 bits) : 25 (raw : 3861199010)

Data Offset (4 bits) : 5 (5 words = 5*4 bytes = 20 bytes)

Reserved (6 bits) : Reserved for future use and are set to 0

Flags (6 bits) :

URG : 0

ACK : 1

PSH : 0

RST : 1 (Resets the connection. Used only when there is no chance of terminating TCP connection normally or there are unrecoverable errors)

SYN : 0

FIN : 0

Window Size (16 bits) : 0

Checksum (16 bits) : 64236 (hex: 0xfaec)

Urgent Pointer (16 bits) : 0