GUNTUPALLI SUDHARSHAN

B190512CS

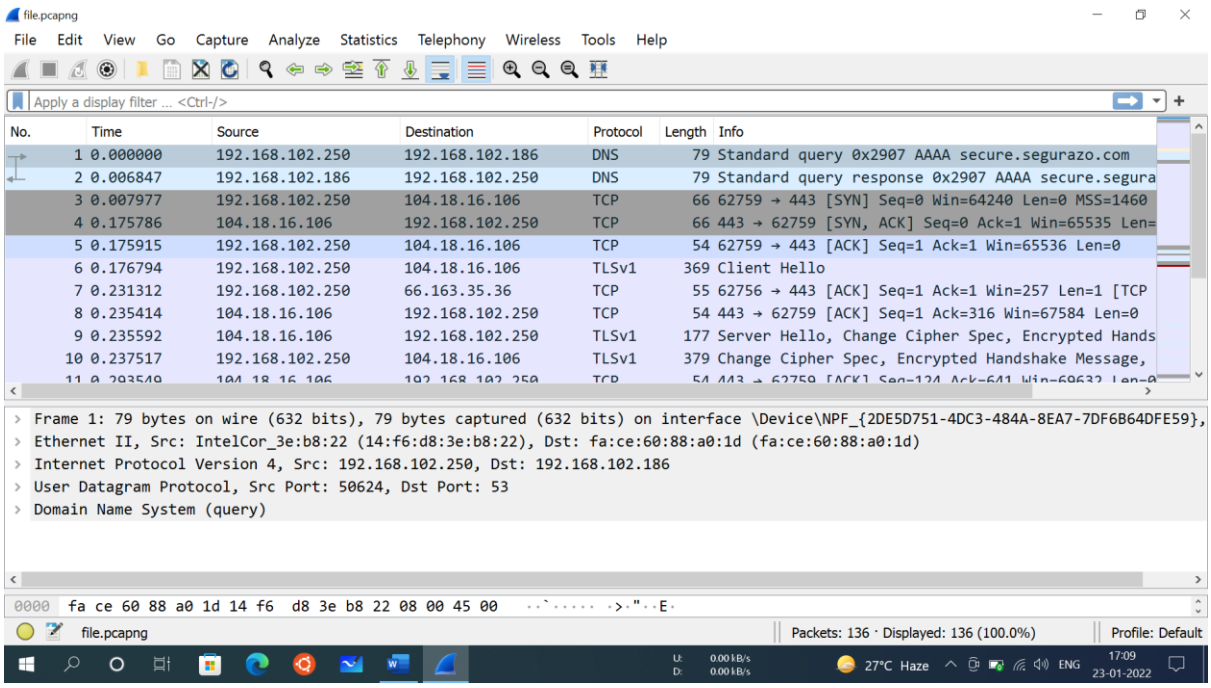
CSE A BATCH

Networks Lab Assignment 2

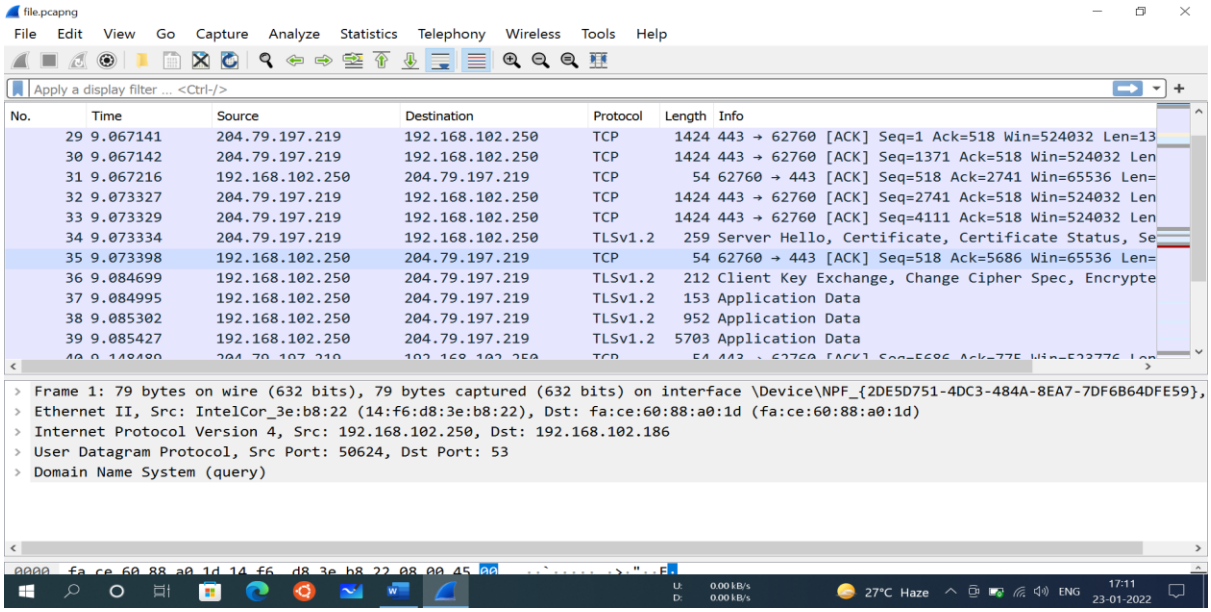
The assignment introduces packet sniffer, Wireshark. Wireshark is a free open source network protocol analyzer. It is used for network troubleshooting and communication protocol analysis. Wireshark captures network packets in real time and display them in human-readable format. It provides many advanced features including live capture and offline analysis, three-pane packet browser, coloring rules for analysis. Wireshark can be downloaded from the location https://www.wireshark.org/download.html

1.Executed the given command while running wireshark parallelly and captured packets and saved the file in the laptop.

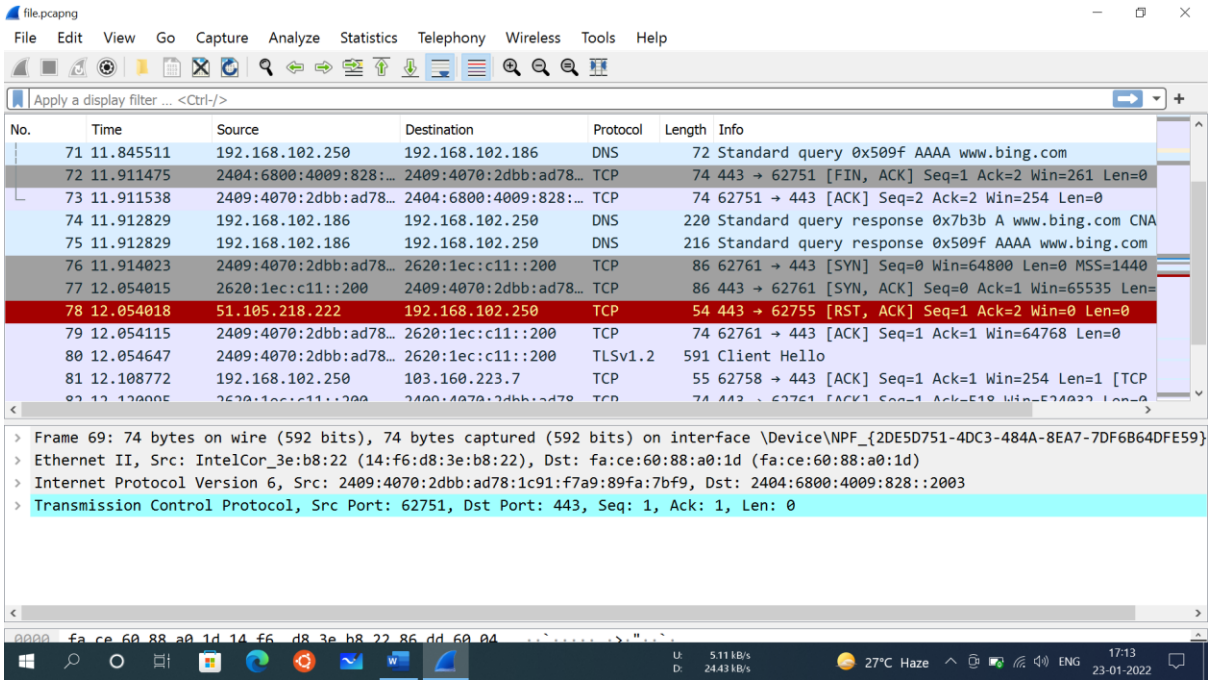
For this download our laptop might setup multiple tcp connections to given web server,for to filter all packets of a particular tcp connection right click on any packet of that tcp connection and select conversation filter and select tcp.will display only packets of that particular tcp connection.very useful filter to analyse the tcp connection separately without other packets in middle.



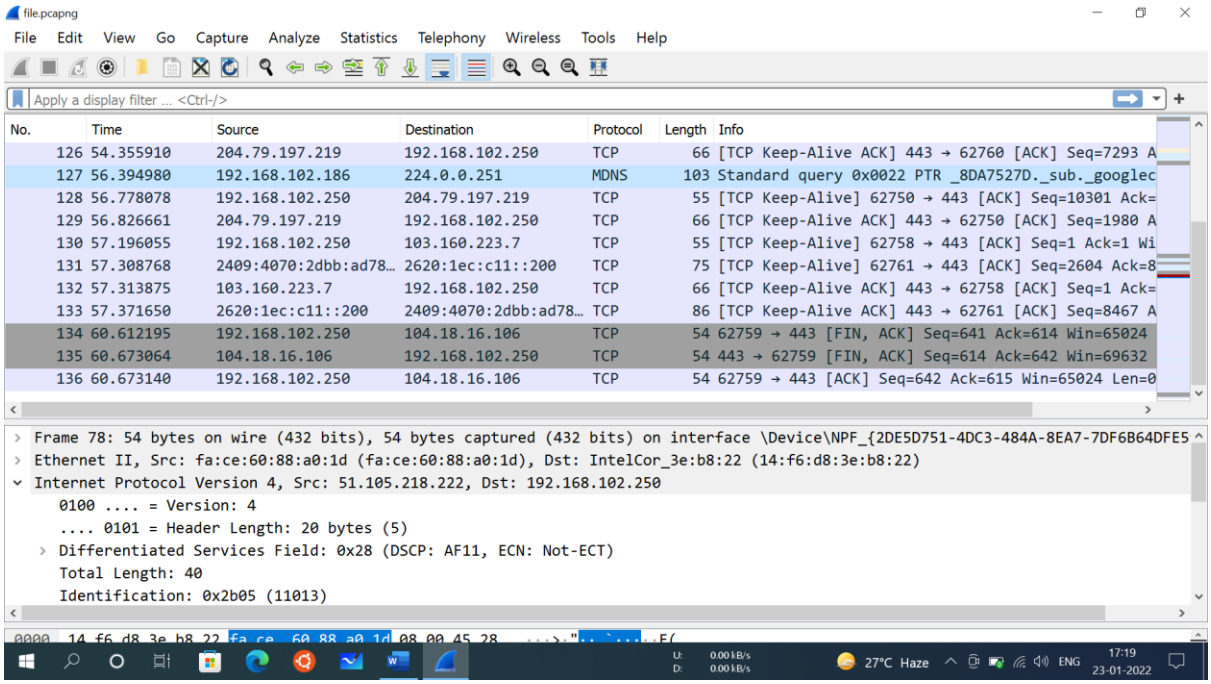
The download started with finding ip address of given web server using dns protocol at application layer and subsequently 3-way handshake for establishing tcp connection to web server.



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.



After receiving whole pdf tcp connection terminated using flags such as fin,ack.

This download used https at application layer,TCP at transport layer,IPV4 at network layer mainly.Given URL contains “https”+”web server domain name”+”location of pdf”.

2.

User has made a connection to an unsecure website(web server) and user has sent his confidential information to web server through a html form over plaintext with no encryption at all mistakenly.

We can observe that user application has used http protocol at application layer and since the credentials are sent from user to web server and packets are captured from user system definitely the credentials packets must use the http post method.In the given file001.pcap only one packet(540th packet) uses http post method as shown in the info section of wire shark of that particular packet.

a.

540th packet in the given file uses http post method and contains credentials information

src ip address of 540th packet=192.168.44.53

dest ip address of 540th packet=192.168.44.1

both are private ipv4 addresses so may be NAT is in use for this communication.

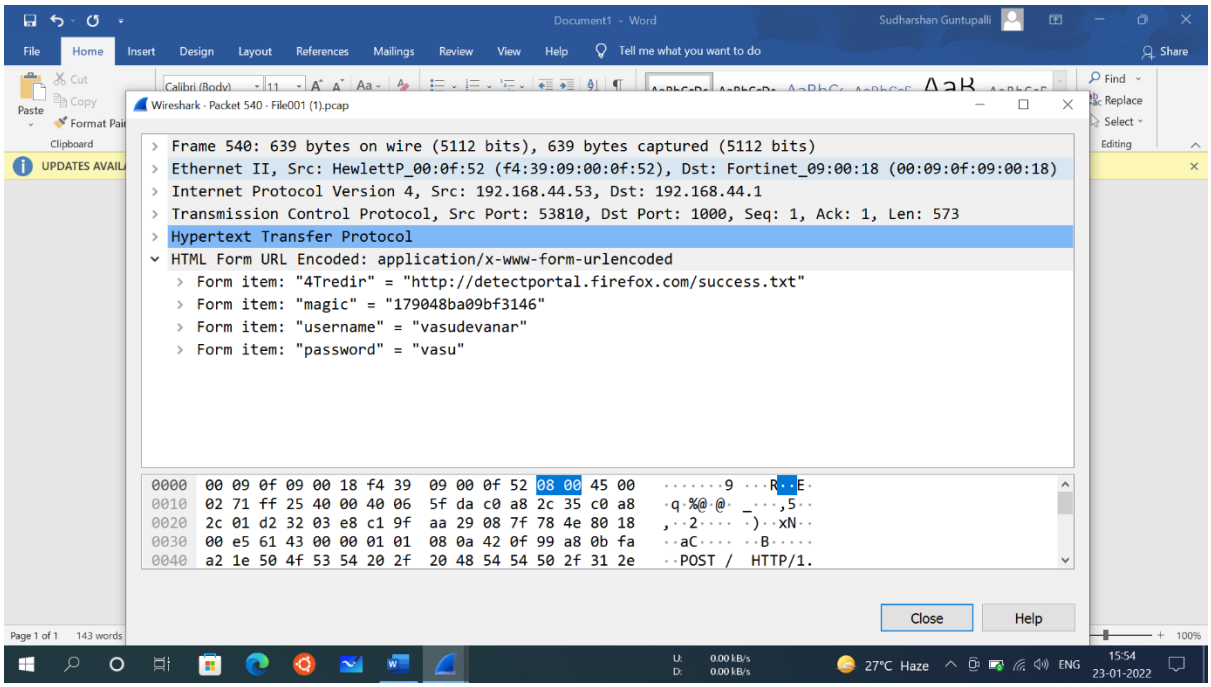
b.

540th packet uses ipv4 at network layer,tcp at transport layer,http post method at application layer.

c.

login credentials: username=”vasudevanar” password=”vasu”

username and password are separately shown in wireshark software may be because these credentials are sent as a html form and they can be opened by wireshark if no encryption is present.(I think so not sure).



3.

a)27th packet tcp header details in given file002.pcap:

Src port=443(110111011)

Dest port=59138(1110011100000010)

Sequence number(raw)= 3056868986(10110110001101000001111001111010)

Acknowledgement number(raw)= 1084580465(10000001010010101100010011100001)

Data offset(header length)=5(0101)(20 bytes)

Reserved(6 bits)=000000

Urg flag=0

Ack flag=1

Psh flag=0

Rst flag=0

Syn flag=0

Fin flag=1

Window size=60(111100)

Checksum=0x5442(0101010001000010)

Urgent pointer=0(0000000000000000)

Options=timestamps are mentioned

b)32nd packet tcp header details in given file002.pcap:

Src port=59139(1110011100000011)

Dest port=443(11011101)

Sequence number(raw)=1660956066(11000110000000000101101101000010)

Acknowledgement number(raw)= 3861199016(11100110001001010011100010101000)

Data offset(header length)=5(0101)(20 bytes)

Reserved(6 bits)=000000

Urg flag=0

Ack flag=1

Psh flag=0

Rst flag=1

Syn flag=0

Fin flag=0

Window size=0(0000000000000000)

Checksum=0xfaec(1111101011101100)

Urgent pointer=0(0000000000000000)

Options=timestamps are mentioned.

*For sequence number and acknowledgement fields raw values should be considered,relative values are just given by wireshark software for the user convienience to analyse the packets easily.

*Data offset is same as header length in tcp header.

*Asked header details only so options and data is not shown properly by wireshark software.

*checksum is generally given in hexadecimal by wireshark software.

*in assignment pdf it is indirectly mentioned that reserved is 6 bits however 3 bits are utilised for nonce flag,congestion window reduced(CWR) flag,echo(ECH) flag nowadays.