

GUNTUPALLI SUDHARSHAN

B190512CS

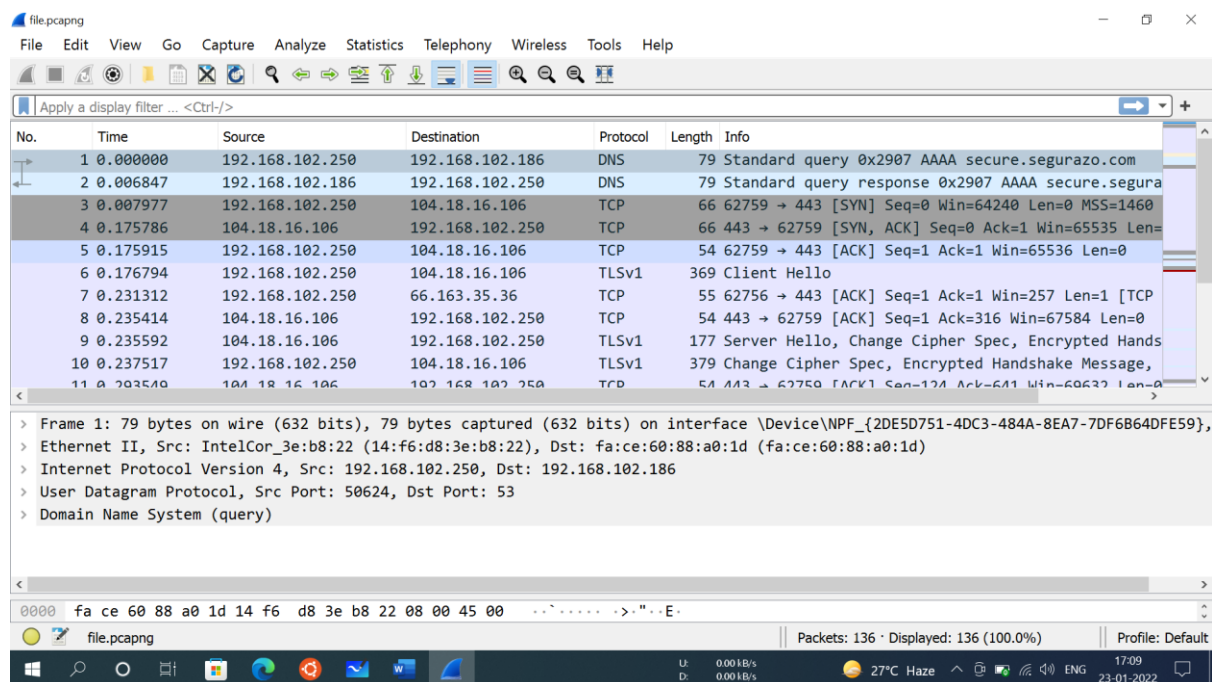
CSE A BATCH

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.

file.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
29	9.067141	204.79.197.219	192.168.102.250	TCP	1424	443 → 62760 [ACK] Seq=1 Ack=518 Win=524032 Len=13
30	9.067142	204.79.197.219	192.168.102.250	TCP	1424	443 → 62760 [ACK] Seq=1371 Ack=518 Win=524032 Len=
31	9.067216	192.168.102.250	204.79.197.219	TCP	54	62760 → 443 [ACK] Seq=518 Ack=2741 Win=65536 Len=
32	9.073327	204.79.197.219	192.168.102.250	TCP	1424	443 → 62760 [ACK] Seq=2741 Ack=518 Win=524032 Len=
33	9.073329	204.79.197.219	192.168.102.250	TCP	1424	443 → 62760 [ACK] Seq=4111 Ack=518 Win=524032 Len=
34	9.073334	204.79.197.219	192.168.102.250	TLSv1.2	259	Server Hello, Certificate, Certificate Status, Se
35	9.073398	192.168.102.250	204.79.197.219	TCP	54	62760 → 443 [ACK] Seq=518 Ack=5686 Win=65536 Len=
36	9.084699	192.168.102.250	204.79.197.219	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypte
37	9.084995	192.168.102.250	204.79.197.219	TLSv1.2	153	Application Data
38	9.085302	192.168.102.250	204.79.197.219	TLSv1.2	952	Application Data
39	9.085427	192.168.102.250	204.79.197.219	TLSv1.2	5703	Application Data

> Frame 1: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface \Device\NPF_{2DE5D751-4DC3-484A-8EA7-7DF6B64DFE59}, Ethernet II, Src: IntelCor_3e:b8:22 (14:f6:d8:3e:b8:22), Dst: fa:ce:60:88:a0:1d (fa:ce:60:88:a0:1d)
 > Internet Protocol Version 4, Src: 192.168.102.250, Dst: 192.168.102.186
 > User Datagram Protocol, Src Port: 50624, Dst Port: 53
 > Domain Name System (query)

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.

file.pcapng

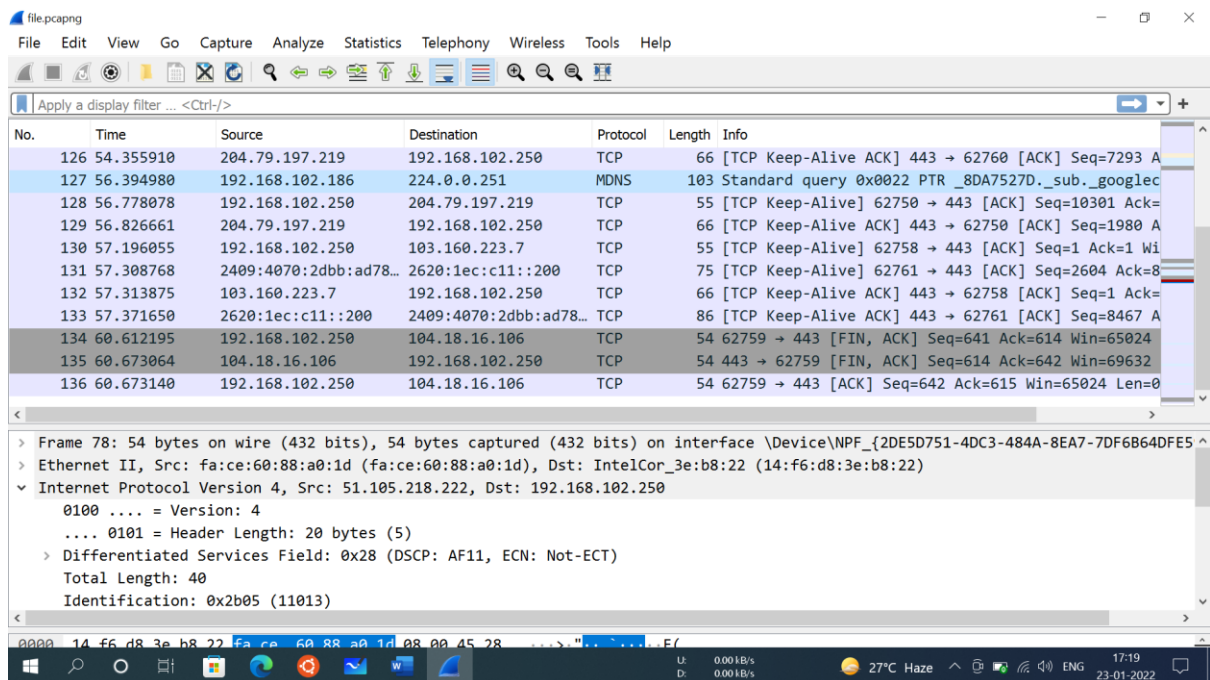
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
71	11.845511	192.168.102.250	192.168.102.186	DNS	72	Standard query 0x509f AAAA www.bing.com
72	11.911475	2404:6800:4009:828:...	2409:4070:2dbb:ad78:...	TCP	74	443 → 62751 [FIN, ACK] Seq=1 Ack=2 Win=261 Len=0
73	11.911538	2409:4070:2dbb:ad78:...	2404:6800:4009:828:...	TCP	74	62751 → 443 [ACK] Seq=2 Ack=2 Win=254 Len=0
74	11.912829	192.168.102.186	192.168.102.250	DNS	220	Standard query response 0x7b3b A www.bing.com CNA
75	11.912829	192.168.102.186	192.168.102.250	DNS	216	Standard query response 0x509f AAAA www.bing.com
76	11.914023	2409:4070:2dbb:ad78:...	2620:1ec:c11::200	TCP	86	62761 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440
77	12.054015	2620:1ec:c11::200	2409:4070:2dbb:ad78:...	TCP	86	443 → 62761 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=
78	12.054018	51.105.218.222	192.168.102.250	TCP	54	443 → 62755 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
79	12.054115	2409:4070:2dbb:ad78:...	2620:1ec:c11::200	TCP	74	62761 → 443 [ACK] Seq=1 Ack=1 Win=64768 Len=0
80	12.054647	2409:4070:2dbb:ad78:...	2620:1ec:c11::200	TLSv1.2	591	Client Hello
81	12.108772	192.168.102.250	103.160.223.7	TCP	55	62758 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1 [TCP

> Frame 69: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{2DE5D751-4DC3-484A-8EA7-7DF6B64DFE59}
 > Ethernet II, Src: IntelCor_3e:b8:22 (14:f6:d8:3e:b8:22), Dst: fa:ce:60:88:a0:1d (fa:ce:60:88:a0:1d)
 > Internet Protocol Version 6, Src: 2409:4070:2dbb:ad78:1c91:f7a9:89fa:7bf9, Dst: 2404:6800:4009:828::2003
 > Transmission Control Protocol, Src Port: 62751, Dst Port: 443, Seq: 1, Ack: 1, Len: 0

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.

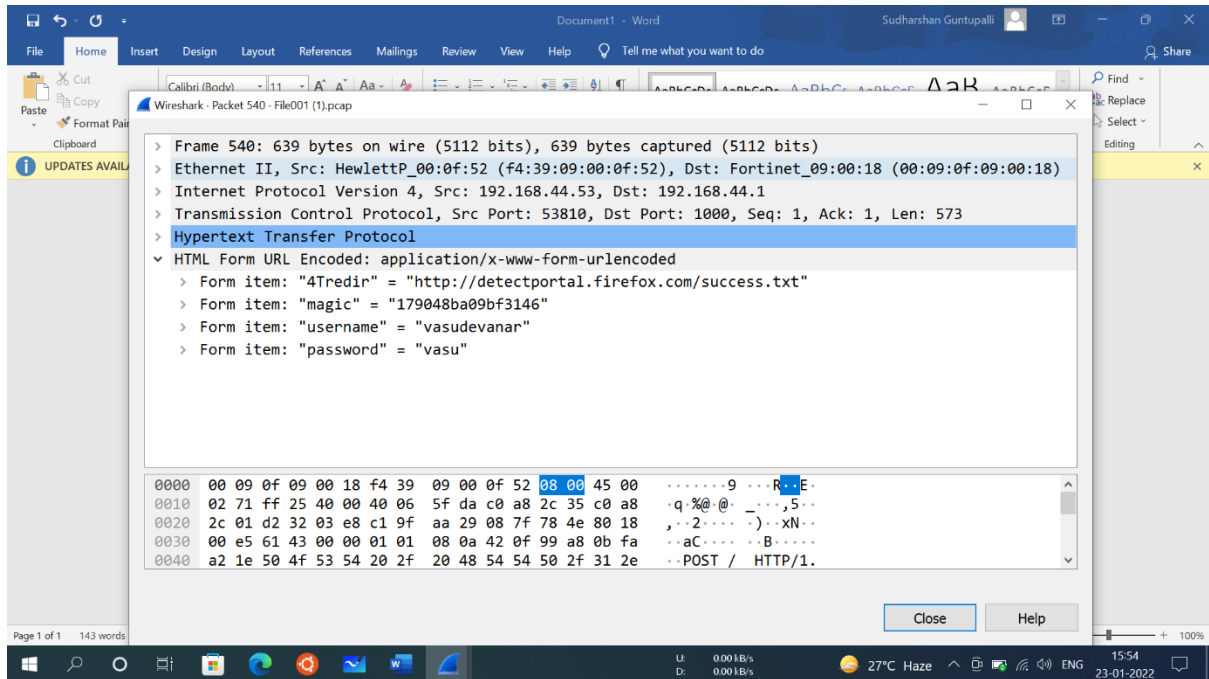
b.

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(1000000101001010110001001110001)

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(1100011000000000010110110100010)

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 convenience 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.