

CS3093D: Networks Lab

Assignment – II

Hanna Nechikkadan
B190420CS
NIT Calicut
22/01/2022

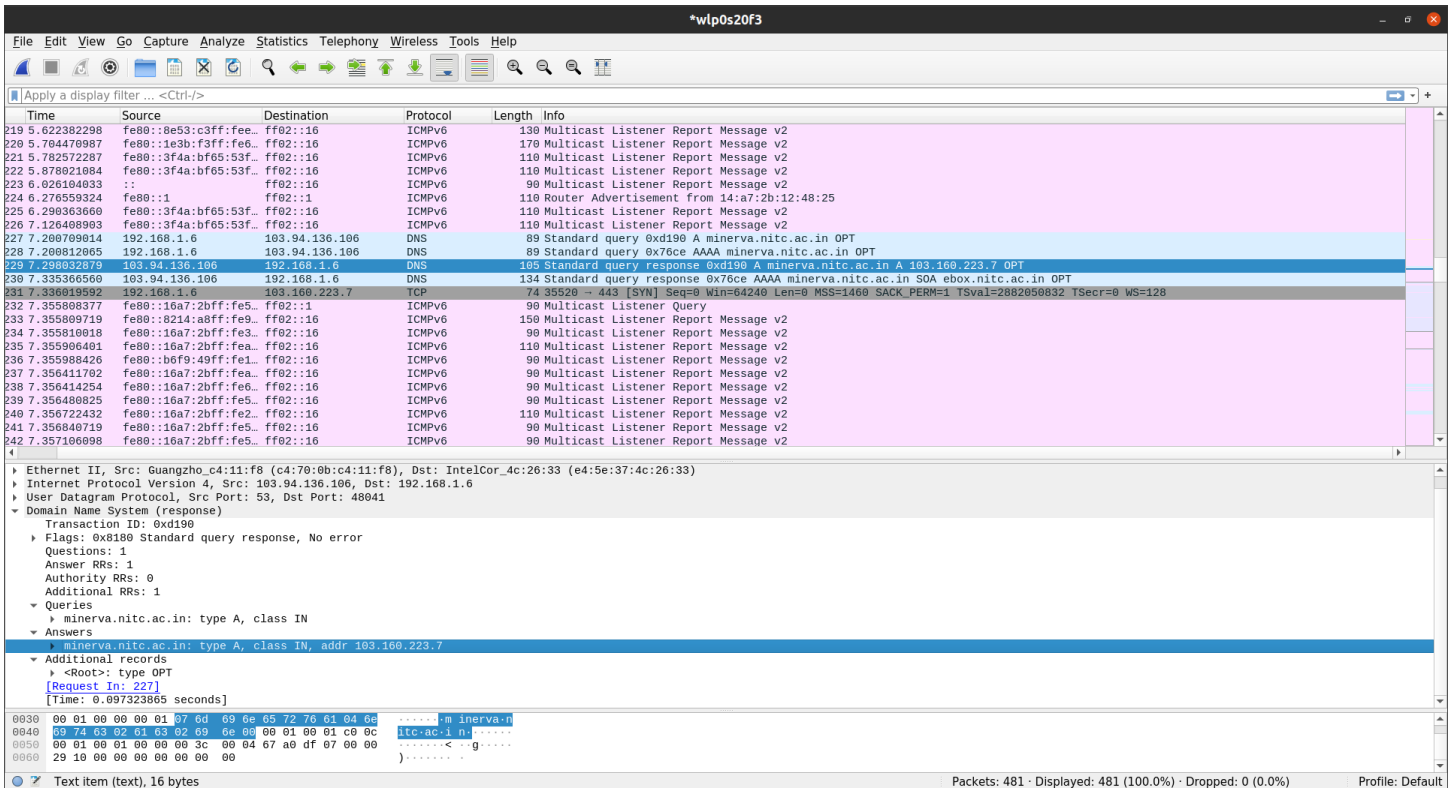
CONTENTS

1. [Question 1 and Answers](#)

2. [Question 2 and Answers](#)

3. [Question 3 and Answers](#)

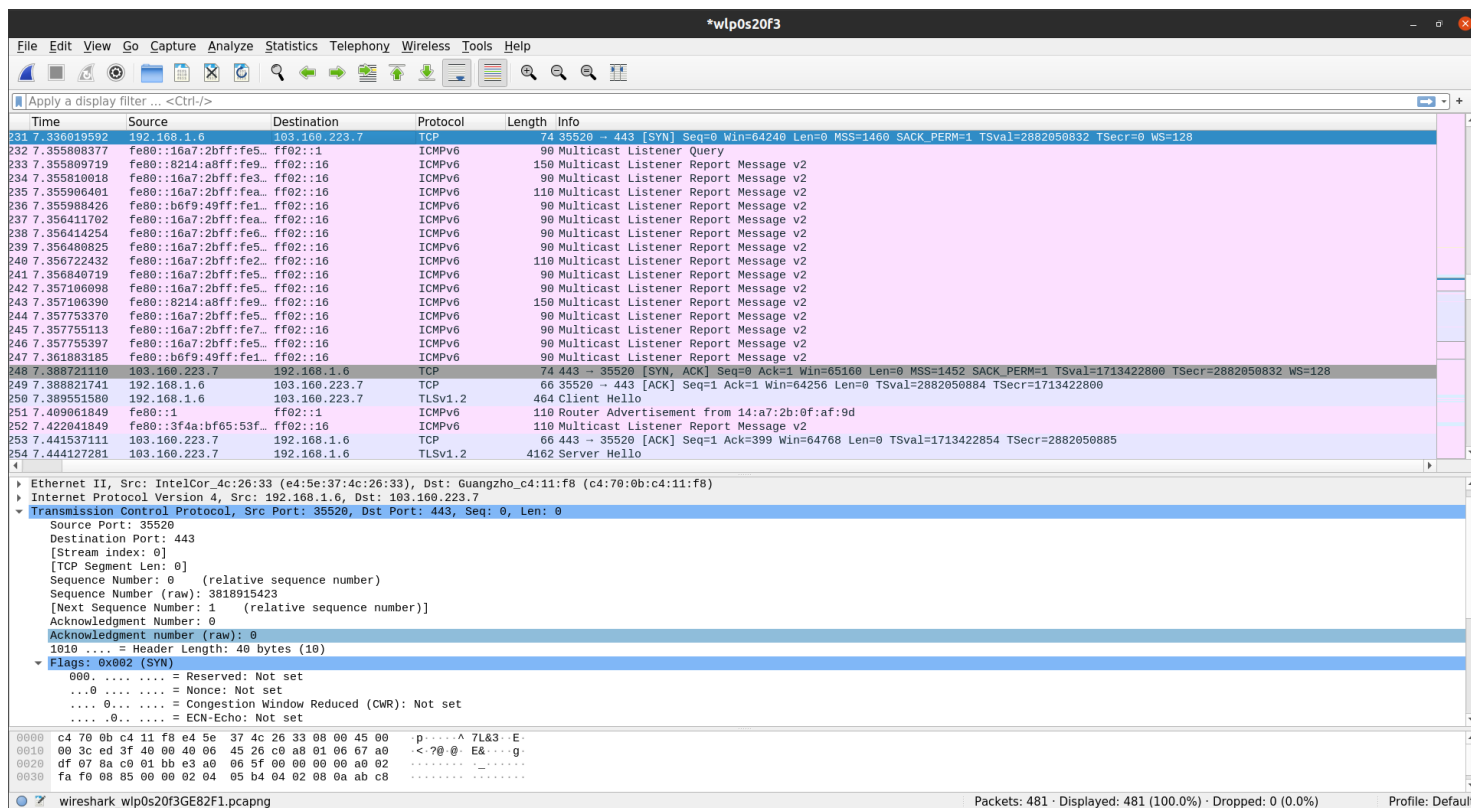
1. Execute the following command in the terminal,
wget
https://minerva.nitc.ac.in/sites/default/files/attachments/news/TT_Winter2021-2022%20%281%29.pdf
 Parallely run the wireshark tool. Note down your network analysis of the command.



- 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.

Wireshark capture of a TLS handshake on interface wlp0s20f3. The packet list shows frames 250 through 272. Frame 250 is a Client Hello (464 bytes). Frames 254, 256, 258, and 259 show the server's response, including a Certificate (442 bytes), Change Cipher Spec (117 bytes), and Encrypted Handshake Message (11586 bytes). The packet details for frame 250 show the Client Hello structure: Source Port: 35520, Destination Port: 443, Sequence Number: 1, Acknowledgment Number: 1, and Flags: PSH, ACK.

- 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.

The screenshot shows a Wireshark packet capture on interface wlp0s20f3. The packet list shows a series of TCP segments. Packet 275 is selected, showing details of a TCP segment with the ACK flag set. The packet bytes show the raw data of the segment.

Time	Source	Destination	Protocol	Length	Info
279.7664123467	192.168.223.7	192.168.1.6	TLSv1.2	7266	Application Data [TCP segment of a reassembled PDU]
280.7664158066	192.168.1.6	192.168.223.7	TCP	66	35520 → 443 [ACK] Seq=735 Ack=57804 Win=84352 Len=0 TSval=2882051160 TSecr=1713423075
281.7665343658	192.168.223.7	192.168.1.6	TCP	7266	443 → 35520 [ACK] Seq=57804 Ack=735 Win=64640 Len=7200 TSval=1713423075 TSecr=2882051160 [TCP segment of a reassembled PDU]
282.7665381411	192.168.1.6	192.168.223.7	TCP	66	35520 → 443 [ACK] Seq=735 Ack=65004 Win=98688 Len=0 TSval=2882051161 TSecr=1713423075
283.7665344200	192.168.223.7	192.168.1.6	TCP	2946	443 → 35520 [ACK] Seq=65004 Ack=735 Win=64640 Len=2880 TSval=1713423076 TSecr=2882051160 [TCP segment of a reassembled PDU]
284.7665420095	192.168.1.6	192.168.223.7	TCP	66	35520 → 443 [ACK] Seq=735 Ack=67884 Win=104448 Len=0 TSval=2882051161 TSecr=1713423076
285.7667523941	192.168.223.7	192.168.1.6	TLSv1.2	2946	Application Data [TCP segment of a reassembled PDU]
286.7667577813	192.168.1.6	192.168.223.7	TCP	66	35520 → 443 [ACK] Seq=735 Ack=70764 Win=110208 Len=0 TSval=2882051163 TSecr=1713423076
287.7667524344	192.168.223.7	192.168.1.6	TCP	11586	443 → 35520 [ACK] Seq=70764 Ack=735 Win=64640 Len=11520 TSval=1713423076 TSecr=2882051160 [TCP segment of a reassembled PDU]
288.7667627047	192.168.1.6	192.168.223.7	TCP	66	35520 → 443 [ACK] Seq=735 Ack=82284 Win=133248 Len=0 TSval=2882051163 TSecr=1713423076
289.7667639076	192.168.223.7	192.168.1.6	TCP	1506	443 → 35520 [ACK] Seq=82284 Ack=735 Win=64640 Len=1440 TSval=1713423077 TSecr=2882051160 [TCP segment of a reassembled PDU]
290.7667648187	192.168.1.6	192.168.223.7	TCP	66	35520 → 443 [ACK] Seq=735 Ack=83724 Win=136192 Len=0 TSval=2882051163 TSecr=1713423077
291.7668858238	192.168.223.7	192.168.1.6	TCP	1506	443 → 35520 [ACK] Seq=83724 Ack=735 Win=64640 Len=1440 TSval=1713423077 TSecr=2882051160 [TCP segment of a reassembled PDU]
292.7668915948	192.168.1.6	192.168.223.7	TCP	66	35520 → 443 [ACK] Seq=735 Ack=85164 Win=139008 Len=0 TSval=2882051165 TSecr=1713423077
293.7668858087	192.168.223.7	192.168.1.6	TLSv1.2	17346	Application Data [TCP segment of a reassembled PDU]
294.7668976450	192.168.1.6	192.168.223.7	TCP	66	35520 → 443 [ACK] Seq=735 Ack=102444 Win=173568 Len=0 TSval=2882051165 TSecr=1713423078
295.7692538369	fe80::e21c:fcff:fea...	ff02::16	ICMPv6	130	Multicast Listener Report Message v2
296.766883974	192.168.223.7	192.168.1.6	TLSv1.2	4386	Application Data [TCP segment of a reassembled PDU]
297.766732064	192.168.1.6	192.168.223.7	TCP	66	35520 → 443 [ACK] Seq=735 Ack=106764 Win=182272 Len=0 TSval=2882051212 TSecr=1713423128
298.766869337	192.168.223.7	192.168.1.6	TCP	4386	443 → 35520 [ACK] Seq=106764 Ack=735 Win=64640 Len=4320 TSval=1713423128 TSecr=2882051160 [TCP segment of a reassembled PDU]
299.7668101733	192.168.1.6	192.168.223.7	TCP	66	35520 → 443 [ACK] Seq=735 Ack=111084 Win=190848 Len=0 TSval=2882051214 TSecr=1713423128
300.766869624	192.168.223.7	192.168.1.6	TCP	1506	443 → 35520 [ACK] Seq=111084 Ack=735 Win=64640 Len=1440 TSval=1713423129 TSecr=2882051160 [TCP segment of a reassembled PDU]
301.7668140073	192.168.1.6	192.168.223.7	TCP	66	35520 → 443 [ACK] Seq=735 Ack=112524 Win=193792 Len=0 TSval=2882051214 TSecr=1713423129
302.766832891	192.168.223.7	192.168.1.6	TCP	1506	443 → 35520 [PSH, ACK] Seq=112524 Ack=735 Win=64640 Len=1440 TSval=1713423129 TSecr=2882051160 [TCP segment of a reassembled PDU]

Frame 275: 7266 bytes on wire (58128 bits), 7266 bytes captured (58128 bits) on interface wlp0s20f3, id 0
 Ethernet II, Src: Guangzho_c4:11:f8 (c4:70:0b:c4:11:f8), Dst: IntelCor_4c:26:33 (e4:5e:37:4c:26:33)
 Internet Protocol Version 4, Src: 192.168.223.7, Dst: 192.168.1.6
 Transmission Control Protocol, Src Port: 443, Dst Port: 35520, Seq: 40524, Ack: 735, Len: 7200
 Source Port: 443
 Destination Port: 35520
 [Stream index: 0]
 [TCP Segment Len: 7200]
 Sequence Number: 40524 (relative sequence number)
 Sequence Number (raw): 1691282174
 [Next Sequence Number: 47724 (relative sequence number)]
 Acknowledgment Number: 735 (relative ack number)
 Acknowledgment number (raw): 3818916158
 1000 = Header Length: 32 bytes (8)
 Flags: 0x010 (ACK)
 000. = Reserved: Not set
 ...0 = Nonce: Not set
0 = Congestion Window Reduced (CWR): Not set

0000 e4 5e 37 4c 26 33 c4 70 0b c4 11 f8 00 00 45 00 ..^L&3.p....E.
 0010 1c 54 7c 0b 40 00 38 06 a2 42 67 a0 df 07 0c a8 .T|@8..Bg....
 0020 01 06 01 bb 8a c0 64 ce ea fe e3 a0 09 3e 80 10d.....>..
 0030 01 f9 24 9d 00 00 01 01 08 0a 66 20 c2 af ab c8 ..\$.-----f....

- 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.

The image shows a Wireshark packet capture of a TCP connection termination. The packet list shows frames 314 and 337. Frame 314 is a FIN packet from 192.168.1.6 to 192.168.1.6. Frame 337 is an ACK packet from 192.168.1.6 to 192.168.1.6. The packet details for frame 314 show the FIN flag set. The packet details for frame 337 show the ACK flag set.

No.	Time	Source	Destination	Protocol	Length	Info
312	7.722036424	192.168.223.7	192.168.1.6	TLSv1.2	6969	Application Data
313	7.722069679	192.168.1.6	192.168.223.7	TCP	66	35520 → 443 [ACK] Seq=735 Ack=143907 Win=256512 Len=0 TSval=2882051218 TSecr=1713423132
314	7.724564439	192.168.1.6	192.168.223.7	TCP	66	35520 → 443 [FIN, ACK] Seq=735 Ack=143907 Win=256512 Len=0 TSval=2882051220 TSecr=1713423132
315	7.732467740	fe80::16a7:2bff:fe5...	ff02::1	ICMPv6	90	Multicast Listener Query
316	7.732503230	fe80::b6f9:49ff:fe1...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
317	7.732512533	fe80::16a7:2bff:fe3...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
318	7.732512726	fe80::8214:a8ff:fe9...	ff02::16	ICMPv6	150	Multicast Listener Report Message v2
319	7.732512832	fe80::16a7:2bff:fe5...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
320	7.732595364	fe80::8214:a8ff:fe9...	ff02::16	ICMPv6	150	Multicast Listener Report Message v2
321	7.732595522	fe80::16a7:2bff:fe8...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
322	7.734593761	fe80::4eae:1c7f:fe4...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
323	7.734596474	fe80::16a7:2bff:fe6...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
324	7.734596689	fe80::16a7:2bff:fe3...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
325	7.734599482	fe80::16a7:2bff:fe5...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
326	7.734600194	fe80::16a7:2bff:fe5...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
327	7.734599613	fe80::16a7:2bff:fe5...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
328	7.734599746	fe80::16a7:2bff:fe5...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
329	7.734627567	fe80::16a7:2bff:fea...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
330	7.734630822	fe80::16a7:2bff:fe7...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
331	7.734637350	fe80::16a7:2bff:fe5...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
332	7.736148099	fe80::16a7:2bff:feb...	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
333	7.736151253	fe80::16a7:2bff:fea...	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
334	7.736152510	fe80::b6f9:49ff:fe1...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
335	7.736153072	fe80::16a7:2bff:fe2...	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
336	7.736180771	fe80::16a7:2bff:fe5...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
337	7.776399587	192.168.223.7	192.168.1.6	TCP	66	443 → 35520 [FIN, ACK] Seq=143907 Ack=736 Win=64640 Len=0 TSval=1713423188 TSecr=2882051220
338	7.776471056	192.168.1.6	192.168.223.7	TCP	66	35520 → 443 [ACK] Seq=736 Ack=143908 Win=256512 Len=0 TSval=2882051272 TSecr=1713423188
339	7.776537004	fe80::9e9d:7eff:fe1...	ff02::16	ICMPv6	130	Multicast Listener Report Message v2
340	7.911554265	fe80::16a7:2bff:fe8...	ff02::1	ICMPv6	90	Multicast Listener Query

1000 = Header Length: 32 bytes (8)

Flags: 0x011 (FIN, ACK)

000. = Reserved: Not set

...0 = Nonce: Not set

...0 = Congestion Window Reduced (CWR): Not set

...0 = ECN-Echo: Not set

...0 = Urgent: Not set

...1 = Acknowledgment: Set

...0 = Push: Not set

...0 = Reset: Not set

...0 = Syn: Not set

...1 = Fin: Set

[TCP Flags:A...F]

0000 e4 5e 37 4c 26 33 c4 70 0b c4 11 f8 08 00 45 00 ^7L&3 pE-

0010 00 34 7c 53 40 00 38 06 be 1a 67 a0 df 07 c0 a8 4|S0 8g....

0020 01 06 01 bb 8a c0 84 d0 7e d5 e3 a0 09 3f 80 11B. ~....?..

0030 01 f9 9d 99 00 00 01 61 08 8a 66 20 c3 54 ab c8f .T...

wireshark_wlp0s20f3GE82f1.pcapng Packets: 481 · Displayed: 481 (100.0%) · Dropped: 0 (0.0%) Profile: Default

- 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.

The image shows a Wireshark network traffic capture of File001.pcap. The main display area shows a list of captured packets. Packet 540 is selected, which is an HTTP POST request to / HTTP/1.1 (application/x-www-form-urlencoded). The packet details pane shows the following structure:

- Frame 540: 639 bytes on wire (5112 bits), 639 bytes captured (5112 bits)
- Ethernet II, Src: HewlettP_00:0f:52 (f4:39:09:00:0f:52), Dst: Fortinet_09:00:18 (00:09:0f:09:00:18)
- Internet Protocol Version 4, Src: 192.168.44.53, Dst: 192.168.44.1
- Transmission Control Protocol, Src Port: 53810, Dst Port: 1000, Seq: 1, Ack: 1, Len: 573
- Hypertext Transfer Protocol
- HTML Form URL Encoded: application/x-www-form-urlencoded
 - Form item: "ifredir" = "http://detectportal.firefox.com/success.txt"
 - Form item: "magic" = "179048ba09bf3146"
 - Form item: "username" = "vasudevanar"
 - Form item: "password" = "vasu"

The packet bytes pane shows the raw data of the packet, with the form data being URL encoded. The status bar at the bottom indicates that 756 packets are displayed, with 31 (4.1%) of them being the selected packet.

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.

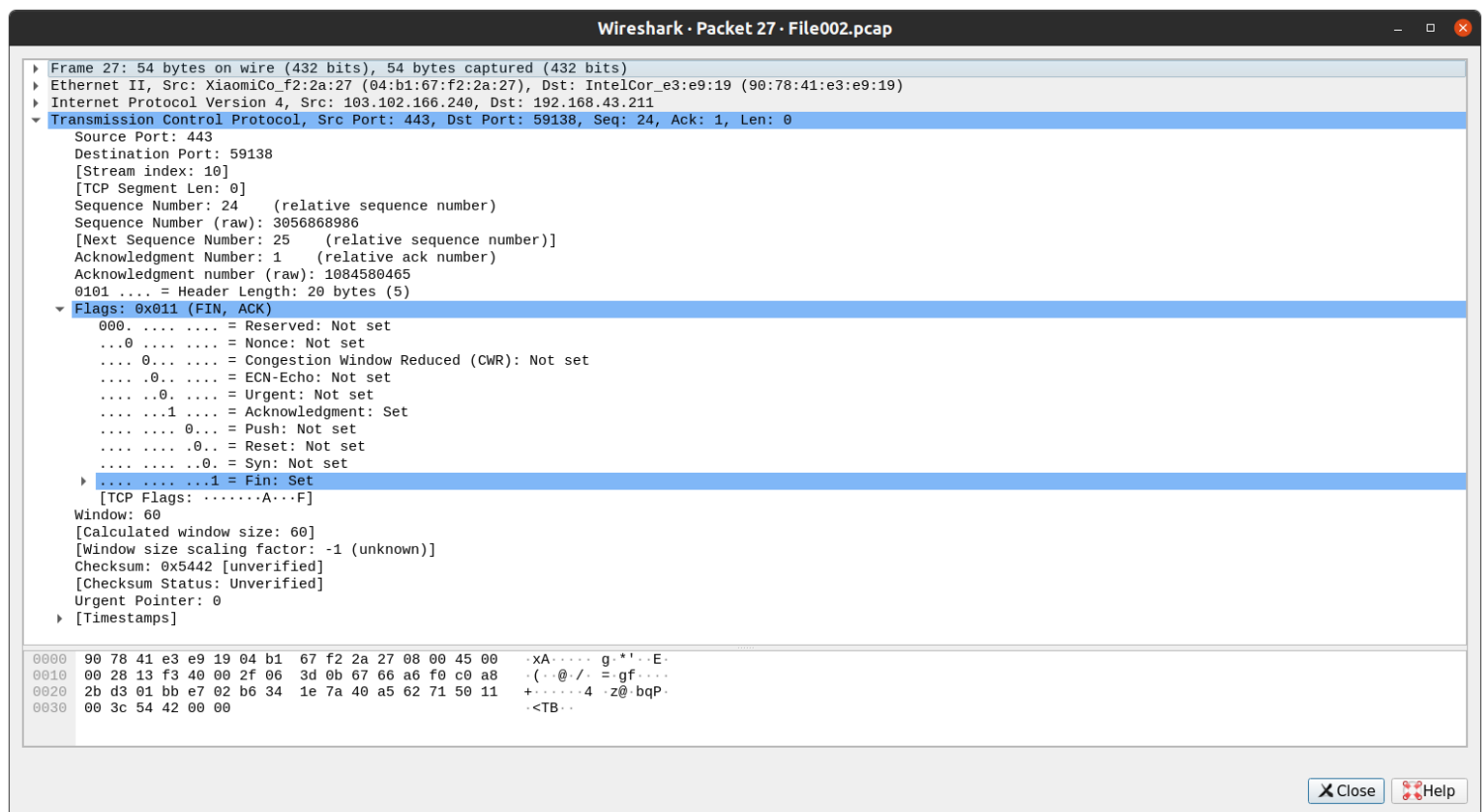
Ans. The protocol used to send the user credentials is HTTP (HyperText Transfer Protocol) as application layer protocol and is sent over TCP (Transmission Control Protocol) in the transport layer.

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

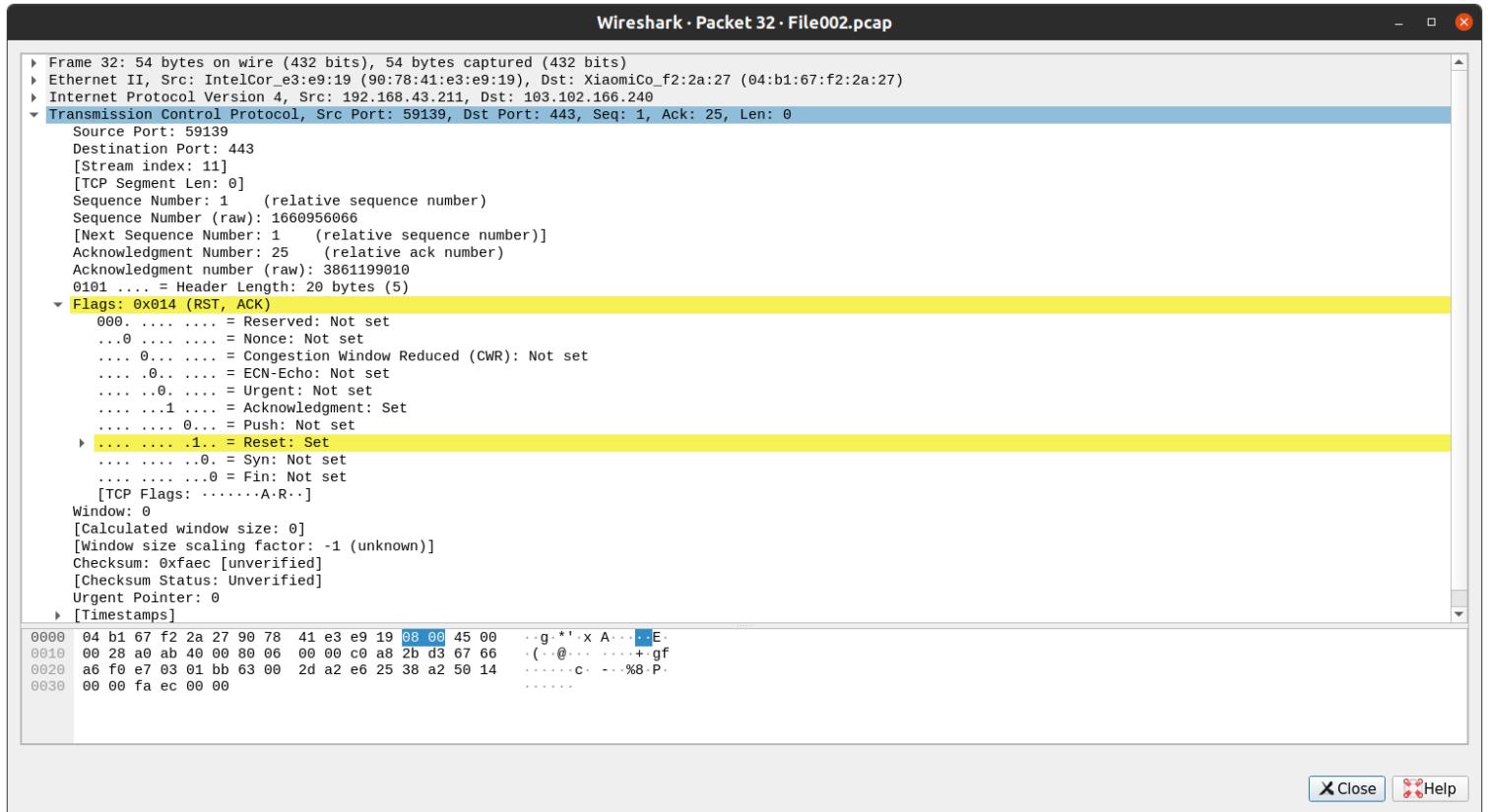
FIN : 1 (indicates that no more data is sent from the sender)

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