

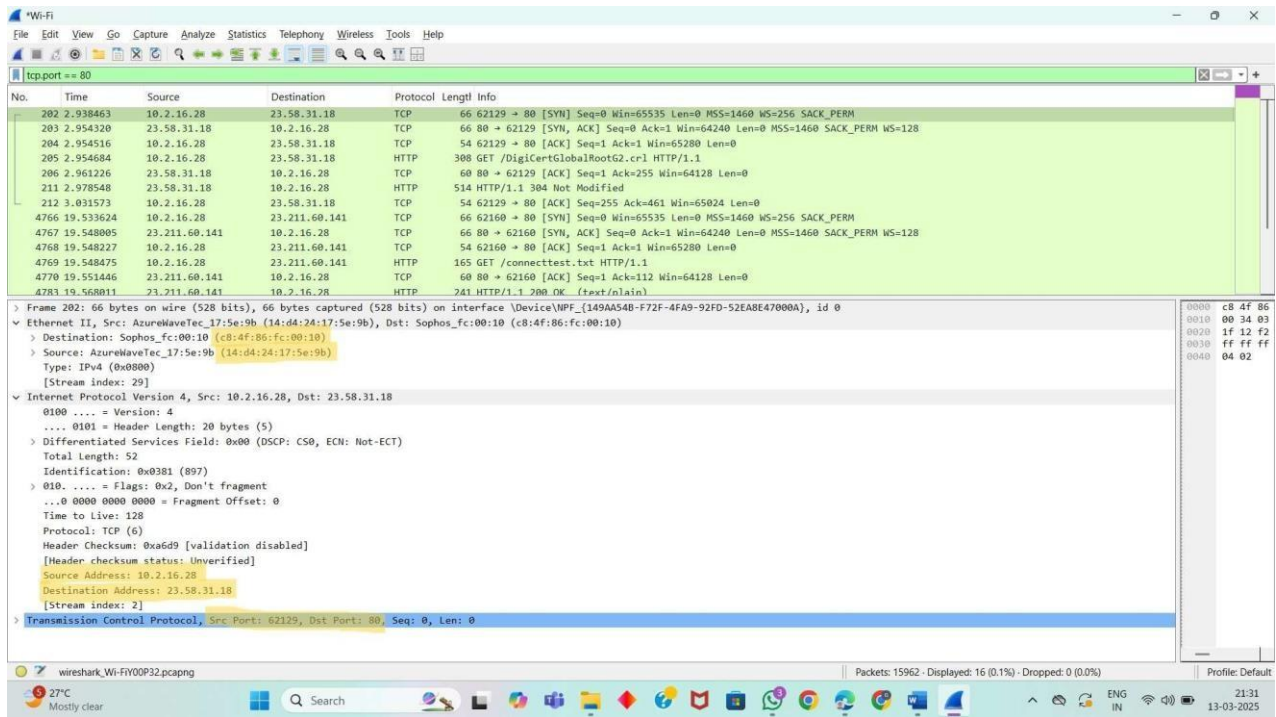
Register No:	99220040772
Name:	V Vishwaradhya
Class/Section :	9312/S24
Ex.No:	11b
Name of the Experiment	Capture and Analyzing TCP 3 way handshake
Google Drive link of the packet tracer file(give view permission):	https://drive.google.com/drive/folders/1KKvWcTv4dDyqVKTF9T6KLfM2asYIVCg?usp=sharing

1. Visit any one website by opening a browser fill your machine details.

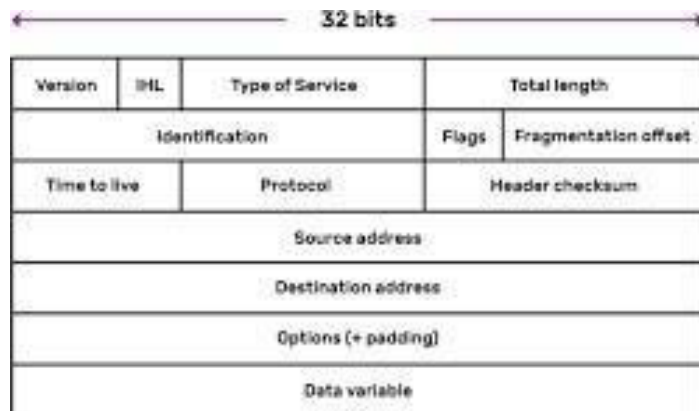
Parameter	Value
Your Machine IP Address.	10.2.16.28
Your Machine MAC Address	14:d4:24:17:5e:9b
Default Gateway address	10.2.0.1
Website URL	www.amazon.in
Website IP Address	23.58.31.18

2. Fill the following details:

Field Name	Field Length (no of bits)	Field value
Destination MAC address	48 bits	c8:4f:86:fc:00:10
Source MAC address	48 bits	14:d4:24:17:5e:9b
Destination IP address	32 bits	23.58.31.18
Source IP Address	32 bits	10.2.16.28
Destination TCP port	16 bits	80
Source TCP port	16 bits	62129

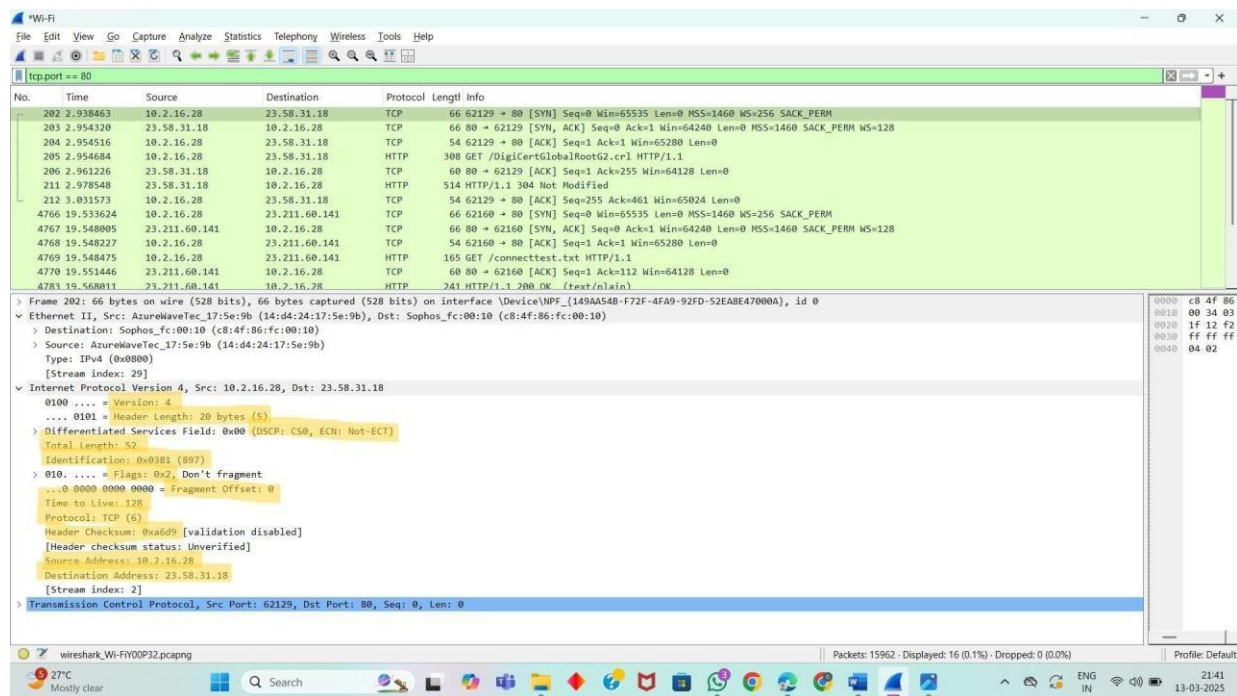


3. Fill the details as per the IP frame format .(highlight the details for each of the output and paste screenshot)

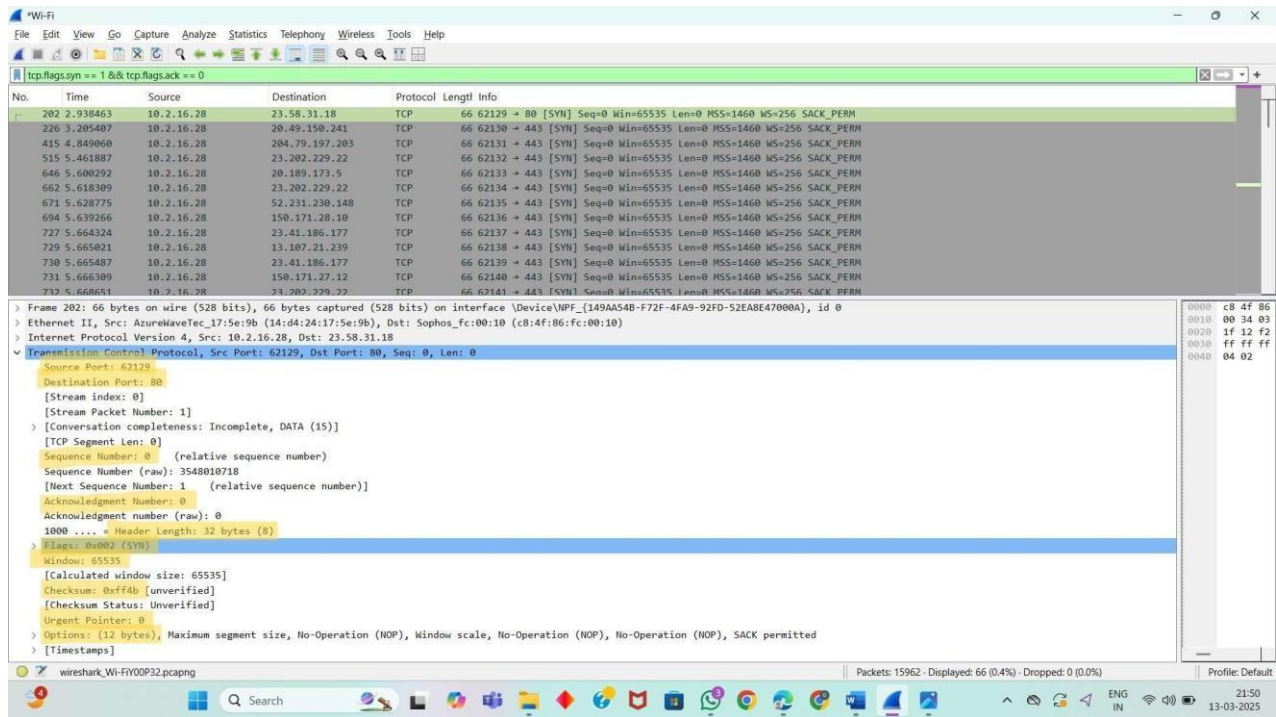


4	20 bytes	DSCP:CS0	52
0x0381 (897)		0x2	0

128	TCP (6)	0xa6d9
10.2.16.28		
23.58.31.18		
None		
None		

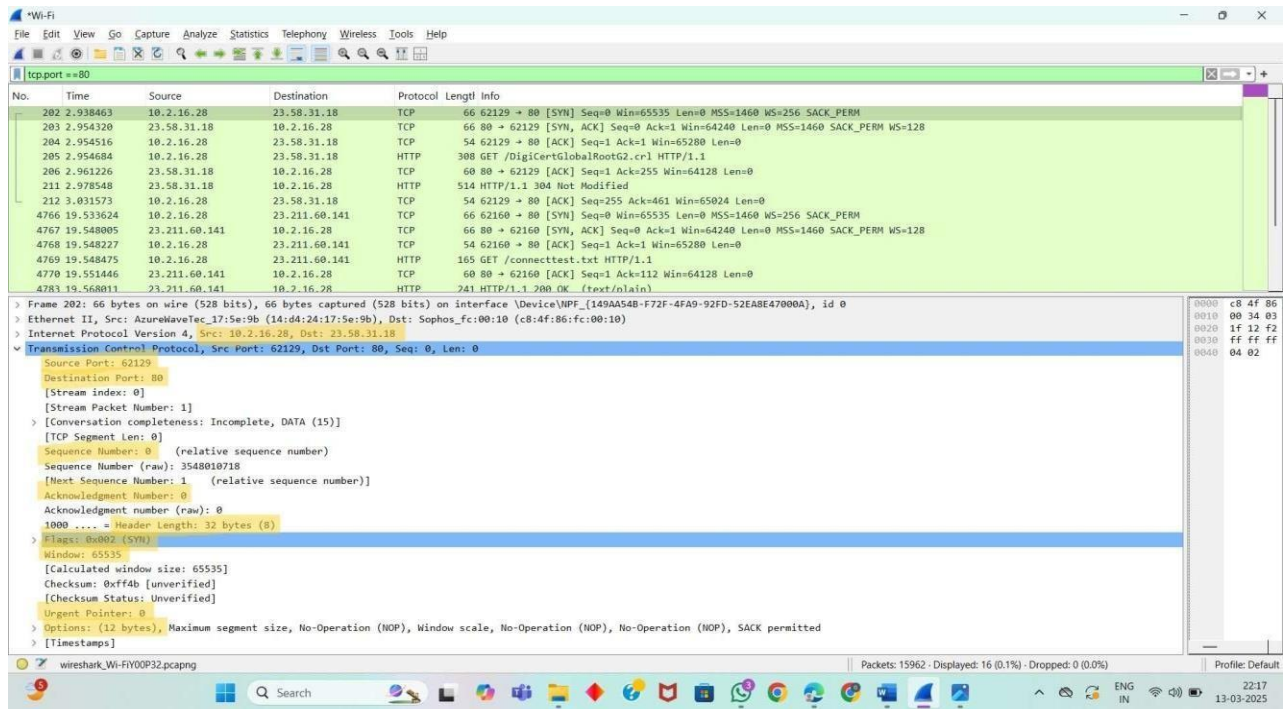


- Using the Wireshark capture of the first TCP session startup (SYN bit set to 1), fill in information about the TCP header. (paste screenshot for each of the output). Capture the packet and analyze it.



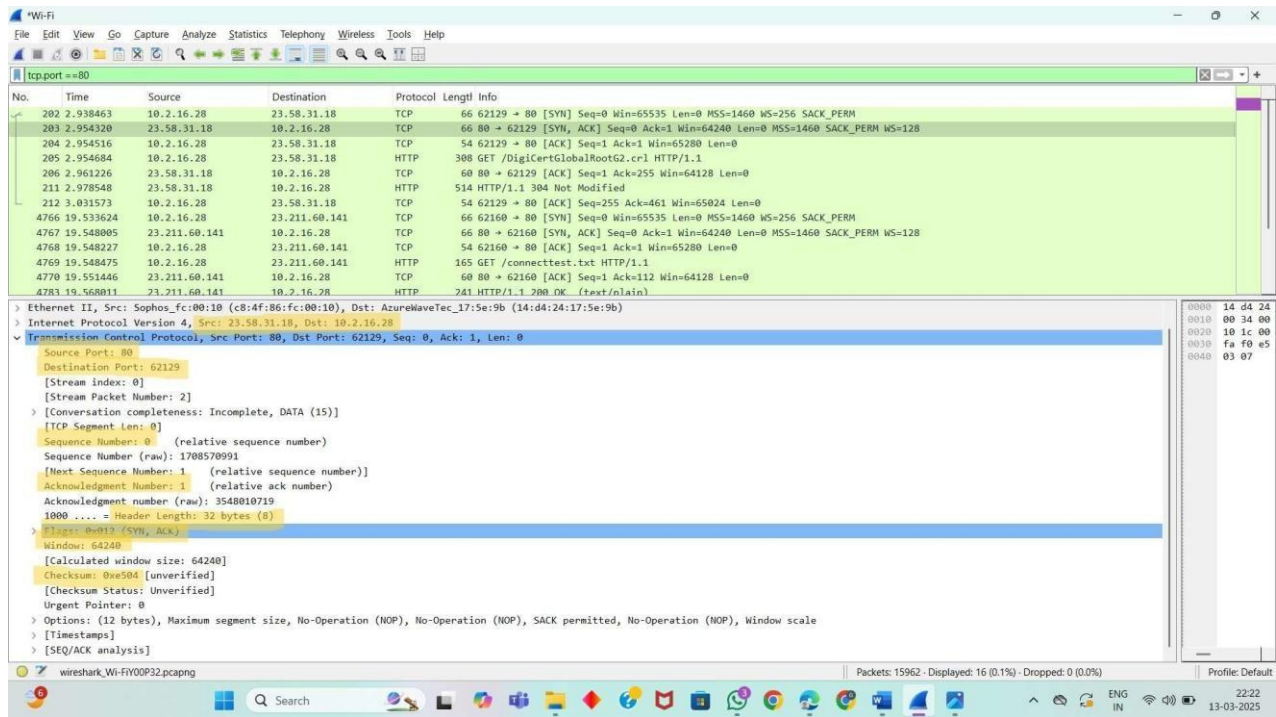
5. Fill in the following information regarding the SYN message. (highlight the details for each of the output and paste screenshot)

Source IP address	10.2.16.28
Destination IP address	23.58.31.18
Source port number	62129
Destination port number	80
Sequence number	0
Acknowledgement number	0
Flags	0x002 (SYN)
Header length	32 bytes (8)
Window size	65535
Checksum	0xff4b



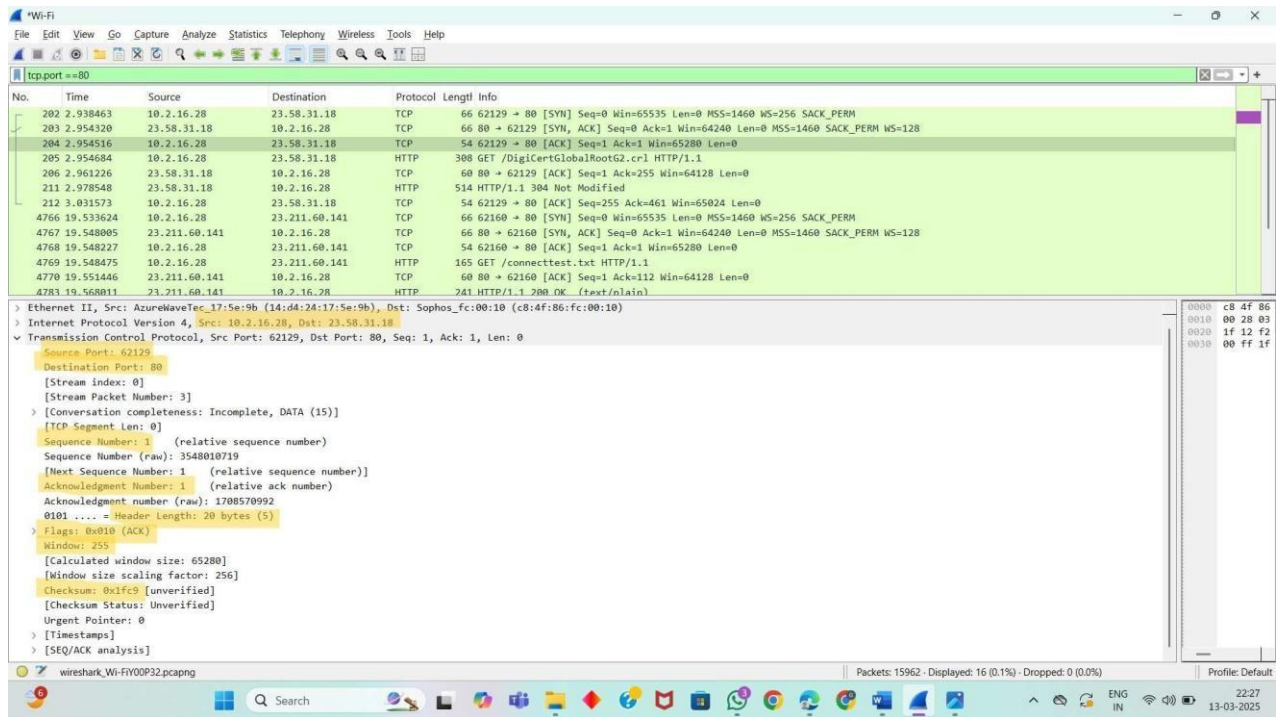
6. Fill in the following information regarding the SYN-ACK message (highlight the details for each of the output and paste screenshot)

Source IP address	23.58.31.18
Destination IP address	10.2.16.28
Source port number	80
Destination port number	62129
Sequence number	0
Acknowledgement number	1
Header length	32 bytes (8)
Window size	64240
Flags	0x012 (SYN, ACK)
Checksum	0xe504



7. Fill in the following information regarding the ACK message. (highlight the details for each of the output and paste screenshot)

Source IP address	10.20.16.28
Destination IP address	23.58.31.18
Source port number	62129
Destination port number	80
Sequence number	1
Acknowledgement number	1
Header length	20 bytes (5)
Window size	255
Flags	0x010 (ACK)
Checksum	0x1fc9



Rubrics for Wireshark labs: (To be Filled by the Class Teacher)

Rubrics	Excellent	Fair	Poor	Marks
Understanding (2)	Understand the Concept very well. (2)	Understand the Concept (1)	Poor Understand the Concept (0)	
Usage of filters (3)	Identified and applied the filter correctly (3)	Identified the filter, but not applied correctly (2-1)	Couldn't identify and apply the filter. Just captured the packets (1)	
Attach relevant Screenshots (3)	clearly Highlighted the answers and attached the screenshots (3)	attached the screenshots, but not highlighted. (2-1)	Did not attach the screenshots (0)	
On time Submission (2)	Early or on time submission (2)	Submitted after deadline (1)	Did not Submit (0)	
Total				