Register No:	**99220040772**
Name:	**V** **Vishwaradhya**
Class/Section:	**9312/S24**
Ex No:	**10**
Date of Submission	09-03-2025
Name of the Experiment	**Capture and Analyze TCP and IP packets**
Google Drive link of the packet tracer file (give view permission):	https://drive.google.com/drive/folders/1MATwQmmGnAX8MqvfLqVHf4oSZeJo7jgL?usp=drive_link

Objective(s):

To capture and analyse TCP and IP packet using Wireshark.

Introduction

Packet Analysis is a technique used to intercept data in information security, where many of the tools that are used to secure the network can also be used by attackers to exploit and compromise the same network. The core objective of sniffing is to steal data, such as sensitive information, email text, etc., or sniff the traffic that is being transmitted between two parties.

Packet Analysis involves intercepting network traffic between two target network nodes and capturing network packets exchanged between nodes. A packet sniffer is referred to as a network monitor that is used legitimately by a network administrator to monitor the network for vulnerabilities by capturing the network traffic and should there be any issues, proceeds to troubleshoot the same. Similarly, sniffing tools can be used by attackers in promiscuous mode to capture and analyze all the network traffic. Once attackers have captured the network traffic they can analyze the packets and view the user name and password information in a given network as this information is transmitted in a cleartext format. An attacker can easily intrude into a network using this login information and compromise other systems on the network.

Hence, it is very crucial for an Information Security Auditor or a Penetration Tester to be familiar with network traffic analyzers and he or she should be able to maintain and monitor a network to detect rogue packet sniffers, MAC attacks, DHCP attacks, ARP poisoning, spoofing, or DNS poisoning, and know the types of information that can be detected from the captured data and use the information to keep the network running smoothly.

Exercise:

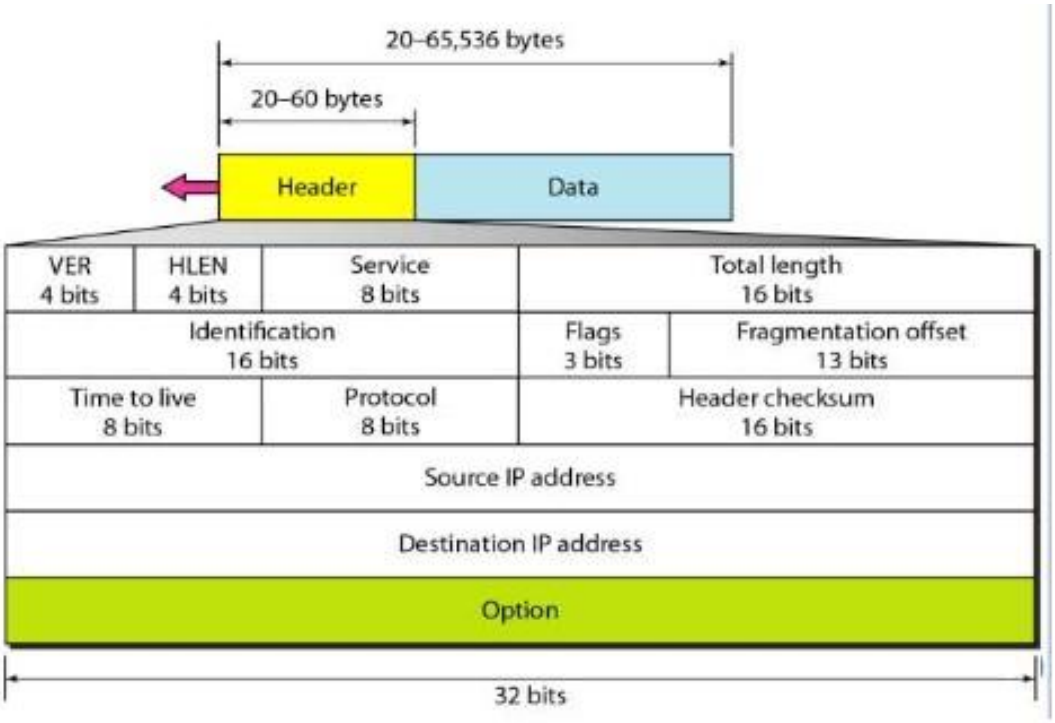
1. Visit any one website by opening a browser and fill your machine details (attach relevant screenshots).

Parameter	**Value**
Your Machine IP Address.	10.1.14.75
Your Machine MAC Address	B4-8C-9D-D7-8A-25
Default Gateway address	10.1.0.1
Website URL	www.amazon.in
Website IP Address	23.221.86.98

2. Fill the following IP packet details:

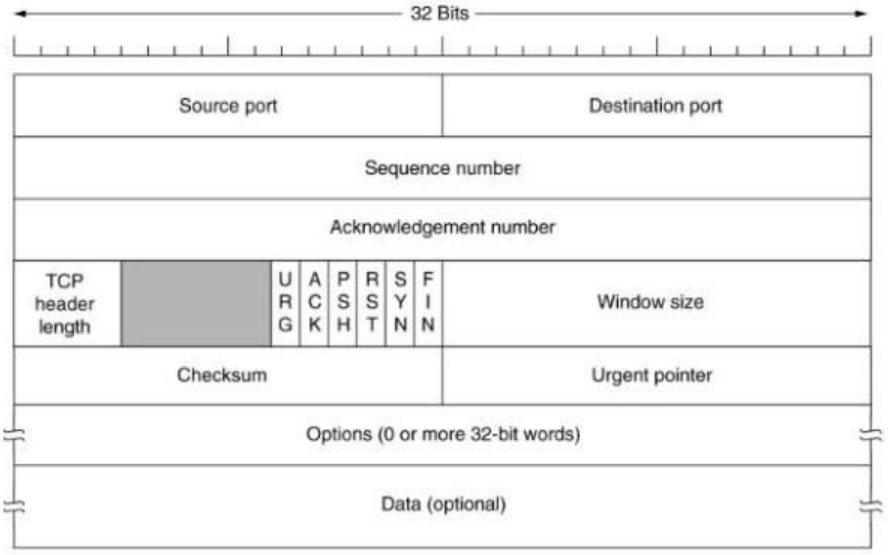
Field Name	Field Length (no of bits)	Field value
Destination MAC address	48 bits	c8-4f-86-fc-00-0f
Source MAC address	48 bits	B4-8C-9D-D7-8A-25
Destination IP address	32 bits	23.221.86.98
Source IP Address	32 bits	10.1.14.75
Destination TCP port	16 bits	56429
Source TCP port	16 bits	443

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



Field Name	Field Value (# of bits)	Field Value
		(Either Binary or Hex Value)
Version	4	0100
Header Length	4	0101
Type of service	8	0x00
Datagram Length	16	1181
16 bit Identifier	16	0x055b9(40)
Flags	3	010
13-bit Fragment offset	13	0 0000 0000 0000
Time-to-live	8	(80)128
Upper layer protocol	8	6
Header Checksum	16	0x6eea
32 bit Source Address	32	10.1.14.75
32 bit destination address	32	23.221.86.98
Options (if any)	-	-
Date	-	-

TCP Header Format:

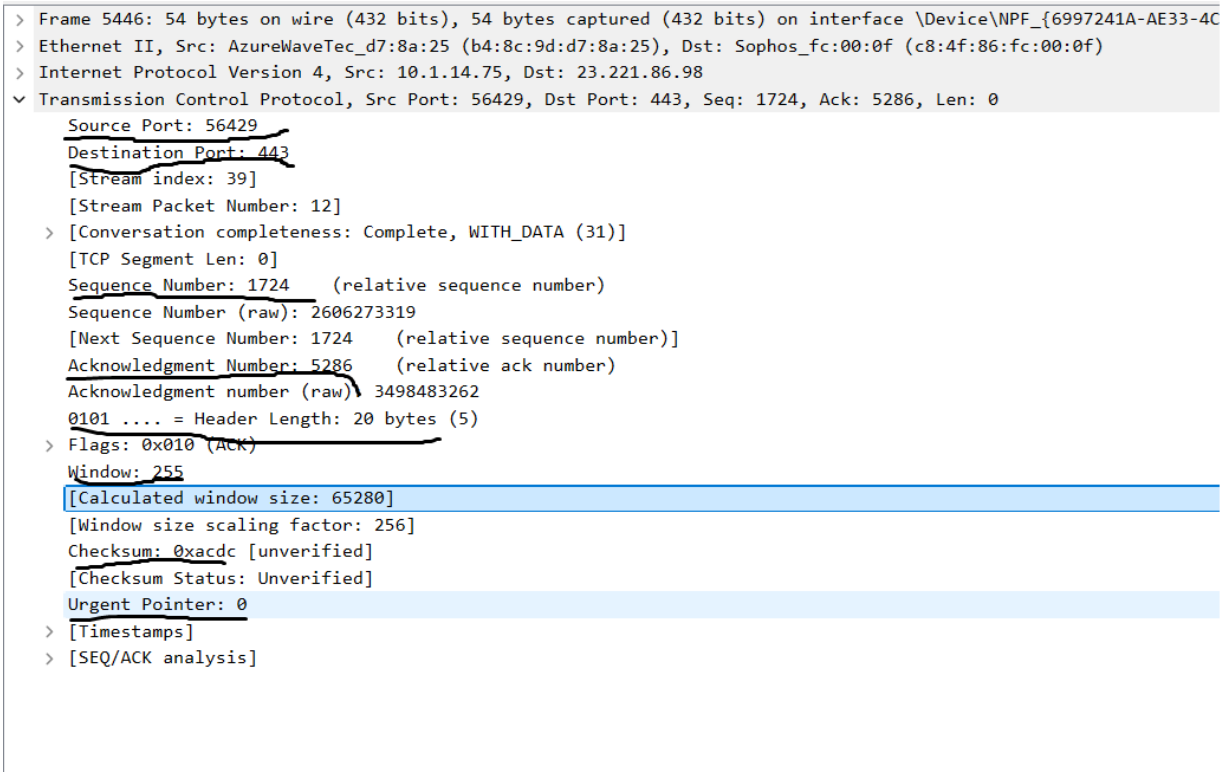


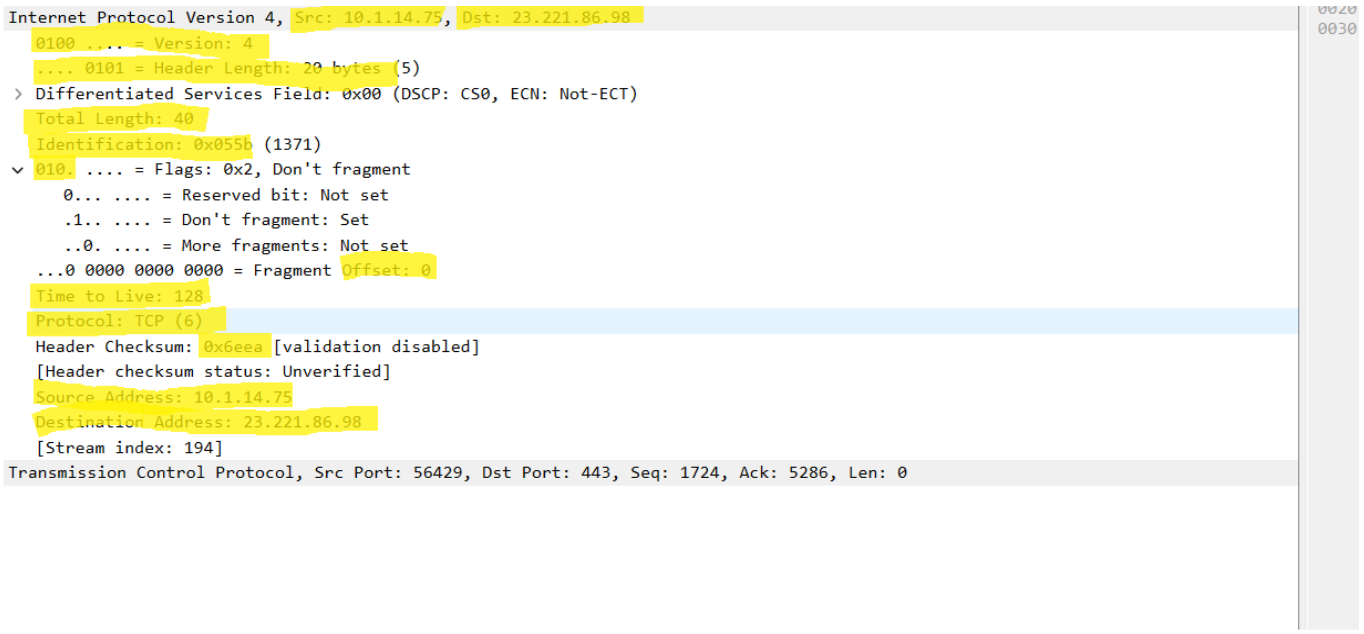
TCP Header.

Field Name	Field Value (# of bits)	Field Value (Either Binary or Hex Value)

Source Port	16	56429
Destination Port	16	443
Sequence No.	32	1724
Acknowledgement No	32	5286
Header Length	4	50
FLSGS (URG,PSH,ACK,RST,SYN,FIN)	6	000010
Receive Window Size	16	65280
Checksum	16	0xacdc
Urgent Pointer	16	-
Options	-	-
Data	-	-

Paste the screenshot and highlight the above details:





Rubrics for Wireshark labs:

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	

Conclusion: To capturing and analyzing TCP and IP packet using Wireshark has done Successfully.