EXNO:5	**Use a tool like wireshark to capture packets andexamine the packtes**
DATE:	

AIM:

To use a tool like wireshark to capture packets and examine the packets

PROCEDURE:

Introduction

Wireshark is a software tool used to monitor the network traffic through a network interface. It is the most widely used network monitoring tool today.

Uses of Wireshark:

Wireshark can be used in the following ways:

1. It is used by network security engineers to examine security problems.
2. It allows the users to watch all the traffic being passed over the network.
3. It is used by network engineers to troubleshoot network issues.
4. It also helps to troubleshoot latency issues and malicious activities on your network.
5. It can also analyze dropped packets.
6. It helps us to know how all the devices like laptop, mobile phones, desktop, switch, routers, etc., communicate in a local network or the rest of the world.

Functionality of Wireshark:

Wireshark is similar to tcpdump in networking. Tcpdump is a common packet analyzer which allows the user to display other packets and TCP/IP packets, being transmittedand received over a network attached to the computer. It has a graphic end and some sorting and filtering functions. Wireshark users can see all the traffic passing throughthe network.Wireshark can also monitor the unicast traffic which is not sent to the networks MAC address interface. But, the switch does not pass all the traffic to the port. Hence, the promiscuous mode is not sufficient to see all the traffic. The various network taps or port mirroring is used to extend capture at any point. Port mirroring is a method to monitor network traffic. When it is enabled, the switch sends the copies of all the network packets present at one port to another port.

What is color coding in Wireshark?

The packets in the Wireshark are highlighted with blue, black, and green color. These colors help users to identify the types of traffic. It is also called as packet colorization. The kinds of coloring rules in the Wireshark are temporary rules and permanent rules.

- The temporary rules are there until the program is in active mode or until we quit the program.
- The permanent color rules are available until the Wireshark is in use or the next time you run the Wireshark.

Installation of Wireshark Software

Below are the steps to install the Wireshark software on the computer:

○ Open the web browser.

○ Search for “Download Wireshark”

○ Select the Windows installer according to your system configuration, either 32-bt or 64-bit. Save the program and close the browser.

○ Now, open the software, and follow the install instruction by accepting the license.

○ The Wireshark is ready for use.

Wireshark Layout Explanation

Wireshark Packet Capturing Mechanism

One of the core functions of Wireshark as a network analysis tool is to capture packets of data. Learning it’s important to note that it can be difficult to capture packets when you’re new to Wireshark. Before you start to capture packets, there are three things you need to do:

1. Make sure that you have the administrative privileges to start a live capture on your device
2. Choose the correct network interface to capture packet data
3. Capture packet data from the correct location in your network

Once you’ve done these three things, you’re ready to start the capture process. When you use Wireshark to capture packets, they are displayed in a human-readable format to make them legible to the user. You can also break packets down with filters and color-coding if you wish to see more specific information.

Fig:1 Analyzing captured packets

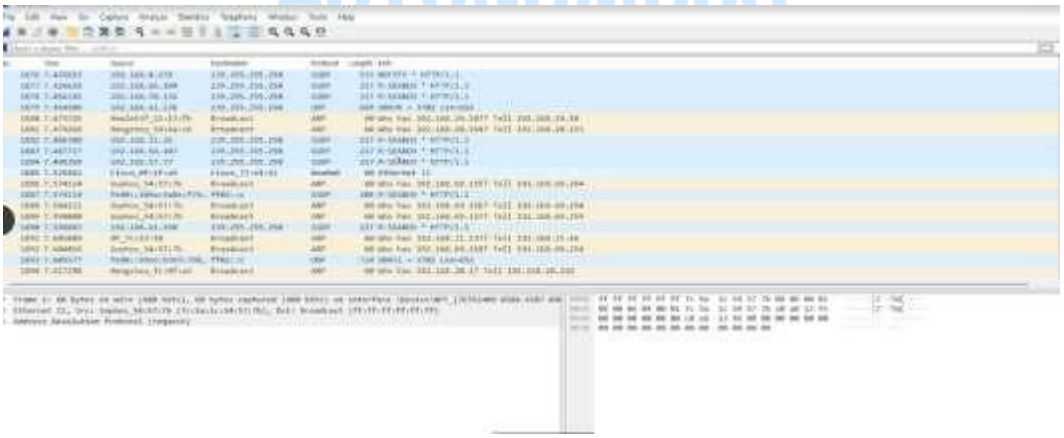


Fig:2 View->Coloring Rules

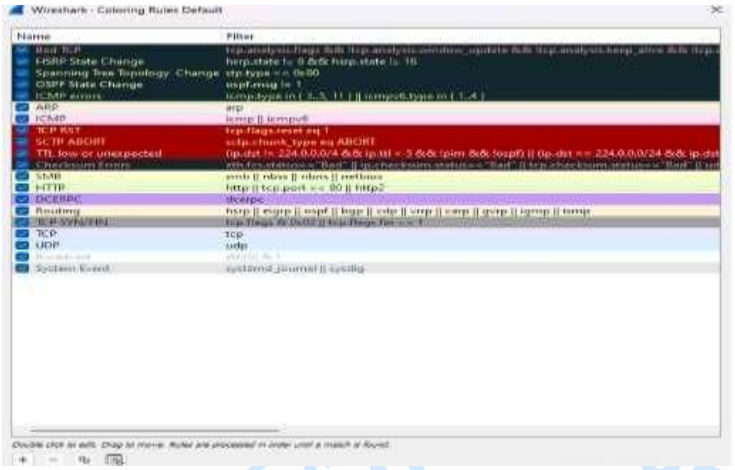


Fig:3 Analyze->Apply as Fliter

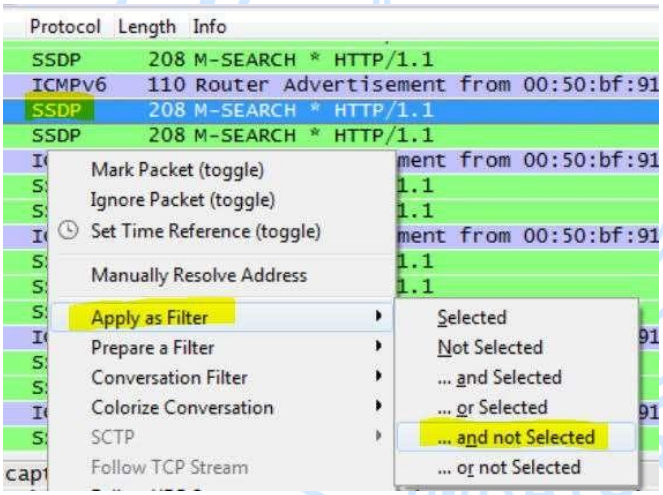


Fig:4 Statistics -> options all

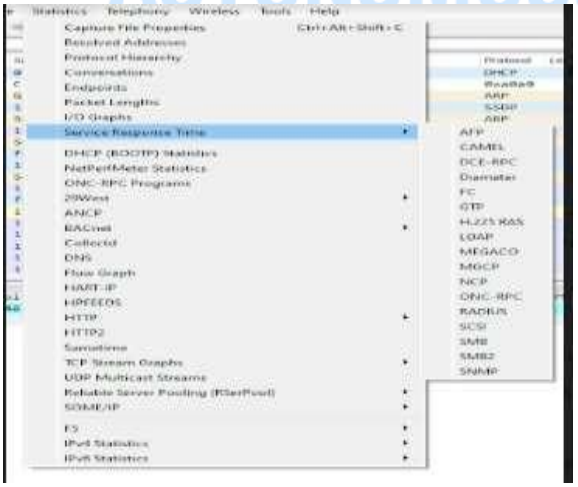


Fig:5 Statistics-> Flow Graph

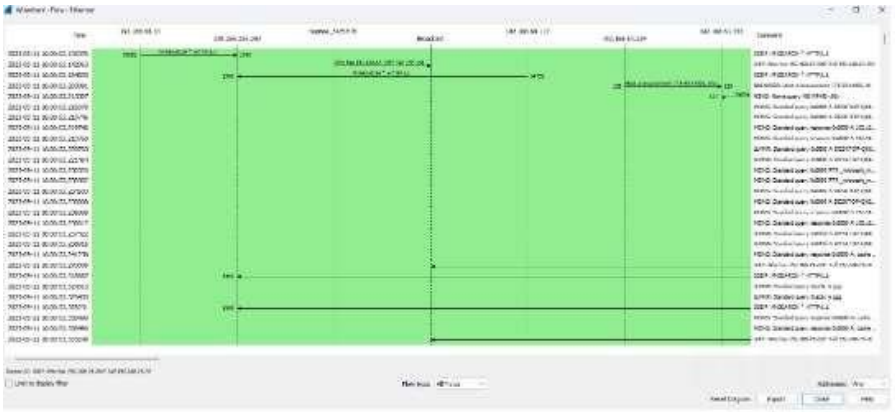
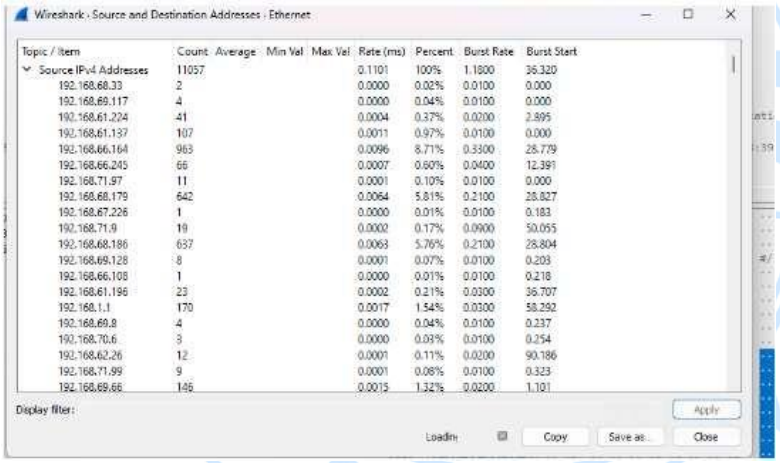


Fig:6 Statistics->IPV4 statistics->Source to Destination



ig:7 Statistics->IPV4 statistics->All Address

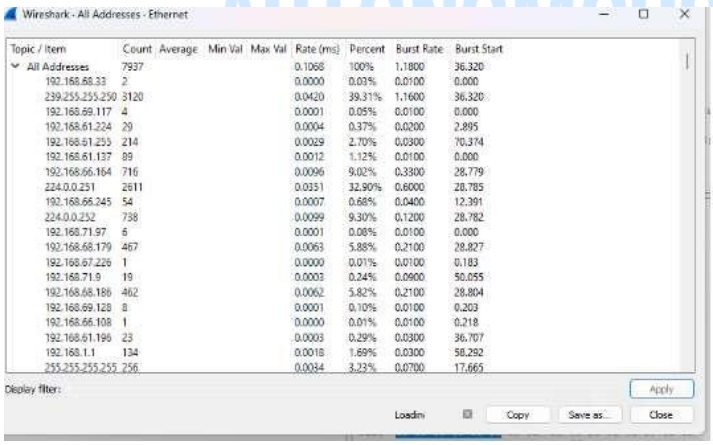


Fig:8 Statistics->Protocol Hierarchy

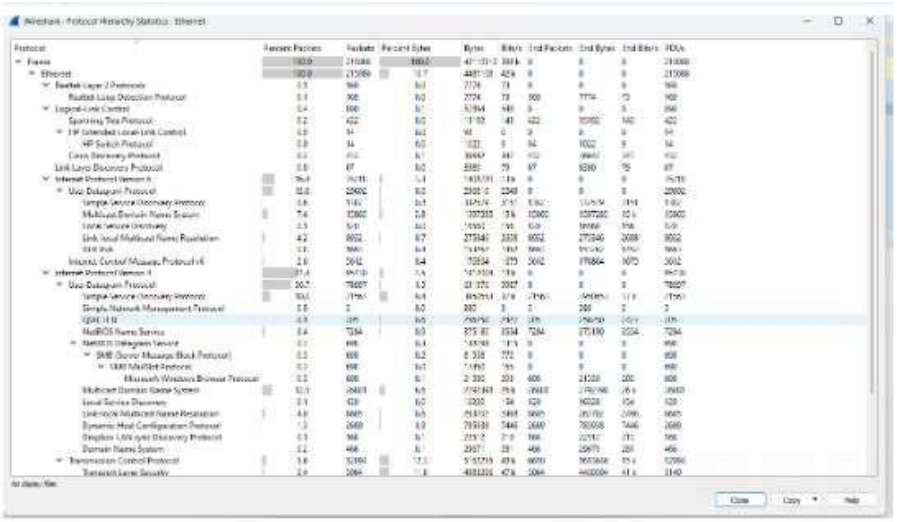
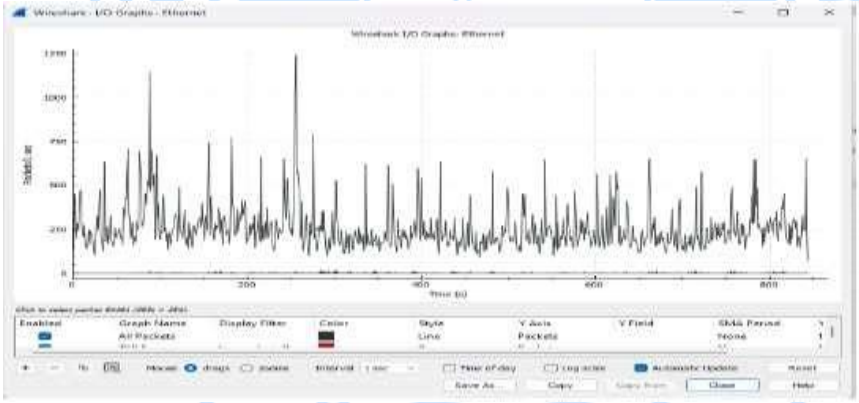


Fig:9 Statistics->I/O graphs



Result:

Thus the tool like wireshark to capture packets and to examine the packets have been studied successfully