

EXNO:5	Use a tool like wireshark to capture packets and examine the packets
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 transmitted and 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 through the network. Wireshark can also monitor the unicast traffic which is not sent to the network's 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-bit 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

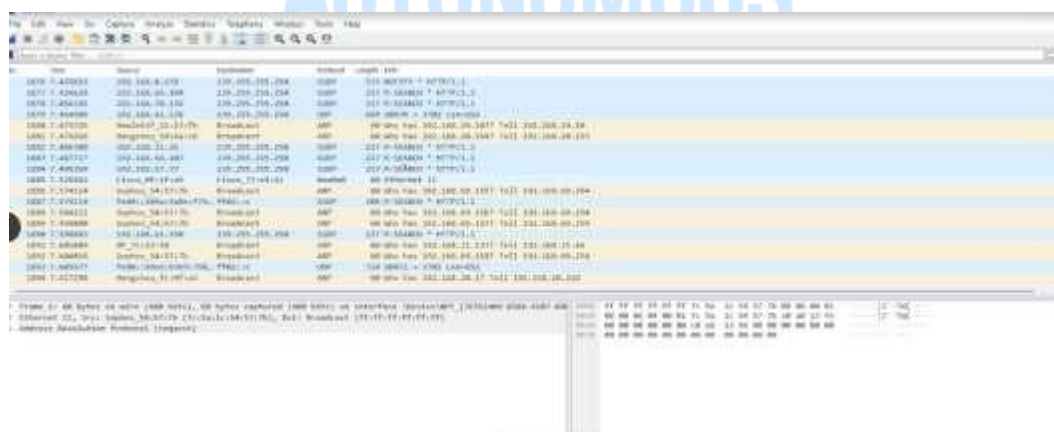
Wireshark Packet Capturing Mechanism

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



[illegible]

The screenshot shows the Wireshark interface with a packet list on the left. The selected packet is an SSDP M-SEARCH message. A right-click context menu is open over this packet, showing various actions. The 'Apply as Filter' option is highlighted in yellow, and its sub-menu is also open, with the '... and not Selected' option highlighted in yellow.

Protocol	Length	Info
SSDP	208	M-SEARCH * HTTP/1.1
ICMPv6	110	Router Advertisement from 00:50:bf:9...
SSDP	208	M-SEARCH * HTTP/1.1
SSDP	208	M-SEARCH * HTTP/1.1

Context Menu Options:

- Mark Packet (toggle)
- Ignore Packet (toggle)
- ⌚ Set Time Reference (toggle)
- Manually Resolve Address
- Apply as Filter**
 - Selected
 - Not Selected
 - ... and Selected
 - ... or Selected
 - ... and not Selected**
 - ... or not Selected
- Prepare a Filter
- Conversation Filter
- Colorize Conversation
- SCTP
- Follow TCP Stream

The screenshot shows the Mikrotik WinBox interface. The 'Statistics' menu is open, and the 'Service Response Time' option is selected. A submenu is visible, listing various protocols and services for which response time statistics can be monitored. The protocols listed include DHCP, ICMP, NetPerfMeter Statistics, ONC-RPC Programs, 29West, ANCP, BACnet, Collectd, DNS, Flow Graph, HART-IP, HPEFOS, HTTP, HTTPS, SAVANNAH, TCP Stream Graphs, UDP Multicast Stream, Reliable Server Pooling (RSPool), SDRM-IP, FS, IPv6 Statistics, and IPv6 Statistics.

Fig:5 Statistics-> Flow Graph**Fig:6 Statistics->IPv4 statistics->Source to Destination**

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Source IPv4 Addresses	11057	0.1101	100%	1.1800	36.320			
192.168.68.33	2	0.0000	0.02%	0.0100	0.000			
192.168.69.117	4	0.0000	0.04%	0.0100	0.000			
192.168.61.224	41	0.0004	0.37%	0.0200	2.895			
192.168.61.137	107	0.0011	0.97%	0.0100	0.000			
192.168.66.164	963	0.0096	8.71%	0.3300	28.779			
192.168.66.245	66	0.0007	0.60%	0.0400	12.391			
192.168.71.97	11	0.0001	0.10%	0.0100	0.000			
192.168.68.179	642	0.0064	5.81%	0.2100	28.827			
192.168.67.226	1	0.0000	0.01%	0.0100	0.183			
192.168.71.9	19	0.0002	0.17%	0.0900	50.055			
192.168.68.186	637	0.0063	5.76%	0.2100	28.804			
192.168.69.128	8	0.0001	0.07%	0.0100	0.203			
192.168.66.108	1	0.0000	0.01%	0.0100	0.218			
192.168.61.196	23	0.0002	0.21%	0.0300	36.707			
192.168.1.1	170	0.0017	1.54%	0.0300	58.292			
192.168.69.8	4	0.0000	0.04%	0.0100	0.237			
192.168.70.6	3	0.0000	0.03%	0.0100	0.254			
192.168.62.26	12	0.0001	0.11%	0.0200	90.186			
192.168.71.99	9	0.0001	0.08%	0.0100	0.323			
192.168.69.66	146	0.0015	1.32%	0.0200	1.101			

Fig:7 Statistics->IPv4 statistics->All Address

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
All Addresses	7937	0.1068	100%	1.1800	36.320			
192.168.68.33	2	0.0000	0.03%	0.0100	0.000			
239.255.255.250	3120	0.0420	39.31%	1.1600	36.320			
192.168.69.117	4	0.0001	0.05%	0.0100	0.000			
192.168.61.224	29	0.0004	0.37%	0.0200	2.895			
192.168.61.235	214	0.0029	2.70%	0.0300	70.374			
192.168.61.137	89	0.0012	1.12%	0.0100	0.000			
192.168.66.164	716	0.0096	9.02%	0.3300	28.779			
224.0.0.251	2611	0.0351	32.90%	0.6000	28.785			
192.168.66.245	54	0.0007	0.68%	0.0400	12.391			
224.0.0.252	738	0.0099	9.30%	0.1200	28.782			
192.168.71.97	6	0.0001	0.08%	0.0100	0.000			
192.168.68.179	467	0.0063	5.88%	0.2100	28.827			
192.168.67.226	1	0.0000	0.01%	0.0100	0.183			
192.168.71.9	19	0.0003	0.24%	0.0900	50.055			
192.168.68.186	462	0.0062	5.82%	0.2100	28.804			
192.168.69.128	8	0.0001	0.10%	0.0100	0.203			
192.168.66.108	1	0.0000	0.01%	0.0100	0.218			
192.168.61.196	23	0.0003	0.29%	0.0300	36.707			
192.168.1.1	134	0.0018	1.69%	0.0300	58.292			
255.255.255.255	256	0.0034	3.33%	0.0700	17.665			

Fig:8 Statistics->Protocol Hierarchy

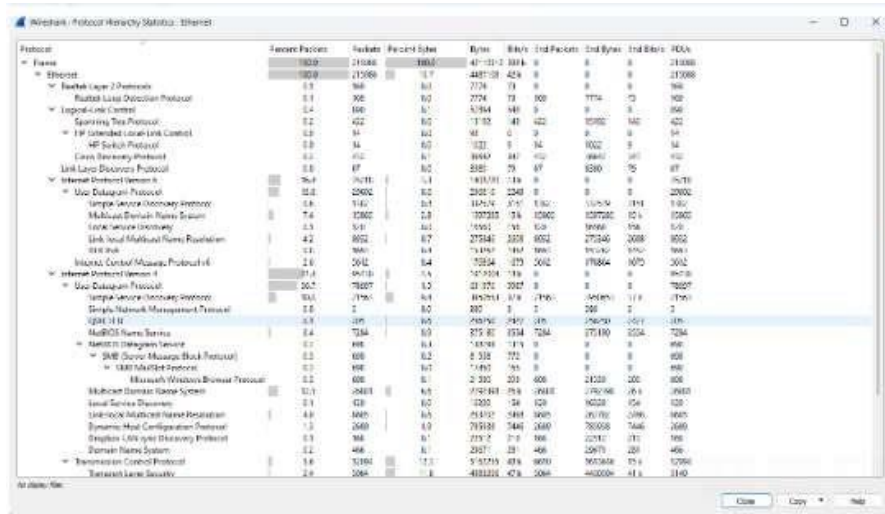
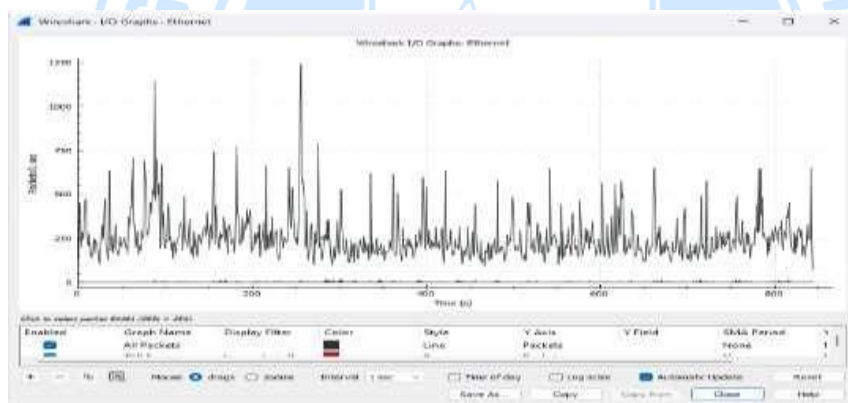


Fig:9 Statistics->I/O graphs



Result:

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

