

## **Experiment-5**

### **Wireshark**

#### **AIM: Experiments on Packet capture tool**

##### **Packet Sniffer**

- Sniffs messages being sent/received from/by your computer
- Store and display the contents of the various protocol fields in the messages.

#### **DESCRIPTION:**

##### **WIRESHARK**

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark includes filters, color coding, and other features that let you dig deep into network traffic and inspect individual packets. You can use Wireshark to inspect a suspicious program's network traffic, analyze the traffic flow on your network, or troubleshoot network problems.

##### **What we can do with Wireshark:**

- ☐ Capture network traffic
- ☐ Decode packet protocols using dissectors
- ☐ Define filters – capture and display
- ☐ Watch smart statistics
- ☐ Analyze problems
- ☐ Interactively browse that traffic

##### **Wireshark used for:**

- ☐ Network administrators: troubleshoot network problems
- ☐ Network security engineers: examine security problems
- ☐ Developers: debug protocol implementations
- ☐ People: learn network protocol internals Getting Wireshark

Wireshark can be downloaded for Windows or macOS from its official website. For Linux or another UNIX-like system, Wireshark will be found in its package repositories. For Ubuntu, Wireshark will be found in the Ubuntu Software Center.

## **Capturing Packets**

After downloading and installing Wireshark, launch it and double-click the name of a network interface under Capture to start capturing packets on that interface. As soon as you click the interface's name, you'll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system. If you have promiscuous mode enabled—it's enabled by default—you'll also see all the other packets on the network instead of only packets addressed to your network adapter. To check if promiscuous mode is enabled, click Capture > Options and verify the "Enable promiscuous mode on all interfaces" checkbox is activated at the bottom of this window. Click the red "Stop" button near the top left corner of the window when you want to stop capturing traffic.

### **The "Packet List" Pane**

The packet list pane displays all the packets in the current capture file. The "Packet List" pane Each line in the packet list corresponds to one packet in the capture file. If you select a line in this pane, more details will be displayed in the "Packet Details" and "Packet Bytes" panes.

### **The "Packet Details" Pane**

The packet details pane shows the current packet (selected in the "Packet List" pane) in a more detailed form. This pane shows the protocols and protocol fields of the packet selected in the "Packet List" pane. The protocols and fields of the packet shown in a tree which can be expanded And collapsed.

### **The "Packet Bytes" Pane**

The packet bytes pane shows the data of the current packet (selected in the "Packet List" pane) in a hexdump style.

## **Color Coding**

You'll probably see packets highlighted in a variety of different colors. Wireshark uses colors to help you identify the types of traffic at a glance. By default, light purple is TCP traffic, light blue is UDP traffic, and black identifies packets with errors—for example, they could have been delivered out of order.

To view exactly what the color codes mean, click View > Coloring Rules. You can also customize and modify the coloring rules from here, if you like.

### **Sample Captures:**

If there's nothing interesting on your own network to inspect, Wireshark's wiki has you covered. The wiki contains a page of sample capture files that you can load and inspect. Click File > Open in Wireshark and browse for your downloaded file to open one. You can also save your own captures in Wireshark and open them later. Click File > Save to save your captured packets.

### **Filtering Packets**

If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters come in.

### **CAPTURING AND ANALYSING PACKETS USING WIRESHARK TOOL**

To filter, capture, view, packets in Wireshark Tool. Capture 100 packets from the Ethernet: IEEE 802.3 LAN Interface and save it.

Procedure 1. Create a Filter to display only TCP/UDP packets, inspect the packets and provide the flow graph

2. Create a Filter to display only ARP packets and inspect the packets.

Procedure

3. Create a Filter to display only DNS packets and provide the flow graph.

4. Create a Filter to display only HTTP packets and inspect the packets

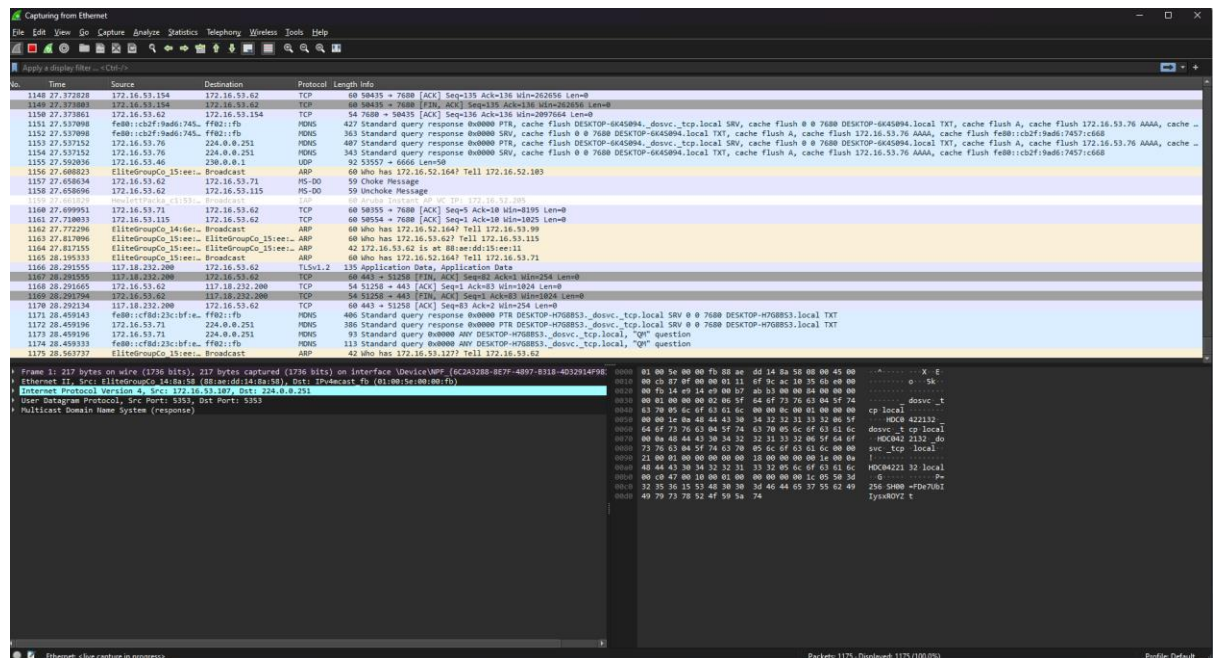
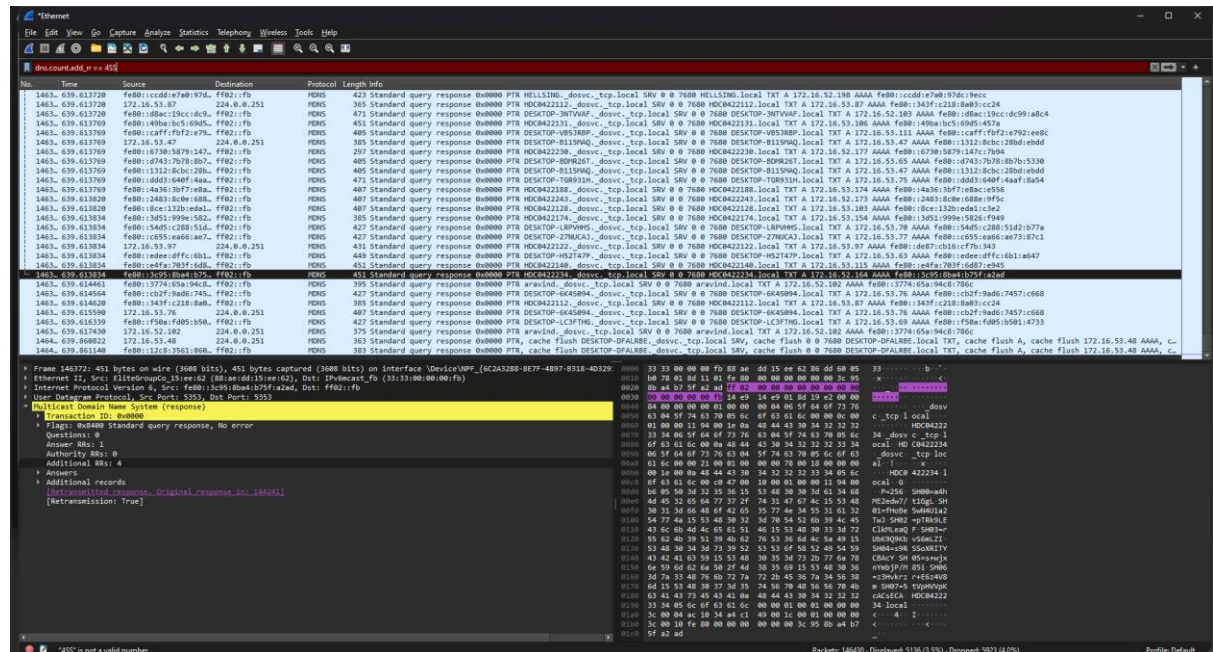
Procedure

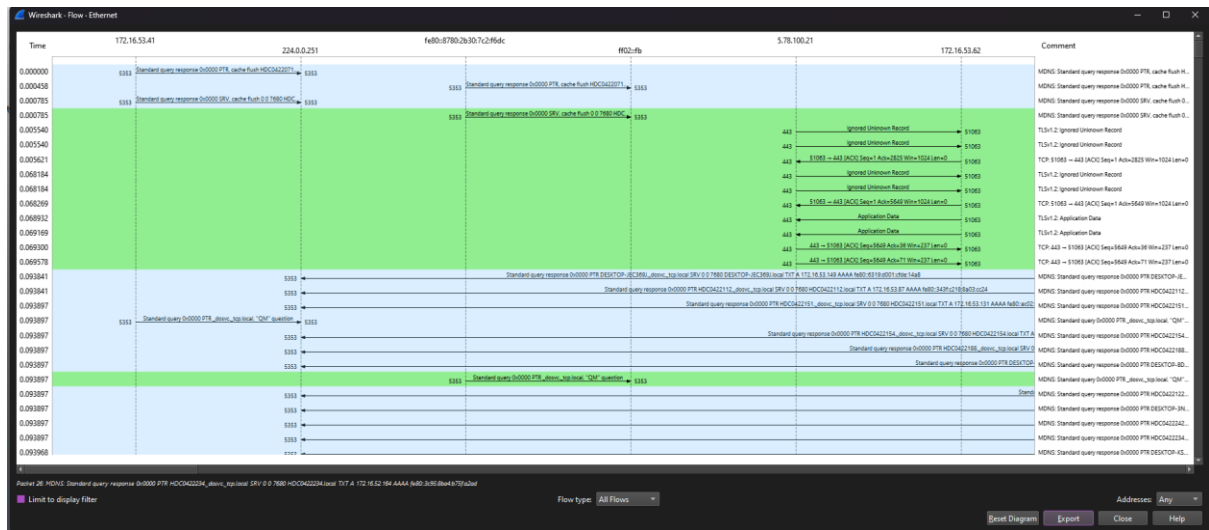
5. Create a Filter to display only IP/ICMP packets and inspect the packets.

Procedure

6. Create a Filter to display only DHCP packets and inspect the packets.

# Procedure :





## RESULT:

The Experiments on Packet capture tool has been executed successfully.