Ex. No: 4

04.08.25

Experiment on Packet capture tool using wireshark

Aim:

Experiments on Packet capture tool wireshark

What is wireshark ?

A network analysis tool that captures real-time network packets and displays them in human-readable format.

Key features :

- Real-time packet capture
- Protocol decoding using dissectors
- Filtering
- color coding for better analysis
- Traffic browsing and smart statistics

uses :-

- Network admins : Troubleshoot network issues
- Security engineers : Analyze security incidents
- Learners : Understand protocol internals

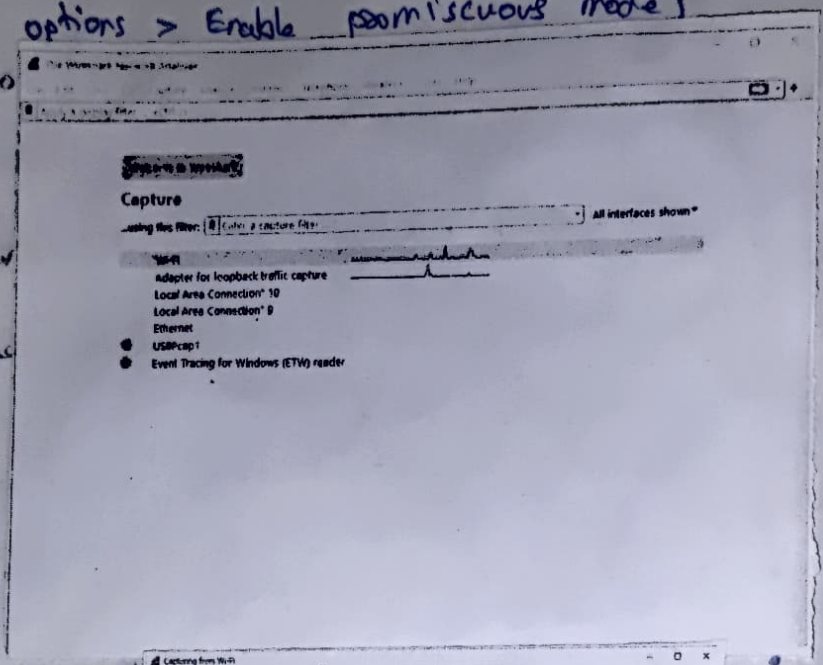
How to Get wireshark

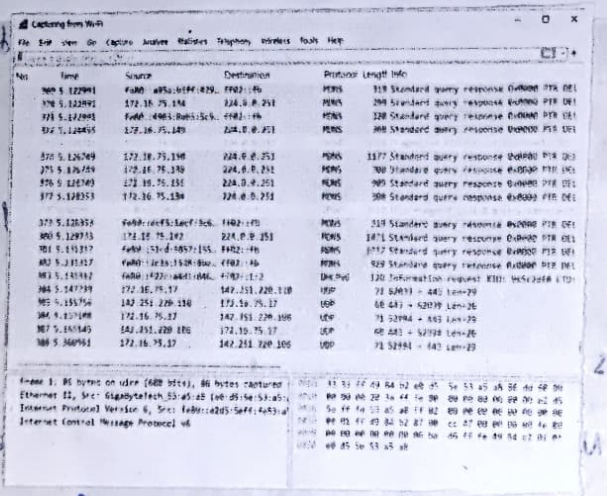
- windows/macOS : Download from official website.
- linux/Ubuntu : Available in Package managers or Ubuntu Software centre

Capturing Packets :

- Launch wireshark and double click a network interface

- Packets appear in real-time and include all traffic if promiscous mode is enabled (Capture options > Enable promiscuous mode)



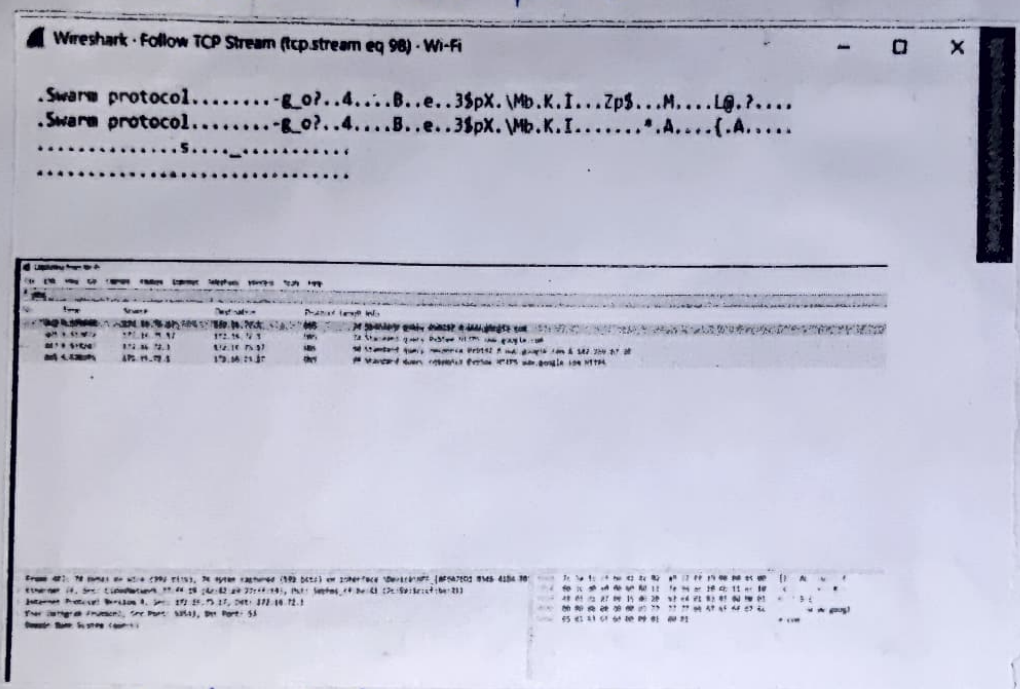


The Packet Panes

- Packet List Pane: lists all captured packets; selecting one shows more details.
- Packet Byte Pane shows Packet data in hex and ASCII.

Color coding:

- Light purple = TCP
- Light blue = UDP
- Black = Error packets

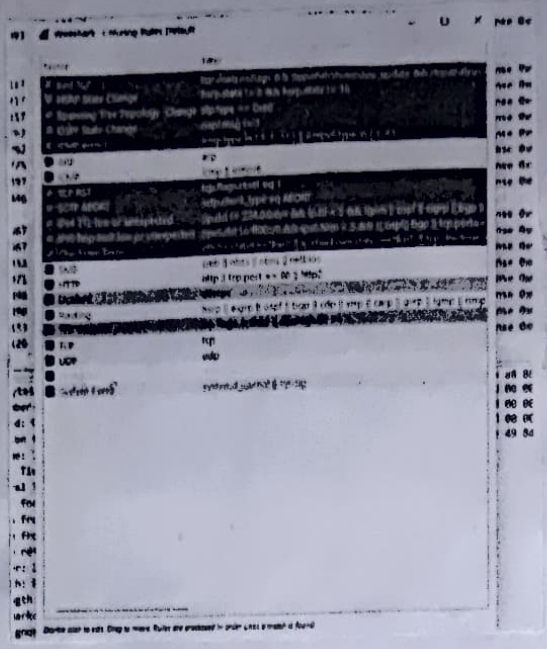


Sample captures

- Load sample captures from wireshark's wiki via File > open
- Save your own captures using File > Save.

Filtering Packets:

- Use the filter bar to isolate traffic (eg. type dns to see DNS packets)
- Press Enter or click Apply to use the filter
- Access default/custom filter via Analyze > Display Filters.

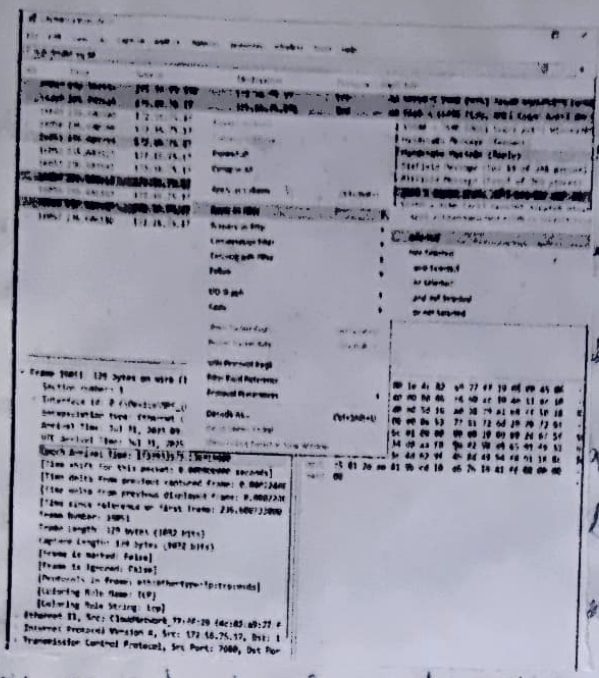


Following TCP Streams !

- Right-click a packet → Follow > TCP Stream (or other protocols).
- close the windows to auto-apply a filter for the conversation

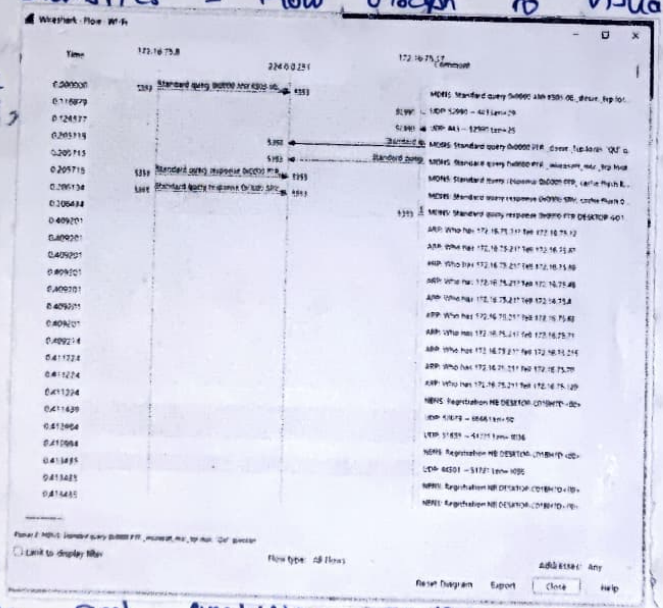
Inspecting Packets

- click a packet to see it detail
- Right-click protocol Field → Apply as filter to filter based on it



Flow Graph

- use Statistics > Flow Graph to visualize traffic



Capturing and analysing packets using wireshark tool.

Task : Capture 100 Packets from Ethernet Interface

Procedure

- select local Area connection
- Capture > options → set stop after 100 packets.

- click start
- save packets

1. Filter : Display TCP/UDP Packets & show Flow Graph

Procedure

- start capture as above
- In filter bar, search tcp or udp
- statistics > Flow Graph to view
- save packets.

2. filter : Diplay only ARP Packets

Procedure

- start capture as above
- In filter bar, type arp
- save packets

3. Filter : Display only DNS Packets & Show Flow Graph

Procedure :

- start capture as above
- In filter bar, type dns
- statistics > Flow Graph to view
- save packets.

4- Filter : Display only HTTP Packets procedure.

- start capture as above
- In filter box, type http
- save packets.

Student observation :

1) what is promiscuous mode ?

Promiscuous mode allows a network card to capture all packets on a network. Its used in tools like wireshark for monitoring.

2) Does ARP packets have transport layer header ? Explain.

No, ARP works at the data link layer and does not use transport layer headers like TCP or UDP.

3) which transport layer protocol is used by DNS ?

DNS primarily uses UDP on port 53 and uses TCP for larger data like zone transfers.

4) what is the port number used by http protocol ?

The default port for HTTP protocol is 80.

5) what is broadcast IP address)

A broadcast IP address (eg., 255.255.255.255) sends data to all hosts in a local network.

Result:

This the Packet capture tool wireshark is executed and Packets are captured.