Ex.No:12

M.Dhivya

Date:13/10/25

241901027

TO CAPTURE, SAVE, AND ANALYZE NETWORK TRAFFIC USING WIRESHARK TOOL

Aim:

To capture, save, and analyze network traffic on TCP/UDP/IP/HTTP/ARP/DHCP/ICMP /DNS using Wireshark Tool.

Procedure:

1. Install Wireshark

Download and install Wireshark from https://www.wireshark.org/

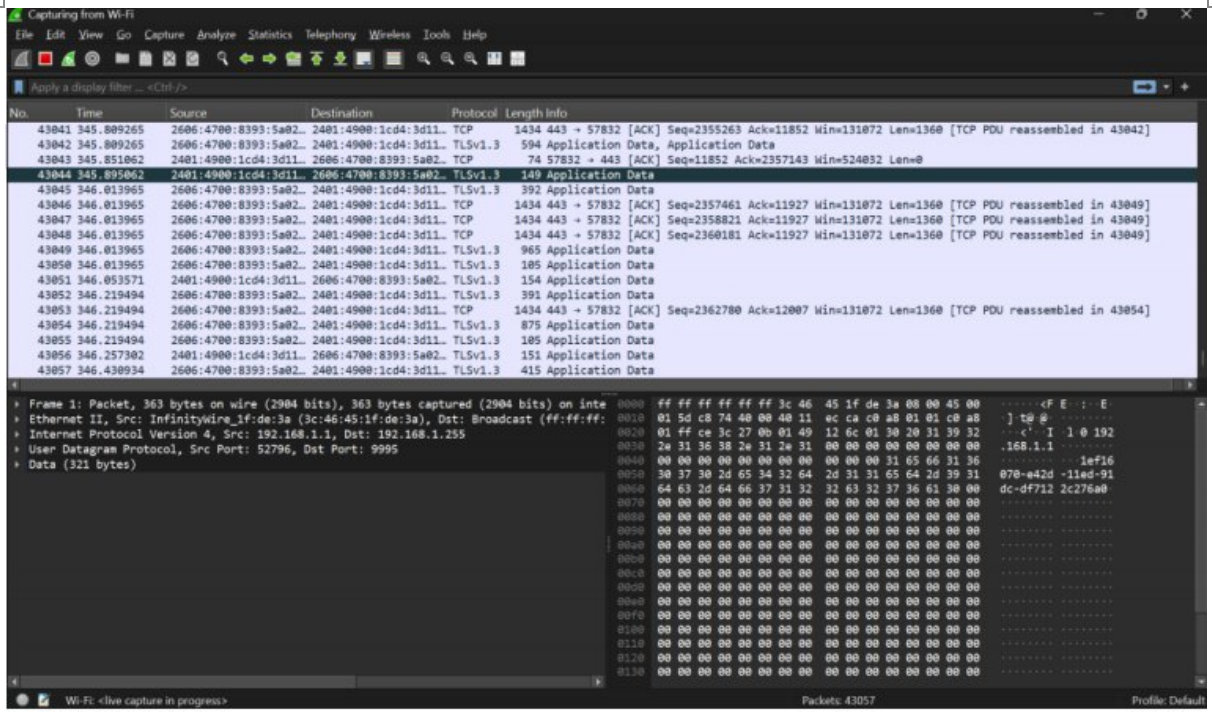
Make sure to install the required packet capture drivers (e.g., WinPcap or Npcap on Windows).

2. Start Capturing Traffic

Open Wireshark.

Select the correct network interface for capturing (Wi-Fi, Ethernet, etc.).

Click on the interface to start live capture.



3. Apply Capture Filters

To reduce the amount of data captured, you can apply capture filters.

Example filters for protocols:

TCP only: tcp

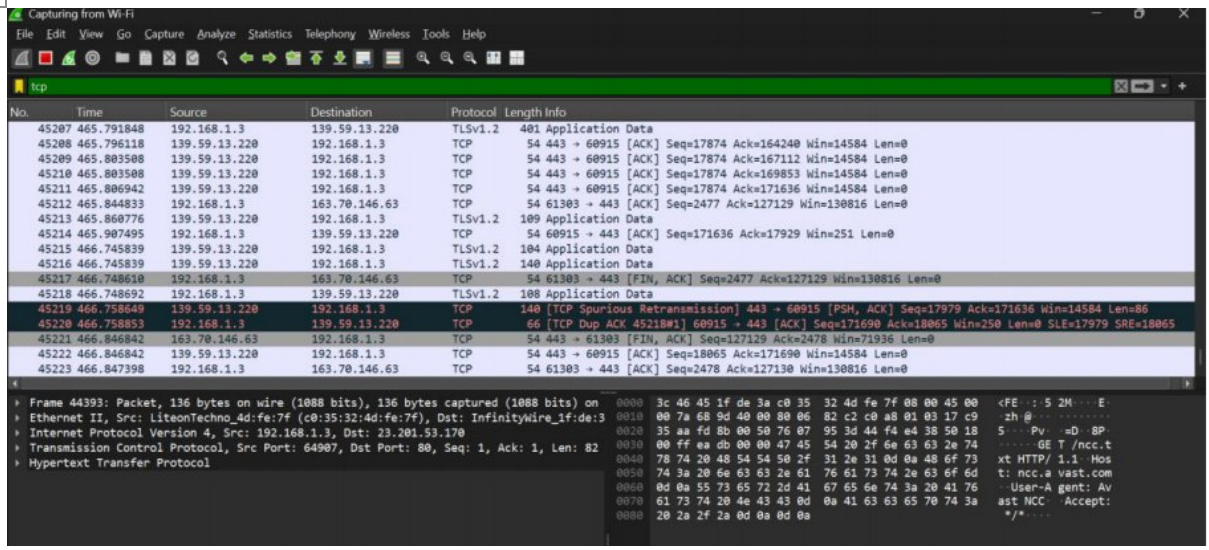
UDP only: udp

ARP only: arp

ICMP only: icmp

DHCP (uses UDP ports 67 and 68): udp port 67 or udp port 68

DNS (uses UDP or TCP port 53): port 53



4. Save Captured Traffic

When done capturing, go to File > Save As.

Save the capture file in .pcapng or .pcap format for later analysis

5. Analyze Captured Traffic

Wireshark provides powerful tools to filter and analyze packets:

Display Filters:

You can filter displayed packets without limiting the saved capture.

Examples:

TCP: tcp

UDP: udp

IP: ip

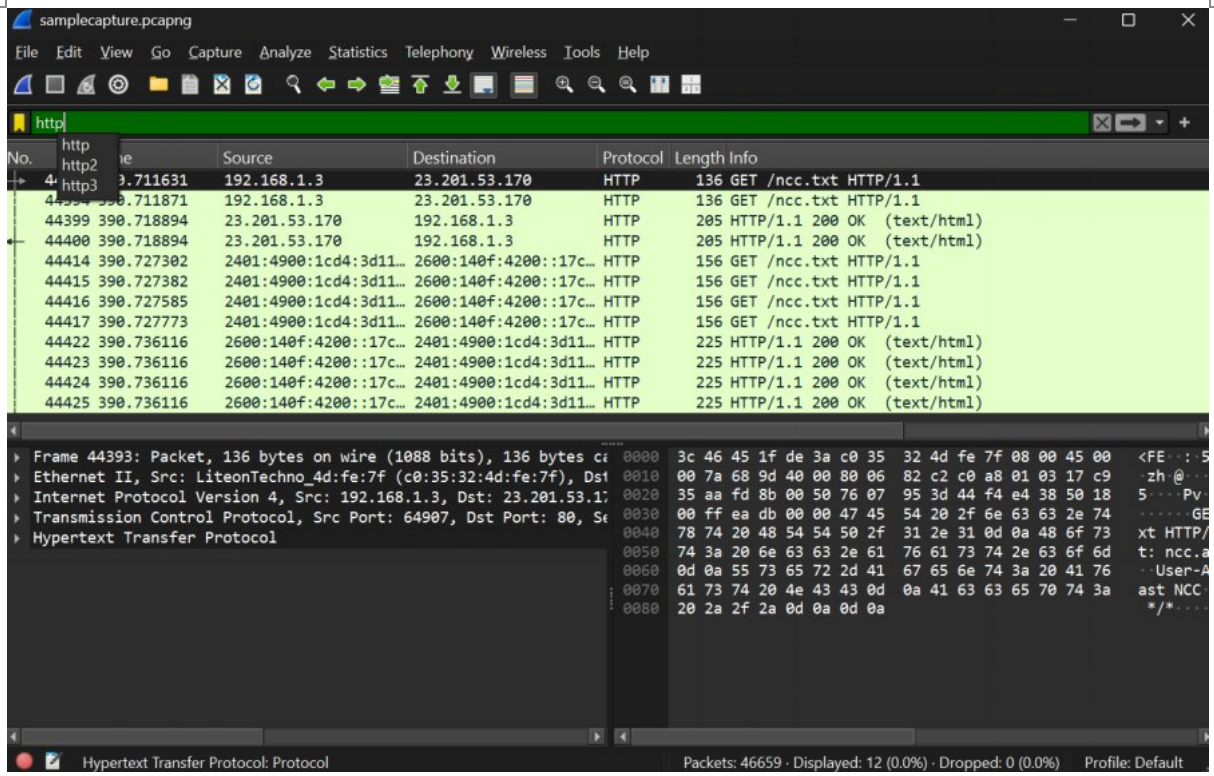
HTTP: http

ARP: arp

DHCP: bootp (DHCP is part of the BOOTP protocol)

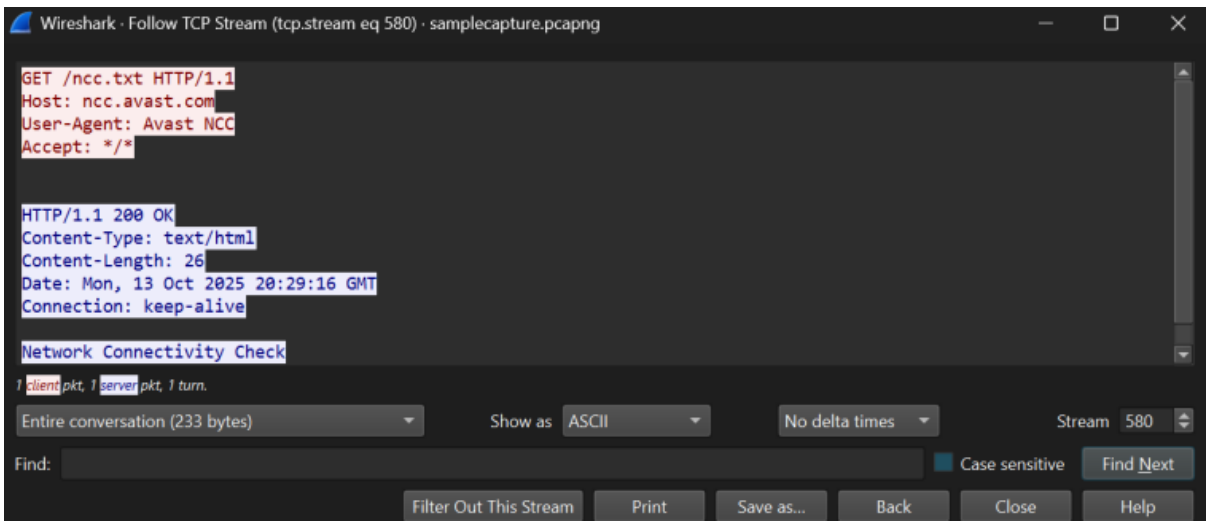
ICMP: icmp

DNS: dns



Follow Streams:

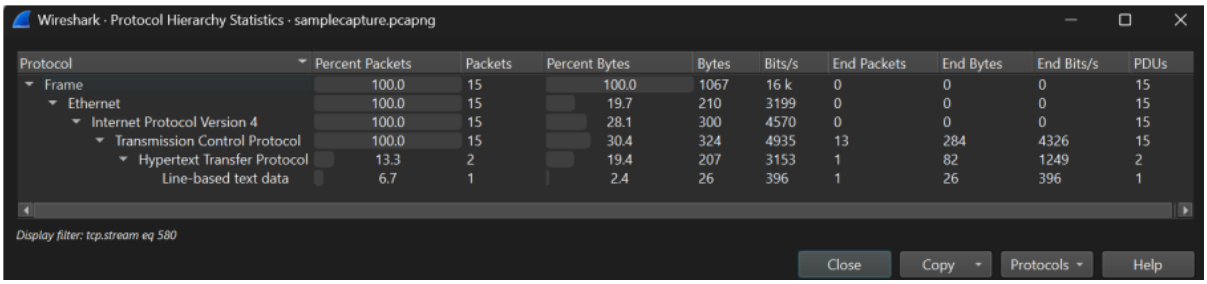
For TCP or UDP conversations, right-click a packet and select Follow > TCP Stream or Follow > UDP Stream to see the conversation in readable form.



Protocol Hierarchy:

Use Statistics > Protocol Hierarchy to get an overview of protocols

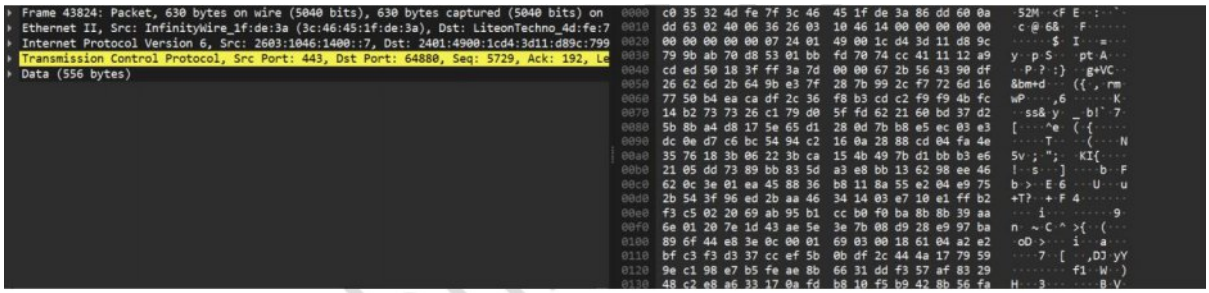
present.



Packet Details:

Select any packet and expand protocol layers in the middle pane to analyze

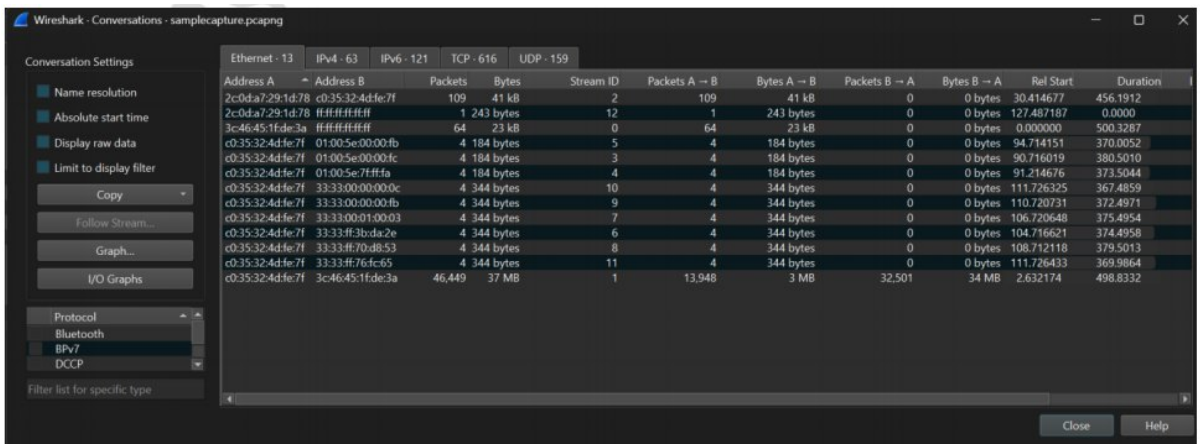
headers and payload details



Conversations:

Use Statistics > Conversations to analyze communication between source

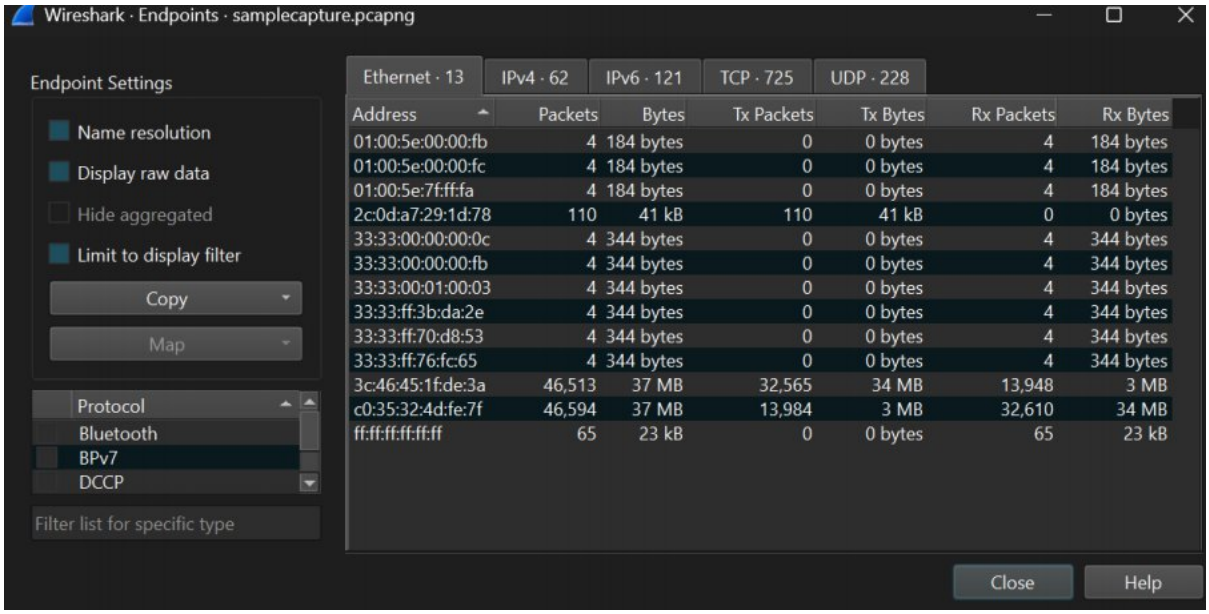
and destination hosts.



Endpoints:

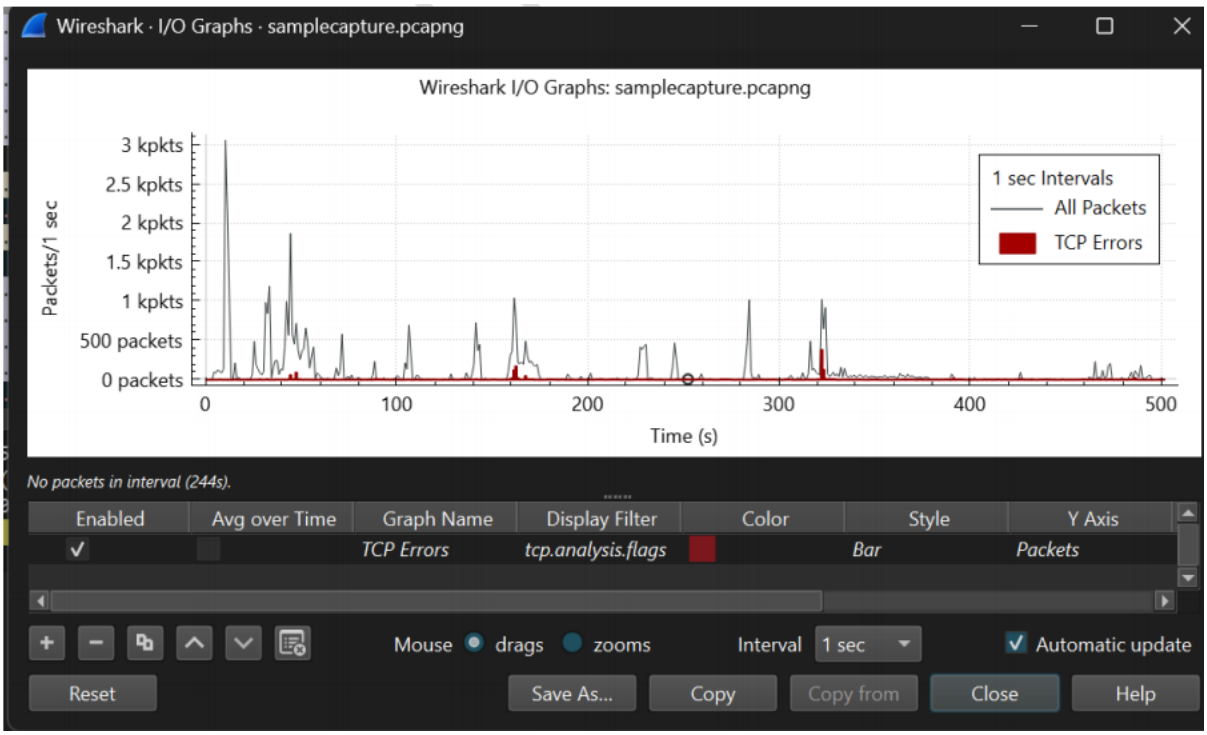
Go to Statistics > Endpoints to list all active IP/MAC addresses involved

in the capture.



I/O Graphs:

Use Statistics > I/O Graphs to visualize traffic rate and identify spikes or drops over time.



Expert Information:

Open Analyze > Expert Information to detect errors, warnings, and

retransmissions.

Result:

Thus network traffic on TCP/UDP/IP/HTTP/ARP/DHCP/ICMP /DNS were analyzed using Wireshark Tool.