08/08/2024

Experiment No.: 5 Packet Capture Tool

Aim:

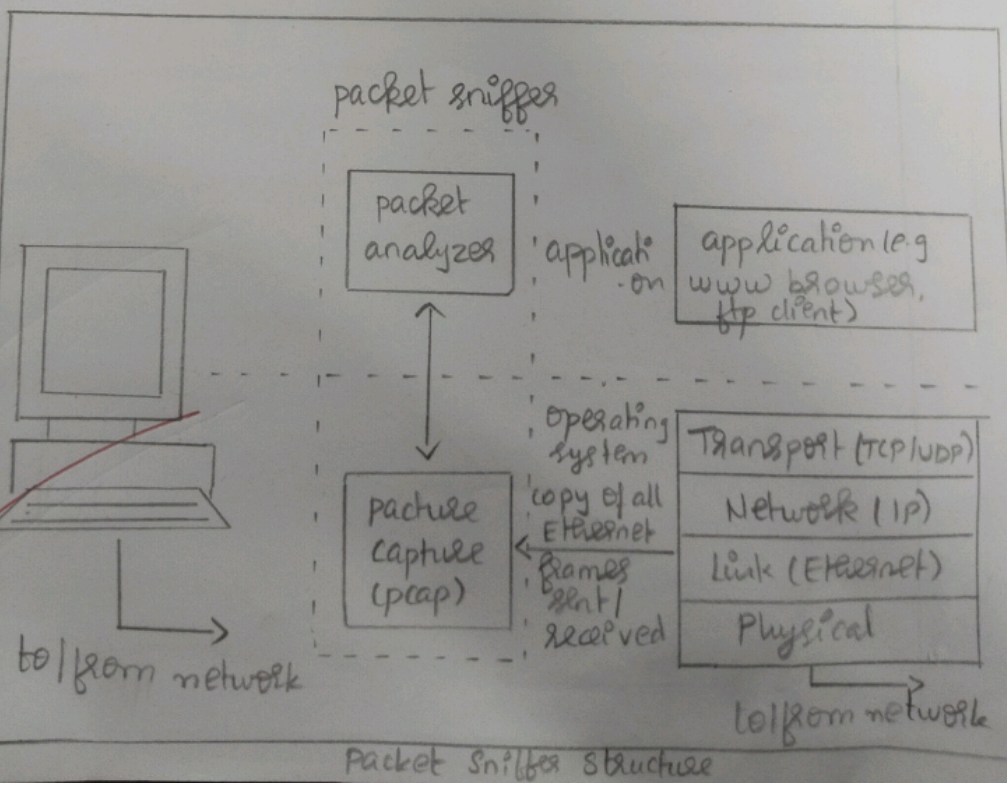
Experiments on Packet Capture Tool: Wireshark.

Packet Sniffer:

1. Sniffs messages being sent/received from/by your computer.
2. Store and display the contents of the various protocols fields in the messages.
3. Passive program
   - Never sends packet itself
   - No packets addressed to it
   - Receives a copy of all packets (sent/received)

Packet Sniffer Structure Diagnostic Tools:

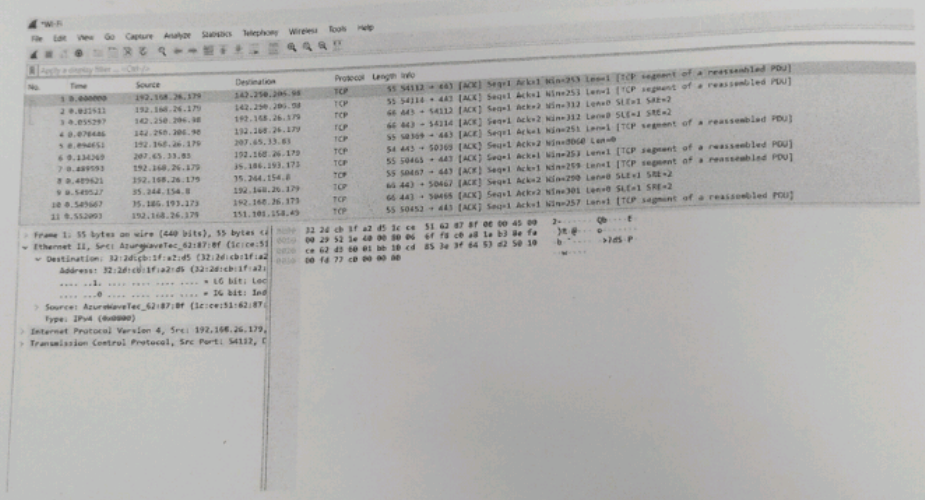
1. Tcpdump
   - Eg. tcpdump -enx host 10.129.41.2 -w ex3.out
2. Wireshark
   - wireshark -r ex3.out

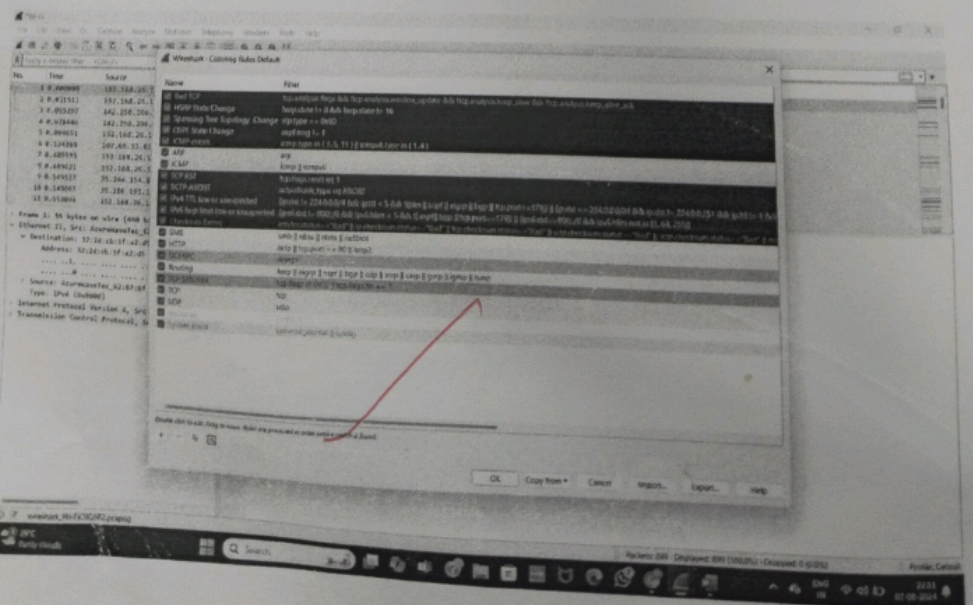


Packet Sniffer Structure

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.

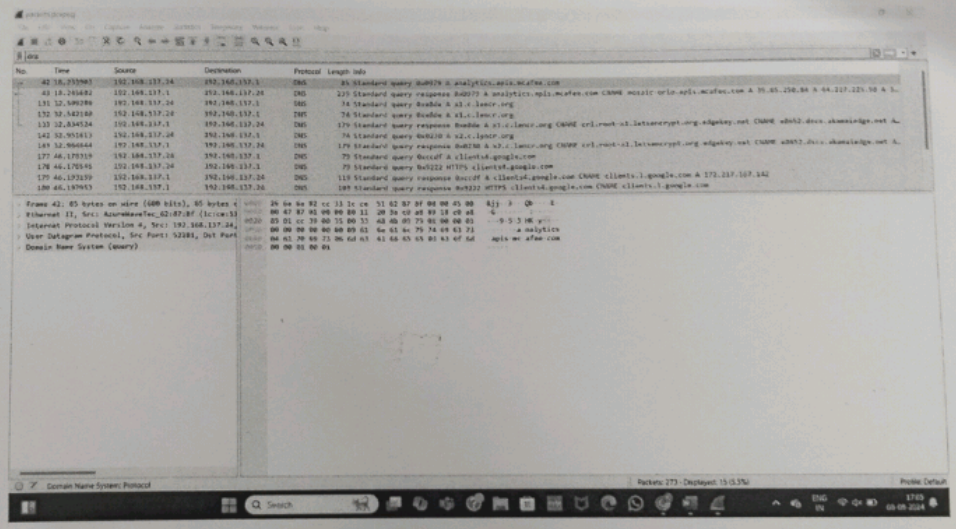


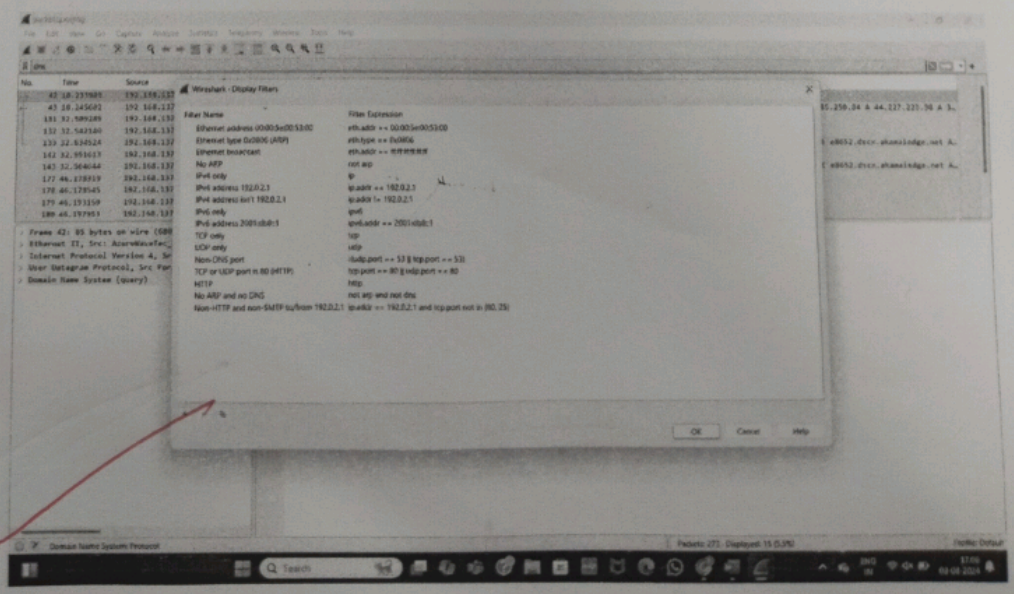


talling
click the
capture
interface.
s name,
pears in
packet

Filtering Packets:

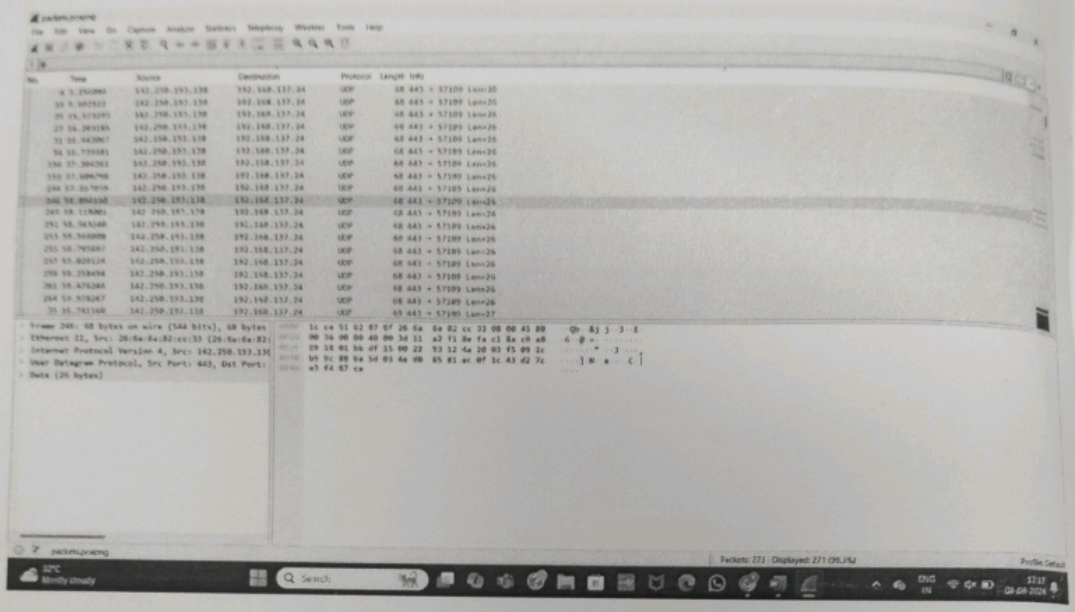
If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all others applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark filters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

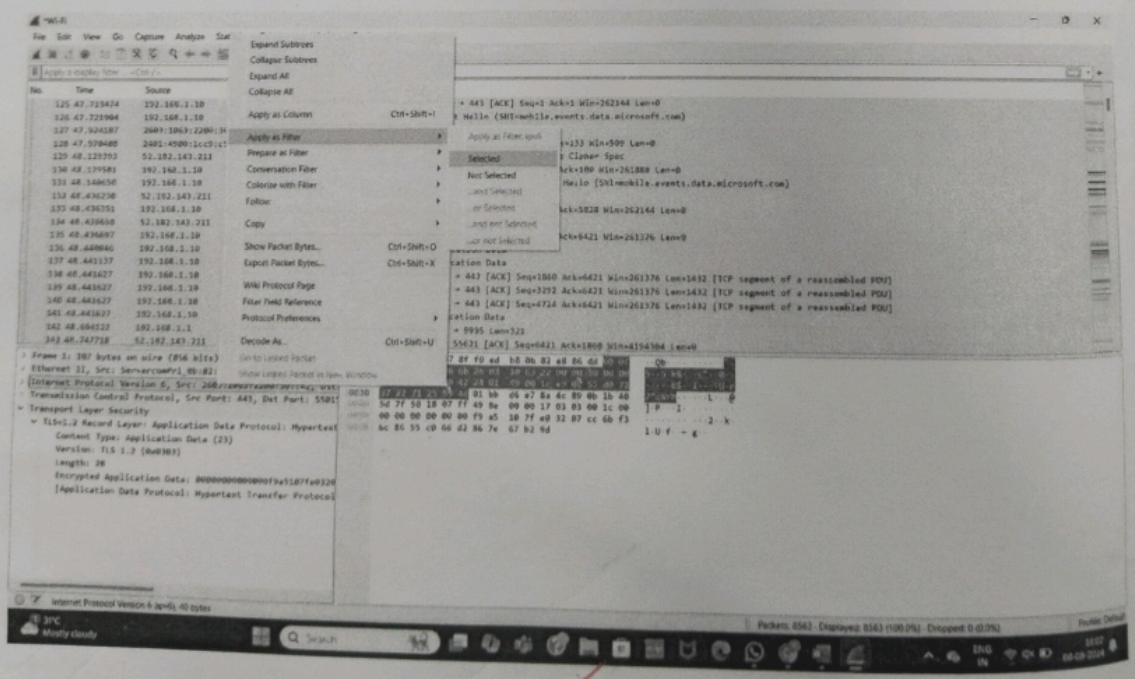


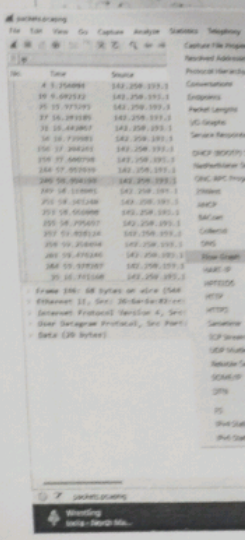


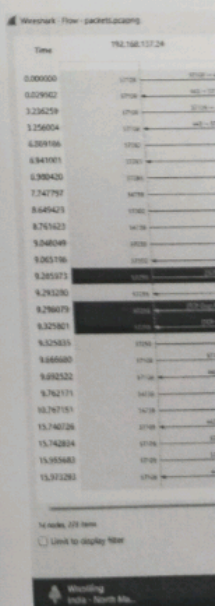
Inspecting Packets:

Click a packet to select it and you can dig down to view its details.

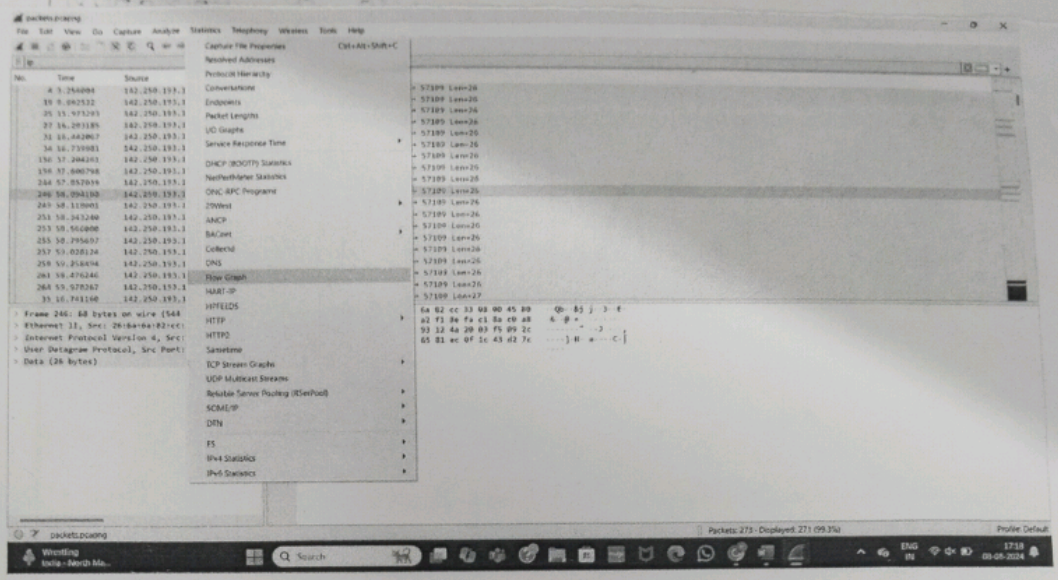


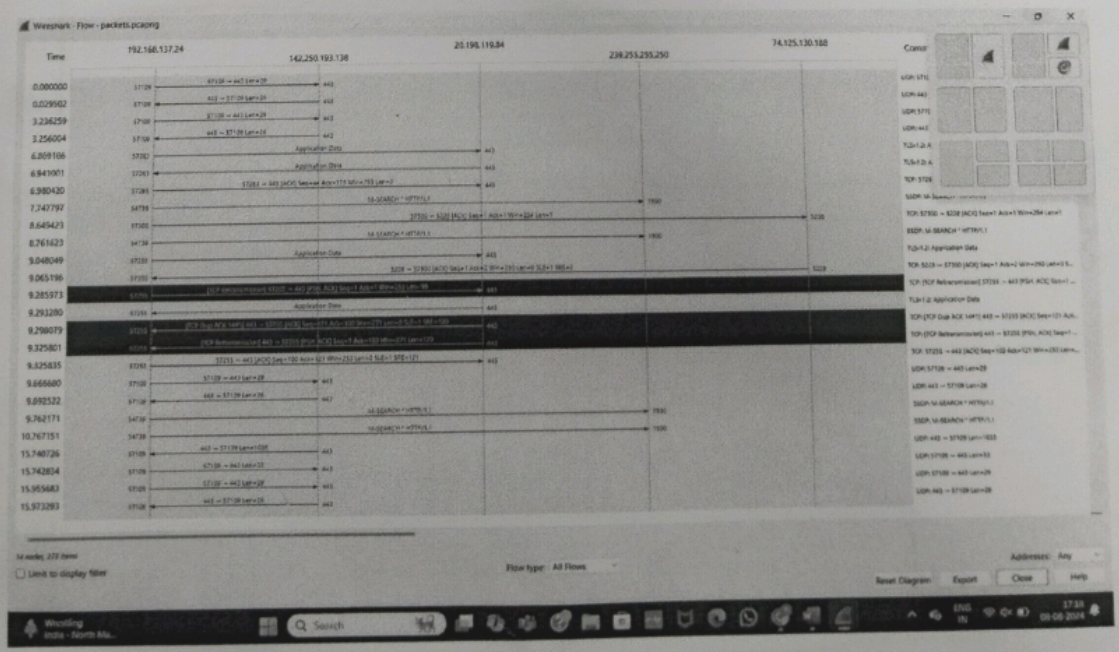






Flow Graph:


Statistics
Capture File Properties
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graphs
Service Response Time
DHCP (BOOTP) Statistics
NetPerfMeter Statistics
ONC-RPC Programs
29West
ANCP
BACnet
Collectd
DNS
Flow Graph
HART-IP
HPFEEDS
HTTP
HTTP2
Sametime
TCP Stream Graphs
UDP Multicast Streams
Reliable Server Pooling (RSerPool)
SCMIP
DTN
F5
IPv4 Statistics
IPv6 Statistics


Wireshark · Flow · packets.pcapng
Time
192.168.137.24
142.250.193.138
20.198.119.84
239.255.255.250
74.125.130.188
Flow type: All Flows
Reset Diagram
Export
Close
Help

Observation:

1) What is promiscuous mode?

Ans: It is a mode of operation where a network device can intercept and read in its entirety each packet that passes through.

2) Does ARP packets has transport layer header Explain.

Ans: ARP packets do not have a transport layer header. ARP operates at the link layer (layer 2) of the OSI model, which is responsible for local network communication between devices on the same network segment.

3) Which transport layer protocol is used by DNS:

Ans: DNS uses two transport layer protocol: 1. UDP (User Datagram Protocol)
2. TCP (Transmission control Protocol)

4) What is the port number used by http protocol

Ans: 80 is the port numbers used by http

5) What is a broadcast ip address?

Ans: A broadcast ip address is a network address used to transmit to all devices connected to a multiple-access communication network.

Result:

9/8/24 Thus, the features of wireshark as a packet capture tool is observed and studied about the encapsulation of information at various layers of a protocol layer stack.