09/08/2024

Practical 5

Aim:

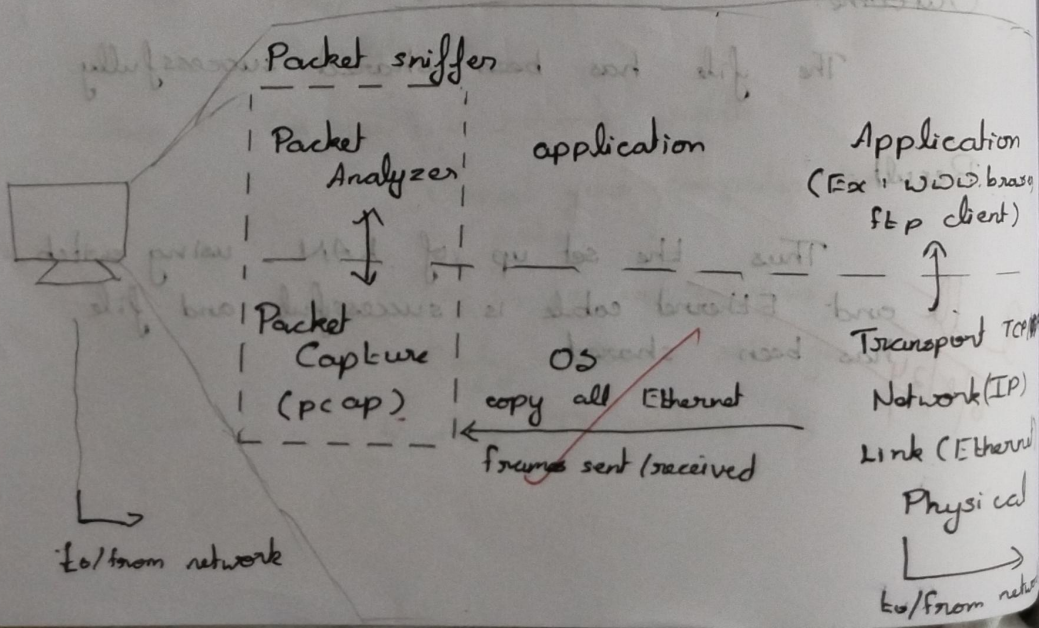
Experiments on Packet capture tool Wireshark

Packet Sniffer

- Sniffs messages being sent/received from/by your computer
- Store and display the contents of the various protocol fields in the messages.
- Passive program
  - -> Nvr sends packets to itself
  - -> No packets addressed to it.
  - -> Receives a copy of all packets

Packet Sniffer Structure: Diagnostic Tools

- TCPdump
- Wireshark



Wireshark

A network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format

What we can do?

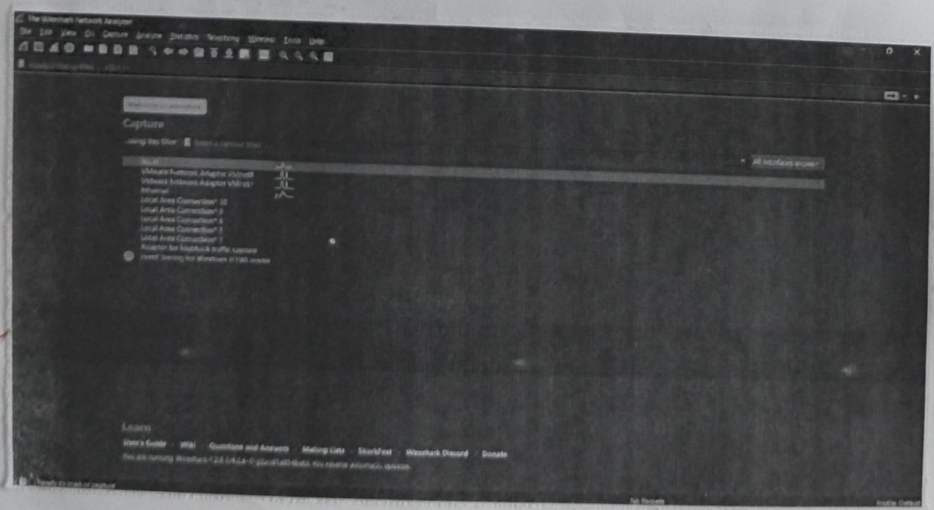
- Capture network traffic
- Analyze problems

Uses

- Network admin: Trouble shoot network problems
- Develops : Debug protocol implementations

Capturing Packets

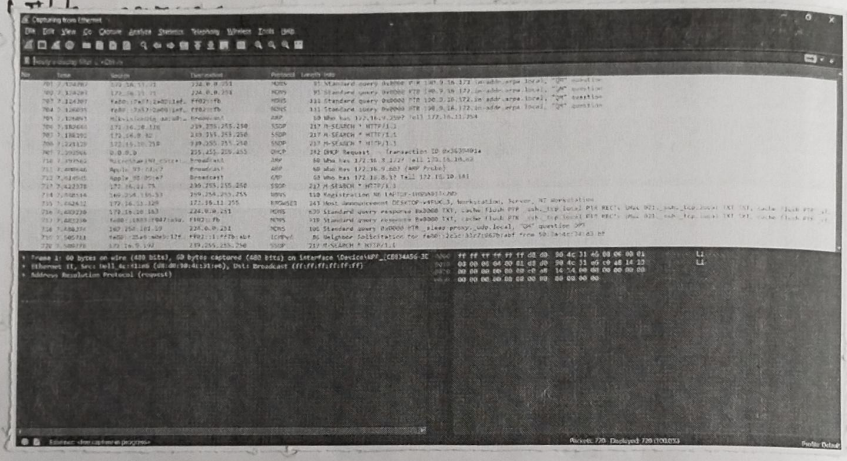
Launch Wireshark and double-click the name of a network interface under Capture to start capturing packets on the interface.



Colour Coding

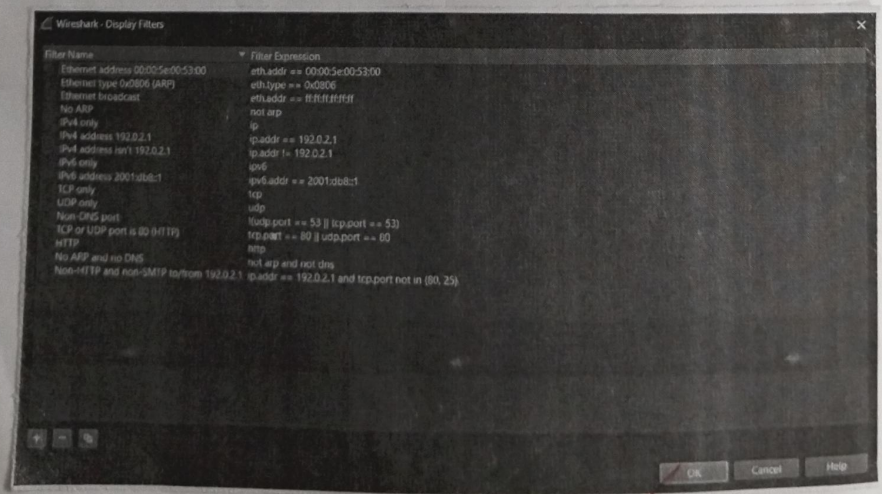
Wireshark uses colours to help you identify the types of traffic at a glance.

By default, light purple is TCP traffic, light blue is UDP traffic and black identifies packets



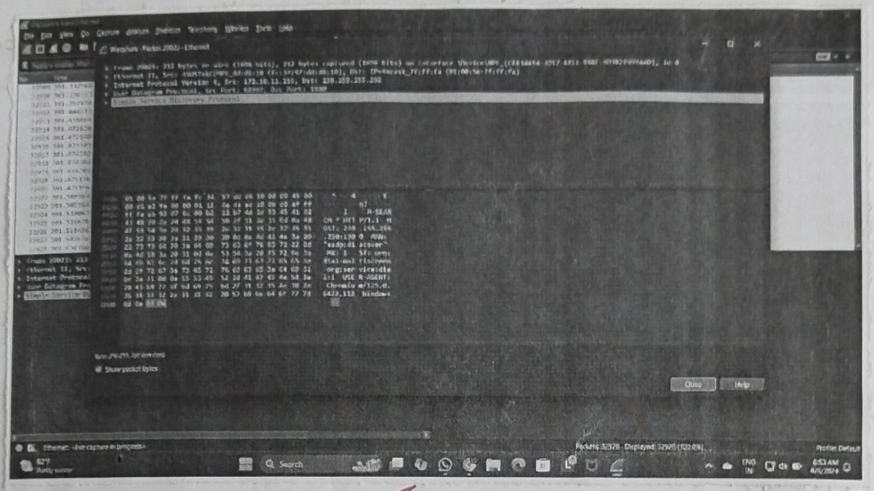
Filtering Packets

The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking apply.



Inspecting Packets

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



Student Observation

1. What is promiscous mode in Wireshark?

— Settings that allow Network Interface Card that allows the device to capture all network-traffic on the segment it is connected to.

2. Which transport layer is used by DNS?

UDP

3. Does ARP packets has transport layeyar header?

Explain

No. The operate at data link layer and are used for mapping IP to MAC address

4. What is the port number used by http protocol

80

5. What is a broadcast ip address?

Used to send a packet to all devices in the network segment.

Result:

Wireshark tool has been experimented with and packet transfer has been studied.

9/8/24