Ex. NO: 5

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 various protocol fields in the messages.

. Passive program
  - never sends packets itself
  - no packets addressed to it
  - receives a copy of all packets

Packet Sniffer Structure Diagnostic Tools

. Tcpdump
  - Eg. tcpdump -enx host 10.129.41.2 -w exe.out

. Wireshark
  - wireshark -r exe3.out

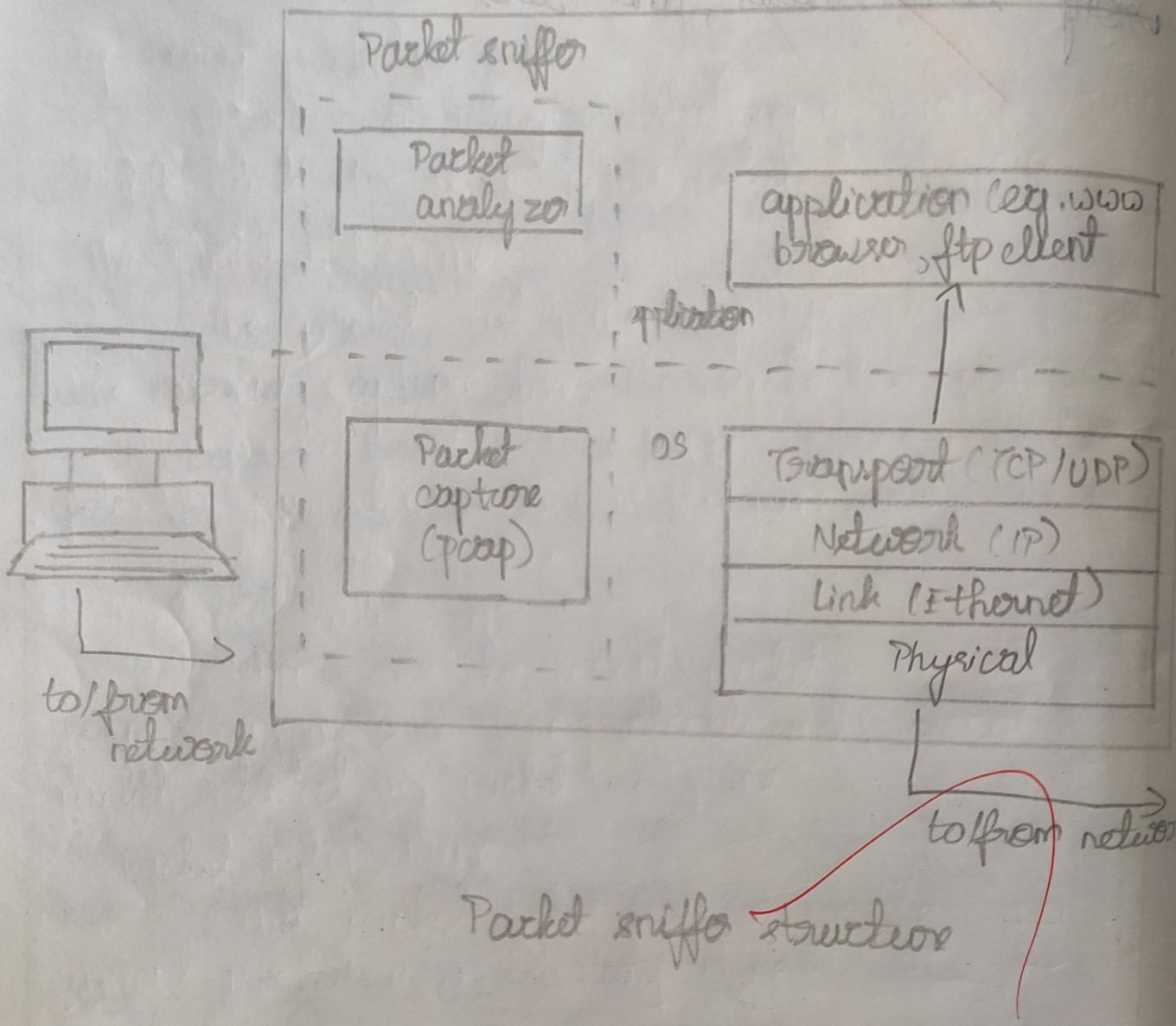
Description:

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.

What we can do with Wireshark:

. Capture network traffic
. Decode packet protocols using directors
. Define filters - capture and display
. Watch smart statistics.
. Analyze problems
. Interactively browse the traffic.



Packet sniffer structure

Wireshark used for:
- Network administrators: troubleshoot network problems
- Network security engineers: examine security problems
- Developers: debug protocol implementations.

Getting wireshark:

Wireshark can be downloaded for Windows or macOS.

Captuaring packets:

After downloading & installing wireshark, launch it double-click the name of a network interface.

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 capture file. If you select a line in this pane, more details will be in "Packet Details" panes

"Packet Details" Pane

This shows the current packet in a more detailed form. This pane shows the protocols and protocol fields of packet selected in "Packet List" pane.

"Packet Bytes" Pane

This packet bytes pane shows the data of the current packet in a hexdump style.

Color Coding

Packets highlighted in a variety of different colors Wireshark uses colors to help you identify the types of traffic at a glance.

Sample Captures

If there's 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.

Filtering packets;

To inspect something specific, such as 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.

Capturing and analyzing packets:

Procedure:

i) Select local area Connection is wireless.
ii) Go to capture → option
iii) Select stop capture after 10 packets.
iv) Then click start capture.

1. Procedure:
   → Select LAN in wireshark
   → Go to capture → option
   → Select stop capture
   → search Tcp packets in search bar.
   → Save packets.
2. Create a file to filter display ARP Packet.
   → Go to capture → option
   → Select stop capture hub for 100 packets.
   → Then stop capture and save.

Result:

Thus wireshark tool is used to handle and inspect packets.