Ex. No: 05

DATE : 11-9-25

PACKET CAPTURE TOOL.

(16)

(25)

AIM:

Experiments on packet capture tool wireshark.

Packet Sniffer:

: Sniff messages being sent / received from / by your computer.

- Store and display the contents of the various protocol fields in the messages.

: Passive program

- never sends packet 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 ex3.out.
- Wireshark.
  - Wireshark → ex3.out.

Description:

WIRESHARK.

It's a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format.

Steps:

. open wireshark and select the network interface (eg. local to area connection).

. Go to capture → options.

. Check stop capture automatically after 100 packets.

. click start capture to begin capturing packets.

. once capture stops apply filters to display specific packets by typing the protocol name in the filter box.

. Inspect the filtered packets, their detailed fields.

. For TCP or DNS packets, generate a flow graph by clicking statistics > flow graph.

. Save the captured packets using file > Save as < file name >.

Result:

Hence, the capturing network packet on local interface using wireshark, applying filters to display specific protocol packets, analysing two packet detail, flow graph is done.

10/10 9/10