Ex: 5 Experiment on Packet Capture tool: Wireshark.

Aim: Experiment on packet capture tool: Wireshark.

Wireshark: A network analysis tool that captures real time network packets and displays them in human readable format.

Key features:
1) Real time packet capture
2) Filtering
3) Protocol decoding using dissectors
4) Traffic browsing and smart statistics.

Uses of Wireshark:
1. Network Admin: Trouble shoot network issue.
2. Analysis security incidents
3. Debug network protocol implementation
4. Understand protocols internals.

Window: Download wireshark from official website.

a) Capturing packets:

Launch wireshark and double click a network interface to begin capturing packets.

Packets appear in real time and include all traffic of promiscous mode is enabled (Capture > options > enable promiscous mode.

b) Coding Colour:

Using of light purple to TCP.
Light blue for UDP
Black refer to error packets
View (or) customize colour: view → Colouring rule.

c) Sample capture:-

* Load sample capture from wireshark, wifi via file > open.
* Save your own capture using file > save.

d) Filtering packets:-

a) Use the filter bar to isolate traffic

* Press enter (or) click Apply

* Access default/custom filter via analyse → display filter.

e) Following TCP streams:

* right click a packet → follow → TCP stream.
* close window auto apply a filter for that conversion.

Inputing packets:

* click a packet to see its details.
* Right click protocol fields → apply a filter based on it.

Flow graph:

* Use statistics
* Visually traffic flow between devices flow graph.

Capturing and analysing using wireshark tool:

Procedure:

* Select Local Area selection.
* Capture > options > set stop after 100 packets.
* click start
* save packets

Filter: Display TCP/UDP packets and show flow graph.

procedure:

* Start capture as above
* In filter bar, search tcp or udp.
* statistics > flow graph to view.
* save packets.

Filter: Display only ARP packets:

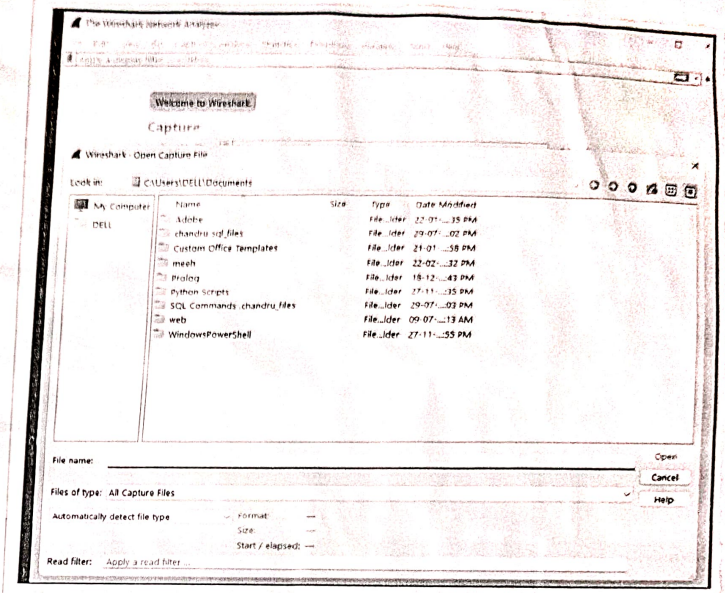
* Start capture as above
* In filter bar, type UDP
* save packets.

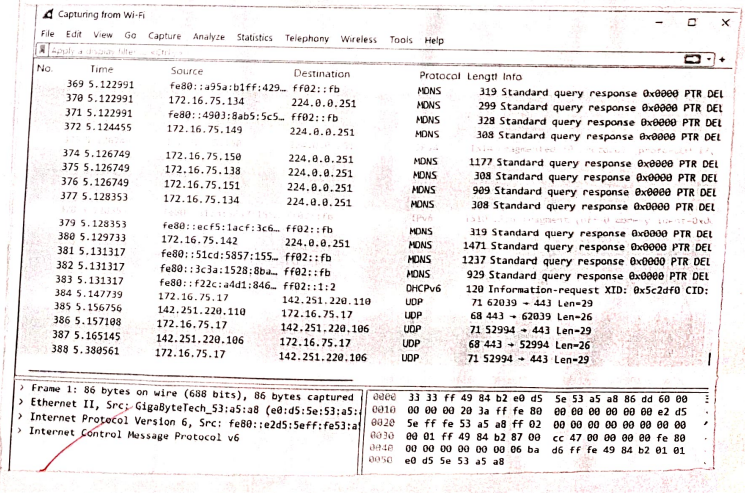
Filter: Display only DNS packets and show flow graph.

* Start capture as above
* In filter bar, type dns
* statistics > flow graph to view
* save packets.

Filter: Display only HTTPs packets:

* Start capture as above.
* In filter bar, type HTTP...
* Save presets.





Student Observation:

1) What is promiscous mode?

It allows a network device to capture all packets on the network, not just those addressed to it.

2) Does ARP packets has transport layer header? explain?

No, ARP operates at data link and network layer and does not have a transfer layer header.

3) Which transport layer protocol is used by DNS

DNS uses UDP by default and TCP for large queries like zone transfer.

4) What is the port number used by http protocol?

Port is used by http protocol.

5) What is broadcast ip address?

It is 255.255.255.255 used to send data to all hosts on a local network.

Result:

Thus the above experiment successfully completed and executed.