EXP NO: 5
DATE: 31.07.25

Experiment on packet capture tool WIRESHARK

AIM:

To capture and analyze network packets using wireshark and apply filters to display specific Protocols.

Packet Sniffer:

⇒ Sniffs messages being sent/received from/by your computer.
⇒ store and displays the contents of the various protocols fields in the message.

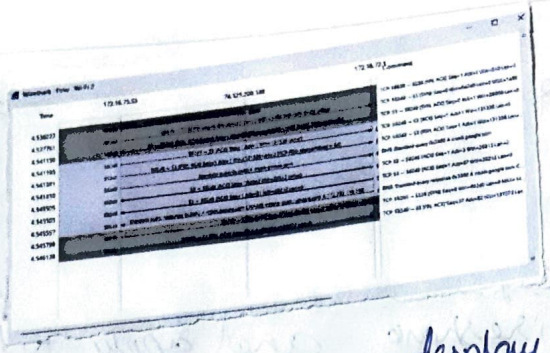
DESCRIPTION:

Wireshark, a network analyser tool formerly known as Ethereal, captures packet in real time and displays them in human-readable format. wireshark includes filters, color coding and other features that let you dig deeper into network traffic and inspect individual packets.

Capturing and Analysing packets using wireshark tool
⇒ To filter, capture, view packets in wireshark tool
⇒ capture 100 packets from the Ethernet/IEEE 802.3 LAN interface and Save it.

Procedure:

⇒ Select Local area connection in wireshark
⇒ Go to capture → option

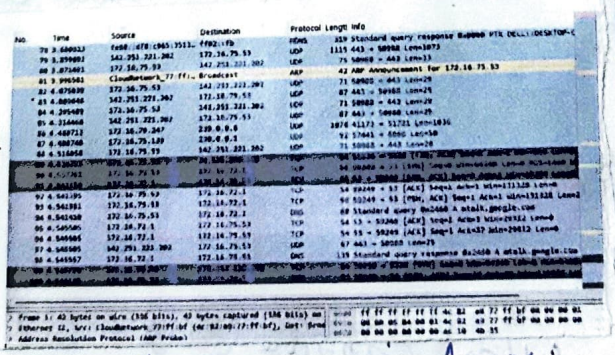


1. Create a filter to display only TCP / UDP packet inspect the packets and provide the flow graph.

Procedure:

→ select LAN in wireshark
→ Go to Capture → Option
→ select Stop Capture automatically after 100 Packets.
→ Search TCP packets in search box.
→ To see flow graph click statistic → flow graph

Flow Graph:



2. Create a filter to display only ARP packets and inspect the packets.

Procedure:

→ Search ARP packets in search box
→ Save the packets

splay only TCP / UDP
and provide the

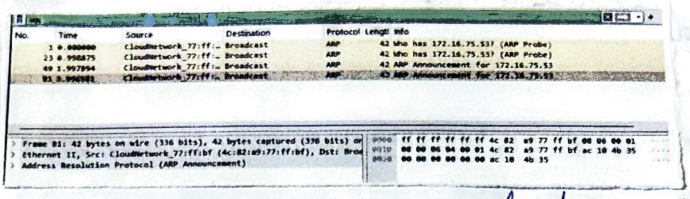
shark
on
tomatically after 100

search box.
click statistic
→ flow graph

ay only ARP
ts.

search box

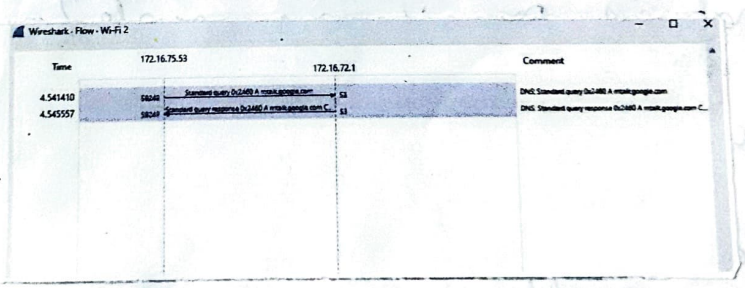
Output:



3. Create a filter to display only DNS packets and provide the flow graph

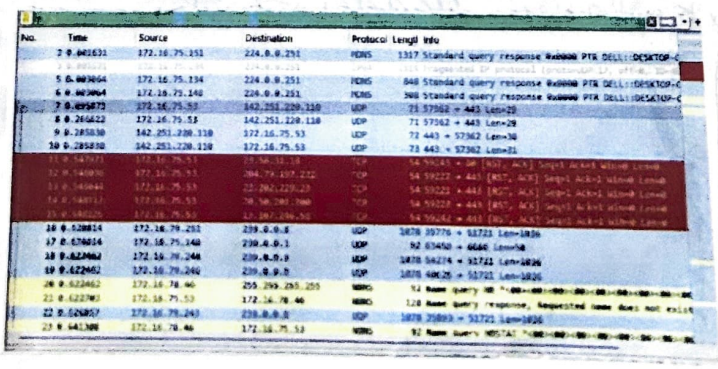
Procedure:
→ search DNS packets in search bar.
→ To see flow graph click Statistics → flow graph
→ Save the packets

Output:



4. Create a filter to display only IP/ICMP packets and inspect the packets.

procedure:
→ search IP packets in search bar
→ Save the packets.



3) Create a filter to display only DHCP packets and inspect the packets.

Procedure:

→ search DHCP packets in the search box
→ Save the packets.

Student observation:

1) What is promiscuous mode?

Promiscuous mode is a setting for a network interface card (or IC) that allows it to capture all network packets, passing through it regardless of the destination MAC address.

2. Does ARP packets has transport layer Header? : Explain.

No, ARP Packets "DO NOT have" transport layer Header. It sits between the network and data link layers - there is NO TCP or UDP involved so no transport layer existing.

3. Which transpo
It uses UD
TCP for large

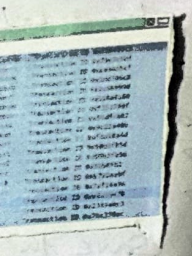
4. What is t
protocol?
. It us

5. What is
Address
network: C

RESULT:
. Th
tools

splays only DHCP packets

ets in the search box



node?

a setting for a
NIC that allows it
packets, passing
the destination

transport layer

not have
between the
es - there is
so no transport

3. Which transport layer protocol is used by DNS?
It uses UDP for normal queries and TCP for large responses/zone transfers.

4. What is the port number used by HTTP protocol?
It uses port 80 by default.

5. What is broadcast IP address?
Address to reach all hosts in a network.

RESULT:
Thus the experiments on packets capture tools: WIRESHARK has been done successfully.