Ex NO: 5 EXPERIMENT ON PACKET CAPTURE

DATE: 14.08.2025 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 display the contents of the various protocol fields in the message.

Description:

wireshark, a network analysis tool formerly known as Ethereal, captures packet in real time and display 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

→ select stop capture automatically after 100 packets

Procedure :

→ select local Area connection in wireshark

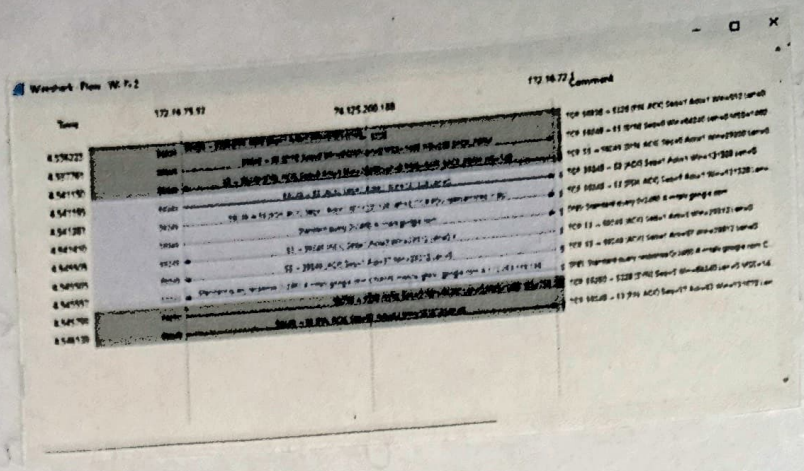
→ go to capture → option

→ select stop capture automatically after 100 packets.

→ then click start capture

→ save the packets.

output :



1) Create a filter to display only TCP, UDP packets the packets and provide the flow graph.

Procedure.

⇒ Select LAN in wireshark

⇒ go to capture → option

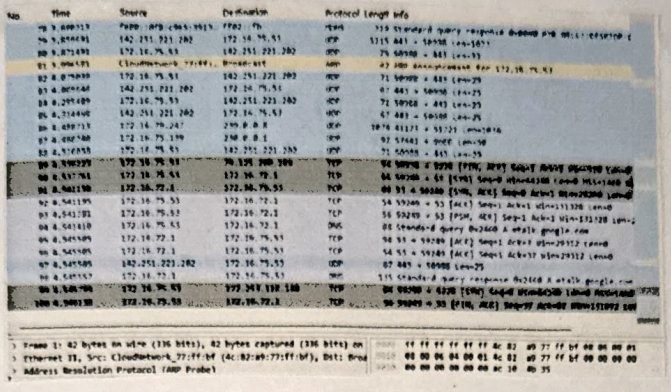
⇒ select stop capture

⇒ search TCP packets in search bar.

⇒ to see flow graph click statistics → flow graph

→ save the packets.

Flow graph :



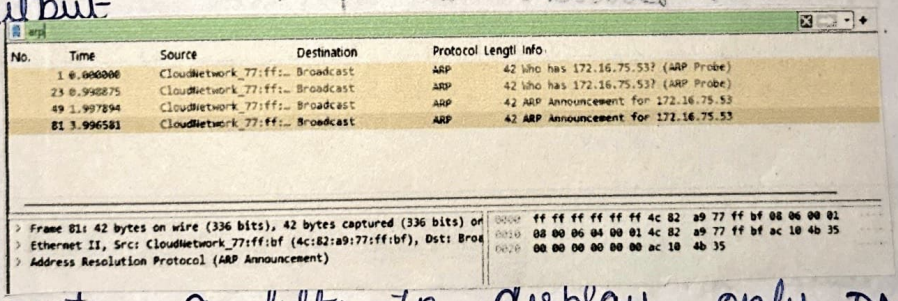
2) Create a filter to display only ARP packets and inspect the packets.

Procedure:

→ search ARP packets in search bar

→ save the packets.

output:



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

Procedure:

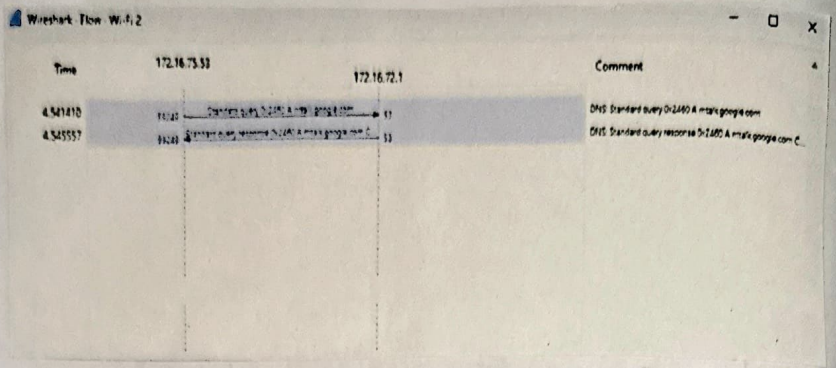
→ search DNS packets in search bar.

→ to see flow graph click Statistics

→ flow graph.

→ save the packets.

Output :



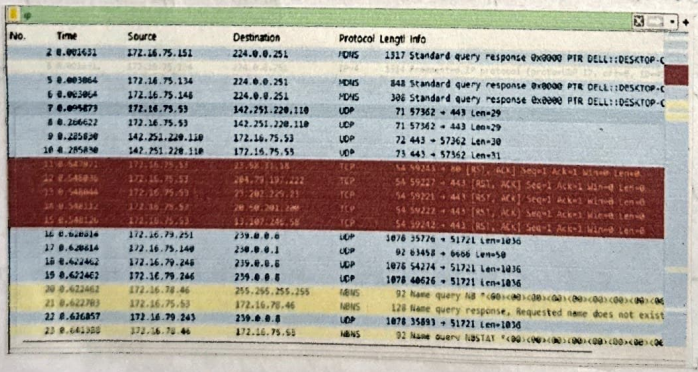
4) Create a filter to display any IP | ICMP Packets and inspect the packets

Procedure :

→ Search IP packets in search bar

→ Save the packets

Output



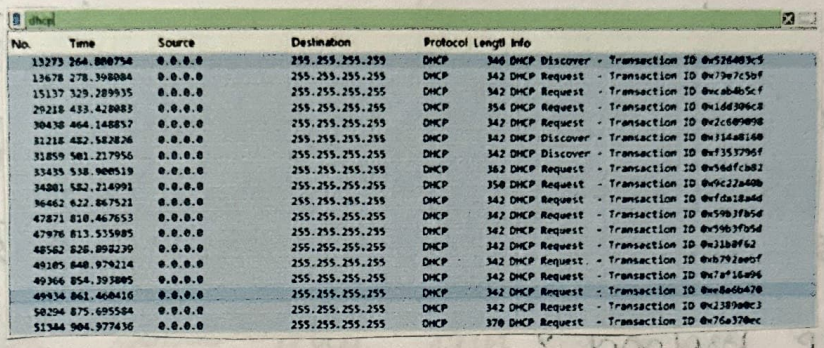
5) Create a filter to display only DHCP packets and the packets

Procedure:

→ search DHCP packets in search bar.

→ save the packets.

output:



No.	Time	Source	Destination	Protocol	Length	Info
13273	264.800758	0.0.0.0	255.255.255.255	DHCP	346	DHCP Discover - Transaction ID 0x526483c5
13678	278.398084	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x79e7c5bf
15137	329.289935	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xcab4b5cf
29218	433.428883	0.0.0.0	255.255.255.255	DHCP	354	DHCP Request - Transaction ID 0x1dd3096c8
30438	464.148857	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x2c609098
31218	482.582826	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3144a8140
31859	501.217956	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xf353796f
33435	538.900519	0.0.0.0	255.255.255.255	DHCP	362	DHCP Request - Transaction ID 0x56dfcb82
34081	582.214991	0.0.0.0	255.255.255.255	DHCP	350	DHCP Request - Transaction ID 0x9c22a40b
36462	622.867521	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xfda18a4d
47871	810.467653	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x59b3fb5d
47976	813.535985	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x59b3fb5d
48562	828.898239	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x31b8f62
49105	848.979214	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xb792ee0f
49366	854.393805	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x7af16a96
49434	861.460416	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xe8e6b470
50294	875.695584	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x2389e0c3
51344	904.977436	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x76a370ec

Student observation:

1) what is promiscuous mode?

Ans: Promiscuous mode is a setting for a network interface card (NIC) 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.

Ans: NO, ARP packets do not have a transport layer header. it sits between the network and data link layer - there is no TCP or UDP involved,

so no transport layer header exists.

3. which transport layer protocol is used by DNS?

Ans: It uses UDP for normal queries and TCP for large responses / Zone Transfer

4. what is the port number used by HTTP protocol?

Ans. It uses PORT 80 by default.

5) what is broadcast IP address?

ANS: Address to reach all hosts in a network (192.168.1.255/24)

RESULT:

thus the experiment on packet capture tool: wireshark has been done successfully.