Ex No: 5 Experiment on Packet Capture
DATE: 27/7 Tool: WIRESHARK.

Aim:
To capture and analyze network packets using wireshark and apply filters to display specific protocols.

Packet Sniffer:

→ sniffs message 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.

Getting Wireshark :-

Wireshark can be downloaded for windows or macOS from its official website.

Capturing packets :

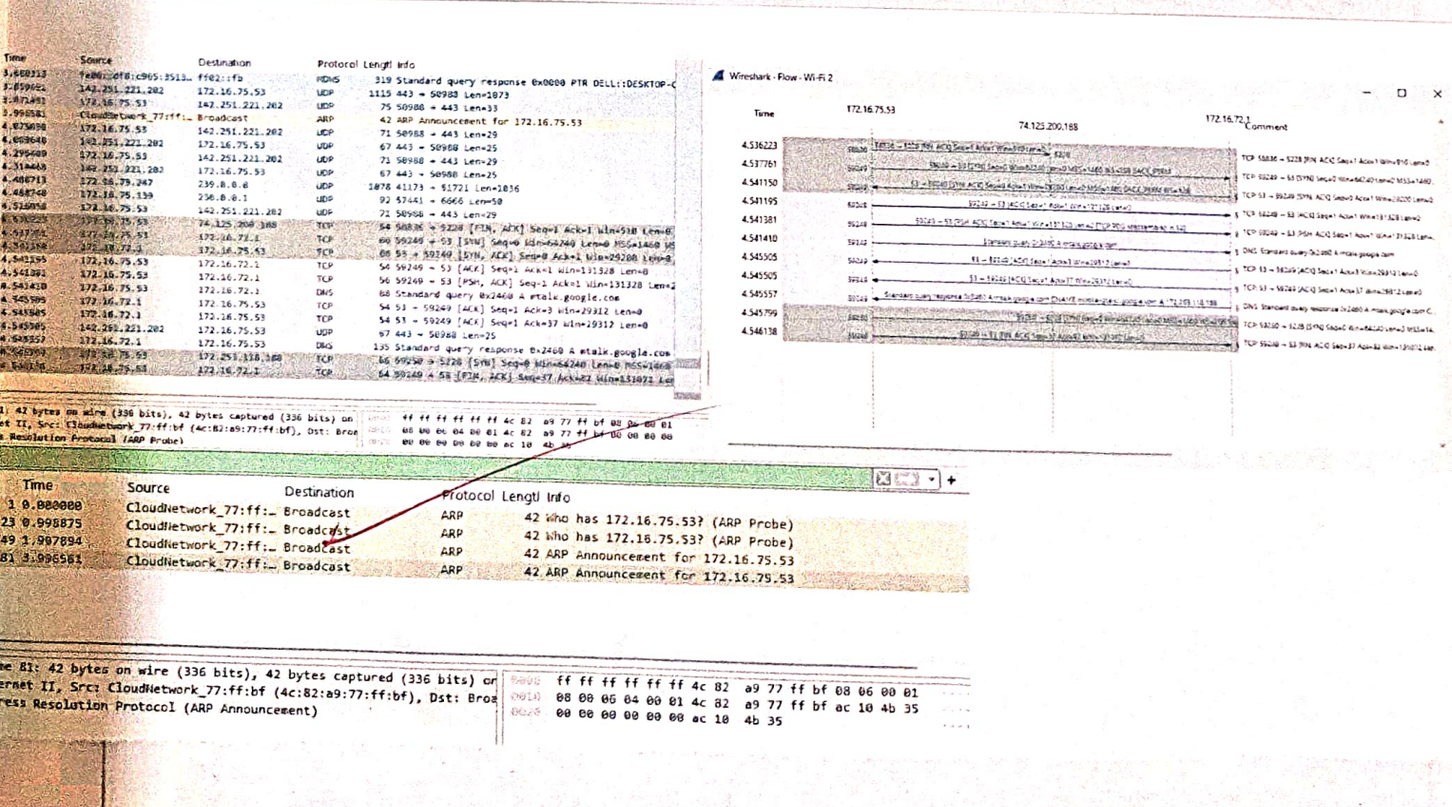
After downloading and installing wireshark launch it and double-click the name of a network interface under capture to start capturing packets on that interface.

The "Packet Bytes" Pane

The packet byte pane shows the data of the current packets I selected in the "Packet List" pane in a hexdump style

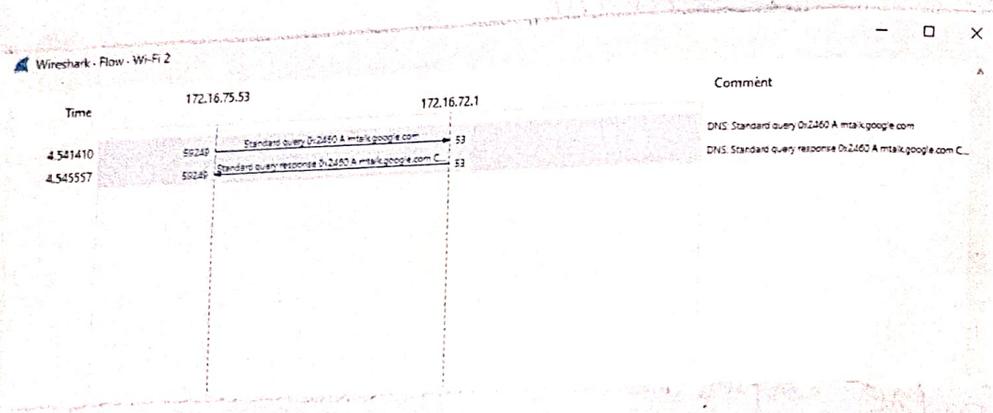
Sample Captures

If there's nothing interesting on your network to impact, wireshark's wiki has you covered

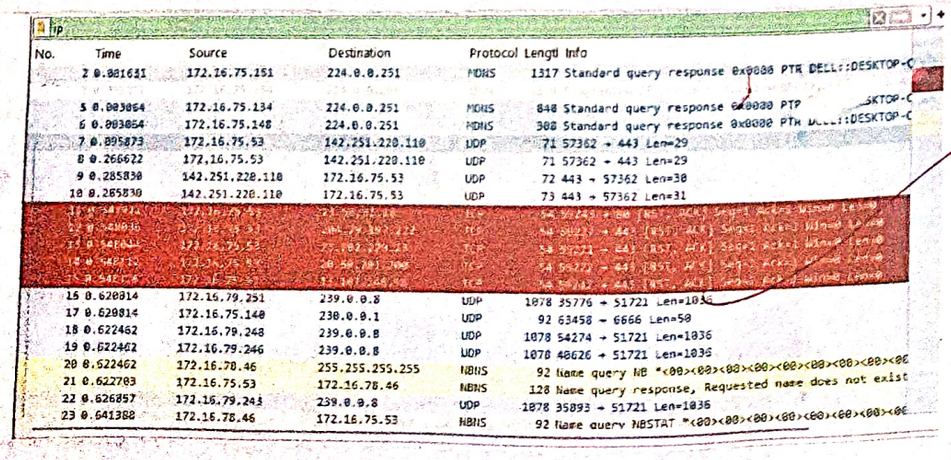


Filtering packet :-

If you're trying to impact something specific, such as the traffic a program sends when phoning home, it helps to close down the traffic. still, you'll likely have a large amount of packets to shift through. That's where Wireshark's filters come in.

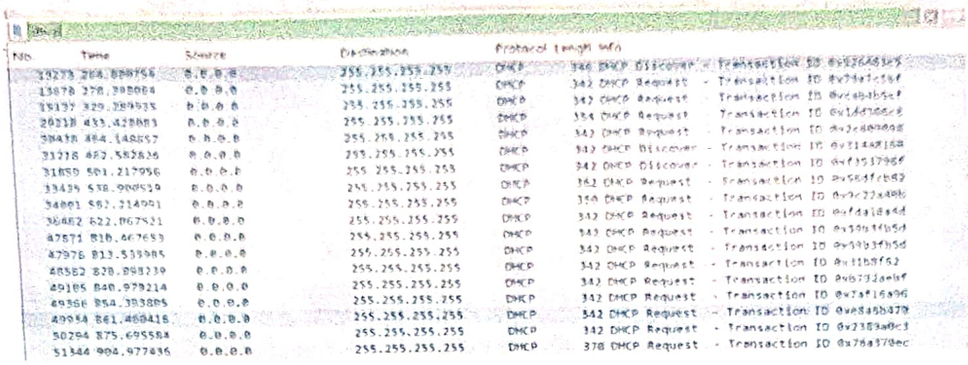


You can also click Analyze > Display Filters to choose a filter from among the default filters included in Wireshark Close the window and you'll find a filter has been applied automatically Wireshark is showing you the packets that make up the conversion.



Inspecting packets :-

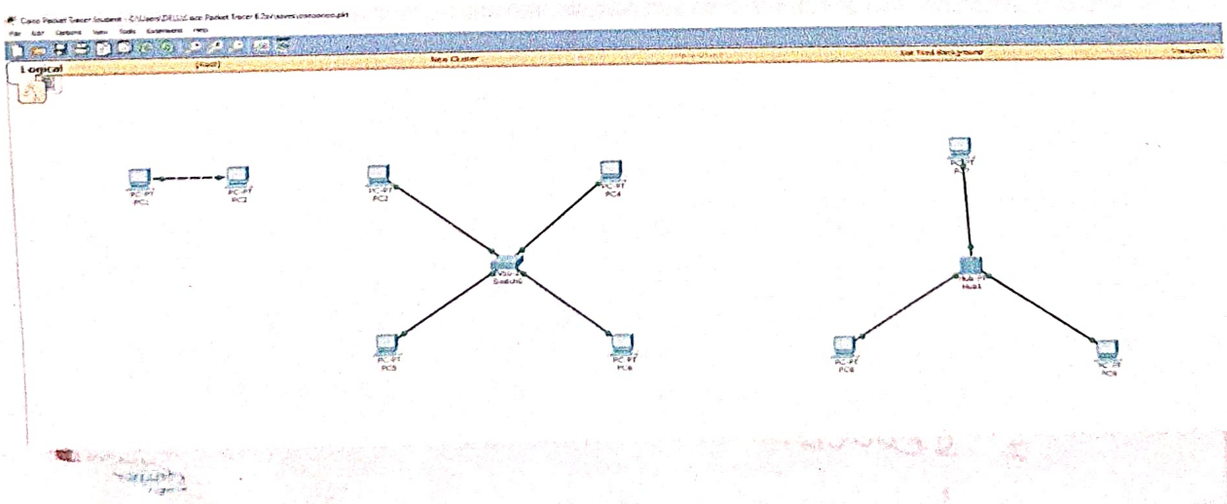
click a packet to select it and you can dig down to view its details



No.	Time	Source	Destination	Protocol	Length	Info
39279	268.898756	0.0.0.0	255.255.255.255	DHCP	346	DHCP Discover - Transaction ID 0x52648165
13878	270.388084	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x74e7c56f
19197	329.289933	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xc4b4b5cf
20218	433.428883	0.0.0.0	255.255.255.255	DHCP	354	DHCP Request - Transaction ID 0x1d47065e
38438	464.148857	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x2c4d0008
31218	482.582836	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3144f188
31859	501.217956	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xf3517986
33439	578.900559	0.0.0.0	255.255.255.255	DHCP	362	DHCP Request - Transaction ID 0x5b1fcb82
34001	582.214091	0.0.0.0	255.255.255.255	DHCP	350	DHCP Request - Transaction ID 0x2c22a486
36482	622.067521	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xfda18a4d
47571	810.467653	0.0.0.0	255.255.255.255	DHCP	343	DHCP Request - Transaction ID 0x599a14b5d
47976	813.533985	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x599b34b5d
48582	828.898239	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x11b9f62
49105	840.979214	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x6731a4bf
49356	854.383885	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x7af16a96
49954	861.469418	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xe845b479
50294	875.695584	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x2383a0c1
51344	904.977496	0.0.0.0	255.255.255.255	DHCP	378	DHCP Request - Transaction ID 0x78a370ec

You can also create filters from here - just - right - click one of the details and use the Apply as filters submenu to create a filter based on it.

Flow Graph :- Gives a ~~better~~ understanding of what we see.



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:

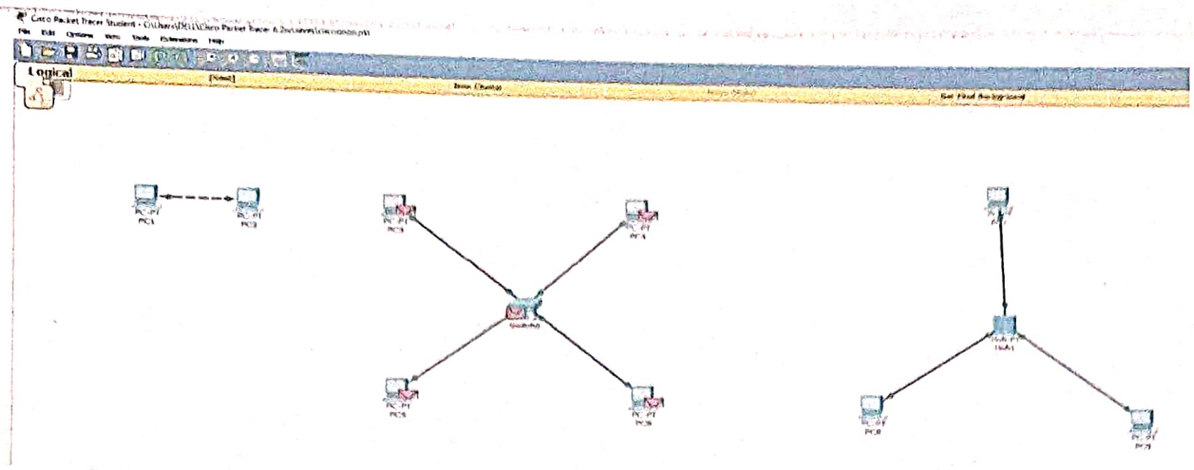
- Select Local Area connection in wireshark
- go to capture → option
- Select stop capture automatically after 100 packets.
- Then click stall capture & save the packets.

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

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

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

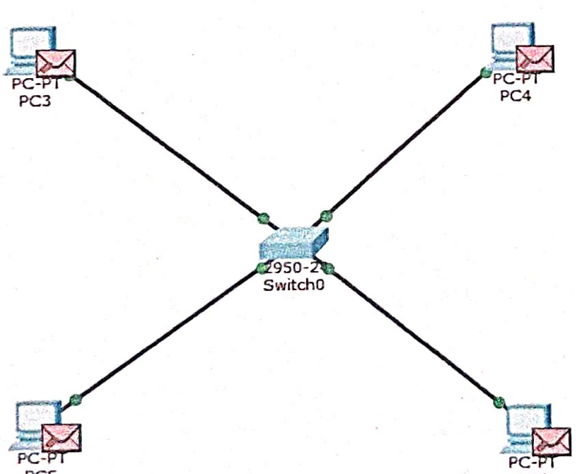
   * Go to captured → option
   * Select stop capture automatically after 100 packets.
   * then click start capture.
   * search DNS packets in search bar
   * To see flow graph click statics → Flow graph
   * Save the packets



4. Create a filter to display only HTTP packets and inspect the packets.

procedure:

- select Local Area connection in wireshark
- Go to capture → option
- select stop capture automally after 100 packet
- Then click start capture.
- search HTTP packets and save packets.



5. create a filters to display only IP / Icmp packets to Inspect the packets.

- Select local Area connection in Wireshark
- Go to capture → option
- select stop capture automatically after 100 packets.
- think click start capture
- select search ICMP/ IP packets in search box
- save the packets.

6. Create a Filter to display only DHCP packets and inspect the packets

Student Observation :-

1) What is promiscuous mode?

Promiscuous mode is a setting for a network interface card (NIC) where it captures all network packets that pass through it, not just the ones addressed to it. It is used in packet switching and network Monitoring

2) Does ARP packets have transport layer header? Explain

No, ARP (Address Resolution protocol) packets do not have a transport layer header, ARP works at Datalink Layer to map an IP address to MAC addresses.

3) Which transport layer protocol is used by DNS?

DNS can use: UDP on port 53 for most queries (factor) TCP on port 53 for tasks like zone transfers or responses exceeding 512 bytes.

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

HTTP uses port 80 (TCP) for secure HTTP (HTTPS) the port is 443 (TCP).

5. What is a broadcast IP address?

A broadcast IP address is An address used to send data to all hosts in a network simultaneously.

In IPV4, it's highest address in a subn

Eg:-

For network 192.168.1.0/24, the broadc is 192.168.1.255

15/10/2

Result:

Experiments on packet capture tool. wireshark was ~~supplied~~ successfully studied.