Experiments on packet capture tool : Wireshark

Aim: Experiments on Packet Capture tool : Wireshark Exp No: 5

Packet Sniffer:

- Sniffs messages being Sent / Received from / by your Computer.
- Store and display the contents of the various Protocols / fields in the messages.
- Passive program
  - never sends packet itself
  - no packets addressed to it.
  - receives a copy of all packets (sent / received)

Packet Sniffer Structure Diagnostic Tools :-

- Tcpdump
  - E.g. tcpdump -enx host 10.129.41.2 -w exe3.out
- Wireshark
  - wireshark -r exe3.out

Wireshark:

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

What we can do with wireshark:

- Capture network traffic
- Decode packet protocols using dissectors
- watch smart statistics
- Analyze problems.

Wireshark used for:

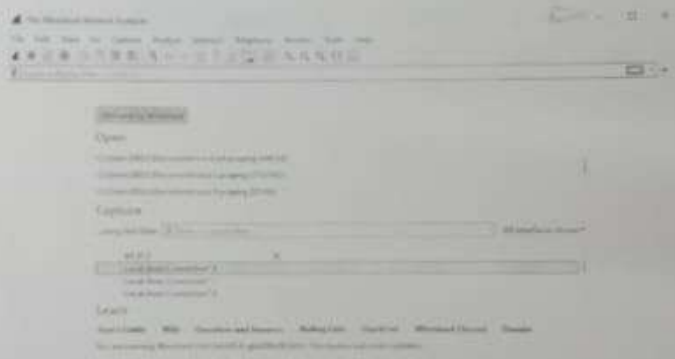
- Network administrators: Troubleshoot network problems
- Developers: Debug protocol implementations
- people: Learn network protocol internals

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 Bytes pane shows the data of the current packet (selected in the "Packet list" pane) in a "hexdump" style.

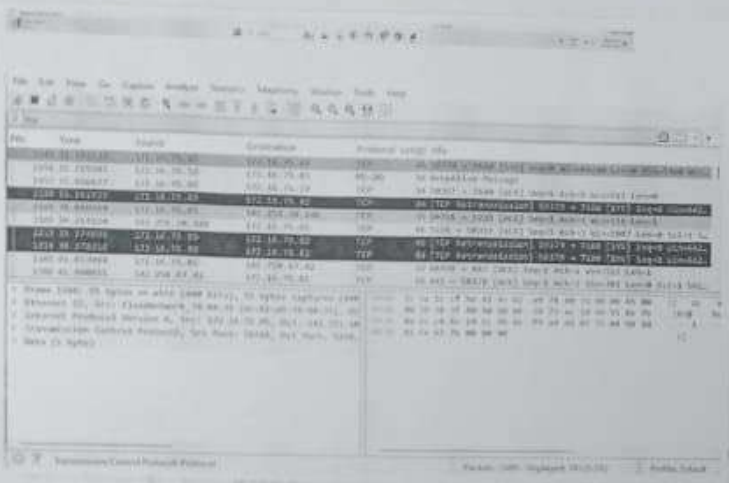
Sample Captures:-

If there's nothing interesting on your own network to inspect, Wireshark's wiki has you covered.

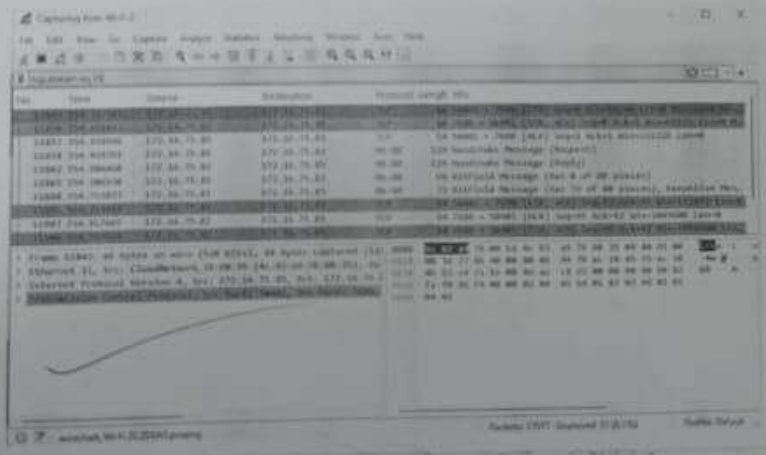
Filtering packets:-

If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using network so you can narrow down the traffic

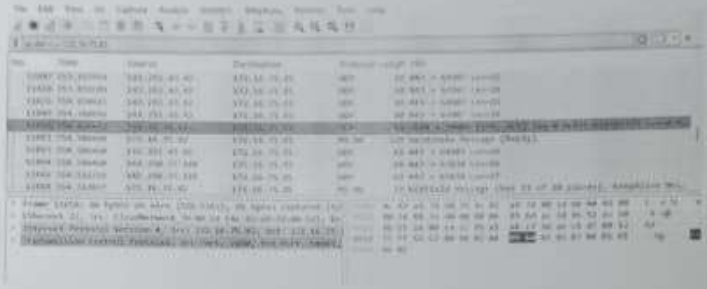
Still you'll likely have a large amount of packets to sift through. That's where wireshark's filters come in.



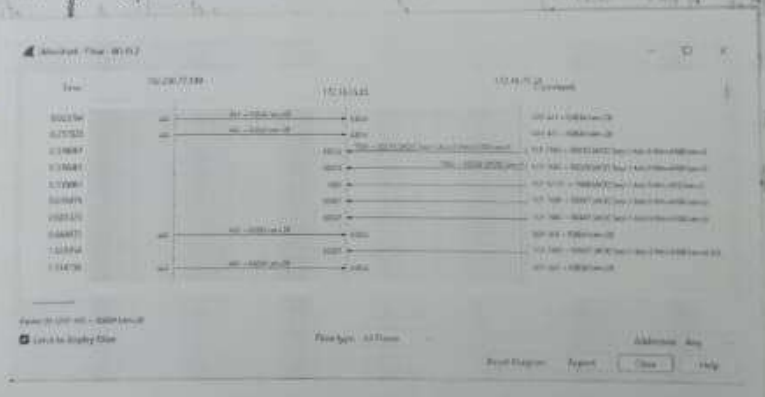
You can also click Analyze > Display Filters to choose a filter from among the default filters included in wireshark. Close the window and you'll find a filter has been applied automatically. Wireshark is showing you the packet that make up the conversation.



Inspecting Packets -
Click a packet to select it and you can dig down to view its details.



You can also create filters from here - just right-click one of the details and use the Apply as filters submenus to create a filter based on it.
Flow Graph: Gives a better understanding of what we



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.

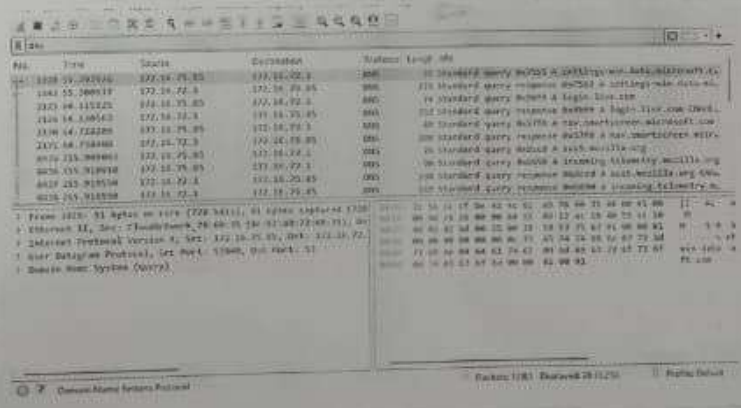
Procedure :-
- Select local area connection in Wireshark.
- Go to capture → option.
- Select stop capture automatically after 100 packets
- Then click start capture & save the packets.

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 packet & provide the flow graph:

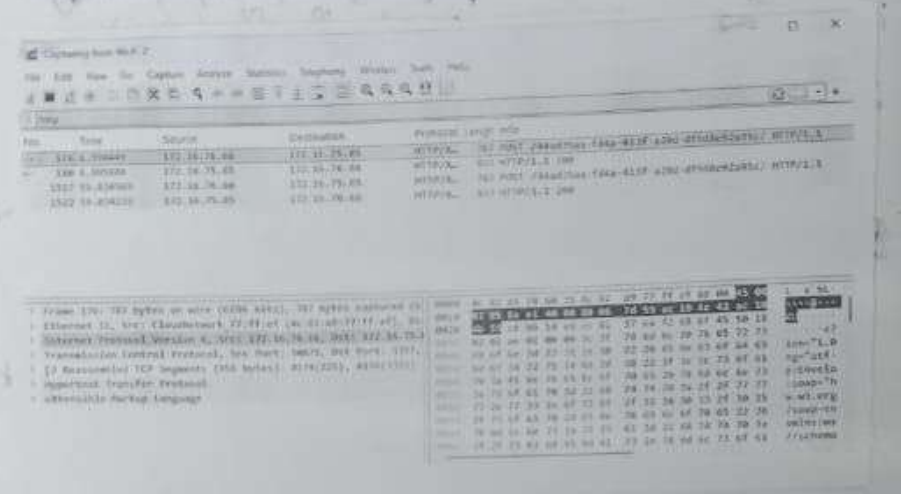
- Go to capture → option
- Select Stop capture automatically after 100 packet
- Then click Start capture.
- Search DNS packets in search bar.
- To see flow graph click Statistics → Flow Graph.
- Save the packets.



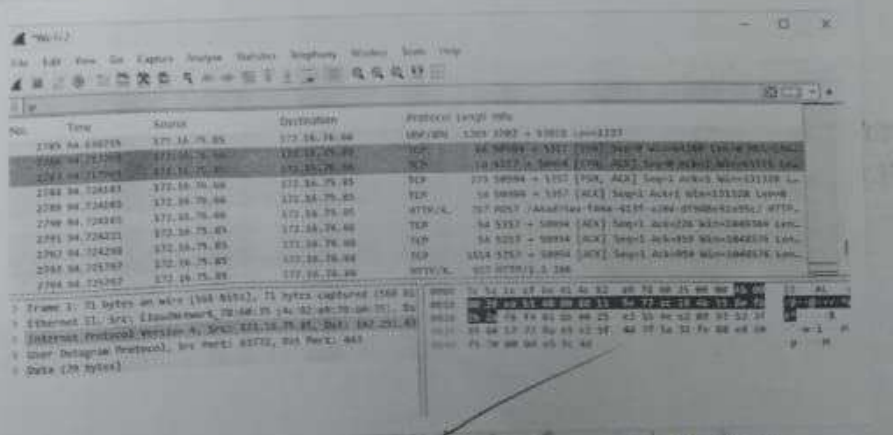
4. Create a filter to display only HTTP packets and inspect the packets.

Procedure:

* Select Local area connection in wireshark
* Go to Capture → option
* Select Stop capture automatically after 100 packet
* Then click Start capture
* Search HTTP packets and save packets.



5. Create a Filter to display only IP/ICMP packets & inspect the packets :-
   - Select local area connection in wireshark.
   - Go to Capture → option.
   - Select stop capture automatically after 100 packet.
   - Then click Start capture.
   - Search ICMP/IP packets in Search bar.
   - 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 setting for a network interface card (NIC) where it captures all network packet that pass through it, not just the ones addressed to it. It is used in packet sniffing 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 Data link layer to map an IP address to a MAC address.

(3) Which Transport layer protocol is used by DNS?

DNS can use : UDP on port 53 for most queries (faster). 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 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 subnet.

Eg: For network 192.168.1.0/24, the broadcast address is 192.168.1.255.

Result :-

Experiments on packet capture tool, wireshark was successfully studied.

14/8/25