06/08/24

PRACTICAL - 5

EXPERIMENT ON PACKET CAPTURE TOOL: WIRESHARK.

Packet Snipper.

→ Sniffs messages being sent/received from/by your computer.

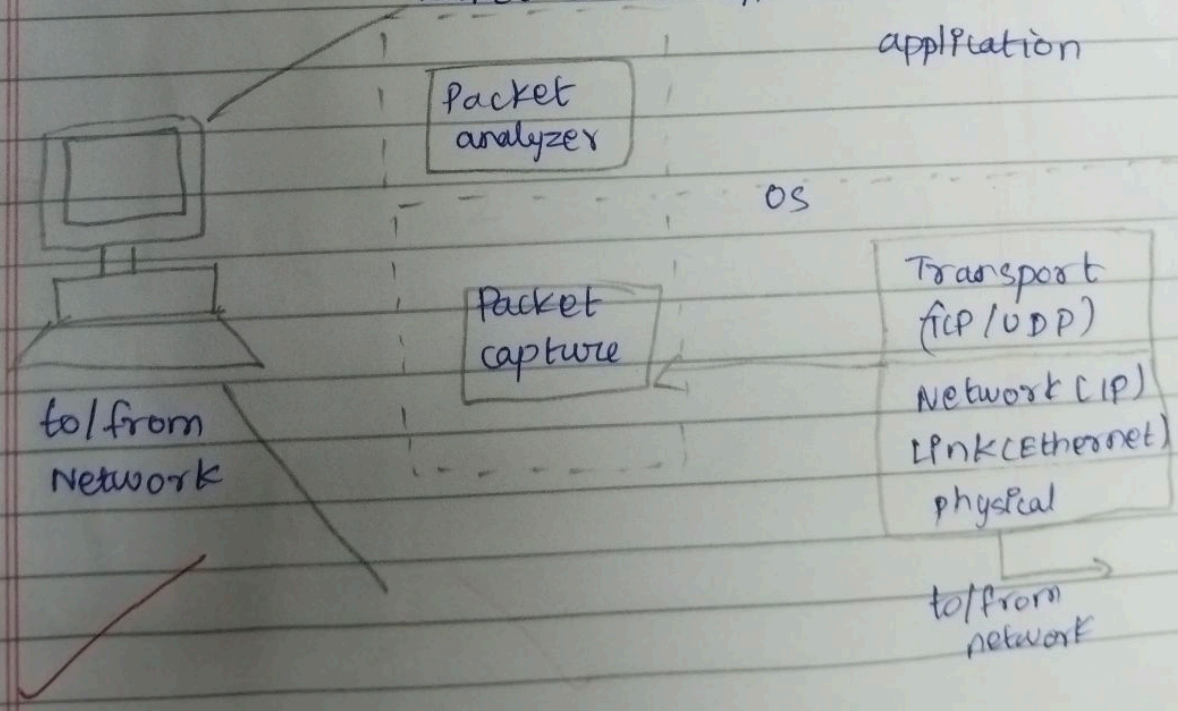
→ Store and display the contents of the various protocol fields in the messages

→ Passive program

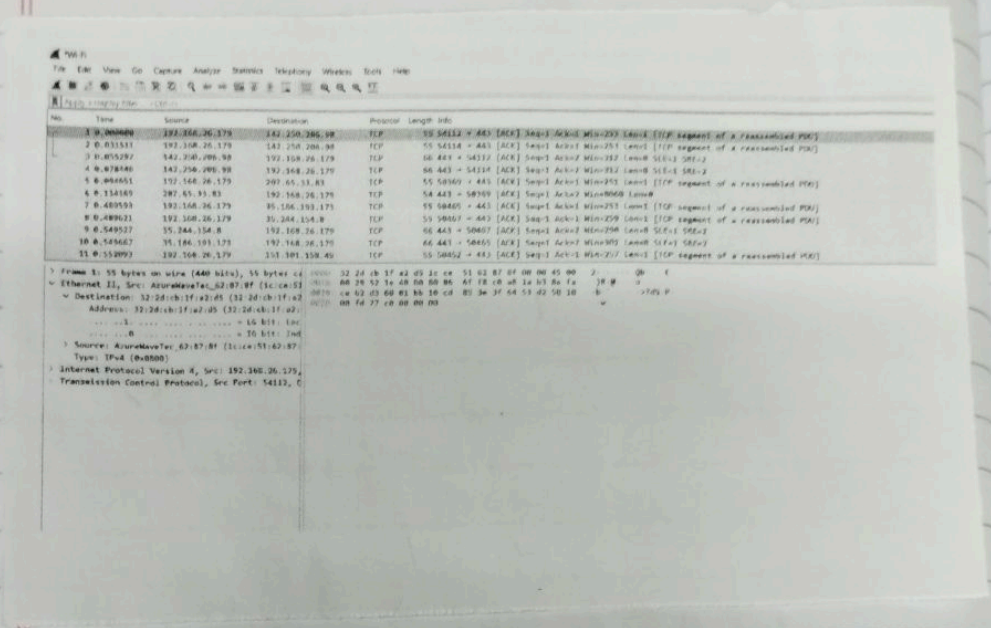
- Never sends packets itself
- no packets addressed to it
- receives a copy of all packets (sent/received)

Packet sniffer structure Diagnostic Tools.

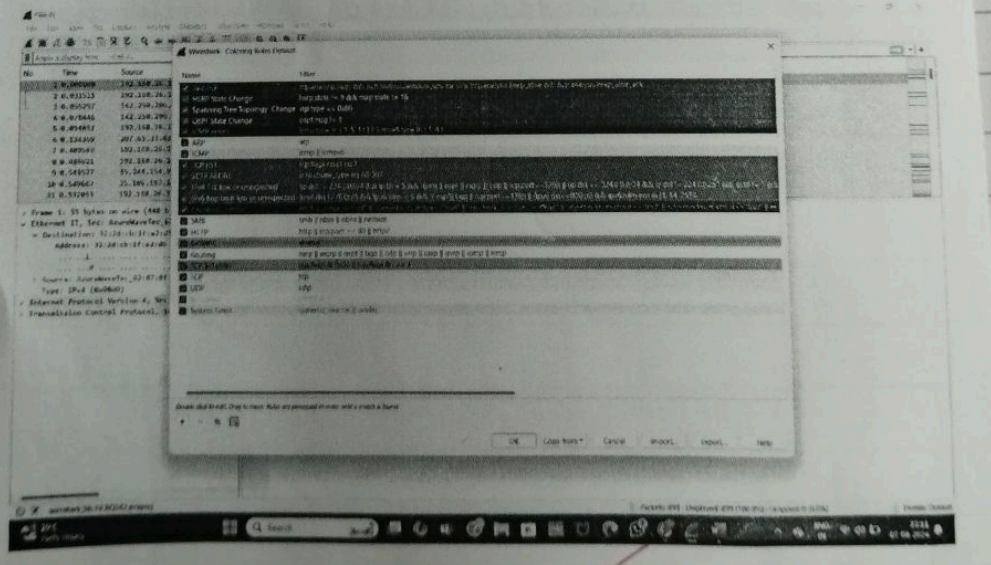
- Tepdump
  - Eg. tedpump -enx host 10.129.41.2-w. exe3.out.
- Wireshark
  - wireshark -r exe3.out.



capturing packets :

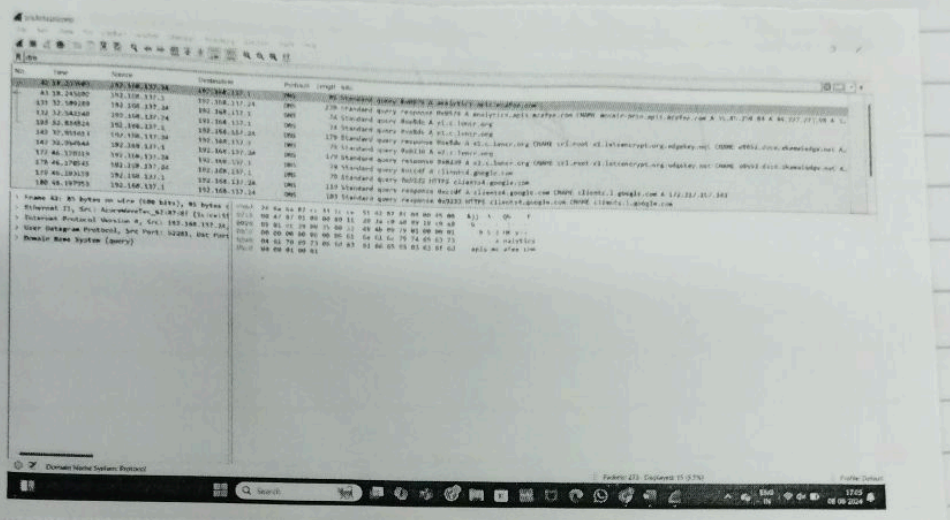


color coding :

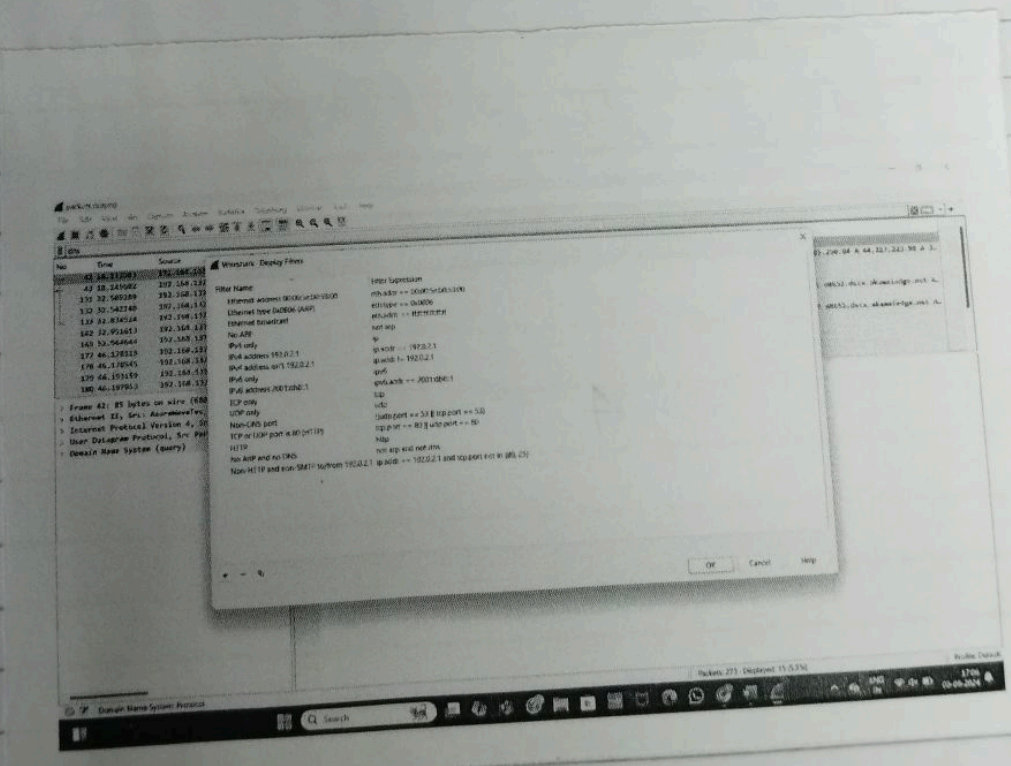


Filtering packets:

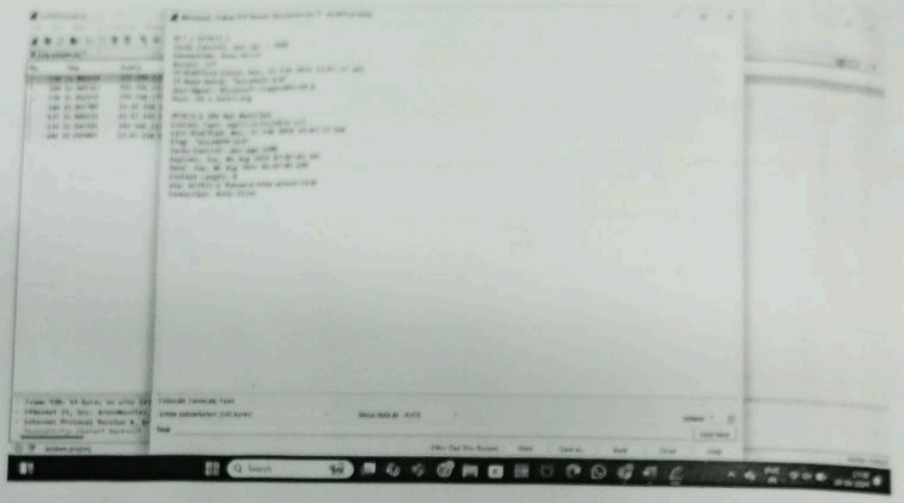
way1 - apply filter by typing it into the filterbox at the top of the window.



way2 - click analyze > Display filters we can custom filters and access them.



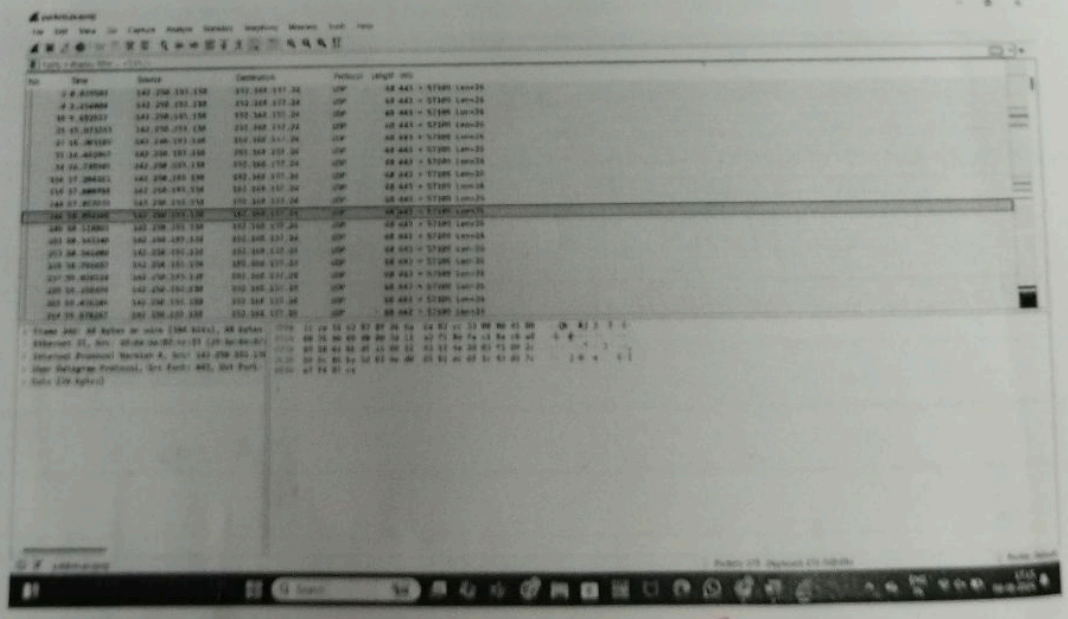
way 3- Right click at packet and select follow > TCP stream.



we can see at the back that filter box as know changed to tcp.stream eq 4.

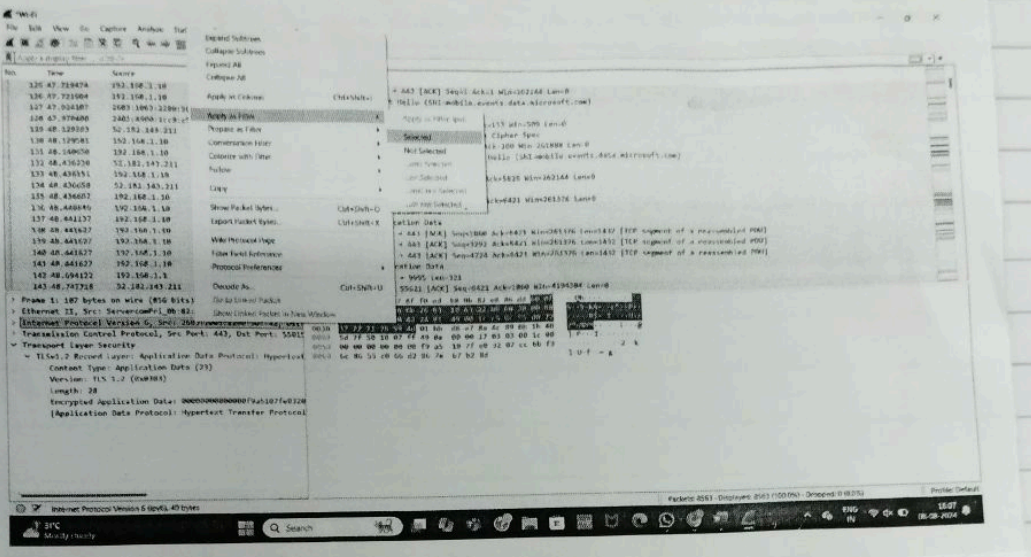
Inspecting packets:

click a packet and the packet is inspected on packet details & packet bytes.

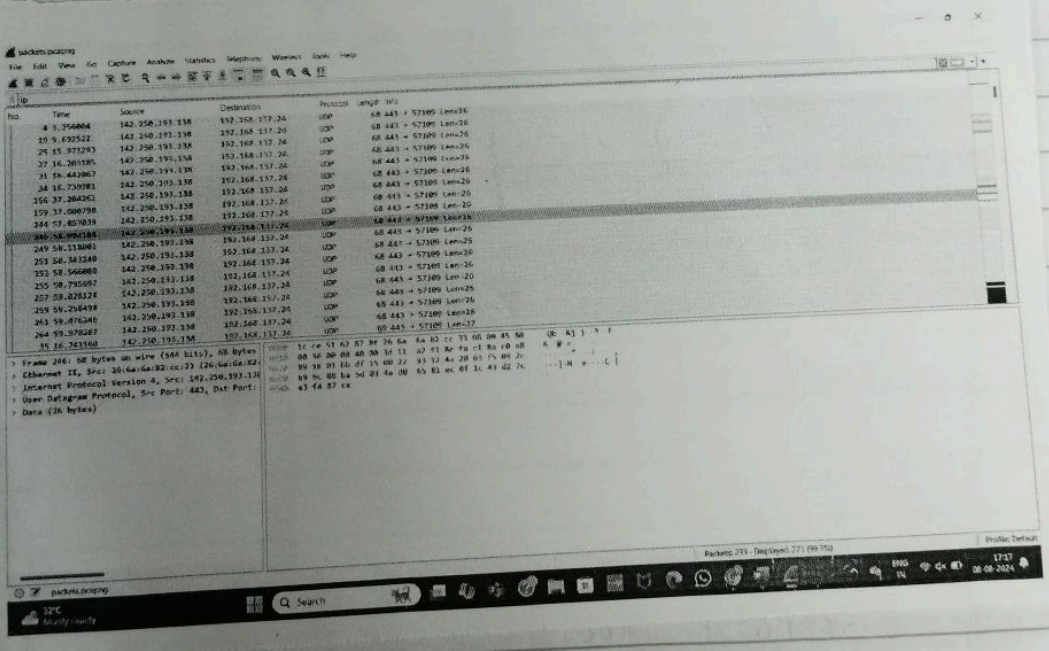


we can also select filters through packet details

right click → apply as filter → selected.

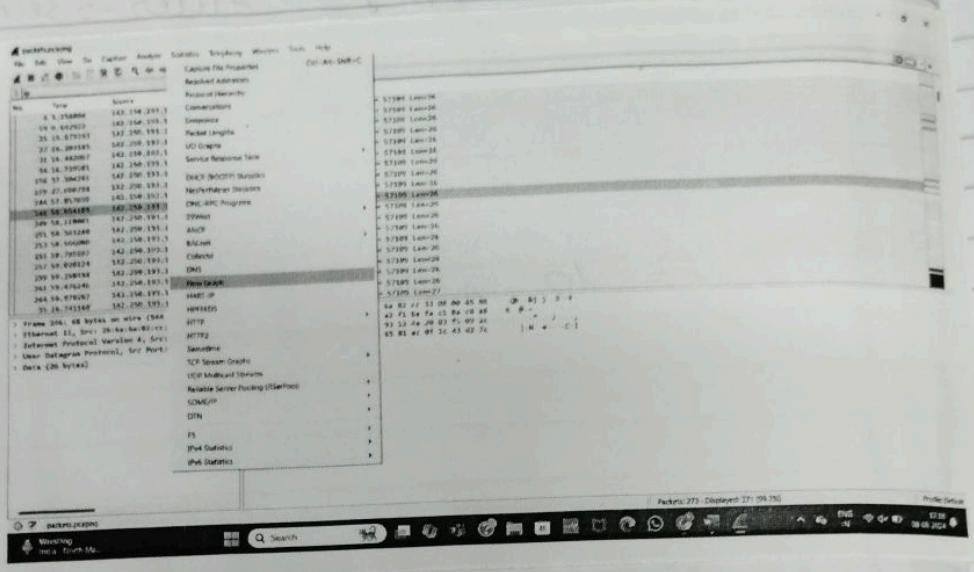


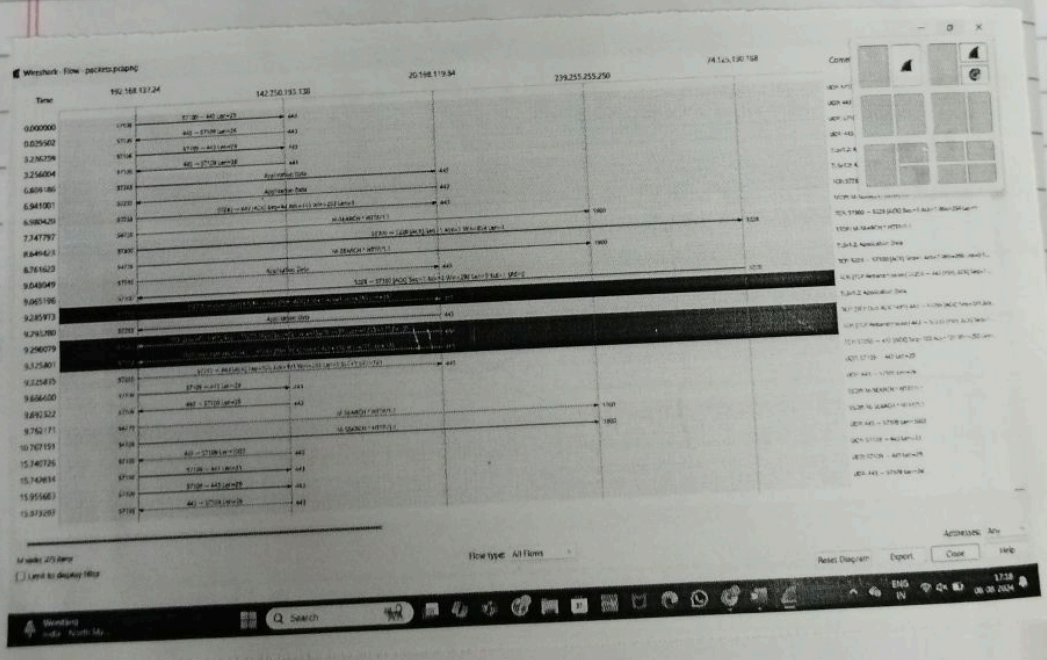
filter applied : ip.



Flow Graph:

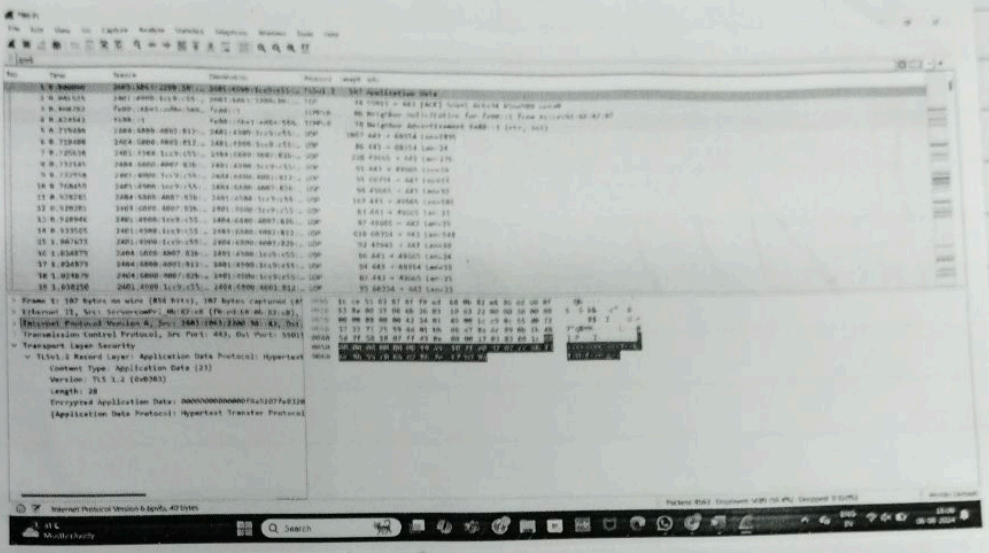
Statistics → Flow Graph.





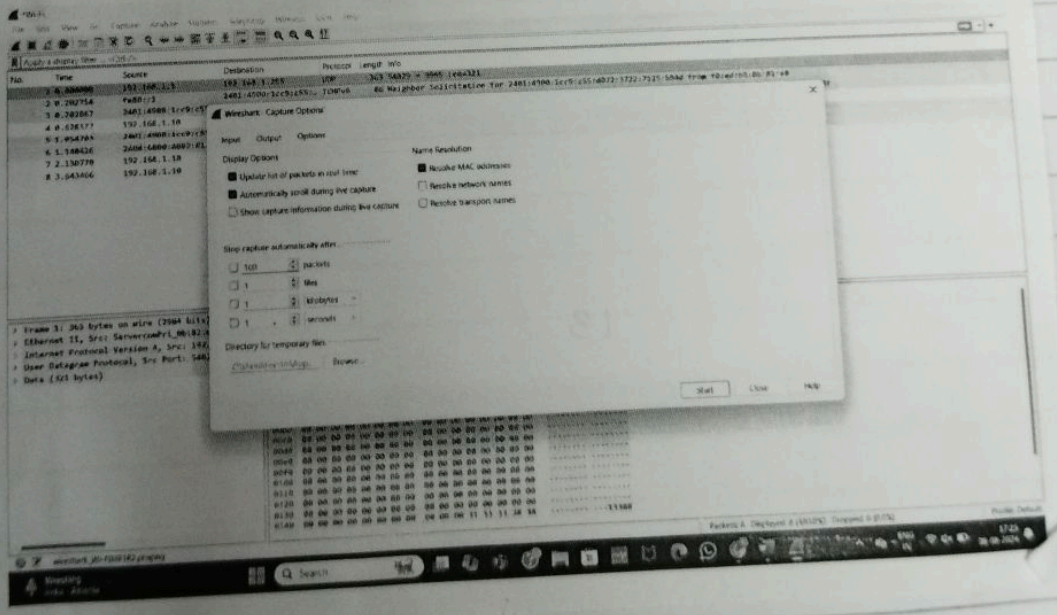
Capturing & analysing packets using wireshark tool:

Go to capture, click start capture.

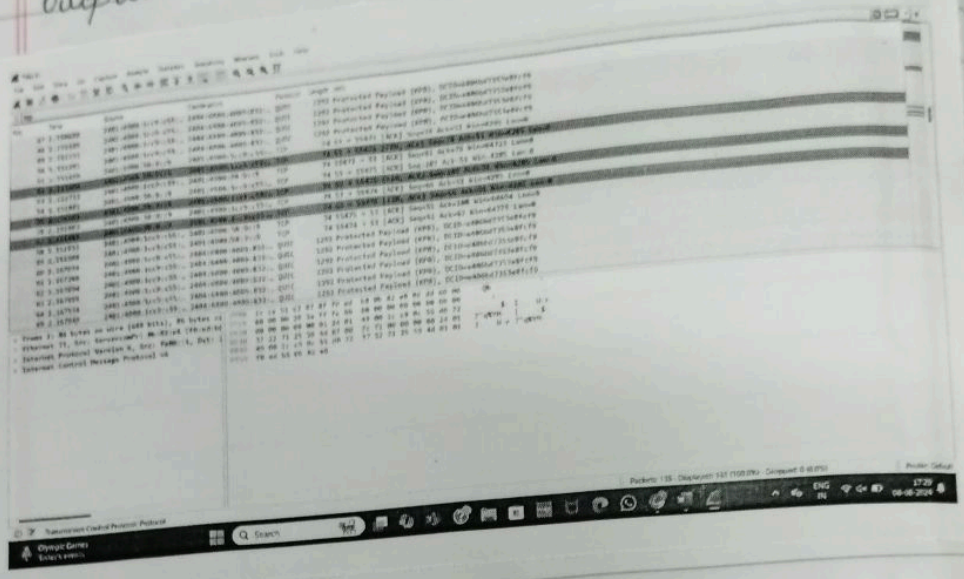


i) Create a filter to display only TCP / UDP packets, inspect the packets.

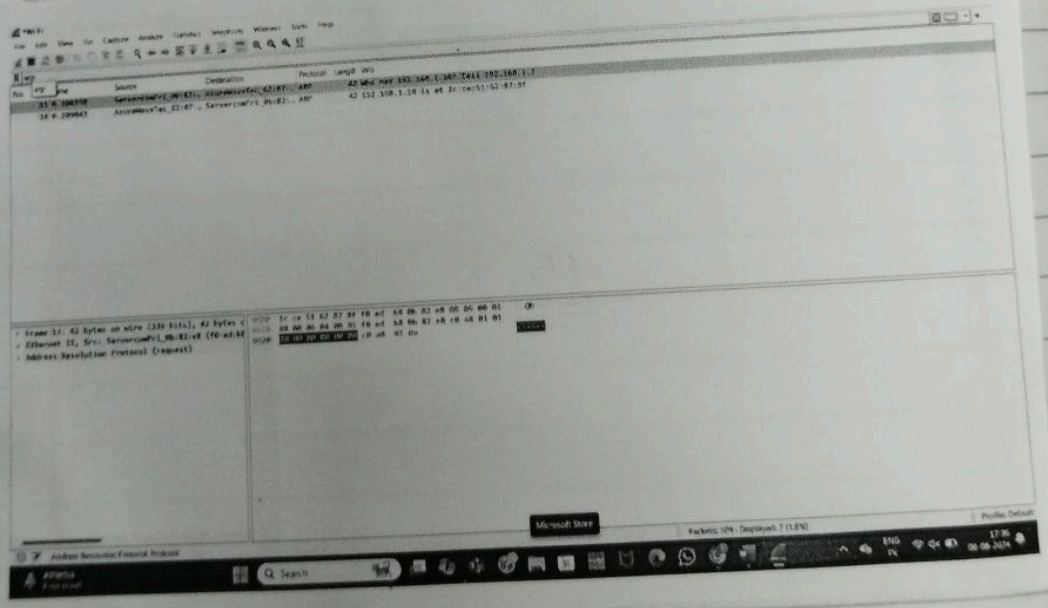
Go to capture → option → stop capture automatically after 100 packets.



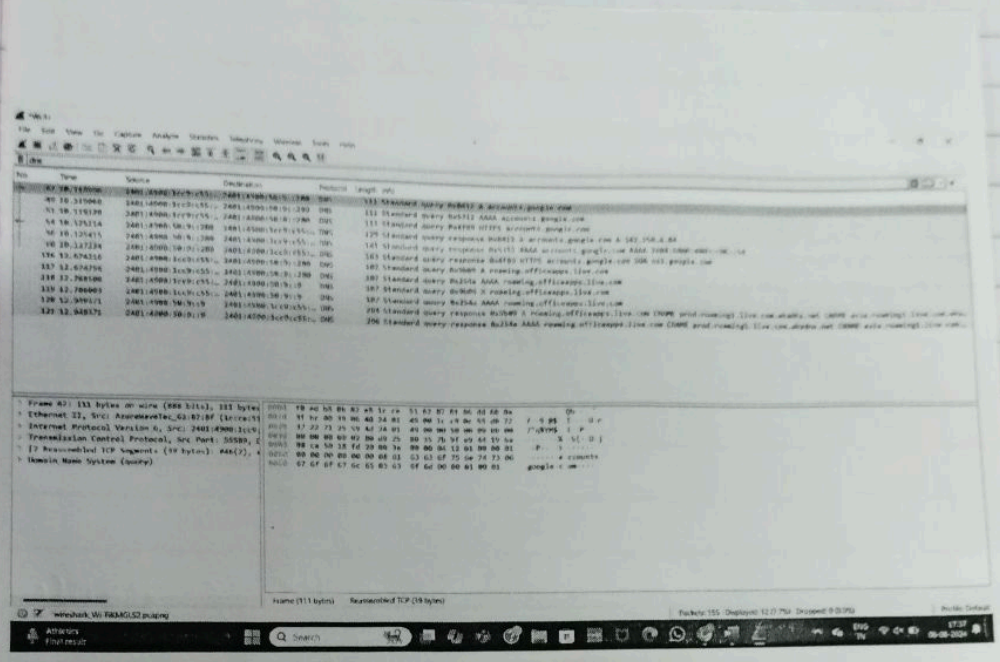
Output -

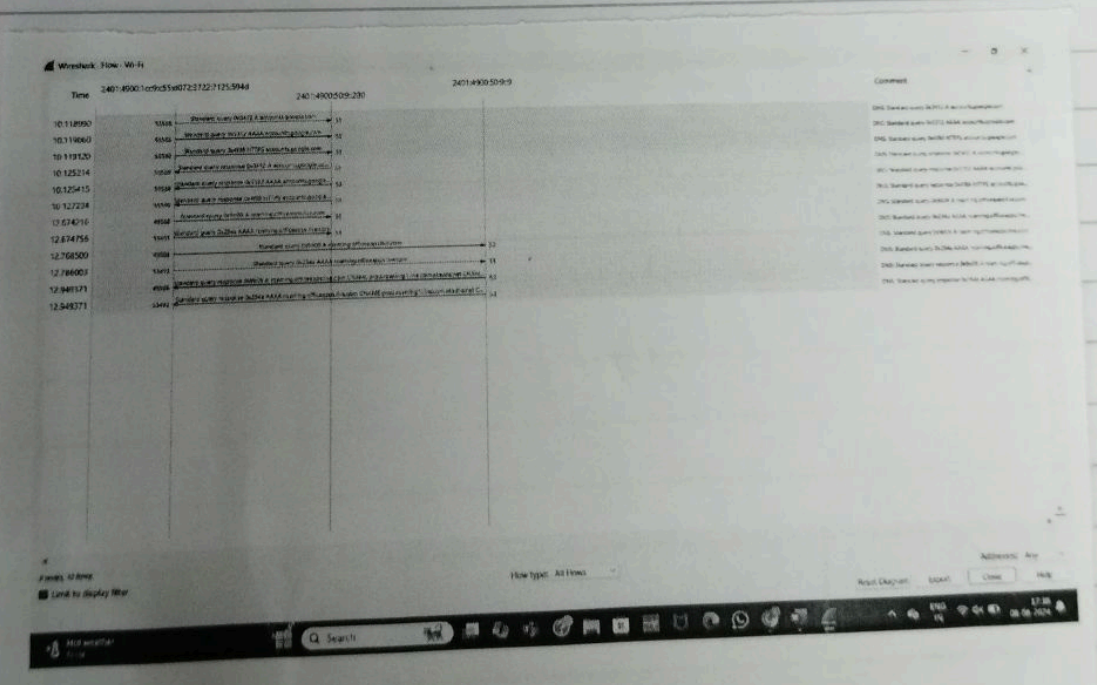


2. Create a filter to display only ARP packets and inspects the packets

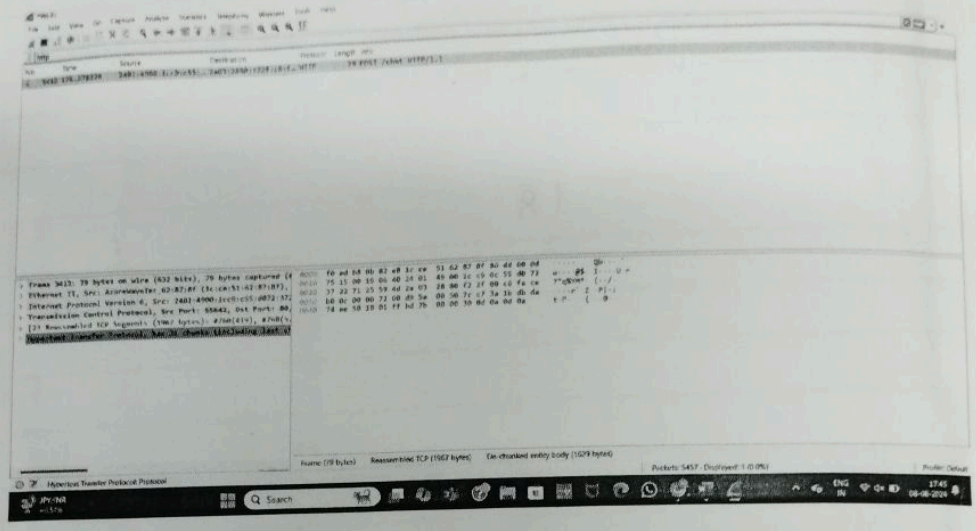


3 Create a filter to display only DNS packets and provide the flow chart.

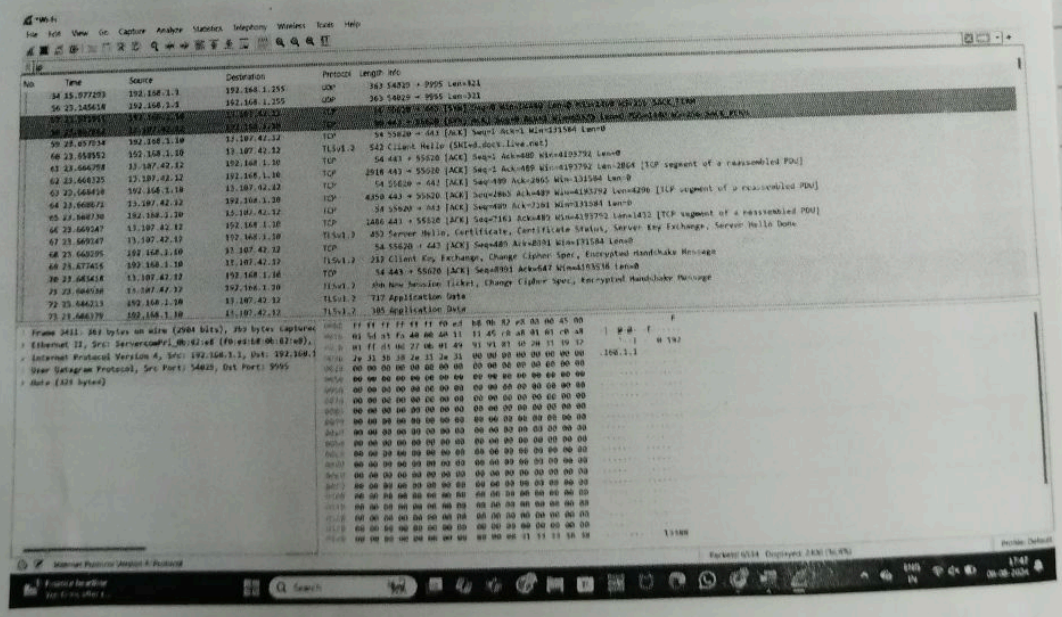


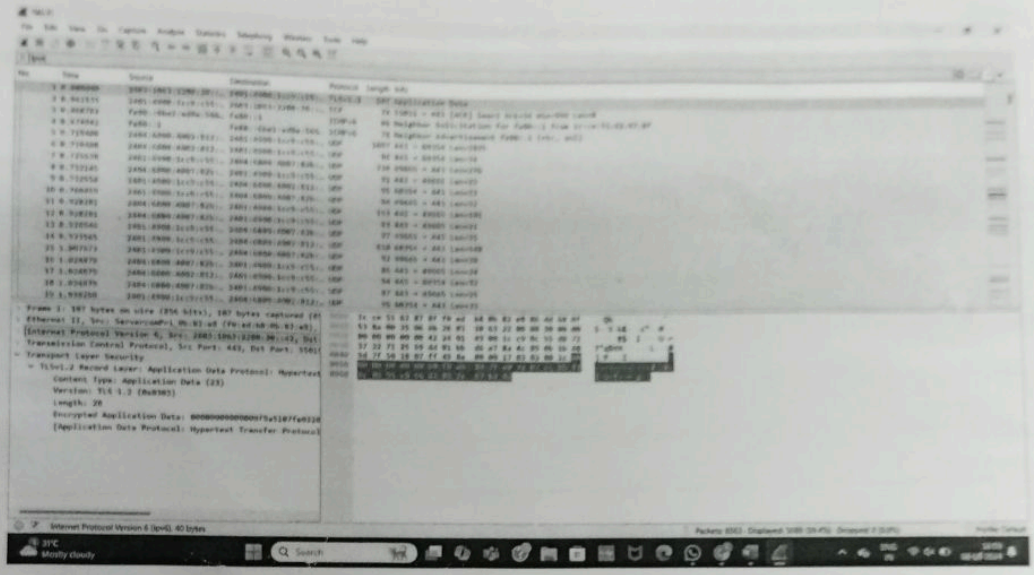


4) Create a filter to display only HTTP packets and inspect the packet.



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





Result:

The experiment on packet capture tool: wireshark is observed and studied.

9/8/24.