NEW MAHADEV GOLD
Page
Date

EX : 5 PACKET CAPTURE TOOL :
DATE : 08-08-24 WIRESHARK

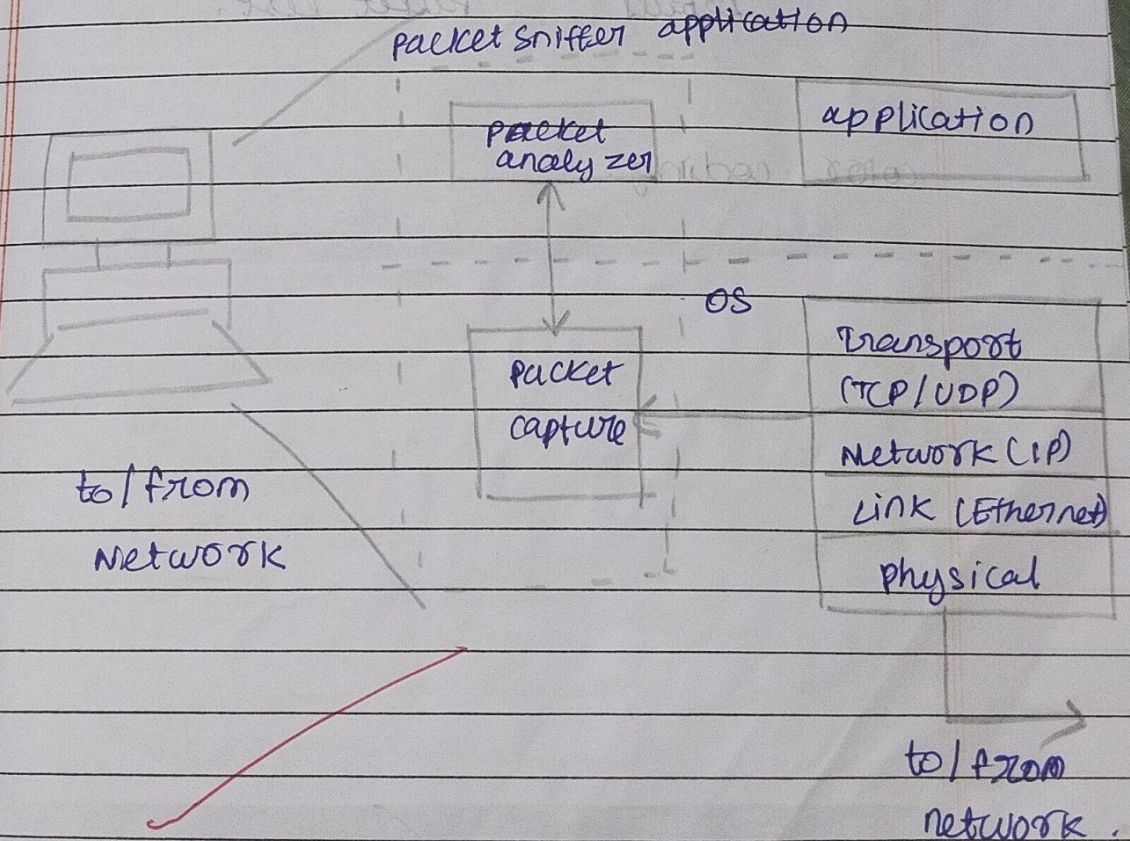
~~Packet sniffer~~:

Aim:

To Experiment on Packet capture tool: Wireshark.

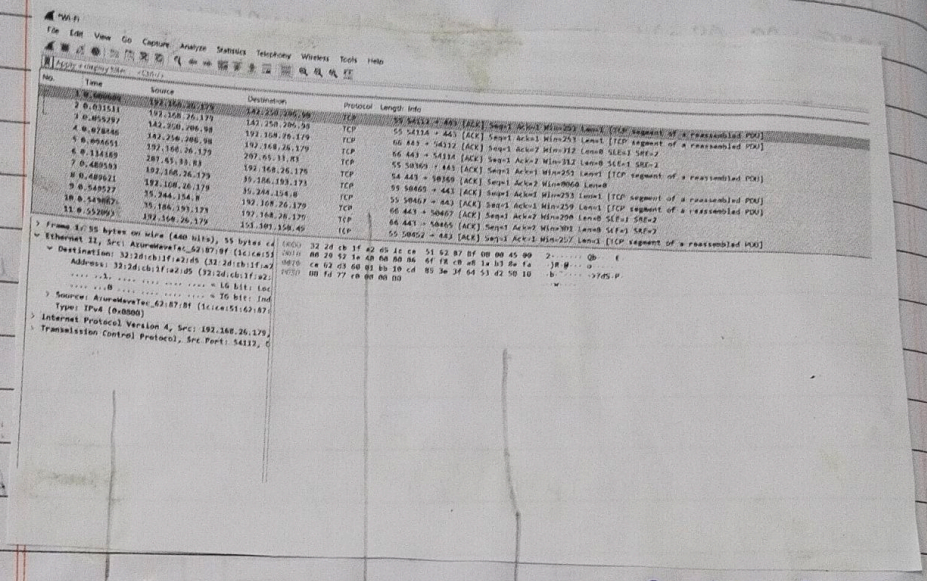
Packet sniffer structure Diagnostic Tools:

- TCPDump - Eg: tcpdump -enx host 10.129.41.2 -w exe3.out.
- wireshark - wireshark -r exe3.out.



NEW MAHADEV GOLD
Page
Date

capturing packets:

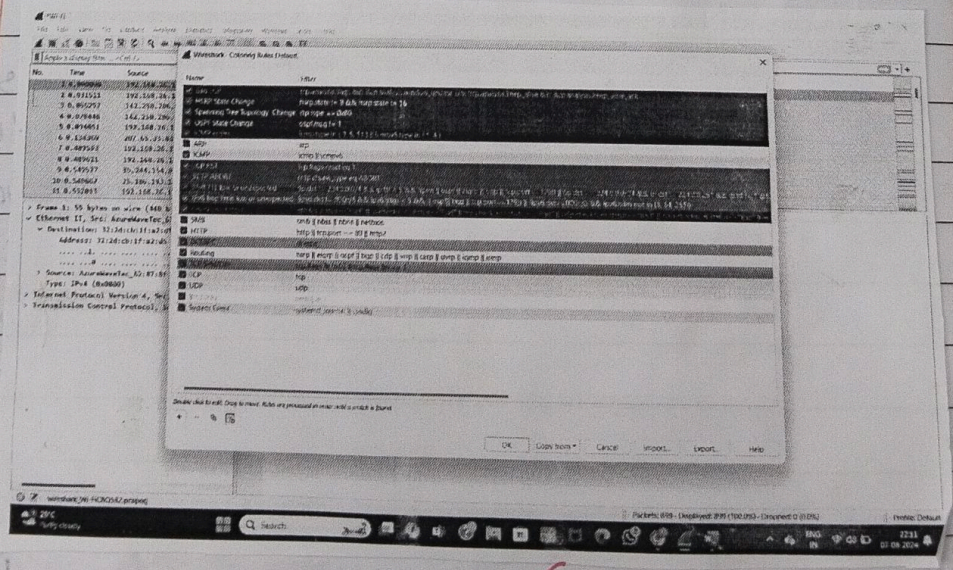


Packet Bytes

Packet Details

Packet list.

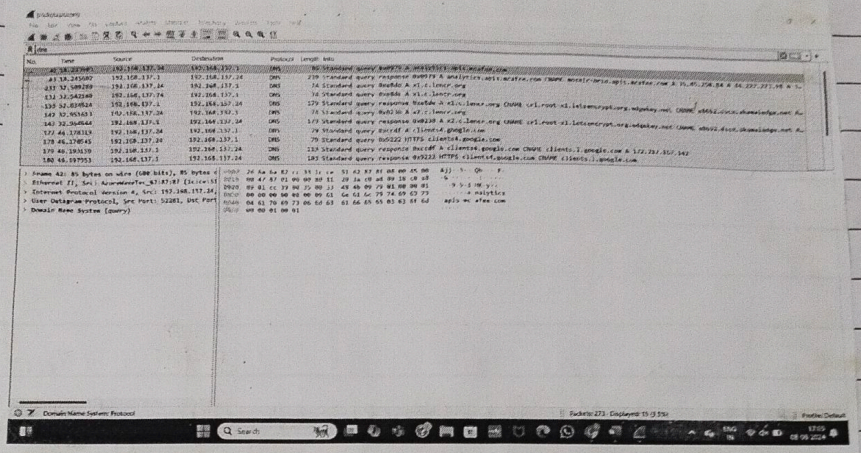
color coding:



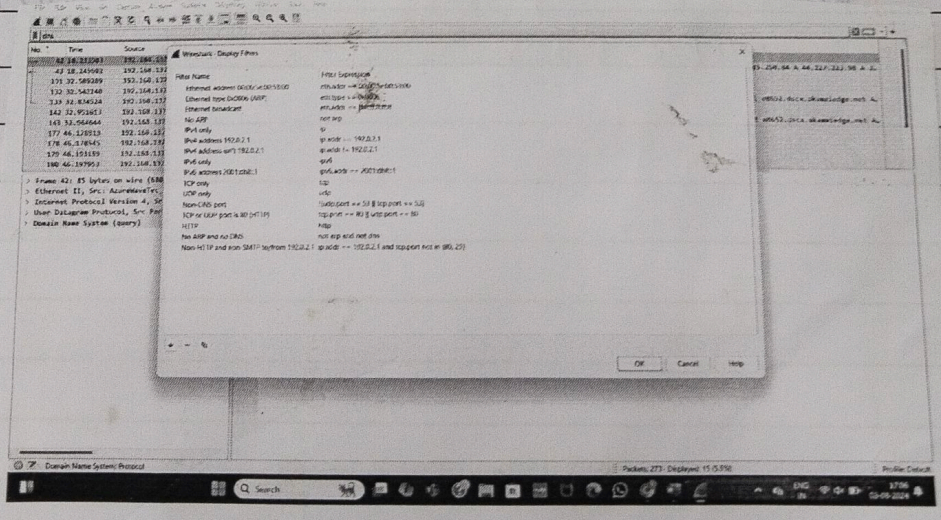
NEW MAHADEV GOLD
Page
Date

Filtering packets:

way-1: apply filters by typing it into the filterbox at the top of the window.

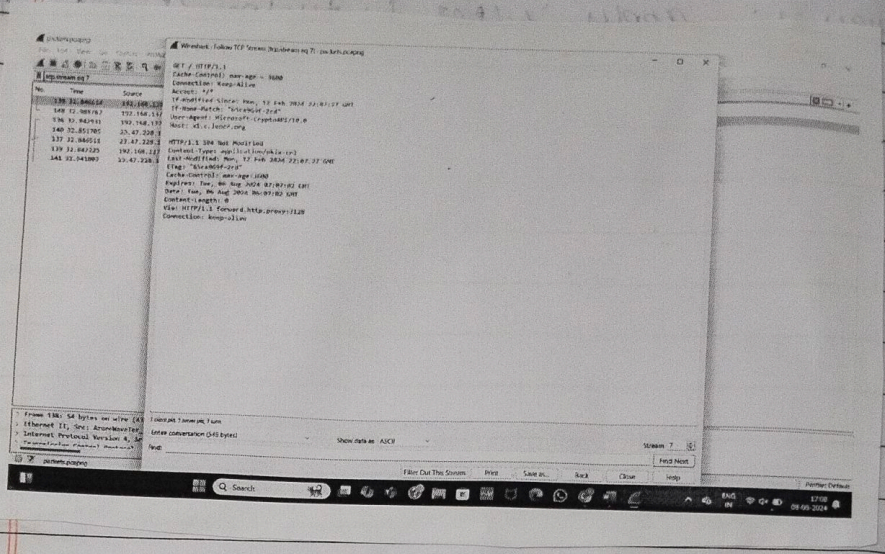


way-2: Click analyze > Display filters we can custom filteres and access them



NEW MAHADEV GOLD
Page
Date

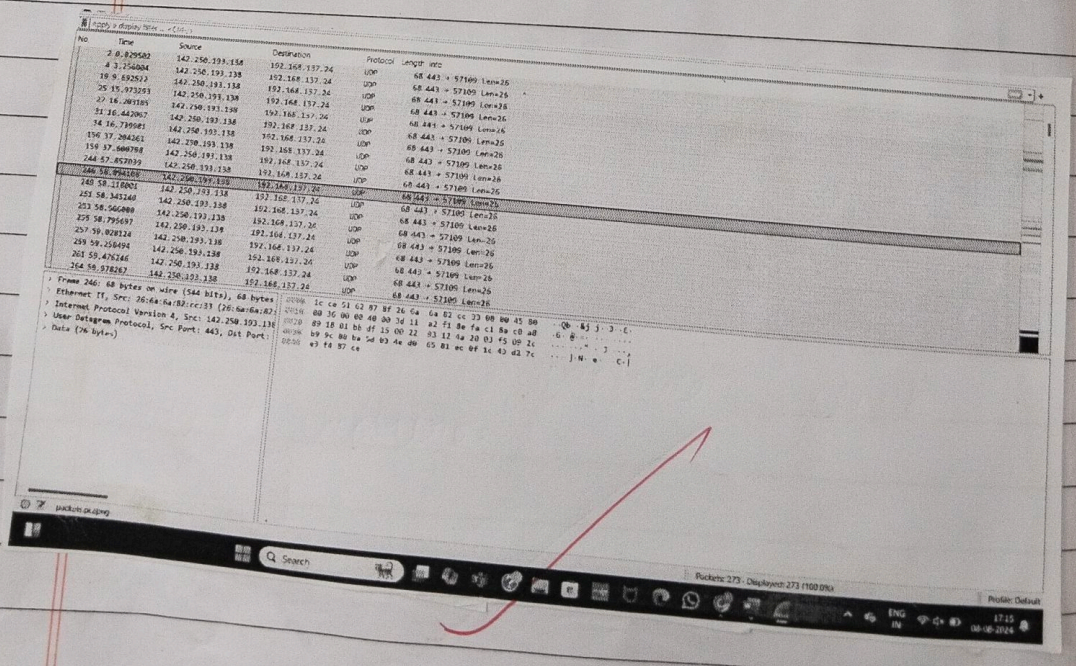
way-3: Right click on packet and select Follow > TCP stream.



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

Inspecting packets:

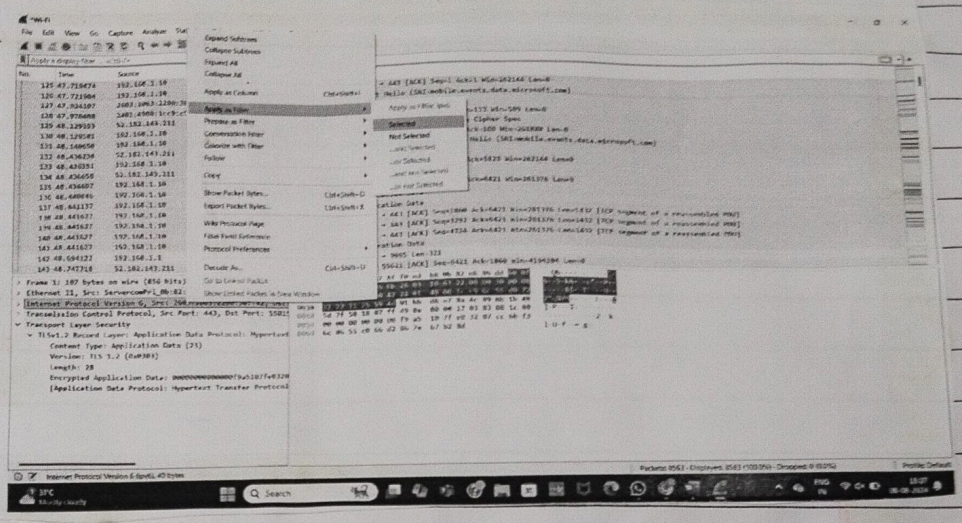
click a packet and the packet is inspected on packet details & packet bytes.



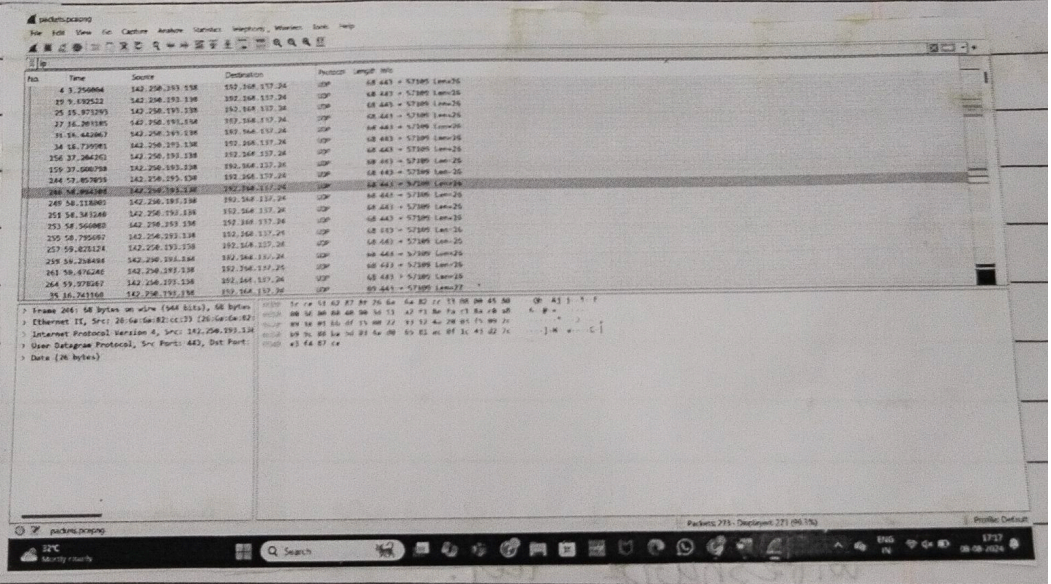
NEW MAHADEV GOLD
Page
Date

We can also select filters through packet details

right click ⇒ apply as filter → selected.

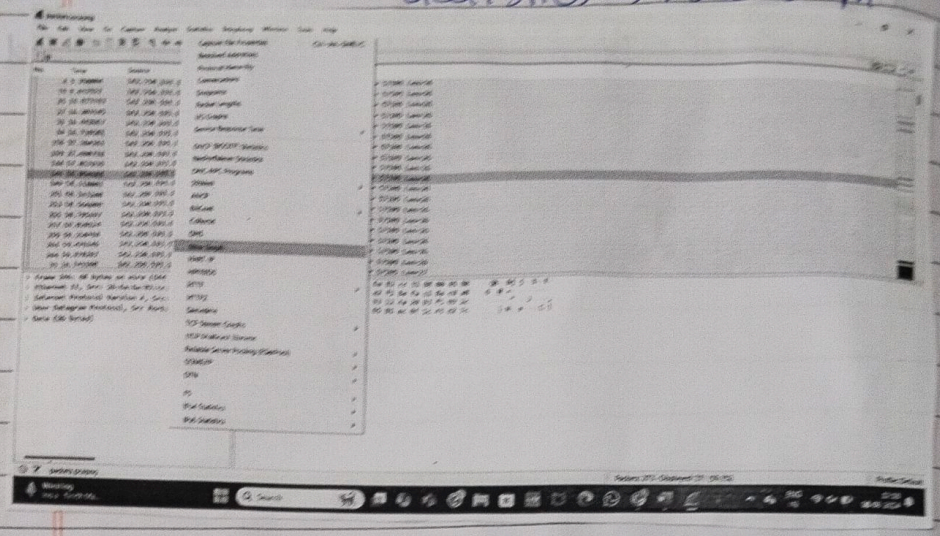


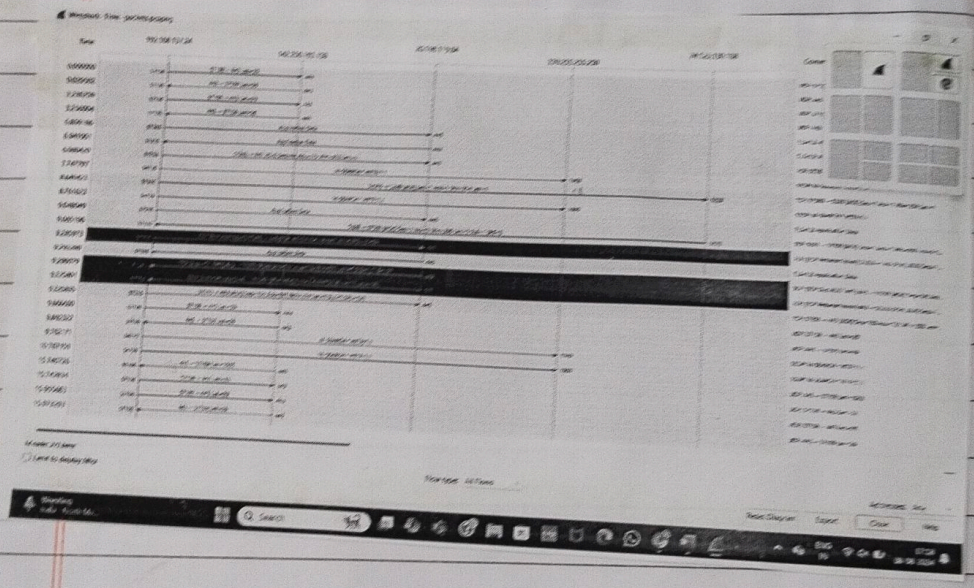
filter applied : ip.



Flow Graph:

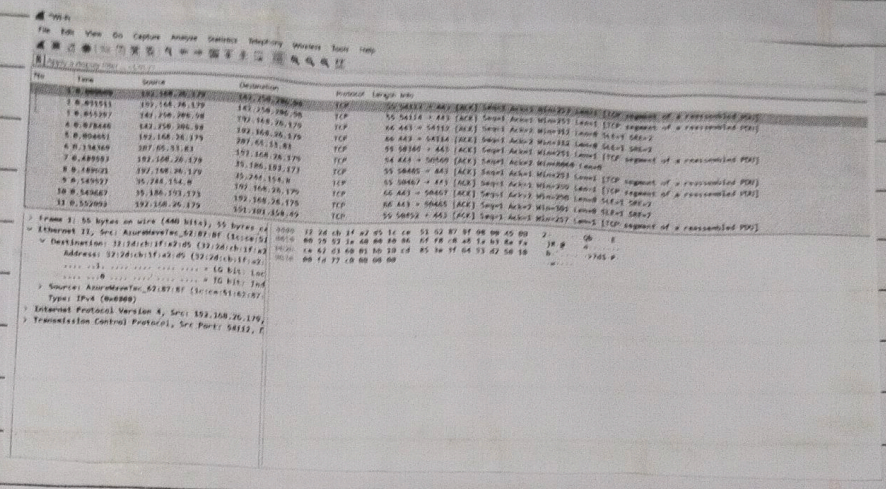
Statistics → Flow Graph





capturing & analysing packets using wireshark tool:

Go to capture, click start capture.



1. Create a bilties to display only TCP/UDP packets, inspect the packets

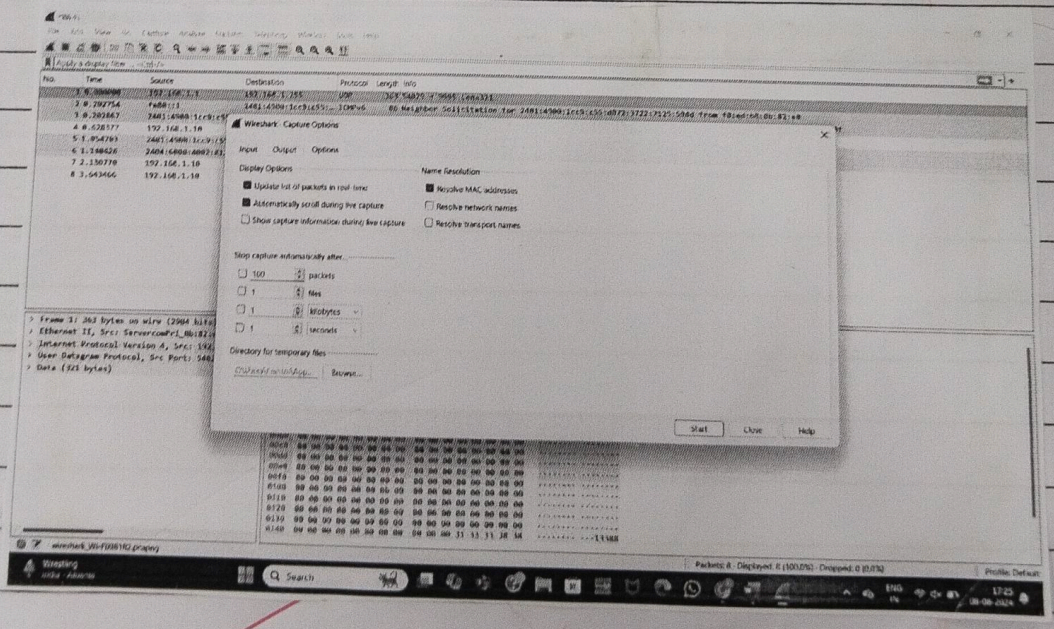
Go to capture

↓

option

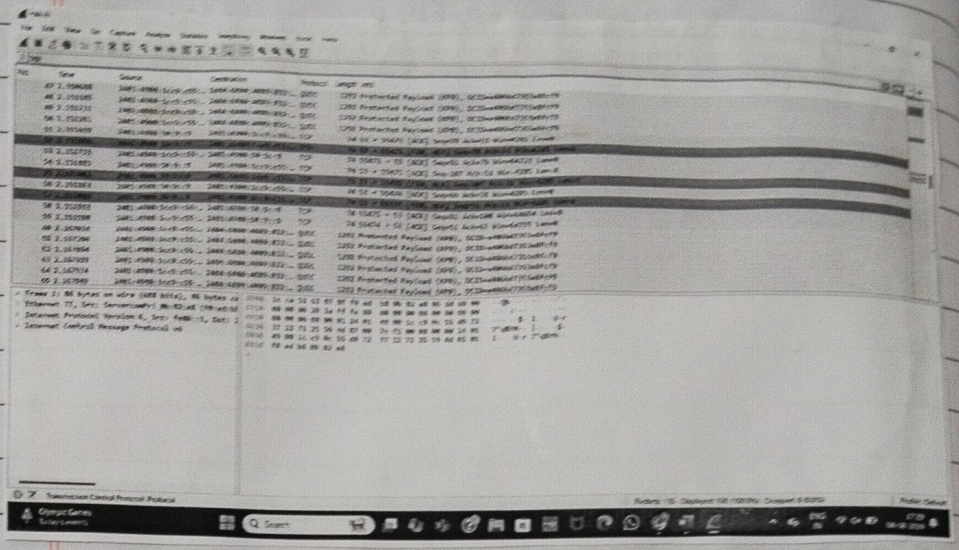
↓

Stop capture automatically after 100 packets

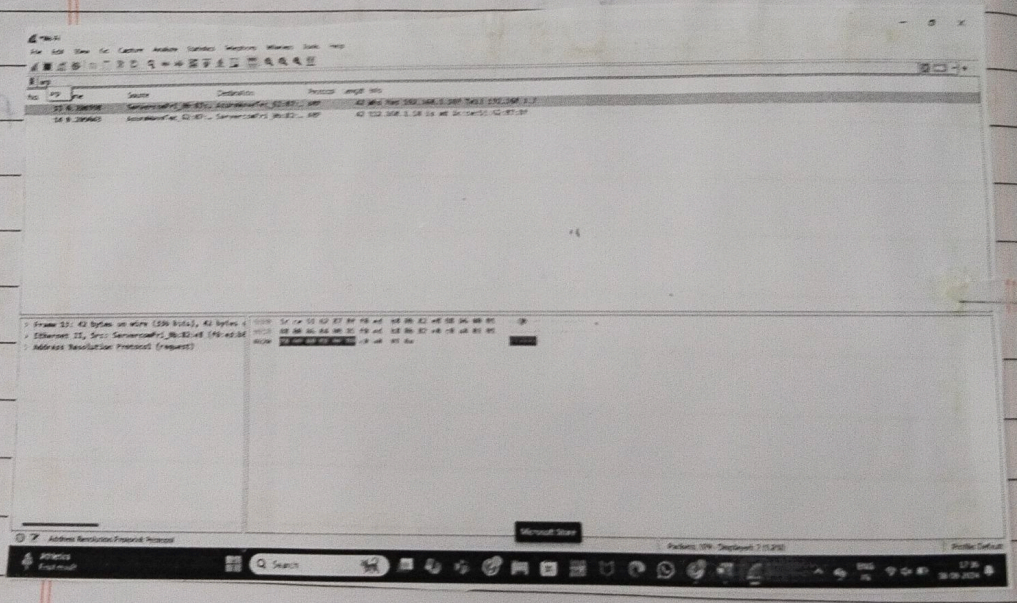


NEW MAHADEV GOLD
Page
Date

Output:

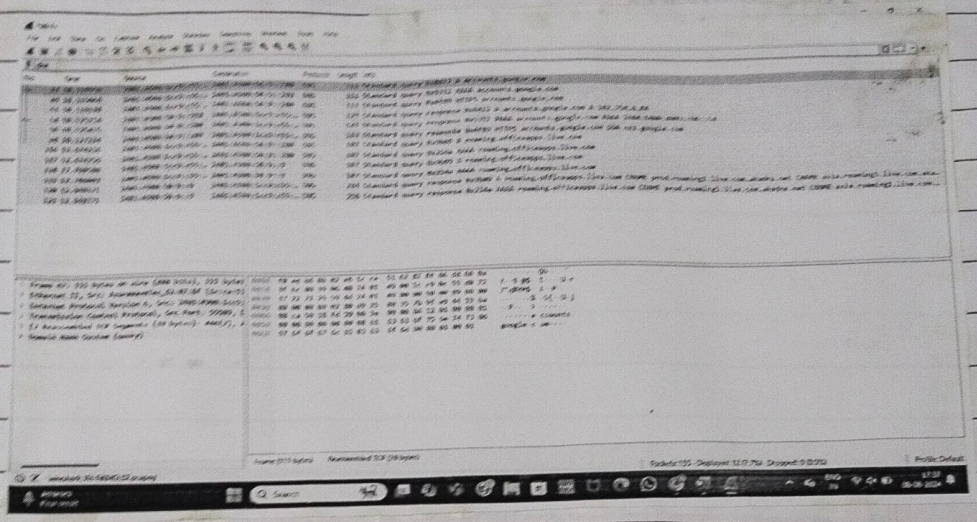


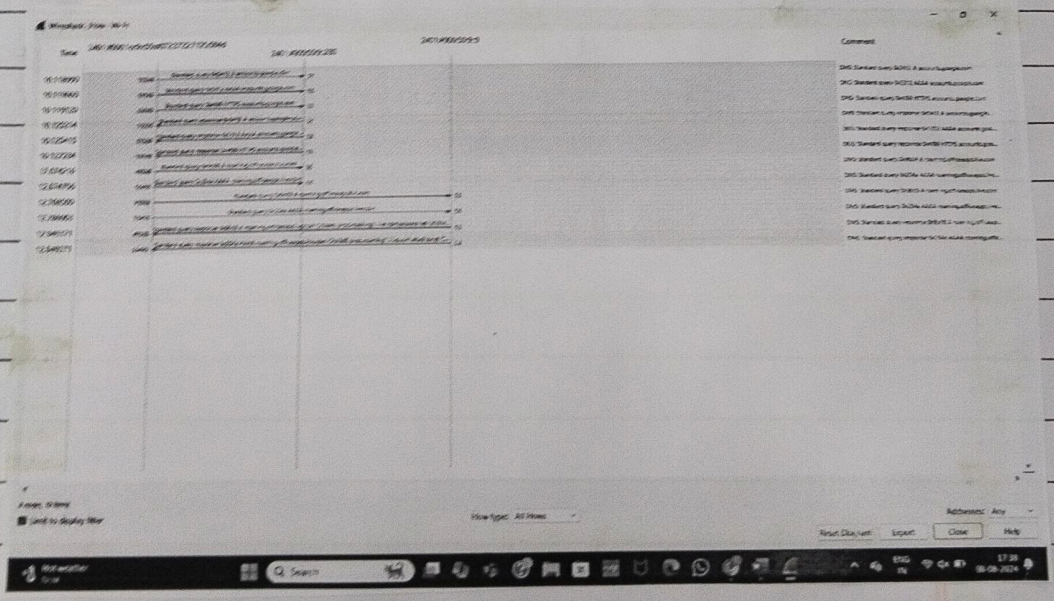
2. Create a Filter to display only ARP packets and inspects the packets.

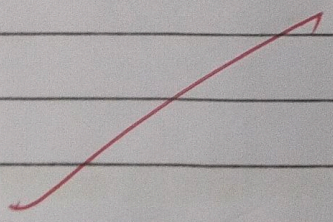


NEW MAHADEV GOLD
Page
Date

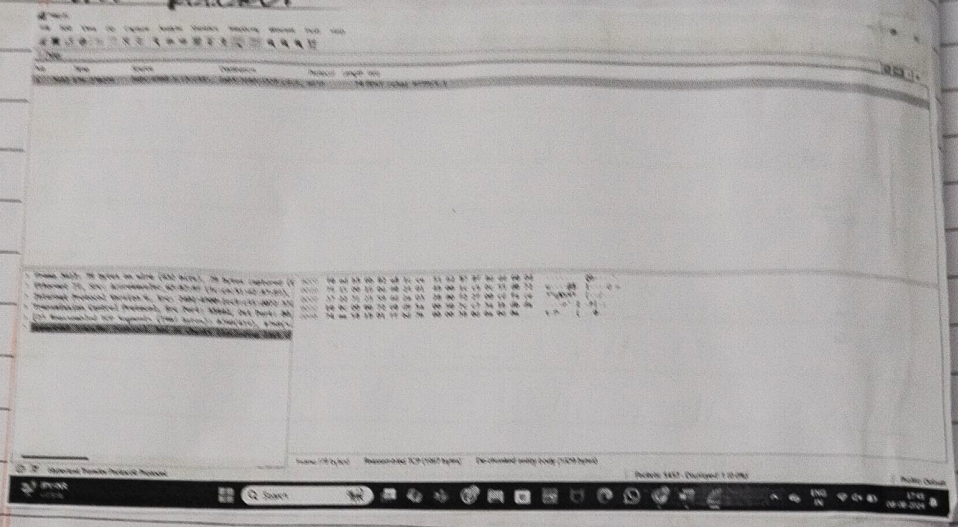
3. Create a Filter to display only DNS packet and provide the flow chart.



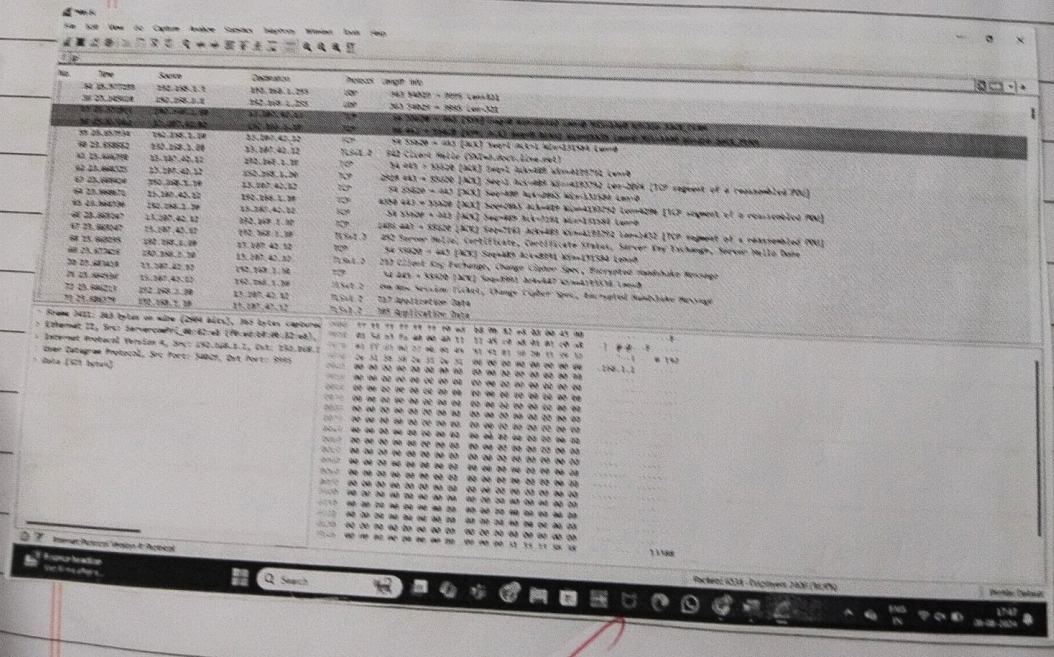


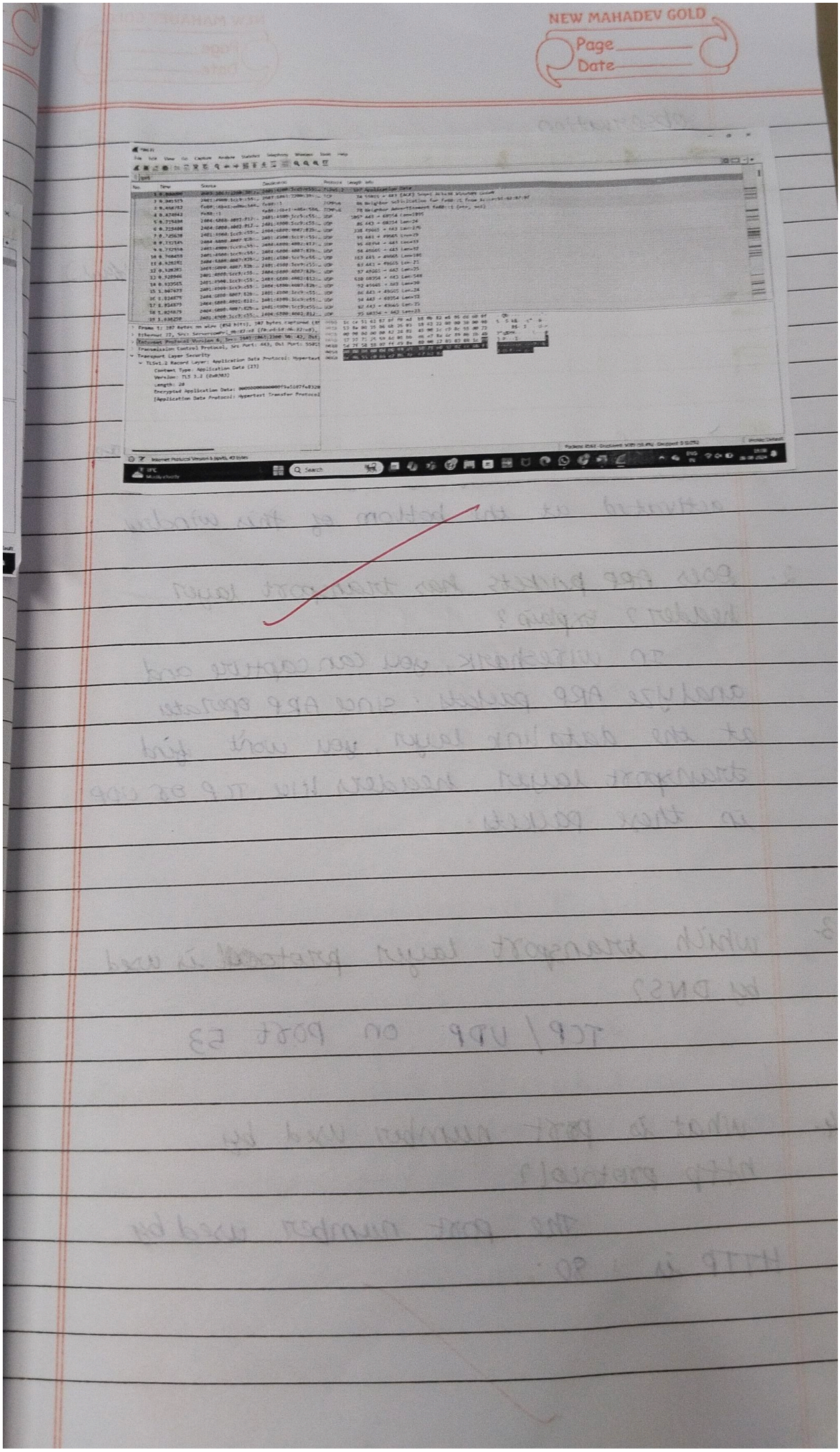


4. Create a filter to display only HTTP packets and inspect the packet.



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





NEW MAHADEV GOLD
Page
Date

Observation

1. what is promiscous mode?

It is network sniffing Tool. If you have promiscous mode enabled (default) you will also see all the other packets on the Network instead of only packets addressed to your network adapter adapter to check if it is enabled, click capture > option and verify the "Enable promiscous Mode on all interfaces" checkbox is activated at the bottom of this window.

2. Does ARP packets has transport layer header? Explain?

In wireshark, you can capture and analyze ARP packets. since ARP operates at the data link layer, you won't find transport layer headers like TCP or UDP in these packets.

3. which transport layer protocol is used by DNS?

TCP / UDP on port 53

4. what is port number used by http protocol?

The port number used by HTTP is 80.

NEW MAHADEV GOLD
Page
Date

5. What is broad cast ip address?

wireshark can capture broadcast traffic, including packets sent to the broadcast IP address. This allows you to see message intended for all devices on the network.

Result:

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

9/8/24