6/8/24 Exercise: 5

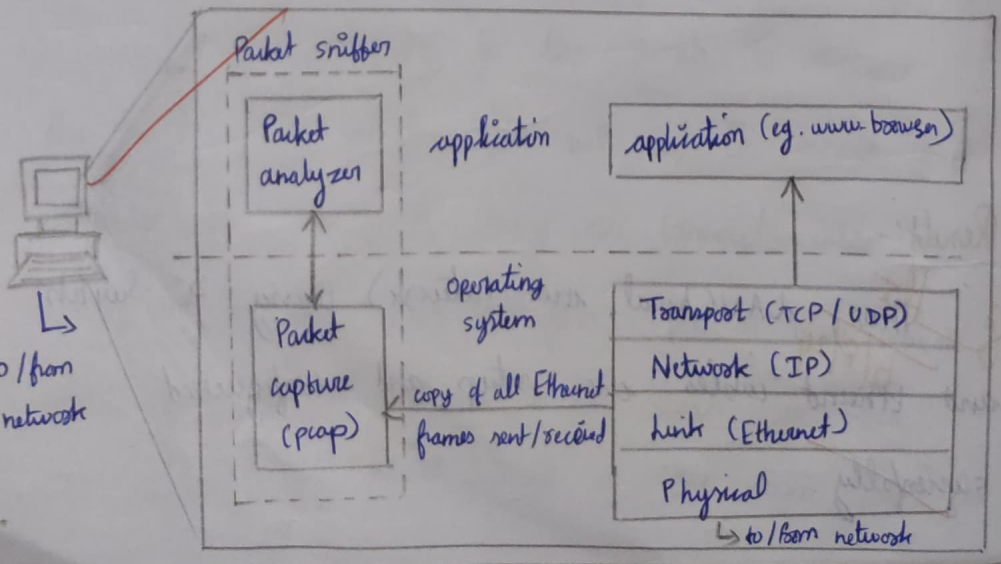
Aim:- Experiments on Packet capture tool: Wireshark.

Packet Sniffer:-

* 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.

Packet Sniffer Structure Diagnostic Tools:-

* Tcpdump
  - Eg: tcpdump -enx host 10.129.41.2 -w exe3.out
* Wireshark
  - wireshark -r exe3.out



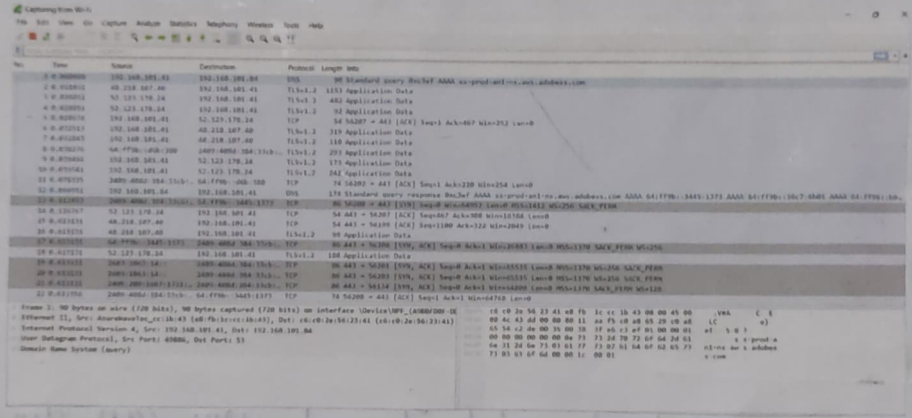
Capturing network traffic :-

After downloding and installing Wireshark, lanch it and double-click the name of a network inferace to capture.

Procedure :-

1) Select local Area Connection in Wireshark
2) Go to capture → option
3) Select stop capture automatically after 100 packets
4) Save the packets.

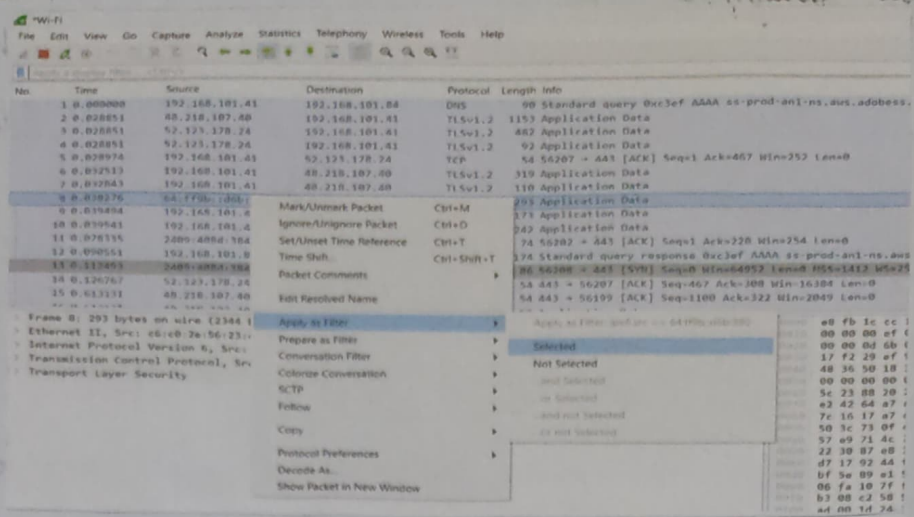
Output :-

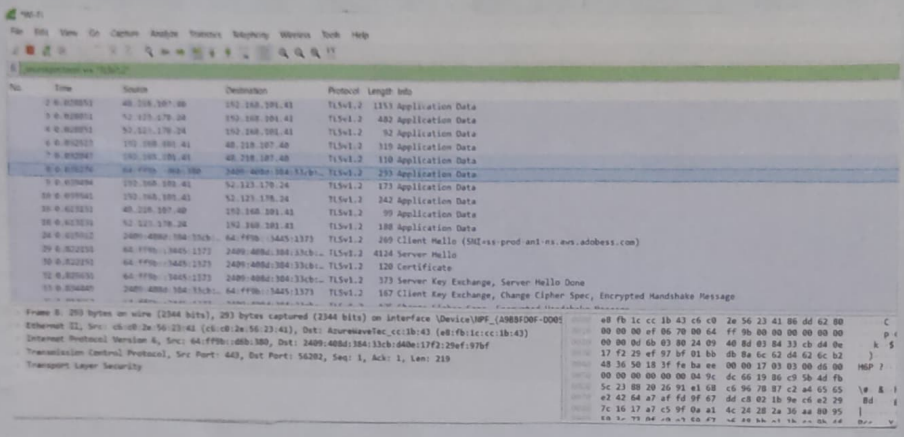


Filtering Packets :-

The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). We can also apply filter by selecting the packet → Apply as Filter → Selected.

Output:-

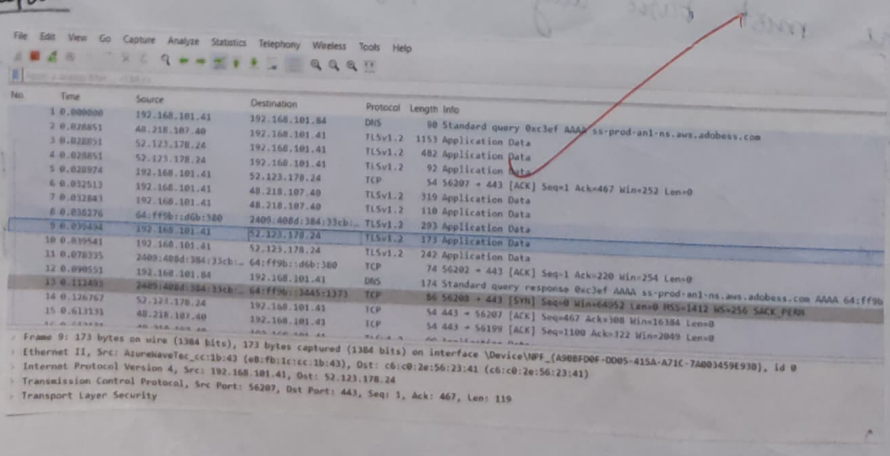




Inspecting Packets:-

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

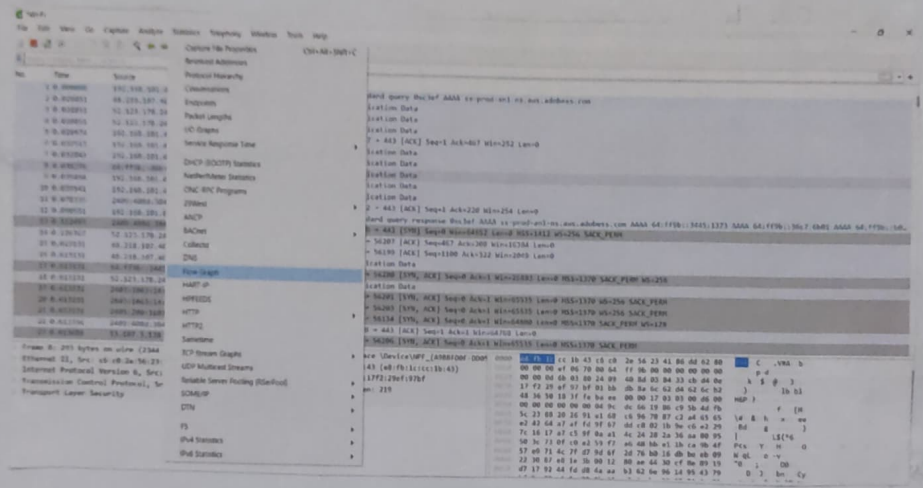
Output:-

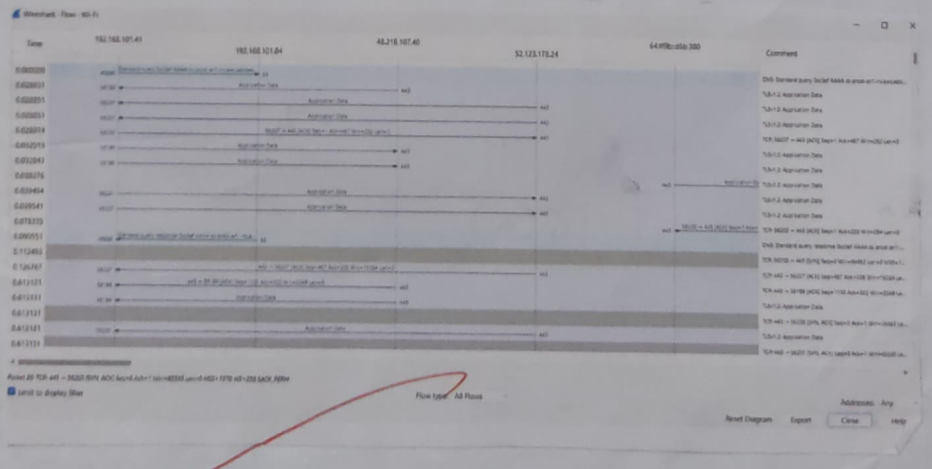


Flow Graph:-

We can see the flow graph of the packets. by clicking on the statistics and selecting the flow graph and it displays the flow graph of the packets.

Output:-





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

Procedure :-

→ Go to capture → option.

→ Select stop capture automatically after 100 packets.

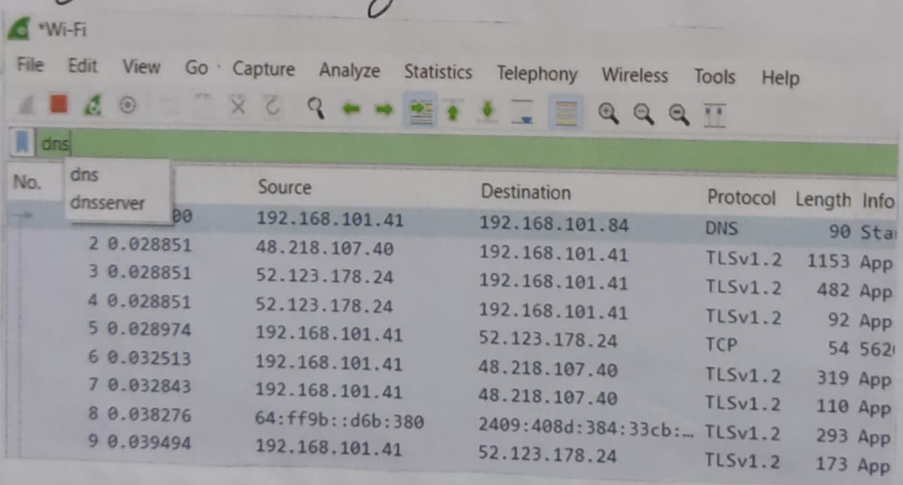
→ Then click start capture.

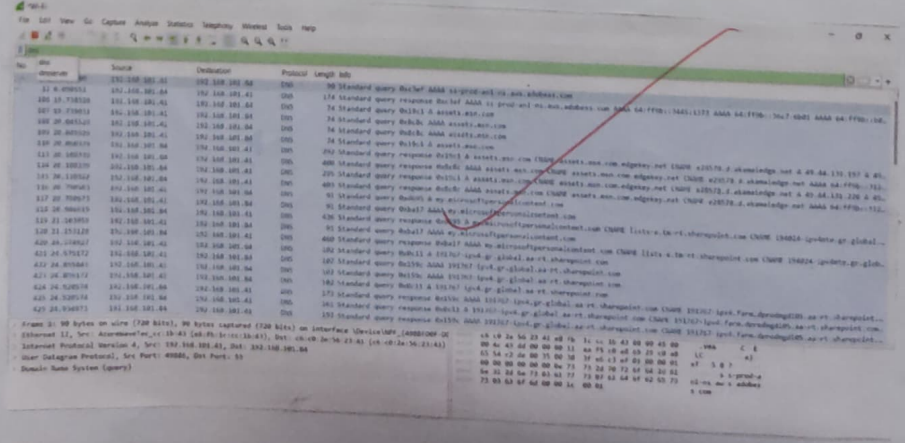
→ Search DNS packets in search bar.

→ To see flow graph click Statistics → Flow graph.

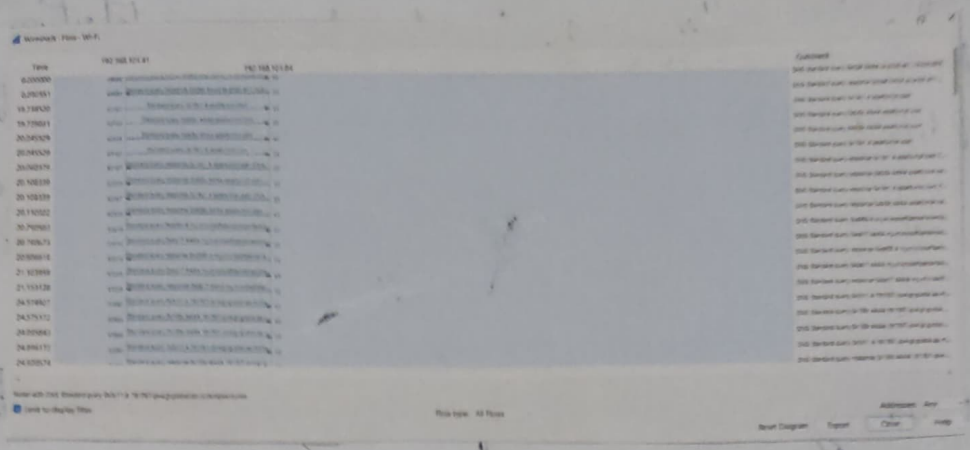
→ Save the packets.

Capturing and Filtering :-

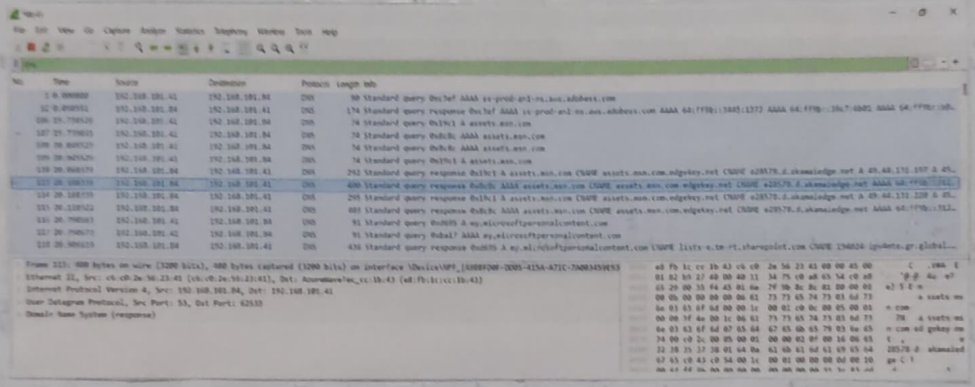




Inspecting :-



Flow Graph :-



9/8/24

Result :-

Thus, the experiments on packet capture tools like capturing; inspecting, filtering and displaying flow graph in wireshark is succesfully executed.