Task-5 Cybersecurity

Capture live network packets and identify basic protocols and traffic types

Report

1.Install Wireshark……

2.Start capturing on your active network interface……

3.Browse a website or ping a server to generate traffic……

4.Stop capture after a minute……

5.Filter captured packets by protocol (e.g., HTTP, DNS, TCP)……..

6.Identify at least……

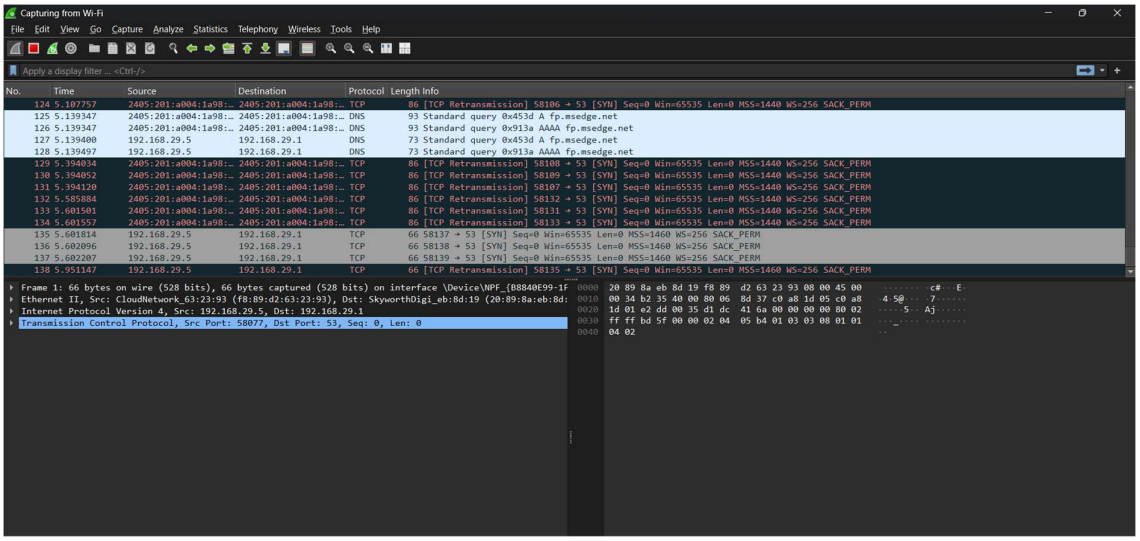
3 different protocols in the capture……

7.Export the capture as a .pcap file……..

8.Summarize your findings and packet details……

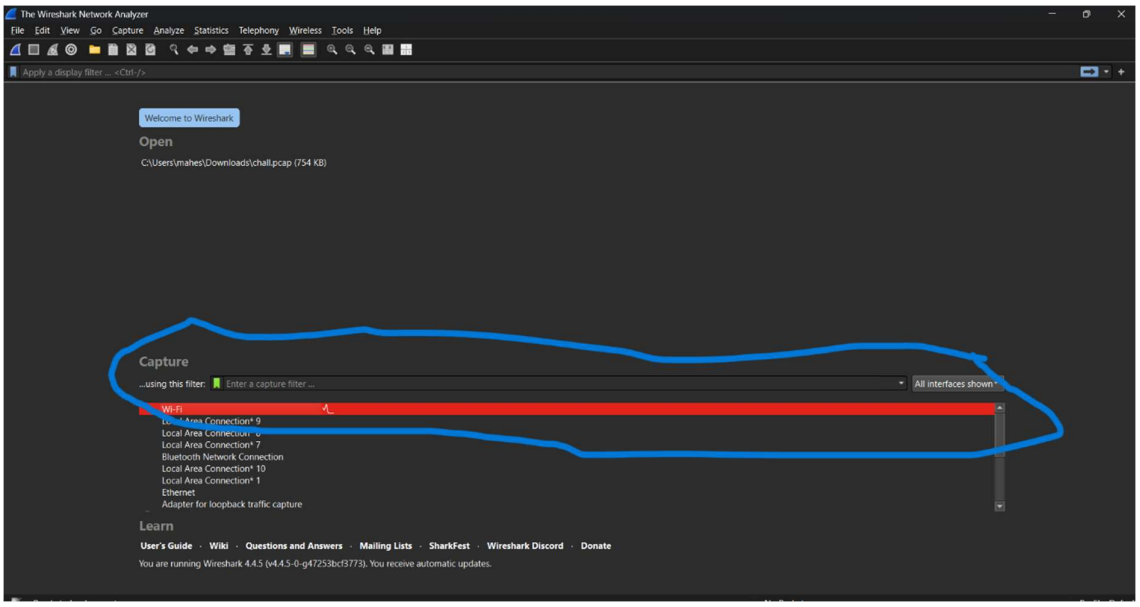
1.Install Wireshark

We need to install wireshark from official site

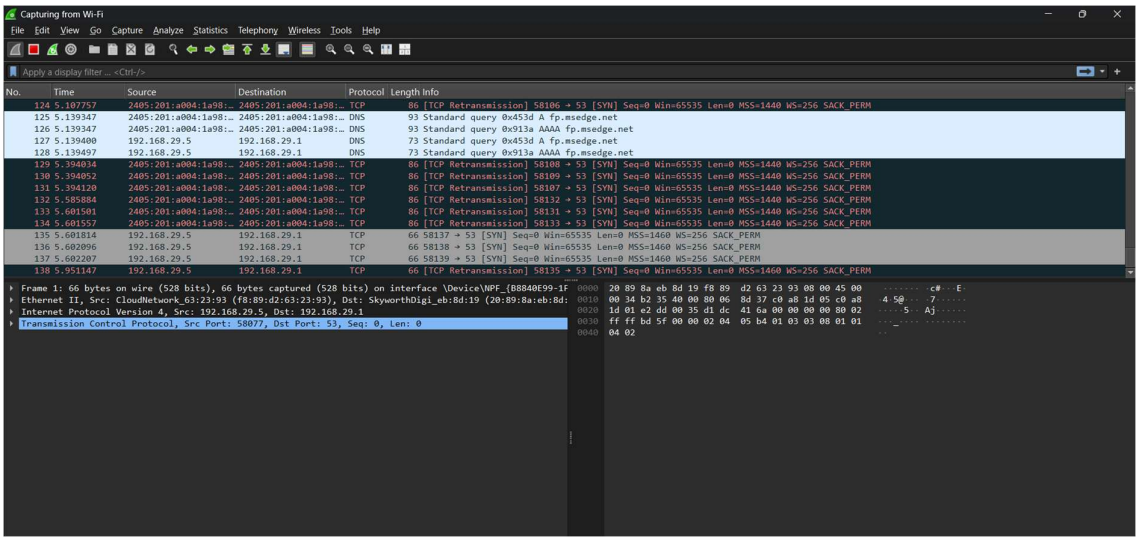


2.Start capturing on your active network interface.

So for start capturing our active network interface we first need to selct which network interface we need to monitor

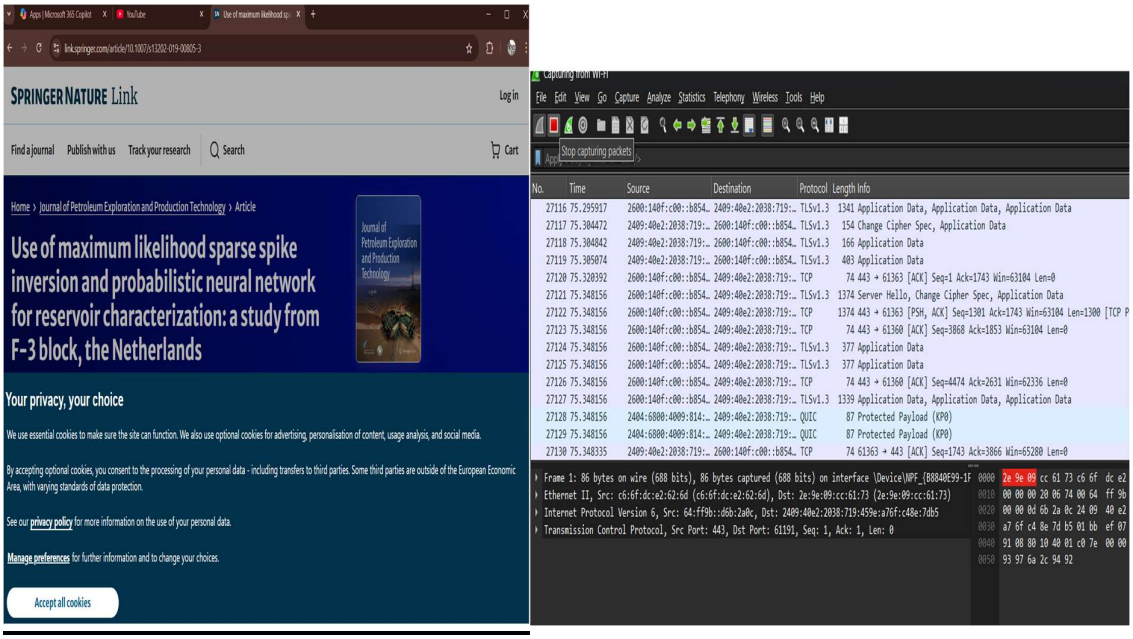


Then we start capturing the packets



3.Browse a website or ping a server to generate traffic.

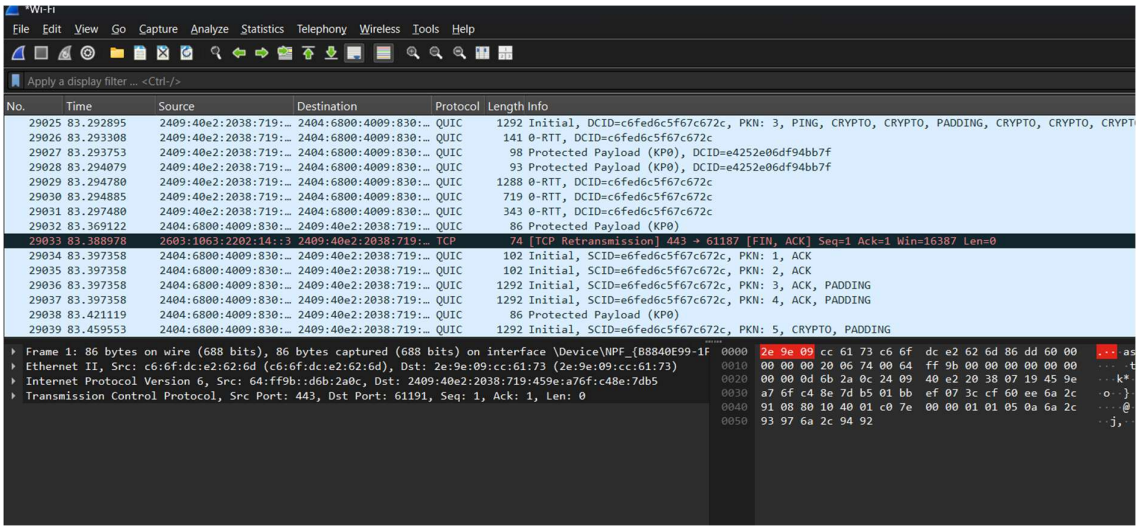
While we move to the browser and start browse



Then there is a sudden increase in network packets traffic in wireshark

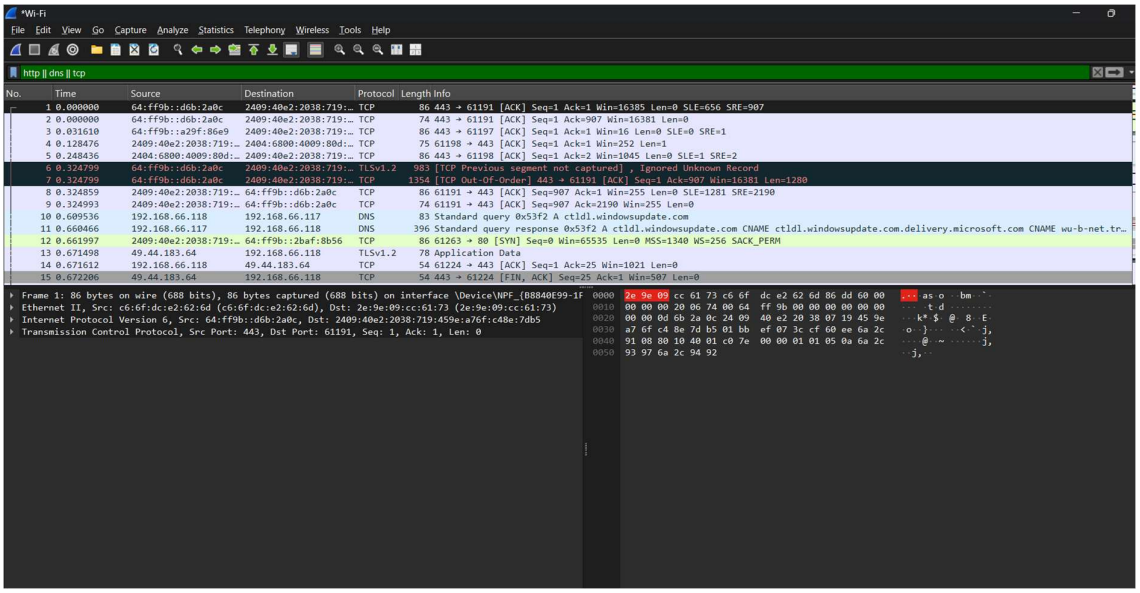
4.Stop capture after a minute.

By clicling the button marked in the screenshot we can stop the capturing



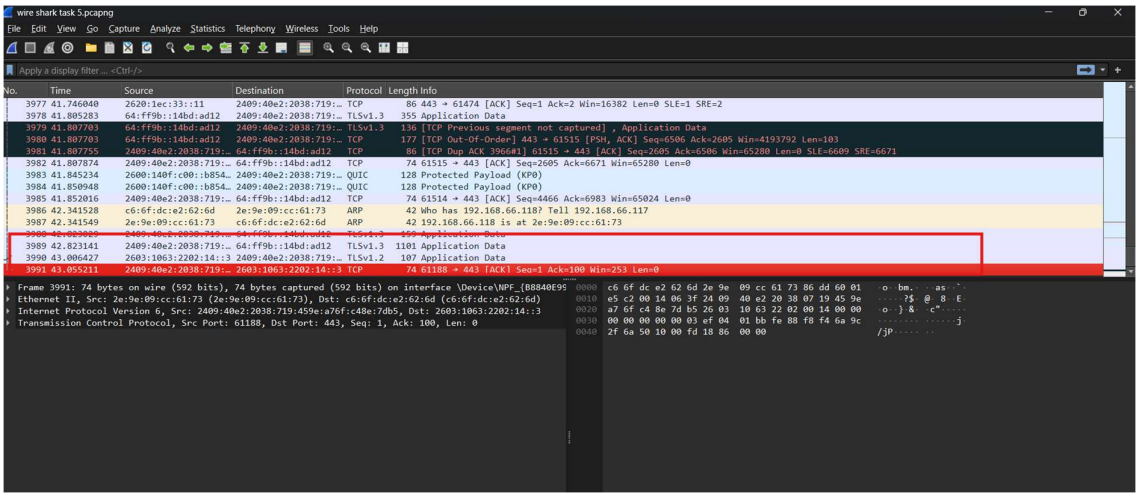
5.Filter captured packets by protocol (e.g., HTTP, DNS, TCP).

Here we search for HTTP || DNS || TCP in search filter part.



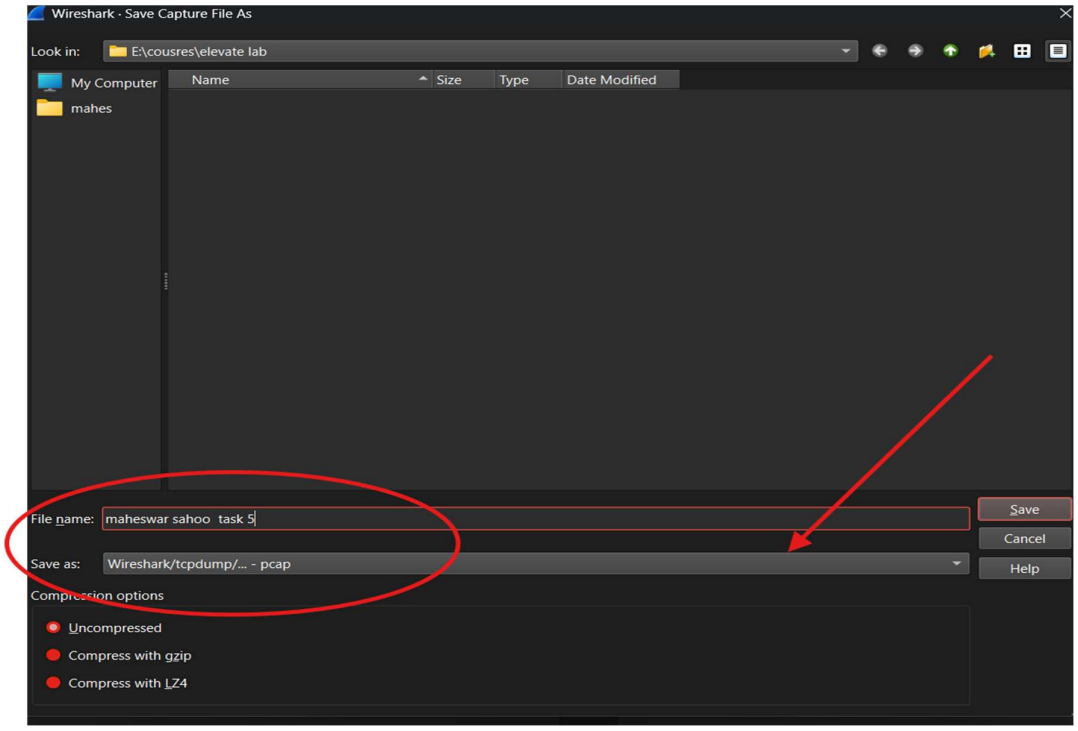
6.Identify at least 3 different protocols in the capture.

Last 3 packets capture are



7.Export the capture as a .pcap file.

For exporting the capture in .pcap file we need to stop capturing and press ctrl+shift+s



8.Summarize your findings and packet details.

In the above packet capturing we found all the packets running in the back ground of our system.