

## **Wireshark –**

`sudo apt install wireshark`

`sudo wireshark`

After opening wireshark,

If network interfaces are not shown, do ‘`sudo apt install libpcap0.8`’

After interfaces are shown, press CAPTURE

Then ‘START’ capture and it displays real time traffic of packets.

Also we go to STATISTICS on the top bar, and press I/O graph to get graphical representation.

## **Analyzing pcap file...**

Click FILE on the top bar and open the pcap file.

Then click ANALYZE on the top bar and try out different options.