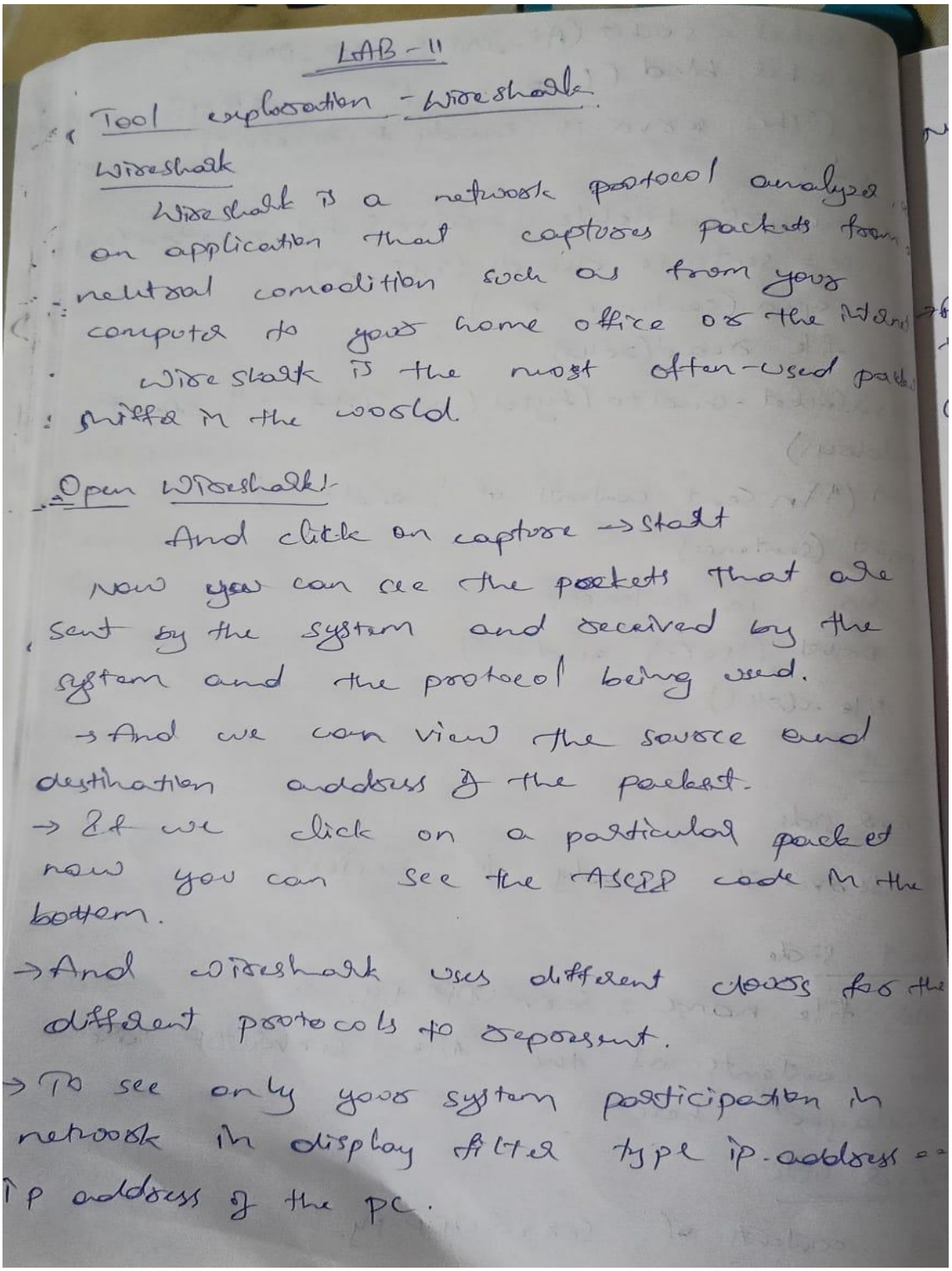
# LAB 15

Tool Exploration -Wireshark

**Observation:**



LAB - 11

Tool exploration - Wireshark

Wireshark

Wireshark is a network protocol analyzer, an application that captures packets from a network condition such as from your computer to your home office or the Internet. Wireshark is the most often-used packet sniffer in the world.

Open Wireshark!

And click on capture → start

Now you can see the packets that are sent by the system and received by the system and the protocol being used.

→ And we can view the source and destination address of the packet.

→ If we click on a particular packet now you can see the ASCII code in the bottom.

→ And Wireshark uses different colors for the different protocols to represent.

→ To see only your system participation in network in display filter type ip.address == ip address of the pc.

Ex:- Ipaddr = 10.124.7.1

Note:- To know ip address of the system open cmd & type ipconfig
you can now see the ip address of your system.

And we can even filter packets by the type of the protocol.

Goto to analyze & display filters to see the filters to stop capturing go to capture & click on stop.

To colors packet best go to view and click on colorize packet list.