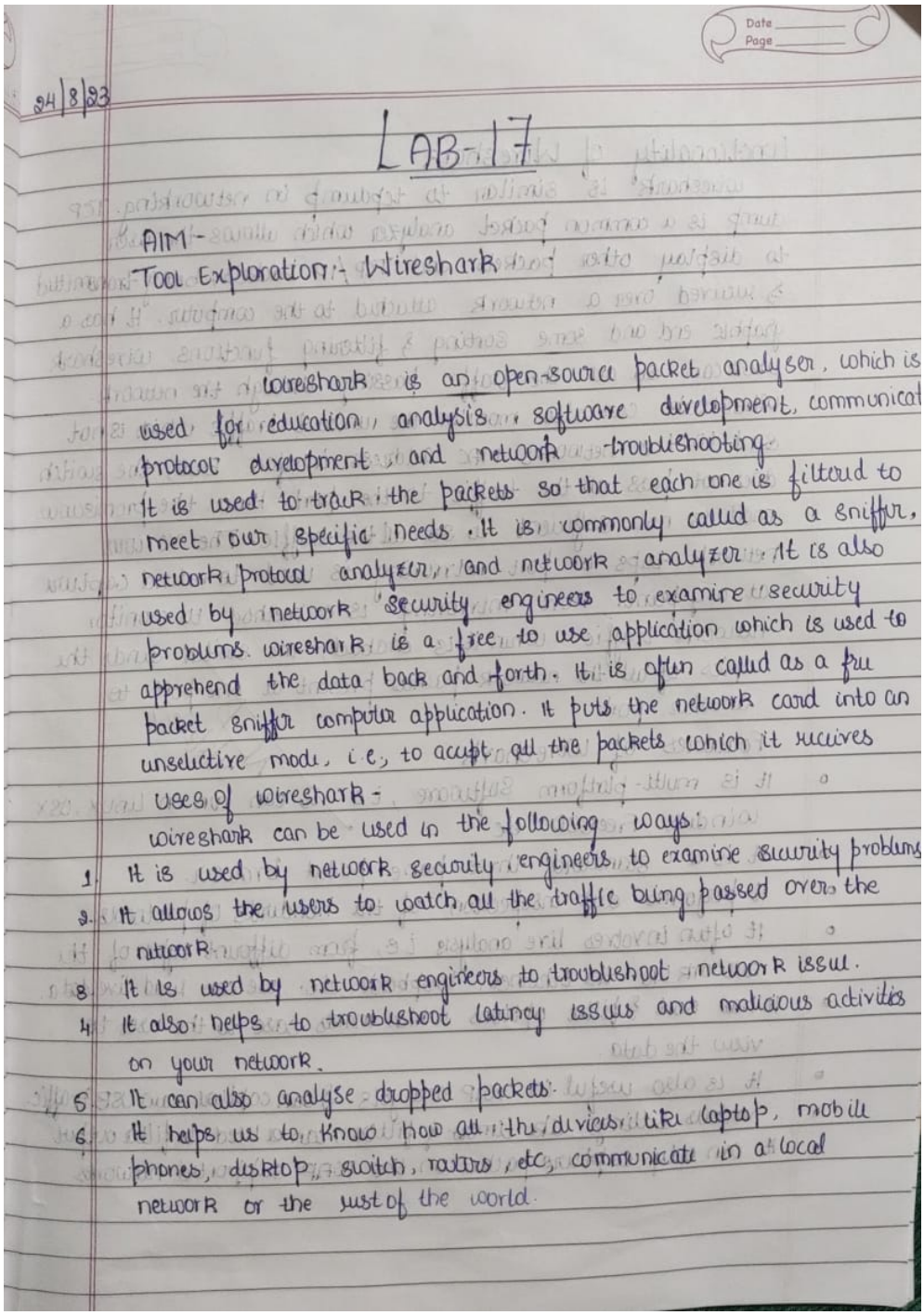
WEEK 17

Tool Exploration -Wireshark

OBSERVATION:



24/8/23

LAB-17

AIM-

Tool Exploration:- Wireshark

Wireshark is an open-source packet analyser, which is used for education, analysis, software development, communicat protocol development and network troubleshooting.

It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called as a sniffer, network protocol analyzer, and network analyzer. It is also used by network security engineers to examine security problems. Wireshark is a free to use application which is used to apprehend the data back and forth. It is often called as a fre packet sniffer computer application. It puts the network card into an unselective mode, i.e, to accept all the packets which it receives

Uses of Wireshark -

Wireshark can be used in the following ways:

1. It is used by network security engineers to examine security problems
2. It allows the users to watch all the traffic being passed over the network.
3. It is used by network engineers to troubleshoot network issues.
4. It also helps to troubleshoot latency issues and malicious activities on your network.
5. It can also analyse dropped packets.
6. It helps us to know how all the devices like laptop, mobile phones, desktop, switch, routers, etc, communicate in a local network or the rest of the world.

Functionality of Wireshark

Wireshark is similar to tcpdump in networking. TCP dump is a common packet analyzer which allows the user to display other packets and TCP/IP packets, being transmitted & received over a network attached to the computer. It has a graphic end and some sorting & filtering functions. Wireshark users can see all the traffic passing through the network. Wireshark can also monitor the unicast traffic which is not sent to the network's MAC address interface. But, the switch does not pass all the traffic to the port. Hence, the promiscuous mode is not sufficient to see all the traffic. The various network taps or port mirroring is used to extend capture at any point. Port mirroring is a method to monitor network traffic. When it is enabled, the switch sends the copies of all the network packets present at one port to another port.

Features of Wireshark

- It is multi-platform software, i.e. it can run on Linux, OSX, Windows, FreeBSD, etc.
- It is a standard three-pane packet browser.
- It performs deep inspection of the hundreds of protocols.
- It often involves live analysis i.e, from different types of the network like the Ethernet, loopback, etc. we can read live data.
- It has sort & filter options which makes ease to the user to view the data.
- It is also useful in VOIP analysis & can capture raw USB traffic.
- various settings, like timers & filters, can be used to filter output.
- It can only capture packet on the PCAP supported networks.