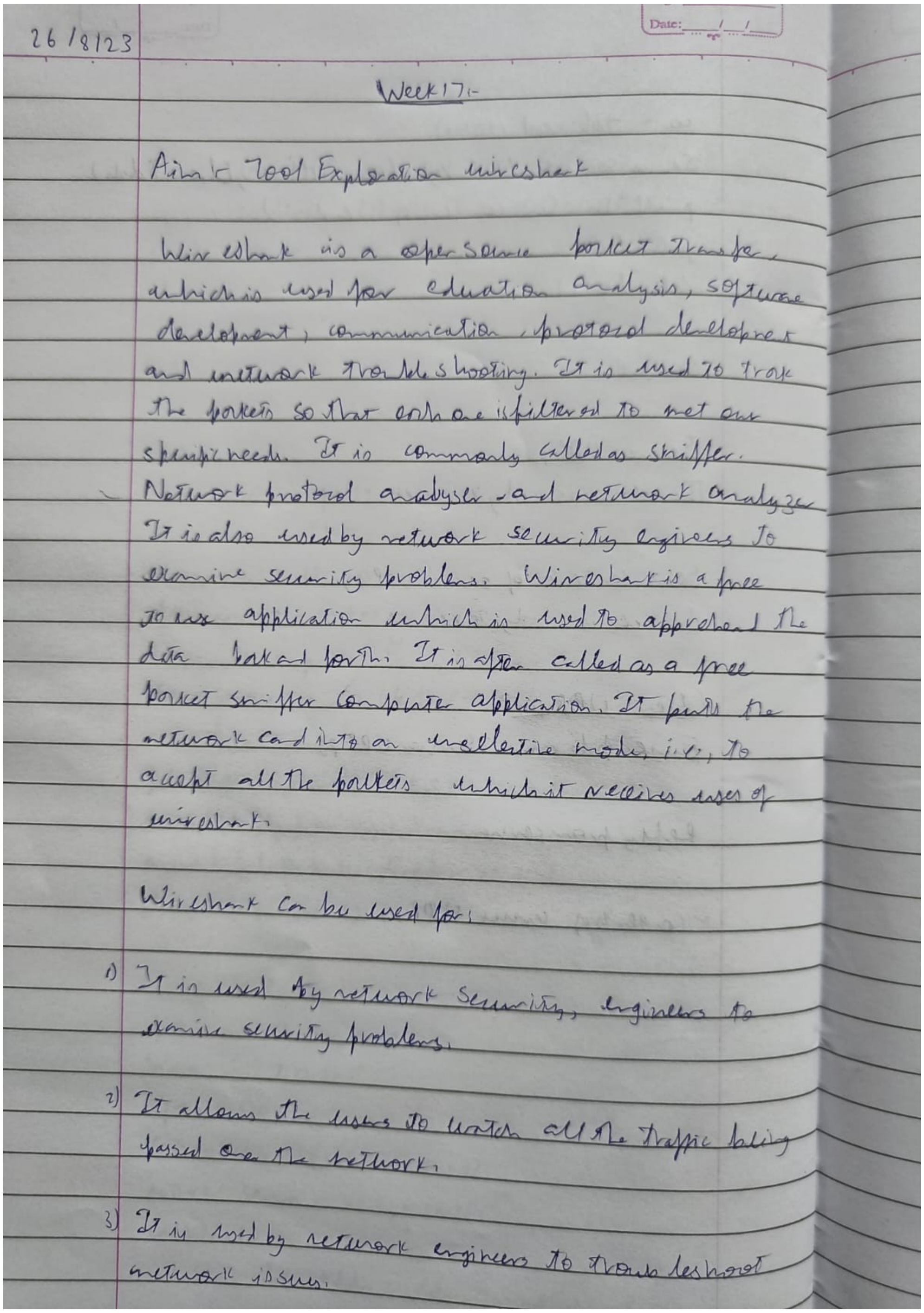
WEEK 17

Tool Exploration -Wireshark

OBSERVATION:



26/8/23

Date: / /

Week 17:-

Aim:- Tool Exploration wireshark

Wireshark is a open source packet transfer, which is used for education analysis, software development, communication, protocol developmet and network troubleshooting. It is used to track the packets so that each one is filtered to met our specific needs. It is commonly called as sniffer, Network protocol analyser 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 free packet sniffer computer application. It puts the network card into an unselective mode, i.e., to accept all the packets which it receives users of wireshark.

Wireshark can be used for:

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.

Functionality:-

Wireshark is similar to dump in networking. TCP dump is a common packet analyser which allows the user to display other packets and TCP/IP packets, being transmitted and received over a network attached to the computer. It has a graphic end and some sorting and filtering functions. Wireshark users can see all the traffic passing through the network.

But the switch does not pass all the traffic to the port. The various network taps or port mirroring is used to extend capture at any point. When it is enabled, the switch sends the copies of all the network packets present at one port to another port.

Features:-

- It is multi platform software, it can run on Linux, Windows, Free BSD etc.
- It is a standard three pane packet browser.

- It performs deep inspection of hundreds of protocols.
- It also useful in voip analysis and can capture any raw USB traffic.
- Various settings like timers and filters, can be used to filter output.
- It can only capture packets on the PCAP supported networks.