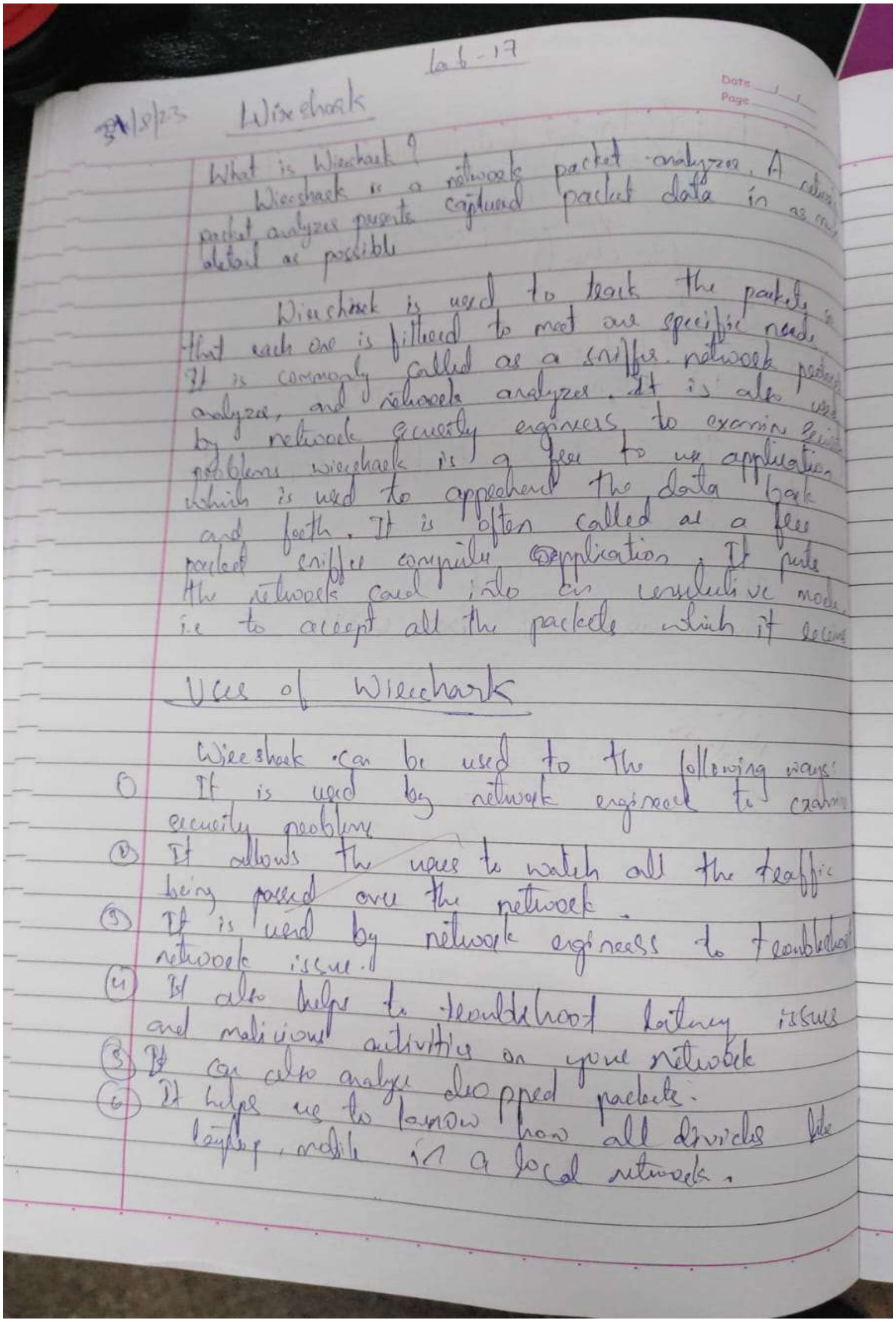
# WEEK 17

Tool Exploration -Wireshark

OBSERVATION:



lab-17

Date / /
Page

31/8/23 Wireshark

What is Wireshark ?

Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible

Wireshark 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 free 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 to the following ways:

1. It is used by network engineers to examine security problems
2. It allows the user to watch all the traffic being passed over the network.
3. It is used by network engineers to troubleshoot network issue.
4. It also helps to troubleshoot latency issues and malicious activities on your network
5. It can also analyze dropped packets.
6. It helps us to know how all devices like laptop, mobile in a local network.

Date __/__/__
Page ______

## 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 mac address interface. But, the switch doesnot pass all the traffic to the port. Hence, the switch doesnot pass all the traffic to the port.

31/8/2023.

## Features of wireshark

(1) It is a multi-platform software, i.e it can run on linux, osx, windows, Free BSD etc

(2) It is a standard three-pane packet browser

(3) It performs deep inspection of the hundreds of protocols

(4) It often involves live analysis i.e from different types of the network like the ethernet, loopback etc

(5) It has sort of filter options which makes easy to the user to view the data.

(6) It is also useful in VOIP analysis & can capture raw USB traffic

(7) Various settings, like timers & filters, can be used to filter output.