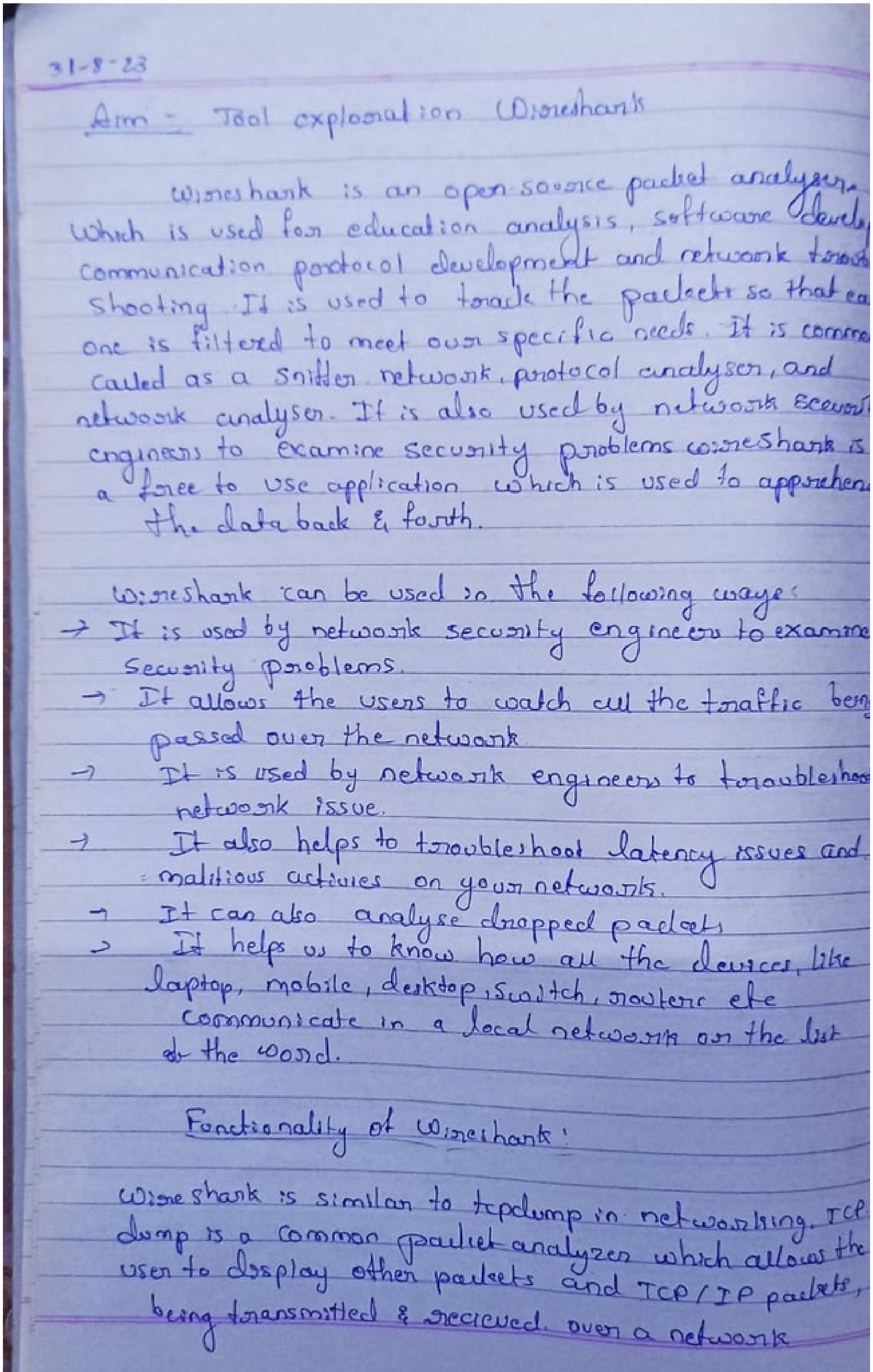
WEEK 17

Tool Exploration -

Wireshark OBSERVATION:



31-8-23

Aim - Tool exploration Wireshark

Wireshark is an open-source packet analyser. Which is used for education analysis, software develo communication protocol development and network trou shooting. It is used to track the packets so that ea one is filtered to meet our specific needs. It is comme called as a sniffer network, protocol analyser, and network analyser. It is also used by network securi engineers to examine security problems wireshark is a free to use application which is used to apprehen the data back & forth.

Wireshark can be used in the following ways:

→ It is used by network security engineers to examine security problems.

→ It allows the users to watch all the traffic bein passed over the network.

→ It is used by network engineers to troubleshoo network issue.

→ It also helps to troubleshoot latency issues and malitious activies on your network.

→ It can also analyse dropped packets

→ It helps us to know how all the devices, like laptop, mobile, desktop, switch, router etc communicate in a local network or the list of the word.

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 & recieved. 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 networks MAC address intetace. But, the switch does not pass all the traffic to port.

Hence, the promiscious 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.

1/9/2023