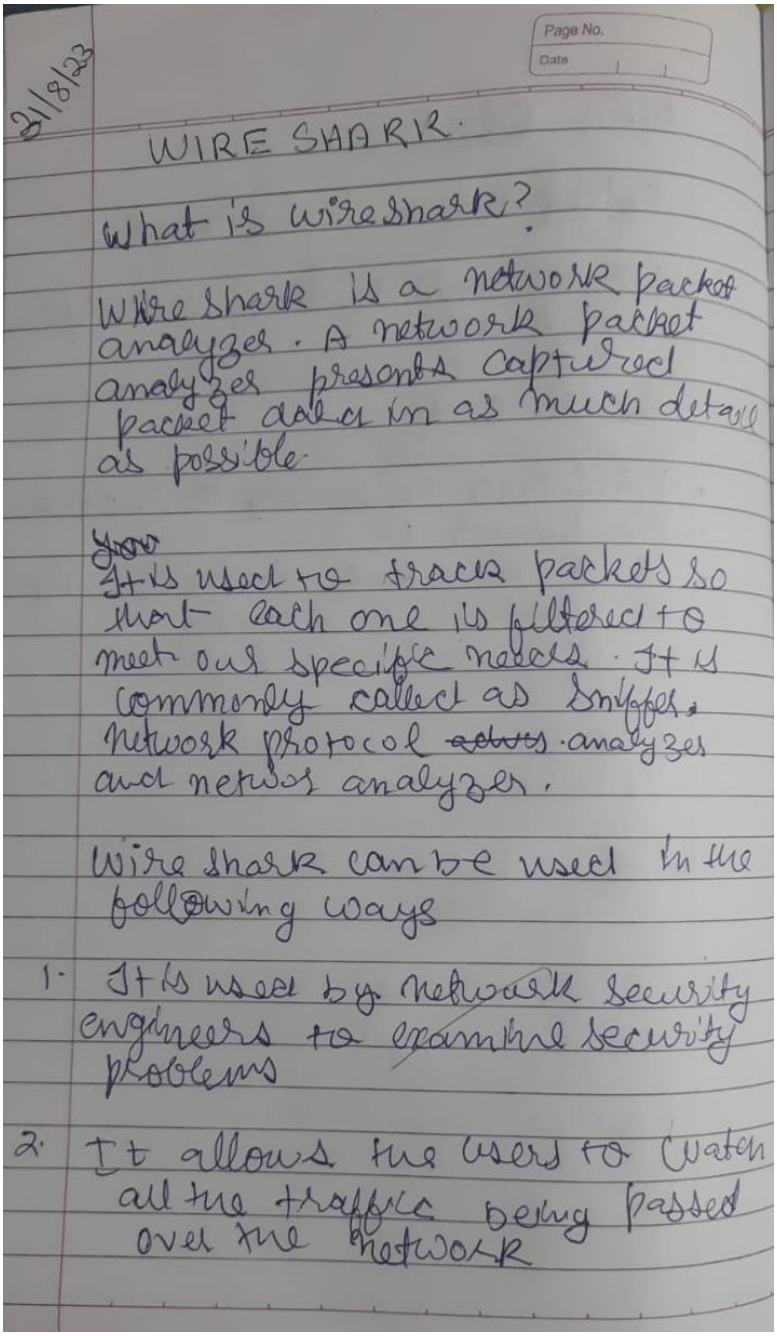
WEEK17

Tool Exploration -Wireshark

OBSERVATION:



21/8/23

Page No.
Date

WIRE SHARK.

What is wireshark?

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

~~You~~
It is used to track packets so that each one is filtered to meet our specific needs. It is commonly called as Sniffer, network protocol ~~advis~~ analyzer and network analyzer.

Wire shark 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 engineering to troubleshoot latency and malicious activities on your network.

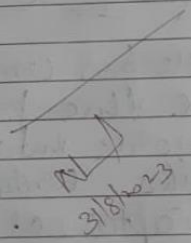
4. It can analyse dropped packets

5. It helps us to know all the devices like laptop, mobile, desktop, switch etc. communicate in local network.

Features of wireshark

→ Available for unix and windows
→ Capture live packet data from a network interface.
→ Open files containing packet data captured with tcpdump/ WinDump, wireshark and many other packet capture programs
→ Display packets with very detailed protocol information
→ Save packet data captured
→ Filter packets on many criteria

→ Search for packets on many criteria.

→ colorize packet display based on filters.

→ create various statistics