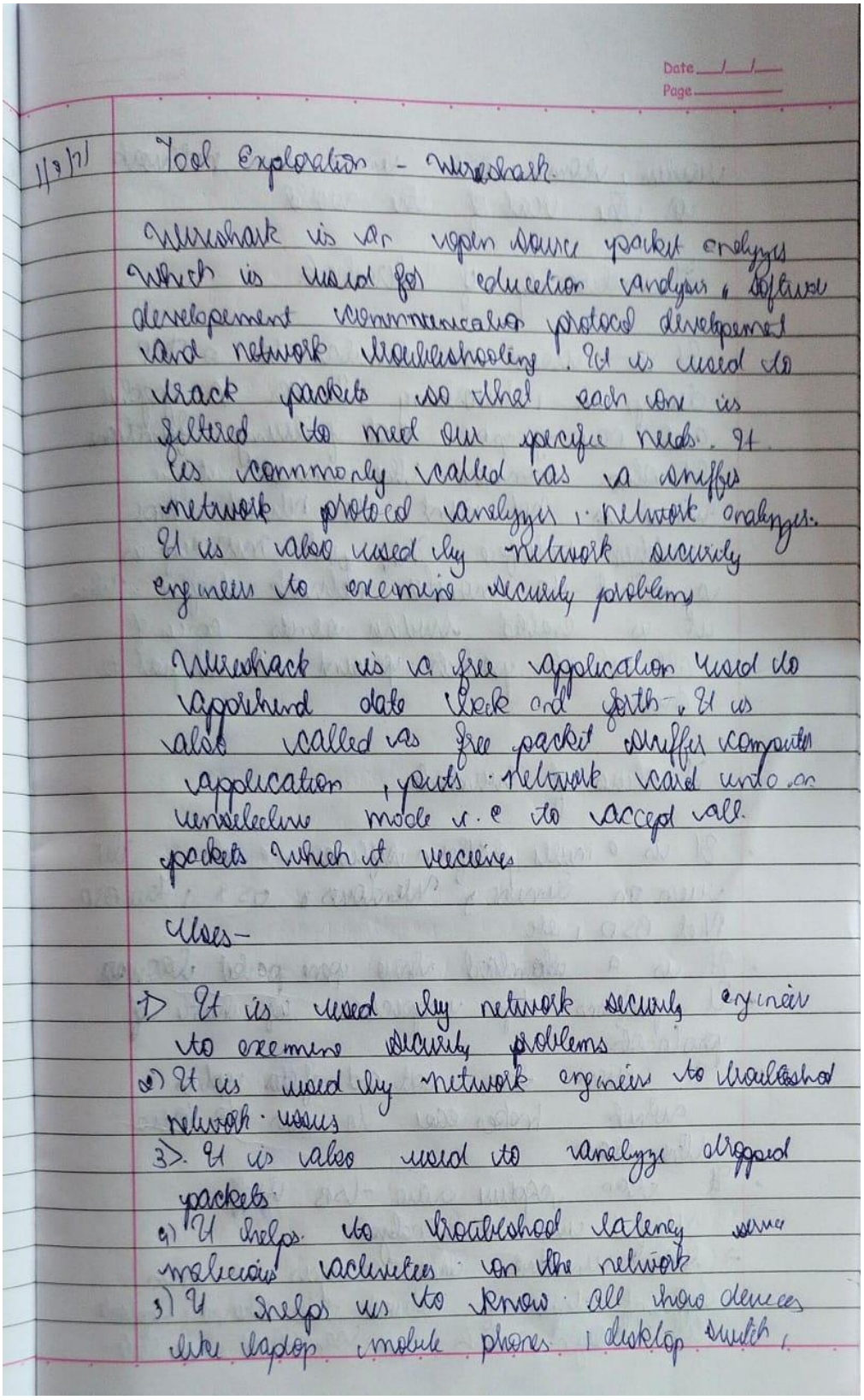
CN LAB-17

OBSERVATION



Date / /
Page

1/9/21 Tool Exploration - Wireshark

Wireshark is an open source packet analyzer which is used for education analysis, software development communication protocol development and network troubleshooting. It is used to track packets so that each one is filtered to meet our specific needs. It is commonly called as a sniffer network protocol analyzer, network analyzer. It is also used by network security engineers to examine security problems

Wireshark is a free application used to apprehend data back and forth. It is also called as free packet sniffer computer application, ports. network card into an unselective mode i.e to accept all packets which it receives

Uses -

1) It is used by network security engineer to examine security problems
2) It is used by network engineers to troubleshoot network issues
3) It is also used to analyze dropped packets
4) It helps to troubleshoot latency issues malicious activities on the network
5) It helps us to know all those devices like laptop, mobile phones, desktop, switch,

Date / /
Page

wireless, communicate in a lan network all the world

Functionality of Wireshark

It is used to similar to a TCP dump in networking. It has a graphic and non-graphic and filtering functions. It also monitors the unicast traffic which is not sent to network's NIC. adapter interface. The port mirroring is a method to monitor network traffic. When it is enabled switch sends copies of all network packets present at one port to another.

Features of wireshark

- It is a multi platform software i.e it can run on Linux, Windows, OS X, FreeBSD, NetBSD, etc
- It is a standard three pane packet browser.
- It performs deep inspection of hunts of protocols
- It even has sort and filter option which helps user to view also know the data
- It can capture raw USB traffic
- Useful in VP analysis
- Also involves live analysis i.e from different types of network like ethernet, loopback through which we can read live data