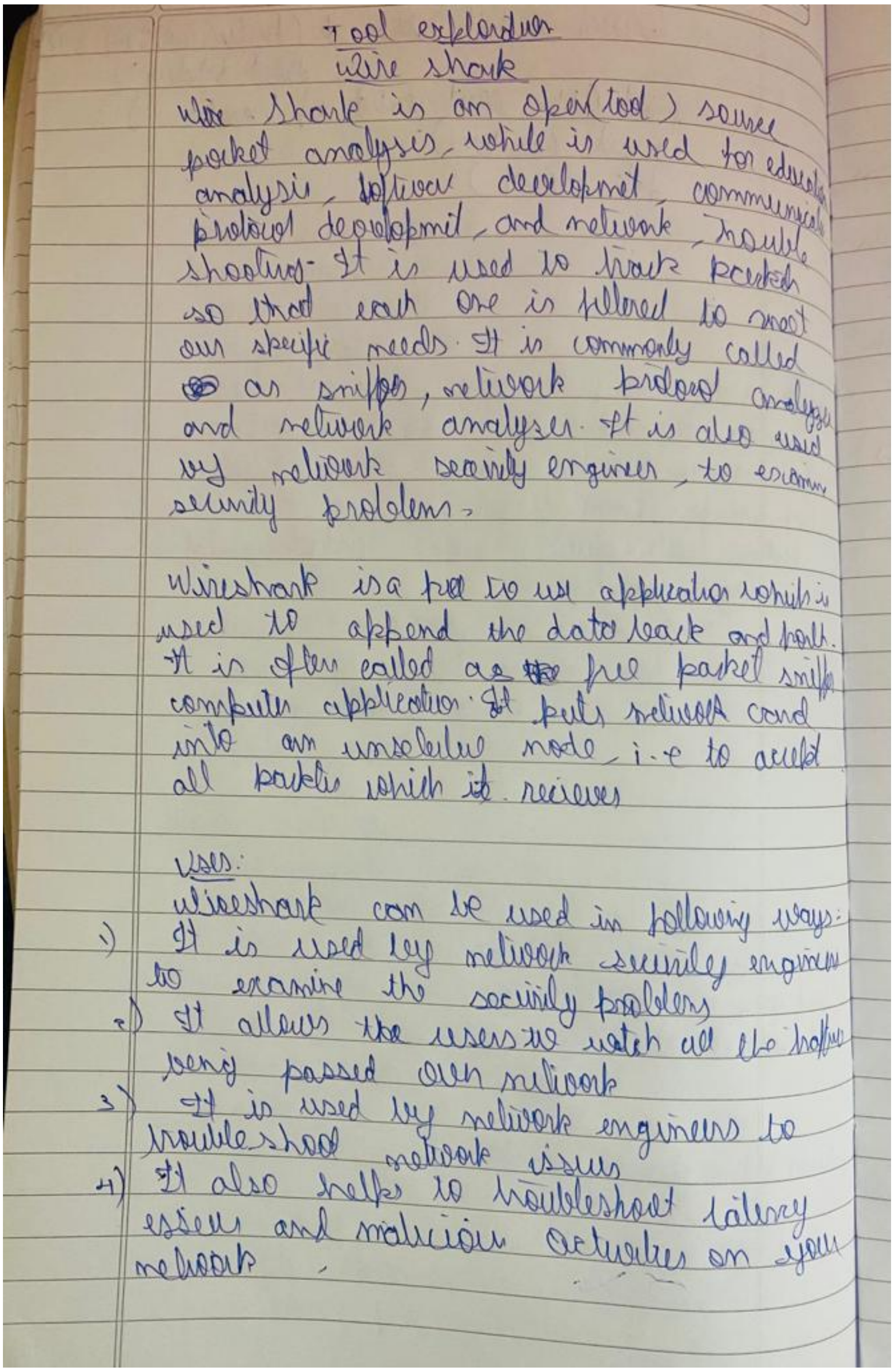
Wireshark



Tool exploration

Wire shark

Wire Shark is an open (tool) source packet analysis, which is used for education analysis, software development, communication protocol development, and network trouble shooting. 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 analyser and network analyser. It is also used by network security engineer, to examine security problems.

Wireshark is a free to use application which is used to append the data back and forth. It is often called as free packet sniffer computer application. It puts network card into an unselective mode i.e to accept all packets which it recieves

Uses:

Wireshark can be used in following ways:

1) It is used by network security engineers to examine the security problems
2) It allows the users to watch all the traffic being passed over network
3) It is used by network engineers to troubleshoot network issues
4) It also helps to troubleshoot latency issues and malicious activities on your network.

5) → It can also analyse dropped packet
6) It helps to know how all the devices like laptop, mobile, switch etc communicate in a local network or rest of the wall.

Functionality of wireshark:
Wireshark is similar to tcpdump in networking. TCP dump is a common packet analyzer which allows the user to display other packet and TCP/IP packets being transmitted and received over a network attached to computer. It has a graphic end and some sorting and filtering functions.

Wireshark users can see all traffic passing through the network.

Wireshark can also monitor the unicast traffic which is not sent to network's MAC address interface. But the switch does not pass all the traffic to port. Hence, the promiscuous mode is not sufficient to see all traffic

Port mirroring is method to monitor the network traffic. When it is enabled the switch sends the copies of all the network packets present at one port to another port

There are a few features of wireshark which are significant

DATE :

Features of Wireshark :

1) It is a multiplatform software i.e it can run on Linux, Window, Net BSD etc
2) It is a standard three pane packet browser
3) It performs deep inspection of hundreds of protocol.
4) It often involves live analysis i.e from different types of network like Ethernet, loopback we can read live data.
5) It has sort and filter options which makes ease to user to view the data.
6) It is also useful in VoIP analysis.
7) It can also capture raw USB traffic.