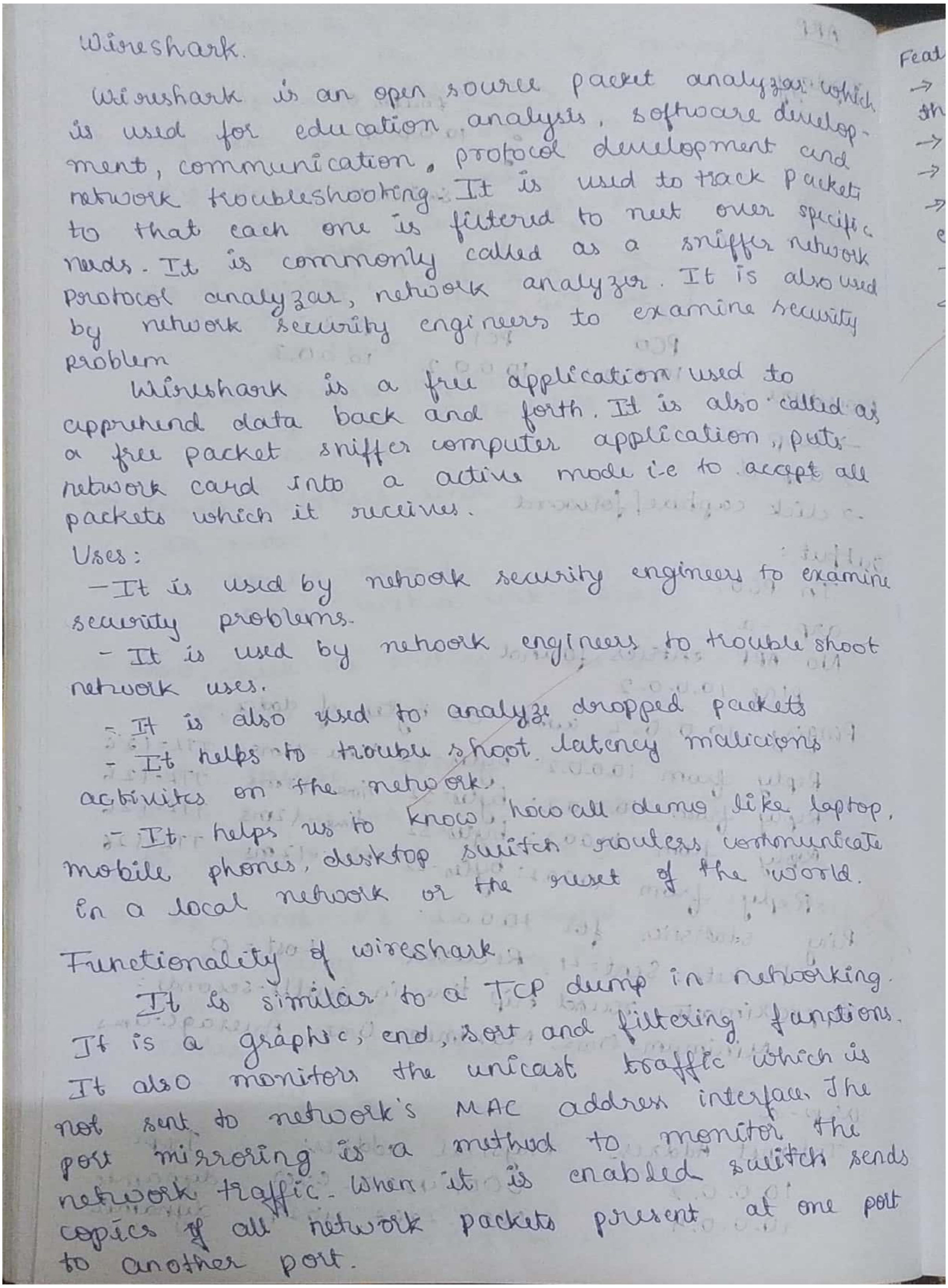
Tool Exploration -Wireshark



Wireshark.

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

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

Uses:

- It is used by network security engineers to examine security problems.
- It is used by network engineers to trouble shoot network uses.
- It is also used to analyze dropped packets
- It helps to trouble shoot latency malicions activites on the network.
- It helps us to know, how all demo like laptop, mobile phones, desktop switch routers communicate in a local network or the reset of the world.

Functionality of wireshark:

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

Features of wireshark:

→ It is a multi platform software i.e it can run on the linux, windows, OS x, TrueBSD, NetBSD etc.

→ It is a standard three pane packet browser.

→ It performs deep inspection of hunk of protocols.

→ It even has standard filters option which makes ease to user to view the data

→ It can caphure raw USB traffic

→ It is useful in IP analysis.

5/9