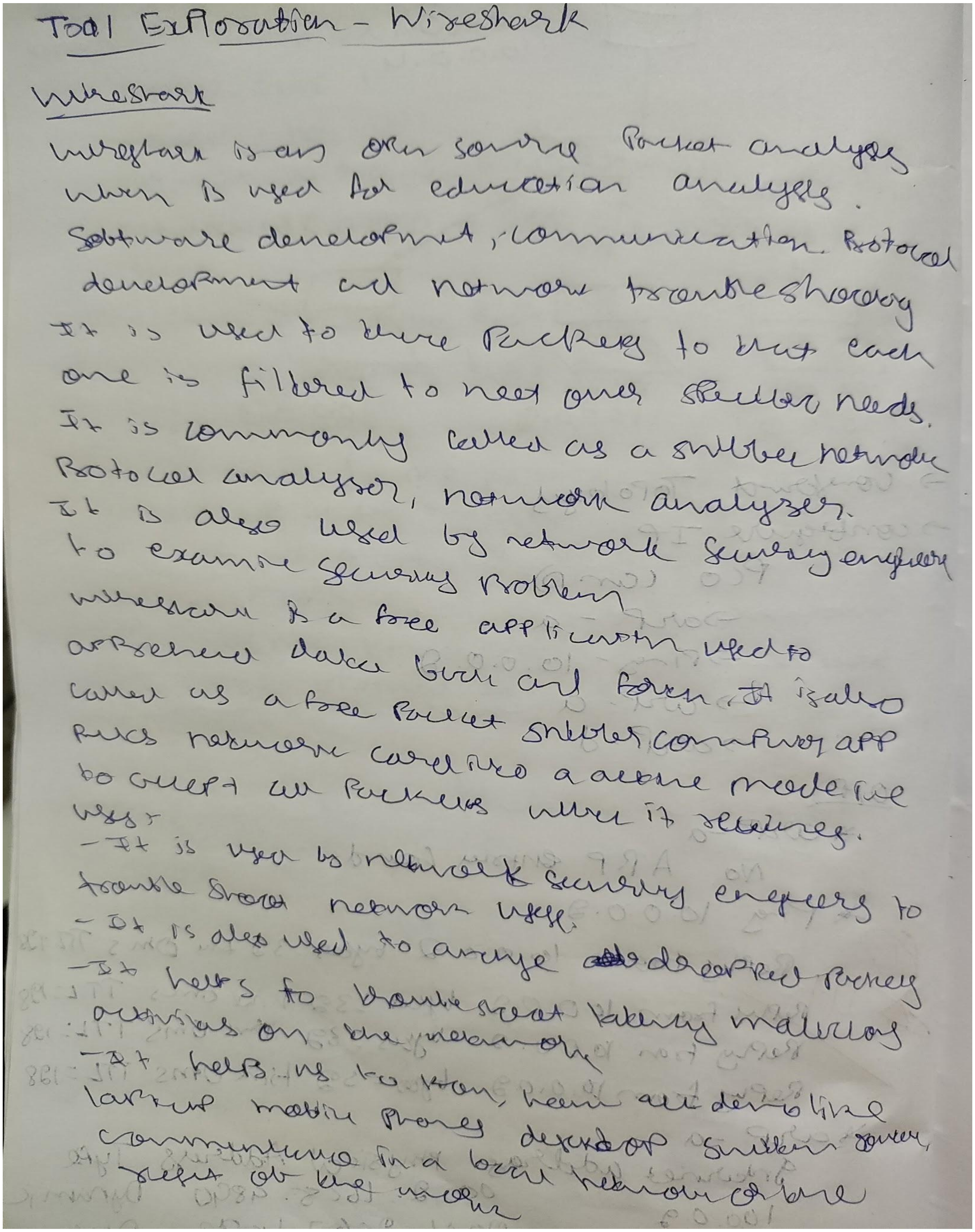
Tool Exploration -Wireshark



Tool Exploration - Wireshark

Wireshark

Wireshark is an open source packet analyser 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 analyser, network analyser. 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 app. Puts network card into a unique mode i.e. to accept all packets which it receives.

- It is used by network security engineers to trouble shoot network issues.
- It is also used to analyse ~~[illegible]~~ dropped packets
- It helps to troubleshoot latency malicious activities on the network.
- It helps us to know, how all devices like laptop mobile phones desktop switches server, communicate in a local network or the rest of the world

Functionalities of wireshark:

It is similar to a TCP Dump in networking. It is a graphic end sort and filtering functions. It is 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, Free BSD, NetBSD etc.
- It is a standard three pane packet browser.
- It performs deep inspection of hundreds of protocols.
- It even has standard filtering option which makes easy to user to view the data
- It can capture raw USB traffic
- It is useful in VoIP analysis