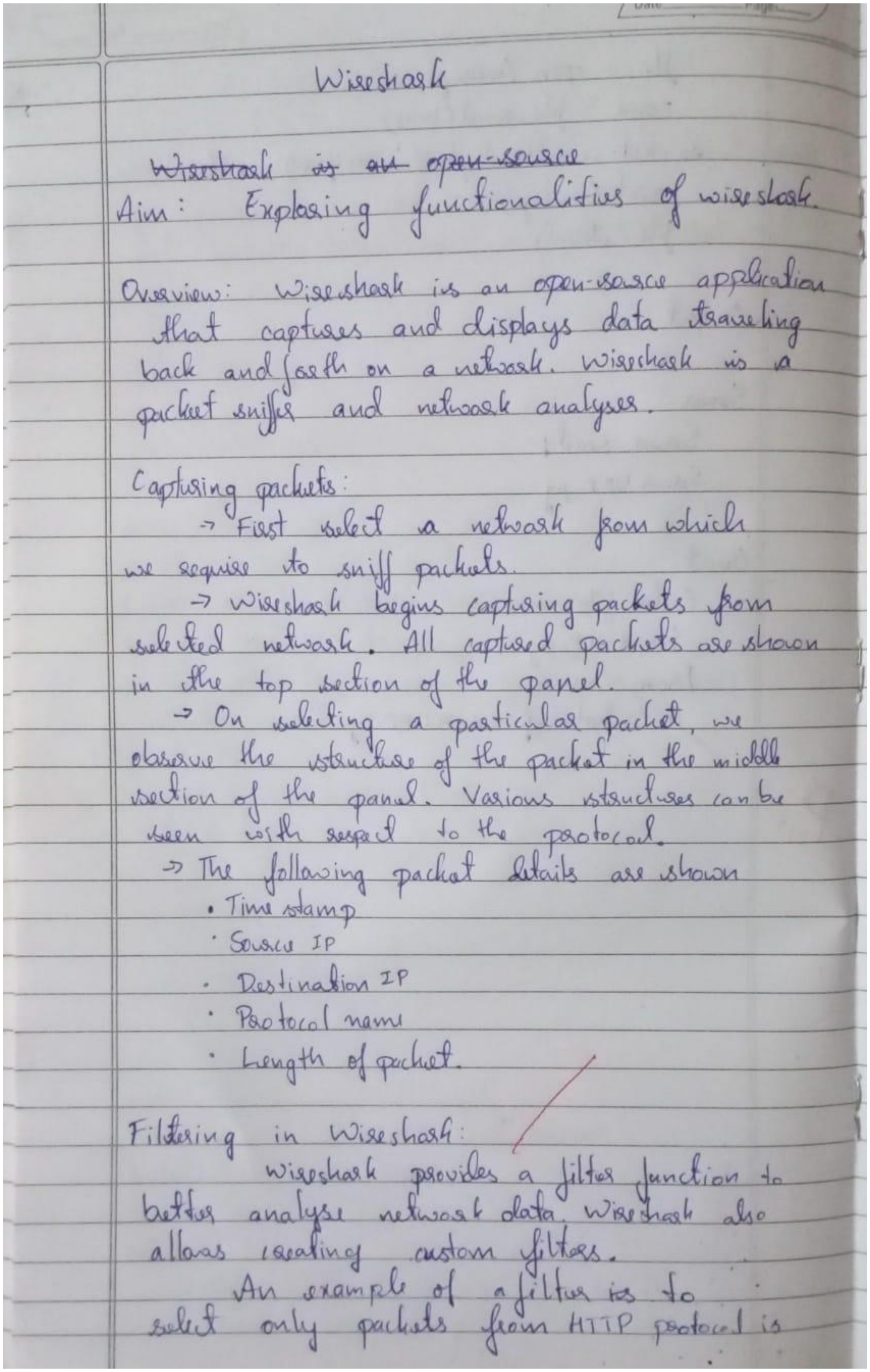
Wireshark



Wireshark

~~Wireshark is an open-source~~

Aim: Exploring functionalities of wireshark.

Overview: Wireshark is an open-source application that captures and displays data traveling back and forth on a network. Wireshark is a packet sniffer and network analyser.

Capturing packets:

→ First select a network from which we require to sniff packets.

→ Wireshark begins capturing packets from selected network. All captured packets are shown in the top section of the panel.

→ On selecting a particular packet, we observe the structure of the packet in the middle section of the panel. Various structures can be seen with respect to the protocol.

→ The following packet details are shown

- Time stamp
- Source IP
- Destination IP
- Protocol name
- Length of packet.

Filtering in Wireshark:

Wireshark provides a filter function to better analyse network data. Wireshark also allows creating custom filters.

An example of a filter is to select only packets from HTTP protocol is tcp.port ==80 || udp.port ==80

Packet details:

The middle section of the panel, detail panel, presents the protocols and protocol fields of the selected packet in a collapsible format. We can apply additional filters and right on click on protocol ~~to~~ ~~vie~~ for a detailed view.

At the bottom panel, raw data of the selected packet is seen in hexadecimal format. It is called as hex dump. It contains 16 ~~a~~ hexadecimal bytes and 16 ASCII bytes alongside the data offset.

Selecting a specific portion of this raw data automatically highlights its corresponding section in packet details pane. Bytes that cannot be represented is shown as a period ('.').