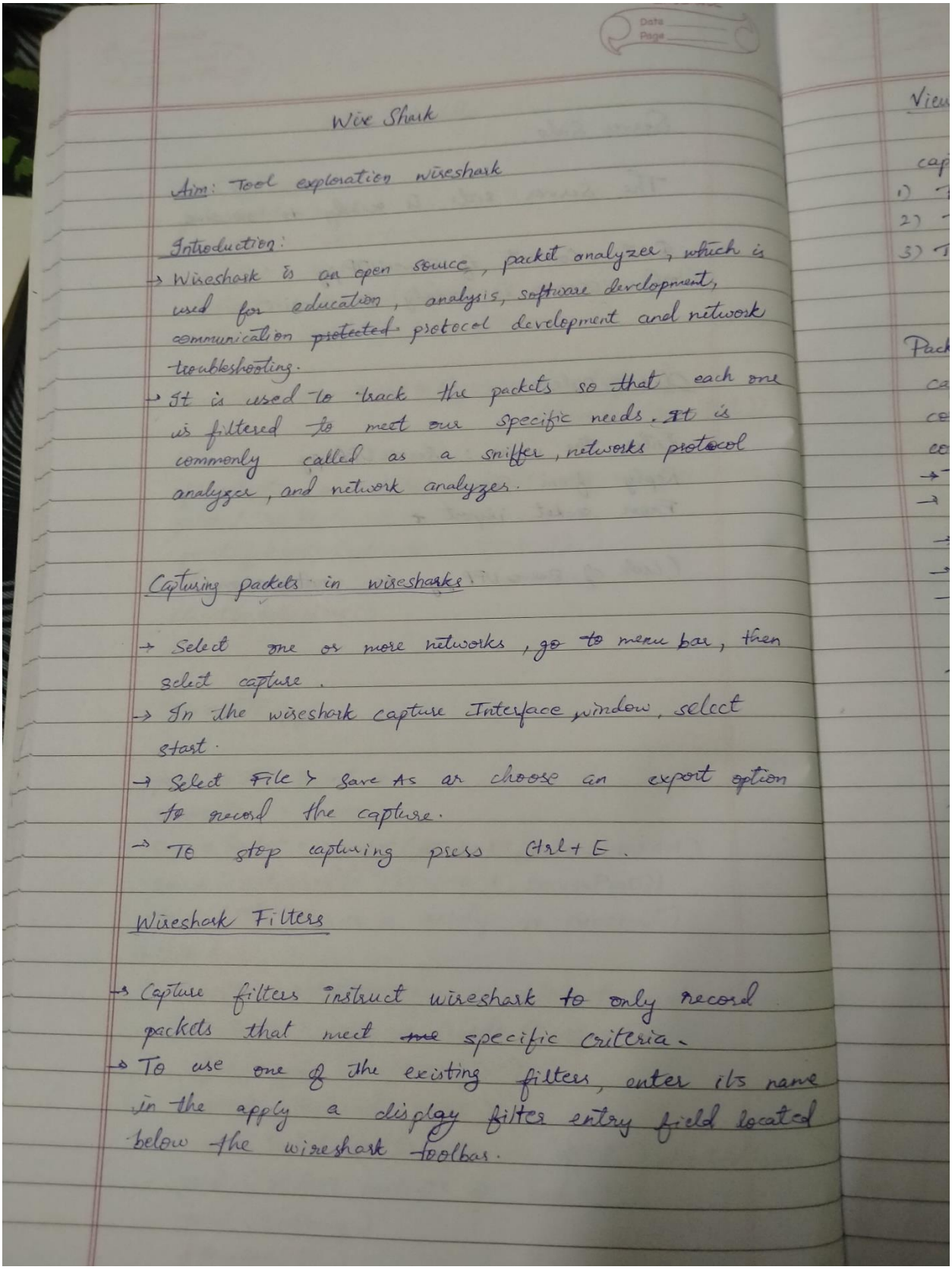
Tool Exploration - Wireshark



Wire Shark

Aim: Tool exploration wireshark

Introduction:

→ 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 the packets so that each one is filtered to meet our specific needs. It is commonly called as a sniffer, networks protocol analyzer, and network analyzer.

Capturing packets in wiresharks

→ Select one or more networks, go to menu bar, then select capture.

→ In the wireshark capture Interface window, select start.

→ Select File > Save As or choose an export option to record the capture.

→ To stop capturing press Ctrl + E.

Wireshark Filters

→ Capture filters instruct wireshark to only record packets that meet specific criteria.

→ To use one of the existing filters, enter its name in the apply a display filter entry field located below the wireshark toolbar.

View and Analyze the packets

captured data interface contains three main sections;
1) The packet list panel (the top section)
2) The packet details panel (middle section)
3) The packet bytes pane (bottom section)

Packet list pane shows all packets found in active capture file. Each packet has its own row and a corresponding number assigned to it. Each packet contain
- → Timestamp
- → Source IP
- → Destination IP
- → Protocol
- → Length

The details pane, presents protocol and protocol fields of the selected packet in a collapsible format, which can be expanded on click.

Packets byte pane is present at the bottom of the bytes pane, which displays the raw data of the selected packet in hexadecimal bytes.
Selecting a specific position of this data automatically highlights its corresponding section in the packet details and vice versa.
Any bytes that cannot be printed are represented by a period.