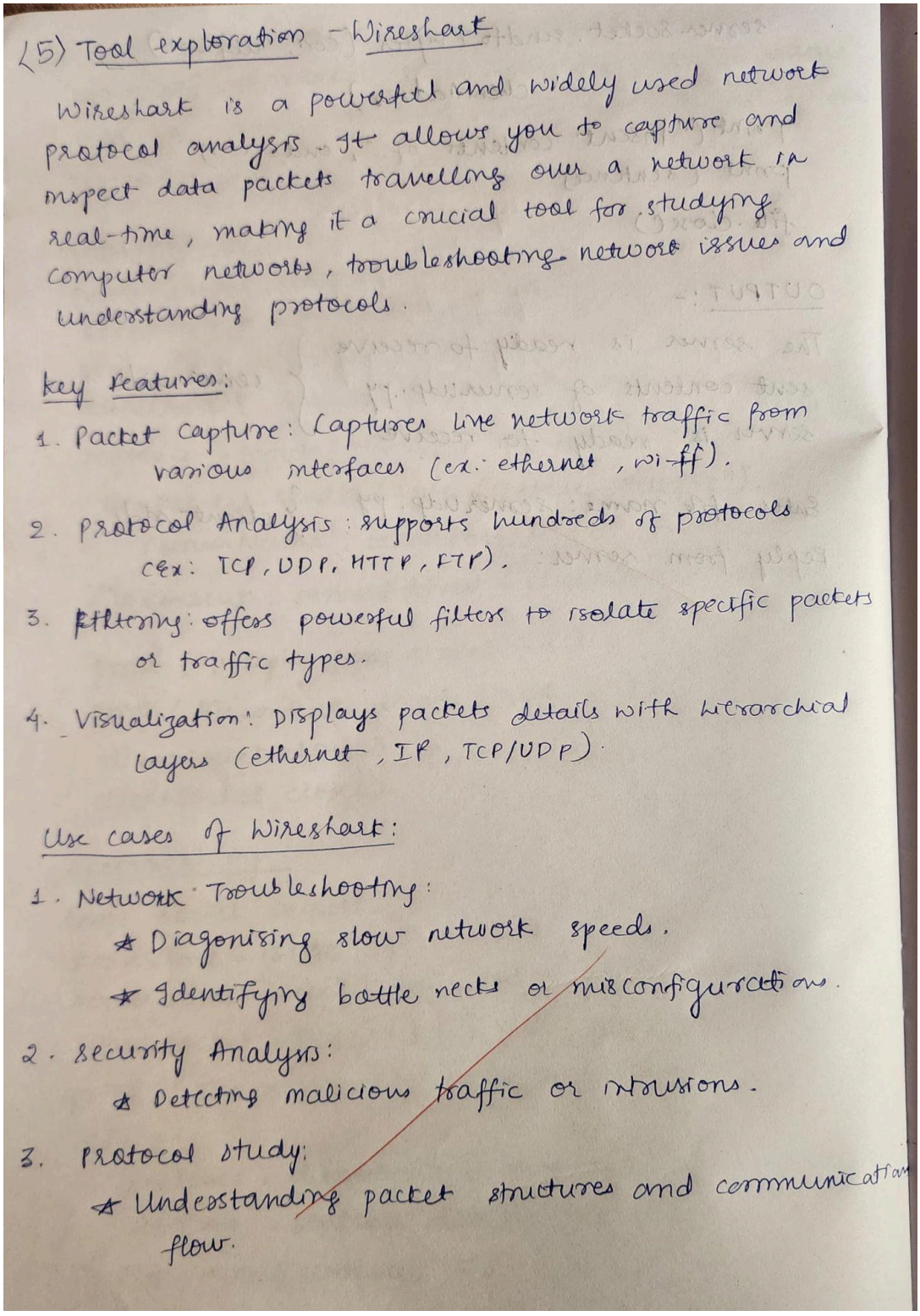
3/1/25

Tool exploration - Wireshark:



(5) Tool exploration - Wireshark

Wireshark is a powerful and widely used network protocol analysis. It allows you to capture and inspect data packets travelling over a network in real-time, making it a crucial tool for studying computer networks, troubleshooting network issues and understanding protocols.

Key features:

1. Packet capture: Captures live network traffic from various interfaces (ex: ethernet, wi-ff).
2. Protocol Analysis: supports hundreds of protocols (ex: TCP, UDP, HTTP, FTP).
3. Filtering: offers powerful filters to isolate specific packets or traffic types.
4. Visualization: Displays packets details with hierarchial layers (ethernet, IP, TCP/UDP).

Use cases of Wireshark:

1. Network Troubleshooting:
   - ★ Diagonising slow network speeds.
   - ★ Identifying bottle necks or misconfigurations.
2. Security Analysis:
   - ★ Detecting malicious traffic or intrusions.
3. Protocol study:
   - ★ Understanding packet structures and communication flow.

Common Fitness:

* http : show only HTTP traffic.
* tcp.port == 80 : Show traffic on TCP port 80
* ip.addr == 192.168.1.1: Show packets to or from a specific IP address.
* udp : show only UDP traffic.