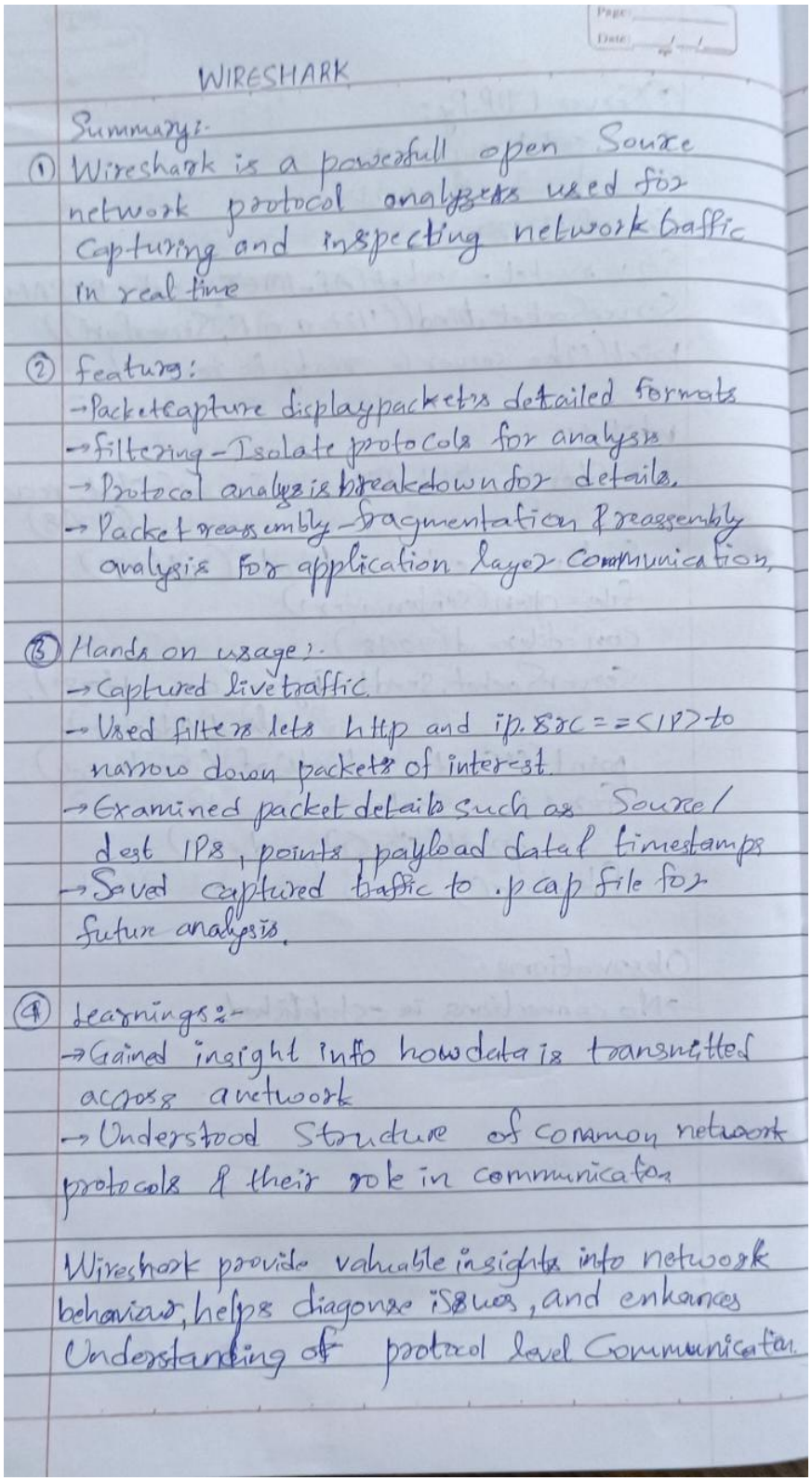
Wireshark



WIRESHARK

Summary:-

① Wireshark is a powerfull open Source network protocol analyzers used for capturing and inspecting network traffic in real time

② Features:
→ Packetcapture displaypackets detailed formats
→ filtering - Isolate protocols for analysis
→ Protocal analysis breakdown for details.
→ Packet reassembly - fragmentation & reassembly analysis for application layer communication,

③ Hands on usage:-
→ Captured live traffic
→ Used filters lets http and ip.src == <IP> to narrow down packets of interest
→ Examined packet details such as Source/ dest IPs, points, payload data & timestamps
→ Saved captured traffic to .pcap file for future analysis.

④ Learnings:-
→ Gained insight into how data is transmitted across a network
→ Understood Structure of common network protocols & their role in communication

Wireshark provide valuable insights into network behaviour, helps diagonse issues, and enhances Understanding of protocol level Communication.