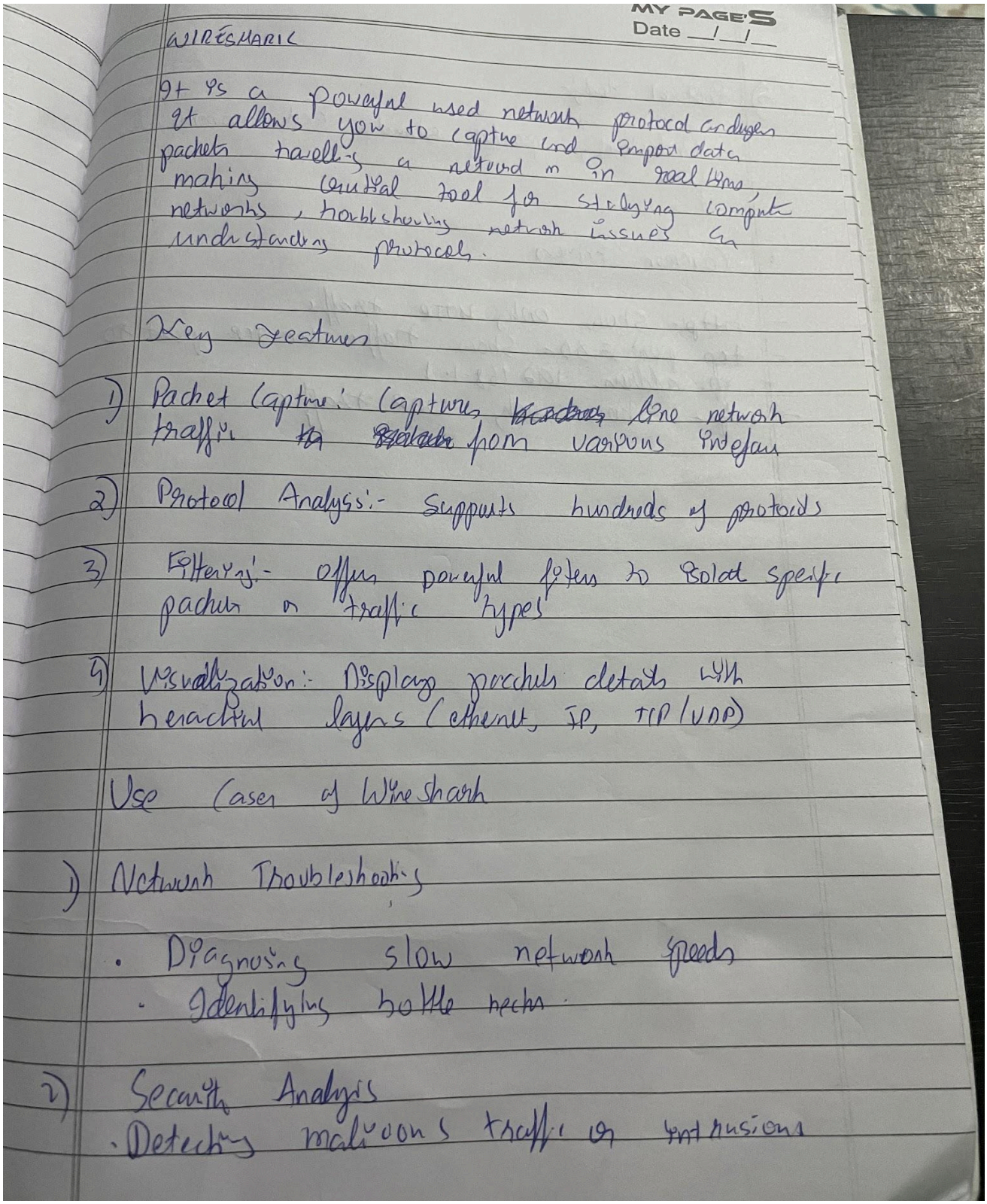
18. WIRESHARK



WIRESHARK

It is a powerful used network protocol analyzer. It allows you to capture and interact data packets travelling in a network in real time, making crucial tool for studying computer networks, troubleshooting network issues & understanding protocols.

Key features

1) Packet Capture: Captures live network traffic from various interfaces.
2) Protocol Analysis:- Supports hundreds of protocols
3) Filtering:- offers powerful filters to isolate specific packets or traffic types
4) Visualization: Displays packets details with hierarchical layers (ethernet, IP, TCP/UDP)

Use Cases of Wireshark

1) Network Troubleshooting
   - Diagnosing slow network speeds
   - Identifying bottlenecks
2) Security Analysis
   - Detecting malicious traffic or intrusions

3) Protocol Study:

- Understanding packet structure and communication flow

1. Common Filters

- http - Show only HTTP traffic
- tcp port == 80 - Show traffic on TCP port 80
- ip.addr == 192.168.1.1
- udp - Show only UDP traffic.