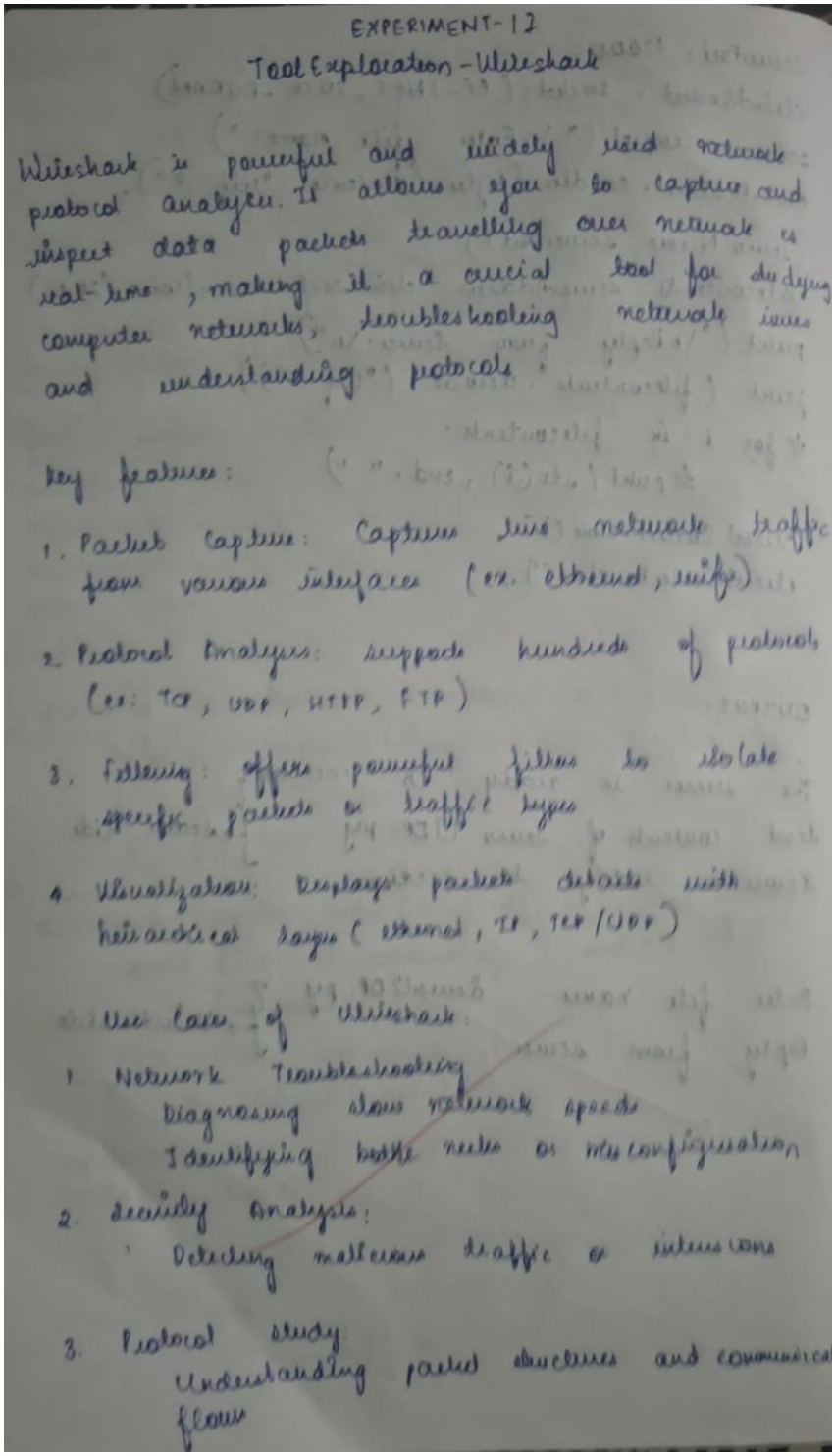
**Program 5:**

**Tool Exploration –Wireshark**



EXPERIMENT-12

Tool Exploration - Wireshark

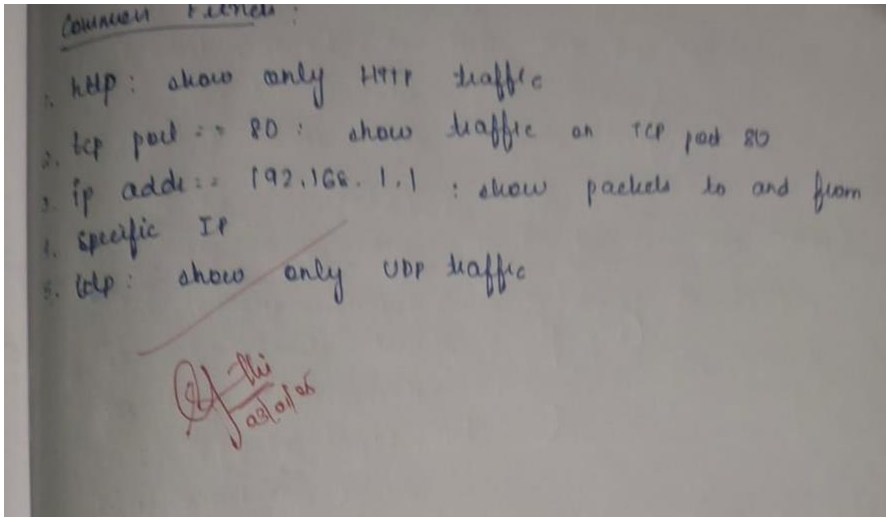
Wireshark is powerful and widely used network protocol analyzer. It allows you to capture and inspect data packets travelling over network in real-time, making it a crucial tool for studying computer networks, troubleshooting network issues and understanding protocols.

key features:

1. Packet Capture: Captures live network traffic from various interfaces (ex. ethernet, wifi)
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 packet details with hierarchical layers (ethernet, IP, TCP/UDP)

Use Cases of Wireshark

1. Network Troubleshooting
   Diagnosing slow network speeds
   Identifying bottlenecks or misconfigurations
2. Security Analysis:
   Detecting malicious traffic or intrusions
3. Protocol study
   Understanding packet structures and communication flows

Common Packets :

1. http : show only HTTP traffic
2. tcp port == 80 : show traffic on TCP port 80
3. ip addr == 192.168.1.1 : show packets to and from specific IP
4. udp : show only UDP traffic