17 Tool Exploration - Wireshark

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

Key Features:

1. Packet Capture: Captures live network traffic from various interfaces (ex: ethernet, wi-fi)

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:
   * Diagnosing 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