XPERIMENT-17 - WIRESHARK

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

ey features :

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

2) Protocol Analysis : Support hundreds of protocols (Ex: TCP, UDP, HTTP, FTP)

) Filtering : Offers powerful filters to isolate specific packets or traffic types.

4) Visualisation : Displays packet details with hierarchical layers (ethernet, IP, TCP/UDP)

Use cases of Wireshark

1) Network Troubleshooting :
 - * Diagnosing slow network speeds
 - * Identifying bottle necks and misconfigurations

2) Security analysis :
 - * Detecting malicious traffic or intrusions

3) Protocol Study :
 - * Understanding packet structures and communication flow.

Common filters :
 - * http : show only http traffic
 - * udp : show only UDP traffic
 - * tcp.port == 80 : show traffic on TCP port 8