Wireshark Network Analysis and Troubleshooting

# Project Overview

This project demonstrates the use of Wireshark, a powerful network protocol analyzer, to inspect live traffic, identify issues, and understand how protocols work.

# Key Features Used

- Live packet capturing (Ethernet/Wi-Fi)  
- Protocol filtering (e.g., HTTP, IP, TCP)  
- Packet inspection (headers, payloads)  
- Stream reassembly (TCP sessions)  
- Offline `.pcap` file analysis  
- Statistics and protocol hierarchy tools

# Use Cases Demonstrated

- Basic web browsing capture (HTTP filter)  
- IP-based filtering to monitor specific devices  
- TCP handshake observation  
- Identifying unencrypted data in packets

# Files Included

- Wireshark\_Project\_Report.docx — Full written report with analysis  
- capture.pcap \*(optional, add only if <25MB)\*  
- screenshots/ folder \*(if screenshots are used)\*

# Conclusion

Wireshark is a vital tool for network troubleshooting, protocol learning, and security analysis. This project offers hands-on experience in analyzing real-time traffic and applying it in cybersecurity contexts.  
  
For educational and learning purposes only.