

Title: Network Traffic Analysis Using Wireshark

Objective:

To capture and analyze network traffic using Wireshark.

Tool Used:

Wireshark

Procedure:

1. Installed Wireshark
2. Captured live network traffic
3. Generated traffic by visiting websites
4. Applied protocol filters
5. Analyzed DNS, TCP, HTTP, and HTTPS traffic

Observations:

- DNS queries showed domain name resolutions
- TCP three-way handshake was observed
- HTTP traffic was in plain text
- HTTPS traffic was encrypted
- DNS traffic used UDP protocol

Identify plain-text vs encrypted traffic

Type	Observation
HTTP	Can read URLs, data
HTTPS	Data unreadable
DNS	Domain names visible
TLS	Encrypted

Conclusion:

This task helped understand how network traffic flows and how Wireshark can be used for basic cyber-security analysis.