.

Network Packet Capture & Analysis Report

Objective:

Capture live network packets and identify basic protocols and traffic types using Wireshark.

Tools Used:

* Wireshark (free, open-source network protocol analyzer)

Procedure:

1. Installed Wireshark.

2. Started capturing traffic on the active network interface.

3. Generated traffic by browsing a website and pinging a server.

4. Stopped the capture after one minute.

5. Applied protocol filters (HTTP, DNS, TCP).

6. Identified multiple protocols in the capture.

7. Exported the capture as a `.pcap` file.

Protocols Identified:

* **HTTP:** Used for web browsing traffic.

* **DNS:** Used for resolving domain names to IP addresses.

* **TCP:** Transport protocol ensuring reliable data delivery.

Findings:

* The capture contained a mix of web browsing, DNS queries, and TCP session establishment.

* Multiple IP addresses were contacted, indicating connections to various servers.

* DNS queries confirmed name resolution before HTTP requests.