**Task 5: Capture and Analyze Network Traffic Using Wireshark**

**Objective**: Capture live network packets and identify basic protocols and traffic types.

**Tools**: Wireshark (free).

1. **Captured packets using Wireshark**

A screenshot of a computer

AI-generated content may be incorrect.

2. **Ping to my Local campus Server**

A computer screen shot of a black screen

AI-generated content may be incorrect.

3. **Filter captured packets by protocol (e.g., HTTP, DNS, TCP)**

***-http***

A screenshot of a computer

AI-generated content may be incorrect.

***-DNS***

***A screenshot of a computer

AI-generated content may be incorrect.***

***-TCP***

***A screenshot of a computer

AI-generated content may be incorrect.***

**4. Other Protocols**

A screenshot of a computer

AI-generated content may be incorrect.

***-ICMP***

*A screenshot of a computer

AI-generated content may be incorrect.*

***-SMB (Server Message Block)***

***A screenshot of a computer

AI-generated content may be incorrect.***

***-UDP***

***A screenshot of a computer

AI-generated content may be incorrect.***

**5. Summary of Findings (from your capture file)**

During packet capture and analysis with Wireshark, the following protocols were identified:

1. **DNS (Domain Name System):**
   * Found several **DNS queries and responses**.
   * Example: My system queried a DNS server to resolve a domain name (e.g., google.com) into an IP address.
   * Transport: **UDP** packets on port **53**.
2. **TCP (Transmission Control Protocol):**
   * Observed **TCP 3-way handshake** (SYN, SYN-ACK, ACK) before data transfer.
   * TCP segments carried higher-level protocols like HTTP and SMB.
   * Ports observed: **80 (HTTP)**, **445 (SMB)**.
3. **HTTP (Hypertext Transfer Protocol):**
   * Captured **HTTP GET and response packets** when browsing a website.
   * Example: A request to fetch a webpage was visible.
4. **UDP (User Datagram Protocol):**
   * Used for lightweight, connectionless communication.
   * Found in **DNS queries** and other background services.
5. **SMB (Server Message Block):**
   * Detected **file-sharing traffic** on port **445**.
   * Indicates local or background Windows network services.
6. **ICMP (Internet Control Message Protocol):**
   * Observed **echo request and echo reply** packets (ping).
   * Example: My system sent ICMP requests to test connectivity and got replies.

**6. Packet Details (Examples from Capture)**

* **DNS:** Query from client → server 8.8.8.8, response with IP address.
* **TCP Handshake:** Source port 51520 → Destination port 80, packets with flags SYN, SYN-ACK, ACK.
* **HTTP:** GET /index.html request observed, followed by server response.
* **ICMP:** Echo request (Type 8) and echo reply (Type 0) between my system and external host.
* **SMB:** Traffic on TCP port 445 showing protocol negotiation packets.