# Task 5: Network Traffic Analysis using Wireshark

Submitted by: Satwik Adapa

Cybersecurity Intern, Pragati Engineering College

Email: asatwik34@gmail.com

## Objective

To capture live network packets using Wireshark and identify at least three different protocols and traffic types.

## Tools Used

• Wireshark (Free and open-source network protocol analyzer)

## Steps Performed

1. Installed and launched Wireshark.  
2. Selected the active network interface.  
3. Began packet capture while browsing websites and pinging servers.  
4. Stopped the capture after around one minute.  
5. Applied filters to isolate specific protocol types (TCP, DNS, HTTP).  
6. Saved the capture as a .pcap file.

## Protocols Identified

1. TCP - Transmission Control Protocol

- Reliable, connection-oriented protocol used for data transmission.

2. DNS - Domain Name System

- Used to translate domain names to IP addresses.

3. HTTP - HyperText Transfer Protocol

- Protocol used for web communication over port 80.

## Outcome

Successfully captured and analyzed network traffic using Wireshark, gaining hands-on experience with packet filtering and protocol inspection.

## Note

The file 'capture\_sample.pcap' is a placeholder and should be replaced with an actual capture file obtained during the hands-on task.

**SatwikAdapa**