# Network Packet Capture Report

## Objective

The objective of this task is to use Wireshark to capture live network packets, analyze them to identify basic protocols, and summarize the traffic observed during the capture.

## Tools Used

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

## Procedure

1. Installed Wireshark on the system.
2. Started capturing packets on the active network interface.
3. Generated network traffic by browsing a website and/or pinging a server.
4. Stopped the capture after approximately one minute.
5. Applied protocol filters in Wireshark (e.g., HTTP, DNS, TCP) to view specific types of traffic.
6. Identified at least three different protocols present in the captured traffic.
7. Exported the capture as a .pcap file for submission.
8. Summarized findings including identified protocols and packet details.

## Observations

During the packet capture session, multiple protocols were observed in the network traffic. These included Transmission Control Protocol (TCP), Domain Name System (DNS), User Datagram Protocol (UDP), File Transfer Protocol (FTP), Address Resolution Protocol (ARP), and Transport Layer Security (TLS).

### Packet Details by Protocol

|  |  |  |  |
| --- | --- | --- | --- |
| Protocol | Packet Count | Percent of Total Packets | Total Bytes |
| Domain Name System (DNS) | 12 packets | 8.6% | 787 bytes |
| Transmission Control Protocol (TCP) | 95 packets | 68.3% | 1972 bytes |
| User Datagram Protocol (UDP) | 27 packets | 19.4% | 216 bytes |
| File Transfer Protocol (FTP) | 10 packets | 7.2% | 581 bytes |
| Address Resolution Protocol (ARP) | 14 packets | 10.1% | 392 bytes |
| Transport Layer Security (TLS) | 25 packets | 18.0% | 9625 bytes |

## Summary

The capture demonstrated the presence of various protocols in normal network activity. TCP formed the majority of traffic, indicating connections for web browsing and secure communication. DNS traffic showed domain name resolution requests, and UDP was used for lightweight, connectionless transmissions. Additional protocols like FTP, ARP, and TLS were also observed, representing file transfers, local network communication, and encrypted sessions, respectively. The .pcap file contains the full details for further analysis.