# Task 3: Networking Basics for Cyber Security – Detailed Explanation

### Introduction

This document explains networking fundamentals through hands-on packet analysis using Wireshark. The objective is to understand how data moves across networks and how protocols operate.

### Packet Sniffing

Packet sniffing is the process of capturing and analyzing network packets to understand communication between systems. Wireshark allows visibility into live traffic.

### TCP Three-Way Handshake

TCP establishes connections using SYN, SYN-ACK, and ACK packets. Observing this handshake helps understand reliable communication.

### DNS Analysis

DNS translates domain names into IP addresses. Capturing DNS queries shows how systems locate servers.

### HTTP vs HTTPS

HTTP traffic is transmitted in plain text, making it vulnerable to interception. HTTPS encrypts data, providing confidentiality and integrity.

### Conclusion

Analyzing network traffic builds foundational skills for cybersecurity, helping identify normal and suspicious communication patterns.