CYBR 2200 Network Analysis
Lewis Joseph Feik
Week 1 Lab Worksheet

Wireshark Setup and Network Security Monitoring Foundations

Purpose

This lab introduces you to professional network traffic analysis practices. You will configure Wireshark for analysis, open the provided packet capture file, review basic packet information, and learn foundational Network Security Monitoring concepts. This is an orientation lab. You are not expected to analyze malicious traffic.

Part A Wireshark Environment Setup

1 I opened Wireshark.
2 I adjusted the display settings to make traffic easier to read by increasing the font size to 16 and increasing the row height so each packet row was clearly visible.
3 I confirmed Wireshark was set to use UTC time for packet timestamps.

Part B Open the Provided PCAP File

1 I downloaded the packet capture file from Blackboard for Week 1.
2 In Wireshark I selected File then Open and loaded the PCAP file.
3 I confirmed packets appeared in the Packet List pane.

Part C Packet Familiarization

Packet number selected 15
Source IP address 192.168.1.25
Destination IP address 142.250.72.174
Protocol TCP
Source port 51544
Destination port 443

Part D Network Security Monitoring Concepts

1 What is Network Security Monitoring NSM
Network Security Monitoring is the process of collecting and reviewing network traffic so you can understand normal activity and quickly detect suspicious behavior or potential security issues.

2 Why is full packet capture valuable for security analysis
Full packet capture is valuable because it records the complete contents of network communications. This makes it easier to investigate incidents, confirm exactly what happened, and recreate sessions when you need the most detailed evidence.

Part E Ethical and Legal Considerations

Packet capture can include private information such as logins messages and files. Capturing or inspecting traffic on a network without permission can violate privacy rules policies and laws. You should only perform traffic analysis when you own the network or have clear written authorization so everyone understands what is being collected and why. This protects users data and also protects you from serious legal and academic consequences.