CS 3516 - Computer Networks

Project 0 (20 points)
Assigned: Tuesday, March 12, 2024
Checkpoint: Not Required
Due: Tuesday, March 19, 2024 at 11:59pm

Project 0: Wireshark

In this solo project, you will use Wireshark, a tool to capture network packets. Wireshark can be used to capture network activity directly from your network interface card and display it or write it to a file. Wireshark can also read prior activity from a file, allowing post-hoc forensic analysis. To complete this assignment, you must download and install Wireshark. You may do this on your own machine or in a virtual machine environment. If you do not have a machine in which you can use Wireshark, contact the teaching staff immediately.

In this project, we will be reading from a pre-recorded session. The SMTP session file available at `https://web.cs.wpi.edu/~staneja/cs3516/wireshark_smtp.pcap` is an example packet capture from the Wireshark Web site. We will **NOT** be using Wireshark to "capture" packets from the network interface. Performing a packet capture in promiscuous mode can collect traffic from other users, which is a violation of the WPI network acceptable use policy (AUP) and can easily be detected by the network operations staff.

Your assignment is to open the SMTP packet capture file, analyze it with Wireshark, and answer the following questions. Some textbook authors have created an assignment (available at `https://web.cs.wpi.edu/~staneja/cs3516/wireshark_guide_intro.pdf`) using Wireshark that may provide useful background on the tool. However, you do not need to complete the walkthrough in that document. Instead, answer the following about the smtp.pcap file:

1. How many packets are in the capture?
2. How long in seconds did the capture last?
3. The capture is an email message. What is the mail sender's email address?
4. The email contains a data portion. What does it look like the sender is transmitting?
5. There are several types of protocols in the Protocols column. What are the protocols?

Checkpoint Contributions

This project does not have a checkpoint.

Deliverables and Grading

Students should use the following checklist in turning in their projects to avoid forgetting any deliverables:

1. Submit your answers as a plain-text file, `README`, via InstructAssist (URL: `https://ia.wpi.edu/cs3516/files.php`).