CIT 485/585 Network Investigation

For this assignment, analyze the Nitroba University Harrassment Scenario, identify the person instigating the harrassment, and write a report detailing the evidence for your case.

1 Student Learning Outcomes

1. Apply your network forensics knowledge to identify the culprit in a case study.
2. Write a report that provides the supporting analysis to prove your case.

2 Analysis

Your analysis process should follow the general procedure below.

1. Map out the Nitroba dorm room network.
2. Find who sent email to *lilytuckrige@yahoo.com*.
   - Look for a TCP flow that includes the hostile message
   - Find information that can tie that message to a particular web browser.
3. Identify the other TCP connections that below to the attacker
4. Find information in one of those TCP connections that IDs the attacker.

3 Data

The scenario description and a `pcap` containing the relevant network data is available at `https://digitalcorpora.org/corpora/scenarios/nitroba-university-harassment-scenario`. The `pcap` data can be converted to network flow data if the student finds that useful.

The teacher of the class is Lily Tuckrige. The students in the class are

- Amy Smith
- Burt Greedom
- Tuck Gorge
- Ava Book
- Johnny Coach
- Jeremy Ledvkin
- Nancy Colburne
- Tamara Perkins
- Esther Pringle

- Asar Misrad
- Jenny Kant

4 Deliverables

This assignment is due at the beginning of class on Wednesday, May 1.

The investigation report must be at least 4 single spaced pages long. Tables showing evidence can be used if desired. The report consist of 3 sections. It must begin with an introductory paragraph describing the scenario and the goals of the investigation: to identify the culprit in the Nitroba harrassment case. The next section should describe the investigation process, with the final section providing your conclusion, identifying the harrasser and showing the evidence proving your identity.

The conclusion must provide multiple sources of evidence identifying the harrasser. It is not sufficient to just identify the harrasser with a single TCP flow. The conclusion must also contain a table of students from the CHEM 109 class whose first or last names are found in at least one network packet. The table should provide the student name and a description of network activities associated with that student.

Your conclusion should provide answers the following questions:

1. **Who:** who are the person sending the harrassing e-mails. Identify the person by first and last name, e-mail address, IP address, and web browser.
2. **When:** when did the harrassing communication occur. Wireshark provides times as seconds from the start of the capture by default. You want to report times as 24-hour timestamps in Coordinated Universal Time (UTC).
3. **What:** what happened on the network during this capture. How did the harrasser send the e-mail and attempt to obfuscate his or her identity.

E-mail the report as a `docx` format document via e-mail to the instructor. The name of the attachment must be `a3-LASTNAME-FIRSTNAME.docx` with appropriate substitutions to put your name into the filename. The e-mail must be from your NKU address and have a subject line of "CIT 485 Assignment 3."