Program Submission Instructions:

- You must submit one zip file or tarball in Webcourses
- Acceptable formats for compressed file: .zip, .tar, .gz, .bz
- You must name your compressed file as: your_last_name_your_first_name_Bonus
- Acceptable file formats for report: .doc, .docx, .pdf
- Your zip file must contain the capture files and the report that is described in the "Submission" section below.

CIS 3360 – Security in Computing
Summer 2020
Homework Assignment: Analyzing Packets with Wireshark

Wireshark is an open source network packet/protocol analyzer. A network packet analyzer captures network packets and tries to display that packet data as detailed as possible. Wireshark is perhaps one of the best open source packet analyzers available today for UNIX and Windows. Wireshark isn't an intrusion detection system. Wireshark will not manipulate data on the network.

Legitimate Uses of Wireshark:

- Network administrators use it to troubleshoot network problems
- Network security engineers use it to examine security problems
- Developers use it to debug protocol implementations
- People use it to learn network protocol internals

Resources:

1) The wireshark main page: http://www.wireshark.org
2) http://wiki.wireshark.org
3) http://wiki.wireshark.org/SampleCaptures
4) http://www.wireshark.org/download/docs/user-guide-us.pdf

Assignment Part I

1. Watch the "Introduction to Wireshark" video that you will find in the videos section on the Wireshark main page.

Assignment Part II

1. Download and install Wireshark (Windows, Mac, or Linux) from http://www.wireshark.org/
   This was tested with Version 2.6.8 (v2.6.8-0-gbede2087)
2. Capture data from an interface in your computer (e.g., Ethernet or WiFi) *(10 points)*
   - Remember to set the encryption if required
   - Store the captured data
3. Store the captured data in a file named **captured_LastName_FirstName** *(3x10 points)*
   - Break the captured files each 10 seconds and record during 30 seconds (you should end up with 3 files, each with the name above plus timestamp information)
   - **Make sure all name resolution options are unchecked.**

Assignment Part III

1. Load the **BonusAssignment-A.pcapng.gz** file into Wireshark
2. What are the two IP addresses of the computers in the HTTP session? *(10 points)*
3. Use Wireshark's data window to examine the XML data
   - Using the Go menu, go to packet 520
   - Use the HTTP view to examine the captured XML data in the packet
4. Answer the following questions:
   - What is Dish DSS25 tracking? *(10 points)*
   - What is the antenna's azimuth angle? *(10 points)*
   - What is the antenna's elevation angle? *(10 points)*
   - What is the antenna's wind speed? *(10 points)*
   - What is the downsignal power? *(10 points)*

Submission

- You must submit a zip file with your 3 captured files and a report document containing the following:
  - Your name - please make sure your name is on every page submitted.
  - A description of what features of Wireshark you tried, including part II and part III, and your observations and impressions of the tool.
  - A screenshot with your capturing settings (part II)
  - The name of your computer's network interface that you used for captures (part II)
  - The two IP addresses on (part III)
  - The answers to the questions derived from data in Packet 520 below (part III)
    - What is Dish DSS25 tracking?
    - What is the antenna's azimuth angle?
    - What is the antenna's elevation angle?
    - What is the antenna's wind speed?
    - What is the downsignal power?