Name: Alexander Chatron-Michaud
Student Number: 260611509
COMP 307 Fall 2016
Mini Assignment 1

1. Identify the exact location where you were when recording your two wifi packet recording sessions.
    - Trottier Building
    - Tim Hortons on University/Sherbrooke

2. Look at each session individually and report the quality of the security. Specifically, based on your data set, what percentage of packets revealed packet header information, and what percentage of packets revealed payload information. Write a short evaluation.
    - Trottier: Header information was available for a majority of the packets observed during the 2 minutes (>90%). Information on the source and destination IP addresses were available for almost all packets. As for payload information, about half of the packets' payload was actually encrypted and couldn't be read, but since there were a huge amount of broadcast packets it turns out that only about 2-3% of the packets overall had readable payload info
    - Tim Hortons: Header information here was similarly available for almost all of the packets observed. Interestingly, about 33% of the packets had 8.8.8.8 as the destination IP (Google DNS). Here, almost none (<2%) of the packets were marked as having encrypted payloads and more information could be retrieved from the display of the payload, totaling about 50% of the packets having readable payload information.

3. Looking at each session individually, select a sender IP address and try to deduce what they were trying to do.
    - In Trottier I was able to find one user who had a bunch of packets whose payloads were connected to iTunes. After looking up some of the information in the payload display below I was able to figure out that they were streaming Apple Music.
    - In Tim Hortons I was able to find some of the URLs that a user was exploring, it seems as though they were looking up a tutorial in the documentation of an API's docs website (spotted another programmer!)

4. Now, comparing your two data sets. Which location was more secure? Could you identify the default security that was present at each data set?
    - Judging just from the information I was able to retrieve from these tests, I would say that the internet at Trottier was more secure. This is because I was able to get a lot less information out of the payload information and a much bigger number of them were encrypted. It looks like in Trottier there is some kind of payload based encryption for some of the packets (not all of them were encrypted) whereas in Tim Hortons didn't have payload encryption at all. In both places, HTTPS would have been secure, however there was no indication of entire packet encryption in Trottier given that we could still get some info.