**Packet Captures:** In this folder are packet captures taken from real IoT devices via WireShark. WireShark works by using your computers Wi-Fi or ethernet adapter to read traffic going on around you. This is a very powerful tool that can be used by hackers and security professionals alike because of its ability to expose security flaws. In previous challenges you have learned about encryption and how it can hide information from prying eyes. In an ideal world all traffic would be encrypted and WireShark would be mostly useless aside from some basic debugging use cases. However, this is far from the case in the real world and it is very common to find plain text traffic being sent out to anyone listening.

A hacker could take advantage of this by using WireShark to look for any key information that could be useful in their attack. It is important to take all plain text traffic seriously as although a piece of information may seem harmless it could potentially be the only thing a hacker needs in order to carry out an attack. Some common culprits of sending out sensitive information over plain text are IoT devices. These devices can sometimes drop security keys and even log in credentials all over plain text!

**Exercise:** It is your job to take a look at screenshots of some real packet captures and identify what is in plain text. You should also explain how this plain text output could be detrimental if a hacker were to find this using WireShark.