Pcap Analysis

Subtask 1

This assignment reviews the basics of pcap analysis. We will look at packet capture of an ancient chat protocol AIM. This chat protocol is interesting for educational purposes because it was completely unencrypted. The internet was a different place back when this was popular.

Download the pcap and open it in Wireshark. AIM had two ports 443, and 5190. If you go to preferences->Protocol->AIM and change the default port to 443, you will be able to read the AIM traffic.

What username do you see in the traffic?

You should produce a report that answers the following questions.

1. What username do you see in the traffic?