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. Check the traffic for 5190(port AIM used for file transfer). Follow the stream you discover. Change your view to hex and carve out the file that is being transfered. Past the data into a hex editor and save the file. What is the magic number of the file? What file type does this indicate? What was in the file?

You should produce a report that answers the following questions.

1. What was the magic number?
2. What file type did you obtain?
3. What was in the file?