## Wireshark Exercise – Part 2

**IMPORTANT NOTE:**
**For these next exercises you will need to first download these files from Brightspace (Lecture 4-Wireshark Files).**

**1.Telnet (Capture file located on Brightspace)**
Investigate the Telnet capture file.
You will need to download this file to your own PC first, then open Wireshark and then click open and select file.

**1.1** What is the significance of the first 3 packets of the capture? Tip: what's the purpose of this communication?
**1.2** Can you identify the username and password used to login? **HINT: Research how to use the follow TCP stream option in Wireshark.**
**1.3** What do they do when a user logs onto the server? What commands do they run?

**1.4 – FTP (Capture file located on Brightspace)**
Investigate the FTP capture file.
You will need to download this file to your own PC first, then open Wireshark and then click open and select file.
**1.5** Can you identify the username and password used to login? **HINT: Research how to use the follow TCP stream option in Wireshark.**

**1.6** What FTP commands are issued from the client to server?

**Exercise 2 – DHCP (Capture file located on Brightspace)**
Investigate the DHCP capture file. You may need to open Wireshark and then click open and select file.
**2.1** What is the meaning of DORA?
**2.2** What IP address / subnet mask did the machine receive.
**2.3** What was the lease time?

**Exercise 3 – SMTP (Capture file located on Brightspace)**
3.1 Open the SMTP trace. Can you read the email message?

**More information - [https://wiki.wireshark.org/SMTP](https://wiki.wireshark.org/SMTP)**