# Objective:

* Analyzing the **FTP** packets using Wireshark

**Lab Statement 1: Capturing FTP packets using Wireshark (10)**

**Step 1**: **Start a Wireshark capture*. (JUST FOR UNDERSTANDING)***

**a.** Close all unnecessary network traffic, such as the web browser, to limit the amount traffic during the Wireshark capture.

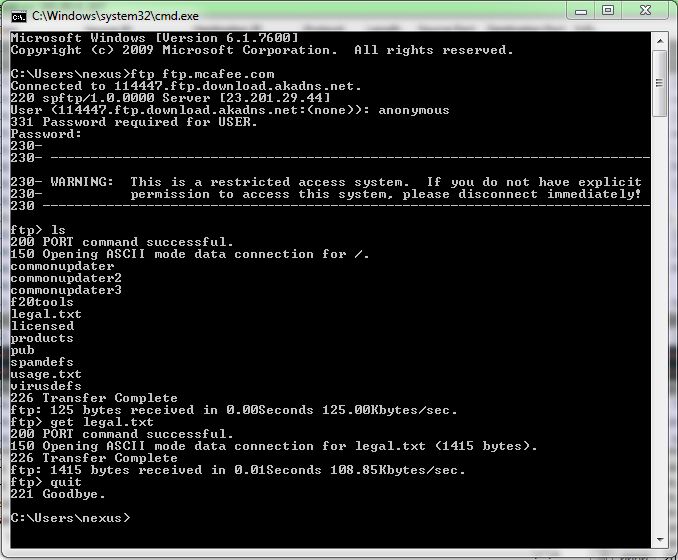
**b.** Start the Wireshark capture.

**Step 2: Download the .txt file. *(JUST FOR UNDERSTANDING)***

**a.** From the command prompt, enter ftp [ftp.mcafee.com](ftp://ftp.mcafee.com)

**b.** Log into the FTP site for mcafee.com with user **anonymous** and no password.

**c.** Locate and download any .txt file.



**Step 3: Stop the Wireshark capture.**

**Step 4: View the Wireshark Main Window**

Wireshark captured many packets during the FTP session to [ftp.mcafee.com](ftp://ftp.mcafee.com). To limit the amount of data for analysis, type **tcp and ip.addr == 195.89.6.167** in the Filter. The IP address, **195.89.6.167**, is the address for [ftp.mcafee.com](ftp://ftp.mcafee.com).

**Step 5: Analyze the packets**

Carefully analyze the packets in Wireshark windows and answer the following question:

**Use the FTP\_Session.pcapng (Wireshark Capture File) to answer the questions below**

1. FTP uses two port numbers: 20 and 21. Apply **tcp.port==20** and **tcp.port==21**. Analyze the result and write down the purposes of these two ports for FTP.
2. Filter out each packet using either FTP or FTP-DATA Protocol (using **ftp || ftp-data** filter). Mention each packet number and its purpose with reference to request made and response received in the above mentioned FTP Session in command line to get file legal.txt (screenshot show above). Also look for **Response Code** and **Response Arg** in the FTP Header for each packet

**(**There are **19 such packets** and you have to write one/two lines explanation for each packet, what the packet is doing w.r.t FTP Session (Screenshot shown above) **e.g., Packet 104: Client asks server to send the data on IP:192.168.1.2 and Port:16341** [63(0x3F),213(0xD5) and **(0x3FD5=16341**)**] )**