

CSCI 4220 Lab 5

Lab 5: FTP Wireshark Trace

This lab is heavily adapted from Bill Buchanan [here](#), but we're only focusing on FTP. You can find the zip file under Course Materials on Submittity (Lab5_ftp2.zip), which contains a single capture file to open in Wireshark. You may want to consult Internet sources including the RFC to fill in any knowledge gaps.

Part 1, answer the following questions:

1. Using the filter of `ftp.command`, determine the FTP commands that the user has used:
2. Using the filter of `ftp.response`, determine the FTP codes that have been returned:
3. What is the username and password for the access to the FTP server:
4. What is the name of the file which is uploaded:
5. What is the name of the file which is downloaded:
6. Using the filter of `ftp.request.command=="LIST"`, determine the first packet number which performs a "LIST":
7. In performing in the list of the files on the FTP server, which TCP port is used on the server for the transfer:
8. From the final "LIST" command, which are the files on the server?
9. What does the filter `ftp.response.code==227` identify in terms of the ports that are used for the transfer:

Next open a terminal. For all instructions, you may need to type `?` and press enter to see a list of commands in your FTP client. You should be using a command-line FTP client for this lab.

Mac users may find [this guide](#) useful since you will need to use one of these methods to get a command line FTP client (usually in the `inetutils` package).

1. Inside it, run `ftp ftp.cdc.gov`. Log in with `anonymous` as your username, and anything as a password.
2. Get a list of what's in the current working directory (this will probably be `ls`). If the server never responds, your computer's firewall is probably blocking the connection. You can work around this by setting your FTP client to passive mode (probably by using `passive`). This is not the same as the `PASV` FTP instruction, but tells the client/server to treat all data in a similar manner to how `PASV` works.
3. Navigate to the `pub/FOIAREQ` directory. (probably involves one or more `cd` commands)
4. Download `085226-A45.pdf` in ASCII mode as `085226-A45-ascii.pdf` (this is usually the default transfer mode) (probably `ascii` and `get` commands)
5. Download `085226-A45.pdf` in binary mode as `085226-A45-bin.pdf` (probably `binary` command)
6. Quit/log off from the server (the server will eventually disconnect you after enough inactivity, but it's polite to quit when we're done. Probably the `bye` command.)
7. Open both downloaded PDF files in a PDF viewer and compare. If they're different, why are they different?

To get checked off answer the questions in Part 1, show the grader both versions of the PDF file as well as your terminal with FTP output, and explain why the two files are different (if they are).