Justin Chen

October 31, 2025

CSCI 4220 - Network Programming

Lab 7 Submission

1.

```
tshark -r Lab7/ftp2.pcap -Y "ftp.request.command" -T fields -e ftp.request.command | sort | uniq
```

The user used the following FTP commands:

```
CWD, FEAT, LIST, PASS, PASV, PWD, RETR, STOR, SYST, TYPE, USER
```

2.

```
tshark -r Lab7/ftp2.pcap -Y "ftp.response" -T fields -e ftp.response.code | sort | uniq
```

FTP codes returned:

```
125, 200, 211, 215, 220, 226, 227, 230, 250, 257, 331
```

3.

```
tshark -r Lab7/ftp2.pcap -Y "ftp.request.command == USER || ftp.request.command == PASS" -T fields -e ftp.request.command -e ftp.rec
```

```
USER Administrator
PASS napier
```

4.

```
tshark -r Lab7/ftp2.pcap -Y "ftp.request.command == STOR" -T fields -e ftp.request.arg
```

Uploaded file:

```
111.png
```

5.

```
tshark -r Lab7/ftp2.pcap -Y "ftp.request.command == RETR" -T fields -e ftp.request.arg
```

Downloaded file:

```
manual.txt
```

6.

```
tshark -r Lab7/ftp2.pcap -Y "ftp.request.command==LIST" -T fields -e frame.number
```

First packet number: 21

```
21, 126, 145
```

7.

```
tshark -r Lab7/ftp2.pcap -Y "ftp.response.code == 227" -T fields -e frame.number -e ftp.response.arg | head -n 1
```

```
Entering Passive Mode (192,168,47,134,4,54)
```

Port number is encoded in the last two numbers of the IP address. In this case, $p1=4$ and $p2=54$.

Port number is calculated as $p1*256 + p2 = 4*256 + 54 = 1078$.

8.

```
tshark -r Lab7/ftp2.pcap -Y "frame.number == 144" -T fields -e ftp.response.arg
```

```
Entering Passive Mode (192,168,47,134,4,57).
```

```
tshark -r Lab7/ftp2.pcap -Y "tcp.port == 1081" -T fields -e tcp.stream | head -n 1
```

```
5
```

```
tshark -r Lab7/ftp2.pcap -q -z "follow,tcp,ascii,5"
```

```
 Follow: tcp,ascii
Filter: tcp.stream eq 5
Node 0: 192.168.47.1:49449
Node 1: 192.168.47.134:1081
    98
03-11-13  11:25PM                   64 1.docx
03-11-13  10:35PM                  347 manual.txt
```

The files on the server are `1.docx` and `manual.txt`.

9. The response code `227` signifies that the server is entering passive mode. When a client wants to initiate a data transfer, it can use passive mode to send the `PASV` command. The server then responds with a `227` response. This response contains a n IP address and a port number that the server has opened for the client to connect to. The client then estabioishes a new TCP connection to that specifife port on the server to transfer the data.

The filter `ftp.response.code==227` identifies the packets where the server is telling the client which port it should connect to for a data trasnfer.

10.

```
ftp ftp.ncbi.nlm.nih.gov
Connected to ftp.wip.ncbi.nlm.nih.gov.
220-
 This warning banner provides privacy and security notices consistent with
 applicable federal laws, directives, and other federal guidance for accessing
 this Government system, which includes all devices/storage media attached to
 this system. This system is provided for Government-authorized use only.
 Unauthorized or improper use of this system is prohibited and may result in
 disciplinary action and/or civil and criminal penalties. At any time, and for
 any lawful Government purpose, the government may monitor, record, and audit
 your system usage and/or intercept, search and seize any communication or data
 transiting or stored on this system. Therefore, you have no reasonable
 expectation of privacy. Any communication or data transiting or stored on this
 system may be disclosed or used for any lawful Government purpose.
220 FTP Server ready.
Name (ftp.ncbi.nlm.nih.gov:ustin): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> passive
Passive mode on.
ftp> ls
227 Entering Passive Mode (130,14,250,11,196,225).
150 Opening BINARY mode data connection for file list
dr-xr-xr-x   4 ftp      anonymous     4096 Oct 31 02:48 1000genomes
-r--r--r--   1 ftp      anonymous 10738466816 May 13 21:18 10GB
-r--r--r--   1 ftp      anonymous 1074790400 May 13 21:18 1GB
lr--r--r--   1 ftp      anonymous       29 Mar 28  2025 asn1-converters -> toolbox/ncbi_tools/converters
dr-xr-xr-x  12 ftp      anonymous   188416 Feb  8  2022 bigwig
dr-xr-xr-x   5 ftp      anonymous     4096 Oct 31 09:19 bioproject
dr-xr-xr-x   2 ftp      anonymous     4096 Oct 31 15:40 biosample
```

```
dr-xr-xr-x   2 ftp      anonymous     4096 Oct 31 15:46 biosample
dr-xr-xr-x  13 ftp      anonymous     4096 Oct 31 02:48 blast
dr-xr-xr-x   3 ftp      anonymous     4096 May  3  2023 cgap
dr-xr-xr-x   4 ftp      anonymous     4096 May 17  2023 cn3d
dr-xr-xr-x   7 ftp      anonymous   122880 Oct 31 06:01 comparative-genome-viewer
dr-xr-xr-x  29 ftp      anonymous     4096 Oct 31 02:48 dbgap
dr-xr-xr-x   2 ftp      anonymous     4096 May  3  2023 diffexpIR-notebook
dr-xr-xr-x  12 ftp      anonymous     4096 May  3  2023 entrez
dr-xr-xr-x   7 ftp      anonymous     4096 Feb  8  2022 epigenomics
dr-xr-xr-x   4 ftp      anonymous     4096 Oct  5  2023 eqtl
dr-xr-xr-x   6 ftp      anonymous     4096 May  3  2023 fa2htgs
-r--r--r--   1 ftp      anonymous     3262 Mar 28  2025 favicon.ico
-r--r--r--   1 ftp      anonymous      106 Mar 28  2025 fufuter.html
dr-xr-xr-x  14 ftp      anonymous   806912 Oct 31 02:48 genbank
dr-xr-xr-x   6 ftp      anonymous     4096 Feb  8  2022 gene
dr-xr-xr-x  16 ftp      anonymous    49152 Oct 31 02:48 genomes
dr-xr-xr-x 1073741824 ftp      anonymous        0 Oct 30 05:03 geo
dr-xr-xr-x   4 ftp      anonymous     4096 Oct 31 02:48 giab
dr-xr-xr-x  25 ftp      anonymous     8192 May  3  2023 hapmap
dr-xr-xr-x  22 ftp      anonymous     4096 Aug  6 19:06 hmm
dr-xr-xr-x  15 ftp      anonymous     4096 Nov  6  2024 mmdb
dr-xr-xr-x   8 ftp      anonymous   258048 Oct 31 02:48 ncbi-asn1
dr-xr-xr-x   5 ftp      anonymous     8192 Apr 27  2023 nist-immsa
dr-xr-xr-x   3 ftp      anonymous    12288 Sep  1  2021 osiris
dr-xr-xr-x  10 ftp      anonymous     4096 Oct 31 02:48 pathogen
dr-xr-xr-x 176 ftp      anonymous    12288 Aug 21 16:49 pub
dr-xr-xr-x  27 ftp      anonymous     8192 Sep 30 13:42 pubchem
dr-xr-xr-x  45 ftp      anonymous     4096 Oct 21 04:49 pubmed
dr-xr-xr-x   4 ftp      anonymous     4096 Jun 16 21:45 rapt
-r--r--r--   1 ftp      anonymous     2136 Mar 28  2025 README.ftp
dr-xr-xr-x 1073741824 ftp      anonymous       40 Oct 15 00:54 ReferenceSamples
dr-xr-xr-x  22 ftp      anonymous     4096 Sep  5 18:29 refseq
dr-xr-xr-x  57 ftp      anonymous     4096 Feb  8  2022 repository
-r--r--r--   1 ftp      anonymous       26 Mar 28  2025 robots.txt
dr-xr-xr-x   8 ftp      anonymous     4096 Feb  8  2022 SampleData
dr-xr-xr-x   3 ftp      anonymous     4096 Oct 31 02:48 seqc
dr-xr-xr-x   3 ftp      anonymous     4096 May  3  2023 sequin
dr-xr-xr-x   4 ftp      anonymous     4096 May  3  2023 sky-cgh
dr-xr-xr-x  12 ftp      anonymous     4096 Oct 31 02:48 snp
dr-xr-xr-x  23 ftp      anonymous     4096 Oct 31 02:48 sra
dr-xr-xr-x   2 ftp      anonymous     4096 Jan 12  2024 tech-reports
dr-xr-xr-x  11 ftp      anonymous     4096 Mar 25  2025 toolbox
dr-xr-xr-x   8 ftp      anonymous     4096 May  3  2023 tpa
dr-xr-xr-x   5 ftp      anonymous     4096 May  3  2023 variation
226 Transfer complete
ftp> cd pub/pmc/oa_pdf/01/01
250 CWD command successful
ftp> ascii
200 Type set to A
ftp>     get main.PMC5757905.pdf main.PMC5757905.ascii.pdf
227 Entering Passive Mode (130,14,250,11,195,146).
150 Opening ASCII mode data connection for main.PMC5757905.pdf (370765 bytes)
226 Transfer complete
371799 bytes received in 0.0434 seconds (8.17 Mbytes/s)
ftp> binary
200 Type set to I
ftp>     get main.PMC5757905.pdf main.PMC5757905.bin.pdf
227 Entering Passive Mode (130,14,250,11,197,15).
150 Opening BINARY mode data connection for main.PMC5757905.pdf (370765 bytes)
226 Transfer complete
370765 bytes received in 0.0724 seconds (4.89 Mbytes/s)
ftp> bye
221 Goodbye.
```

11. The difference between the two files is that the ASCII mode is designed for transferring text files, and can change line ending characters to match the conventions of the local machine's OS. This can sometimes misinterpret certain byte sequences as line endings and corrupt the file structure of the PDF,

making it unreadable. The BINARY mode simply transfers the file byte-for-byte with no modifications.