ELEC-5220

Info. Networks

FROM: Jacob Howard

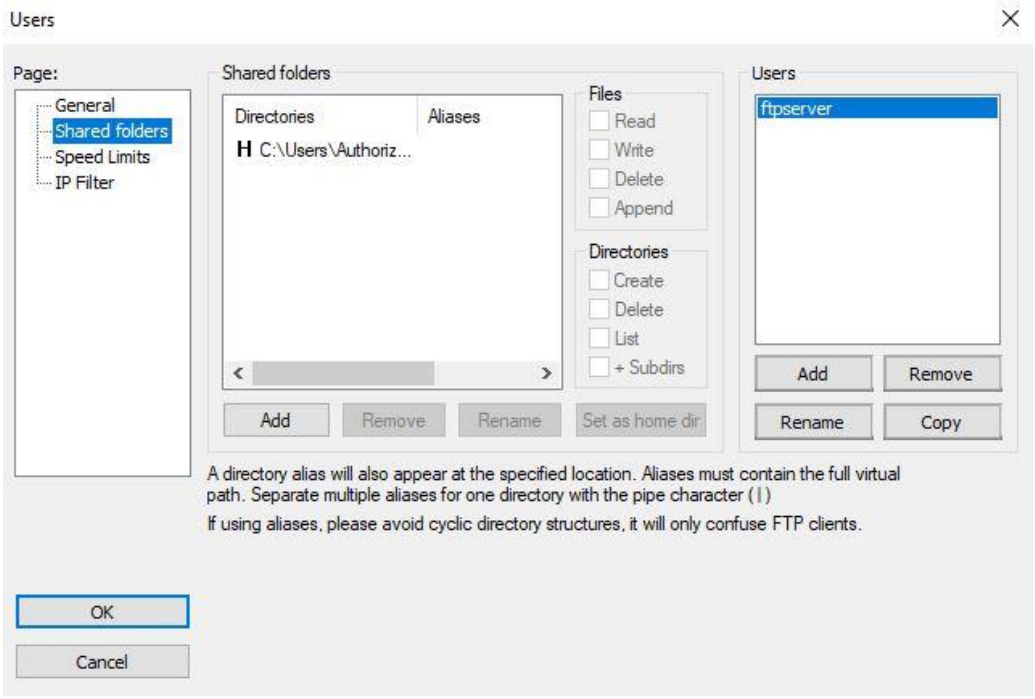
TO: Dr. Yihan Li & Chao Yang,

DUE DATE: 10/19/21

Lab 4

Introduction

In this lab, we observed TCP and how it processes file transfer between servers. We used two PCs; one for control connection and another for data connection to send files and observe how TCP works. The image blow shows settings for connecting to the server.



Ex 2 : Q1-Q4

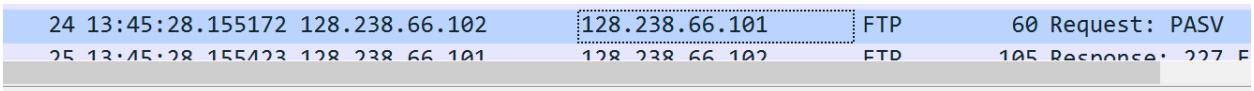
Q1: Show three FTP request commands sent from the client by highlighting them in an output screenshot.

There were multiple FTP requests (more than 3) and they are highlighted in blue in the screenshot below.

	Time	Source	Destination	Protocol	Length	Info
9	13:45:28.147055	128.238.66.101	128.238.66.102	FTP	197	Response: 220-FileZilla Server 0.9.60 beta
10	13:45:28.148052	128.238.66.102	128.238.66.101	FTP	64	Request: AUTH TLS
11	13:45:28.148179	128.238.66.101	128.238.66.102	FTP	99	Response: 502 Explicit TLS authentication not allowed
12	13:45:28.149281	128.238.66.102	128.238.66.101	FTP	64	Request: AUTH SSL
13	13:45:28.149357	128.238.66.101	128.238.66.102	FTP	99	Response: 502 Explicit TLS authentication not allowed
14	13:45:28.149896	128.238.66.102	128.238.66.101	FTP	70	Request: USER ftpserver
15	13:45:28.149957	128.238.66.101	128.238.66.102	FTP	91	Response: 331 Password required for ftpserver
16	13:45:28.150518	128.238.66.102	128.238.66.101	FTP	61	Request: PASS
17	13:45:28.150692	128.238.66.101	128.238.66.102	FTP	69	Response: 230 Logged on
18	13:45:28.151760	128.238.66.102	128.238.66.101	FTP	61	Request: CWD /

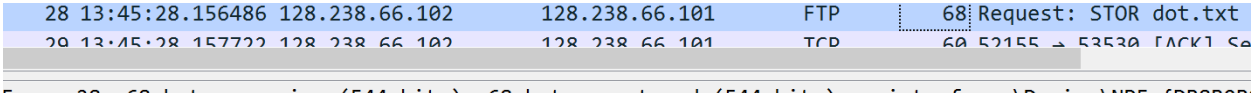
Q2: In an FTP request from the client, what is server's port number? What is client's port number? Please attach the relevant output to support your answer.

In the screenshot below, the client port appears to be 52155 and the server port is 21.



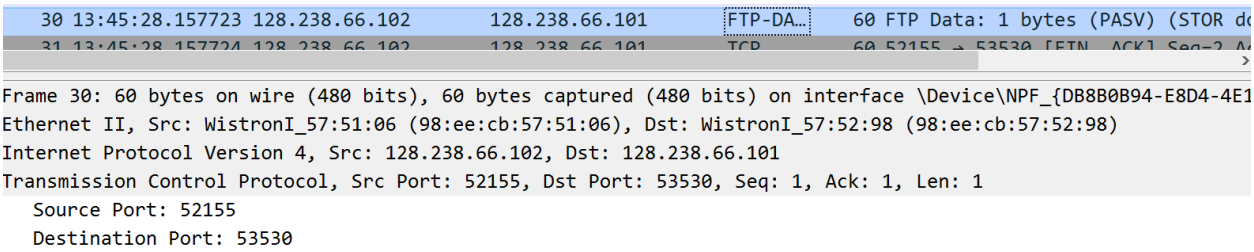
Q3: Show the data transfer packet for the file "dot" by highlight it in an output screenshot. What are server's port number and client's port number, respectively? Please attach the relevant output to support your answer.

When looking at the request and response, we see the client requested the file "dot.txt" and later, we see that the server successfully trasncmitted the file to the client. The server IP is 128.238.66.102 and the the client is 128.238.66.101. The client port still seems to be 52154 and the server port being 21.



Q4: Show the data transfer packet for server's directory list updating by highlighting it in an output screenshot. What are server's port number and client's port number, respectively? Please attach the relevant output to support your answer.

The client port seems to be 52155 and the server port being 53530. The data transfer packet is highlighted in blue below.



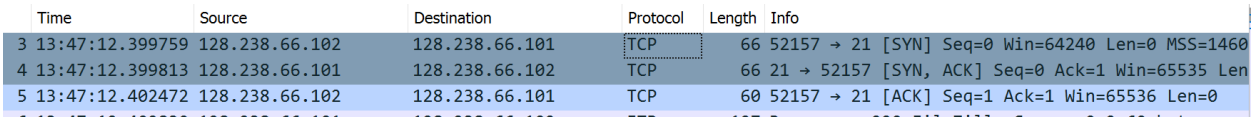
Ex 3 : Q5-Q7

Q5: TCP uses three-way handshake to set up a connection. How many TCP connections have been established according to your result?

There were 3 TCP handshakes but overall there were 20 TCP Protocols according to my results.

Q6: For each connection, answer the following questions and attach the relevant output to support your answer.

(1) Highlight the three-way handshake segments, and explain the purpose of each segment. For each segment,



Time	Source	Destination	Protocol	Length	Info
21 13:47:12.411856	128.238.66.102	128.238.66.101	FTP	69	Request: STOR 20kb.txt
22 13:47:12.411876	128.238.66.102	128.238.66.101	TCP	66	52158 → 64350 [SYN] Seq=0 Win=65535 Len=0 MSS=1
23 13:47:12.411924	128.238.66.101	128.238.66.102	TCP	66	64350 → 52158 [SYN, ACK] Seq=0 Ack=1 Win=65535
24 13:47:12.412557	128.238.66.102	128.238.66.101	TCP	60	52158 → 64350 [ACK] Seq=1 Ack=1 Win=4194304 Len

Time	Source	Destination	Protocol	Length	Info
50 13:47:12.511485	128.238.66.101	128.238.66.102	FTP	105	Response: 227 Entering Passive Mode (128,238,66
51 13:47:12.512372	128.238.66.102	128.238.66.101	FTP	60	Request: MLSD
52 13:47:12.512422	128.238.66.102	128.238.66.101	TCP	66	52159 → 50443 [SYN] Seq=0 Win=65535 Len=0 MSS=1
53 13:47:12.512609	128.238.66.101	128.238.66.102	TCP	66	50443 → 52159 [SYN, ACK] Seq=0 Ack=1 Win=65535
54 13:47:12.513946	128.238.66.102	128.238.66.101	TCP	60	52159 → 50443 [ACK] Seq=1 Ack=1 Win=4194304 Len

(a) specify the value of the sequence number field, and

The first 2 handshakes have a Seq of zero while the third has a Seq of 1.

(b) specify the value of the ACK number field if it is valid.

ACK number field is 1 on second and third handshake.

(2) Is it a control connection or data connection?

Control Connection

(3) What are server's port number and client's port number, respectively?

Server port is 21 and client is 52157 as shown below.

```
> Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \
> Ethernet II, Src: WistronI_57:51:06 (98:ee:cb:57:51:06), Dst: WistronI_57:52:98 (
> Internet Protocol Version 4, Src: 128.238.66.102, Dst: 128.238.66.101
> Transmission Control Protocol, Src Port: 52157, Dst Port: 21, Seq: 0, Len: 0
```

(4) After the TCP connection is established, consider the first TCP segment exchanged. What is the value of the sequence number field? What is the value of the ACK field if it is valid?

Once the connocction is made, the sequence number should be 1 and the ACK number should be 1.

(5) Which side initiate the TCP connection termination, the server or the client? How many segments are involved? Highlight all involved segments. For each of those segments,

I believe the client initiates the TCP connection termination. Segment length seems to be 0. There were 3 teminate segments from what I saw; 2 segments are highlighted in blue below.

	Time	Source	Destination	Protocol	Length	Info
43	13:47:12.414819	128.238.66.101	128.238.66.102	TCP	54	64350 → 52158 [FIN, ACK] Seq=1 Ack=19794 Win=525568 Len=0
44	13:47:12.415995	128.238.66.102	128.238.66.101	TCP	60	52158 → 64350 [ACK] Seq=19794 Ack=2 Win=4194304 Len=0
45	13:47:12.466505	128.238.66.102	128.238.66.101	TCP	60	52157 → 21 [ACK] Seq=80 Ack=470 Win=65024 Len=0
46	13:47:12.506970	128.238.66.101	128.238.66.102	FTP	96	Response: 226 Successfully transferred "/20kb.txt"
47	13:47:12.509690	128.238.66.102	128.238.66.101	FTP	62	Request: TYPE I
48	13:47:12.509846	128.238.66.101	128.238.66.102	FTP	73	Response: 200 Type set to I
49	13:47:12.511057	128.238.66.102	128.238.66.101	FTP	60	Request: PASV
50	13:47:12.511485	128.238.66.101	128.238.66.102	FTP	105	Response: 227 Entering Passive Mode (128,238,66,101,197,11
51	13:47:12.512372	128.238.66.102	128.238.66.101	FTP	60	Request: MLSD
52	13:47:12.512422	128.238.66.102	128.238.66.101	TCP	66	52159 → 50443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128
53	13:47:12.512609	128.238.66.101	128.238.66.102	TCP	66	50443 → 52159 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1
54	13:47:12.513946	128.238.66.102	128.238.66.101	TCP	60	52159 → 50443 [ACK] Seq=1 Ack=1 Win=4194304 Len=0
55	13:47:12.514144	128.238.66.101	128.238.66.102	FTP	109	Response: 150 Opening data channel for directory listing o
56	13:47:12.514173	128.238.66.101	128.238.66.102	FTP-DA…	157	FTP Data: 103 bytes (PASV) (MLSD)
57	13:47:12.514197	128.238.66.101	128.238.66.102	TCP	54	50443 → 52159 [FIN, ACK] Seq=104 Ack=1 Win=65536 Len=0

(a) specify its valid flags,

Flags are shown in image below.

```
Flags: 0x011 (FIN, ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...1 = Fin: Set
    [TCP Flags: ·······A···F]
```

(b) specify the value of the sequence number field, and

Sequence number field is 1 and shown below.

```
60 52159 → 50443 [FIN, ACK] Seq=1 Ack=105 Win=4194176 Len=0
```

(c) specify the value of the ACK number field if it is valid.

The ACK is shown above and for this specific termination segment, the ACK is 105.

Q7: Consider the data connection for the file transmission.

(1) Dose the server send an ACK for every data segment it receives?

No, it appears to not send an ACK for every data segment.

(2) How many bytes are sent in one segment (except the last one)? Why?

1460 bytes in one segment.

(3) Consider the first ACK by the server for the file data it receives from the client.

(a) What is the value of the sequence number field? (b) What is the value of the ACK number field?

Once the file is received, the seq number field is 1 and the ACK is 8761

```
[TCP Segment Len: 0]
Sequence Number: 1    (relative sequence number)
Sequence Number (raw): 3045695989
[Next Sequence Number: 1    (relative sequence number)]
Acknowledgment Number: 8761    (relative ack number)
```

(4) Consider the last ACK by the server for the file data transmission before the first FIN segment.

(a) What is the value of the sequence number field? Is it the same as the result from question Q7(3a)? Why or why not? (b) What is the value of the ACK number field?

The values are the same because the server hasn't sent anything back to the client.

Ex 4 : Q8-Q9

Q8: Consider the example plot shown in the figure above. How long does it take to transfer all segments? Can you identify where slow start phase begins and ends, and where congestion avoidance takes over?

The transfer begins at around 0.2 seconds and congestion starts after.

Q9: Consider the plot you get from Step 4. How long does it take to transfer all segments? Can you observe TCP's slow start in this plot? Why or Why not? Please attach the screen shot of your plot.

It takes around 0.00175 seconds to transfer all segments and you cannot observe the TCP slow state because it happens in less than a second.