HES-SO Valais Wallis

File Transfer Protocol

Digital Team Academy

Dasek Joiakim

19/10/2022

Table of contents

tudy the protocol
sage of FTP
pload and Download a file
Upload
Download
What are active/passive modes
Data port
1. During the Download, which server's port was used to transfer the file
2. During the Upload, which server's port was used to transfer the file
reate a folder1
ownload a file14
pload a file15

FTP stands for file transfer protocol, and it refers to a set of rules that define how computers transfer files to each other. It is used, among other things, by developers to upload their source files to web hosts, which is a remote server. This protocol is designed on a client-server model, the server has the server-like tool installed on its system and the client has the client-like ftp on its system.

Here is the complete suite of the FTP tool, its arguments and their definitions:²

FTP Command	Description of Command
!	This command toggles back and forth between the operating system and
	ftp. Once back in the operating system, typing exit takes you back to the
	FTP command line.
?	Accesses the Help screen.
append	Append text to a local file.
ascii	Switch to ASCII transfer mode.
bell	Turns bell mode on or off.
binary	Switches to binary transfer mode.
bye	Exits from FTP.
cd	Changes directory.
close	Exits from FTP.
delete	Deletes a file.
debug	Sets debugging on or off.
dir	Lists files, if connected.
	dir -C = lists the files in wide format.
	dir -1 = Lists the files in bare format in alphabetic order.
	dir -r = Lists directory in reverse alphabetic order.
	dir -R = Lists all files in current directory and sub directories.
	dir -S = Lists files in bare format in alphabetic order.
disconnect	Exits from FTP.
get	Get file from the remote computer.
glob	Sets globbing on or off. When turned off, the file name in
	the put and get commands is taken literally, and wildcards will not be
	looked at.
hash	Sets hash mark printing on or off. When turned on, for each 1024 bytes of
	data received, a hash-mark (#) is displayed.
help	Accesses the Help screen and displays information about the command if
	the command is typed after help.
Icd	Displays local directory if typed alone or if path typed after lcd will change
	the local directory.
literal	Sends a literal command to the connected computer with an expected one-
	line response.
ls	Lists files of the remotely connected computer.

¹ https://www.techtarget.com/searchnetworking/definition/File-Transfer-Protocol-FTP

² https://www.serv-u.com/ftp-server-windows/commands

mdelete	Multiple delete.
mdir	Lists contents of multiple remote directories.
mget	Get multiple files.
mkdir	Make directory.
mls	Lists contents of multiple remote directories.
mput	Send multiple files.
open	Opens address.
prompt	Enables or disables the prompt.
put	Send one file.
pwd	Print working directory.
quit	Exits from FTP.
quote	Same as the literal command.
recv	Receive file.
remotehelp	Get help from remote server.
rename	Renames a file.
rmdir	Removes a directory on the remote computer.
send	Send single file.
status	Shows status of currently enabled and disabled options.
trace	Toggles packet tracing.
type	Set file transfer type.
user	Send new user information.
verbose	Sets verbose on or off.

We can refer to this list for the rest of the exercises. all these arguments allow us to activate a function of the FTP tool on our terminal.

Usage of FTP

First thing to do, you must install FileZilla-client to be able to connect to the FTP server, here is the official link: <u>Download link</u>. After installing it we can talk a little about the graphical interface of this software. We see a bar with the labels Host, username, password and port. These elements are essential to establish a connection between the client and the server.

The IP address is provided, we could also insert a domain name which is therefore linked with the IP address, without authentication, and the default port is 21. You can establish a connection by pressing "quickconnect".

Under this same bar is the verbose console. The left side is the local file system, i.e., the client side, and the right side is the file explorer on the server side. Under this part we have the inside of the tree of the folder selected in the upper part. And for the last part of this software is the historical or pending queue of files transiting between client and server.



We can see the connection established in the following image:

2 10.130.25.239 - FileZilla File Edit View Transfer Server Bookmarks Help 111 ↓ 6 11 11 11 11 11 11 11 11 11 11 11 11 1		- 0 ×
Host: 10.130.25.239 Username: Password: Port: Quickconnect		
Status: Insecure server, it does not support FTP over TLS. Status: Logged in Status: Relieving directory listing Status: Directory listing of "/" successful		
Local site: C:\Users\jowad\	V Remote site: /	~
→ Users → →	Construction Construction Construction Construction Construction Construction Construction Construction Construction	I
Filename AFilesize Filetype Last modified	Filename Filesize Filetype Last modifi Permissi Owner/Gr	
android File folder 23.09.2022 12 android File folder 23.09.2022 12 android File folder 23.09.2022 13 android File folder 19.10.2022 08 android File folder 23.09.2022 12 android File folder 19.10.2022 08 android File folder 19.10.2022 08 appData File folder 19.10.2022 08 Cisco Packer Tarer File folder 17.10.2022 16 Cookies File folder 17.10.2022 16 Documents File folder 19.10.2022 08 Documents File folder 19.10.2022 16 Documents File folder 17.10.2022 16 Links File folder 19.10.2022 08 Documents File folder 19.10.2022 08 Links File folder 19.10.2022 08 Mexu Demarer File folder 19.10.2022 08 Mexu Demarer File folder 19.10.2022 08 Mexu Demarer File folder 19	#recycle File folder 19.10.2022 0777 root root 11 CR0VABELginEx File folder 17.10.2022 0777 anonymo AAAAAAAAAA File folder 17.10.2022 0777 anonymo AAAAAAAAAAA File folder 19.10.2022 0777 anonymo Bannan TruckDep File folder 19.10.2022 0777 anonymo B Jest File folder 18.10.2022 0777 anonymo DosserPlaste File folder 18.10.2022 0777 anonymo FolderTEST File folder 18.10.2022 0777 anonymo Nohen File folder 18.10.2022 0777 anonymo In folderTEST File folder 18.10.2022 0777 anonymo In ketscholder File folder 16.10.2022 0777 anonymo In ketscholder File folder 16.10.2022 0777 anonymo In ketscholder File folder 16.10.2022 0777	
Server/Local file Direc. Remote file Size Priority Status Queued files Failed transfers Successful transfers		요 @ Queue: empty

Wireshark let us know the exchange of requests between the client and the server. In these unsecured exchanges, we find the anonymous connection and the default password, as well as the port, the commands of connection, file listing etc...

A *14	/i_Ei				- a x
Fichie	er Editer Vue Aller	Canture Analyser Statist	iques Telephonie Wireless ()	utils Airle	5 A
1		3 9 🗰 🗰 🕮 🐺 🐓		ana Tuar	
	addr == 10.130.25.239.8/8	tcp port == 21			
No	Time	Source	Dectination	Protocol Length lefo	
140.	277 21 197647	10 93 1 105	10 130 25 239	TTD 66.60589 - 21.5VNI Son-0 Win-64240 Lon-0 MSS-1460 WS-256. SACK DERM	
-	278 21.203029	10.130.25.239	10.93.1.105	TCP 66.21 \rightarrow 60588 [SVN, ACK] Sec=0 Ack=1 Win=1460 Len=0 MSs=1382 SACK PERM WS=128	
	279 21,203264	10.93.1.105	10.130.25.239	TCP 54.60588 \Rightarrow 21 [ACK] Segal Ack=1 Win=131072 Len=0	
	280 21,209334	10.130.25.239	10.93.1.105	FTP 85 Response: 220 profbox FTP server ready.	
	281 21,209920	10.93.1.105	10,130,25,239	ETP 64 Request: AUTH TLS	
	282 21,212746	10,130,25,239	10,93,1,105	TCP 60 21 + 60588 [ACK] Seg=32 Ack=11 Win=14720 Len=0	
	283 21,214133	10.130.25.239	10.93.1.105	FTP 109 Response: 504 AUTH: security mechanism 'TLS' not supported(17).	
	284 21,214656	10,93,1,105	10,130,25,239	FTP 64 Request: AUTH SSL	
	285 21,217596	10.130.25.239	10,93,1,105	FTP 109 Response: 504 AUTH: security mechanism 'SSI' not supported(17).	
	286 21,220403	10.93.1.105	10,130,25,239	FTP 70 Request: USER anonymous	
	287 21,240379	10,130,25,239	10,93,1,105	FTP 112 Response: 331 Guest Login ok, send your email address as password.	
	288 21,241235	10.93.1.105	10,130,25,239	FTP 82 Request: PASS anonymous@example.com	
	289 21,280357	10,130,25,239	10.93.1.105	FTP 102 Response: 230 Guest login ok, access restrictions apply.	
	290 21,281352	10.93.1.105	10.130.25.239	FTP 68 Request: OPTS UTF8 ON	
	291 21.285847	10.130.25.239	10.93.1.105	FTP 77 Response: 200 OK, UTF-8 enabled	
	292 21.290930	10.93.1.105	10.130.25.239	FTP 59 Request: PWD	
	293 21.295450	10.130.25.239	10.93.1.105	FTP 85 Response: 257 "/" is current directory.	
L	294 21.336357	10.93.1.105	10.130.25.239	TCP 54 60588 → 21 [ACK] Seq=84 Ack=302 Win=130816 Len=0	
> Fr	ame 277: 66 bytes	s on wire (528 bits)	. 66 bytes captured (5	8 bits) on interface 0000 00 00 0c 9f f4 45 3c e9 f7 4e 97 29 08 00 45 00 ·····E<	
> Et	thernet II, Src: I	IntelCor 4e:97:29 (3	c:e9:f7:4e:97:29), Dst	Cisco 9f:f4:45 (00: 0010 00 34 f3 bf 40 00 80 06 00 00 0a 5d 01 69 0a 82 .4.0].i	
> Ir	nternet Protocol V	/ersion 4, Src: 10.9	3.1.105, Dst: 10.130.2	.239 0020 19 ef ec ac 00 15 ac 3f 4f 6f 00 00 00 00 80 02? 00	
> Tr	ansmission Contro	ol Protocol, Src Por	t: 60588, Dst Port: 21	Seq: 0, Len: 0 0030 fa f0 30 5d 00 00 02 04 05 b4 01 03 03 08 01 010]	
				0040 04 02	
0	wireshark Wi-FiLW421	T1.pcapng		Paquets : 300 - Affichés : 18 (6.0%)	Profil : Default

Upload and Download a file

Upload

Create an empty file on the server side as follows and name it 01test.txt. Wireshark will capture this request. In the blue line, selected in the Wireshark image we can see the command "STOR" which allows to create a file on the server side.

10.130.25.239 - FileZilla							- 0 ×
File Edit View Iransfer S	erver <u>B</u> ookmarks <u>H</u> elp	<u>¢</u> 🤊 🚯					
Host: 10.130.25.239 Usern	name: Pa	ass <u>w</u> ord: <u>P</u> ort:	Quickconnect 💌				
Status: Logged in Status: Retrieving directory list Status: Directory listing of "/": Status: Connection closed by s	ting successful server						
Local site: C:\Users\jowad\				Remote site: /	Contract for		~
Users In Users				- 2 #recycle	Create empty file	e of the file which should be	^I
Default	ar .			2 1CROYABLEjaiREUSSI	created:	e of the file which should be	
				AAAAAAAAAAAZotrimUka	01test.txt		
⊞- Public ⊞- Windows				BananaTruckDepot		OK Cancel	
· Windows.old				DossierPatate	-		
Filename File	size Filetype Las	at modified		Filename Filesize Filetype	Last modifi Permissi	Owner/Gr	
android	File folder 23.	09.2022 12:		#recycle File folder	19.10.2022 0777	root root	
dbus-keyrings	File folder 26. File folder 23.	09.2022 09: 09.2022 13:		1CROYABLEjaiRE File folder	17.10.2022 0777 17.10.2022 0777	anonymo anonymo	
jdks	File folder 19.	10.2022 08:		AAAAAAAAAA File folder	19.10.2022 0777	anonymo	
m2 AppData	File folder 23.	09.2022 12:		BananaTruckDep File folder	17.10.2022 0777	anonymo	
Application Data	File folder 19.	10.2022 09		DossierPatate File folder	18.10.2022 0777	anonymo	
Cisco Packet Tracer	File folder 28	09.2022 13:		Enfin File folder	18.10.2022 0777	anonymo	
Contacts Cookies	File folder 17. File folder 17.	10.2022 16:		Nohen File folder	18.10.2022 0777 02.04.2022 0777	anonymo anonymo	
Desktop	File folder 17.	10.2022 16:		NvtestCMDAntho File folder	16.01.2022 0777	anonymo	
Documents	File folder 19.	10.2022 08:		Pourquoicestplus File folder	16.01.2022 0777	anonymo	
Favorites	File folder 19.	10.2022 09		testFolderTeams File folder	18.10.2022 0777	anonymo	
Links	File folder 17.	10.2022 16:		Testionathan File folder	19.10.2022 0777	anonymo	
Local Settings	File folder 19. File folder 17.	10.2022 09:		Tutu File folder	14.04.2022 0777 14.04.2022 0777	anonymo	
Mes documents	File folder 19.	10.2022 08:		AAA_Jo 0 File	18.10.2022 0777	anonymo	
8 files and 30 directories. Total si	ze: 13701328 bytes	05 2022 07-		25 files and 16 directories. Total size: 122 385 b	10 10 2022 0777	3808-880	
Capture en cours de Wi-Fi Eichier Editer Vue Aller	Capture Analyser Sta	tistiques Telephonje Wireless Q	utils <u>A</u> ide				후 ④ Queue: empty -
	ଣ ୧ 🗢 🕈 🖺 Ŧ .	1 I Q Q Q II					
ip.addr == 10.130.25.239 &8	tcp.port == 21	Destination	Protocol Longth Info				+
389 70.425907	10.93.1.105	10.130.25.239	FTP 64 Request: A	AUTH TLS			
390 70.428841	10.130.25.239	10.93.1.105	TCP 60 21 → 60600	5 [ACK] Seq=32 Ack=11 Win=14720 L	en=0		
391 70.428841	10.130.25.239	10.93.1.105	FTP 109 Response:	504 AUTH: security mechanism 'TL	S' not supported(17).	
393 70.432321	10.130.25.239	10.93.1.105	FTP 109 Response:	504 AUTH: security mechanism 'SS	L' not supported(17).	
394 70.434456	10.93.1.105	10.130.25.239	FTP 70 Request: U	JSER anonymous			
395 70.451511	10.130.25.239	10.93.1.105	FTP 112 Response:	331 Guest login ok, send your em DASS aponymous@example.com	ail address as pa	issword.	
397 70.495737	10.130.25.239	10.93.1.105	TCP 60 21 → 60606	5 [ACK] Seq=200 Ack=65 Win=14720	Len=0		
398 70.495737	10.130.25.239	10.93.1.105	FTP 102 Response:	230 Guest login ok, access restr	ictions apply.		
399 70.496183	10.93.1.105	10.130.25.239	FTP 68 Request: 0 TCP 60.21 → 60600	DPIS UIF8 ON 5 [ACK] Seg=248 Ack=79 Win=14720	len=0		
401 70.499912	10.130.25.239	10.93.1.105	FTP 77 Response:	200 OK, UTF-8 enabled			
402 70.500546	10.93.1.105	10.130.25.239	FTP 61 Request: (CWD /			
403 70.508472	10.130.25.239	10.130.25.239	FTP 59 Request: F	250 CWD command successful. PWD			
405 70.512307	10.130.25.239	10.93.1.105	FTP 85 Response:	257 "/" is current directory.			
406 70.513151	10.93.1.105	10.130.25.239	FTP 62 Request: 1	TYPE I			
407 70.516465	10.130.25.239	10.130.25.239	FTP 60 Request: F	200 Type set to 1. PASV			
409 70.520679	10.130.25.239	10.93.1.105	FTP 104 Response:	227 Entering Passive Mode (10,13	0,25,239,217,56)		
-> 410 70.521772 415 70 520650	10.93.1.105	10.130.25.239	FTP 71 Request: 5	STOR 01test.txt	naction for '01to	et tyt!	
415 70.529659	10.130.25.239	10.93.1.105	FTP 78 Response:	226 Transfer complete.	nection for bite	stitxt .	
418 70.529824	10.93.1.105	10.130.25.239	TCP 54 60606 → 21	1 [ACK] Seq=122 Ack=484 Win=13056	0 Len=0		· · · · · ·
 > Frame 410: 71 bytes > Ethernet II, Src: 1 > Internet Protocol V > Transmission Contro > File Transfer Proto > STOR Øltest.txt\ Request commar Request arg: 6 [Current working di Command response 	s on wire (568 bit IntelCor_4e:97:29 Version 4, Src: 16 Dl Protocol, Src F Docol (FTP) r\n hd: STOR Ditest.txt irectory: /]	:s), 71 bytes captured (5) (3c:e9:f7:4e:97:29), 0st (33.1.105, Dst: 10.130.2) ort: 60606, Dst Port: 21	38 bits) on interf: 0000 : Cisco_9f:f4:45 (f 0010 .239 0020 , Seq: 105, Ack: 4€ 0030 0040	00 00 00 05 9f 74 45 3c e9 77 4e 9 00 39 75 3d 54 00 80 80 06 00 00 0 19 ef ec be 00 15 f5 e7 ce 24 1 01 ff 30 62 00 00 53 54 4f 52 20 77 2e 74 78 74 0d 0a	7 29 08 00 45 00 a 5d 01 69 0a 82 a d4 21 c4 50 18 0 30 31 74 65 73	E< .N.).E. .9.@\$\$	
[Command response b	frames: 0] bytes: 0]						
[Command response b [Command response f	frames: 0] bytes: 0] <u>first frame: 0]</u>						

Download

It's pretty much the same for downloading files, we must right click on the server side on the file we have previously created. Then press download. This same file will be uploaded to the client in the current folder on the left side.



With Wireshark we see in blue the request line with the command "RETR" followed by the name of the file, in our case "01test.txt".

4	Capture en cours de Wi-Fi					- 0 ×
Fic	hier Editer Vue Aller	Capture Analyser Statis	tiques Telephonie <u>W</u> ireless <u>O</u>	utils <u>A</u> ide		
1	📕 👩 💿 📄 🗎 🕅	ରି 🍳 👄 👄 著 🔮				
	ip.addr == 10.130.25.239 &d	& tcp.port == 21				× +
No	Time	Source	Destination	Protocol	Length Info	
	156 73.782864	10,130,25,239	10.93.1.105	FTP	109 Response: 504 AUTH: security mechanism 'SSL' not supported(17).	
	157 73,790861	10,93,1,105	10,130,25,239	ETP	70 Request: USER anonymous	
	158 73,810838	10,130,25,239	10.93.1.105	FTP	112 Response: 331 Guest login ok, send vour email address as password.	
	159 73.811595	10.93.1.105	10.130.25.239	FTP	82 Request: PASS anonymous@example.com	
	160 73.852584	10.130.25.239	10.93.1.105	FTP	102 Response: 230 Guest login ok, access restrictions apply.	
	161 73.853514	10.93.1.105	10.130.25.239	FTP	68 Request: OPTS UTF8 ON	
	162 73.857201	10.130.25.239	10.93.1.105	FTP	77 Response: 200 OK, UTF-8 enabled	
	163 73.861313	10.93.1.105	10.130.25.239	FTP	61 Request: CWD /	
	164 73.868601	10.130.25.239	10.93.1.105	FTP	83 Response: 250 CWD command successful.	
	165 73.869362	10.93.1.105	10.130.25.239	FTP	62 Request: TYPE I	
	166 73.873107	10.130.25.239	10.93.1.105	FTP	74 Response: 200 Type set to I.	
	167 73.873689	10.93.1.105	10.130.25.239	FTP	60 Request: PASV	
	168 73.877416	10.130.25.239	10.93.1.105	FTP	104 Response: 227 Entering Passive Mode (10,130,25,239,217,34)	
	169 73.878437	10.93.1.105	10.130.25.239	FTP	60 Request: MLSD	
	173 73.887978	10.130.25.239	10.93.1.105	FTP	112 Response: 150 Opening BINARY mode data connection for 'file list'.	
	177 73.889281	10.130.25.239	10.93.1.105	FTP	78 Response: 226 Transfer complete.	
	180 73.889751	10.93.1.105	10.130.25.239	TCP	54 60609 → 21 [ACK] Seq=106 Ack=452 Win=130816 Len=0	
	183 73.891546	10.93.1.105	10.130.25.239	FTP	62 Request: TYPE A	
	185 73.896175	10.130.25.239	10.93.1.105	FTP	74 Response: 200 Type set to A.	
	186 73.896419	10.93.1.105	10.130.25.239	FTP	60 Request: PASV	
4	187 73.899569	10.130.25.239	10.93.1.105	FTP	103 Response: 227 Entering Passive Mode (10,130,25,239,217,3)	
+	188 73.900398	10.93.1.105	10.130.25.239	FTP	71 Request: RETR 01test.txt	
	192 73.907236	10.130.25.239	10.93.1.105	FTP	123 Response: 150 Opening BINARY mode data connection for '01test.txt' (0 bytes).	
	193 73.907236	10.130.25.239	10.93.1.105	FTP	78 Response: 226 Transfer complete.	
L	195 73.907366	10.93.1.105	10.130.25.239	TCP	54 60609 → 21 [ACK] Seq=137 Ack=614 Win=130560 Len=0	
	Frame 188: 71 byte	s on wire (568 hits). 71 bytes cantured (56	58 hits) (on interf: 0000 00 00 0c 9f f4 45 3c e9 f7 4e 97 29 08 00 45 00 ·····E<	
5	Ethernet II. Src:	IntelCor 4e:97:29 (3c:e9:f7:4e:97:29). Dst:	Cisco 9	6: fa: 45 (6 0010 00 39 f3 ep 40 00 80 06 00 00 0a 5d 01 69 0a 82 9 0 0 0 0 1 1 1	
5	Internet Protocol	Version 4. Src: 10.	93.1.105. Dst: 10.130.2	5.239	0020 19 ef ec c1 00 15 99 72 45 36 e4 38 2d 7f 50 18	
>	Transmission Contr	ol Protocol, Src Po	rt: 60609. Dst Port: 21	Sea: 12	0. Ack: 52 0030 01 fo 30 62 00 00 52 45 54 52 20 30 31 74 65 73 0b. RE TR 01tos	
~	File Transfer Prot	ocol (FTP)			0040 74 20 74 78 74 0d 0a t txt ··	
	<pre>v RETR 01test.txt</pre>	\r\n				
	Request comma	nd: RETR				
	Request arg:	01test.txt				
1	[Current working d	irectory: /]				
	[Command response	frames: 0]				
	[Command response	bytes: 0]				
	[Command response	first frame: 0]				
	F 10					

○ Wi-Fi: <live capture in progress>

What are active/passive modes³

- For the active mode, this was originally the only mode available. The client will first establish a connection to the server with the "ACTV" command on the terminal and send its ports, the FTP server will create a data tunnel to the client and start the transfer.
- In passive mode, the client will have to issue the "PASSV" command and this time the server will send information such as the port to establish a data connection with the server. This method is useful to counteract the firewall which could block incoming connections to the client.



³ https://www.techtarget.com/searchnetworking/definition/File-Transfer-Protocol-FTP

⁴ https://cdn.ttgtmedia.com/rms/onlineImages/FTP_active_passive.jpg

Data port

I use active mode on FileZilla, so the control port is 21 and the data transfer port is 20. But when in passive mode. When the client sends the command to be in passive then the server responds with this: "227 Entering Passive Mode: (192,168,150,90,195,149).

The representation of the parenthesis is (B1, B2, B3, B4, P1, P2), B means Byte so Byte number 1 of the IP address of the server then we have the P's, these are the ports. Here is the calculation so that the client knows which port to connect to and establish a data connection. P1 * 256 + P2, in this example it would be 195 * 256 + 149 = 50'069. So, we have found our port.

```
testbox1: {/home/p-t/slacker/public html} % ftp -d testbox2
Connected to testbox2.slacksite.com.
220 testbox2.slacksite.com FTP server ready.
Name (testbox2:slacker): slacker
---> USER slacker
331 Password required for slacker.
Password: TmpPass
---> PASS XXXX
230 User slacker logged in.
---> SYST
215 UNIX Type: L8
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> passive
Passive mode on.
ftp> 1s
ftp: setsockopt (ignored): Permission denied
---> PASV
227 Entering Passive Mode (192,168,150,90,195,149).
---> LIST
150 Opening ASCII mode data connection for file list
drwx----- 3 slacker users 104 Jul 27 01:45 public_html
226 Transfer complete.
ftp> quit
---> OUIT
221 Goodbye.
```

5

⁵ https://www.cosmos.esa.int/documents/772136/977578/psa_activeVsPassiveFtp.pdf/5e36a7b8-8732-4e65-ab6b-6cf94a742ea6

	1. Dur	ring the [)ownload,	whicł	server's port was used to transf	er the file.
	273 118.465122	10.93.1.105	10.130.25.239	FTP	60 Request: PASV	
-	274 118.470112	10.130.25.239	10.93.1.105	FTP	104 Response: 227 Entering Passive Mode (10,130,25,239,217,10)	
	275 118.471295	10.93.1.105	10.130.25.239	FTP	71 Request: RETR 01test.txt	
	279 118.480090	10.130.25.239	10.93.1.105	FTP	123 Response: 150 Opening BINARY mode data connection for '01tes	t.txt' (0 bytes).
	280 118.480090	10.130.25.239	10.93.1.105	FTP	78 Response: 226 Transfer complete.	
L	282 118.480378	10.93.1.105	10.130.25.239	TCP	54 60617 → 21 [ACK] Seq=117 Ack=463 Win=130816 Len=0	
	304 139.297125	10.130.25.239	10.93.1.105	FTP	110 Response: 421 Timeout (300 seconds): closing control connect	ion.
	305 139.297125	10.130.25.239	10.93.1.105	TCP	60 21 → 60606 [FIN, ACK] Seq=57 Ack=1 Win=115 Len=0	
	306 139.297125	10.130.25.239	10.93.1.105	тср	60 [TCP Retransmission] 21 → 60606 [FIN, ACK] Seq=57 Ack=1 Win=	115 Len=0
	307 139.297381	10.93.1.105	10.130.25.239	TCP	54 60606 → 21 [ACK] Seq=1 Ack=58 Win=510 Len=0	
	308 139.297473	10.93.1.105	10.130.25.239	тср	54 [TCP Dup ACK 307#1] 60606 → 21 [ACK] Seq=1 Ack=58 Win=510 Le	n=0
	309 139.300778	10.93.1.105	10.130.25.239	TCP	54 60606 → 21 [FIN, ACK] Seq=1 Ack=58 Win=510 Len=0	
	310 139.304947	10.130.25.239	10.93.1.105	TCP	60 21 → 60606 [ACK] Seq=58 Ack=2 Win=115 Len=0	
> 1	internet Protocol V	Version 4, Src: 10.	93.1.105, Dst: 10.130.	25.239	0000 00 00 0c 9f f4 45 3c e9 f7 4e 97 29 08 00 45 00	····E<· ·N·)··E·
~ T	ransmission Contro	ol Protocol, Src Po	rt: 60617, Dst Port: 2	l, Seq: 100	ck: 37 0010 00 39 f4 00 40 00 80 06 00 00 0a 5d 01 69 0a 82	·9··@··· ···]·i··
	Source Port: 606	17			0020 19 ef ec c9 00 15 65 7b d7 ba 86 a0 c9 ce 50 18	····• <mark>•·•</mark> e{ ·····•P·
	Destination Port	: 21			0030 01 ff 30 62 00 00 52 45 54 52 20 30 31 74 65 73	· · Øb · · RE TR Ø1tes
	[Stream index: 1	5]			0040 74 2e 74 78 74 0d 0a	t.txt··
	[Conversation co	mpleteness: Incompl	ete, DATA (15)]			
	[TCP Segment Len	: 17]				
	Sequence Number:	100 (relative s	equence number)			
	Sequence Number	(raw): 1702614970				
	[Next Sequence N	umber: 117 (rela	tive sequence number)]			
	Acknowledgment N	umber: 370 (rela	tive ack number)			
	Acknowledgment n	umber (raw): 225868	4366			
-						
	Destination Port (tcp.)	dstport), 2 byte(s)			Paquets : 319 · Affichés : 38 (11.5	96) Profil : Def

..... , ٢٠١

2. During the Upload, which server's port was used to transfer the file.

		-												
4	26 1.267600	10.130.25.239	10.93.1.105	FTP	105 R	esponse:	227 Er	ntering	Passive Mo	de (10	,130,25,239,217,10	ð9)		
4	 27 1.268346 	10.93.1.105	10.130.25.239	FTP	85 R	equest:	STOR W	ireshark	- Shortcu	t.lnk				
	34 1.278525	10.130.25.239	10.93.1.105	FTP	127 R	esponse:	150 O	oening B	INARY mode	data	connection for 'W	ireshark - Shortcut.lnk'.		
	36 1.278525	10.130.25.239	10.93.1.105	FTP	78 R	esponse:	226 Ti	ransfer	complete.					
L	- 38 1.278856	10.93.1.105	10.130.25.239	TCP	54 6	0620 → 2	1 [ACK]] Seq=13	1 Ack=468	Win=13	0816 Len=0			
>	Ethernet II, Src:	IntelCor_4e:97:29 (3c:e9:f7:4e:97:29), Ds	st: Cisco_9f:	f4:45 (@	0000	00 00	0c 9f f	4 45 3c e9	f7 4	97 29 08 00 45 0	00 ····E<· ·N·)··E·		-
>	Internet Protocol	Version 4, Src: 10.	93.1.105, Dst: 10.130.	25.239		0010	00 47	f4 15 4	0 00 80 06	00 00	0 0a 5d 01 69 0a 8	32 ·G··@··· ···]·i··		
~	<pre>/ Transmission Control</pre>	ol Protocol, Src Po	rt: 60620, Dst Port: 2	21, Seq: 100,	Ack: 37	0020	19 ef	ec cc 🛛	0 15 6f 49	4c 31	F 99 70 19 62 50 1	.8 ••••••••••••••••••••••••••••••••••••		
	Source Port: 606	520				0030	01 ff	30 70 0	0 00 53 54	4f 52	2 20 57 69 72 65 7	'3 ·· 0p··ST OR Wires		
	Destination Port	: 21				0040	68 61	72 6b 2	0 2d 20 53	68 61	F 72 74 63 75 74 2	e hark - S hortcut.		
	[Stream index: 1	1]				0050	6c 6e	6b 0d 0	a			lnk··		
	[Conversation co	ompleteness: Incompl	ete, DATA (15)]											
	[TCP Segment Len	n: 31]												
	Sequence Number:	: 100 (relative s	equence number)											
	Sequence Number	(raw): 1867074623												
	[Next Sequence N	lumber: 131 (rela	tive sequence number)]										
	Acknowledgment N	lumber: 371 (rela	tive ack number)											
(Destination Port (tcp.	dstport), 2 byte(s)									Paquets : 98 · Affichés : 27	(27.6%)	Profil : D	efa

Create a folder

We will create a file on the remote server in the command line. First open PuTTY, and to establish the connection we need to enter the IP address of the server and port 21, then choose the RAW method and finally press connect.

This is what is displayed afterwards. In order to have the rights to create a folder, you will have to do a few things on the command line, first you must authenticate yourself. We will consult the list of commands implemented by the FTP server and enter "help".

	10.130.2	5.239 - PuTTY							_		×
22 HE	0 profb LP	ox FTP sei	rver read	ly.							•
21	4- The	following	commands	are r	ecognized	(* =>'s	unimple	mented).			
	USER	LPRT	MODE	MSOM*	RNTO	SITE	RMD	SIZE	AUTH		
	PASS	EPRT	RETR	MSAM*	ABOR	SYST	XRMD	MDTM	PBSZ		
	ACCT*	PASV	STOR	MRSO*	DELE	STAT	PWD	MLST	PROT		
	SMNT*	LPSV	APPE	MRCP*	CWD	HELP	XPWD	MLSD	CCC		
	REIN*	EPSV	MLFL*	ALLO	XCWD	NOOP	CDUP	MFMT			
	QUIT	TYPE	MAIL*	REST	LIST	MKD	XCUP	FEAT			
	PORT	STRU	MSND*	RNFR	NLST	XMKD	STOU	OPTS			
21	4 Direc	t comments	s to ftp-	-bugs@p	rofbox.						
1											
/											
q											
D 1	100	Det: 10 1.	20 25 220)		1 0000	10 04 0		10 00	- fh	20.00

Here is the one we are interested in: So, enter the command "USER anonymous" and then "PASS anonymous@example.com". The user value "anonymous" is mandatory and the password is the one you want.

ß	1 0.130.2	5.239 - PuTTY							—	×
220) profb	ox FTP se	rver rea	ady.						
HEI	LP									
214	l- The	following	comman	ds are re	ecognized	d (* =>'s	unimpl	Lemented)		
	USER	LPRT	MODE	MSOM*	RNTO	SITE	RMD	SIZE	AUTH	
	PASS	EPRT	RETR	MSAM*	ABOR	SYST	XRMD	MDTM	PBSZ	
	ACCT*	PASV	STOR	MRSQ*	DELE	STAT	PWD	MLST	PROT	
	SMNT*	LPSV	APPE	MRCP*	CWD	HELP	XPWD	MLSD	CCC	
	REIN*	EPSV	MLFL*	ALLO	XCWD	NOOP	CDUP	MFMT		
	QUIT	TYPE	MAIL*	REST	LIST	MKD	XCUP	FEAT		
	PORT	STRU	MSND*	RNFR	NLST	XMKD	STOU	OPTS		
214	1 Direc	t comment:	s to ft	p-bugs@p:	rofbox.					
use	er anon	ymous								
331	L Guest	: login ok	, send	your ema:	il addres	ss as pas	sword.			
pas	ss anon	ymous@exa	mple.com	n						
230) Guest	: login ok	, acces	s restri	ctions ap	oply.				
										-

We are authenticated now we want to create a new folder, the command is "make directory" so mkd followed by the folder name "mkd myFolder". The server replies that the folder has been created successfully! This way we can check if everything went well on FileZilla and if so, the file is present.



Download a file

Downloading is more complicated. We have to go through the same steps as before but with a few more. The connection, then the authentication commands are done as before but we are not going to create a folder this time but to download so for that we are going to put ourselves in passive mode here is the command to send to the server: "pasv". The server answers us, and we have to calculate the port: P1 * 256 + P2 = 217 * 256 + 21 = 55573.

The PORT verb

6

A PORT request asks the server to use a different mechanism of creating a data connection: the server makes a TCP connection to the client.
The PORT request has a parameter in the form
h1,h2,h3,h4,p1,p2
meaning that the client is listening for connections on TCP port p1*256+p2 at IP address h1.h2.h3.h4. (The RFC 959 formal syntax does not allow any of these numbers to be 0. The formal syntax is wrong.)
The server normally accepts PORT with code 200. If the server was listening for a connection, it stops, and drops any connections already made.
The server does not connect to the client's port immediately. After the client sends RETR and after the server sends its initial mark, the server attempts to connect. It rejects the RETR request with code 425 if the connection attemptails; otherwise it proceeds normally.
In theory, the client can send RETR without a preceding PORT or PASV. The server is then supposed to connect to port 20 at the client's IP address. In practice, however, servers refuse to do this.
For security reasons, clients should never use PORT. However, some clients still rely on PORT, and will give up on a file transfer if PORT is rejected. My current recommendation is that servers continue to support PORT.

We must use the "retrieve" command followed by the name of the file to download so that the server understands and listens, waiting for a connection from the client, therefore "retr O1test.txt" and press the "Enter" key. At this time, we must create a second tunnel to receive the file and for this we will create a second PuTTY session.

So, we launch a second PuTTY process, and we enter the IP address and the port calculated previously, 55573. With the RAW connection method and finally press connect. A new window opens and initializes the connection. If the window disappears, it means that the passive mode is not activated or that the port calculation is incorrect or that you went too slow between the "retr O1test.txt" command step of the first session and the opening of the second session.

🖉 10.130.25.239 - PuTTY - 🗆 🗙	
Re	
	🧬 10.130.25.239 - PuTTY − 🗆 X
	425 Can't build data connection: Connection timed out.
	500 : command not understood.
	nelp 214- The following commands are recognized (* =>'s unimplemented).
	USER LEFT MODE MSOM* RNTO SITE RND SIZE AUTH
	PASS EFRT RETR MSAM* ABOR SYST XEMD MDTM FBSZ
	ACCT* PASV STOR MRSQ* DELE STAT FWD MLST FROT SMNT* LPSV APPE MRCP* CWD HELP XFWD MLSD CCC
	REIN* EPSV MLFL* ALLO XCWD NOOP CDUP MFMT
	QUIT TYPE MAIL' REST LIST MKD XCUP FEAT
	214 Direct comments to fub-busgbprofbox.
	pasv
	227 Entering Passive Mode (10,130,25,239,217,21)
PUTTY X	550 Oltest.txt: No such file or directory.
	retr Jowa/Oltest.txt
	150 Opening BINARY mode data connection for 'Jowa/Oltest.txt' (0 bytes). 226 Transfer complete.
Connection dosed by remote host	
OK	

⁶ https://cr.yp.to/ftp/retr.html

Upload a file

The process for uploading is the same as the download step and moreover we can directly write in the second window the content of the file to be uploaded. The command to send our file is "stor 02test.txt".

When the second window is open you can write whatever you want, and the data is transferred when this same window is intentionally closed.

You can then for all exercises check your terminal actions on the FileZilla interface. So, you can see that the file has been sent!

