

## How to enable Case Sensitivity on NTFS Guided Exercise

APFS (Apple File System), the file system used by both iOS and Mac Operating Systems, is case sensitive. NTFS (New Technology File System), a file system used for Windows OSs, is case insensitive. As such, iOS images often contain files that conflict when extracted from an archive such as a GrayKey Full File System extraction. During Hexordia's HMFA class in March 2023, a student ran into this exact issue while using a Windows Machine to extract the Magnet User Summit 2022 iOS 15 Full File System image. The iOS image contains two PList files in the same directory with the same name, but with differences in capitalization; namely, com.apple.Prefernces.plist and com.apple.preferences.plist. After the class, Troy Schnack wrote a blog regarding the issue, which can be found here <a href="https://troy4n6.blogspot.com/2023/03/try-to-be-more-sensitive.html">https://troy4n6.blogspot.com/2023/03/try-to-be-more-sensitive.html</a>. Microsoft has additional information regarding case sensitivity here:</a>

To deal with iOS images on an NTFS partition, the destination folder for the extracted contents needs to be case sensitive. To set case sensitivity on a Windows machine, open the command prompt as an administrator.





Create a folder that has no content in it on the drive that the zip file will be extracted. Run command "fsutil.exe file SetCaseSensitiveInfo <insert path> enable" and hit "enter". Be sure to use the path from the folder that is being updated.



There should be a resulting "reply" in the command prompt that says "Case sensitive attribute on directory <path> is enabled."

\*\*To test case sensitivity, navigate to the folder that was just programmed and create two .txt files, one all lower case and one all upper case. Both files created should be present without errors.

Desktop > Test			
Name	Date modified	Туре	Size
Test.txt	7/25/2023 2:10 PM	Text Document	0 KB
	1/25/2025 2.10 FW	Text Document	UKD

Once these steps have been completed, we can now extract the zip file from the iOS image.



## **USING 7ZIP GUIDED EXERCISE**

#### TO START, PLEASE DOWNLOAD 7ZIP FROM https://www.7-zip.org/download.html

Prior to installation, verify the hash value to the known good value from the syllabus for students enrolled in the HMFA Virtual Live course. The MD5 hash value for the 7z2201-x64.exe is a6a0f7c173094f8dafef996157751ecf

Select the file to be extracted. Right click on file, select "7-zip" and then "Extract Here".



The extraction may take a few minutes to complete as this is a Gray Key extraction and contains multiple types of files, as well as a pdf file about the extraction. The forensic image itself is a compressed file. The .zip file can be loaded into many tools, such as iLEAPP. However, in order to fully navigate in tools like Autopsy, it is necessary to extract the .zip file so that the contents can be loaded.

Elapsed time:	00:00:18	Total size:	8317 ME
Remaining time:	00:02:11	Speed:	55 MB/
Files:	1	Processed	1009 ME
		Compressed size:	682 ME
		Compression ratio:	679
Extracting			

Double click or right click and select "open" the extracted file to open its contents.



> T7 Shield (E:) > Archive > Archive > Walkthrough

Name	Date modified	Туре	Size
Jess_CTF_iPhone8	2/14/2022 2:45 PM	File folder	
2022 CTF - iOS Full File System.zip	12/7/2022 9:01 AM	Compressed (zipped) F	4,601,527 KB

#### There is another zipped file within this folder that needs to be extracted.

T7 Shield (E:) > Archive > Archive > Walkthrough > Je	ess_CTF_iPhone8		
Name	Date modified	Туре	Size
🛃 fb028ddefa8af7df5b12d3e729f075d150637a31.pdf	2/14/2022 2:43 PM	Adobe Acrobat Docum	70 K
h028ddefa8af7df5b12d3e729f075d150637a31_files_full	2/14/2022 2:34 PM	Compressed (zipped) F	8,515,278 K
b028ddefa8af7df5b12d3e729f075d150637a31_keychai	2/14/2022 2:43 PM	PLIST File	1,299 K
fb028ddefa8af7df5b12d3e729f075d150637a31_passwor	2/14/2022 2:43 PM	Text Document	54 KI
fb028ddefa8af7df5b12d3e729f075d150637a31_pchistor	2/14/2022 2:43 PM	Text Document	1 K

### Repeat the first step, right click and select "7-zip" and then "Extract File"

	— « iOS Magnet 2023 > 2022 CTF - i		Extract All	0	Search less CTE iDhones	0
			7-Zip >		Open archive	
	Name	5	Select Left Folder for Compare		Open archive	
	🛃 fb028ddefa8af7df5b12d3e729f07	U	Scan		Extract files	
۲	b028ddefa8af7df5b12d3e729f07	۵	Shred		Extract Here	
Þ	b028ddefa8af7df5b12d3e729f07		Pin to Start		Extract to "fb028ddefa8af7df5b12d3	e729f075d150637a31_files_full\"
Þ	fb028ddefa8af7df5b12d3e729f07		Edit with Notenad++		Test archive	
۴	fb028ddefa8af7df5b12d3e729f07	•			Add to archive	

Now select the path for "Extract to" and select the folder that was programmed for case sensitivity.



# **MOBILE FORENSICS**

I

iOS Magnet 2023 > 2022 CTF - iOS Full File	e System > Jess_CTF_iPhone8 ~ C Search Jess_CTF_iPhone8	<u>د</u> م
Name	Date modified Type Size	
🚖 fb028ddefa8af7df5b12d3e729f075d1506	2/14/2022 1:42 DM Adoba Account D 70 VD	defa8a X
fb028ddefa8af7df5b12d3e729f075d1506	2/14/2	
b028ddefa8af7df5b12d3e729f075d1506	2/14/2 Extract to:	
fb028ddefa8af7df5b12d3e729f075d1506	2/14/2 C:\Users\sarah\Desktop\Extracted Image	✓ …
fb028ddefa8af7df5b12d3e729f075d1506	2/14/2 b028ddefa8af7df5b12d3e729f075d150637a31_fi Password	
	Path mode:	
	Full pathnames	
	Eliminate duplication of root folder	
	Overwrite mode: Restore file security	
	Ask before overwrite V	
	OK Cancel	нер

### This may take a few minutes to complete.

et 2023 a31_files_full.zip	)	- 0	×
00:00:30	Total size:		8272 MB
00:00:30	Speed:		135 MB/s
5017	Processed:		4091 MB
	Compressed size:		4091 MB
	Compression ratio:		100%
a\AppliPINDiskCache.PIN %2Fsnoovatar%2 runways'	NRemotelmageManagerCache %2F6vOjO8Bc5v4_Asset_72_5	e\ 552x%2Epng	
Background	Pause	Cance	el l
	et 2023 a31_files_full.zip 00:00:30 00:00:30 5017 a\AppliPINDiskCache.PIN %2Fsnoovatar%2 runways	et 2023 a31_files_full.zip 00:00:30 Total size: 00:00:30 Speed: 5017 Processed: Compressed size: Compression ratio: a\AppliPINDiskCache.PINRemoteImageManagerCache %2Fsnoovatar%2 runways%2F6vOjO8Bc5v4_Asset_72_5	et 2023 a31_files_full.zip – 00:00:30 Total size: 00:00:30 Speed: 5017 Processed: Compressed size: Compression ratio: a\AppliPINDiskCache.PINRemoteImageManagerCache\ %2Fsnoovatar%2 runways%2F6vOjO8Bc5v4_Asset_72_552x%2Epng

# Resulting Folder - the folder should still be called fb028ddefa8af7df5b12d3e729f075d150637a31\_files\_full just in an unzipped state.

Desktop > Extracted Image	ge	~ C
Name	^	Date modified
📒 fb028ddefa8af7df5b12d3e	729f075d150637a31_files_full	7/25/2023 1:08 PM

### Once complete, double check path

fb028ddefa8af7df5b12d3e729f075d150637a31\_files\_full\private\var\mobile\Library\Preferences to make sure both files were unzipped.

com.apple.Preferences.plist	2/14/2022 12:06 PM	PLIST File	2 KB
com.apple.preferences.plist	1/6/2022 5:41 PM	PLIST File	1 KB

Once these steps have been completed, this forensic image can be processed in Autopsy. For instructions on how to process a forensic image in Autopsy please review: <u>https://www.hexordia.com/s/Autopsy\_Walkthrough\_Final.pdf</u>



## **TROUBLESHOOTING AND ERROR MESSAGES**

## **EXFAT ERROR**

Ensure the extraction is to an NTFS partition. If the destination folder is on an exFAT partition, fsutil.exe cannot be used to create a case sensitive folder.

C:\Windows\System32\cmd.e ×	+ ~
Microsoft Windows [Versio	n 10.0.22621.1992]
(c) Microsoft Corporation	. All rights reserved.
C:\Windows\System32>fsuti	l.exe file SetCaseSensitiveInfo D:\Test enable
A volume supporting case-	sensitivity is required for this operation (e.g., a local REFS or NTFS volume).

Another way to identify if the destination folder is incorrect is if Windows prompts that there are files with the same names, that the destination already contains the same file or to select which file to keep. Upon seeing the prompt below, one should start over and ensure the destination folder is set as case sensitive using the steps in this document.





## **FSUTIL.EXE NOT RECOGNIZED**

There may be the error "fsutil.exe file SetCaseSensitiveInfo <path> enable and an error occurs 'fsutil.exe' is not recognized as an internal or external command, operable program or batch file", then run the command again from the location that the "fsutil.exe" file is located in. Run the command from the location of the fsutil.exe file.

Command Prompt ×	+ ~
Microsoft Windows [Versi	on 10.0.22621.1992]
(c) Microsoft Corporatio	n. All rights reserved.
C:\Users\sarah>fsutil.ex	e file SetCaseSensitiveInfo C:\Users\sarah\Desktop\Test enable
'fsutil.exe' is not reco	gnized as an internal or external command,
operable program or batc	h file.

In the computers search type "fsutil" and select "open file location"

Doot motob		
<b>fsutil</b> Run command		
Search work and web		<b>fsutil</b> Run command
<ul> <li>fsutil - See work and web results</li> <li>fsutil cmd</li> </ul>	>	[∠] Open
	>	<ul> <li>Run as administrator</li> <li>Open file location</li> </ul>
<ul> <li>fsutil repair</li> <li>fsutil file createnew</li> </ul>	> >	
♀ fsutil <b>dirty query</b>	>	
Stutil windows Stutil behavior set	> >	
disableencryption 0		
648 words LSZ Text Predictions: On LSZ Accessibility		e
Q fsutil	J	



Once the location is open, in the address bar type in "cmd" to open the command prompt.

	🚞 cmd			$\rightarrow$	Search System32	
L	CMD		L			
	cmd.exe			Гуре		Size
	cmdext.dll					
	cmdial32.dll		/ /	Application extension		340 KB
'	cmdkey.exe	ey.exe			ion extension	276 KB
	cmdl32.exe			Application extension		100 KB
,	Search for "cmd"		, I	Applicat	ion	36 KB
			,	Applicat	ion	131 KB
	💼 fsmgmt.msc	5/7/2022 1:19 AM	I	Microsoft Common Con		142 KB
,	FsNVSDeviceSource.dll	5/7/2022 1:20 AM	/	Application extension		748 KB
	🛞 fsquirt.exe	5/7/2022 1:19 AM	/	Applicat	ion	164 KB
	fsutil.exe	5/7/2022 1:20 AM	1	Applicat	ion	250 KB

Run the command: "fsutil.exe file SetCaseSensitiveInfo <path> enable"

