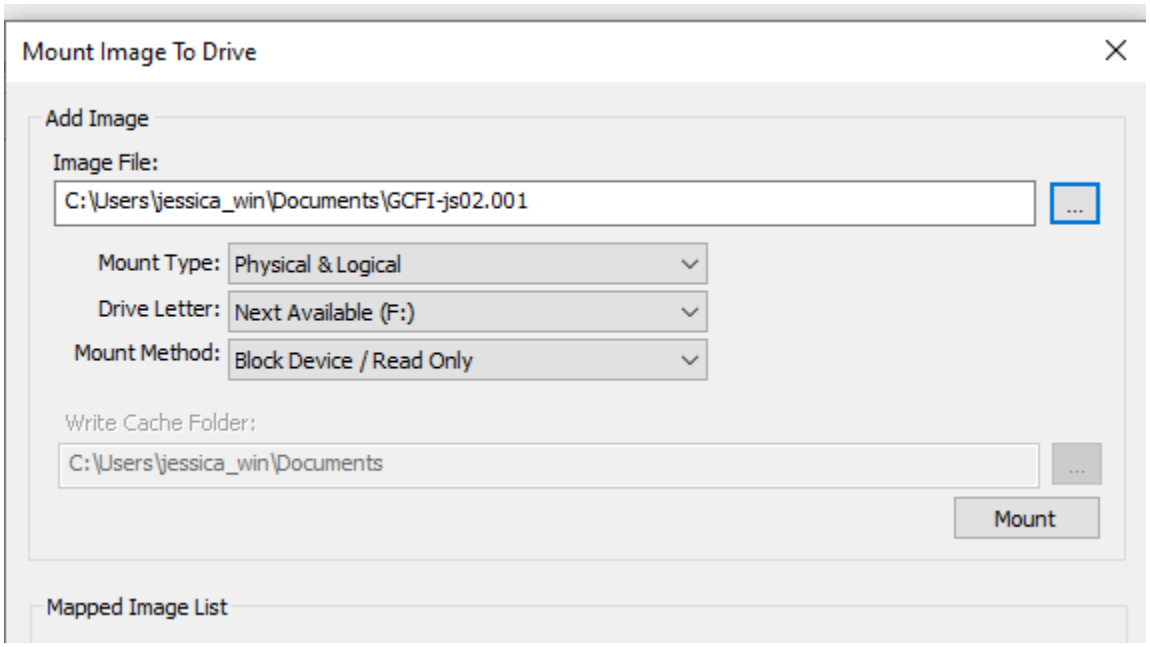
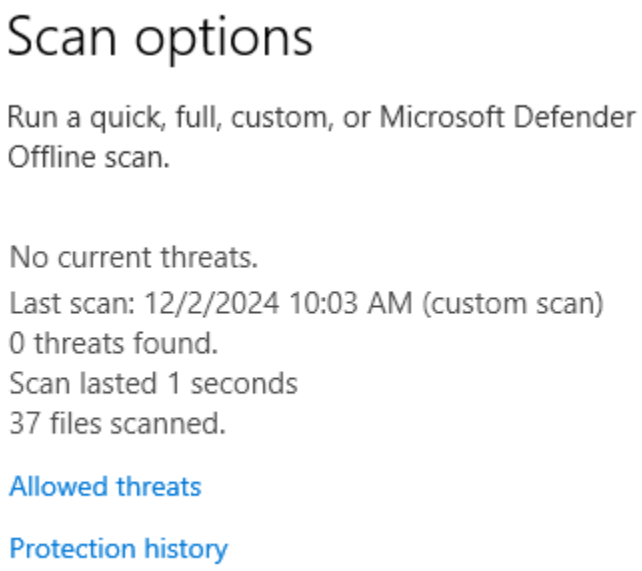
Task 1: Malware Case

Step 1: Mount Image



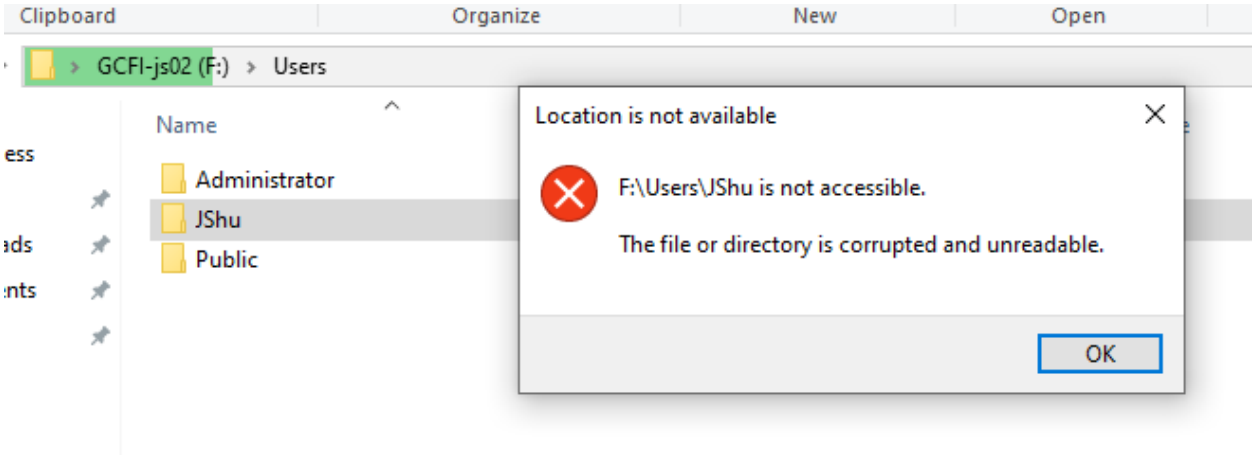
Successfully mounted the image onto FTK Imager.

Step 2: Antivirus Scan

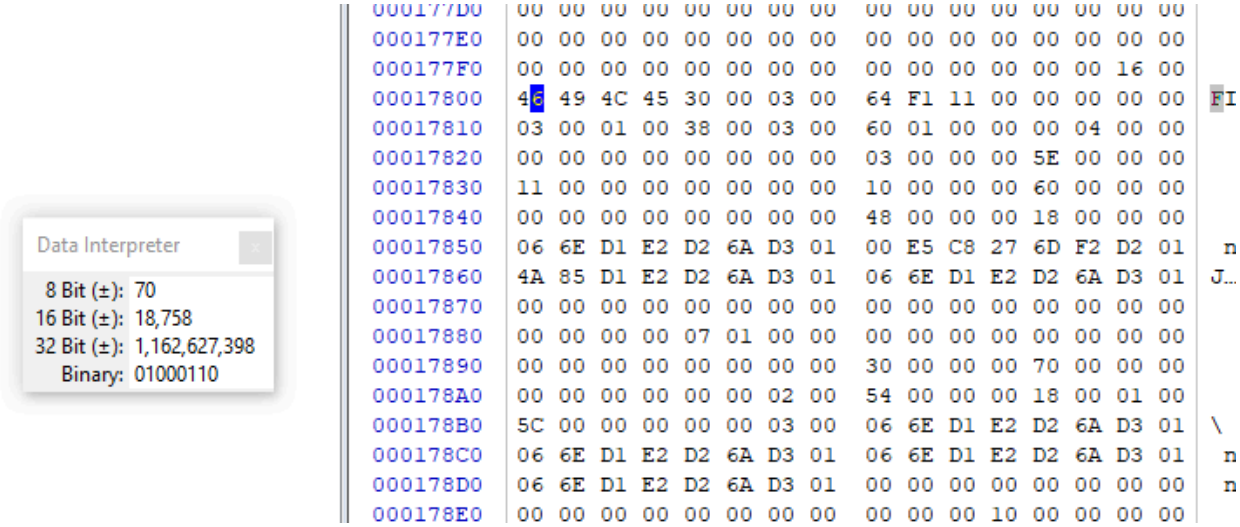


Successfully ran a scan on the mounted image, resulting in no threats found.

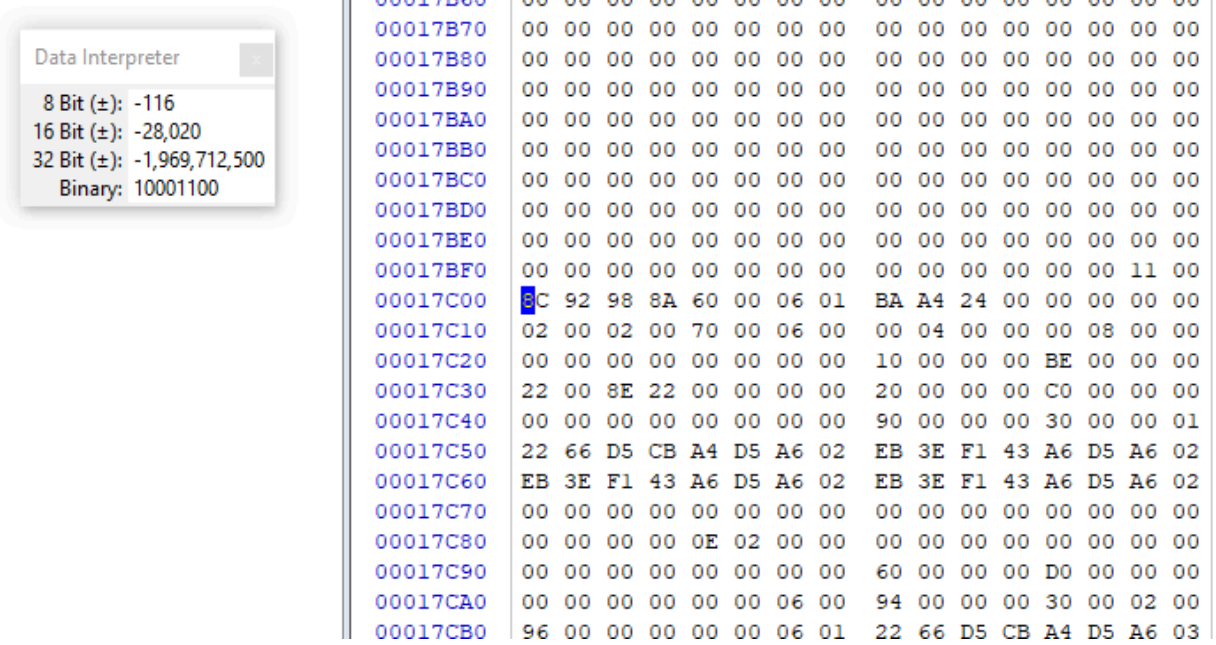
Step 3: Analyze File System



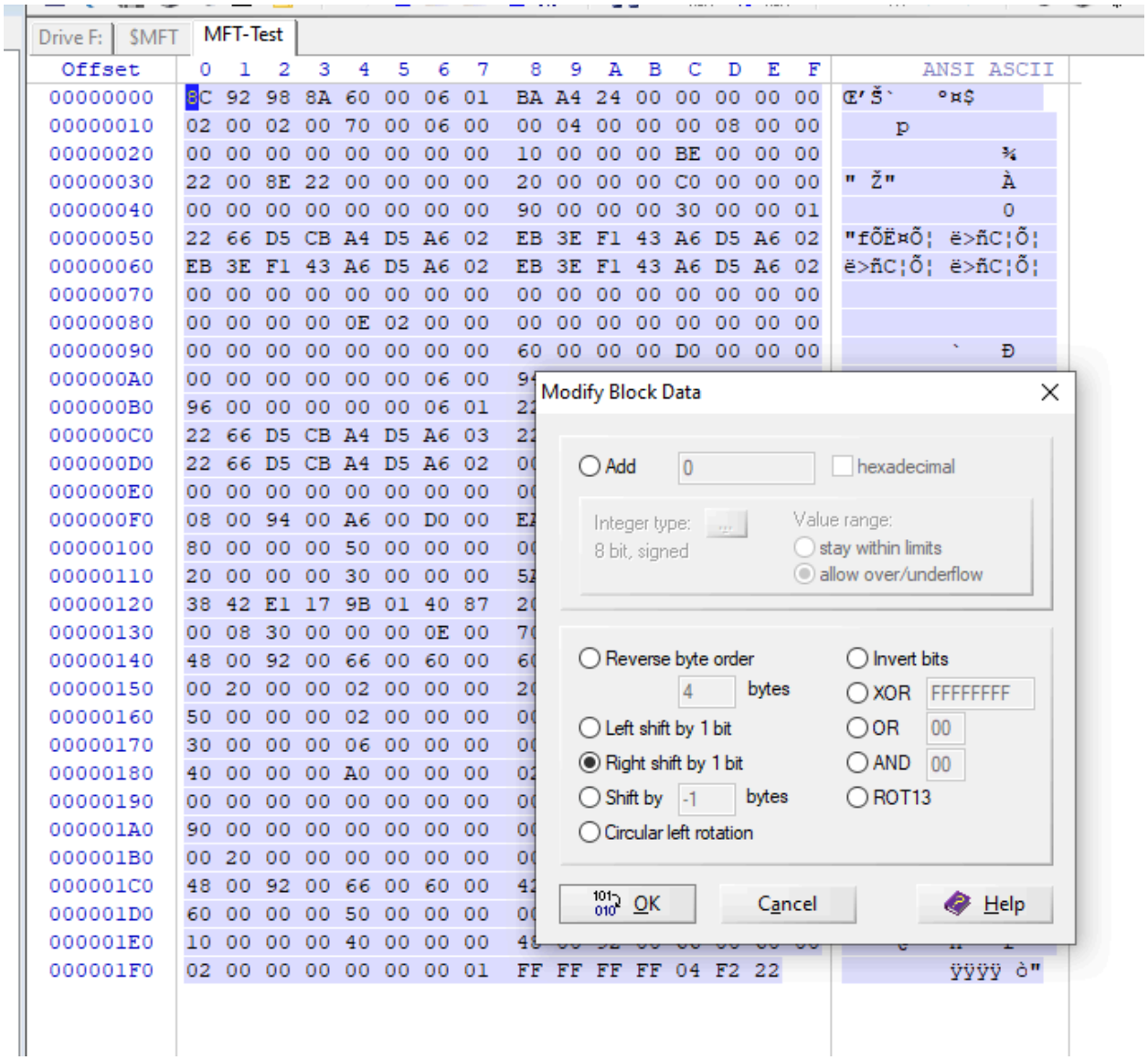
The JShu User folder is not accessible through usual methods.



Opened the disk in Winhex to find the underlying reason why the folder won't open. At this offset, we see that a file record starts with FILE0.



At the beginning of the next file, we see that the binary encoding might have been bit-shifting. This requires further examination.

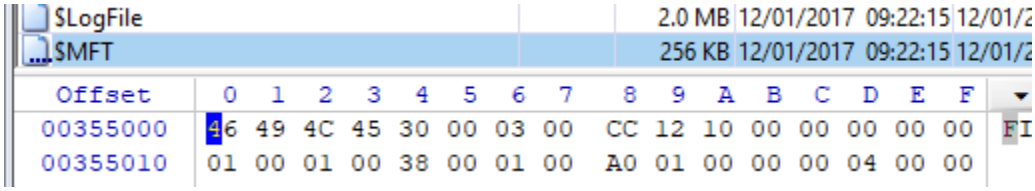


After copying the entire file's contents into a separate file, we will now test by shifting the bits to the right by 1.

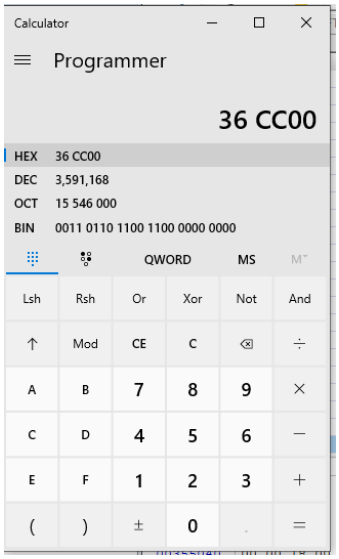
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	46	49	4C	45	30	00	03	00	DD	52	12	00	00	00	00	00	FILE0 ÝR
00000010	01	00	01	00	38	00	03	00	00	02	00	00	00	04	00	00	8
00000020	00	00	00	00	00	00	00	00	08	00	00	00	5F	00	00	00	_
00000030	11	00	47	11	00	00	00	00	10	00	00	00	60	00	00	00	G `
00000040	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00	H
00000050	91	33	6A	E5	D2	6A	D3	01	75	9F	78	A1	D3	6A	D3	01	‘3jåÒjÓ uŸx¡ÓjÓ
00000060	75	9F	78	A1	D3	6A	D3	01	75	9F	78	A1	D3	6A	D3	01	uŸx¡ÓjÓ uŸx¡ÓjÓ
00000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000080	00	00	00	00	07	01	00	00	00	00	00	00	00	00	00	00	
00000090	00	00	00	00	00	00	00	00	30	00	00	00	68	00	00	00	0 h
000000A0	00	00	00	00	00	00	03	00	4A	00	00	00	18	00	01	00	J
000000B0	4B	00	00	00	00	00	03	00	91	33	6A	E5	D2	6A	D3	01	K ‘3jåÒjÓ
000000C0	91	33	6A	E5	D2	6A	D3	01	91	33	6A	E5	D2	6A	D3	01	‘3jåÒjÓ ‘3jåÒjÓ
000000D0	91	33	6A	E5	D2	6A	D3	01	00	00	00	00	00	00	00	00	‘3jåÒjÓ
000000E0	00	00	00	00	00	00	00	00	00	00	00	10	00	00	00	00	
000000F0	04	00	4A	00	53	00	68	00	75	00	00	00	00	00	00	00	J S h u
00000100	40	00	00	00	28	00	00	00	00	00	00	00	00	00	04	00	@ (
00000110	10	00	00	00	18	00	00	00	2D	22	68	1C	A8	D5	E7	11	-"h ¨Õç
00000120	9C	21	70	8B	CD	80	A0	43	90	00	00	00	58	00	00	00	œ!p‹Í€ C X
00000130	00	04	18	00	00	00	07	00	38	00	00	00	20	00	00	00	8
00000140	24	00	49	00	33	00	30	00	30	00	00	00	01	00	00	00	$ I 3 0 0
00000150	00	10	00	00	01	00	00	00	10	00	00	00	28	00	00	00	(
00000160	28	00	00	00	01	00	00	00	00	00	00	00	00	00	00	00	(
00000170	18	00	00	00	03	00	00	00	00	00	00	00	00	00	00	00	
00000180	A0	00	00	00	50	00	00	00	01	04	40	00	00	00	05	00	P @
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000001A0	48	00	00	00	00	00	00	00	00	10	00	00	00	00	00	00	H
000001B0	00	10	00	00	00	00	00	00	00	10	00	00	00	00	00	00	
000001C0	24	00	49	00	33	00	30	00	21	01	BA	09	00	00	00	00	$ I 3 0 ! º
000001D0	B0	00	00	00	28	00	00	00	00	04	18	00	00	00	06	00	° (
000001E0	08	00	00	00	20	00	00	00	24	00	49	00	33	00	30	00	$ I 3 0
000001F0	01	00	00	00	00	00	00	00	FF	FF	FF	FF	82	79	11	00	ÿÿÿÿ,y

Here is the file shifted by 1 bit to the right.

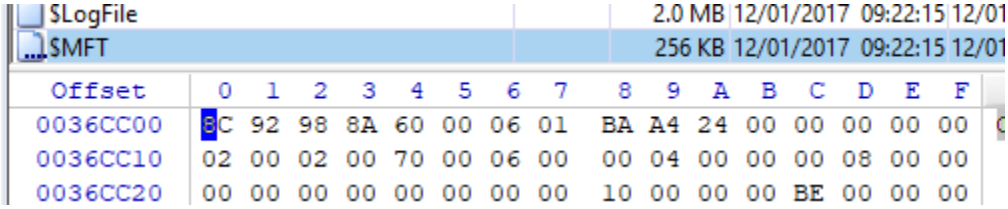
Step 4: Find the Absolute Path of Corrupted File



The MFT file starts at offset 355000 in the image disk.

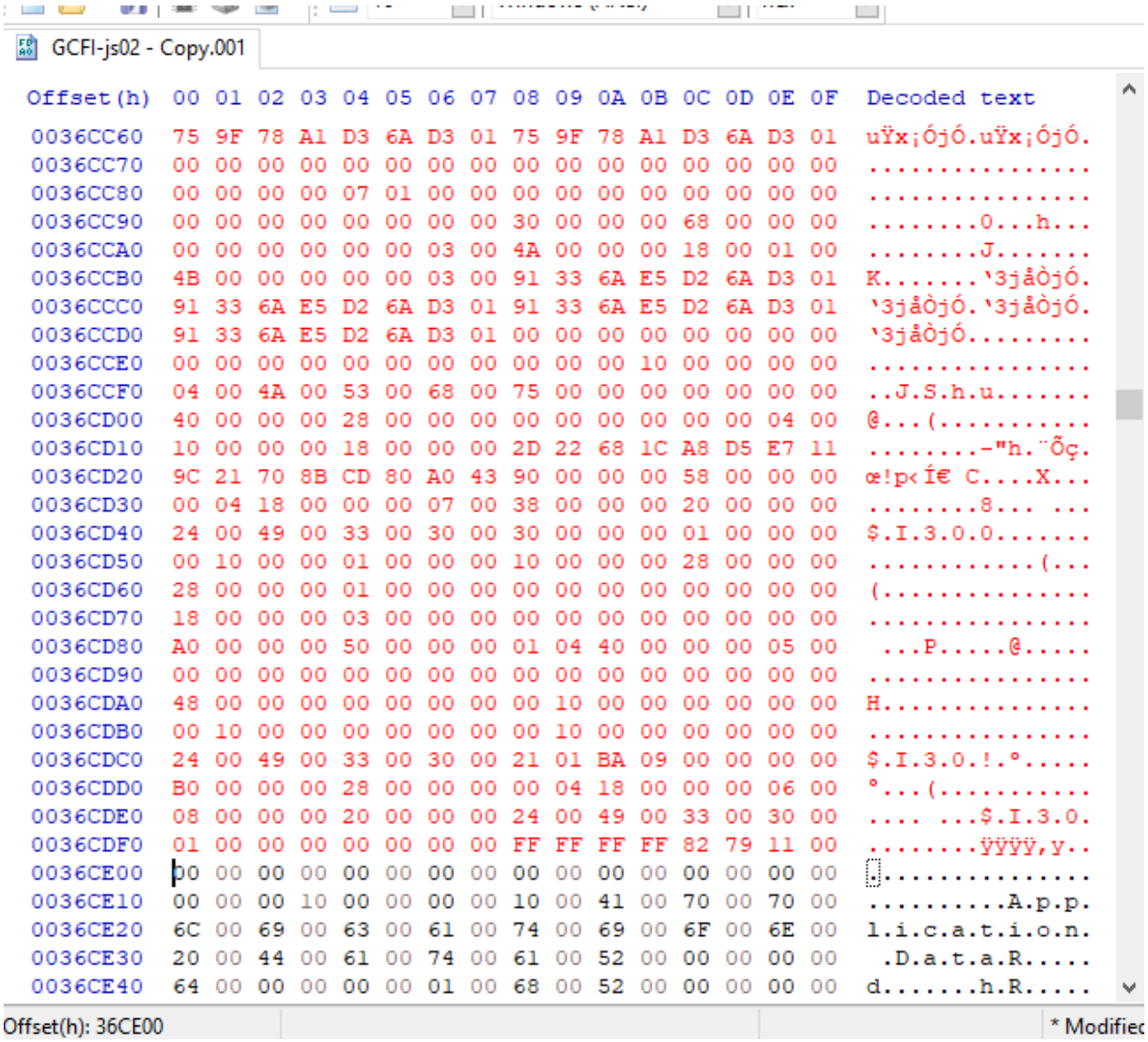


The absolute address of the corrupted folder is at offset 36CC00.

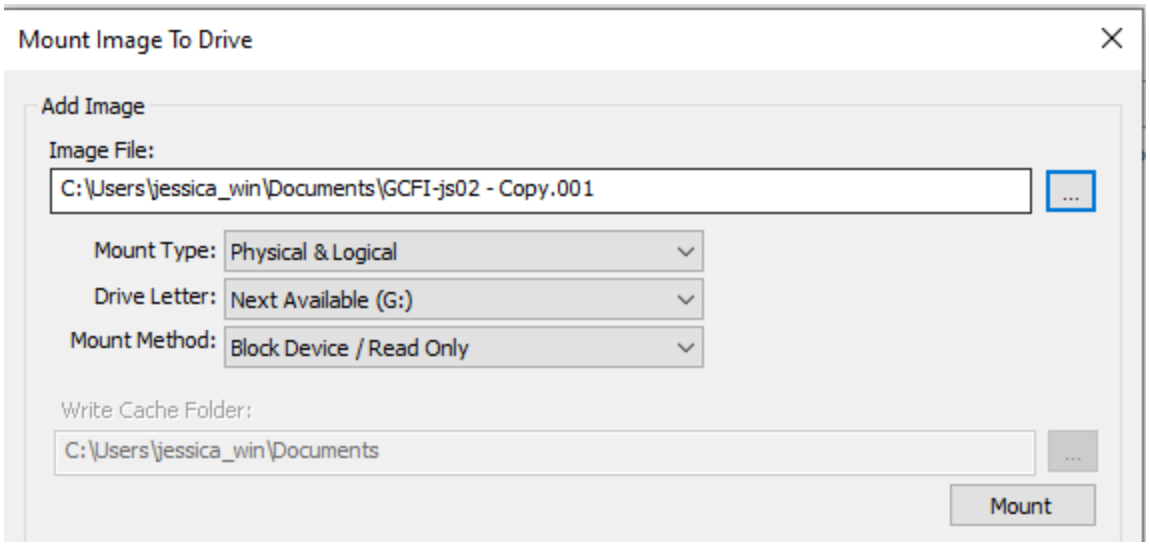


Successfully jumped to correct offset of corrupted file.

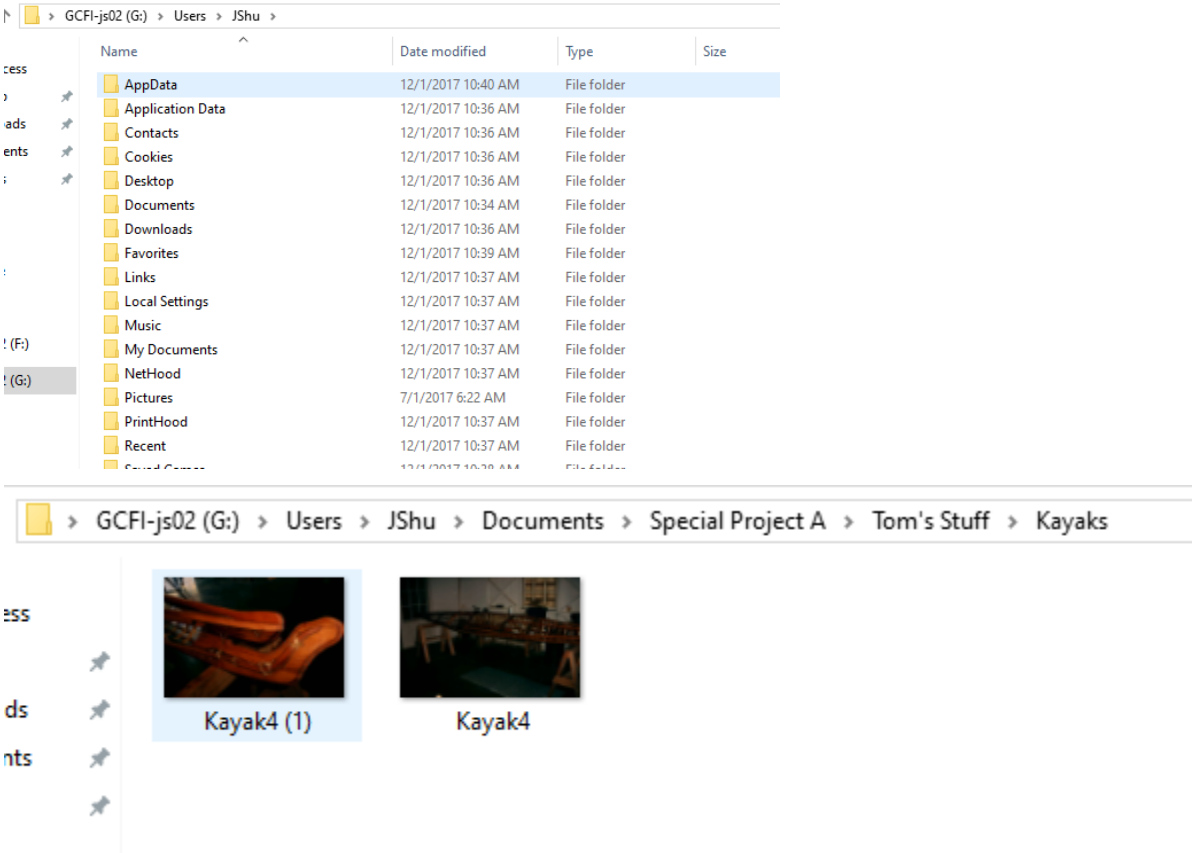
Step 5: Repair Image



Successfully pasted plaintext data onto copy of the image in HxD.



Mounted copy of disk with repaired image.



Successfully opened corrupted JShu folder.

Step 6: Conclusion

In this case, we used WinHex, FTK Imager, and HxD to examine a disk image, repair corrupted data, and determine the cause of the corruption. Throughout the process, the disk image was able to be opened, however a particular user's folder was unable to be accessed. Thus, WinHex and HxD were used to determine the absolute address of the corruption, reverse the alterations done on it, and finally open and access the corrupted data. It was found the JShu's user folder was bit shifted 1 bit to the right and after correcting that, the folder was able to open without a problem. After opening his user folder, we were able to access his images, where we found his kayaks. It is possible that this corruption was contrived by malware, since the entirety of JShu's folder was corruptedandnot just specific files or folders.