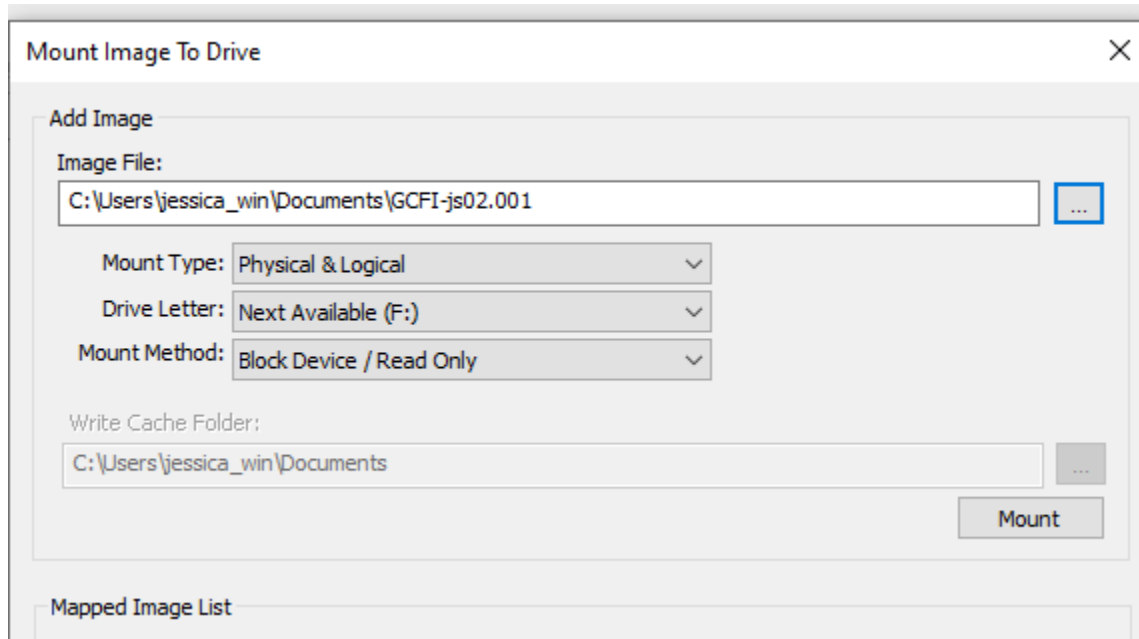


Task 1: Malware Case

Step 1: Mount Image



Successfully mounted the image onto FTK Imager.

Step 2: Antivirus Scan

Scan options

Run a quick, full, custom, or Microsoft Defender
Offline scan.

No current threats.

Last scan: 12/2/2024 10:03 AM (custom scan)

0 threats found.

Scan lasted 1 seconds

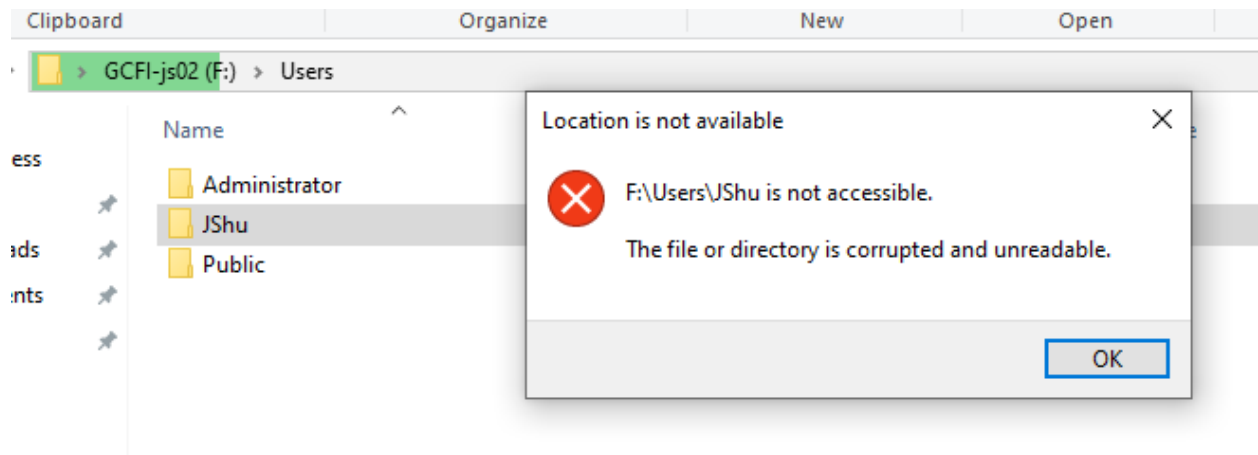
37 files scanned.

[Allowed threats](#)

[Protection history](#)

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.

Data Interpreter

8 Bit (±): 70

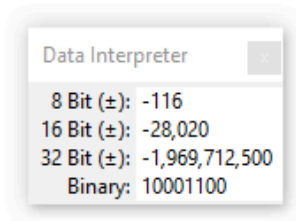
16 Bit (±): 18,758

32 Bit (±): 1,162,627,398

Binary: 01000110

000177D0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
000177E0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
000177F0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 16	
00017800	46 49 4C 45 30 00 03 00	64 F1 11 00 00 00 00 00	FI
00017810	03 00 01 00 38 00 03 00	60 01 00 00 00 04 00 00	
00017820	00 00 00 00 00 00 00 00	03 00 00 00 5E 00 00 00	
00017830	11 00 00 00 00 00 00 00	10 00 00 00 60 00 00 00	
00017840	00 00 00 00 00 00 00 00	48 00 00 00 18 00 00 00	
00017850	06 6E D1 E2 D2 6A D3 01	00 E5 C8 27 6D F2 D2 01	n
00017860	4A 85 D1 E2 D2 6A D3 01	06 6E D1 E2 D2 6A D3 01	J..
00017870	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00017880	00 00 00 00 07 01 00 00	00 00 00 00 00 00 00 00	
00017890	00 00 00 00 00 00 00 00	30 00 00 00 70 00 00 00	
000178A0	00 00 00 00 00 00 02 00	54 00 00 00 18 00 01 00	
000178B0	5C 00 00 00 00 00 03 00	06 6E D1 E2 D2 6A D3 01	\
000178C0	06 6E D1 E2 D2 6A D3 01	06 6E D1 E2 D2 6A D3 01	n
000178D0	06 6E D1 E2 D2 6A D3 01	00 00 00 00 00 00 00 00	n
000178E0	00 00 00 00 00 00 00 00	00 00 00 10 00 00 00 00	

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.



00017B60	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00017B70	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00017B80	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00017B90	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00017BA0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00017BB0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00017BC0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00017BD0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00017BE0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00017BF0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 11 00
00017C00	8C 92 98 8A 60 00 06 01	BA A4 24 00 00 00 00 00
00017C10	02 00 02 00 70 00 06 00	00 04 00 00 00 08 00 00
00017C20	00 00 00 00 00 00 00 00	10 00 00 00 BE 00 00 00
00017C30	22 00 8E 22 00 00 00 00	20 00 00 00 C0 00 00 00
00017C40	00 00 00 00 00 00 00 00	90 00 00 00 30 00 00 01
00017C50	22 66 D5 CB A4 D5 A6 02	EB 3E F1 43 A6 D5 A6 02
00017C60	EB 3E F1 43 A6 D5 A6 02	EB 3E F1 43 A6 D5 A6 02
00017C70	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00017C80	00 00 00 00 0E 02 00 00	00 00 00 00 00 00 00 00
00017C90	00 00 00 00 00 00 00 00	60 00 00 00 D0 00 00 00
00017CA0	00 00 00 00 00 00 06 00	94 00 00 00 30 00 02 00
00017CB0	96 00 00 00 00 00 06 01	22 66 D5 CB A4 D5 A6 03

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

The screenshot shows a hex editor window with the following data:

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI	ASCII
00000000	8C	92	98	8A	60	00	06	01	BA	A4	24	00	00	00	00	00	0	Š
00000010	02	00	02	00	70	00	06	00	00	04	00	00	00	08	00	00	p	
00000020	00	00	00	00	00	00	00	00	10	00	00	00	BE	00	00	00	%	
00000030	22	00	8E	22	00	00	00	00	20	00	00	00	C0	00	00	00	" Z"	À
00000040	00	00	00	00	00	00	00	00	90	00	00	00	30	00	00	01	o	
00000050	22	66	D5	CB	A4	D5	A6	02	EB	3E	F1	43	A6	D5	A6	02	"fÖËxÖ; ë>ñC;Ö;	
00000060	EB	3E	F1	43	A6	D5	A6	02	EB	3E	F1	43	A6	D5	A6	02	ë>ñC;Ö; ë>ñC;Ö;	
00000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00000080	00	00	00	00	0E	02	00	00	00	00	00	00	00	00	00	00		
00000090	00	00	00	00	00	00	00	00	60	00	00	00	D0	00	00	00	`	Đ
000000A0	00	00	00	00	00	00	06	00	90	00	00	00	00	00	00	00		
000000B0	96	00	00	00	00	00	06	01	20	00	00	00	00	00	00	00		
000000C0	22	66	D5	CB	A4	D5	A6	03	20	00	00	00	00	00	00	00		
000000D0	22	66	D5	CB	A4	D5	A6	02	00	00	00	00	00	00	00	00		
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
000000F0	08	00	94	00	A6	00	D0	00	EA	00	00	00	00	00	00	00		
00000100	80	00	00	00	50	00	00	00	00	00	00	00	00	00	00	00		
00000110	20	00	00	00	30	00	00	00	52	00	00	00	00	00	00	00		
00000120	38	42	E1	17	9B	01	40	87	20	00	00	00	00	00	00	00		
00000130	00	08	30	00	00	00	0E	00	70	00	00	00	00	00	00	00		
00000140	48	00	92	00	66	00	60	00	60	00	00	00	00	00	00	00		
00000150	00	20	00	00	02	00	00	00	20	00	00	00	00	00	00	00		
00000160	50	00	00	00	02	00	00	00	00	00	00	00	00	00	00	00		
00000170	30	00	00	00	06	00	00	00	00	00	00	00	00	00	00	00		
00000180	40	00	00	00	A0	00	00	00	02	00	00	00	00	00	00	00		
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
000001A0	90	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
000001B0	00	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
000001C0	48	00	92	00	66	00	60	00	42	00	00	00	00	00	00	00		
000001D0	60	00	00	00	50	00	00	00	00	00	00	00	00	00	00	00		
000001E0	10	00	00	00	40	00	00	00	48	00	00	00	00	00	00	00		
000001F0	02	00	00	00	00	00	00	01	FF	FF	FF	FF	04	F2	22		ÿÿÿÿ ò"	

The 'Modify Block Data' dialog box is open, showing the following options:

- ☐ Add: 0 (hexadecimal)
- Integer type: 8 bit, signed
- Value range: ☐ stay within limits, ☒ allow over/underflow
- ☐ Reverse byte order
- ☐ Invert bits
- ☐ XOR: FFFFFFFF
- ☐ OR: 00
- ☐ AND: 00
- ☐ ROT13
- ☒ Right shift by 1 bit
- ☐ Left shift by 1 bit
- ☐ Shift by -1 bytes
- ☐ Circular left rotation

Buttons: OK, Cancel, Help.

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

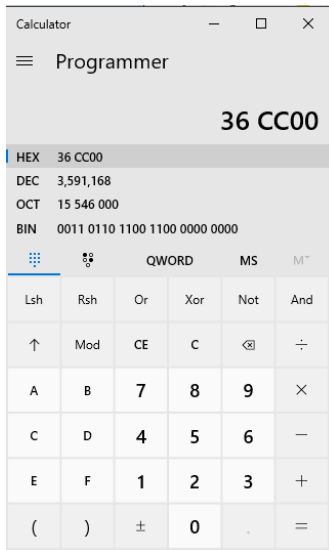
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI	ASCII
00000000	46	49	4C	45	30	00	03	00	DD	52	12	00	00	00	00	00	FILE0	ÝR
00000010	01	00	01	00	38	00	03	00	00	02	00	00	00	04	00	00		8
00000020	00	00	00	00	00	00	00	00	08	00	00	00	5F	00	00	00		
00000030	11	00	47	11	00	00	00	00	10	00	00	00	60	00	00	00	G	
00000040	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	'3jåðjÓ	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	o	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	'3jåðjÓ
000000C0	91	33	6A	E5	D2	6A	D3	01	91	33	6A	E5	D2	6A	D3	01	'3jåðjÓ	'3jåðjÓ
000000D0	91	33	6A	E5	D2	6A	D3	01	00	00	00	00	00	00	00	00	'3jåðjÓ	
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 "Öç
00000120	9C	21	70	8B	CD	80	A0	43	90	00	00	00	58	00	00	00	æ!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 ! °	
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

SLogFile		2.0 MB		12/01/2017 09:22:15		12/01/2017										
SMFT		256 KB		12/01/2017 09:22:15		12/01/2017										
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00355000	46	49	4C	45	30	00	03	00	CC	12	10	00	00	00	00	00
00355010	01	00	01	00	38	00	01	00	A0	01	00	00	00	04	00	00

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



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

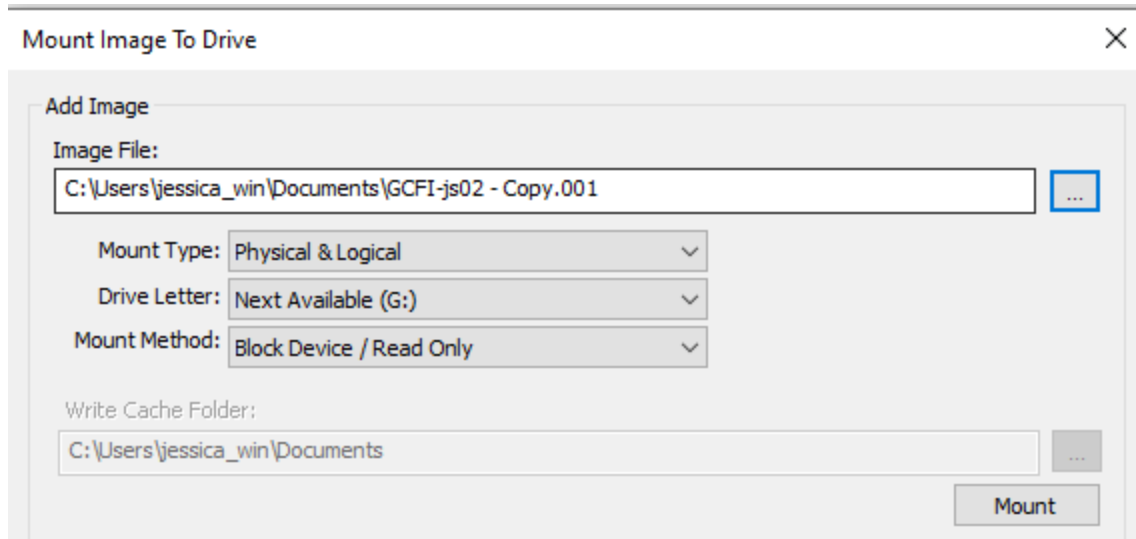
SLogFile		2.0 MB		12/01/2017 09:22:15		12/01/2017										
SMFT		256 KB		12/01/2017 09:22:15		12/01/2017										
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0036CC00	8C	92	98	8A	60	00	06	01	BA	A4	24	00	00	00	00	00
0036CC10	02	00	02	00	70	00	06	00	00	04	00	00	00	08	00	00
0036CC20	00	00	00	00	00	00	00	00	10	00	00	00	BE	00	00	00

Successfully jumped to correct offset of corrupted file.

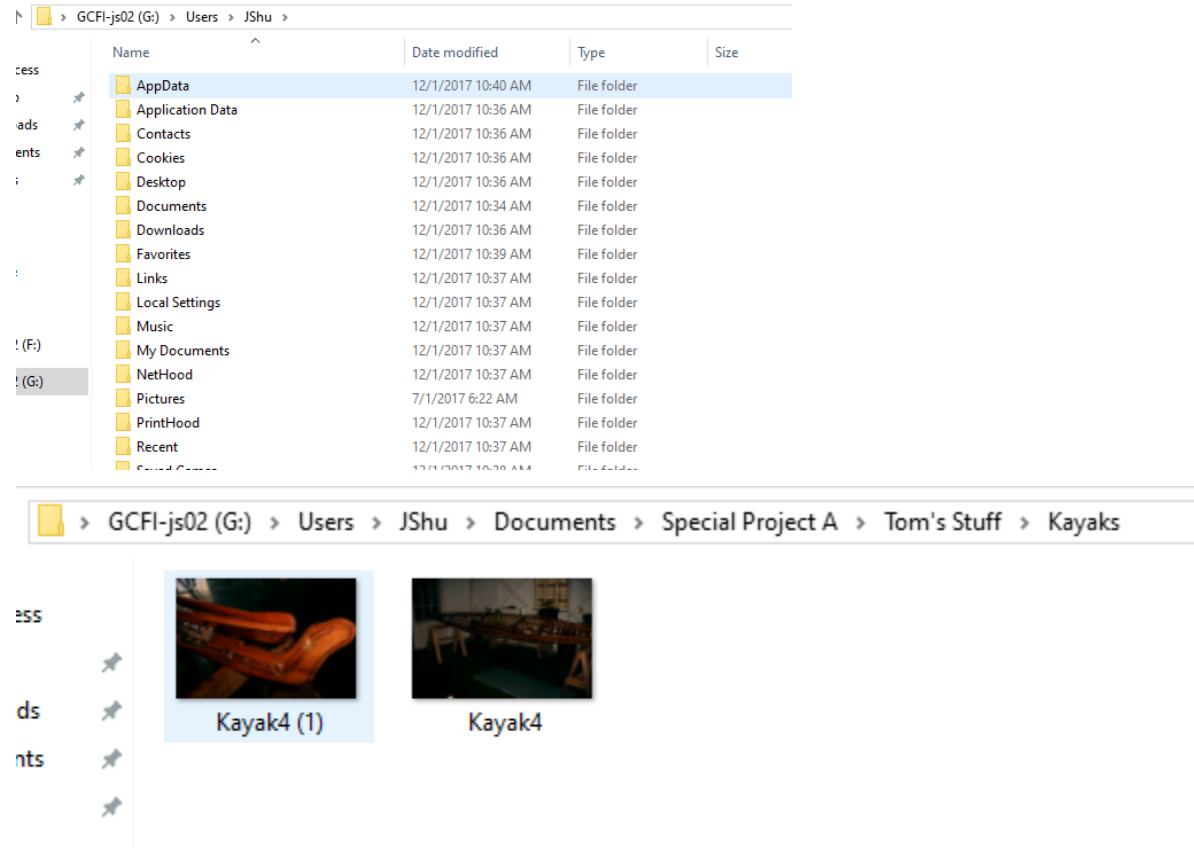
Step 5: Repair Image

GCFI-js02 - Copy.001																	Decoded text
Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
0036CC60	75	9F	78	A1	D3	6A	D3	01	75	9F	78	A1	D3	6A	D3	01	uÿx;ÓjÓ.uÿx;ÓjÓ.
0036CC70	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0036CC80	00	00	00	00	07	01	00	00	00	00	00	00	00	00	00	00
0036CC90	00	00	00	00	00	00	00	00	30	00	00	00	68	00	00	000...h...
0036CCA0	00	00	00	00	00	00	03	00	4A	00	00	00	18	00	01	00J.....
0036CCB0	4B	00	00	00	00	00	03	00	91	33	6A	E5	D2	6A	D3	01	K.....'3jãÒjÓ.
0036CCC0	91	33	6A	E5	D2	6A	D3	01	91	33	6A	E5	D2	6A	D3	01	'3jãÒjÓ.'3jãÒjÓ.
0036CCD0	91	33	6A	E5	D2	6A	D3	01	00	00	00	00	00	00	00	00	'3jãÒjÓ.....
0036CCE0	00	00	00	00	00	00	00	00	00	00	00	10	00	00	00	00
0036CCF0	04	00	4A	00	53	00	68	00	75	00	00	00	00	00	00	00	..J.S.h.u.....
0036CD00	40	00	00	00	28	00	00	00	00	00	00	00	00	00	00	04	@... (.....
0036CD10	10	00	00	00	18	00	00	00	2D	22	68	1C	A8	D5	E7	11-"h."Öç.
0036CD20	9C	21	70	8B	CD	80	A0	43	90	00	00	00	58	00	00	00	æ!p<í€ C....X...
0036CD30	00	04	18	00	00	00	07	00	38	00	00	00	20	00	00	008... ..
0036CD40	24	00	49	00	33	00	30	00	30	00	00	00	01	00	00	00	\$.I.3.0.0.....
0036CD50	00	10	00	00	01	00	00	00	10	00	00	00	28	00	00	00 (...
0036CD60	28	00	00	00	01	00	00	00	00	00	00	00	00	00	00	00	(.....
0036CD70	18	00	00	00	03	00	00	00	00	00	00	00	00	00	00	00
0036CD80	A0	00	00	00	50	00	00	00	01	04	40	00	00	00	05	00	...P.....@.....
0036CD90	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0036CDA0	48	00	00	00	00	00	00	00	10	00	00	00	00	00	00	00	H.....
0036CDB0	00	10	00	00	00	00	00	00	10	00	00	00	00	00	00	00
0036CDC0	24	00	49	00	33	00	30	00	21	01	BA	09	00	00	00	00	\$.I.3.0.!.°.....
0036CDD0	B0	00	00	00	28	00	00	00	04	18	00	00	00	06	00	00	°... (.....
0036CDE0	08	00	00	00	20	00	00	00	24	00	49	00	33	00	30	00\$.I.3.0.
0036CDF0	01	00	00	00	00	00	00	00	FF	FF	FF	FF	82	79	11	00ÿÿÿÿ,y..
0036CE00	p0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0036CE10	00	00	00	10	00	00	00	00	10	00	41	00	70	00	70	00A.p.p.
0036CE20	6C	00	69	00	63	00	61	00	74	00	69	00	6F	00	6E	00	l.i.c.a.t.i.o.n.
0036CE30	20	00	44	00	61	00	74	00	61	00	52	00	00	00	00	00	.D.a.t.a.R.....
0036CE40	64	00	00	00	00	00	01	00	68	00	52	00	00	00	00	00	d.....h.R.....

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 corrupted and not just specific files or folders.