Maria Valencia

CSC 153

Lab 16 – extra credit

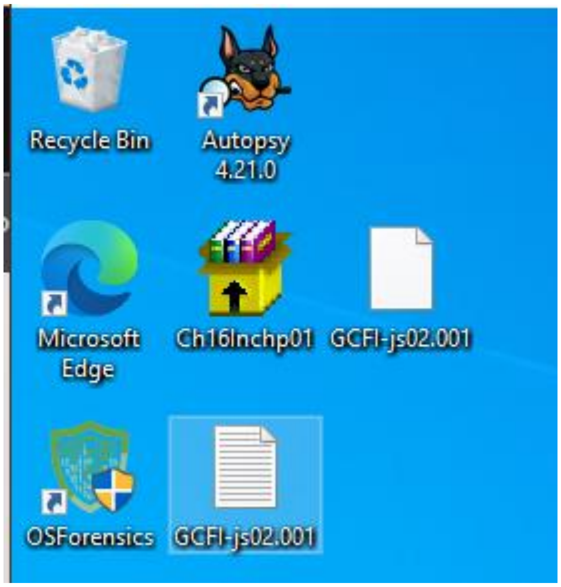
Lab 16 – Ethics

In this lab, I will determine if malware caused corruption on a forensic image.

Task 1 – Malware case

Step 1: Mount Image

On my Windows VM, I downloaded the "Ch16Inchp01.exe" and extracted the "GCFI-js02.001" image by double clicking on the executable.



I launched the FTK imager and mounted the "GCFI-js02.001" image upon extracting the image by navigating the File and "Image Mounting" menu. Here, i selected file and mount. (Drive letter and read only method are selected in the mount method).

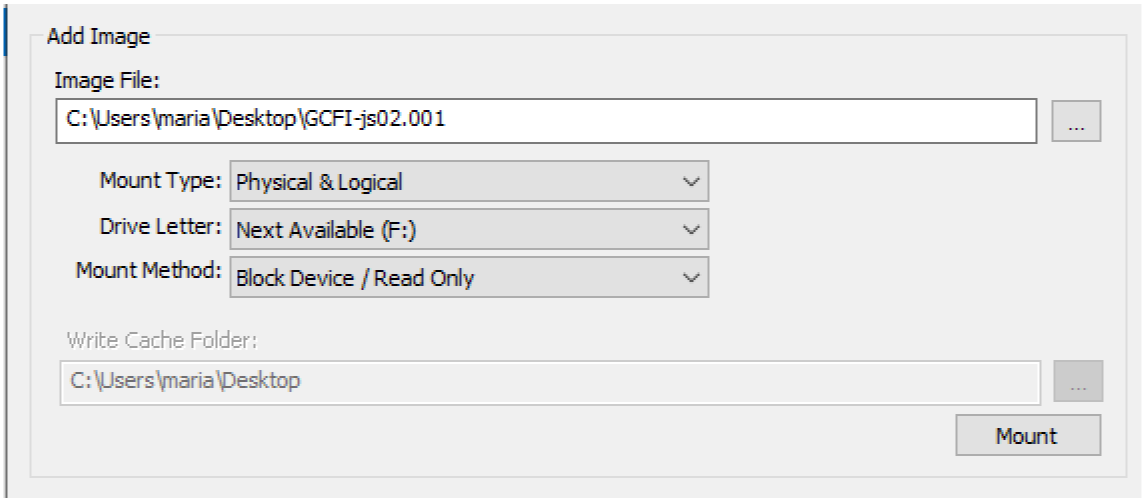


Image File: C:\Users\maria\Desktop\GCFI-js02.001

Mount Type: Physical & Logical

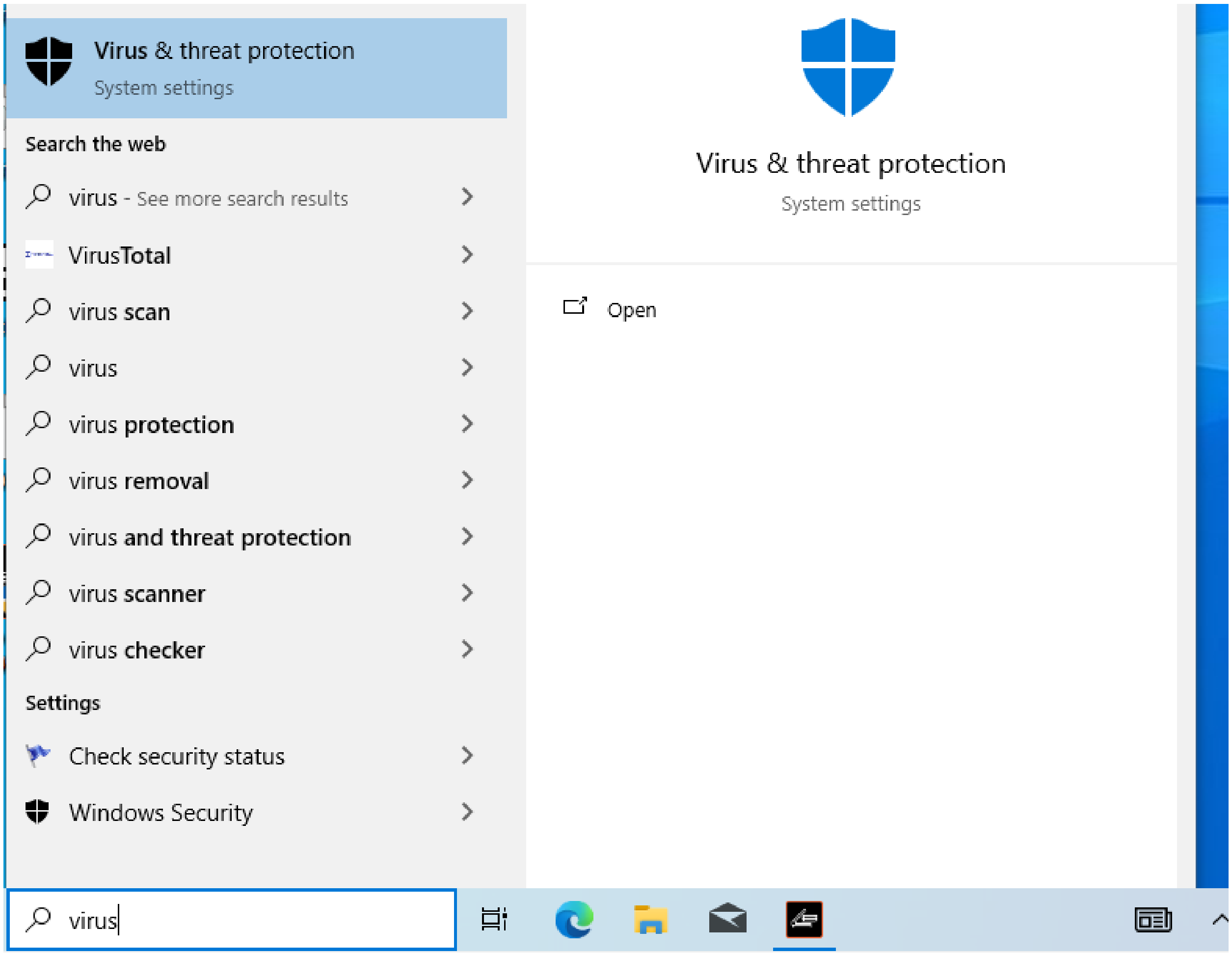
Drive Letter: Next Available (F:)

Mount Method: Block Device / Read Only

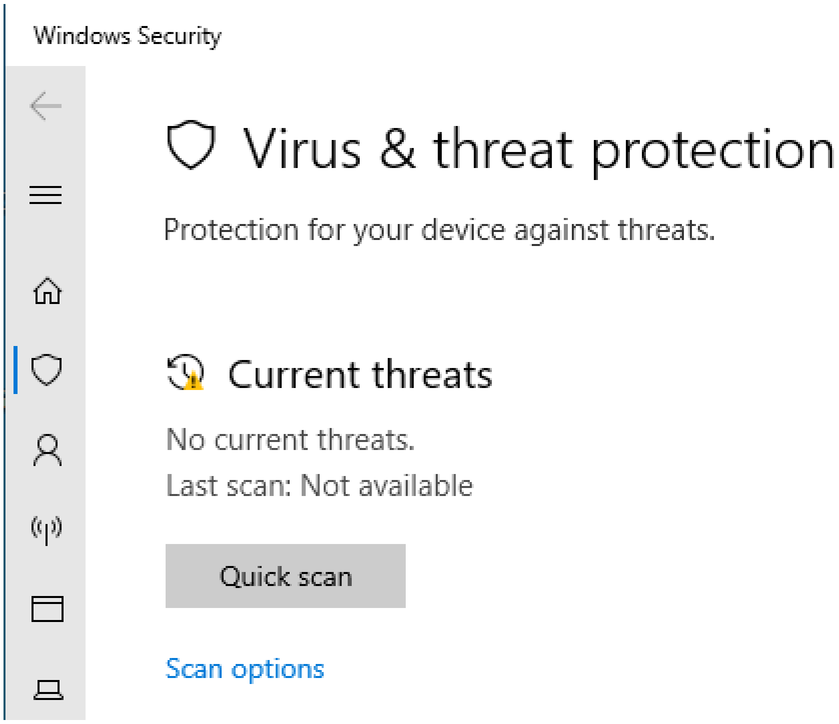
Write Cache Folder: C:\Users\maria\Desktop

Step 2: Antivirus Scan

I launched Windows Defender by searching for “Virus & Threat protection” in the Windows search bar.



I chose the “Scan options” under the current threats section.



Virus & threat protection

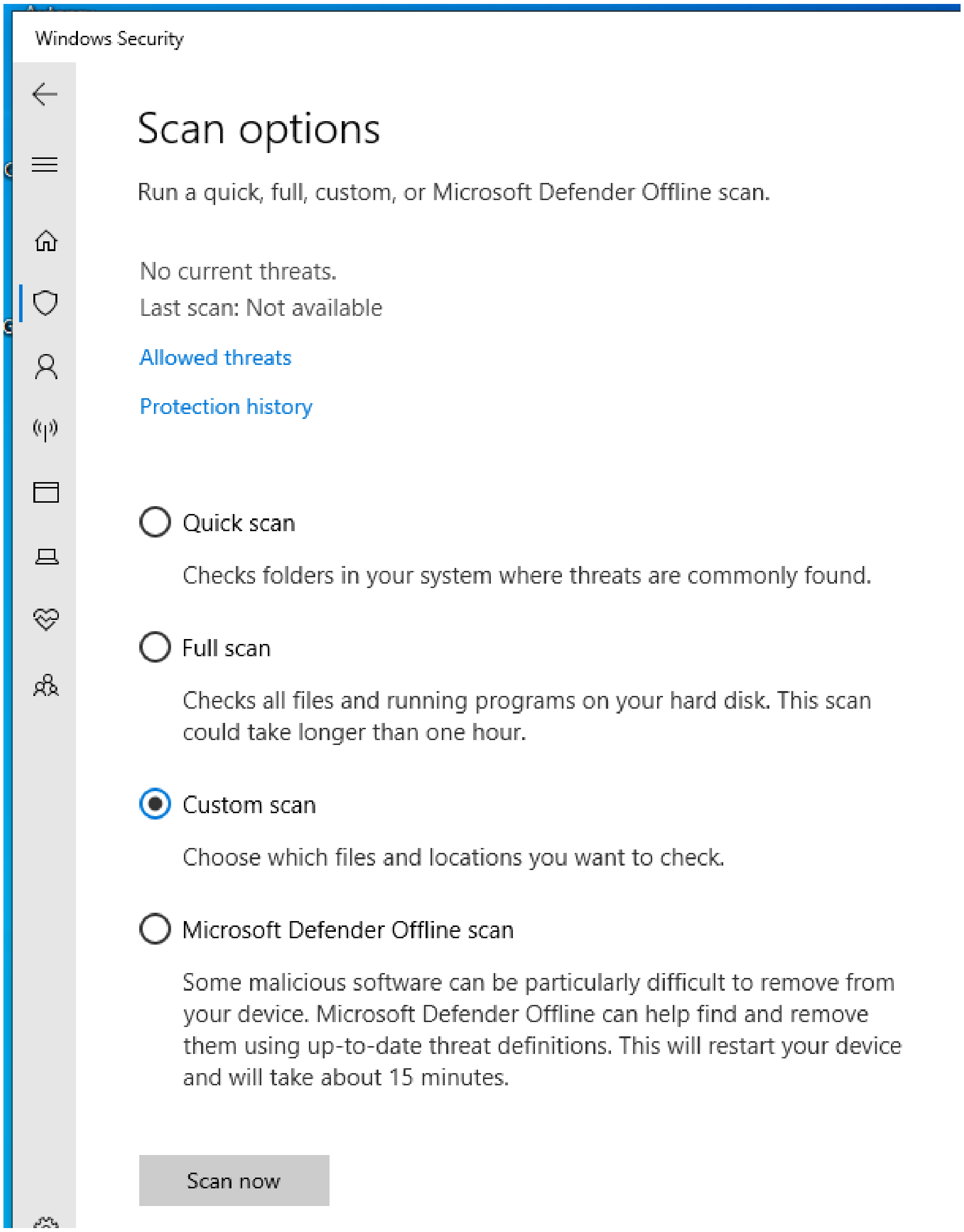
Protection for your device against threats.

Current threats

No current threats.

Last scan: Not available

Next, I selected the “custom scan” radio button and then pressed the “scan now” button.



Windows Security

Scan options

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

No current threats.
Last scan: Not available

○ Quick scan

Checks folders in your system where threats are commonly found.

○ Full scan

Checks all files and running programs on your hard disk. This scan could take longer than one hour.

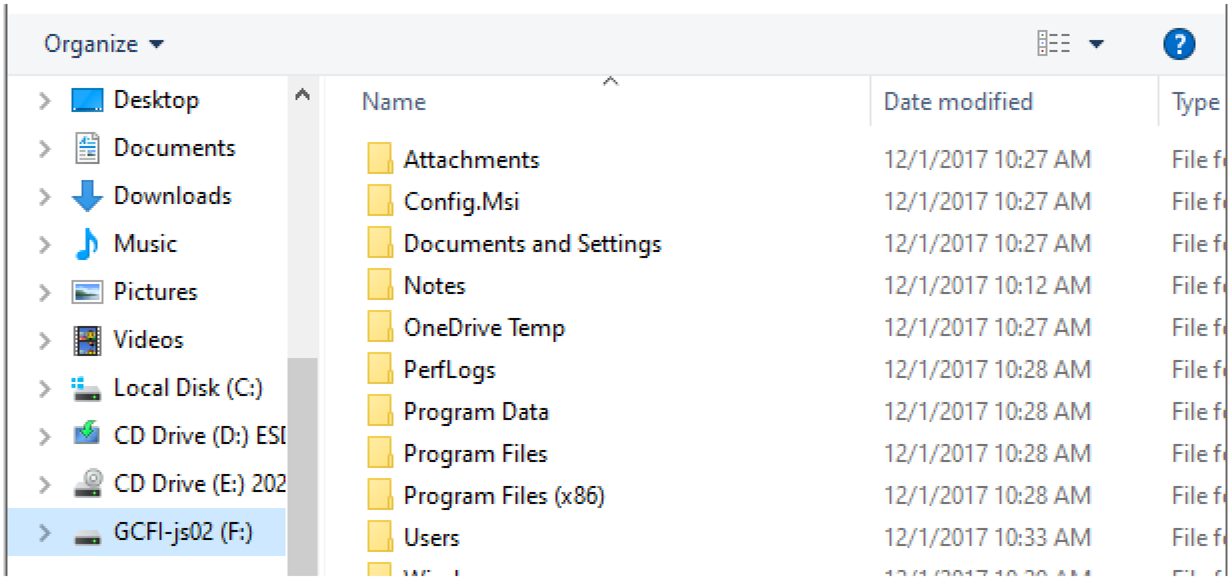
● Custom scan

Choose which files and locations you want to check.

○ Microsoft Defender Offline scan

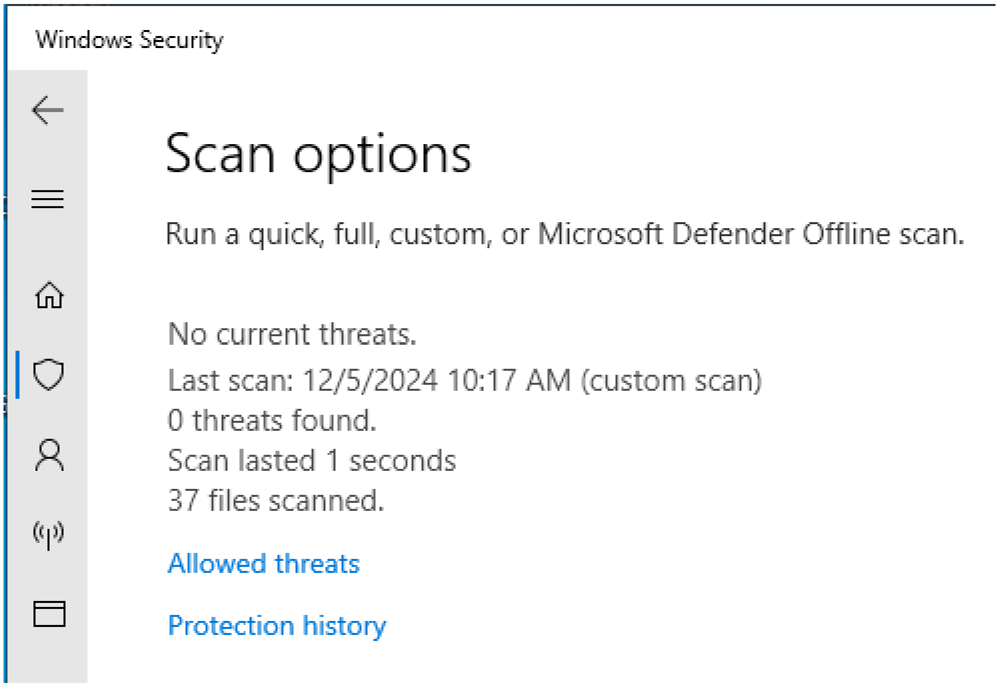
Some malicious software can be particularly difficult to remove from your device. Microsoft Defender Offline can help find and remove them using up-to-date threat definitions. This will restart your device and will take about 15 minutes.

The scan now button launched a Select folder window. I found the mounted image “GCFI-js02” in the left navigation pane and pressed “Select Folder” to launch the antivirus scan.



Name	Date modified	Type
Attachments	12/1/2017 10:27 AM	File f
Config.Msi	12/1/2017 10:27 AM	File f
Documents and Settings	12/1/2017 10:27 AM	File f
Notes	12/1/2017 10:12 AM	File f
OneDrive Temp	12/1/2017 10:27 AM	File f
PerfLogs	12/1/2017 10:28 AM	File f
Program Data	12/1/2017 10:28 AM	File f
Program Files	12/1/2017 10:28 AM	File f
Program Files (x86)	12/1/2017 10:28 AM	File f
Users	12/1/2017 10:33 AM	File f

The scan was completed, and I observed its results under the Scan Options menu.


Windows Security

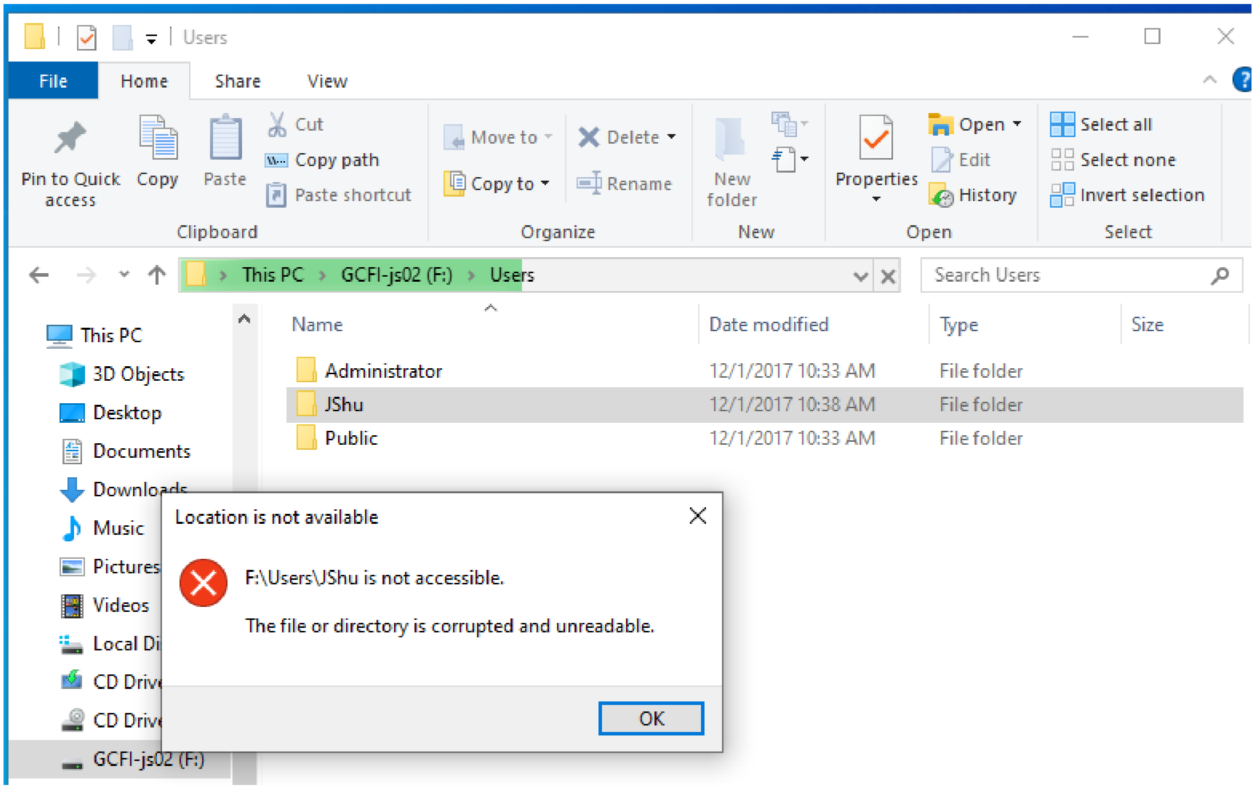
Scan options

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

No current threats.
Last scan: 12/5/2024 10:17 AM (custom scan)
0 threats found.
Scan lasted 1 seconds
37 files scanned.

Step 3: Analyze File System

Now with the virus scan completed, I launched File Explorer and explored the image. I observed that there were errors when trying to access the Users/JShu folder.



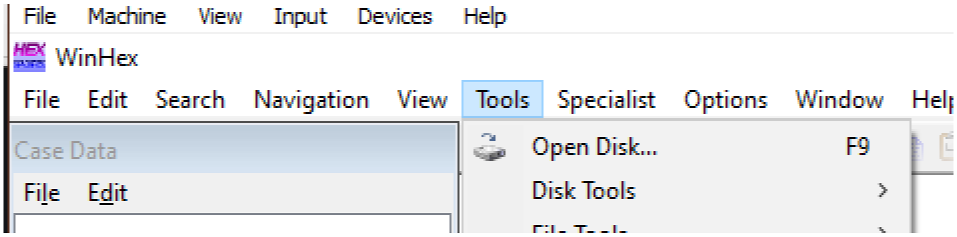
Name	Date modified	Type	Size
Administrator	12/1/2017 10:33 AM	File folder	
JShu	12/1/2017 10:38 AM	File folder	
Public	12/1/2017 10:33 AM	File folder	

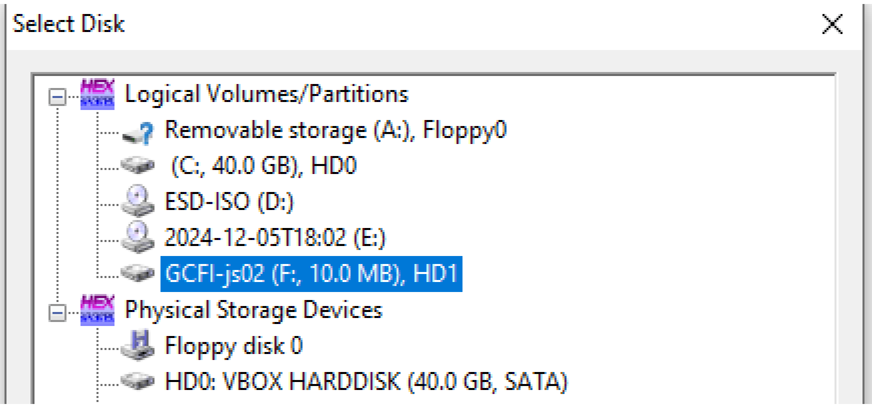
Location is not available

F:\Users\JShu is not accessible.

The file or directory is corrupted and unreadable.

So, I investigated the master file table in the file $MFT using WinHex to identify why JShu's folder won't open. To do this, I launched WinHex as administrator, selected tools and "open Disk" from the menu. Here, I selected the "GCFI-js02" image to load into WinHex.

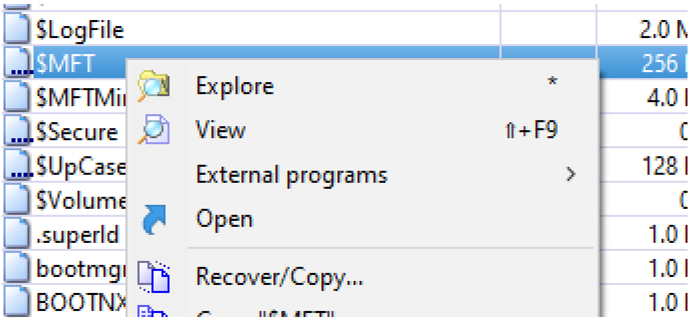




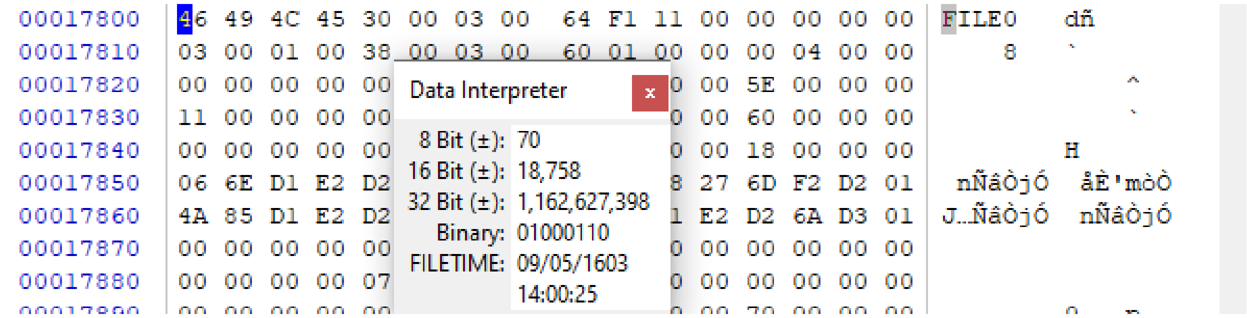
Select Disk

- Logical Volumes/Partitions
  - Removable storage (A:), Floppy0
  - (C:, 40.0 GB), HD0
  - ESD-ISO (D:)
  - 2024-12-05T18:02 (E:)
  - GCFI-js02 (F:, 10.0 MB), HD1
- Physical Storage Devices
  - Floppy disk 0
  - HD0: VBOX HARDDISK (40.0 GB, SATA)

After, I found the $MFT file and right-clicked it then pressed open .



I went to offset 17800 and observed that a file record starts with 46 49 4c 45 30 or FILE0. According to the data interpreter, the converted F value to binary is 01000110.

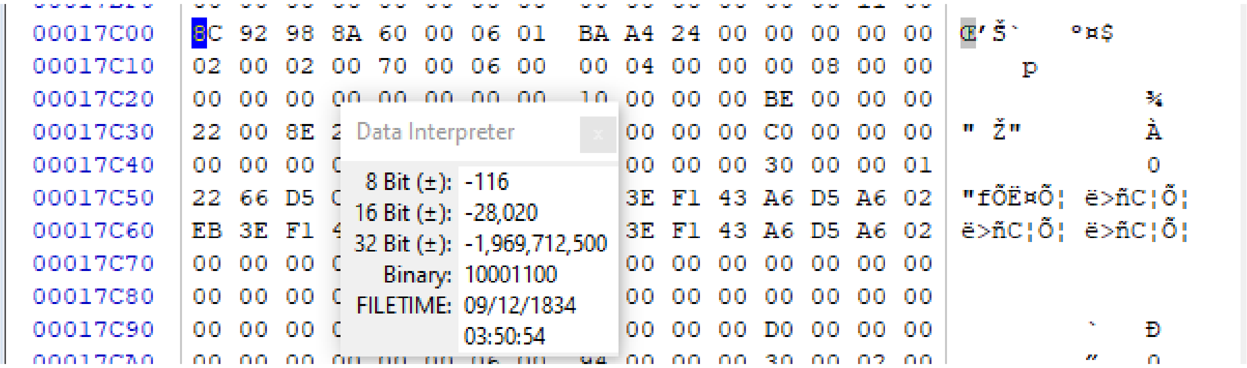


```
00017800  46 49 4C 45 30 00 03 00  64 F1 11 00 00 00 00 00   FILE0   dñ
00017810  03 00 01 00 38 00 03 00  60 01 00 00 00 04 00 00      8   `
00017820  00 00 00 00 00              0 00 5E 00 00 00              ^
00017830  11 00 00 00 00              0 00 60 00 00 00              `
00017840  00 00 00 00 00              0 00 18 00 00 00          H
00017850  06 6E D1 E2 D2              8 27 6D F2 D2 01    nÑâÒjó  åÈ'mòÒ
00017860  4A 85 D1 E2 D2              1 E2 D2 6A D3 01   J…ÑâÒjó  nÑâÒjó
00017870  00 00 00 00 00              0 00 00 00 00 00
00017880  00 00 00 00 07              0 00 00 00 00 00
```

Data Interpreter

8 Bit (±): 70
16 Bit (±): 18,758
32 Bit (±): 1,162,627,398
Binary: 01000110
FILETIME: 09/05/1603 14:00:25

Then, I scrolled down to the next file record (17C00) and selected on its first byte with the hex value 8c. Here I observed the binary value is 10001100 which appears to be bit shifted.

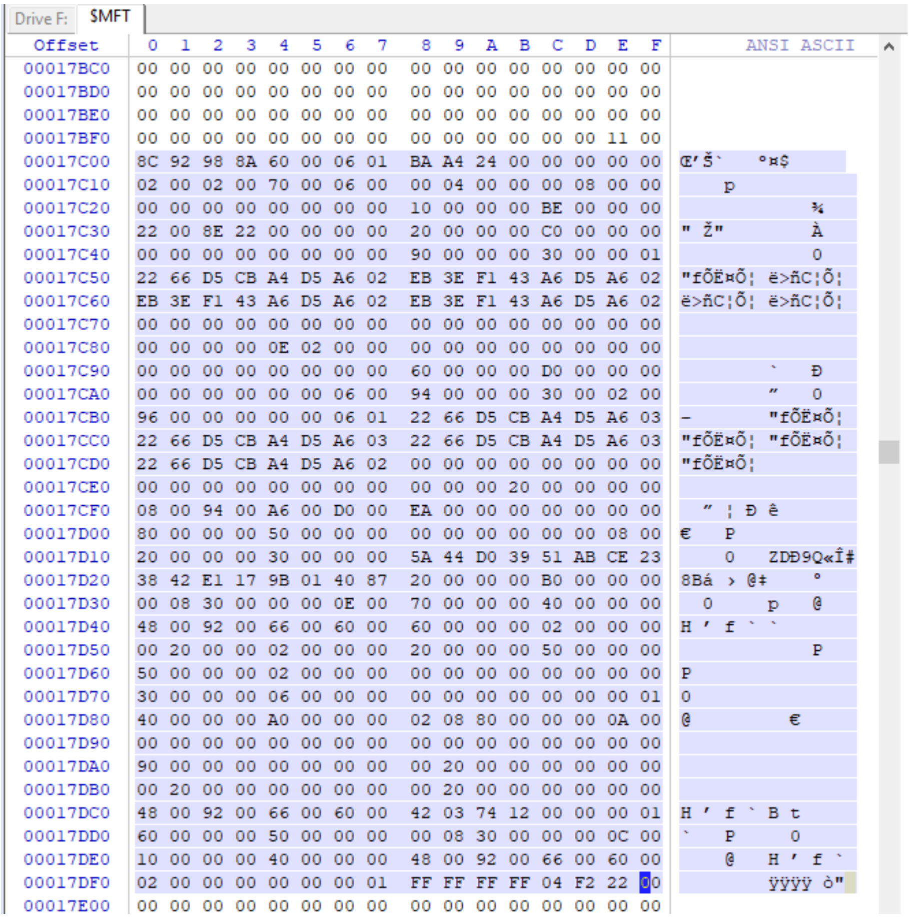


```
00017C00  8C 92 98 8A 60 00 06 01  BA A4 24 00 00 00 00 00   Œ’Š`    º¤$
00017C10  02 00 02 00 70 00 06 00  00 04 00 00 00 08 00 00       p
00017C20  00 00 00                    00 00 00 BE 00 00 00              ¾
00017C30  22 00 8E 2                  00 00 00 C0 00 00 00   " Ž"          À
00017C40  00 00 00 C                  00 00 00 30 00 00 01                 0
00017C50  22 66 D5 C                  3E F1 43 A6 D5 A6 02   "fÕË¤Õ¦ ë>ñC¦Õ¦
00017C60  EB 3E F1 4                  3E F1 43 A6 D5 A6 02   ë>ñC¦Õ¦ ë>ñC¦Õ¦
00017C70  00 00 00 C                  00 00 00 00 00 00 00
00017C80  00 00 00 C                  00 00 00 00 00 00 00
00017C90  00 00 00 C                  00 00 00 D0 00 00 00            `   Ð
```

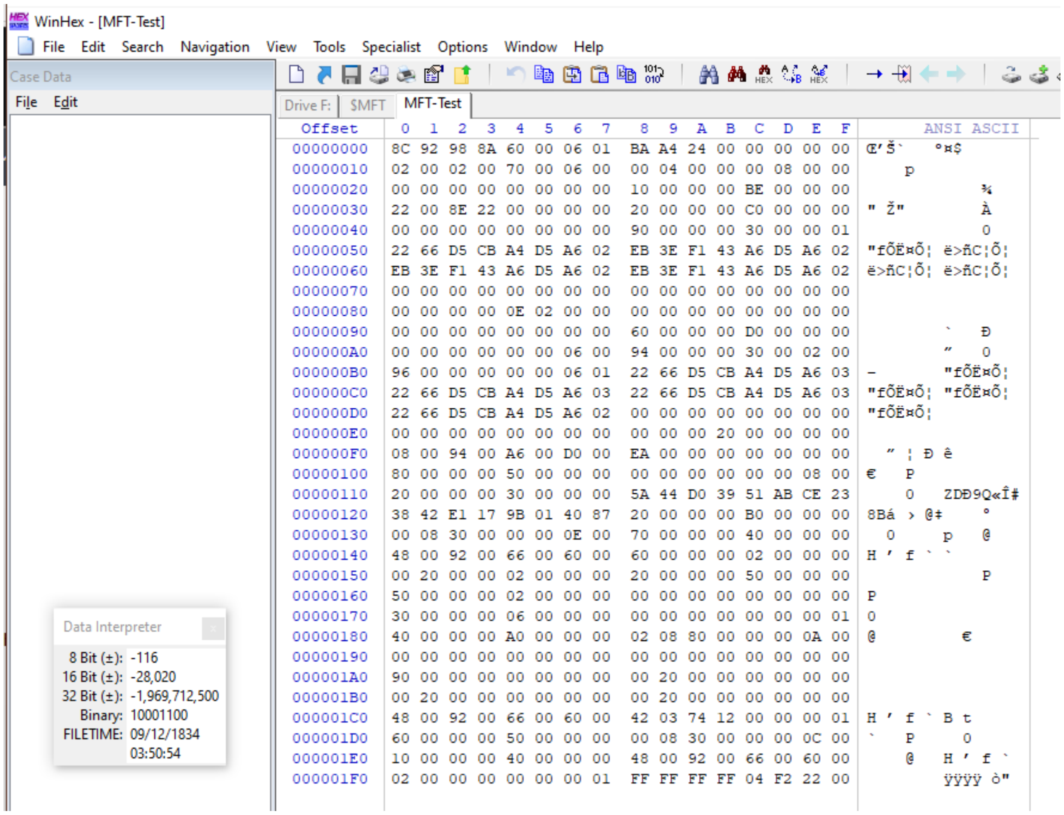
Data Interpreter

8 Bit (±):	-116
16 Bit (±):	-28,020
32 Bit (±):	-1,969,712,500
Binary:	10001100
FILETIME:	09/12/1834 03:50:54

Then, i selected and highlighted the entire section 17C00 through 17DFF and copied to a new file through the edit menu, copy block option and choosing “into new file” saving as MFT-Test.



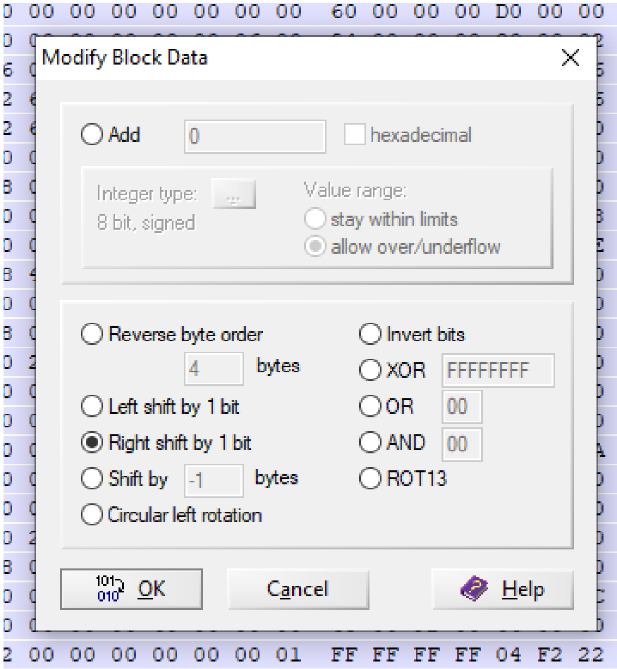
```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F         ANSI ASCII
00017BC0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00017BD0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00017BE0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00017BF0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 11 00
00017C00  8C 92 98 8A 60 00 06 01  BA A4 24 00 00 00 00 00  Œ’Š`    º¤$
00017C10  02 00 02 00 70 00 06 00  00 04 00 00 00 08 00 00      p
00017C20  00 00 00 00 00 00 00 00  10 00 00 00 BE 00 00 00              ¾
00017C30  22 00 8E 22 00 00 00 00  20 00 00 00 C0 00 00 00  " Ž"        À
00017C40  00 00 00 00 00 00 00 00  90 00 00 00 30 00 00 01              0
00017C50  22 66 D5 CB A4 D5 A6 02  EB 3E F1 43 A6 D5 A6 02  "fÕË¤Õ¦ ë>ñC¦Õ¦
00017C60  EB 3E F1 43 A6 D5 A6 02  EB 3E F1 43 A6 D5 A6 02  ë>ñC¦Õ¦ ë>ñC¦Õ¦
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          `   Ð
00017CA0  00 00 00 00 00 00 06 00  94 00 00 00 30 00 02 00          ”   0
00017CB0  96 00 00 00 00 00 06 01  22 66 D5 CB A4 D5 A6 03  –       "fÕË¤Õ¦
00017CC0  22 66 D5 CB A4 D5 A6 03  22 66 D5 CB A4 D5 A6 03  "fÕË¤Õ¦ "fÕË¤Õ¦
00017CD0  22 66 D5 CB A4 D5 A6 02  00 00 00 00 00 00 00 00  "fÕË¤Õ¦
00017CE0  00 00 00 00 00 00 00 00  00 00 00 20 00 00 00 00
00017CF0  08 00 94 00 A6 00 D0 00  EA 00 00 00 00 00 00 00   ” ¦ Ð ê
00017D00  80 00 00 00 50 00 00 00  00 00 00 00 00 00 08 00  €   P
00017D10  20 00 00 00 30 00 00 00  5A 44 D0 39 51 AB CE 23      0   ZDÐ9Q«Î#
00017D20  38 42 E1 17 9B 01 40 87  20 00 00 00 B0 00 00 00  8Bá › @‡    °
00017D30  00 08 30 00 00 00 0E 00  70 00 00 00 40 00 00 00    0     p   @
00017D40  48 00 92 00 66 00 60 00  60 00 00 00 02 00 00 00  H ’ f ` `
00017D50  00 20 00 00 02 00 00 00  20 00 00 00 50 00 00 00              P
00017D60  50 00 00 00 02 00 00 00  00 00 00 00 00 00 00 00  P
00017D70  30 00 00 00 06 00 00 00  00 00 00 00 00 00 00 01  0
00017D80  40 00 00 00 A0 00 00 00  02 08 80 00 00 00 0A 00  @         €
00017D90  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00017DA0  90 00 00 00 00 00 00 00  00 20 00 00 00 00 00 00
00017DB0  00 20 00 00 00 00 00 00  00 20 00 00 00 00 00 00
00017DC0  48 00 92 00 66 00 60 00  42 03 74 12 00 00 00 01  H ’ f ` B t
00017DD0  60 00 00 00 50 00 00 00  00 08 30 00 00 00 0C 00  `   P     0
00017DE0  10 00 00 00 40 00 00 00  48 00 92 00 66 00 60 00      @   H ’ f `
00017DF0  02 00 00 00 00 00 00 01  FF FF FF FF 04 F2 22 00          ÿÿÿÿ ò"
00017E00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```



```
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  Œ'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              ¾
00000030  22 00 8E 22 00 00 00 00  20 00 00 00 C0 00 00 00  " Ž"        À
00000040  00 00 00 00 00 00 00 00  90 00 00 00 30 00 00 01              0
00000050  22 66 D5 CB A4 D5 A6 02  EB 3E F1 43 A6 D5 A6 02  "fÕË¤Õ¦ ë>ñC¦Õ¦
00000060  EB 3E F1 43 A6 D5 A6 02  EB 3E F1 43 A6 D5 A6 02  ë>ñC¦Õ¦ ë>ñC¦Õ¦
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          `   Ð
000000A0  00 00 00 00 00 00 06 00  94 00 00 00 30 00 02 00          ”   0
000000B0  96 00 00 00 00 00 06 01  22 66 D5 CB A4 D5 A6 03  –       "fÕË¤Õ¦
000000C0  22 66 D5 CB A4 D5 A6 03  22 66 D5 CB A4 D5 A6 03  "fÕË¤Õ¦ "fÕË¤Õ¦
000000D0  22 66 D5 CB A4 D5 A6 02  00 00 00 00 00 00 00 00  "fÕË¤Õ¦
000000E0  00 00 00 00 00 00 00 00  00 00 00 20 00 00 00 00
000000F0  08 00 94 00 A6 00 D0 00  EA 00 00 00 00 00 00 00    ” ¦ Ð ê
00000100  80 00 00 00 50 00 00 00  00 00 00 00 00 00 08 00  €   P
00000110  20 00 00 00 30 00 00 00  5A 44 D0 39 51 AB CE 23      0   ZDÐ9Q«Î#
00000120  38 42 E1 17 9B 01 40 87  20 00 00 00 B0 00 00 00  8Bá › @‡    °
00000130  00 08 30 00 00 00 0E 00  70 00 00 00 40 00 00 00    0     p   @
00000140  48 00 92 00 66 00 60 00  60 00 00 00 02 00 00 00  H ' f ` `
00000150  00 20 00 00 02 00 00 00  20 00 00 00 50 00 00 00              P
00000160  50 00 00 00 02 00 00 00  00 00 00 00 00 00 00 00  P
00000170  30 00 00 00 06 00 00 00  00 00 00 00 00 00 00 01  0
00000180  40 00 00 00 A0 00 00 00  02 08 80 00 00 00 0A 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 20 00 00 00 00 00 00
000001B0  00 20 00 00 00 00 00 00  00 20 00 00 00 00 00 00
000001C0  48 00 92 00 66 00 60 00  42 03 74 12 00 00 00 01  H ' f ` B t
000001D0  60 00 00 00 50 00 00 00  00 08 30 00 00 00 0C 00  `   P     0
000001E0  10 00 00 00 40 00 00 00  48 00 92 00 66 00 60 00      @   H ' f `
000001F0  02 00 00 00 00 00 00 01  FF FF FF FF 04 F2 22 00          ÿÿÿÿ ò"
```

8 Bit (±): -116
16 Bit (±): -28,020
32 Bit (±): -1,969,712,500
Binary: 10001100
FILETIME: 09/12/1834 03:50:54

With MFT-Test file created and open, I selected all of the content and shifted each bytes' bits to the right through the Edit menu's Modify Data option.


0 00 00 00 00 00 00 00 60 00 00 00 D0 00 00
2 00 00 00 00 00 00 01 FF FF FF FF 04 F2 22

Modify Block Data

○ Add 0 □ hexadecimal

Integer type: 8 bit, signed

Value range: ○ stay within limits ● allow over/underflow

○ Reverse byte order 4 bytes

○ Invert bits

○ XOR FFFFFFFF

○ Left shift by 1 bit

○ OR 00

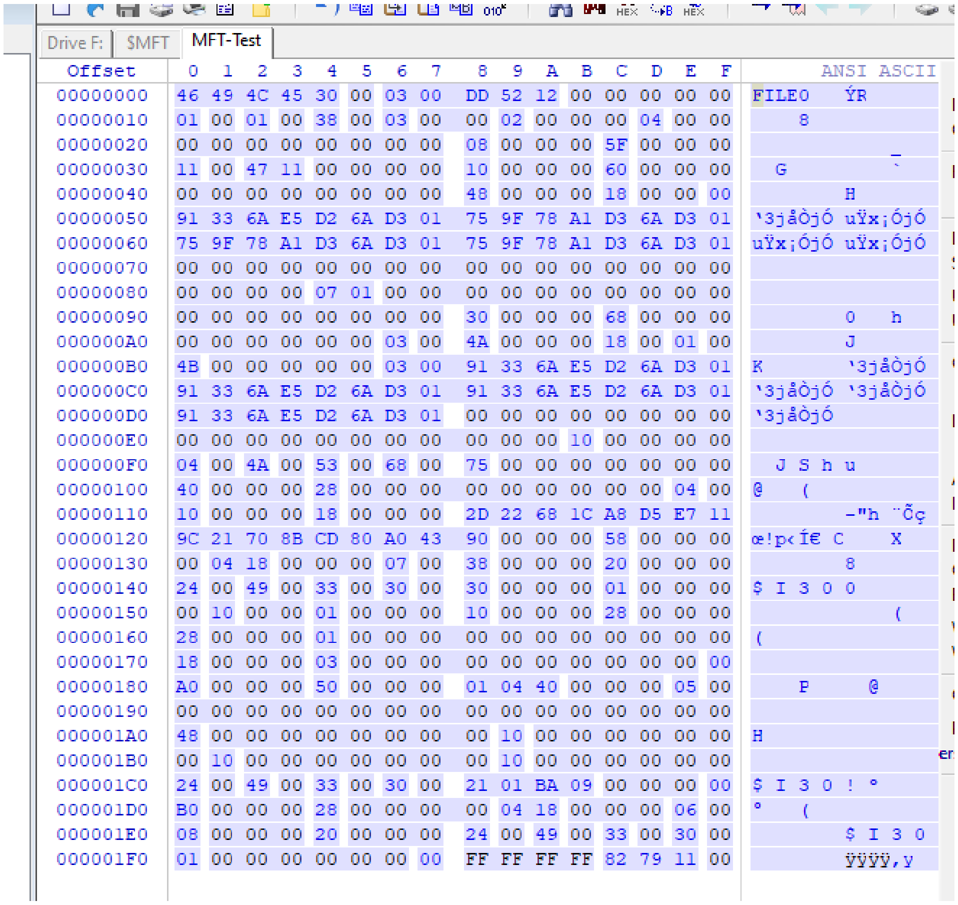
● Right shift by 1 bit

○ AND 00

○ Shift by -1 bytes

○ ROT13

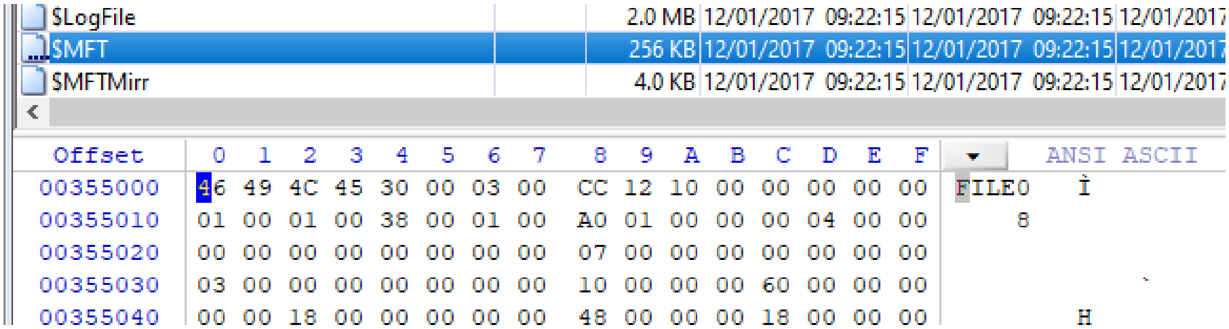
○ Circular left rotation



```
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 ! °
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
```

Step 4: Find Absolute Path of Corrupted File

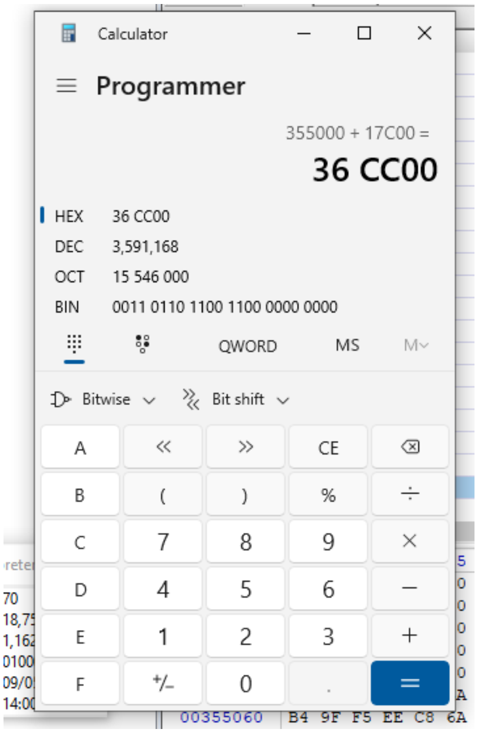
I know that the corrupted JShu folder is located at offset 17C00 from the beginning of the $MFT file. In WinHex, I navigated to the image tab (eg Drive F:) and select the $MFT file. I observe the $MFT file starts at offset 355000.



```
$LogFile     2.0 MB  12/01/2017 09:22:15  12/01/2017 09:22:15  12/01/2017
$MFT         256 KB  12/01/2017 09:22:15  12/01/2017 09:22:15  12/01/2017
$MFTMirr     4.0 KB  12/01/2017 09:22:15  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   ANSI ASCII
00355000  46 49 4C 45 30 00 03 00  CC 12 10 00 00 00 00 00   FILE0   Ì
00355010  01 00 01 00 38 00 01 00  A0 01 00 00 00 04 00 00       8
00355020  00 00 00 00 00 00 00 00  07 00 00 00 00 00 00 00
00355030  03 00 00 00 00 00 00 00  10 00 00 00 60 00 00 00               `
00355040  00 00 18 00 00 00 00 00  48 00 00 00 18 00 00 00           H
```

I found the absolute address of the corrupted folder by launching the calculator app in programmer and Hex mode and adding offset 355000 and offset 17C00.



Calculator

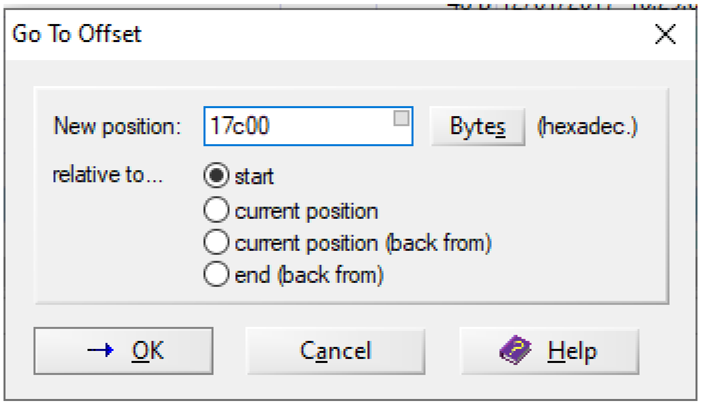
Programmer

355000 + 17C00 =

36 CC00

HEX 36 CC00
DEC 3,591,168
OCT 15 546 000
BIN 0011 0110 1100 1100 0000 0000

I jumped to the corrupted file using WinHex Navigation menu "Go to offset" option and enter the relative offset 17c00 from the current position.



Go To Offset

New position: 17c00 Bytes (hexadec.)

relative to...
● start
○ current position
○ current position (back from)
○ end (back from)

I was unable to finish the lab completely, but I thought I should still turn this in because I had started it a few days ago. Thank you for a wonderful semester! Time to study for the final.