Module B1: File System-FTK Imager Examination

Pre-requisite Knowledge and Skills:

1. Understand the basic of File Systems

Learning Objectives

1. Be familiar to FAT and NTFS file systems.

Recommended Running Environment/Tools:

1. Windows OS
2. AccessData FTK Imager

Material:

1. FAT32.001
2. NTFS.001

Video Lecture:

1. N/A

Lab Assessment:

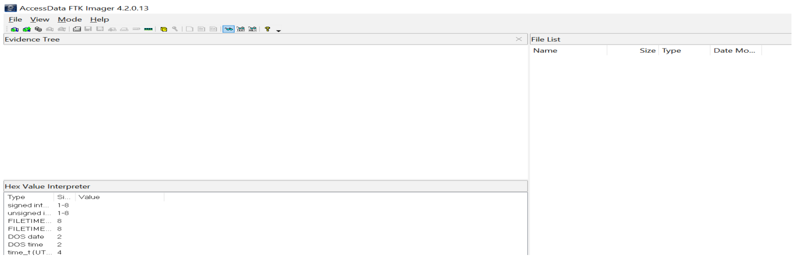
1. ADS Quiz

Lab Instructions:

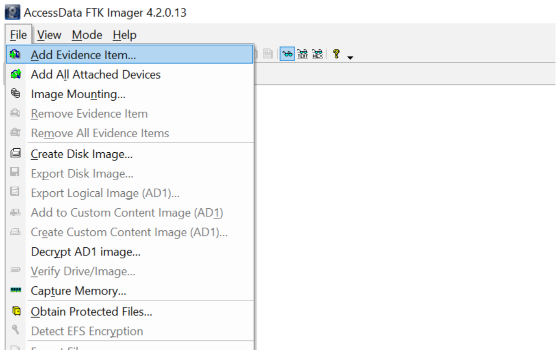
Part I: NTFS File System Examination

Steps:

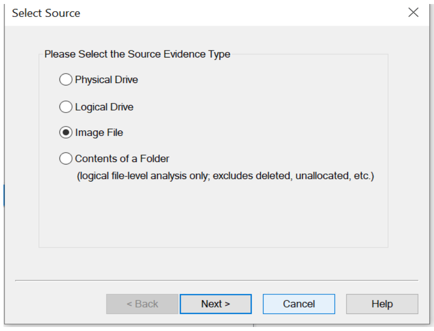
1. Run FTK Imager



2. Select the file and click the add evidence option



3. On the new pop-up window, select the **image file** option (not the default option),



Select Source

Please Select the Source Evidence Type

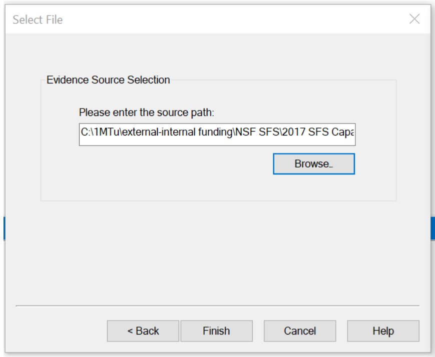
○ Physical Drive

○ Logical Drive

● Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

4. then next, and browse to the *NTFS.001* (not the txt file)

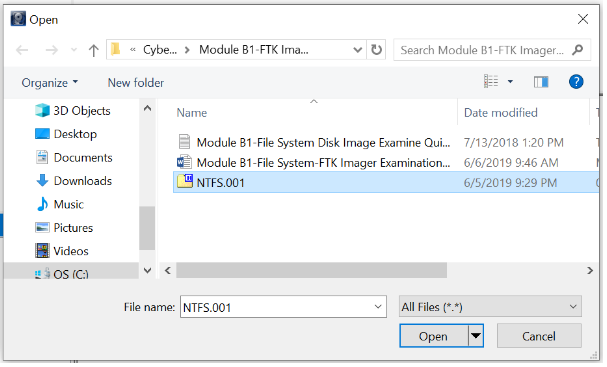


Select File

Evidence Source Selection

Please enter the source path:

C:\1MTu\external-internal funding\NSF SFS\2017 SFS Capa



Open

« Cybe... › Module B1-FTK Ima...

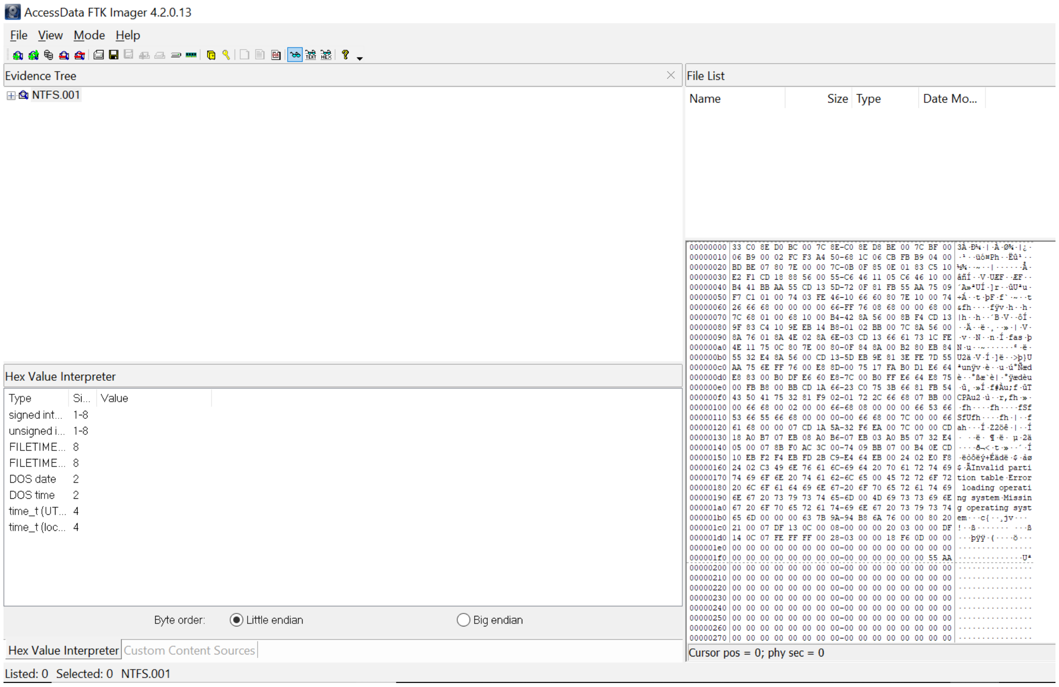
Search Module B1-FTK Imager...

Name	Date modified
Module B1-File System Disk Image Examine Qui...	7/13/2018 1:20 PM
Module B1-File System-FTK Imager Examination...	6/6/2019 9:46 AM
NTFS.001	6/5/2019 9:29 PM

File name: NTFS.001

All Files (*.*)

5. Then click on open and finish.



AccessData FTK Imager 4.2.0.13

```
00000000  33 C0 8E D0 BC 00 7C 8E-C0 8E D8 BE 00 7C BF 00  3À·Ð¼·|·À·Ø¾·|¿·
00000010  06 B9 00 02 FC F3 A4 50-68 1C 06 CB FB B9 04 00  ·¹··üó¤Ph··Ëû¹··
00000020  BD BE 07 80 7E 00 00 7C-0B 0F 85 0E 01 83 C5 10  ½¾··~··|······Å·
00000030  E2 F1 CD 18 88 56 00 55-C6 46 11 05 C6 46 10 00  âñÍ··V·UÆF··ÆF··
00000040  B4 41 BB AA 55 CD 13 5D-72 0F 81 FB 55 AA 75 09  ´A»ªUÍ·]r··ûUªu·
00000050  F7 C1 01 00 74 03 FE 46-10 66 60 80 7E 10 00 74  ÷Á··t·þF·f`·~··t
00000060  26 66 68 00 00 00 00 66-FF 76 08 68 00 00 68 00  &fh····fÿv·h··h·
00000070  7C 68 01 00 68 10 00 B4-42 8A 56 00 8B F4 CD 13  |h··h··´B·V··ôÍ·
00000080  9F 83 C4 10 9E EB 14 B8-01 02 BB 00 7C 8A 56 00  ··Ä··ë·¸··»·|·V·
00000090  8A 76 01 8A 4E 02 8A 6E-03 CD 13 66 61 73 1C FE  ·v··N··n·Í·fas·þ
000000a0  4E 11 75 0C 80 7E 00 80-0F 84 8A 00 B2 80 EB 84  N·u··~·······²·ë·
000000b0  55 32 E4 8A 56 00 CD 13-5D EB 9E 81 3E FE 7D 55  U2ä·V·Í·]ë··>þ}U
000000c0  AA 75 6E FF 76 00 E8 8D-00 75 17 FA B0 D1 E6 64  ªunÿv·è··u·ú°Ñæd
000000d0  E8 83 00 B0 DF E6 60 E8-7C 00 B0 FF E6 64 E8 75  è··°ßæ`è|·°ÿædèu
000000e0  00 FB B8 00 BB CD 1A 66-23 C0 75 3B 66 81 FB 54  ·û¸·»Í·f#Àu;f·ûT
000000f0  43 50 41 75 32 81 F9 02-01 72 2C 66 68 07 BB 00  CPAu2·ù··r,fh·»·
00000100  00 66 68 00 02 00 00 66-68 08 00 00 00 66 53 66  ·fh····fh····fSf
00000110  53 66 55 66 68 00 00 00-00 66 68 00 7C 00 00 66  SfUfh····fh·|··f
00000120  61 68 00 00 07 CD 1A 5A-32 F6 EA 00 7C 00 00 CD  ah···Í·Z2öê·|··Í
00000130  18 A0 B7 07 EB 08 A0 B6-07 EB 03 A0 B5 07 32 E4  ····ë··¶·ë··µ·2ä
00000140  05 00 07 8B F0 AC 3C 00-74 09 BB 07 00 B4 0E CD  ····ð¬<·t·»··´·Í
00000150  10 EB F2 F4 EB FD 2B C9-E4 64 EB 00 24 02 E0 F8  ·ëòôëý+Éädë·$·àø
00000160  24 02 C3 49 6E 76 61 6C-69 64 20 70 61 72 74 69  $·ÃInvalid parti
00000170  74 69 6F 6E 20 74 61 62-6C 65 00 45 72 72 6F 72  tion table·Error
00000180  20 6C 6F 61 64 69 6E 67-20 6F 70 65 72 61 74 69   loading operati
00000190  6E 67 20 73 79 73 74 65-6D 00 4D 69 73 73 69 6E  ng system·Missin
000001a0  67 20 6F 70 65 72 61 74-69 6E 67 20 73 79 73 74  g operating syst
000001b0  65 6D 00 00 00 63 7B 9A-94 B8 6A 76 00 00 80 20  em···c{··¸jv····
000001c0  21 00 07 DF 13 0C 00 08-00 00 00 20 03 00 00 DF  !··ß···········ß
000001d0  14 0C 07 FE FF FF 00 28-03 00 00 18 F6 0D 00 00  ···þÿÿ·(····ö···
000001e0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
000001f0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 55 AA  ··············Uª
00000200  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
00000210  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
00000220  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
00000230  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
00000240  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
00000250  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
00000260  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
00000270  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
```

Hex Value Interpreter

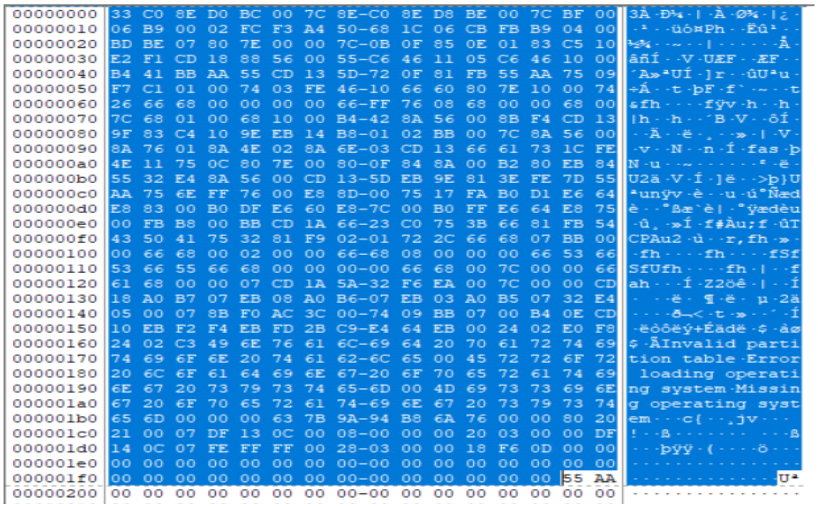
Type	Si...	Value
signed int...	1-8	
unsigned i...	1-8	
FILETIME...	8	
FILETIME...	8	
DOS date	2	
DOS time	2	
time_t (UT...	4	
time_t (loc...	4	

Byte order: ● Little endian ○ Big endian

Cursor pos = 0; phy sec = 0

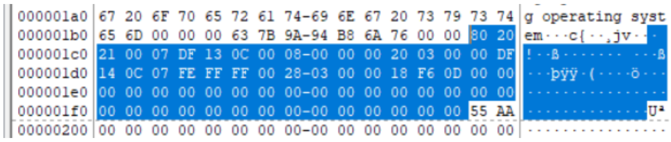
Listed: 0 Selected: 0 NTFS.001

6. The first Sector- 512 bytes-Master Boot Record MBR, define the layout of the NTFS system, including the size, location, basic data storage unit size (cluster size), the partition table of the disk, and the MBR signature (55 AA) at the end of the sector. Please locate the MBR file signature 55 AA.



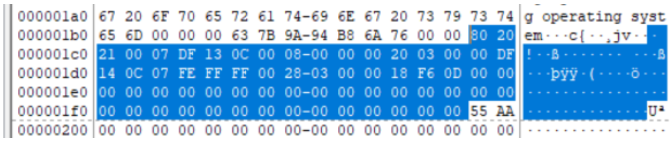
```
00000000  33 C0 8E D0 BC 00 7C 8E-C0 8E D8 BE 00 7C BF 00  3À·Ð¼·|·À·Ø¾·|¿·
00000010  06 B9 00 02 FC F3 A4 50-68 1C 06 CB FB B9 04 00  ·¹··üó¤Ph··Ëû¹··
00000020  BD BE 07 80 7E 00 00 7C-0B 0F 85 0E 01 83 C5 10  ½¾··~··|·······Å·
00000030  E2 F1 CD 18 88 56 00 55-C6 46 11 05 C6 46 10 00  âñÍ··V·UÆF··ÆF··
00000040  B4 41 BB AA 55 CD 13 5D-72 0F 81 FB 55 AA 75 09  ´A»ªUÍ·]r··ûUªu·
00000050  F7 C1 01 00 74 03 FE 46-10 66 60 80 7E 10 00 74  ÷Á··t·þF·f`·~··t
00000060  26 66 68 00 00 00 00 66-FF 76 08 68 00 00 68 00  &fh····fÿv·h··h·
00000070  7C 68 01 00 68 10 00 B4-42 8A 56 00 8B F4 CD 13  |h··h··´B·V··ôÍ·
00000080  9F 83 C4 10 9E EB 14 B8-01 02 BB 00 7C 8A 56 00  ··Ä··ë·¸··»·|·V·
00000090  8A 76 01 8A 4E 02 8A 6E-03 CD 13 66 61 73 1C FE  ·v··N··n·Í·fas·þ
000000a0  4E 11 75 0C 80 7E 00 80-0F 84 8A 00 B2 80 EB 84  N·u··~·······²·ë·
000000b0  55 32 E4 8A 56 00 CD 13-5D EB 9E 81 3E FE 7D 55  U2ä·V·Í·]ë··>þ}U
000000c0  AA 75 6E FF 76 00 E8 8D-00 75 17 FA B0 D1 E6 64  ªunÿv·è··u·ú°Ñæd
000000d0  E8 83 00 B0 DF E6 60 E8-7C 00 B0 FF E6 64 E8 75  è··°ßæ`è|·°ÿædèu
000000e0  00 FB B8 00 BB CD 1A 66-23 C0 75 3B 66 81 FB 54  ·û¸·»Í·f#Àu;f·ûT
000000f0  43 50 41 75 32 81 F9 02-01 72 2C 66 68 07 BB 00  CPAu2·ù··r,fh·»·
00000100  00 66 68 00 02 00 00 66-68 08 00 00 00 66 53 66  ·fh····fh····fSf
00000110  53 66 55 66 68 00 00 00-00 66 68 00 7C 00 00 66  SfUfh····fh·|··f
00000120  61 68 00 00 07 CD 1A 5A-32 F6 EA 00 7C 00 00 CD  ah···Í·Z2öê·|··Í
00000130  18 A0 B7 07 EB 08 A0 B6-07 EB 03 A0 B5 07 32 E4  ····ë··¶·ë··µ·2ä
00000140  05 00 07 8B F0 AC 3C 00-74 09 BB 07 00 B4 0E CD  ····ð¬<·t·»··´·Í
00000150  10 EB F2 F4 EB FD 2B C9-E4 64 EB 00 24 02 E0 F8  ·ëòôëý+Éädë·$·àø
00000160  24 02 C3 49 6E 76 61 6C-69 64 20 70 61 72 74 69  $·ÃInvalid parti
00000170  74 69 6F 6E 20 74 61 62-6C 65 00 45 72 72 6F 72  tion table·Error
00000180  20 6C 6F 61 64 69 6E 67-20 6F 70 65 72 61 74 69   loading operati
00000190  6E 67 20 73 79 73 74 65-6D 00 4D 69 73 73 69 6E  ng system·Missin
000001a0  67 20 6F 70 65 72 61 74-69 6E 67 20 73 79 73 74  g operating syst
000001b0  65 6D 00 00 00 63 7B 9A-94 B8 6A 76 00 00 80 20  em···c{··¸jv····
000001c0  21 00 07 DF 13 0C 00 08-00 00 00 20 03 00 00 DF  !··ß···········ß
000001d0  14 0C 07 FE FF FF 00 28-03 00 00 18 F6 0D 00 00  ···þÿÿ·(····ö···
000001e0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
000001f0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 55 AA  ··············Uª
00000200  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
```

7. Please transform the memory address: hex value of 01f0+16 to decimal: $1*16^2$+f*16+16 = 512, note the decimal value of f is 15. Hex values (0-9, A, B, C, D, E, F)
8. Please locate the Partition table (with 4 entries, each has 16 bytes), 64 bytes before the MBR signature 55 AA



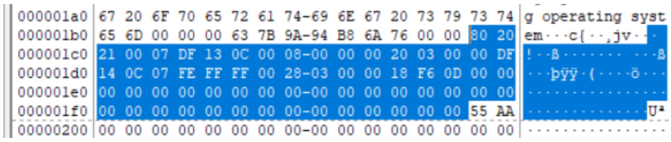
```
000001a0  67 20 6F 70 65 72 61 74-69 6E 67 20 73 79 73 74  g operating syst
000001b0  65 6D 00 00 00 63 7B 9A-94 B8 6A 76 00 00 80 20  em···c{··¸jv····
000001c0  21 00 07 DF 13 0C 00 08-00 00 00 20 03 00 00 DF  !··ß···········ß
000001d0  14 0C 07 FE FF FF 00 28-03 00 00 18 F6 0D 00 00  ···þÿÿ·(····ö···
000001e0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
000001f0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 55 AA  ··············Uª
00000200  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
```

9. Please locate the first entry, the hex value of the first byte – indication of whether this partition is the bootup partition with the operating system, 0 means NO, 8 means YES.



```
000001a0  67 20 6F 70 65 72 61 74-69 6E 67 20 73 79 73 74  g operating syst
000001b0  65 6D 00 00 00 63 7B 9A-94 B8 6A 76 00 00 80 20  em···c{··¸jv····
000001c0  21 00 07 DF 13 0C 00 08-00 00 00 20 03 00 00 DF  !··ß···········ß
000001d0  14 0C 07 FE FF FF 00 28-03 00 00 18 F6 0D 00 00  ···þÿÿ·(····ö···
000001e0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
000001f0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 55 AA  ··············Uª
00000200  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
```

10. Please locate the first entry, the fifth byte with a hex value of 07– indication of what type of file system this partition is, 07 means NTFS, 83 means Linux, 02-04 and some other value means FAT, 05 means extended partition (to hold more partitions).



```
000001a0  67 20 6F 70 65 72 61 74-69 6E 67 20 73 79 73 74  g operating syst
000001b0  65 6D 00 00 00 63 7B 9A-94 B8 6A 76 00 00 80 20  em···c{··¸jv····
000001c0  21 00 07 DF 13 0C 00 08-00 00 00 20 03 00 00 DF  !··ß···········ß
000001d0  14 0C 07 FE FF FF 00 28-03 00 00 18 F6 0D 00 00  ···þÿÿ·(····ö···
000001e0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
000001f0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 55 AA  ··············Uª
00000200  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
```

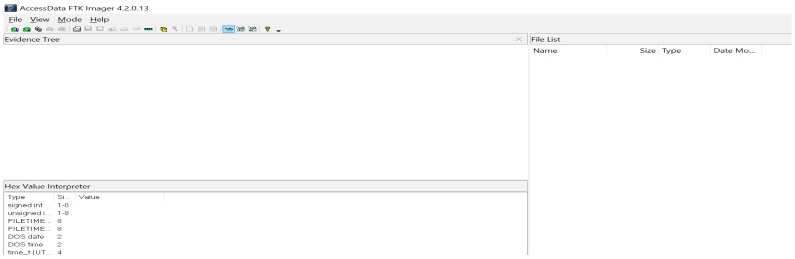
11. The 16 bytes contains many other information, for example, byte 1-3 records the corresponding partition starting address, byte 5-7 records the ending address, while byte 12-15 records the size for each sector, etc.

This is the end of the NTFS File system examination by using FTK Imager

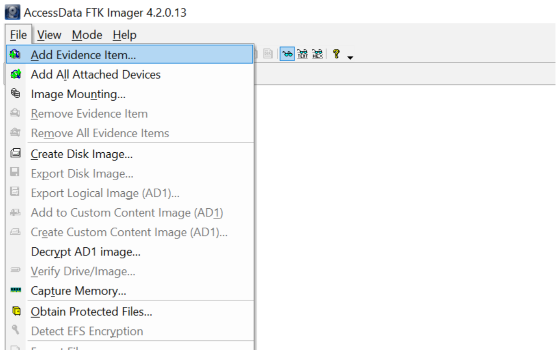
Part II – FAT File System Examination

Steps:

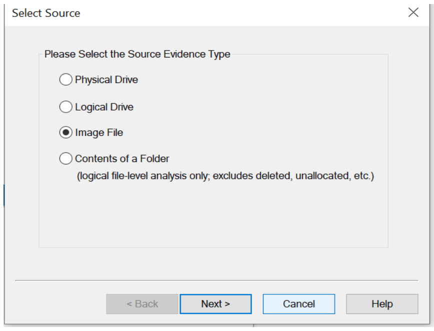
1. Run FTK Imager



2. Select the file and click the add evidence option



3. On the new pop-up window, select the **image file** option (not the default option),


Select Source

Please Select the Source Evidence Type

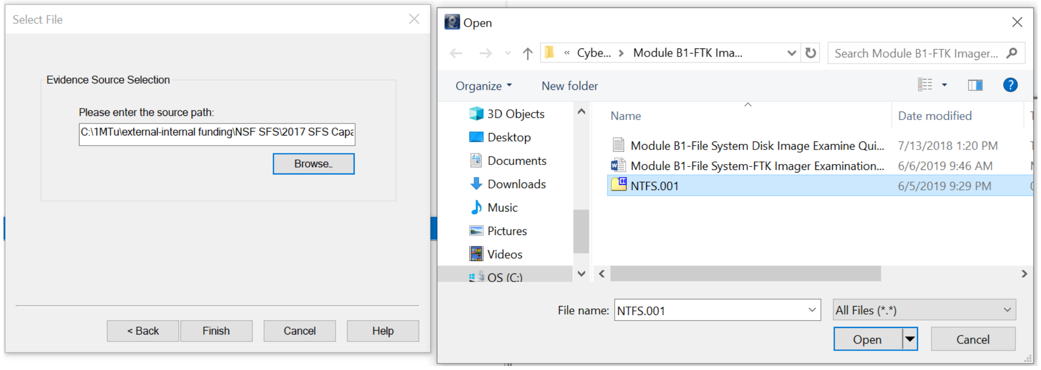
○ Physical Drive

○ Logical Drive

● Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

4. then next, and browse to the *NTFS.001* (not the txt file)


Select File

Evidence Source Selection

Please enter the source path:
C:\1MTu\external-internal funding\NSF SFS\2017 SFS Capa

Name	Date modified
Module B1-File System Disk Image Examine Qui...	7/13/2018 1:20 PM
Module B1-File System-FTK Imager Examination...	6/6/2019 9:46 AM
NTFS.001	6/5/2019 9:29 PM

File name: NTFS.001

All Files (*.*)