Digital forensics: hands-on exercise (Scenario & Step by Step Guide)

July 13, 2021 (Tuesday), 11:00 – 11:45 am
Instructor: Claire Seungeun Lee, Ph.D. (UMass Lowell, claire_lee@uml.edu)

Objectives / tasks of the day
a. Creating a disc image
b. Opening the images of the deleted files

Files to use (please note that option a. and option b. are the same):
Option a. ICNC.001 & Option b. GenCyber2021.001

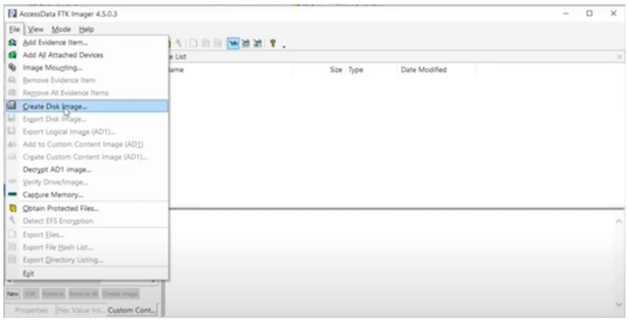
STEP-BY-STEP GUIDE

1. Launch FTK Imager (Pre-requisite: Install the software (it's already installed on your VM))

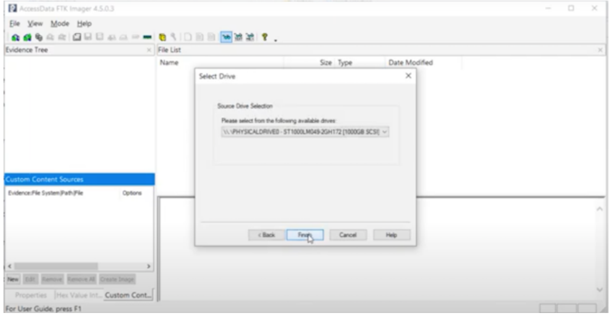
a. Click on the Start Button
b. All Programs --> AccessData --> FTK Imager

2. Create Disk Image

a. File --> Create Disk Image …

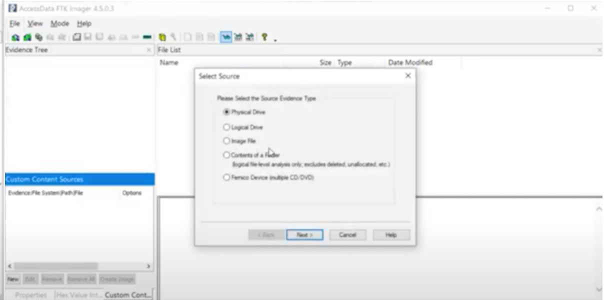


b. A window will appear. Select the correct drive type for the situation. For this exercise, select "Physical Drive" as the Source Evidence Type


Select Drive

Source Drive Selection

Please select from the following available drives:
\\.\PHYSICALDRIVE0 - ST1000LM049-2GH172 [1000GB SCSI]

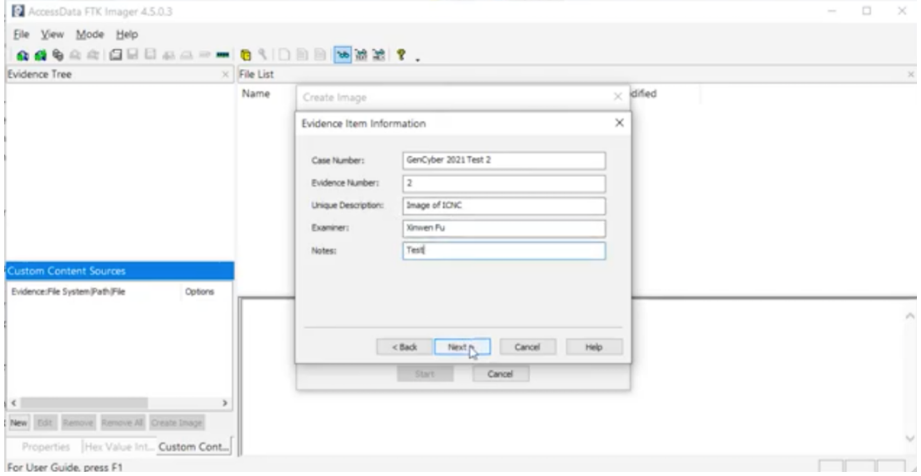

Select Source

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.)
○ Fernico Device (multiple CD/DVD)

c. "Select Image Type": Raw (dd) for this exercise

d. An "Evidence Item Information" window will appear.



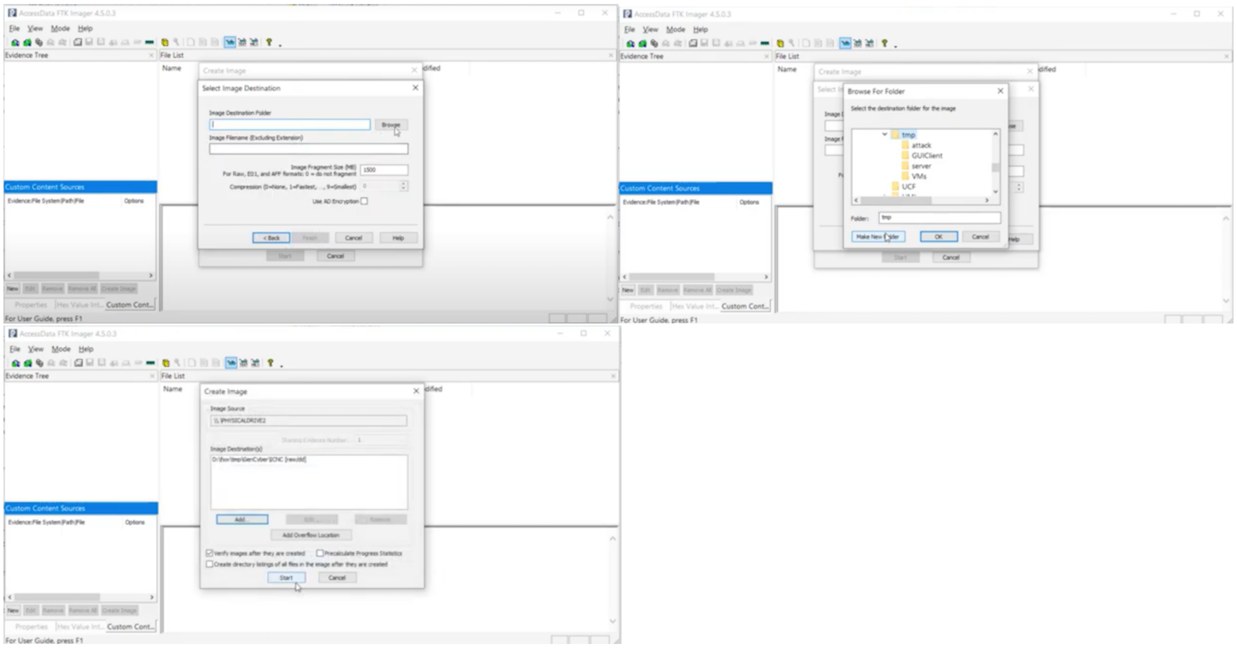
AccessData FTK Imager 4.5.0.3

Evidence Item Information

Case Number: GenCyber 2021 Test 2
Evidence Number: 2
Unique Description: Image of ICNC
Examiner: Xinwen Fu
Notes: Test

Case Number: GenCyber 2021 Test 2
Evidence Number: 2
Unique Description: Image of ICNC
Examiner: Your name
Notes: Test

e. "Select Image Destination" (Choose the relevant path in your VM/computer)



Select Image Destination

Image Destination Folder:
Image Filename (Excluding Extension):
Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment: 1500
Compression (0=None, 1=Fastest, ..., 9=Smallest): 0
Use AD Encryption ☐

Browse For Folder

Select the destination folder for the image

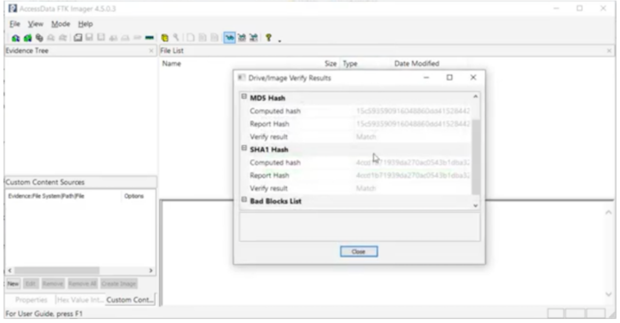
Folder: tmp

Create Image

Image Source: \\.\PHYSICALDRIVE2
Starting Evidence Number: 1
Image Destination(s): D:\fxw\tmp\GenCyber\ICNC [raw/dd]

☑ Verify images after they are created
☐ Precalculate Progress Statistics
☐ Create directory listings of all files in the image after they are created

f. "Drive/Image Verify Results" will pop up.



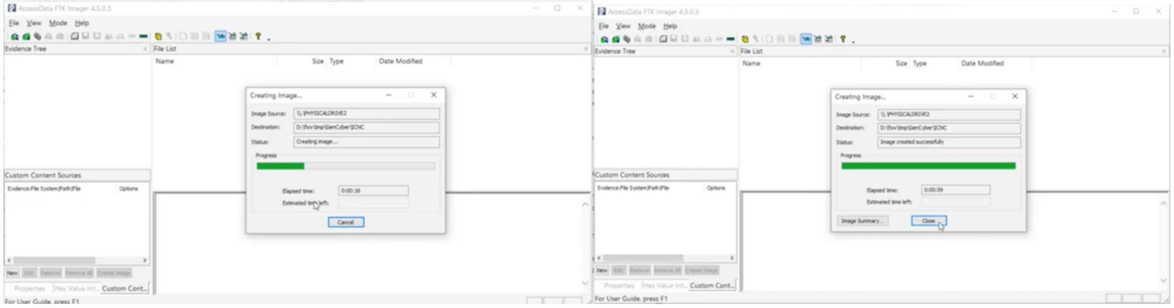
Drive/Image Verify Results

MD5 Hash
Computed hash: 15c5935909160488 60dd41528442
Report Hash: 15c5935909160488 60dd41528442
Verify result: Match

SHA1 Hash
Computed hash: 4ccd1b71939da270ac0543b1dba32
Report Hash: 4ccd1b71939da270ac0543b1dba32
Verify result: Match

Bad Blocks List

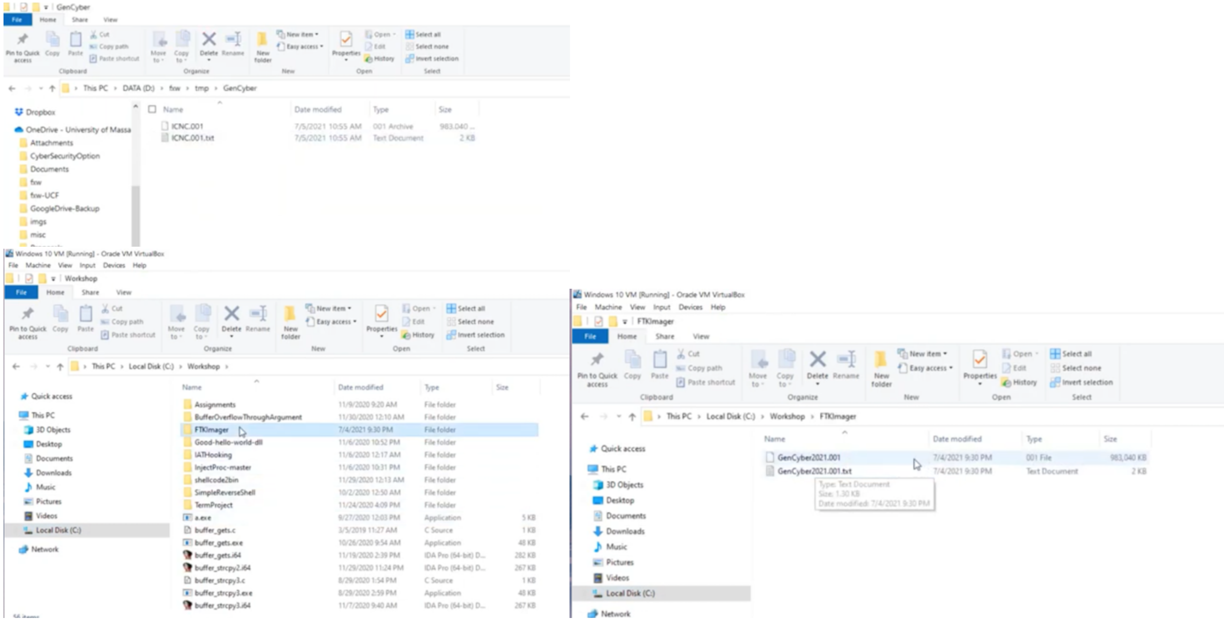
g. Creating Image …



```
Creating Image...
Image Source:   \\.\PHYSICALDRIVE2
Destination:    D:\fxw\tmp\GenCyber\ICNC
Status:         Creating image....
Progress
Elapsed time:         0:00:16
Estimated time left:
                [Cancel]
```

```
Creating Image...
Image Source:   \\.\PHYSICALDRIVE2
Destination:    D:\fxw\tmp\GenCyber\ICNC
Status:         Image created successfully
Progress
Elapsed time:         0:00:59
Estimated time left:
[Image Summary...]      [Close]
```

h. Go to the path/folder you used in d. to check

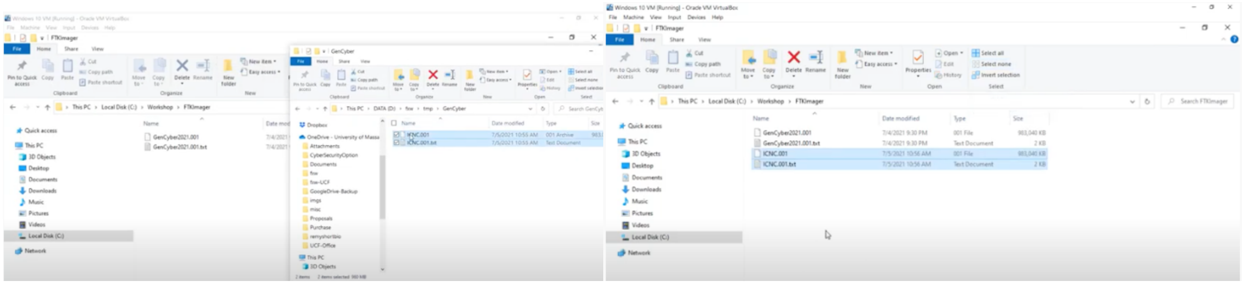


```
This PC > DATA (D:) > fxw > tmp > GenCyber
Name            Date modified        Type           Size
ICNC.001        7/5/2021 10:55 AM    001 Archive    983,040 ...
ICNC.001.txt    7/5/2021 10:55 AM    Text Document  2 KB
```

```
This PC > Local Disk (C:) > Workshop
Name                              Date modified        Type                 Size
Assignments                       11/9/2020 9:20 AM    File folder
BufferOverflowThroughArgument     11/30/2020 12:10 AM  File folder
FTKImager                         7/4/2021 9:30 PM     File folder
Good-hello-world-dll              11/6/2020 10:52 PM   File folder
IATHooking                        11/6/2020 12:17 AM   File folder
InjectProc-master                 11/6/2020 10:31 PM   File folder
shellcode2bin                     11/29/2020 12:13 AM  File folder
SimpleReverseShell                10/2/2020 12:50 AM   File folder
TermProject                       11/24/2020 4:09 PM   File folder
a.exe                             9/27/2020 12:03 PM   Application            5 KB
buffer_gets.c                     3/5/2019 11:27 AM    C Source               1 KB
buffer_gets.exe                   10/26/2020 9:54 AM   Application           48 KB
buffer_gets.i64                   11/19/2020 2:39 PM   IDA Pro (64-bit) D...  282 KB
buffer_strcpy2.i64                11/29/2020 11:24 PM  IDA Pro (64-bit) D...  267 KB
buffer_strcpy3.c                  8/29/2020 1:54 PM    C Source               1 KB
buffer_strcpy3.exe                8/29/2020 2:59 PM    Application           48 KB
buffer_strcpy3.i64                11/7/2020 9:40 AM    IDA Pro (64-bit) D...  267 KB
```

```
This PC > Local Disk (C:) > Workshop > FTKImager
Name                    Date modified       Type           Size
GenCyber2021.001        7/4/2021 9:30 PM    001 File       983,040 KB
GenCyber2021.001.txt    7/4/2021 9:30 PM    Text Document  2 KB
    Type: Text Document
    Size: 1.30 KB
    Date modified: 7/4/2021 9:30 PM
```

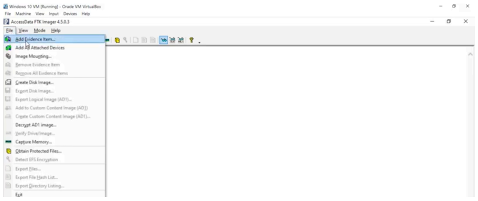
i. (Optional step) Copy the image files



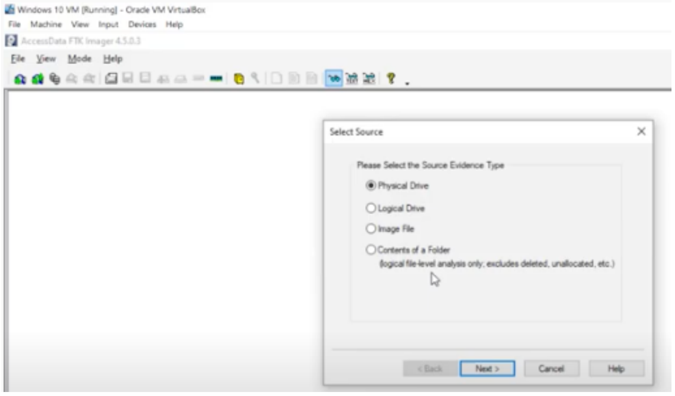
```
This PC > Local Disk (C:) > Workshop > FTKImager
Name                    Date modified       Type           Size
GenCyber2021.001        7/4/2021 9:30 PM    001 File       983,040 KB
GenCyber2021.001.txt    7/4/2021 9:30 PM    Text Document  2 KB
ICNC.001                7/5/2021 10:56 AM   001 File       983,040 KB
ICNC.001.txt            7/5/2021 10:56 AM   Text Document  2 KB
```

3. Add Evidence Item

a. File → Add Evidence Item


Windows 10 VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
AccessData FTK Imager 4.5.0.3
File View Mode Help
Add Evidence Item...
Add All Attached Devices
Image Mounting...
Remove Evidence Item
Remove All Evidence Items
Create Disk Image...
Export Disk Image...
Export Logical Image (AD1)...
Add to Custom Content Image (AD1)
Create Custom Content Image (AD1)...
Decrypt AD1 image...
Verify Drive/Image...
Capture Memory...
Obtain Protected Files...
Detect EFS Encryption
Export Files...
Export File Hash List...
Export Directory Listing...
Exit

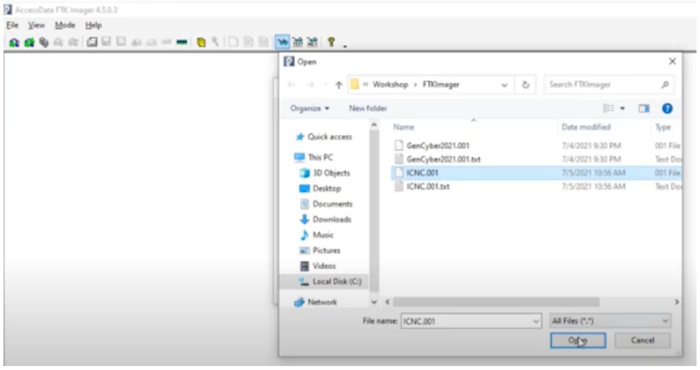
b. A window will appear. Select the correct drive type for the situation. For this exercise, select "Physical Drive" as the Source Evidence Type


Windows 10 VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
AccessData FTK Imager 4.5.0.3
File View Mode Help
Select Source
< Back
Next >
Cancel
Help

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.)

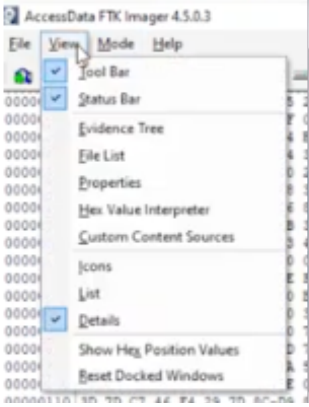
c. Open the image file ("ICNC.001") from the folder where the file is located

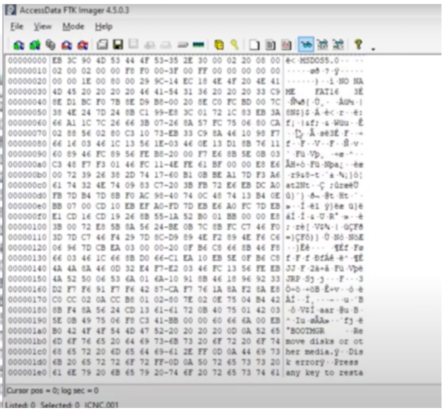


Name	Date modified	Type
GenCyber2021.001	7/4/2021 9:30 PM	001 File
GenCyber2021.001.txt	7/4/2021 9:30 PM	Text Do
ICNC.001	7/5/2021 10:56 AM	001 File
ICNC.001.txt	7/5/2021 10:56 AM	Text Do

File name: ICNC.001
All Files (*.*)

d. "View"



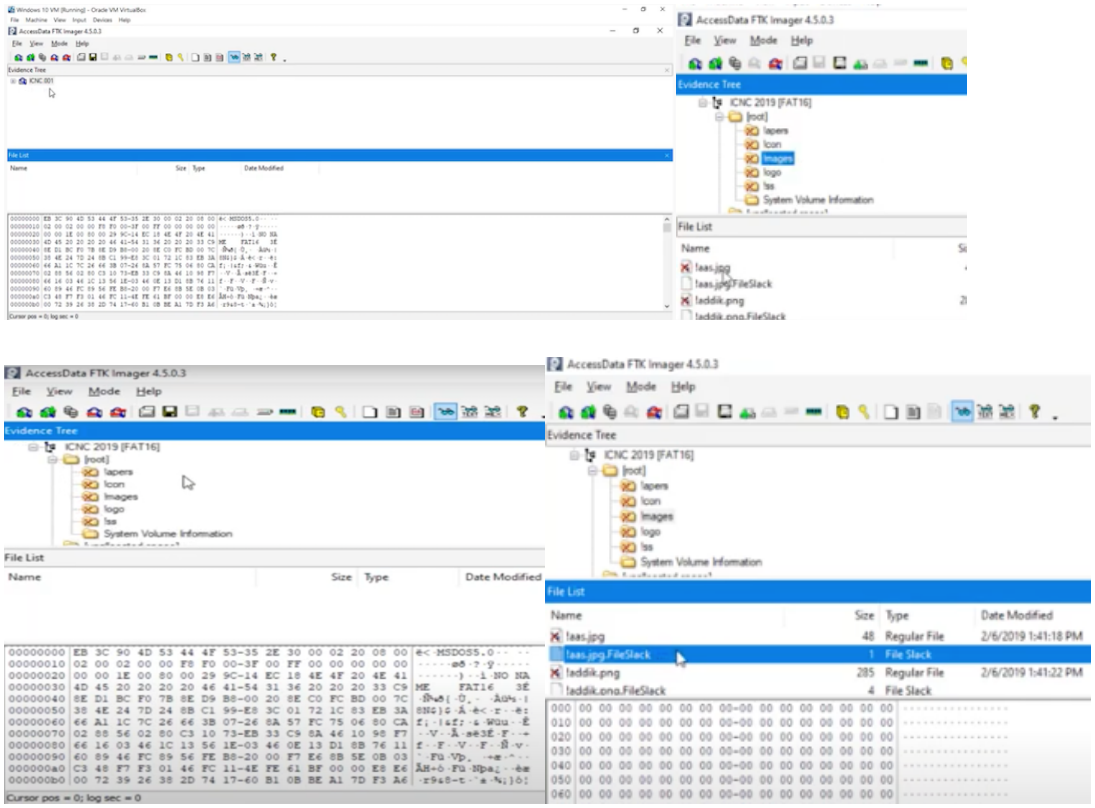


```
00000000 EB 3C 90 4D 53 44 4F 53-35 2E 30 00 02 20 08 00  ë<·MSDOS5.0·· ··
00000010 02 00 02 00 00 F8 F0 00-3F 00 FF 00 00 00 00 00  ·····øð·?·ÿ·····
00000020 00 00 1E 00 80 00 29 9C-14 EC 18 4E 4F 20 4E 41  ······)··ì·NO NA
00000030 4D 45 20 20 20 20 46 41-54 31 36 20 20 20 33 C9  ME    FAT16   3É
00000040 8E D1 BC F0 7B 8E D9 B8-00 20 8E C0 FC BD 00 7C  ·Ñ¼ð{·Ù¸· ·Àü½·|
00000050 38 4E 24 7D 24 8B C1 99-E8 3C 01 72 1C 83 EB 3A  8N$}$·Á·è<·r··ë:
00000060 66 A1 1C 7C 26 66 3B 07-26 8A 57 FC 75 06 80 CA  f¡·|&f;·&·Wüu··Ê
00000070 02 88 56 02 80 C3 10 73-EB 33 C9 8A 46 10 98 F7  ··V··Ã·së3É·F··÷
00000080 66 16 03 46 1C 13 56 1E-03 46 0E 13 D1 8B 76 11  f··F··V··F··Ñ·v·
00000090 60 89 46 FC 89 56 FE B8-20 00 F7 E6 8B 5E 0B 03  `·Fü·Vþ¸ ·÷æ·^··
000000a0 C3 48 F7 F3 01 46 FC 11-4E FE 61 BF 00 00 E8 E6  ÃH÷ó·Fü·Nþa¿··èæ
000000b0 00 72 39 26 38 2D 74 17-60 B1 0B BE A1 7D F3 A6  ·r9&8-t·`±·¾¡}ó¦
000000c0 61 74 32 4E 74 09 83 C7-20 3B FB 72 E6 EB DC A0  at2Nt··Ç ;ûræëÜ
000000d0 FB 7D B4 7D 8B F0 AC 98-40 74 0C 48 74 13 B4 0E  û}´}·ð¬·@t·Ht·´·
000000e0 BB 07 00 CD 10 EB EF A0-FD 7D EB E6 A0 FC 7D EB  »··Í·ëï ý}ëæ ü}ë
000000f0 E1 CD 16 CD 19 26 8B 55-1A 52 B0 01 BB 00 00 E8  áÍ·Í·&·U·R°·»··è
00000100 3B 00 72 E8 5B 8A 56 24-BE 0B 7C 8B FC C7 46 F0  ;·rè[·V$¾·|·üÇFð
00000110 3D 7D C7 46 F4 29 7D 8C-D9 89 4E F2 89 4E F6 C6  =}ÇFô)}·Ù·Nò·NöÆ
00000120 06 96 7D CB EA 03 00 00-20 0F B6 C8 66 8B 46 F8  ··}Ëê··· ·¶Èf·Fø
00000130 66 03 46 1C 66 8B D0 66-C1 EA 10 EB 5E 0F B6 C8  f·F·f·ÐfÁê·ë^·¶È
00000140 4A 4A 8A 46 0D 32 E4 F7-E2 03 46 FC 13 56 FE EB  JJ·F·2ä÷â·Fü·Vþë
00000150 4A 52 50 06 53 6A 01 6A-10 91 8B 46 18 96 92 33  JRP·Sj·j···F···3
00000160 D2 F7 F6 91 F7 F6 42 87-CA F7 76 1A 8A F2 8A E8  Ò÷ö·÷öB·Ê÷v··ò·è
00000170 C0 CC 02 0A CC B8 01 02-80 7E 02 0E 75 04 B4 42  ÀÌ··Ì¸···~··u·´B
00000180 8B F4 8A 56 24 CD 13 61-61 72 0B 40 75 01 42 03  ·ô·V$Í·aar·@u·B·
00000190 5E 0B 49 75 06 F8 C3 41-BB 00 00 60 66 6A 00 EB  ^·Iu·øÃA»··`fj·ë
000001a0 B0 42 4F 4F 54 4D 47 52-20 20 20 20 0D 0A 52 65  °BOOTMGR    ··Re
000001b0 6D 6F 76 65 20 64 69 73-6B 73 20 6F 72 20 6F 74  move disks or ot
000001c0 68 65 72 20 6D 65 64 69-61 2E FF 0D 0A 44 69 73  her media.ÿ··Dis
000001d0 6B 20 65 72 72 6F 72 FF-0D 0A 50 72 65 73 73 20  k errorÿ··Press 
000001e0 61 6E 79 20 6B 65 79 20-74 6F 20 72 65 73 74 61  any key to resta
```

Cursor pos = 0; log sec = 0

Listed: 0 Selected: 0 ICNC.001

e. Check the exiting and deleted files



Name	Size	Type	Date Modified
!aas.jpg	48	Regular File	2/6/2019 1:41:18 PM
!aas.jpg.FileSlack	1	File Slack	
!addik.png	285	Regular File	2/6/2019 1:41:22 PM
!addik.png.FileSlack	4	File Slack	

```
00000000  EB 3C 90 4D 53 44 4F 53-35 2E 30 00 02 20 08 00  ë<·MSDOS5.0·· ··
00000010  02 00 02 00 00 F8 F0 00-3F 00 FF 00 00 00 00 00  ·····øð·?·ÿ·····
00000020  00 00 1E 00 80 00 29 9C-14 EC 18 4E 4F 20 4E 41  ······)··ì·NO NA
00000030  4D 45 20 20 20 20 46 41-54 31 36 20 20 20 33 C9  ME    FAT16   3É
00000040  8E D1 BC F0 7B 8E D9 B8-00 20 8E C0 FC BD 00 7C  ·Ñ¼ð{·Ù¸· ·Àü½·|
00000050  38 4E 24 7D 24 8B C1 99-E8 3C 01 72 1C 83 EB 3A  8N$}$·Á·è<·r··ë:
00000060  66 A1 1C 7C 26 66 3B 07-26 8A 57 FC 75 06 80 CA  f¡·|&f;·&·Wüu··Ê
00000070  02 88 56 02 80 C3 10 73-EB 33 C9 8A 46 10 98 F7  ··V··Ã·së3É·F··÷
00000080  66 16 03 46 1C 13 56 1E-03 46 0E 13 D1 8B 76 11  f··F··V··F··Ñ·v·
00000090  60 89 46 FC 89 56 FE B8-20 00 F7 E6 8B 5E 0B 03  `·Fü·Vþ¸ ·÷æ·^··
000000a0  C3 48 F7 F3 01 46 FC 11-4E FE 61 BF 00 00 E8 E6  ÃH÷ó·Fü·Nþa¿··èæ
000000b0  00 72 39 26 38 2D 74 17-60 B1 0B BE A1 7D F3 A6  ·r9&8-t·`±·¾¡}ó¦
Cursor pos = 0; log sec = 0
```

```
000  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
010  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
020  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
030  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
040  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
050  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
060  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
```

More about the tool: FTK IMAGER

What is FTK Imager?

- The FTK toolkit includes a standalone disk imaging program called FTK Imager.
- The FTK Imager has the ability to save an image of a hard disk in one file or in segments that may be later reconstructed.
- The FTK Imager allows you to write an image file to a single destination or to simultaneously write multiple image files to multiple destinations using the same source data or drive.
- It calculates MD5 hash values and confirms the integrity of the data before closing the files.
- In addition to the FTK Imager tool can mount devices (e.g., drives) and recover deleted files.
- Functions: Image analysis, timeline analysis, data browsing, data recovery, hashing, etc.
- For FTK Imager's detailed user guide, please go to this link.