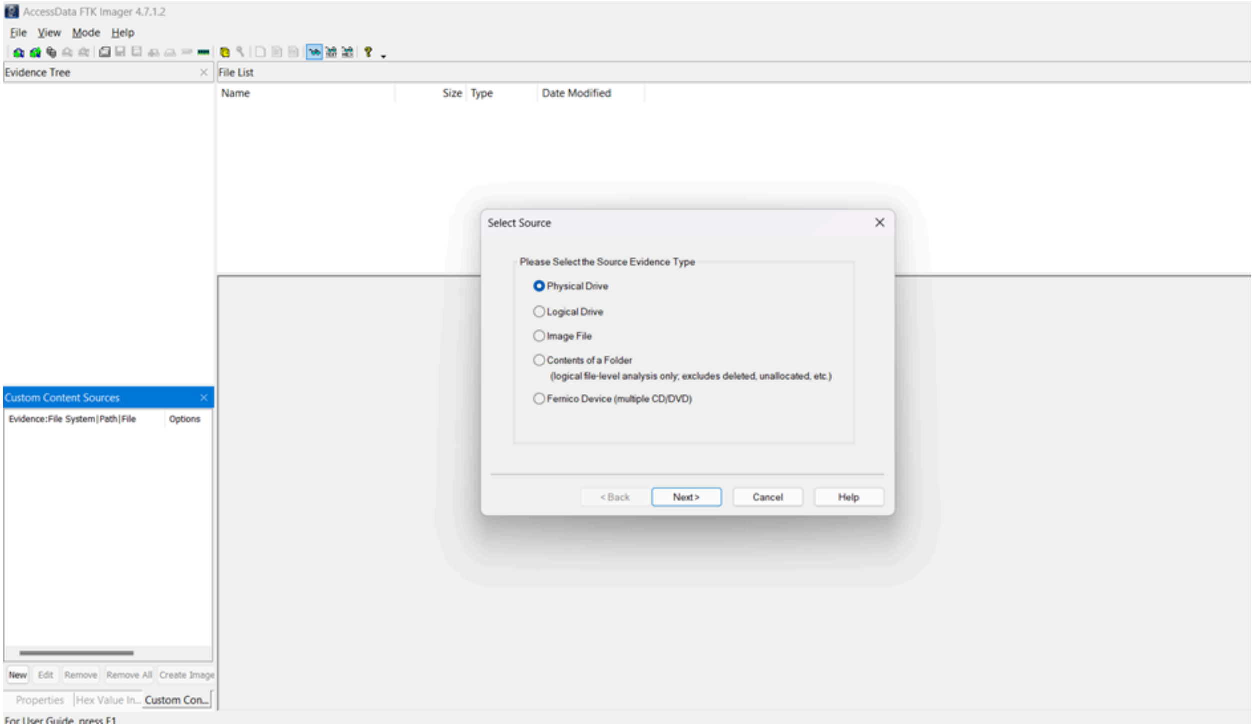
CBS322 DIGITAL FORENSICS LAB

Darisi Priyatham
2021BCY0016

```
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: 123
Evidence Number: 10234
Unique description: somethingunique
Examiner: AG3N7_V1KRAM
Notes: shh

--------------------------------------------------------------

Information for D:\practice\sandisk-santhanam:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1,945
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 31,260,672
[Physical Drive Information]
 Drive Model: SanDisk Cruzer Blade USB Device
 Drive Serial Number: 4C530000070218217325
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 15264 MB
 Sector count:    31260672
[Computed Hashes]
 MD5 checksum:    653a384efa2eff1eda94c18b8a131425
 SHA1 checksum:   6b2971eb32a52aa391748614835215971c26cfb6
```

```
Image Information:
 Acquisition started:   Tue Jan  9 14:40:57 2024
 Acquisition finished:  Tue Jan  9 14:50:43 2024
 Segment list:
  D:\practice\sandisk-santhanam.001
  D:\practice\sandisk-santhanam.002

Image Verification Results:
 Verification started:  Tue Jan  9 14:50:43 2024
 Verification finished: Tue Jan  9 14:51:24 2024
 MD5 checksum:    653a384efa2eff1eda94c18b8a131425 : verified
 SHA1 checksum:   6b2971eb32a52aa3917486148352l5971c26cfb6 : verified
```

Disk Image



Select Source

Please Select the Source Evidence Type

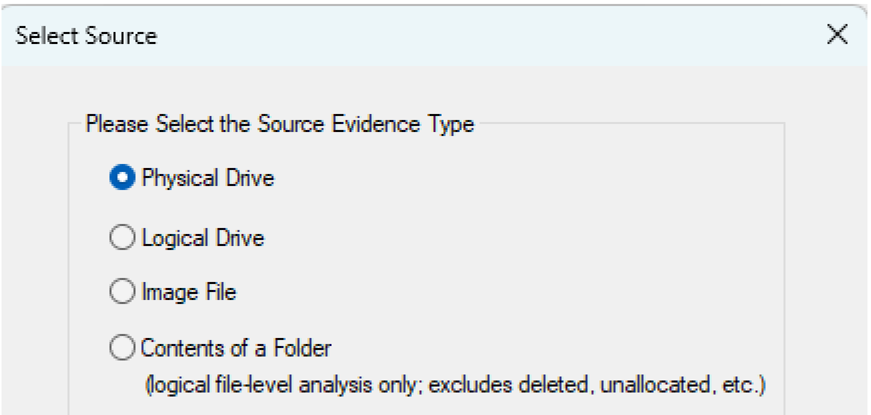
● Physical Drive

○ Logical Drive

○ Image File

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

○ Femico Device (multiple CD/DVD)



Select Source

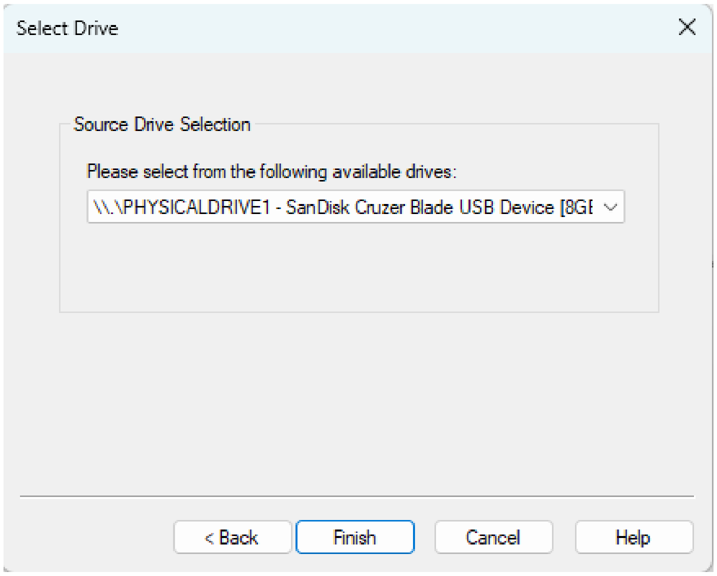
Please Select the Source Evidence Type

● Physical Drive

○ Logical Drive

○ Image File

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

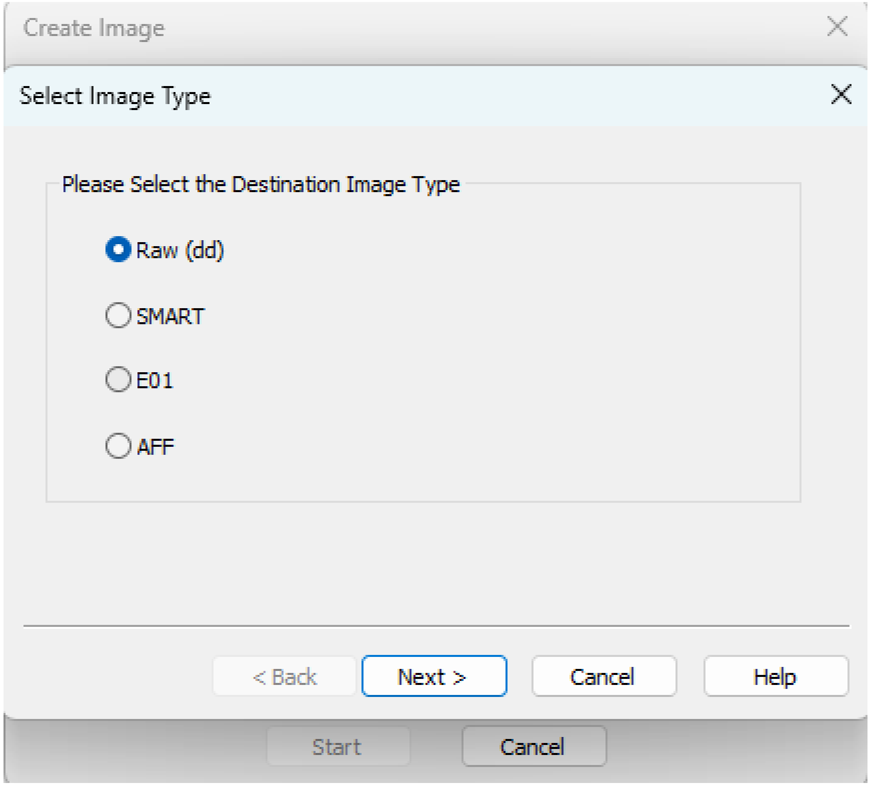


Select Drive

Source Drive Selection

Please select from the following available drives:

\\.\PHYSICALDRIVE1 - SanDisk Cruzer Blade USB Device [8GE



Create Image

Select Image Type

Please Select the Destination Image Type

● Raw (dd)

○ SMART

○ E01

○ AFF

File > Create Disk Image > Physical (bit by bit image) > Select disk > Raw/DD format (others are proprietary) >> Make sure you select "verify image after creation"

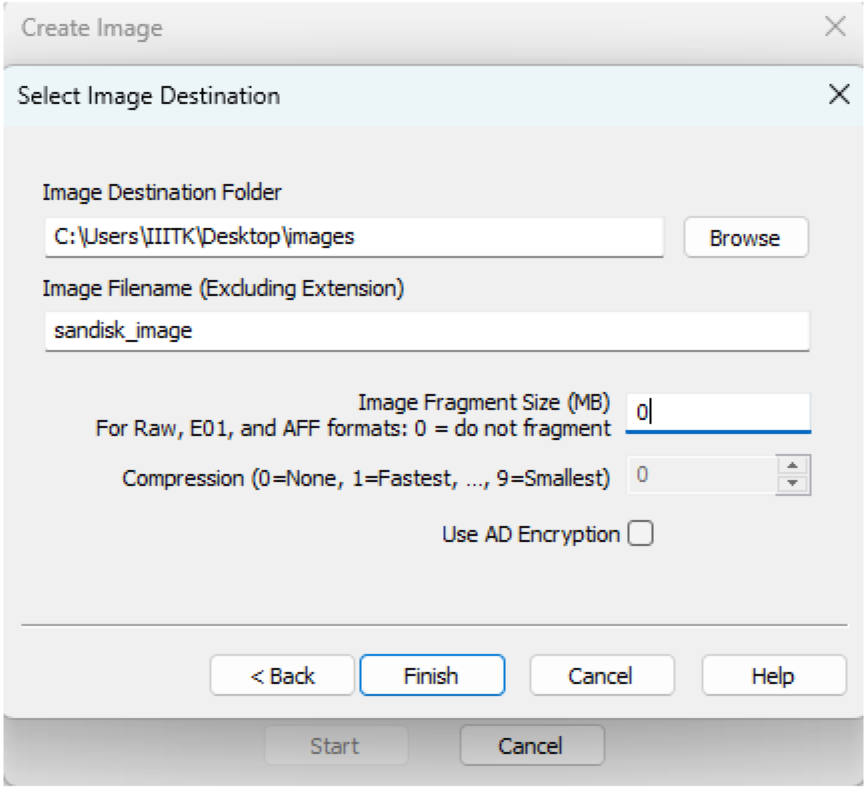


Image Destination Folder: C:\Users\IIITK\Desktop\images

Image Filename (Excluding Extension): sandisk_image

Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment: 0

Compression (0=None, 1=Fastest, ..., 9=Smallest): 0

Use AD Encryption □

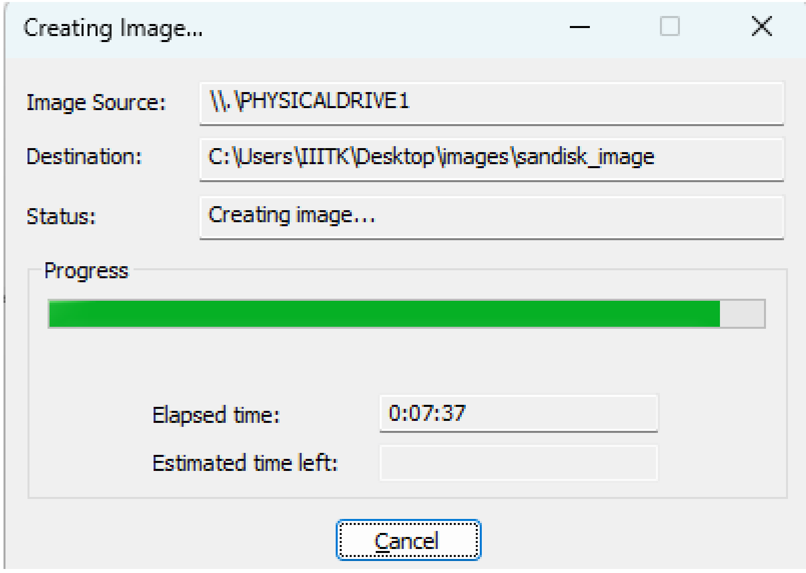


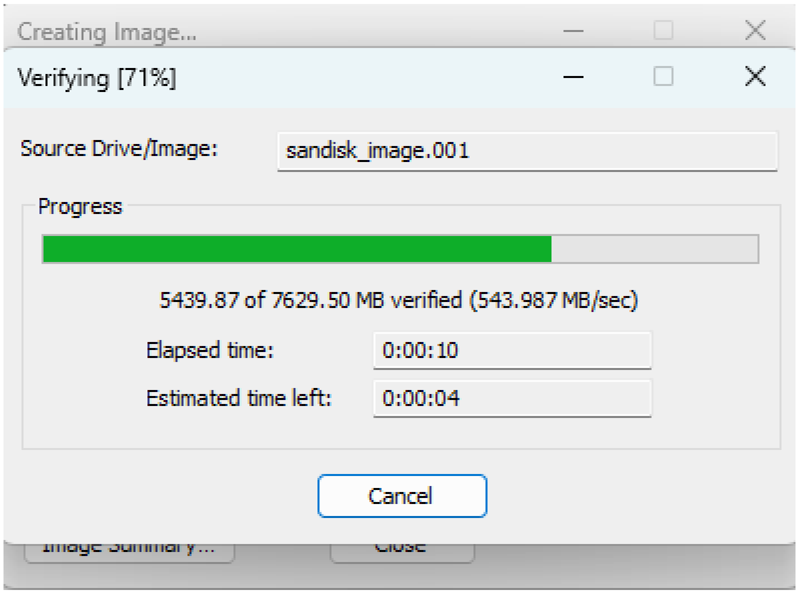
Image Source: \\.\PHYSICALDRIVE1

Destination: C:\Users\IIITK\Desktop\images\sandisk_image

Status: Creating image…

Elapsed time: 0:07:37

Estimated time left:



Creating Image...

Verifying [71%]

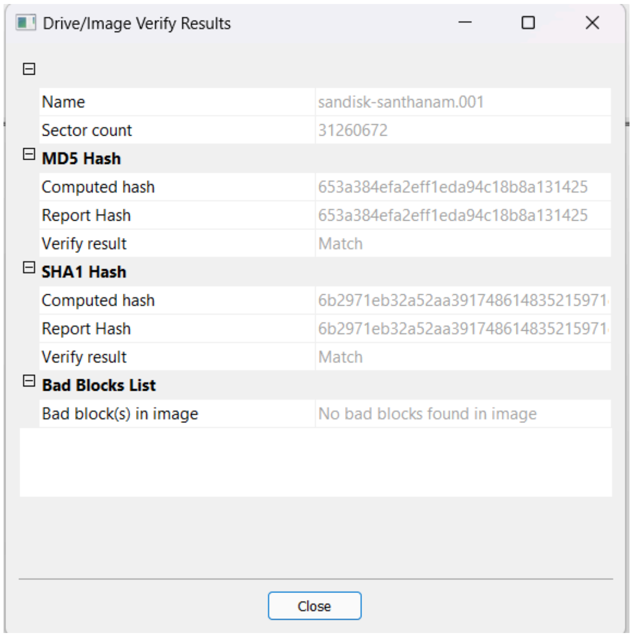
Source Drive/Image: sandisk_image.001

Progress

5439.87 of 7629.50 MB verified (543.987 MB/sec)

Elapsed time: 0:00:10

Estimated time left: 0:00:04

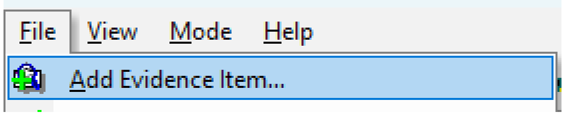


Drive/Image Verify Results

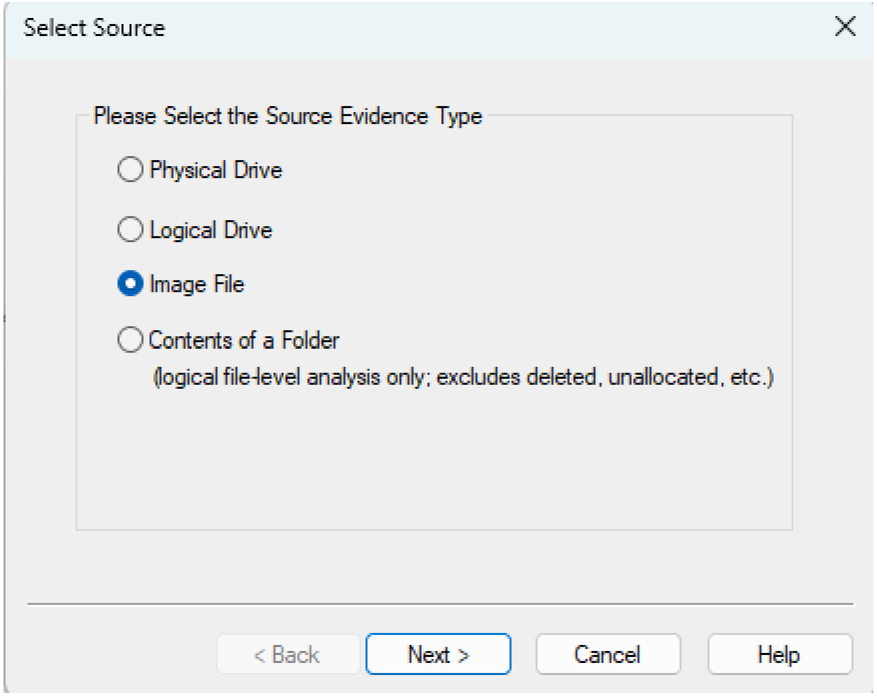
Name	sandisk-santhanam.001
Sector count	31260672
MD5 Hash	
Computed hash	653a384efa2eff1eda94c18b8a131425
Report Hash	653a384efa2eff1eda94c18b8a131425
Verify result	Match
SHA1 Hash	
Computed hash	6b2971eb32a52aa391748614835215971
Report Hash	6b2971eb32a52aa391748614835215971
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Check image summary, segmentation 0 means no segmentation made, change it and try
Pagefile - extension of RAM, when RAM is full, it will be moved to pagefile. It is 1.5x to 2x RAM size. RAW format is a good format since it's a binary format. It's a fast data transfer, but needs the same amount of storage as a disk. If proprietary format is used, that image can only be read by that software.

```
File > Add evidence > select item
```



We can inspect the disk image this way



Select Source

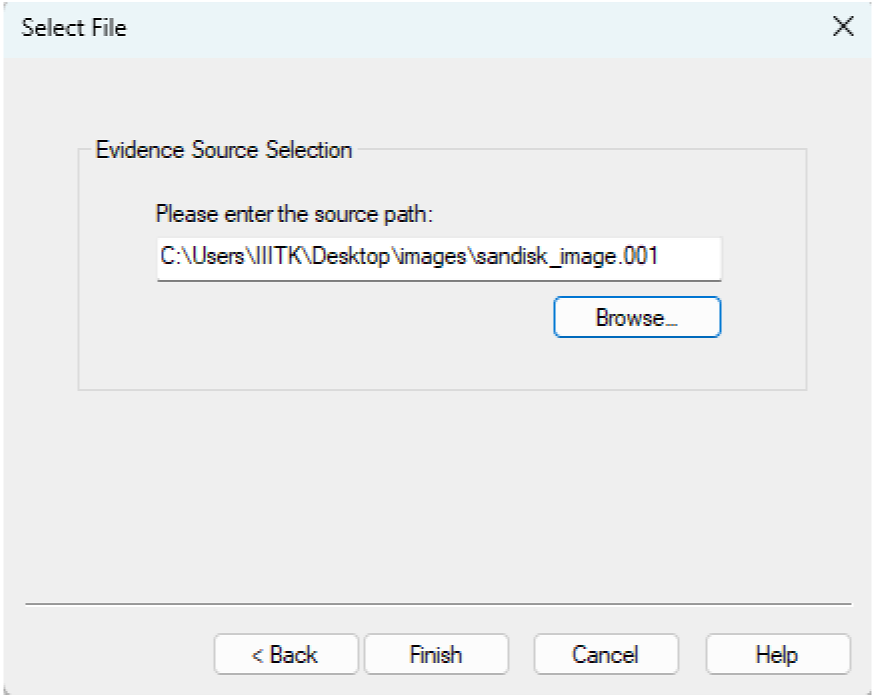
Please Select the Source Evidence Type

○ Physical Drive

○ Logical Drive

● Image File

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

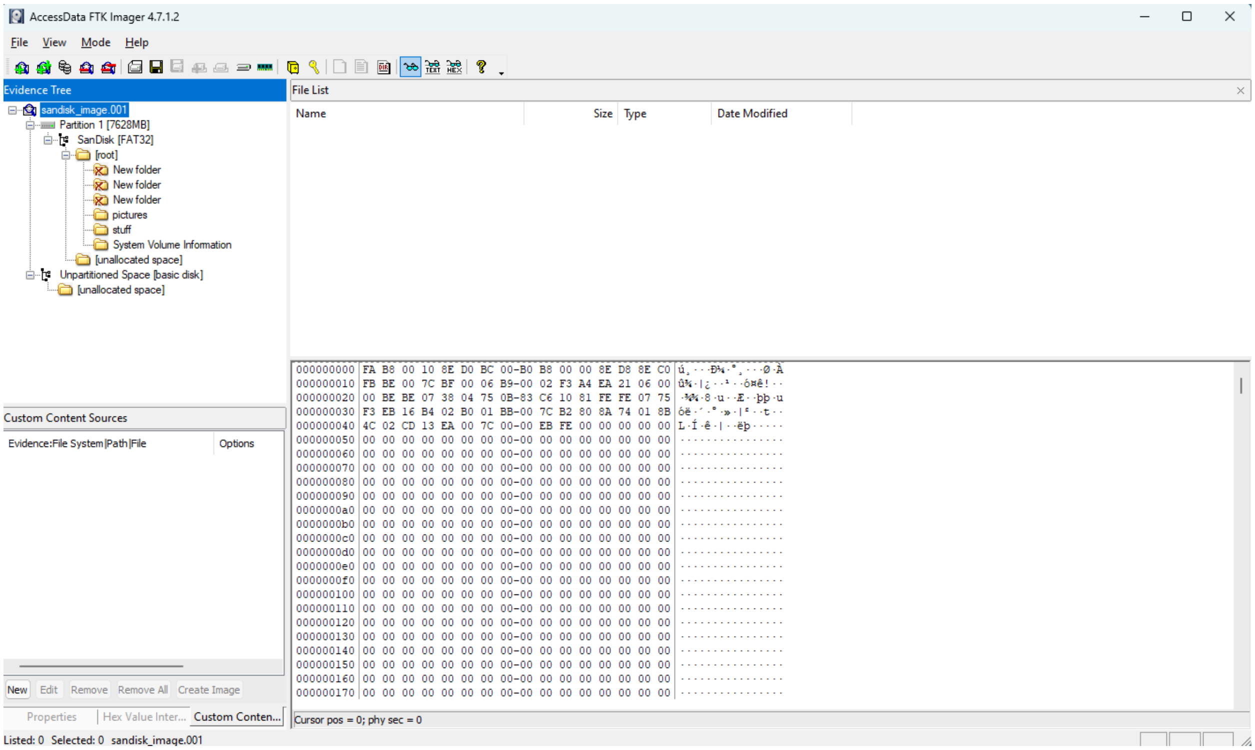


Select File

Evidence Source Selection

Please enter the source path:

C:\Users\IIITK\Desktop\images\sandisk_image.001

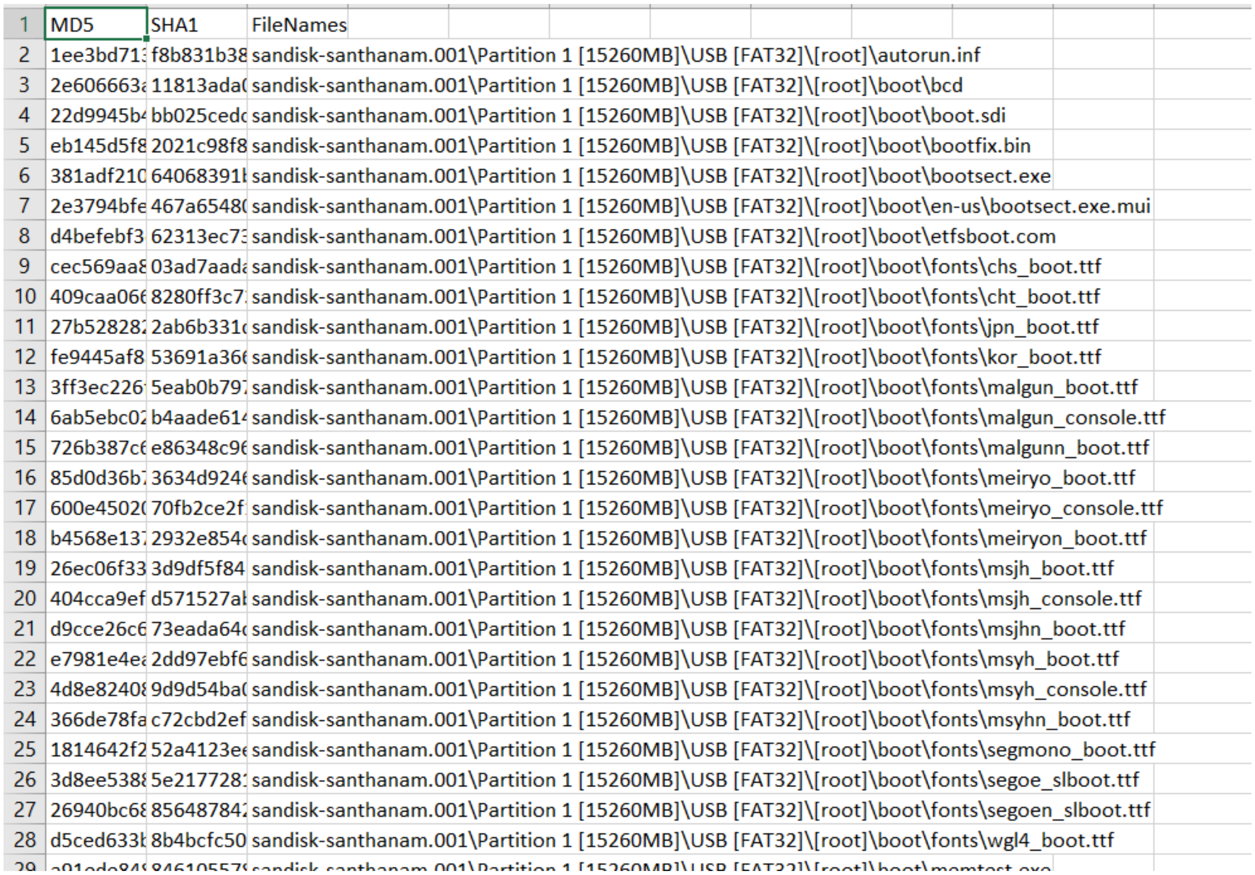


- sandisk_image.001
  - Partition 1 [7628MB]
    - SanDisk [FAT32]
      - [root]
        - New folder
        - New folder
        - New folder
        - pictures
        - stuff
        - System Volume Information
      - [unallocated space]
  - Unpartitioned Space [basic disk]
    - [unallocated space]

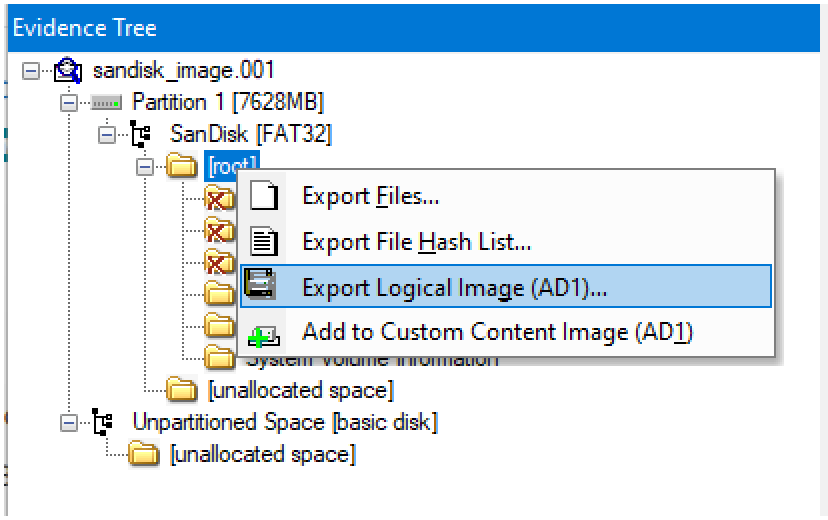
```
000000000 FA B8 00 10 8E D0 BC 00-B0 B8 00 00 8E D8 8E C0 ú¸···Ð¼·°¸···Ø·À
000000010 FB BE 00 7C BF 00 06 B9-00 02 F3 A4 EA 21 06 00 û¾·|¿··¹··ó¤ê!··
000000020 00 BE BE 07 38 04 75 0B-83 C6 10 81 FE FE 07 75 ·¾¾·8·u··Æ··þþ·u
000000030 F3 EB 16 B4 02 B0 01 BB-00 7C B2 80 8A 74 01 8B óë·´·°·»·|²··t··
000000040 4C 02 CD 13 EA 00 7C 00-00 EB FE 00 00 00 00 00 L·Í·ê·|··ëþ·····
000000050 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000000060 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000000070 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000000080 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000000090 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000c0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000000f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000000100 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000000110 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000000120 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000000130 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000000140 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000000150 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000000160 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000000170 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
```

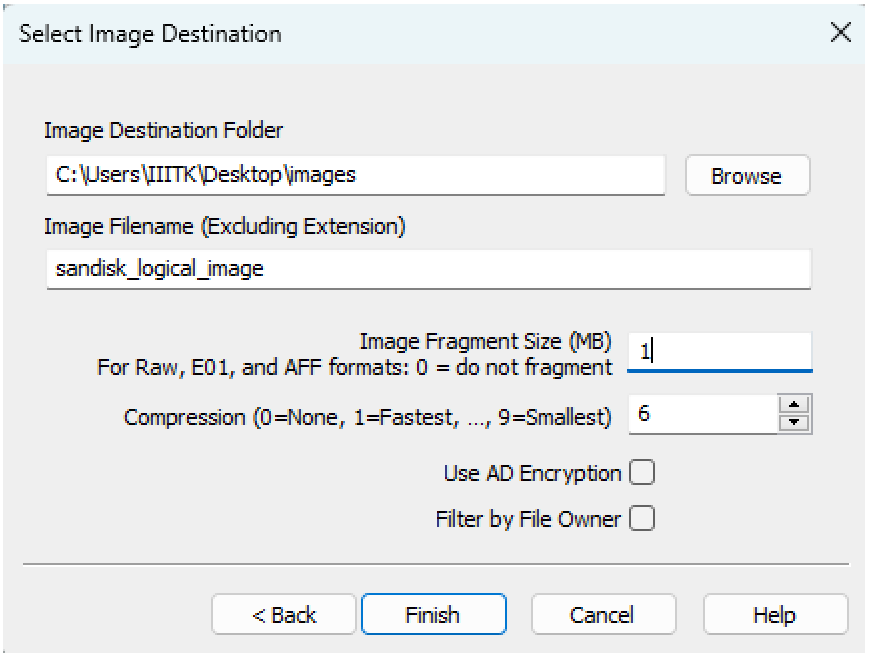
Cursor pos = 0; phy sec = 0

Listed: 0 Selected: 0 sandisk_image.001



	MD5	SHA1	FileNames
2	1ee3bd71	f8b831b38	sandisk-santhanam.001\Partition 1 [15260MB]\USB [FAT32]\[root]\autorun.inf
3	2e606663	11813ada	sandisk-santhanam.001\Partition 1 [15260MB]\USB [FAT32]\[root]\boot\bcd
4	22d9945b	bb025ced	sandisk-santhanam.001\Partition 1 [15260MB]\USB [FAT32]\[root]\boot\boot.sdi
5	eb145d5f8	2021c98f8	sandisk-santhanam.001\Partition 1 [15260MB]\USB [FAT32]\[root]\boot\bootfix.bin
6	381adf210	64068391	sandisk-santhanam.001\Partition 1 [15260MB]\USB [FAT32]\[root]\boot\bootsect.exe
7	2e3794bfe	467a6548	sandisk-santhanam.001\Partition 1 [15260MB]\USB [FAT32]\[root]\boot\en-us\bootsect.exe.mui
8	d4befebf3	62313ec7	sandisk-santhanam.001\Partition 1 [15260MB]\USB [FAT32]\[root]\boot\etfsboot.com
9	cec569aa	03ad7aad	sandisk-santhanam.001\Partition 1 [15260MB]\USB [FAT32]\[root]\boot\fonts\chs_boot.ttf
10	409caa06	8280ff3c7	sandisk-santhanam.001\Partition 1 [15260MB]\USB [FAT32]\[root]\boot\fonts\cht_boot.ttf
11	27b52828	2ab6b331	sandisk-santhanam.001\Partition 1 [15260MB]\USB [FAT32]\[root]\boot\fonts\jpn_boot.ttf
12	fe9445af8	53691a36	sandisk-santhanam.001\Partition 1 [15260MB]\USB [FAT32]\[root]\boot\fonts\kor_boot.ttf
13	3ff3ec226	5eab0b79	sandisk-santhanam.001\Partition 1 [15260MB]\USB [FAT32]\[root]\boot\fonts\malgun_boot.ttf
14	6ab5ebc0	b4aade61	sandisk-santhanam.001\Partition 1 [15260MB]\USB [FAT32]\[root]\boot\fonts\malgun_console.ttf
15	726b387c	e86348c9	sandisk-santhanam.001\Partition 1 [15260MB]\USB [FAT32]\[root]\boot\fonts\malgunn_boot.ttf
16	85d0d36b	3634d924	sandisk-santhanam.001\Partition 1 [15260MB]\USB [FAT32]\[root]\boot\fonts\meiryo_boot.ttf
17	600e4502	70fb2ce2f	sandisk-santhanam.001\Partition 1 [15260MB]\USB [FAT32]\[root]\boot\fonts\meiryo_console.ttf
18	b4568e13	2932e854	sandisk-santhanam.001\Partition 1 [15260MB]\USB [FAT32]\[root]\boot\fonts\meiryon_boot.ttf
19	26ec06f33	3d9df5f84	sandisk-santhanam.001\Partition 1 [15260MB]\USB [FAT32]\[root]\boot\fonts\msjh_boot.ttf
20	404cca9ef	d571527a	sandisk-santhanam.001\Partition 1 [15260MB]\USB [FAT32]\[root]\boot\fonts\msjh_console.ttf
21	d9cce26c6	73eada64	sandisk-santhanam.001\Partition 1 [15260MB]\USB [FAT32]\[root]\boot\fonts\msjhn_boot.ttf
22	e7981e4e	2dd97ebf6	sandisk-santhanam.001\Partition 1 [15260MB]\USB [FAT32]\[root]\boot\fonts\msyh_boot.ttf
23	4d8e8240	9d9d54ba	sandisk-santhanam.001\Partition 1 [15260MB]\USB [FAT32]\[root]\boot\fonts\msyh_console.ttf
24	366de78fa	c72cbd2ef	sandisk-santhanam.001\Partition 1 [15260MB]\USB [FAT32]\[root]\boot\fonts\msyhn_boot.ttf
25	1814642f2	52a4123e	sandisk-santhanam.001\Partition 1 [15260MB]\USB [FAT32]\[root]\boot\fonts\segmono_boot.ttf
26	3d8ee538	5e217728	sandisk-santhanam.001\Partition 1 [15260MB]\USB [FAT32]\[root]\boot\fonts\segoe_slboot.ttf
27	26940bc6	85648784	sandisk-santhanam.001\Partition 1 [15260MB]\USB [FAT32]\[root]\boot\fonts\segoen_slboot.ttf
28	d5ced633	8b4bcfc50	sandisk-santhanam.001\Partition 1 [15260MB]\USB [FAT32]\[root]\boot\fonts\wgl4_boot.ttf
29	a91ede84	84610557	sandisk-santhanam.001\Partition 1 [15260MB]\USB [FAT32]\[root]\boot\memtest.exe





Select Image Destination

Image Destination Folder: C:\Users\IIITK\Desktop\images

Image Filename (Excluding Extension): sandisk_logical_image

Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment: 1

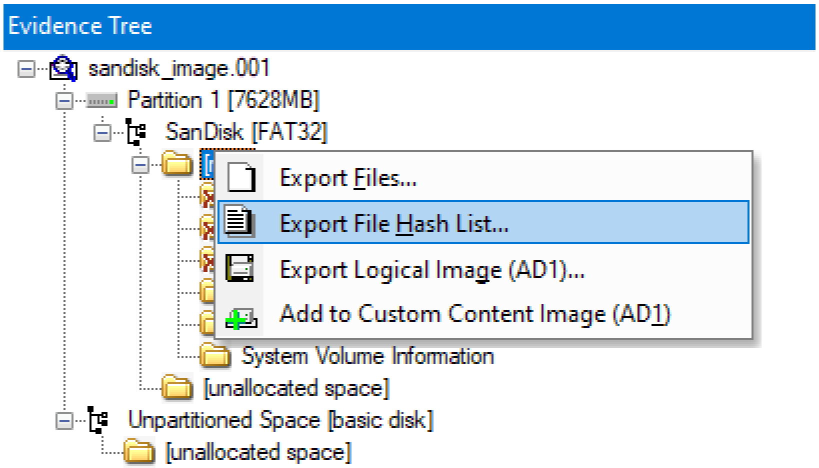
Compression (0=None, 1=Fastest, ..., 9=Smallest): 6

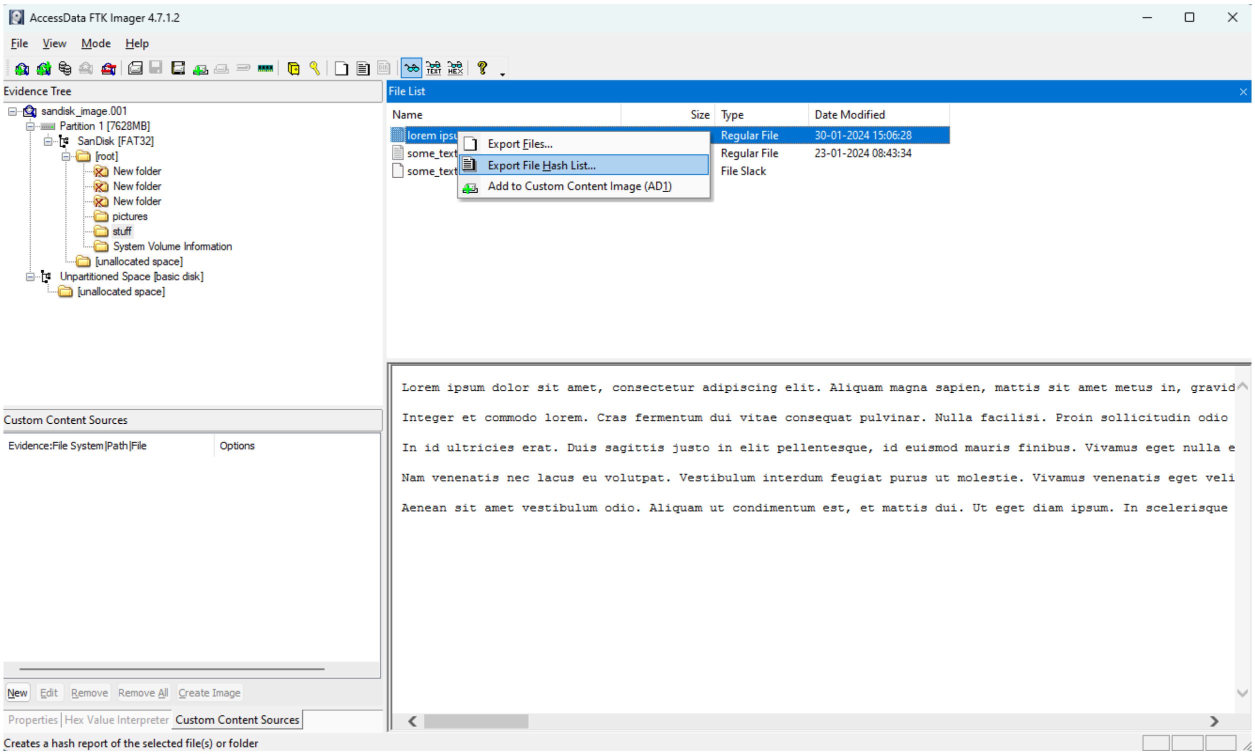
Use AD Encryption ☐

Filter by File Owner ☐

```
Right click > Export hashfile
```

FTK imager only makes images, although can see files in small pane, to see the file properly, we can mount and see



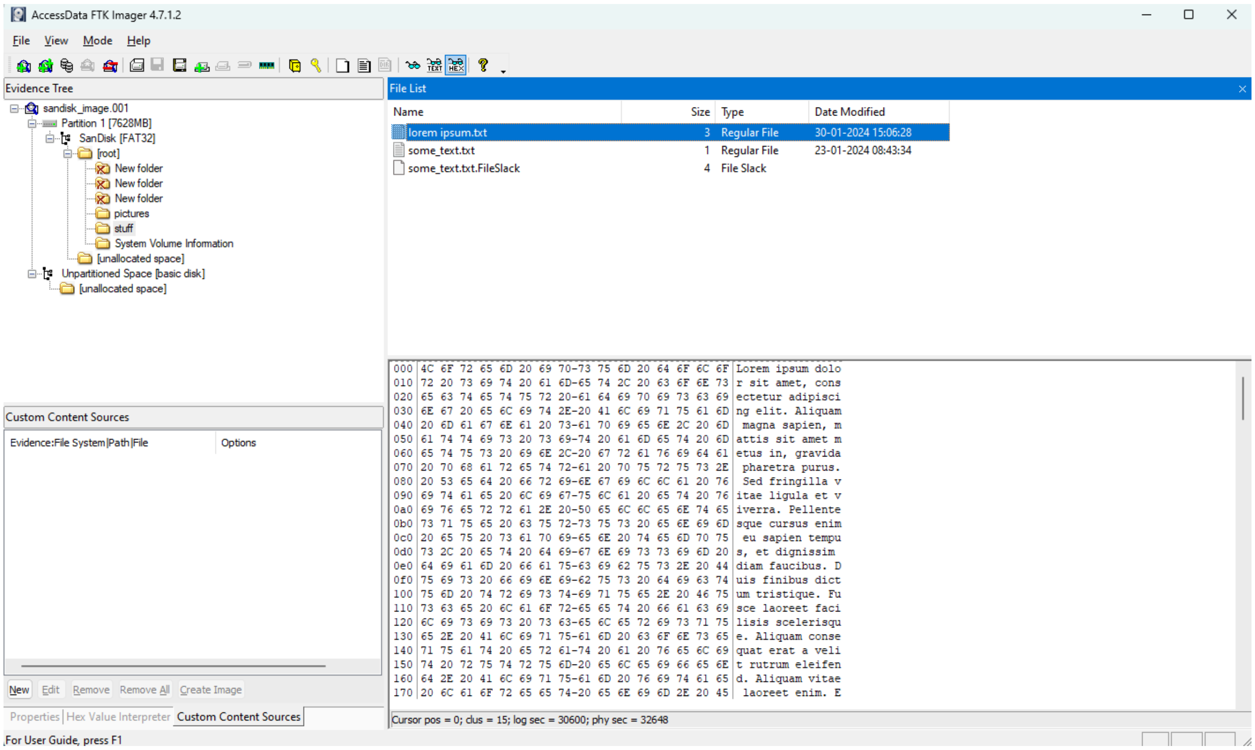


Name	Size	Type	Date Modified
lorem ipsu		Regular File	30-01-2024 15:06:28
some_text		Regular File	23-01-2024 08:43:34
some_text		File Slack	

```
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam magna sapien, mattis sit amet metus in, gravid
Integer et commodo lorem. Cras fermentum dui vitae consequat pulvinar. Nulla facilisi. Proin sollicitudin odio
In id ultricies erat. Duis sagittis justo in elit pellentesque, id euismod mauris finibus. Vivamus eget nulla e
Nam venenatis nec lacus eu volutpat. Vestibulum interdum feugiat purus ut molestie. Vivamus venenatis eget veli
Aenean sit amet vestibulum odio. Aliquam ut condimentum est, et mattis dui. Ut eget diam ipsum. In scelerisque
```

Creates a hash report of the selected file(s) or folder

Hex format



AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
Custom Content Sources
New Edit Remove Remove All Create Image
Properties Hex Value Interpreter Custom Content Sources
For User Guide, press F1

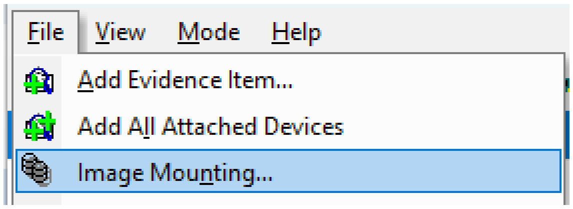
```
sandisk_image.001
  Partition 1 [7628MB]
    SanDisk [FAT32]
      [root]
        New folder
        New folder
        New folder
        pictures
        stuff
        System Volume Information
      [unallocated space]
  Unpartitioned Space [basic disk]
    [unallocated space]
```

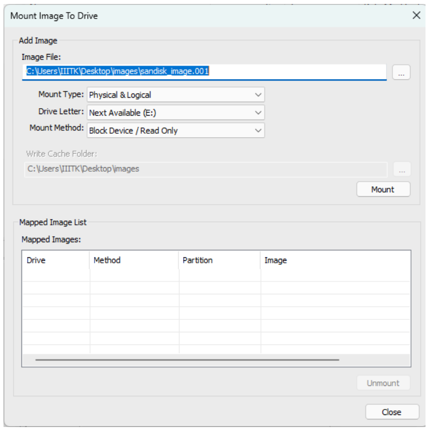
Name	Size	Type	Date Modified
lorem ipsum.txt	3	Regular File	30-01-2024 15:06:28
some_text.txt	1	Regular File	23-01-2024 08:43:34
some_text.txt.FileSlack	4	File Slack	

Evidence:File System|Path|File	Options

```
000 4C 6F 72 65 6D 20 69 70-73 75 6D 20 64 6F 6C 6F Lorem ipsum dolo
010 72 20 73 69 74 20 61 6D-65 74 2C 20 63 6F 6E 73 r sit amet, cons
020 65 63 74 65 74 75 72 20-61 64 69 70 69 73 63 69 ectetur adipisci
030 6E 67 20 65 6C 69 74 2E-20 41 6C 69 71 75 61 6D ng elit. Aliquam
040 20 6D 61 67 6E 61 20 73-61 70 69 65 6E 2C 20 6D  magna sapien, m
050 61 74 74 69 73 20 73 69-74 20 61 6D 65 74 20 6D attis sit amet m
060 65 74 75 73 20 69 6E 2C-20 67 72 61 76 69 64 61 etus in, gravida
070 20 70 68 61 72 65 74 72-61 20 70 75 72 75 73 2E  pharetra purus.
080 20 53 65 64 20 66 72 69-6E 67 69 6C 6C 61 20 76  Sed fringilla v
090 69 74 61 65 20 6C 69 67-75 6C 61 20 65 74 20 76 itae ligula et v
0a0 69 76 65 72 72 61 2E 20-50 65 6C 6C 65 6E 74 65 iverra. Pellente
0b0 73 71 75 65 20 63 75 72-73 75 73 20 65 6E 69 6D sque cursus enim
0c0 20 65 75 20 73 61 70 69-65 6E 20 74 65 6D 70 75  eu sapien tempu
0d0 73 2C 20 65 74 20 64 69-67 6E 69 73 73 69 6D 20 s, et dignissim
0e0 64 69 61 6D 20 66 61 75-63 69 62 75 73 2E 20 44 diam faucibus. D
0f0 75 69 73 20 66 69 6E 69-62 75 73 20 64 69 63 74 uis finibus dict
100 75 6D 20 74 72 69 73 74-69 71 75 65 2E 20 46 75 um tristique. Fu
110 73 63 65 20 6C 61 6F 72-65 65 74 20 66 61 63 69 sce laoreet faci
120 6C 69 73 69 73 20 73 63-65 6C 65 72 69 73 71 75 lisis scelerisqu
130 65 2E 20 41 6C 69 71 75-61 6D 20 63 6F 6E 73 65 e. Aliquam conse
140 71 75 61 74 20 65 72 61-74 20 61 20 76 65 6C 69 quat erat a veli
150 74 20 72 75 74 72 75 6D-20 65 6C 65 69 66 65 6E t rutrum eleifen
160 64 2E 20 41 6C 69 71 75-61 6D 20 76 69 74 61 65 d. Aliquam vitae
170 20 6C 61 6F 72 65 65 74-20 65 6E 69 6D 2E 20 45  laoreet enim. E
```

Cursor pos = 0; clus = 15; log sec = 30600; phy sec = 32648





Mount Image To Drive

Add Image

Image File: C:\Users\IIITK\Desktop\images\sandisk_image.001

Mount Type: Physical & Logical

Drive Letter: Next Available (E:)

Mount Method: Block Device / Read Only

Write Cache Folder: C:\Users\IIITK\Desktop\images

Mapped Image List

Mapped Images:

Drive	Method	Partition	Image