

Investigating NTFS Drive Using DiskExplorer For NTFS

Generating image file

```
theertha@CYS24020-Theertha:~$ lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
fd0          2:0    1    4K  0 disk
loop0        7:0    0   63.4M 1 loop /snap/core20/1974
loop1        7:1    0    4K  1 loop /snap/bare/5
loop2        7:2    0   63.7M 1 loop /snap/core20/2434
loop3        7:3    0   73.9M 1 loop /snap/core22/1722
loop4        7:4    0   73.9M 1 loop /snap/core22/858
loop5        7:5    0  237.2M 1 loop /snap/firefox/2987
loop6        7:6    0  273.7M 1 loop /snap/firefox/5437
loop7        7:7    0  349.7M 1 loop /snap/gnome-3-38-2004/143
loop8        7:8    0   91.7M 1 loop /snap/gtk-common-themes/1535
loop9        7:9    0   12.2M 1 loop /snap/snap-store/1216
loop10       7:10    0  485.5M 1 loop /snap/gnome-42-2204/120
loop11       7:11    0   12.3M 1 loop /snap/snap-store/959
loop12       7:12    0  505.1M 1 loop /snap/gnome-42-2204/176
loop13       7:13    0   53.3M 1 loop /snap/snapd/19457
loop14       7:14    0   44.3M 1 loop /snap/snapd/23258
loop15       7:15    0   568K 1 loop /snap/snapd-desktop-integration/253
loop16       7:16    0   452K 1 loop /snap/snapd-desktop-integration/83
sda          8:0    0   20G  0 disk
├─sda1       8:1    0    1M  0 part
├─sda2       8:2    0   513M  0 part /boot/efi
└─sda3       8:3    0  19.5G  0 part /var/snap/firefox/common/host-hunspell
                                     /
sr0         11:0    1  155.3M  0 rom  /media/theertha/CDROM
sr1         11:1    1  1024M  0 rom
```

```
theertha@CYS24020-Theertha:~$ sudo dd if=/dev/sda1 of=/home/theertha/Downloads/sda1img.dd bs=4M status=progress
[sudo] password for theertha:
0+1 records in
0+1 records out
1048576 bytes (1.0 MB, 1.0 MiB) copied, 0.115619 s, 9.1 MB/s
theertha@CYS24020-Theertha:~$ cd /home/theertha/Downloads
bash: cd /home/theertha/Downloads: No such file or directory
theertha@CYS24020-Theertha:~$ cd /home/theertha/Downloads
theertha@CYS24020-Theertha:~/Downloads$ ls
'archive(1)'      'archive(2).zip'  input_image.png  Untitled.ipynb
'archive(1).zip'  archive.zip        sda1img.dd        Untitled.tex
'archive(2)'      eventlog.csv       splunkforwarder-9.3.2-d8bb32809498-linux-2.6-amd64.deb
theertha@CYS24020-Theertha:~/Downloads$ ls -lh sda1.image.dd
ls: cannot access 'sda1.image.dd': No such file or directory
theertha@CYS24020-Theertha:~/Downloads$ ls -lh sda1img.dd
-rw-r--r-- 1 root root 1.0M Jan  4 22:39 sda1img.dd
theertha@CYS24020-Theertha:~/Downloads$
```

Here,

dd: disk image

if: input device/file

of:output device/file

bs: block size

Runtime's DiskExplorer for NTFS											
File Goto Link Edit View Tools Help											
Sector	Partition table										
x00000000	Valid Partition Table										
0	Entry			Starting			Ending			Relative	Total
	No	System	Boot	Cylinder	Head	Sector	Cylinder	Head	Sector	Start Sector	Sectors
	1	GUID Partition Table	No	x000	x00	x02	x300	xFE	x3F	x00000001	FFFFFFFF
				0	0	2	768	254	63	1	4294967295
	2	Free	No	x000	x00	x00	x000	x00	x00	x00000000	x00000000
x00000001	Invalid Partition Table										
	Entry			Starting			Ending			Relative	Total
	No	System	Boot	Cylinder	Head	Sector	Cylinder	Head	Sector	Start Sector	Sectors
	1	Free	No	x000	x00	x00	x000	x00	x00	x00000000	x00000000
				0	0	0	0	0	0	0	0
x00000002	Invalid Partition Table										
	Entry			Starting			Ending			Relative	Total
	No	System	Boot	Cylinder	Head	Sector	Cylinder	Head	Sector	Start Sector	Sectors
	1	Unknown	???	x100	x00	x23	x100	x00	x24	x00740061	x00200061
				206	0	35	256	0	36	7602273	2097249
2	Invalid Partition Table										
	Entry			Starting			Ending			Relative	Total
	No	System	Boot	Cylinder	Head	Sector	Cylinder	Head	Sector	Start Sector	Sectors
	2	Unknown	???	x100	x00	x21	x100	x00	x34	x00740069	x006F0069
				206	0	33	256	0	52	7602281	7274601
	Invalid Partition Table										
	Entry			Starting			Ending			Relative	Total
	No	System	Boot	Cylinder	Head	Sector	Cylinder	Head	Sector	Start Sector	Sectors
	3	Free	???	x000	x00	x00	x000	x00	x00	x00000000	x00000000
				0	0	0	0	0	0	0	0
	Invalid Partition Table										
	Entry			Starting			Ending			Relative	Total
	No	System	Boot	Cylinder	Head	Sector	Cylinder	Head	Sector	Start Sector	Sectors
	4	Free	No	x000	x00	x00	x000	x00	x00	x00000000	x00000000
				0	0	0	0	0	0	0	0

Goto sector...

Jump to a new position on D:\sda1image.dd:

Sector:	Sector	Offset	OR	Byte:	Offset
	hex 00000002	000			hex 0000000400
	dec 2	0			dec 1024

Valid values are:

Sector: x00000000 - x000007FF (0 - 2,047)


Byte: x000000000 - x00000FFFF (0 - 1,048,575)

OK Cancel Help

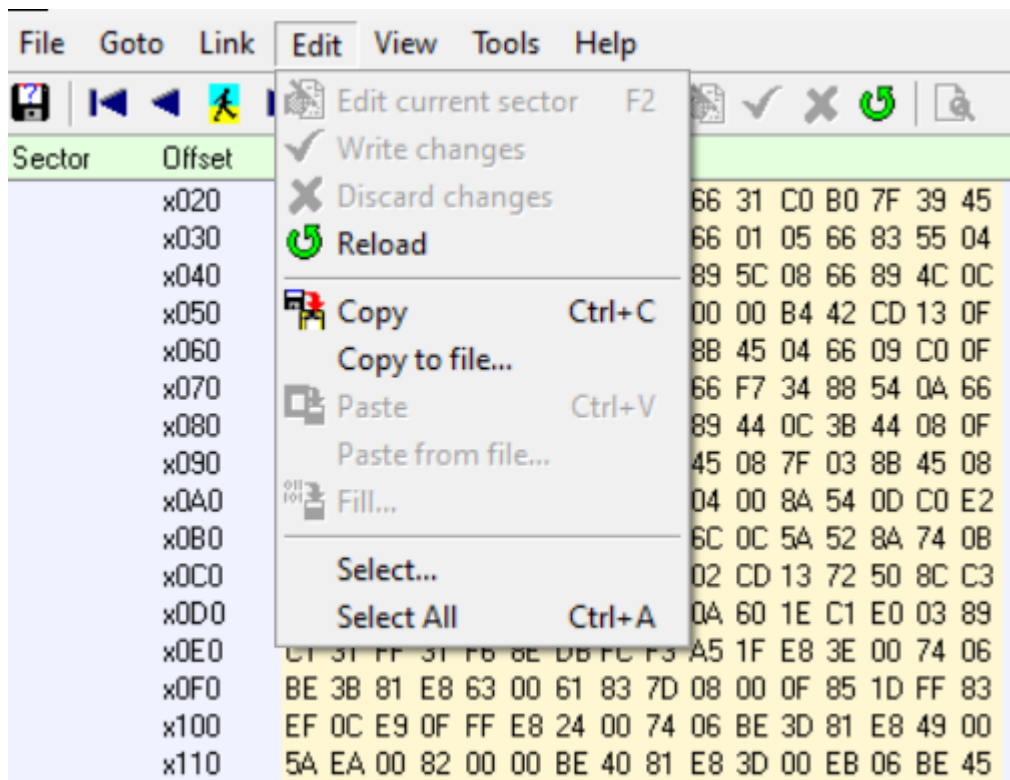
Sector	Offset	Hex values	Ascii values
	x020	74 46 66 88 1D 66 8B 4D 04 66 31 C0 B0 7F 39 45	t F . . . f i M . f 1 Å * i 9 E
	x030	08 7F 03 88 45 08 29 45 08 66 01 05 66 83 55 04
	x040	00 C7 04 10 00 89 44 02 66 89 5C 08 66 89 4C 0C
	x050	C7 44 06 00 70 50 C7 44 04 00 00 B4 42 CD 13 0F
	x060	82 BB 00 BB 00 70 EB 68 66 88 45 04 66 09 C0 0F
	x070	85 A3 00 66 88 05 66 31 D2 66 F7 34 88 54 0A 66
	x080	31 D2 66 F7 74 04 88 54 08 89 44 0C 3B 44 08 0F
	x090	8D 83 00 88 04 2A 44 0A 39 45 08 7F 03 88 45 08
	x0A0	29 45 08 66 01 05 66 83 55 04 00 8A 54 0D C0 E2
	x0B0	06 8A 4C 0A FE C1 08 D1 8A 6C 0C 5A 52 8A 74 08
	x0C0	50 BB 00 70 8E C3 31 DB B4 02 CD 13 72 50 8C C3
	x0D0	8E 45 0A 58 C1 E0 05 01 45 0A 60 1E C1 E0 03 89
	x0E0	C1 31 FF 31 F6 8E DB FC F3 A5 1F E8 3E 00 74 06
	x0F0	BE 3B 81 E8 63 00 61 83 7D 08 00 0F 85 1D FF 83
	x100	EF 0C E9 0F FF E8 24 00 74 06 BE 3D 81 E8 49 00
	x110	5A EA 00 82 00 00 BE 40 81 E8 3D 00 EB 06 BE 45
	x120	81 E8 35 00 BE 4A 81 E8 2F 00 EB FE BB 17 04 F6
	x130	07 03 C3 6C 6F 61 64 69 6E 67 00 2E 00 0D 0A 00
	x140	47 65 6F 6D 00 52 65 61 64 00 20 45 72 72 6F 72
	x150	00 BB 01 00 B4 0E CD 10 46 8A 04 3C 00 75 F2 C3
	x160	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	x170	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	x180	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	x190	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	x1A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	x1B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	x1C0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	x1D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	x1E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	x1F0	00 00 00 00 01 08 00 00 00 00 00 00 6D 00 20 08
x00000001	x000	EA 1C 82 00 00 00 00 00 57 60 00 00 20 BC 00 00
1	x010	99 6E 00 00 58 07 00 00 FF FF FF 00 FA 31 C0 8E
	x020	D8 8E D0 8E C0 66 BD F0 1F 00 00 66 89 EC FB 88
	x030	16 1B 82 CD 13 66 E8 97 00 00 00 FC E8 62 06 00
	x040	00 8B 15 08 82 00 00 81 C2 B8 03 00 00 8B 0D 10
	x050	82 00 00 8D 05 58 89 00 00 FC E8 34 03 00 00 E9
	x060	4E 07 00 00 F0 FF 07 00 90 2E 8D B4 26 00 00 00
	x070	00 2E 8D B4 26 00 00 00 8D B4 26 00 00 00 00 00
	x080	00 00 00 00 00 00 00 00 FF FF 00 00 9A CF 00
	x090	FF FF 00 00 92 CF 00 FF FF 00 00 9E 00 00

(Sector:Offset)=x00000000:x021 (0:33)

Drive: D:\sda1image.dd: (Image file), 2,048 (x00000800) sectors

Path: 

Volume: No volume mounted

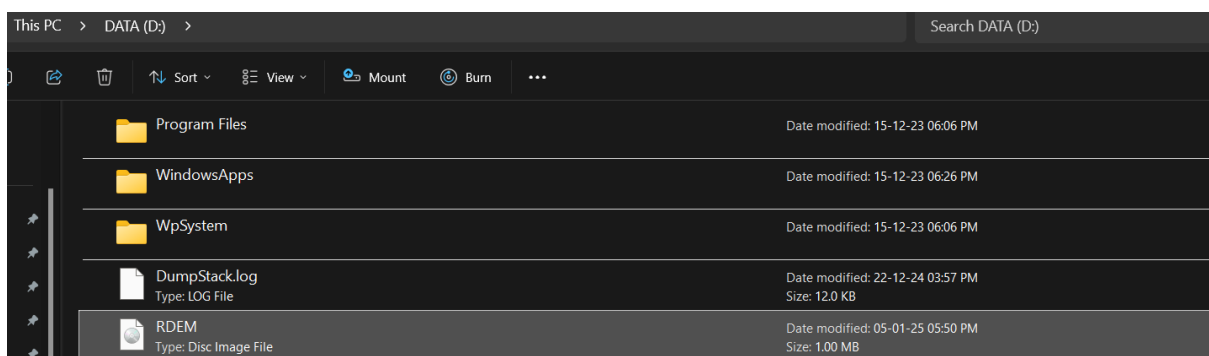
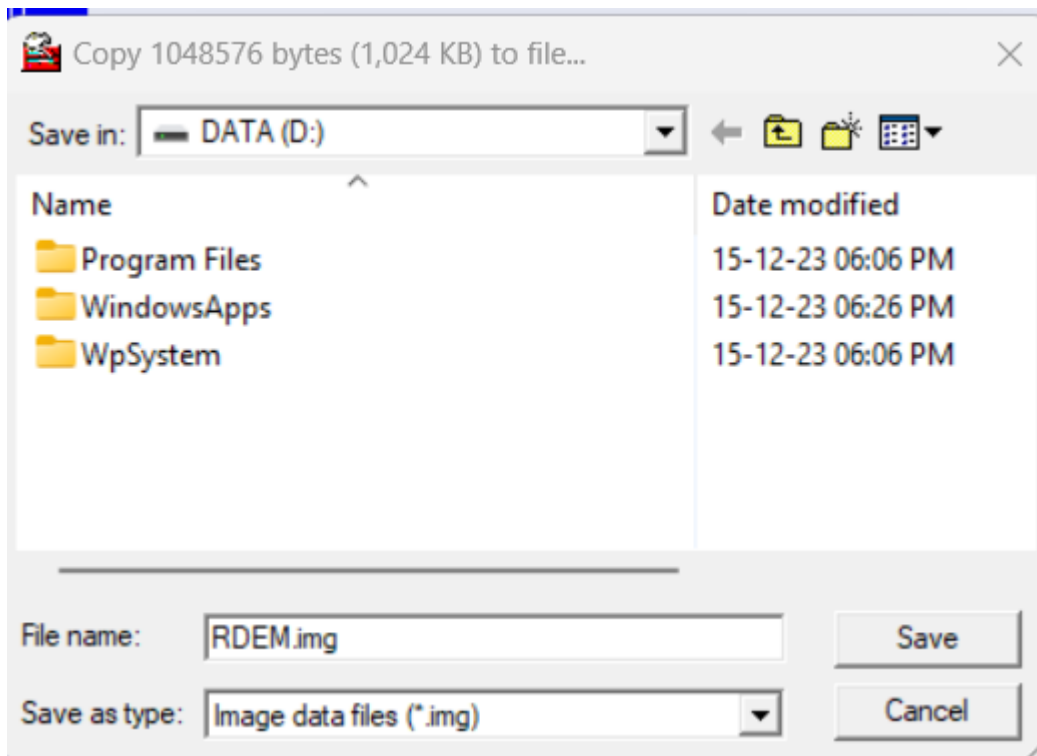
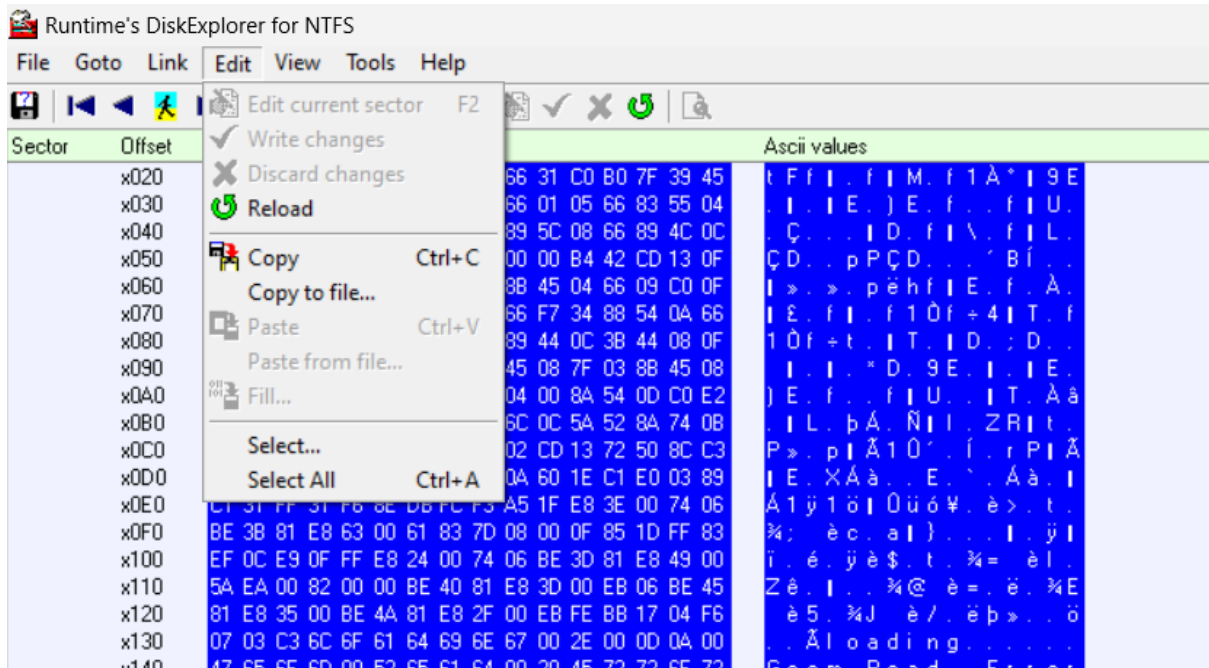


Sector	Offset	Hex values	Ascii values
x020	74 46 66 88 1D 66 88 4D 04 66 31 C0 80 7F 39 45	66 31 C0 80 7F 39 45	66 01 05 66 83 55 04
x030	08 7F 03 88 45 08 29 45 08 66 01 05 66 83 55 04	89 5C 08 66 89 4C 0C	00 00 B4 42 CD 13 0F
x040	00 C7 04 10 00 89 44 02 66 89 5C 08 66 89 4C 0C	88 45 04 66 09 C0 0F	66 F7 34 88 54 0A 66
x050	00 C7 04 06 00 70 50 C7 44 04 00 00 B4 42 CD 13 0F	89 44 0C 3B 44 08 0F	45 08 7F 03 88 45 08
x060	82 B8 00 B8 00 70 EB 68 66 88 45 04 66 09 C0 0F	04 00 8A 54 0D C0 E2	6C 0C 5A 52 8A 74 0B
x070	85 A3 00 66 88 05 66 31 D2 66 F7 34 88 54 0A 66	02 CD 13 72 50 8C C3	0A 60 1E C1 E0 03 89
x080	31 D2 66 F7 74 04 88 54 08 89 44 0C 3B 44 08 0F	01 31 FF 31 F6 8E DB FC F3 A5 1F E8 3E 00 74 06	BE 3B 81 E8 63 00 61 83 7D 08 00 0F 85 1D FF 83
x090	8D 83 00 88 04 2A 44 0A 39 45 08 7F 03 88 45 08	EF 0C E9 0F FF E8 24 00 74 06 BE 3D 81 E8 49 00	5A EA 00 82 00 00 BE 40 81 E8 3D 00 EB 06 BE 45
x0A0	29 45 08 66 01 05 66 83 55 04 00 8A 54 0D C0 E2		
x0B0	06 8A 4C 0A FE C1 08 D1 8A 6C 0C 5A 52 8A 74 0B		
x0C0	50 B8 00 70 8E C3 31 D8 B4 02 CD 13 72 50 8C C3		
x0D0	8E 45 0A 58 C1 E0 05 01 45 0A 60 1E C1 E0 03 89		
x0E0	C1 31 FF 31 F6 8E DB FC F3 A5 1F E8 3E 00 74 06		
x0F0	BE 3B 81 E8 63 00 61 83 7D 08 00 0F 85 1D FF 83		
x100	EF 0C E9 0F FF E8 24 00 74 06 BE 3D 81 E8 49 00		
x110	5A EA 00 82 00 00 BE 40 81 E8 3D 00 EB 06 BE 45		
x120	81 E8 35 00 BE 4A 81 E8 2F 00 EB FE B8 17 04 F6		
x130	07 03 C3 6C 6F 61 64 69 6E 67 00 2E 00 00 0A 00		
x140	47 65 6F 6D 00 62 65 61 64 00 20 45 72 72 6F 72		
x150	00 B8 01 00 B4 0E CD 10 46 8A 04 3C 00 75 F2 C3		
x160	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
x170	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
x180	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
x190	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
x1A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
x1B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
x1C0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
x1D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
x1E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
x1F0	00 00 00 00 01 08 00 00 00 00 00 00 6D 00 20 08		
x00000001	EA 1C 82 00 00 00 00 00 57 60 00 00 20 8C 00 00		
1	x010	99 6E 00 00 58 07 00 00 FF FF FF 00 FA 31 C0 8E	
	x020	D8 8E D0 8E C0 66 8D F0 1F 00 00 66 89 EC FB 88	
	x030	16 1B 82 CD 13 66 E8 97 00 00 00 FC E8 62 06 00	
	x040	00 8B 15 08 82 00 00 81 C2 B8 03 00 00 88 0D 10	
	x050	82 00 00 8D 05 58 89 00 00 FC E8 34 03 00 00 E9	
	x060	4E 07 00 00 F0 FF 07 00 90 2E 8D B4 26 00 00 00	
	x070	00 2E 8D B4 26 00 00 00 8D B4 26 00 00 00 00 00	
	x080	00 00 00 00 00 00 00 FF FF 00 00 9A CF 00	
	x090	FF FF 00 00 92 CF 00 FF FF 00 00 9E 00 00	

(Sector:Offset)=x00000000:x021 (0:33)

Drive: D:\sda1image.dd: (Image file), 2,048 (x00000800) sectors

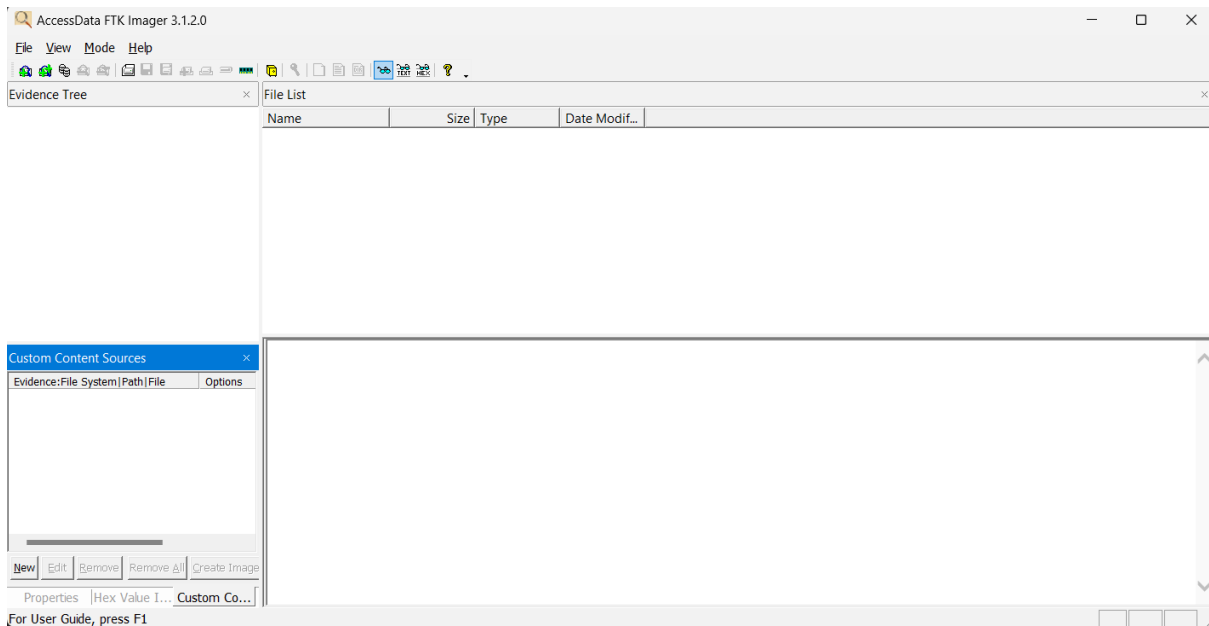
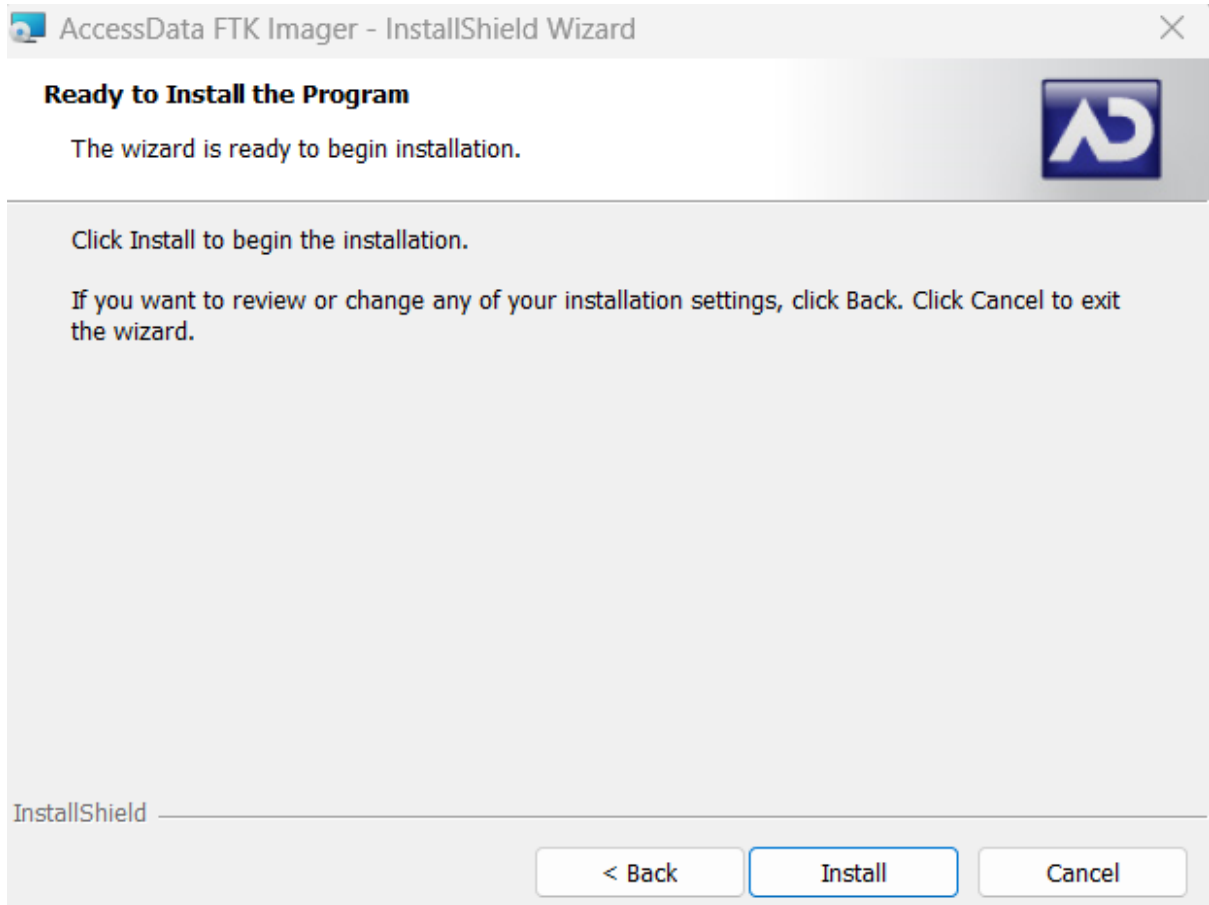
Path:

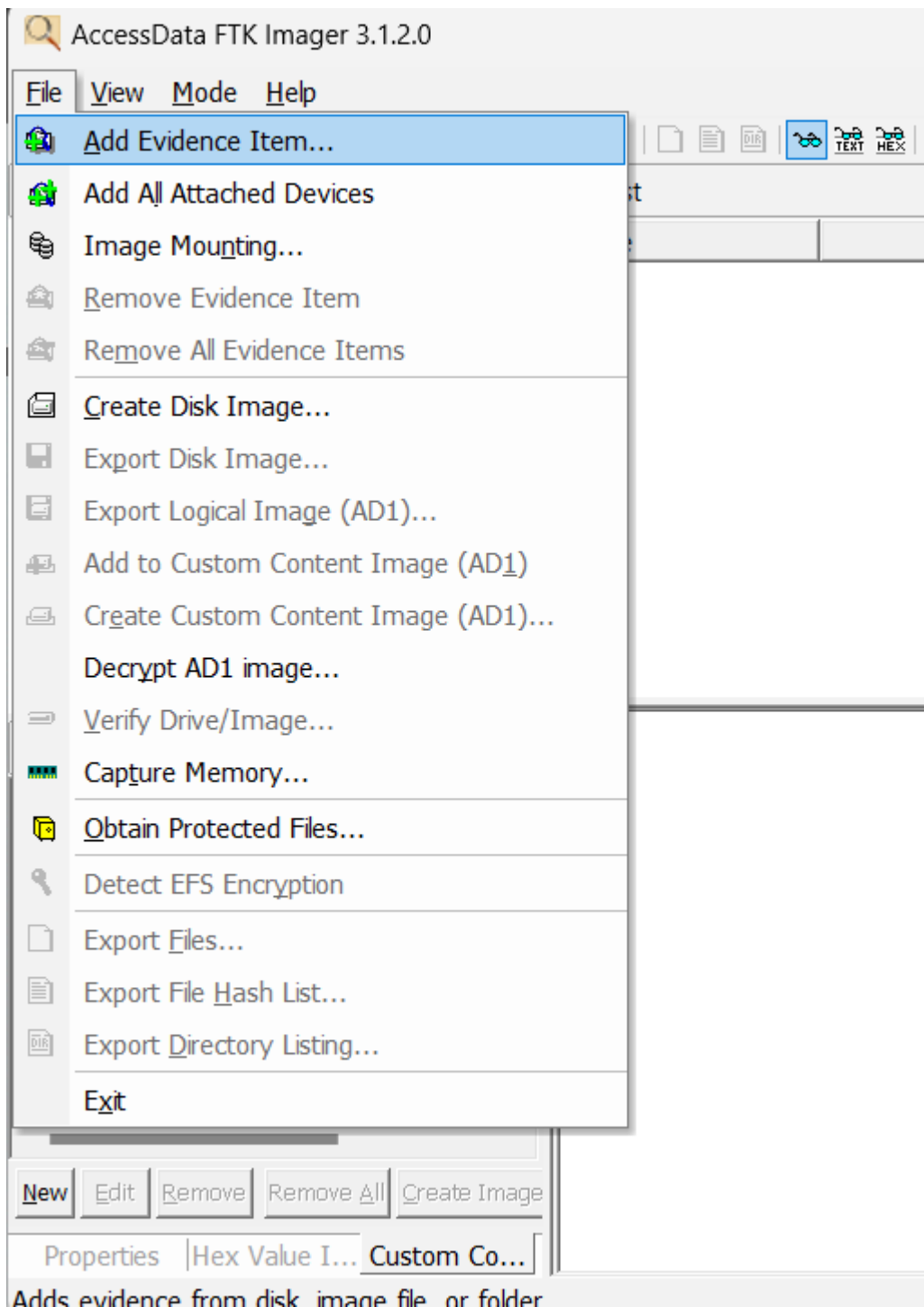


Viewing content of Forensic Image Using Access Data FTK imager Tool

FTK Imager is a powerful tool for forensic analysis, allowing to view, analyze, and recover data from forensic images while maintaining data integrity and ensuring chain-of-custody compliance.







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.)

< Back Next > Cancel Help

Select File

Evidence Source Selection

Please enter the source path:

C:\Users\DELL\Downloads\sda1img.dd

Browse...

< Back Finish Cancel Help

AccessData FTK Imager 3.1.2.0

File View Mode Help

Evidence Tree

- ntfs-img-kw-1.dd
 - KW-SRCH-1 [NTFS]

File List

Name	Size	Type	Date Modif...
------	------	------	---------------

Custom Content Sources

Evidence:File System|Path|File Options

New Edit Remove Remove All Create Image

Properties Hex Value I... Custom Co...

Cursor pos = 0; log sec = 0

```
000000 EB 52 90 4E 54 46 53 20-20 20 20 00 02 01 00 00 ER-NTFS .....
000010 00 00 00 00 00 F8 00 00-3F 00 20 00 3F 00 00 00 .....e-?-?...
000020 00 00 00 00 80 00 00 00-C0 3E 00 00 00 00 00 00 .....>.....
000030 EB 14 00 00 00 00 00 00-60 1F 00 00 00 00 00 00 .....e.....
000040 02 00 00 00 08 00 00 00-23 56 ED 50 92 ED 50 BA .....#VIP-IP*
000050 00 00 00 00 FA 33 C0 8E-D0 BC 00 7C FB B8 C0 07 ....d3A-B4-jd,A
000060 8E D8 E8 16 00 B8 00 0D-8E C0 33 DB C6 06 0E 00 ..e-...-A30E...
000070 10 E8 53 00 68 00 0D 68-6A 02 CB 8A 16 24 00 B4 ..eS-h-hj-E-g-
000080 08 CD 13 73 05 B9 FF FF-8A F1 66 0F B6 C6 40 66 ..I-s-yy-ff-SEff
000090 0F B6 D1 80 E2 3F F7 E2-86 CD C0 ED 06 41 66 0F ..qN-a?-a-IAi-Af
0000a0 B7 C9 66 F7 E1 66 A3 20-00 C3 B4 41 BB AA 55 8A ..Ef+afe-AAw*U
0000b0 16 24 00 CD 13 72 0F 81-FB 55 AA 75 09 F6 C1 01 ..g-I-r-GU+u-aA
0000c0 74 04 FE 06 14 00 C3 66-60 1E 06 66 A1 10 00 66 ..t-b-..Af-..fj-f
0000d0 03 06 1C 00 66 3B 06 20-00 0F 82 3A 00 1E 66 6A .....f;.....fj
0000e0 00 66 50 06 53 66 68 10-00 01 00 80 3E 14 00 00 ..fP-Sfh.....>...
0000f0 0F 85 0C 00 E8 B3 FF 80-3E 14 00 00 0F 84 61 00 .....e'y->.....a
000100 B4 42 8A 16 24 00 16 1F-8B F4 CD 13 66 58 5B 07 ..B-g-...di-fX[
000110 66 58 66 58 1F EB 2D 66-33 D2 66 0F B7 0E 18 00 ..fXfX-e-f30f.....
000120 66 F7 F1 FE C2 8A CA 66-8B D0 66 C1 EA 10 F7 36 ..f-npA-Ef-DrAe-+6
```

AccessData FTK Imager 3.1.2.0

File View Mode Help

Evidence Tree

- ntfs-img-kw-1.dd
 - KW-SRCH-1 [NTFS]

File List

Name	Size	Type	Date Modif...
[orphan]	0	Folder (Plac...	
[root]	1	Directory	24-10-03 0...
[unallocated spac...	0	Unallocate...	

Custom Content Sources

Evidence:File System|Path|File Options

New Edit Remove Remove All Create Image

Properties Hex Value I... Custom Co...

Cursor pos = 0; clus = 0; log sec = 0

```
000000 EB 52 90 4E 54 46 53 20-20 20 20 00 02 01 00 00 ER-NTFS .....
000010 00 00 00 00 00 F8 00 00-3F 00 20 00 3F 00 00 00 .....e-?-?...
000020 00 00 00 00 80 00 00 00-C0 3E 00 00 00 00 00 00 .....>.....
000030 EB 14 00 00 00 00 00 00-60 1F 00 00 00 00 00 00 .....e.....
000040 02 00 00 00 08 00 00 00-23 56 ED 50 92 ED 50 BA .....#VIP-IP*
000050 00 00 00 00 FA 33 C0 8E-D0 BC 00 7C FB B8 C0 07 ....d3A-B4-jd,A
000060 8E D8 E8 16 00 B8 00 0D-8E C0 33 DB C6 06 0E 00 ..e-...-A30E...
000070 10 E8 53 00 68 00 0D 68-6A 02 CB 8A 16 24 00 B4 ..eS-h-hj-E-g-
000080 08 CD 13 73 05 B9 FF FF-8A F1 66 0F B6 C6 40 66 ..I-s-yy-ff-SEff
000090 0F B6 D1 80 E2 3F F7 E2-86 CD C0 ED 06 41 66 0F ..qN-a?-a-IAi-Af
0000a0 B7 C9 66 F7 E1 66 A3 20-00 C3 B4 41 BB AA 55 8A ..Ef+afe-AAw*U
0000b0 16 24 00 CD 13 72 0F 81-FB 55 AA 75 09 F6 C1 01 ..g-I-r-GU+u-aA
0000c0 74 04 FE 06 14 00 C3 66-60 1E 06 66 A1 10 00 66 ..t-b-..Af-..fj-f
0000d0 03 06 1C 00 66 3B 06 20-00 0F 82 3A 00 1E 66 6A .....f;.....fj
0000e0 00 66 50 06 53 66 68 10-00 01 00 80 3E 14 00 00 ..fP-Sfh.....>...
0000f0 0F 85 0C 00 E8 B3 FF 80-3E 14 00 00 0F 84 61 00 .....e'y->.....a
000100 B4 42 8A 16 24 00 16 1F-8B F4 CD 13 66 58 5B 07 ..B-g-...di-fX[
000110 66 58 66 58 1F EB 2D 66-33 D2 66 0F B7 0E 18 00 ..fXfX-e-f30f.....
000120 66 F7 F1 FE C2 8A CA 66-8B D0 66 C1 EA 10 F7 36 ..f-npA-Ef-DrAe-+6
```

File List				
Name	Size	Type	Date Modif...	
[orphan]	0	Folder (Plac...		
[root]	1	Directory	24-10-03 0...	
[unallocated spac...	0	Unallocate...		

00	30 00 00 00 01 00 00 00-00	10 00 00 08 00 00 00	0
10	10 00 00 00 28 00 00 00-28	00 00 00 01 00 00 00 (... (.....
20	00 00 00 00 00 00 00 00-18	00 00 00 03 00 00 00
30	00 00 00 00 00 00 00 00-	

Evidence Tree		File List			
<div> <div>ntfs-img-kw-1.dd</div> <div> <div>KW-SRCH-1 [NTFS]</div> <div> <div>[root]</div> <div>[unallocated space]</div> <div>[orphan]</div> </div> </div> </div>		Name	Size	Type	Date Modif...
		\$Secure	1	Regular File	23-10-03 0...
		\$UpCase	128	Regular File	23-10-03 0...
		\$Volume	0	Regular File	23-10-03 0...
		file-n-1.dat	2	Regular File	23-10-03 0...
		file-n-3.dat	3	Regular File	23-10-03 0...
		file-n-4.dat	2	Regular File	23-10-03 0...
		file-n-4.dat.FileSl...	1	File Slack	
		file-n-5.dat	2	Regular File	23-10-03 0...
		file-r-1.dat	1	Regular File	23-10-03 0...
		file-r-2.dat	1	Regular File	23-10-03 0...
		file-r-3.dat	1	Regular File	23-10-03 0...

Properties	
Create Folders	False
Delete Subfolders and Files	False
Delete	False
Read Permissions	False
Change Permissions	False
Take Ownership	False
NTFS Access Control Entry	
ACE Type	Allow Access

00	30 00 00 00 01 00 00 00-00	10 00 00 08 00 00 00	0
10	10 00 00 00 28 00 00 00-28	00 00 00 01 00 00 00 (... (.....
20	00 00 00 00 00 00 00 00-18	00 00 00 03 00 00 00
30	00 00 00 00 00 00 00 00-	

