# Practical 7 Using FTK Imager to create the image and check the intregrity

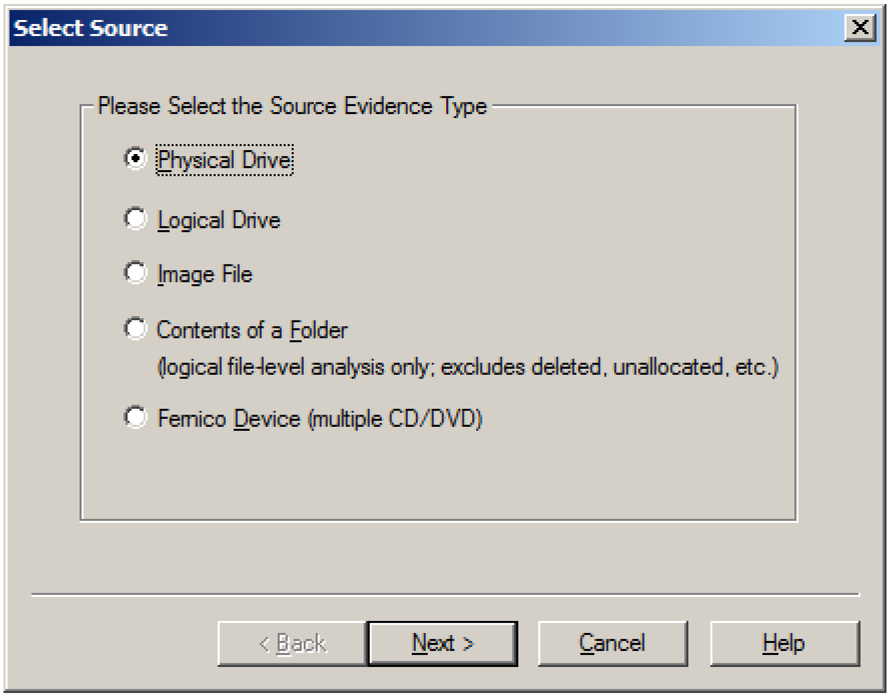
# Date :- 05.02.2025 Submission Date:- 12.02.2025

Write –up

- Cyber forensics vs other forensics
- Phases of Cyber /Digital /computer forensics

## Create an Image Using FTK Imager

**Source Evidence Type:** To image an entire device, select ***Physical Drive*** (a physical device can contain more than one ***Logical Drive***). You can also create an image of an ***Image File***, which seems silly, but it could be desirable if, say, you want to create a more compressed version of the image. You can also image the specific **Contents of a Folder** or of a **Femico Device** (which is ideal for creating images of multiple CDs or DVDs with the same parameters). In this example, we'll select ***Physical Drive*** to create an image of the flash drive.



Select Source

Please Select the Source Evidence Type

● Physical Drive

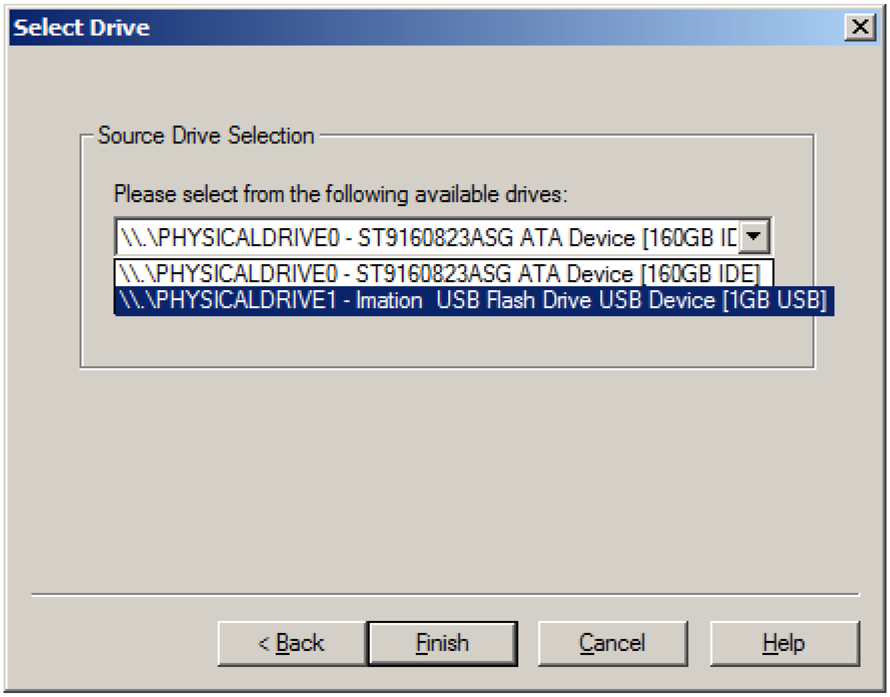
○ Logical Drive

○ Image File

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

○ Femico Device (multiple CD/DVD)

**Source Drive Selection:** Based on our selection of physical drive, we then have a choice of the current physical drives we can see, so we select the drive corresponding to the flash drive.



Select Drive

Source Drive Selection

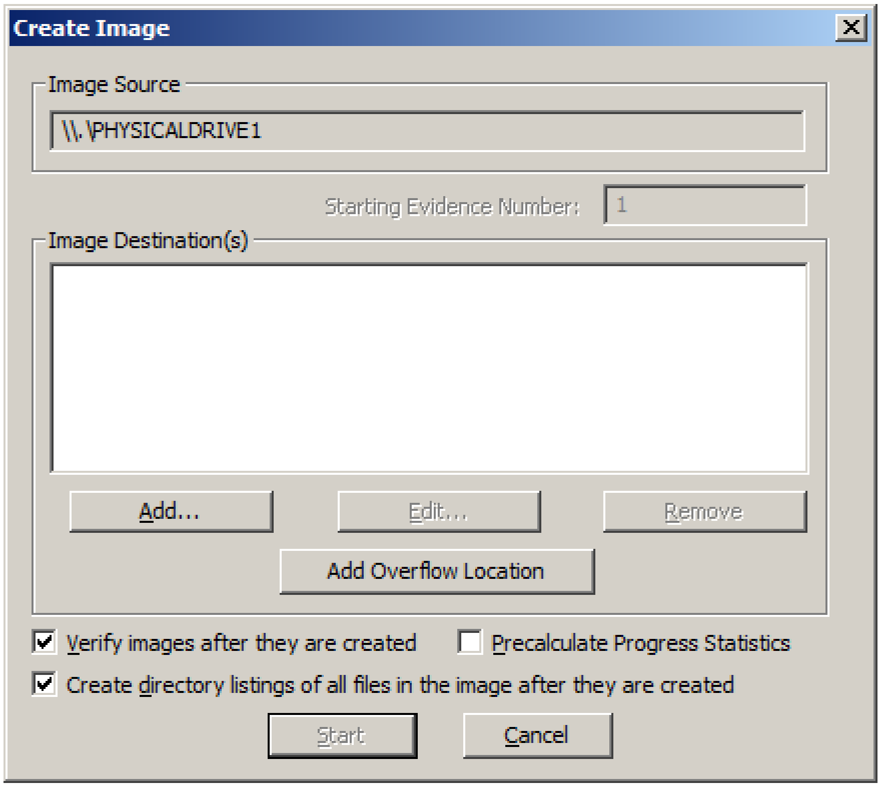
Please select from the following available drives:

\\.\PHYSICALDRIVE0 - ST9160823ASG ATA Device [160GB IDE]

\\.\PHYSICALDRIVE0 - ST9160823ASG ATA Device [160GB IDE]

\\.\PHYSICALDRIVE1 - Imation  USB Flash Drive USB Device [1GB USB]

**Create Image:** Here is where you can specify where the image will be created. We also always choose ***Verify images after they are created*** as a way to run a hash value check on the image file. You can also ***Create directory listings of all files in the image*** after they are created, but be prepared that this will be a huge listing for a typical hard drive with hundreds of thousands of entries.



Create Image

Image Source: \\.\PHYSICALDRIVE1

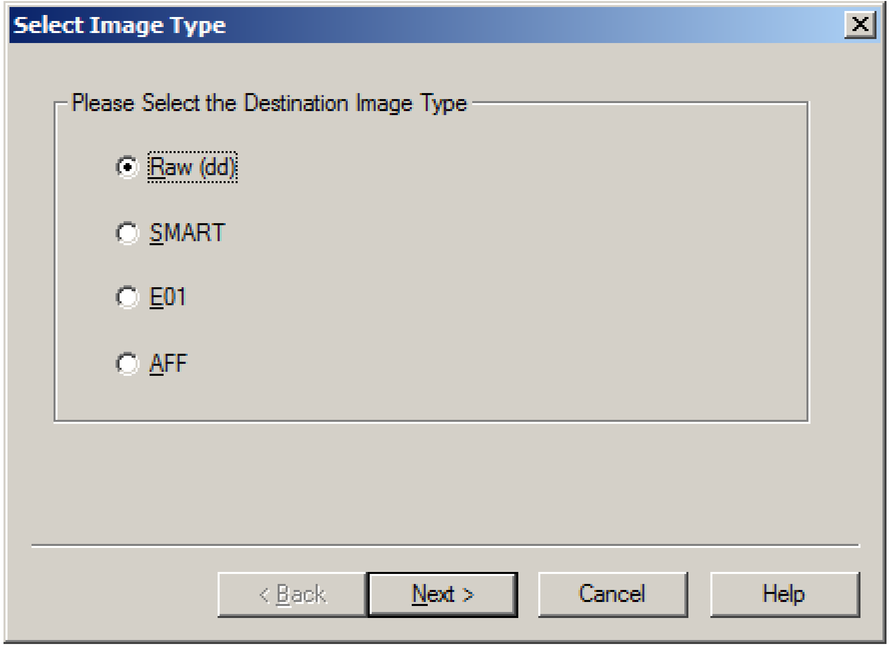
Starting Evidence Number: 1

Image Destination(s)

☑ Verify images after they are created  □ Precalculate Progress Statistics

☑ Create directory listings of all files in the image after they are created

**Select Image Type:** This indicates the type of image file that will be created – Raw is a bit-by-bit uncompressed copy of the original, while the other three alternatives are designed for use with a specific forensics program.  We typically use Raw or E01, which is an EnCase forensic image file format.  In this example, we're using Raw.



Select Image Type

Please Select the Destination Image Type

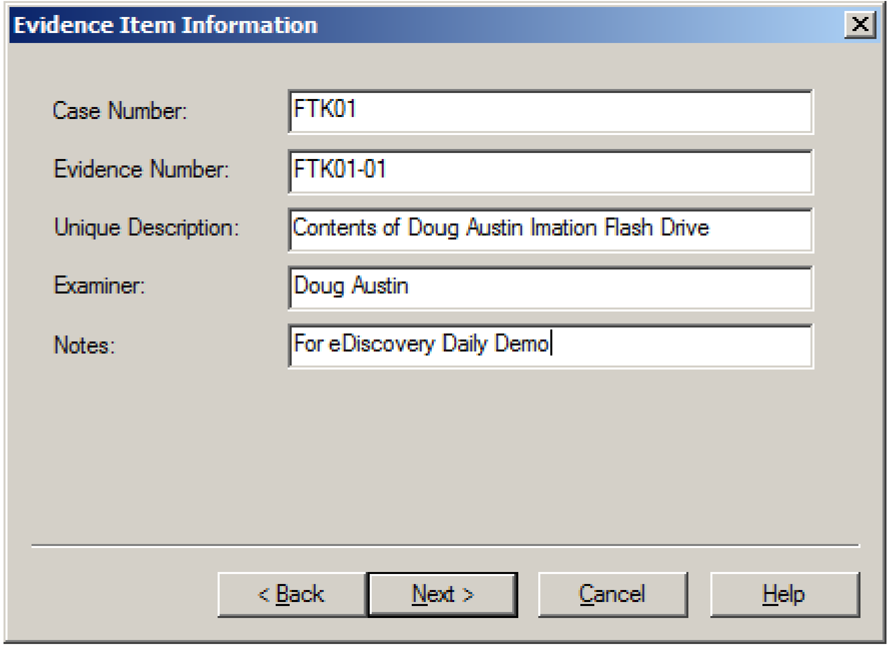
● Raw (dd)

○ SMART

○ E01

○ AFF

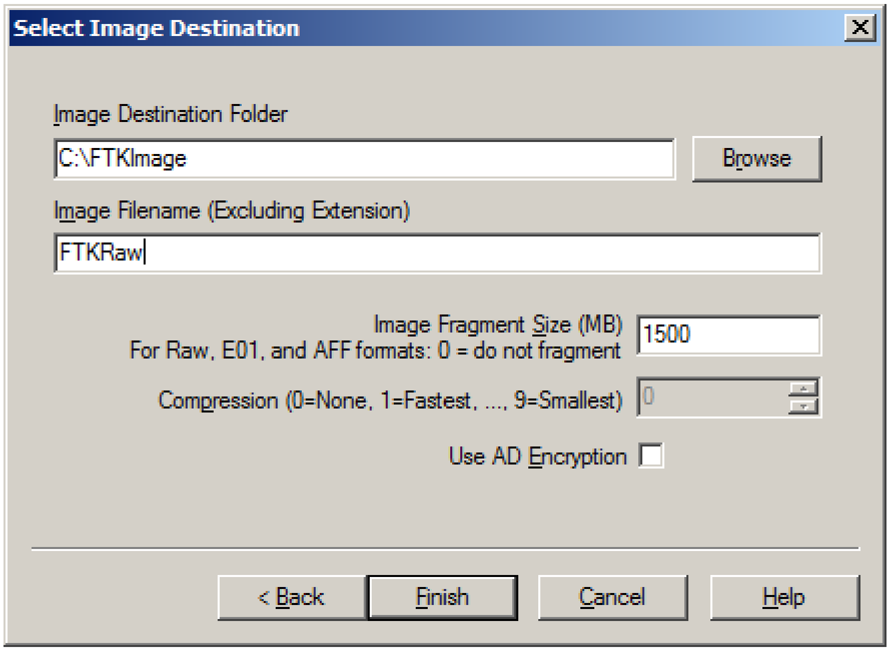
**Evidence Item Information:** This is where you can enter key information about the evidence item you are about to create to aid in documenting the item.  This information will be saved as part of the image summary information once the image is complete.



Evidence Item Information

| | |
|---|---|
| Case Number: | FTK01 |
| Evidence Number: | FTK01-01 |
| Unique Description: | Contents of Doug Austin Imation Flash Drive |
| Examiner: | Doug Austin |
| Notes: | For eDiscovery Daily Demo |

**Select Image Destination:** We'll browse to a folder that I've created called ***"FTKImage"*** on the C: drive and give the image a file name.  Image Fragment Size indicates the size of each fragment when you want to break a larger image file into multiple parts. Compression indicates the level of compression of the image file, from 0 (no compression) to 9 (maximum compression – and a slower image creation process). For Raw uncompressed images, compression is always 0. Use AD Encryption indicates whether to encrypt the image – we don't typically select that, instead choosing to put an image on an encrypted drive (when encryption is desired). Click ***Finish*** to begin the image process and a dialog will be displayed throughout the image creation process. Because it is a bit-by-bit image of the device, it will take the same amount of time regardless of how many files are currently stored on the device.



Select Image Destination

Image Destination Folder

C:\FTKImage

Image Filename (Excluding Extension)

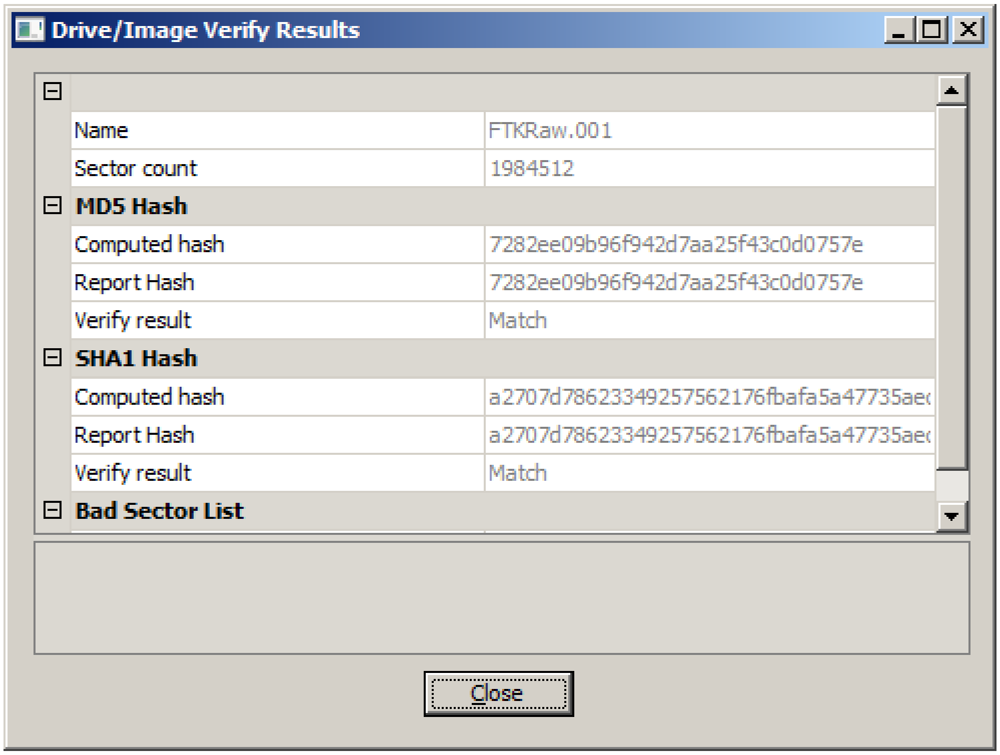
FTKRaw

Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment: 1500

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

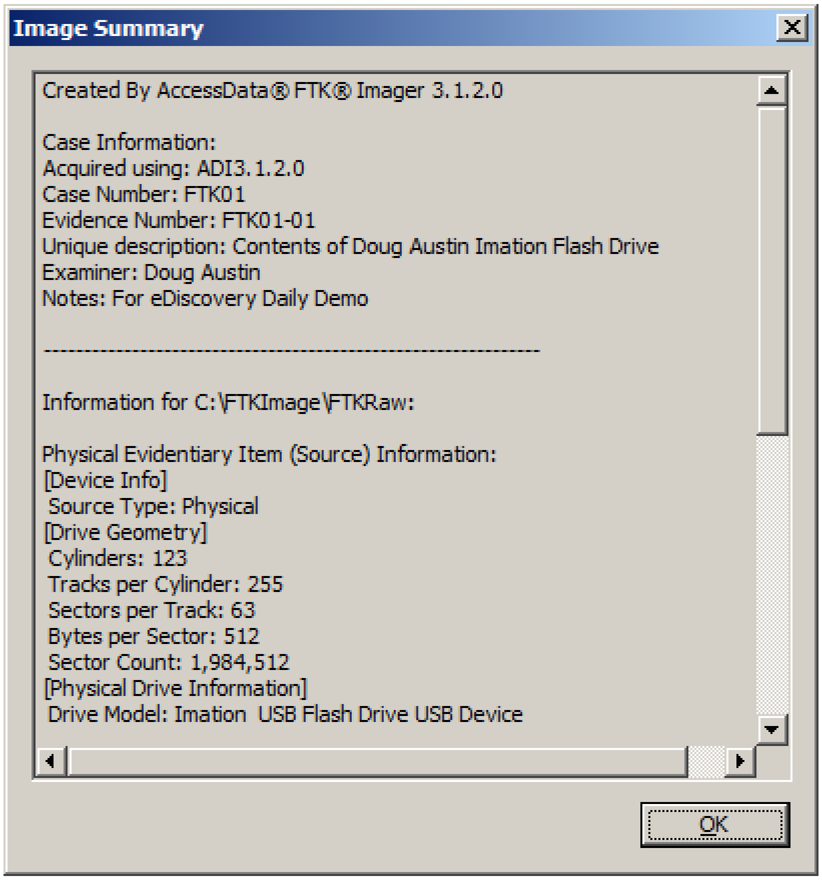
Use AD Encryption □

**Drive/Image Verify Results:** When the image is complete, this popup window will appear to show the name of the image file, the sector count, computed (before image creation) and reported (after image creation) MD5 and SHA1 hash values with a confirmation that they match and a list of bad sectors (if any). The hash verification is a key check to ensure a valid image and the hash values should be the same regardless which image type you create.



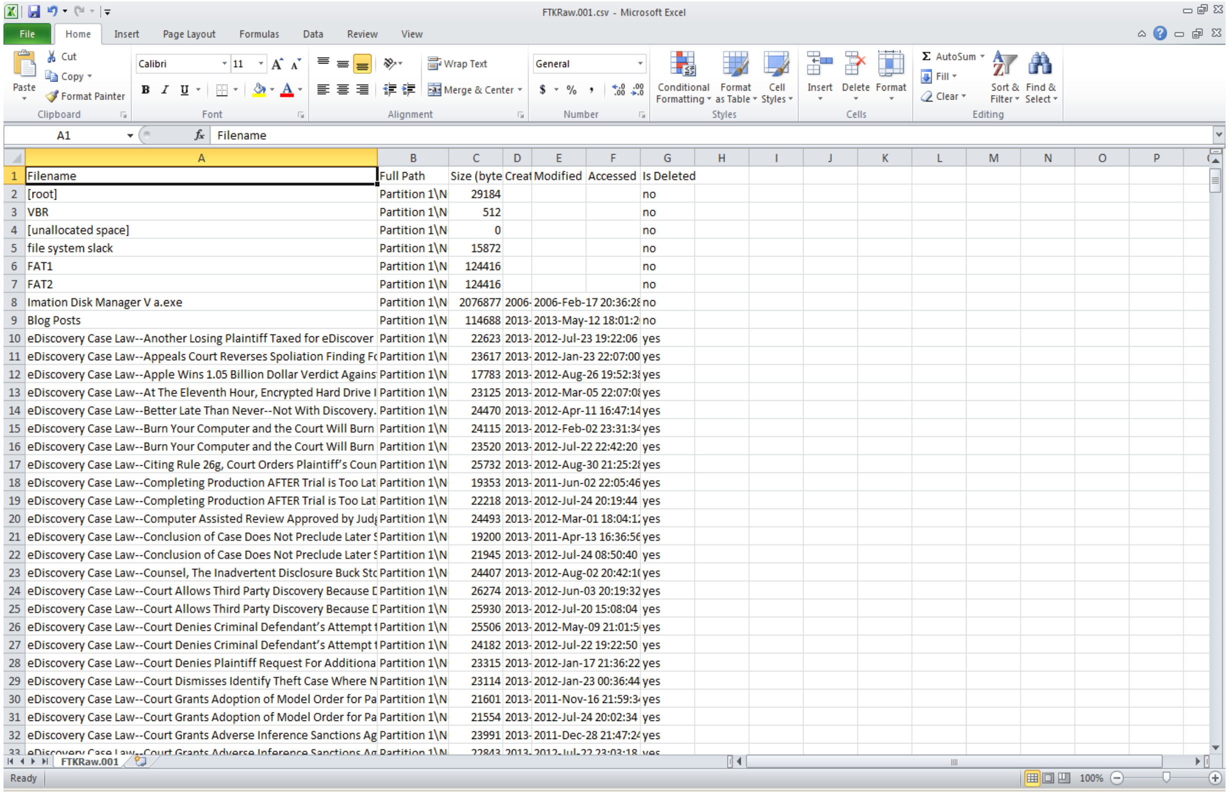
| | |
|---|---|
| Name | FTKRaw.001 |
| Sector count | 1984512 |
| **MD5 Hash** | |
| Computed hash | 7282ee09b96f942d7aa25f43c0d0757e |
| Report Hash | 7282ee09b96f942d7aa25f43c0d0757e |
| Verify result | Match |
| **SHA1 Hash** | |
| Computed hash | a2707d78623349257562176fbafa5a47735ae |
| Report Hash | a2707d78623349257562176fbafa5a47735ae |
| Verify result | Match |
| **Bad Sector List** | |

**Image Summary:** When the image is complete, click the ***Image Summary*** button to see the view a summary of the image that is created, including the evidence item information you entered, drive information, hash verification information, etc.  This information is also saved as a text file.



```
Created By AccessData® FTK® Imager 3.1.2.0

Case Information:
Acquired using: ADI3.1.2.0
Case Number: FTK01
Evidence Number: FTK01-01
Unique description: Contents of Doug Austin Imation Flash Drive
Examiner: Doug Austin
Notes: For eDiscovery Daily Demo

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

Information for C:\FTKImage\FTKRaw:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 123
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 1,984,512
[Physical Drive Information]
 Drive Model: Imation  USB Flash Drive USB Device
```

**Directory Listing:** If you selected ***Create directory listings of all files in the image***, the results will be stored in a CSV file, which can be opened with Excel.



| | A | B | C | D | E | F | G |
|---|---|---|---|---|---|---|---|
| 1 | Filename | Full Path | Size (byte | Creat | Modified | Accessed | Is Deleted |
| 2 | [root] | Partition 1\N | 29184 | | | | no |
| 3 | VBR | Partition 1\N | 512 | | | | no |
| 4 | [unallocated space] | Partition 1\N | 0 | | | | no |
| 5 | file system slack | Partition 1\N | 15872 | | | | no |
| 6 | FAT1 | Partition 1\N | 124416 | | | | no |
| 7 | FAT2 | Partition 1\N | 124416 | | | | no |
| 8 | Imation Disk Manager V a.exe | Partition 1\N | 2076877 | 2006- | 2006-Feb-17 20:36:2 | | no |
| 9 | Blog Posts | Partition 1\N | 114688 | 2013- | 2013-May-12 18:01:2 | | no |
| 10 | eDiscovery Case Law--Another Losing Plaintiff Taxed for eDiscover | Partition 1\N | 22623 | 2013- | 2012-Jul-23 19:22:06 | | yes |
| 11 | eDiscovery Case Law--Appeals Court Reverses Spoliation Finding Fo | Partition 1\N | 23617 | 2013- | 2012-Jan-23 22:07:00 | | yes |
| 12 | eDiscovery Case Law--Apple Wins 1.05 Billion Dollar Verdict Agains | Partition 1\N | 17783 | 2013- | 2012-Aug-26 19:52:3 | | yes |
| 13 | eDiscovery Case Law--At The Eleventh Hour, Encrypted Hard Drive I | Partition 1\N | 23125 | 2013- | 2012-Mar-05 22:07:0 | | yes |
| 14 | eDiscovery Case Law--Better Late Than Never--Not With Discovery. | Partition 1\N | 24470 | 2013- | 2012-Apr-11 16:47:14 | | yes |
| 15 | eDiscovery Case Law--Burn Your Computer and the Court Will Burn | Partition 1\N | 24115 | 2013- | 2012-Feb-02 23:31:3 | | yes |
| 16 | eDiscovery Case Law--Burn Your Computer and the Court Will Burn | Partition 1\N | 23520 | 2013- | 2012-Jul-22 22:42:20 | | yes |
| 17 | eDiscovery Case Law--Citing Rule 26g, Court Orders Plaintiff’s Coun | Partition 1\N | 25732 | 2013- | 2012-Aug-30 21:25:2 | | yes |
| 18 | eDiscovery Case Law--Completing Production AFTER Trial is Too Lat | Partition 1\N | 19353 | 2013- | 2011-Jun-02 22:05:46 | | yes |
| 19 | eDiscovery Case Law--Completing Production AFTER Trial is Too Lat | Partition 1\N | 22218 | 2013- | 2012-Jul-24 20:19:44 | | yes |
| 20 | eDiscovery Case Law--Computer Assisted Review Approved by Judg | Partition 1\N | 24493 | 2013- | 2012-Mar-01 18:04:1 | | yes |
| 21 | eDiscovery Case Law--Conclusion of Case Does Not Preclude Later S | Partition 1\N | 19200 | 2013- | 2011-Apr-13 16:36:5 | | yes |
| 22 | eDiscovery Case Law--Conclusion of Case Does Not Preclude Later S | Partition 1\N | 21945 | 2013- | 2012-Jul-24 08:50:40 | | yes |
| 23 | eDiscovery Case Law--Counsel, The Inadvertent Disclosure Buck Sto | Partition 1\N | 24407 | 2013- | 2012-Aug-02 20:42:1 | | yes |
| 24 | eDiscovery Case Law--Court Allows Third Party Discovery Because D | Partition 1\N | 26274 | 2013- | 2012-Jun-03 20:19:32 | | yes |
| 25 | eDiscovery Case Law--Court Allows Third Party Discovery Because D | Partition 1\N | 25930 | 2013- | 2012-Jul-20 15:08:04 | | yes |
| 26 | eDiscovery Case Law--Court Denies Criminal Defendant’s Attempt t | Partition 1\N | 25506 | 2013- | 2012-May-09 21:01:5 | | yes |
| 27 | eDiscovery Case Law--Court Denies Criminal Defendant’s Attempt t | Partition 1\N | 24182 | 2013- | 2012-Jul-22 19:22:50 | | yes |
| 28 | eDiscovery Case Law--Court Denies Plaintiff Request For Additiona | Partition 1\N | 23315 | 2013- | 2012-Jan-17 21:36:22 | | yes |
| 29 | eDiscovery Case Law--Court Dismisses Identify Theft Case Where N | Partition 1\N | 23114 | 2013- | 2012-Jan-23 00:36:44 | | yes |
| 30 | eDiscovery Case Law--Court Grants Adoption of Model Order for Pa | Partition 1\N | 21601 | 2013- | 2011-Nov-16 21:59:3 | | yes |
| 31 | eDiscovery Case Law--Court Grants Adoption of Model Order for Pa | Partition 1\N | 21554 | 2013- | 2012-Jul-24 20:02:34 | | yes |
| 32 | eDiscovery Case Law--Court Grants Adverse Inference Sanctions Ag | Partition 1\N | 23991 | 2013- | 2011-Dec-28 21:47:2 | | yes |
| 33 | eDiscovery Case Law--Court Grants Adverse Inference Sanctions Ag | Partition 1\N | 22843 | 2013- | 2012-Jul-22 23:03:18 | | yes |

And, there you have it – a bit-by-bit image of the device!  You’ve just captured everything on the device, including deleted files and slack space data.  Next time, we’ll discuss ***Adding an Evidence Item*** to look at contents or drives or images (including the image we created here).