Forensics

Disdks

Thibault Debatty
cylab.be

Overview

Imaging and mounting

File recovery

Timeline creation

Overview

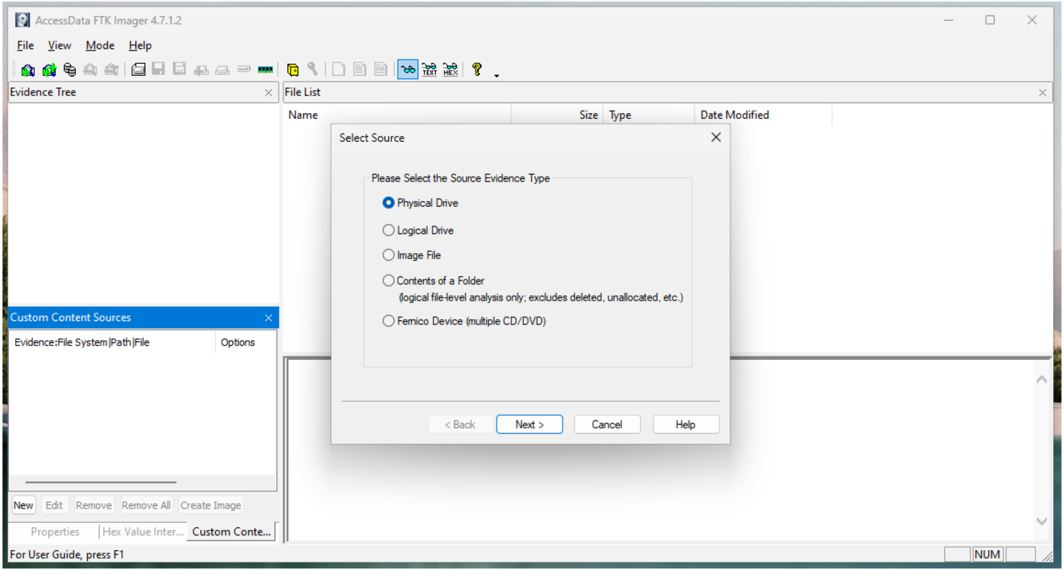
Overview

bit by bit copy if possible to have an exact copy

- We don't want to **alter the orginal disk** => we must create a copy (image)
- Disk is organized in partitions and filesysems FS is used to manage file and directory on a device
  - different imaging strategies
  - image may contain multiple partitions (and filesystems)
- FS don't wipe data => we can recover deleted files
- FS store timings (created, updated, accessed) => we can create timelines

Imaging and mounting

Imaging with FTK Imager



AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
For User Guide, press F1
NUM

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)

< Back | Next > | Cancel | Help

Imaging with FTK Imager

Exercise

1. Download FTK imager
2. Create the image of a USB key (E01 format)

E01 Format add some additional metadata

Mount a dd image in SIFT

dd image = bit to bit image

ro = read only

```
sudo mount -t <fs> -o loop,ro /path/to/image /path/to/mountpoint

sudo mount -t <fs> -o loop,ro,offset=<offset in bytes> /path/to/image /path
```

Mount a dd image in SIFT

Exercise

- Download the exercise file `usb-01.img.zip` from https://cylab.be/s/fFMqA
- This file is a dd image of a USB drive.
- What is the content of the file password.txt ?

Mount an E01 image in SIFT

1. use the ewfmount command to ‘expose’ the raw disk image inside the E01 container:

E01 is a forensic disk image which not only contains the data of the disk but also some other info like metadata, raw disk data (in bytes), the different partitions,...

```
sudo ewfmount /path/to/image.E01 /mnt/e01
```

2. use mount to mount the partition:

```
sudo mount -o ro,loop /mnt/e01/ewf1 /mnt/windows
```

Mount an E01 image in SIFT

umount path/to/mount -> to unmount an image

Exercise

- Download the exercise file `usb-02.E01` from https://cylab.be/s/5Lne8
- This file is an `E01` image of a USB drive.
- What is the content of the file `password.txt` ?

Partitions information

list the partitions contained in an image:

```
mmls <image>
```

display type and details about a file system:

```
fsstat -o <offset in sectors> <image>
```

Partitions information

Exercise

- Download and extract `usb-03.img.zip` from https://cylab.be/s/LOz9Z
- This image contains multiple partitions
- List the different partitions and filesystems

Mount with offset

If the image contains multiple partitions:

```
sudo mount -t <fs> -o loop,ro,offset=<offset> /path/to/image /path/to/moun
```

where `<offset>` must be specified **in Bytes**

Mount with offset

Exercise

Download the image `usb-06.E01` from https://cylab.be/s/Y1seb

This image contains multiple partitions.

- use `ewfmount` and `mmls` to **mount the ext4 partition**
- what is the content of the file `file.txt`?

Mount E01 split file

Exercise

- Download and extract `usb-05.zip` from https://cylab.be/s/iYJtY
- This is a split E01 image
- Mount the partition and extract the contained file

File recovery

File recovery

list deleted files:

```
fls -d <image>
```

-d to filter to only see the deleted files

shows, for each file, the corresponding inode number or FAT entry number (inum)

use icat to extract the content of a file:

```
icat -r <image> <inum>
```

File recovery

Exercise

In usb-01.img, what is the content of the deleted file `deleted.txt` ?

File recovery

Exercise

Download usb-04.E01 from https://cylab.be/s/kbcRa

The image contains 3 deleted files (PDF, DOCX, PNG). Recover the files. . .

Timeline creation

Timeline creation

Extract timings to *body file* format:

```
fls -m -r <image> > <bodyfile.txt>
```

Create report (in chronological order):

```
mactime -b <bodyfile.txt>
```

Timeline creation

File system	m (modified)	a (accessed)	c (changed)	b (birth)
Ext4	Modified	Accessed	Changed	Created
Ext2/3	Modified	Accessed	Changed	N/A
FAT	Written	Accessed	N/A	Created
NTFS	File Modified	Accessed	MFT Modified	Created
UFS	Modified	Accessed	Changed	N/A

Timeline creation

Exercise

Create a timeline from `usb-01.img`