# **Disk Images Exercise**

BitCuratorEdu Last Updated: January 18, 2022

### About This Exercise

#### Author

Cal Lee

### Description

This exercise is meant to introduce students to disk images give them hands-on experience viewing the contents of disk images. These slides are excerpted from Cal Lee's SAA "Advanced Digital Forensics" class. The sample data referenced in these slides is available here: <u>https://github.com/BitCurator/bcc-dfa-sample-data/</u>

### Learning object type

Lesson plan/materials

#### Learning objectives

This learning object might be used in a lesson to satisfy the following learning objectives:

• Practice using tools in the BitCurator Environment.

## Creating Exact Copies of Data from Media – Disk Images

- Getting an "image" of a storage medium involves working at a level below the file system
- Can get at file attributes and deleted files not visible through higher-level copy operations

### Creating a Disk Image in Guymager

Guymag	er	🔜 🖾 🛍 📬 2:12	PM & Bit	Curator 🔱
0	Computer	8 Acquire image of /dev/sdb	Documenta	
	× – □ GUYMA <u>D</u> evices <u>Misc H</u> e ] Rescan	File format         C Linux dd raw image (file extension .dd or .xxx)         Expert Witness Format, sub-format Guymager (file extension .Exx)         C Advanced forensic image (file extension .aff)             Split size 2047		
	Serial nr. VB45b1d326-9557	Case number     1       Evidence number     1       Examiner     BitCurator User       Description     A sample floppy disk image	Bad sectors	Progre
	1	Notes       Additional notes go here         Destination		
         	Size Sector size Image file Info file Current speed Started Hash calculation Source verificatio Image verification	Hash calculation / verification         Image: Calculate MD5       Image: Calculate SHA-1         Image: Re-read source after acquisition for verification (takes twice as long)         Image: Werify image after acquisition (takes twice as long)		
	Trash	Cancel Duplicate image Start		

## **Examples of Disk Image formats**

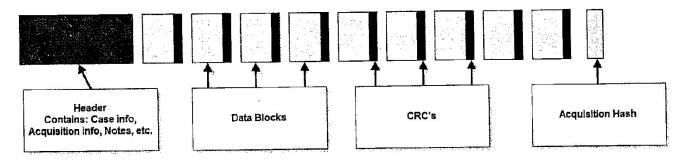
- RAW and Split RAW (RAW stored across multiple files)
- Advanced Forensics Format (AFF) [no longer recommended]
- EnCase Evidence File (.E01)
- ISO (for CD-ROM)
- IMG (floppy or sometimes CD-ROM)

## RAW (dd)

- Copies of the raw media data. Often split into smaller chunks to make them more manageable and so that the resulting images can fit onto limited filesystems and media such as FAT or DVD/CDROM.
- Advantages:
  - Very simple, use simple tools to manipulate the image.
  - Image can be easily split for storage and transport on removable media
  - Output can be piped to other applications for immediate processing
- Disadvantages:
  - Can be very large (no compression). Zipped raw images cannot be operated on directly with regular tools (efficiently perform arbitrary seeks).
  - Often too large to store on FAT formatted media
  - No metadata other than filenames, no hashes.
  - No checksumming on files not robust
    - Missing segments (for example from scratched CD/DVD can sometimes be overwritten with 0's).
    - Overwritten data (unrecoverable no checksums on small blocks in file).

## **Expert Witness Format (EnCase)**

- Evidence file consists (in order) of: Acquisition information, Data Block, CRC (cyclic redundancy check), acquisition hash (MD5)
- Can be split for storage, transport
- CRC computed for every 32K block; balance between integrity and speed, also makes it very difficult to tamper with the evidence file (1 in 4 billion chance of collision)
- Cannot be manipulated with simple (open source UNIX) tools; support reverse engineered in libewf
- Previously limited to 2GB size
- Largely proprietary
- Has been reverse engineered by Joachim Metz in libewf (used in open source tools that read EWF) - <u>http://sourceforge.net/projects/libewf/files/</u>



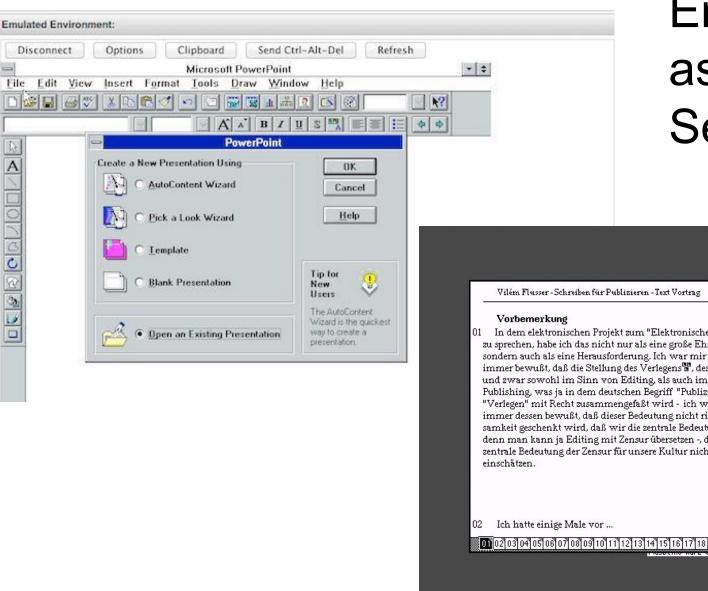
## ISO Images (.iso extension) for CD-ROM or DVD

Similar to raw, but can't contain

- multiple tracks
- audio or video tracks
- Don't contain control headers or error correction fields (raw can include these)
- Filesystem usually will be either ISO 9660 (CD-ROM) or UDF (DVDs)

## Accessing Data in Disk Images

- Virtualization and emulation
- Mounting the original filesystem
- Accessing (but not mounting) disk images using forensics software
- Two options discussed later for end user access:
  - Remote, dynamic access to disk image contents
  - Cross-drive analysis



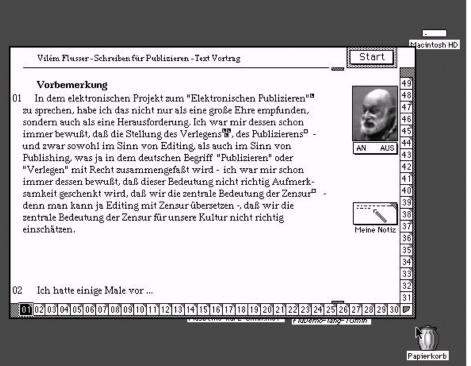
-

File

0033000

1

## Emulation as a Service



#### http://bw-fla.uni-freiburg.de/demos.html

# What's the difference between the two options in FTK Imager shown below?

Q	AccessData FTK Imager 3.1.3.2				Q	AccessData FTK Imager 3.1.3.2			- • • × •
E	e <u>V</u> iew <u>M</u> ode <u>H</u> elp					Tiew Worde Helb			
6	g <u>A</u> dd Evidence Item		) 🐱 🗟 😹 😵 🖕			Add Evidence Item		🗎 🐱 🐮 💡 🖕	
	Add All All of the state	File List		×			File List		×
	Image Mou <u>n</u> ting	Nos	Size Type	Date Modified		Image Mou <u>n</u> ting	Name	Size Type	Date Modified
	Demove Evidence Item				9	<u>Remove Evidence Item</u>			
6	Remove All Evidence Items					Remove All Evidence Items			
G	<u>C</u> reate Disk Image				G	Create Disk Image			
l lie	Export Disk Image					Export Disk Image			
E	Export Logical Image (AD1)				B	Export Logical Image (AD1)			
垂	Add to Custom Content Image (AD <u>1</u> )				40	Add to Custom Content Image (AD <u>1</u> )			
tini.	Create Custom Content Image (AD1)				œ	Cr <u>e</u> ate Custom Content Image (AD1)			
	Decrypt AD1 image					Decrypt AD1 image			
-	<u>V</u> erify Drive/Image				=	<u>V</u> erify Drive/Image			
	Capture Memory					Capture Memory			
	<u>O</u> btain Protected Files	•	III	•		Obtain Protected Files	<		۱.
9	Detect EFS Encryption				9	Detect EFS Encryption			
	Export <u>E</u> lles			_		Export <u>Files</u>			
E	Export File Hash List					Export File Hash List			
1016	Export Directory Listing				10	Export Directory Listing			
	Exit					Exit			

### Mounting a Disk Image to Browse the Contents

							 1, En 💌 4))	2:58 PM
home home Imaging Tools Forensics Tools Accession Tools Additional Tools Shared Folders ar Media Shared Folders ar	<ul> <li>⊘ Recent</li> <li>△ Home</li> <li>Desktop</li> <li>△ Documents</li> <li>◇ Downloads</li> <li>∂ Music</li> <li>△ Pictures</li> <li>✓ Videos</li> <li>☑ Trash</li> <li>sf_bc_share</li> <li>▲</li> <li>Q Network</li> </ul>	buf_exerciseplanning	winXP winxp_reports	WinX	Open         Open With Other Application         Scripts         Cut         Copy         Move To         Copy To         Make Link         Rename         Move to Trash         Email         Compress         Properties	<ul> <li>Disk Image Info</li> <li>File Analysis</li> <li>File Info</li> <li>Find Files</li> <li>Mount Disk Image</li> <li>Open Browser as Root</li> <li>Safe Mount</li> <li>Unmount Disk Image</li> <li>Open Scripts Folder</li> </ul>		2:58 PM
Trash								

### Mounting a Disk Image to Browse the Contents

							🔔 📬 🖪 💌 🕪 3:02 I
	× = □ winXP						
home	C	buf exerciseplanning winXP			Q == ==		
Imaging Tools	⊘ Recent		1 To 10				
	🟠 Home	winxp_beout winxp_re	ports WinXP.E	01			
	Desktop						
Forensics Tools	Documents						
	Downloads						
	dd Music						
Accession Tools		😸 🕘 🔍 WinXP_vol02			-		
	Videos	< > =1.6 GB Volu	ne			Q := :::	
Additional Tools	Trash	⊘ Recent					
	<pre>sf_bc_share</pre>	Home					
		Desktop	Config.Msi	Documents and	\$Extend	Program Files	
Shared Folders ar Media		Desktop		Settings			
Meetid	Computer	↓ Downloads				1 10 101 1010	
	👤 Connect to Server	Husic	RECYCLER	System Volume	WINDOWS	\$AttrDef	
sf_bc_share		Pictures		Information			
		Videos			1 10 101 1010		
		Trash	AUTOEXEC.BAT	\$BadClus	\$Bitmap	boot.ini	
		sf_bc_share	1 10 101 1010			1 10 101 1010	
9		 ☑ Network					
		💶 1.6 GB Volume 🔺	\$Boot	CONFIG.SYS	IO.SYS	\$LogFile	
		Computer	7 10 101 1010		10 101 1010	1 10 101 1010	
		Connect to Server	\$MFTMirr	MSDOS.SYS	NTDETECT.COM	pagefile.sys	
1 6 CB Volume		÷ connece co server					
Hotorewording				China Cases	C) (aluma		
			\$Secure	\$UpCase	\$Volume		

🗕 💿 🖶 🌽 🚍 🖳 🔛 🔟 🚫 🚱 Right Ctrl

### Exporting Selected Files from a Disk Image

Open disk image Close disk image Select All	JeSelect All Export selections Cancel export
File System: Entries in bold are directories Entries in red are unallocated/deleted files	Image Info 4442dcc6-a2a6-8a42-9137-fbe3be4ae9a2
<ul> <li>_urlspersona.txt</li> <li>urlspatents.txt</li> <li>_urlspatents.txt</li> <li>urlscryptography.txt</li> <li>_urlscryptography.txt</li> <li>urlscopyright.txt</li> <li>_urlscopyright.txt</li> <li>_urlscopyright.txt</li> <li>patentauto.py</li> <li>_patentterms.txt</li> </ul>	Media information Media type: fixed disk Is physical: yes Bytes per sector: 512 Number of sectors: 4096000 Media size: 1.9 GiB (2097152000 bytes) Digest hash information MD5: e07f26954b23db1a44dfd28ecd717da9
<ul> <li>patentterms.txt</li> <li>54402.EXE</li> </ul>	Messages
<pre></pre>	/home/bcadmin/Desktop/disk-images/terry-work- usb-2009-12-11.E01 >> Generating DFXML file /home/bcadmin/.bcfa/terry-work- usb-2009-12-11.E01_dfxml.xml
189812_ □ xpadvancedkeylogger.exe ▶ Log □ vnc-4_1_3-x86_win32.exe	>> Success!!! Fiwalk created DFXML file
<ul> <li>Vnc-4_1_3-x86_win32.exe</li> <li>\$MBR</li> <li>\$FAT1</li> </ul>	>> Generating directory tree

## Exercise: Multiple Views into Disk Image Files

- Resources we'll be using:
  - ISO file -<u>https://github.com/BitCurator/bcc-dfa-sample-data/blob/main/25.i</u> <u>so</u> (or from flash drive)
  - 2. IMG file https://github.com/BitCurator/bcc-dfa-sample-data/blob/main/so mething.img (or from flash drive)
  - 3. OSFMount (Windows only)
  - 4. FTK Imager (Windows only)
  - 5. BitCurator Environment

## Exercise: Multiple Views into Disk Image Files

- Step 1 Mount the ISO and IMG files using OSFMount
- Step 2 Find the drives using Windows Explorer and investigate their contents
- Step 3 Open FTK Imager and add both images as evidence items, and explore what we see in the drives
- Step 4 Use the BitCurator environment to mount the disk images [Right click on image file, then select: Scripts > Mount Disk Image]
- Step 5 Use the BitCurator environment to select files within the images to export [Use Forensics Tools > BitCurator Disk Image Access]



## BitCuratorEdu

Advancing the adoption of digital forensics tools and methods in libraries and archives through professional education efforts



This resource was released by the BitCuratorEdu project and is licensed under a <u>Creative Commons</u> <u>Attribution 4.0 International License</u>.

Most resources from the BitCuratorEdu project are intentionally left with basic formatting and without project branding. We encourage educators, practitioners, and students to adapt these materials as much as needed and share them widely.

The <u>BitCuratorEdu project</u> is a three-year effort funded by the <u>Institute of Museum and Library</u> <u>Services (IMLS)</u> to study and advance the adoption of digital forensics tools and methods in libraries and archives through professional education efforts. This project is a partnership between <u>Educopia Institute</u> and the <u>School of Information and Library Science at</u> <u>the University of North Carolina at Chapel Hill</u>, along with the <u>Council of State Archivists (CoSA)</u> and several Masters-level programs in library and information science.