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: https://github.com/BitCurator/bcc-dfa-sample-data/

Learning object type
Lesson plan/materials

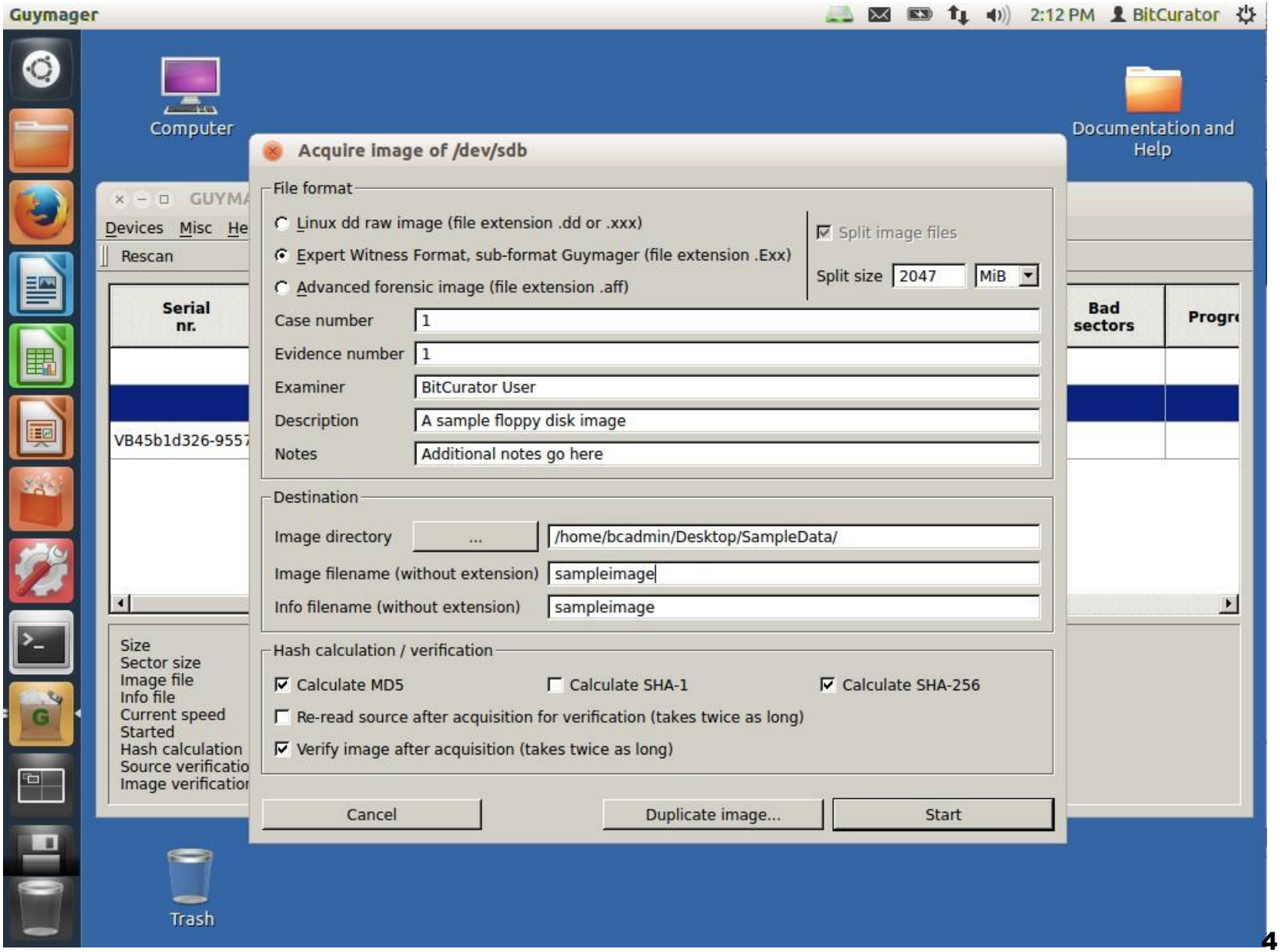
Learning objectives
This learning object might be used in a lesson to satisfy the following learning objectives:

- 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



Examples of Disk Image formats

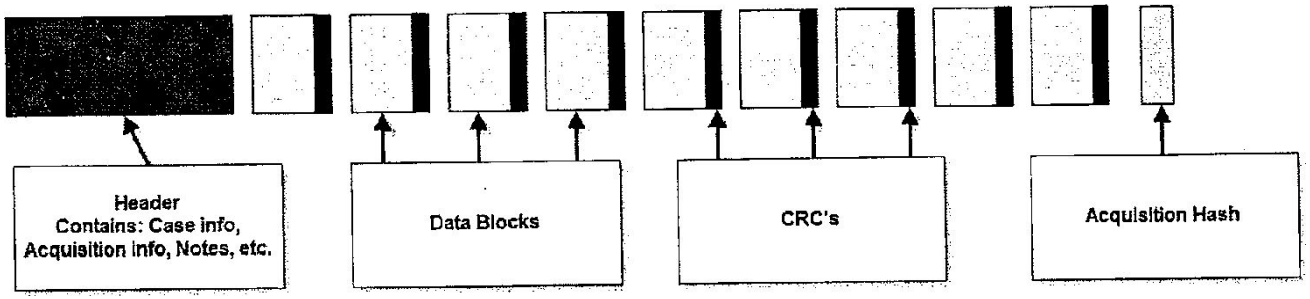
- RAW and Split RAW (RAW stored across multiple files)
- Advanced Forensics Format (AFF) [no longer recommended]
- EnCase Evidence File (.E01)
- ISO (for CD-ROM)
- IMG (floppy or sometimes CD-ROM)

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) - http://sourceforge.net/projects/libewf/files/



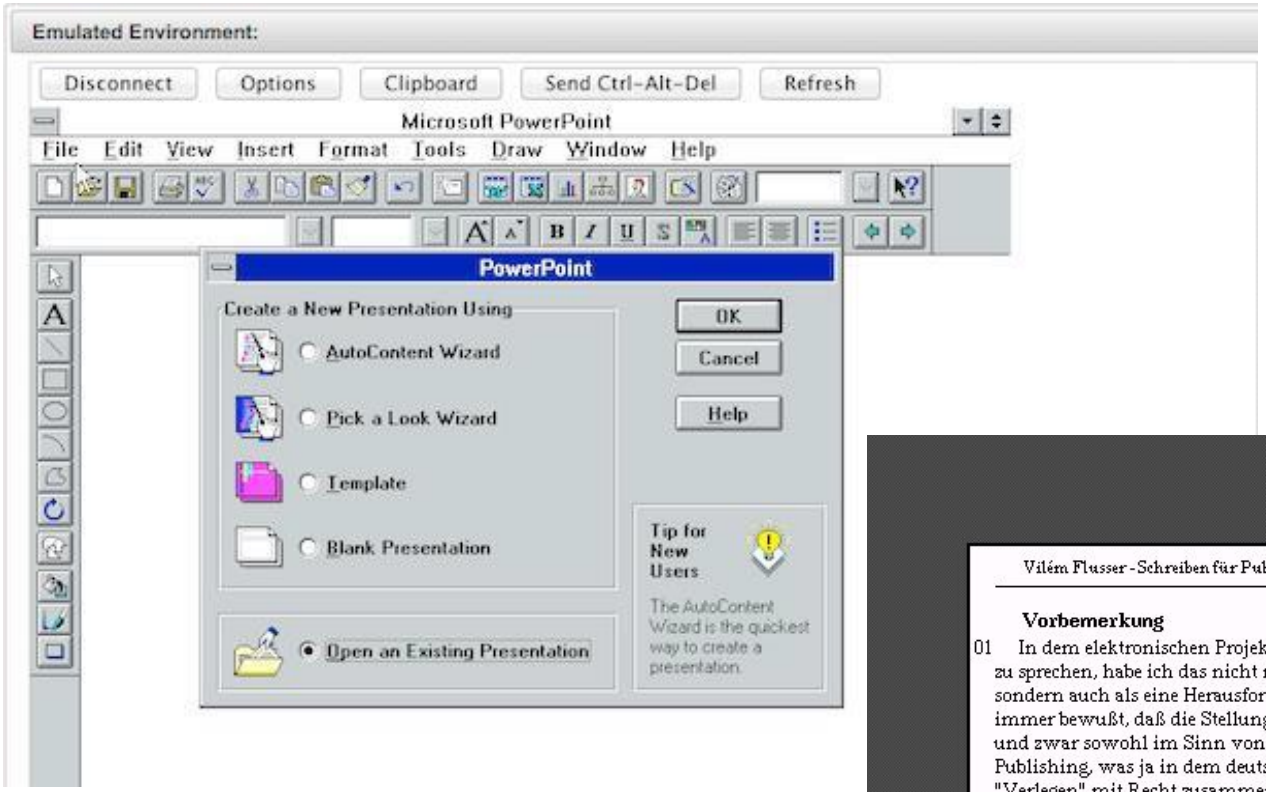
ISO Images (.iso extension) for CD-ROM or DVD

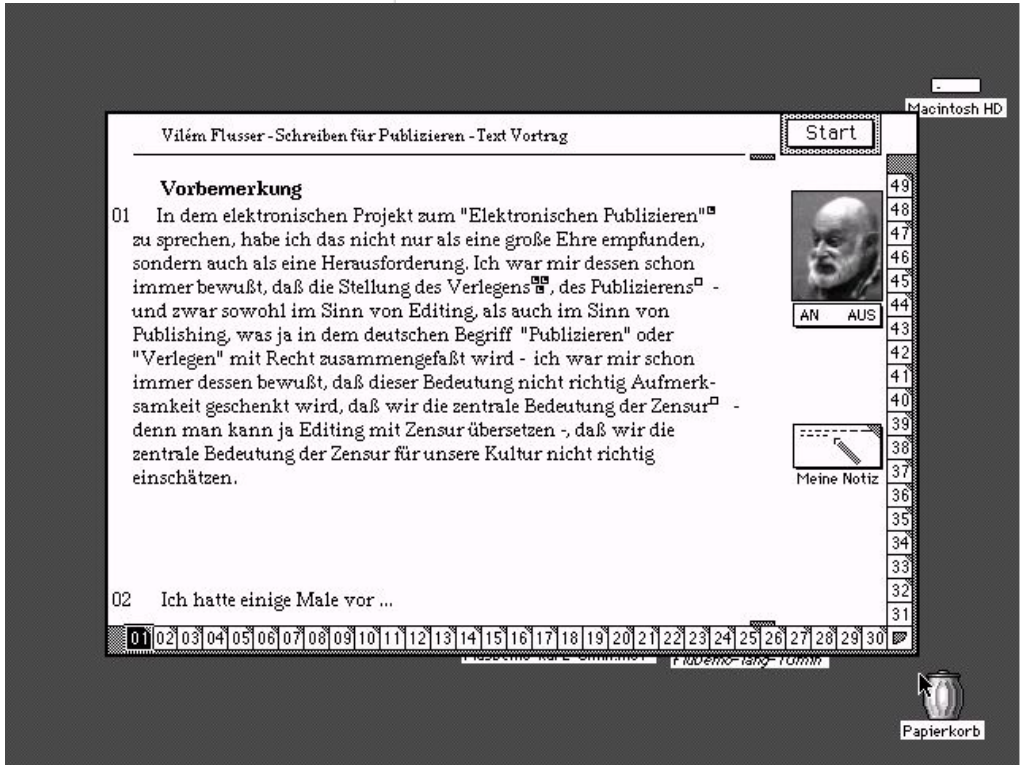
- Similar to raw, but can't contain
  - multiple tracks
  - audio or video tracks
- Don't contain control headers or error correction fields (raw can include these)
- Filesystem usually will be either ISO 9660 (CD-ROM) or UDF (DVDs)

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

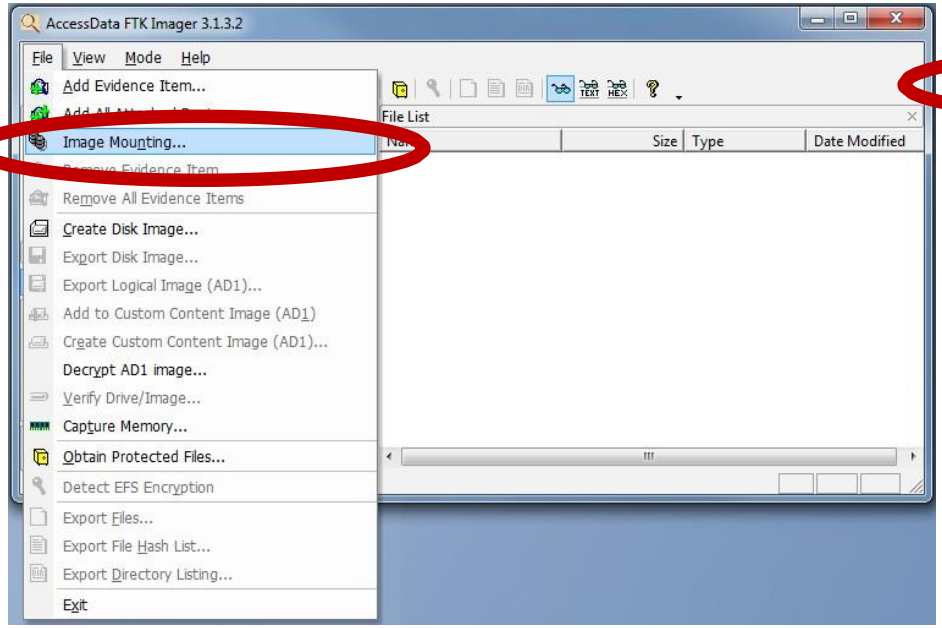
Emulation as a Service

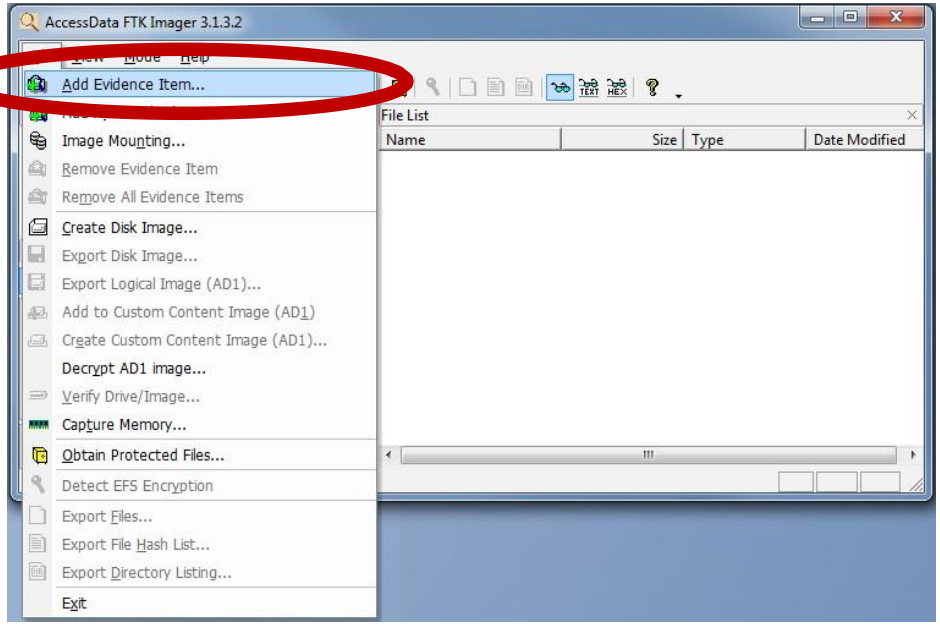




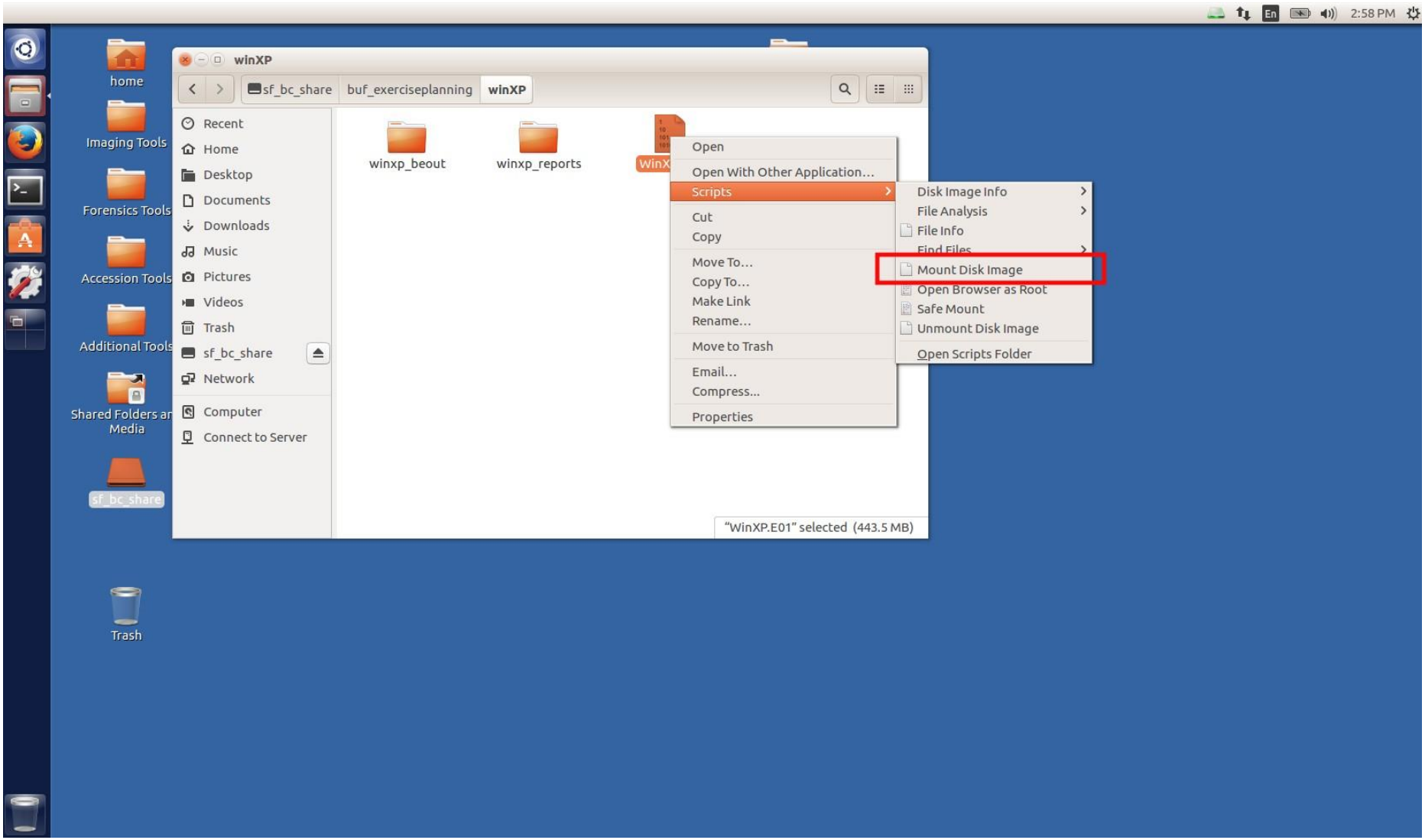
http://bw-fla.uni-freiburg.de/demos.html

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

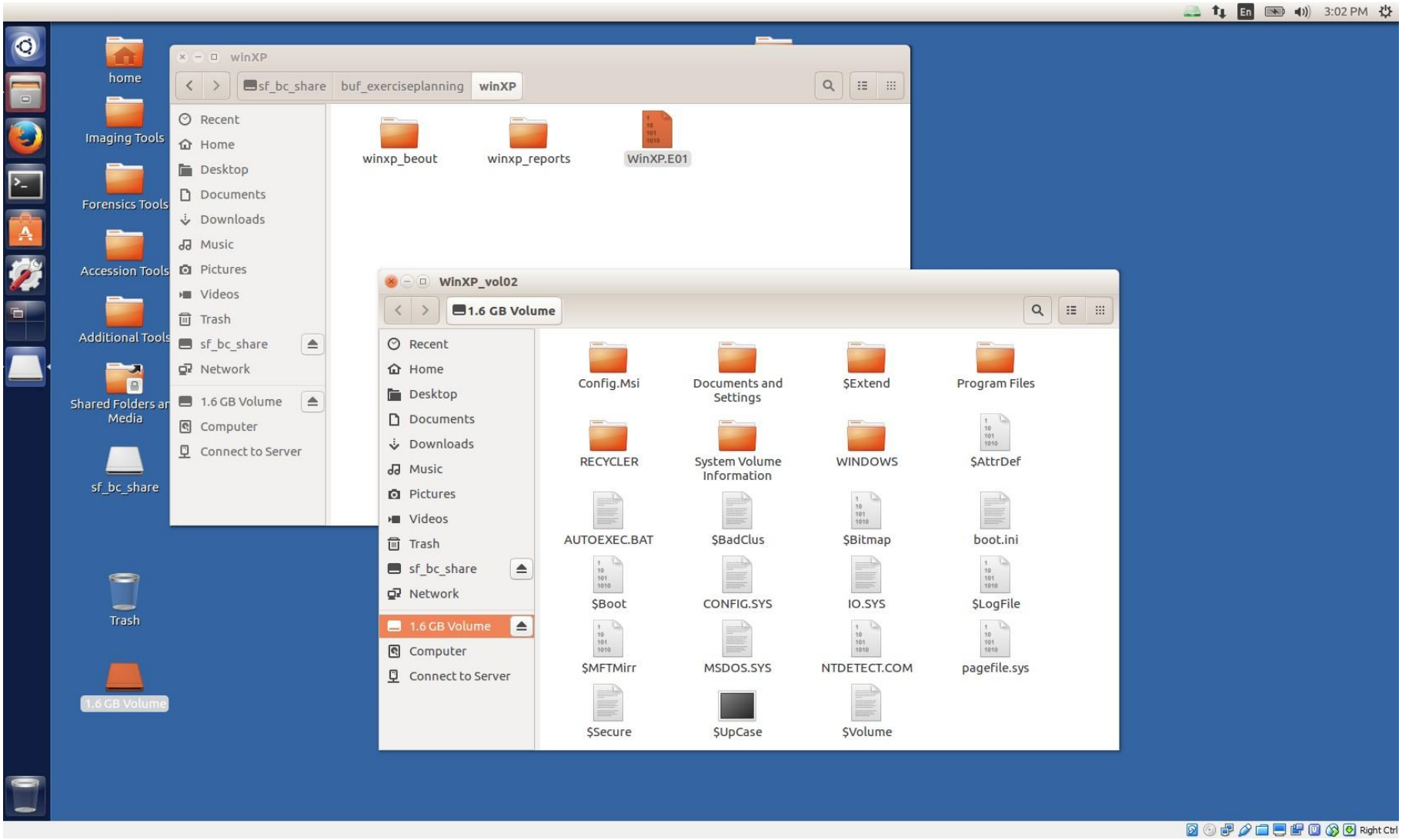




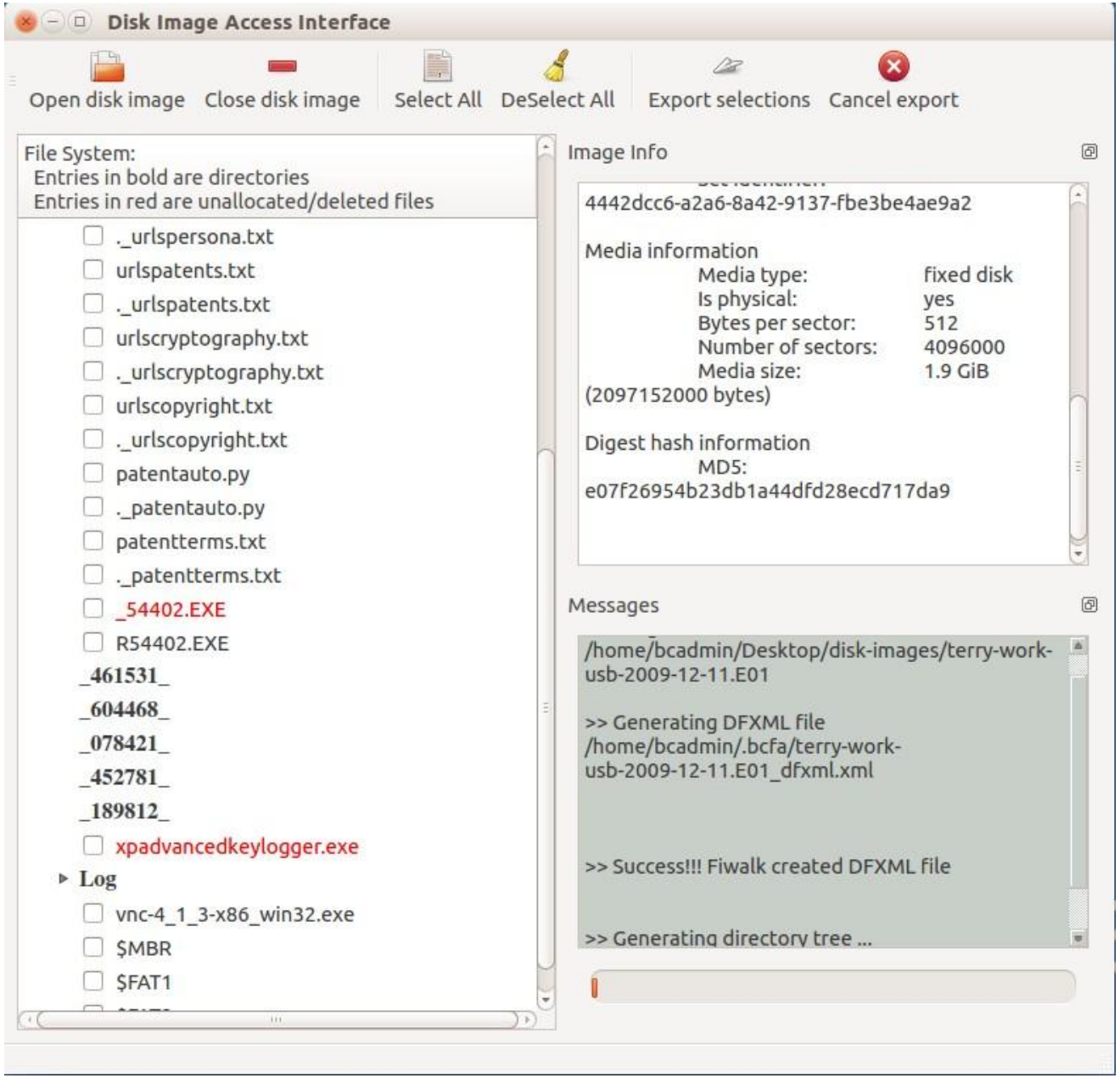
Mounting a Disk Image to Browse the Contents



Mounting a Disk Image to Browse the Contents



Exporting Selected Files from a Disk Image



Exercise: Multiple Views into Disk Image Files

- Resources we'll be using:
  1. ISO file - https://github.com/BitCurator/bcc-dfa-sample-data/blob/main/25.iso (or from flash drive)
  2. IMG file – https://github.com/BitCurator/bcc-dfa-sample-data/blob/main/something.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]

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 BitCuratorEdu project is a three-year effort funded by the Institute of Museum and Library Services (IMLS) 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 Educopia Institute and the School of Information and Library Science at the University of North Carolina at Chapel Hill, along with the Council of State Archivists (CoSA) and several Masters-level programs in library and information science.