

Using BitCurator

This page was moved to <https://confluence.educopia.org/display/BC/BitCurator+Walkthrough>
Click in the link above if you are not automatically redirected in 10 seconds.

Acquire

Whether you are creating forensic disk images, mounting physical media to inspect and analyze digital materials, or transferring files, BitCurator supports multiple acquisition scenarios.

Safely Mount Devices

Provides write-blocked access to removable media (e.g. USB drives, CD-ROMs, floppies)

Create Disk Images

BitCurator uses open source disk imaging tools, including Guymager and [dcfldd](#), to capture bit-identical images from magnetic, optical, solid-state, and hybrid media. Disk images can be captured in various formats, including raw (just the bitstream), E01 (Expert Witness Format, supported using the open source [libewf](#) library), and AFF (Advanced Forensic Format).

Capturing disk images in forensic formats such as E01 and AFF provides many advantages. The images can be stored compressed or uncompressed, can be split into multiple storage containers, can be parsed at the filesystem level without explicitly extracting the raw image, and *embed provenance and capture metadata along with the bitstream*. **Forensic images ensure that no inadvertent changes are made during pre-ingest chain-of-custody**, and provide a consistent baseline for generating different types of access materials.

Analyze and Appraise

BitCurator includes multiple software tools that assist users with identifying and prioritizing important information in raw and forensically packaged disk images. This includes files format identification, location of deleted files and files fragments, cryptographic hashing, and reporting on potentially private and personally identifying information.

Nautilus Scripts

Nautilus is a popular GUI file manager for Linux and it functions similarly to *Windows Explorer* on Windows systems and *Finder* on Macs. One key feature of Nautilus is the ability to add custom functionality by incorporating user-created [back-end scripts](#). These scripts work much like plug-ins for a web browser and extend Nautilus's basic functionality. A number of custom Nautilus scripts are included in the BitCurator Environment specifically geared to assist the digital archivist in pre-ingest data analysis. See below for specific instructions on how to use Nautilus to perform a number of critical data analysis tasks:

- [Calculate and Display MD5 Sums](#)
- [Extract Compressed Files](#)
- [Review File Info and File Details](#)
- [Display Disk Image Metadata](#)
- [Display a file in Hex editor](#)
- [Live Search for Files by Name and Content](#)

Extract metadata from disk images and files

BitCurator includes multiple tools to assist with extracting and exporting technical metadata from both disk images and individual files.

- [Generate Filesystem Metadata as DFXML](#)
- [View, edit, and export metadata from image files](#)
- [View and export information from HFS-formatted disk images](#)

Identify potentially private and sensitive information

BitCurator includes `bulk_extractor` (and the `bulk_extractor` GUI, `BEViewer`) to assist users in finding potentially private and sensitive information. The `bulk_extractor` tool employs stream-based forensics (analyzing the disk image at the block level) to identify features such as email addresses, geolocation metadata, and credit card numbers.

- [Find Potentially Sensitive Information with Bulk Extractor Viewer](#)
-

Generate Forensic Reports

Users can generate human-friendly BitCurator Forensic Reports using the data produced by Guymager, the Bulk Extractor Viewer, fiwalk, and Annotated Features report to explore born-digital materials completely (including hidden or partially deleted files and file fragments) with visualizations, XLSX transcriptions of file system metadata, high-level reports on file types, and overviews of features identified by bulk_extractor.

There are two ways to generate BitCurator Forensic Reports:

1. [Use "Run All" feature to generate all reports in one step](#)
2. [Generate reports](#) after completing individual steps:
 - a. [Find Potentially Sensitive Information with Bulk Extractor Viewer](#)
 - b. [Generate Filesystem Metadata as DFXML](#)
 - c. [Generate an Annotated Features Report](#)