Tools

Overview

The BitCurator Environment includes many individual tools to perform specific curation tasks. Listed here are all tools packaged by default in the environment, organized by the folder found on the BitCurator desktop. Links will take users to the corresponding external site or documentation. Where applicable, relevant BitCurator **Step-by-Step Guides** are listed as well.

Because BitCurator is an Ubuntu environment, users are able to download and install tools as in any other Ubuntu distribution or Linux OS.

In addition, much functionality is found in the file navigation system, Nautilus, through contextual menus. Listed are guides for many of these scripts.

- Data Triage
- Create MD5 Sums
- Display a file in Hex editor
- Disk Image Metadata
- Extract Compressed Files
- Live Search for Files
- Safely Mount Device

Imaging and Recovery

Brasero: GUI application to copy data and audio CD and DVDs

Guymager: Open-source forensic disk imaging tool

- See the Creating a Disk Image Using Guymager **Step-by-Step Guide**.

cdrdao: CD imaging tool (primarily for audio CDs)

Clonezilla: A imaging and cloning program for partitions and disks

dcfldd: A forensics-focused rewrite of **dd**

dd: Create raw disk images and transfer data between devices

ddrescue: A version of **dd** with additional options for data recovery

dumpfloppy: Suite of tools for reading floppy disks in arbitrary formats supported by the PC floppy controller, and for working with the resulting image files

ewfacquire: Acquire Expert Witness packaged disk images from devices on the command line. Part of the libewf library of Expert Witness tools.

- More documentation at the Forensics wiki.

Forensic analysis tools

BitCurator Disk Image Access: A GUI interface to browse raw and forensically-packaged disk images, export files and deleted items, and view disk image metadata.

BitCurator Mounter: A GUI application to list currently attached devices along with technical details. Allows users to mount fixed and removable media according to the current mount policy.

BitCurator Reporting Tool: A GUI-driven (and optionally command-line) tool for running forensics tools in sequence to produce human- and machine-readable reports in DFXML.

- Find instructions at the Creating Disk Image Reports using the BitCurator Reporting Tool **Step-by-Step Guide**.
- Use of the Reporting Tool is also covered in the Quickstart Guide.

Brunnhilde: Generates aggregate reports of files in a directory or disk image based on input from Richard Lehane's Siegfried.

bulk_extractor Viewer (BEViewer): A GUI front-end for bulk_extractor

- See the Bulk Extractor Viewer **Step-by-Step Guide**.
- See the Regular Expressions in Bulk Extractor **Step-by-Step Guide**.
- bulk_extractor is a critical component of the Annotated Features Report **Step-by-Step Guide**.

Disktype: Detects the content format of a disk or disk image

Fiwalk: Fiwalk is part of The Sleuth Kit's collection of digital forensics tools and is used to produce a DFXML (Digital Forensics XML) report on the contents of a disk image within the **BitCurator Reporting Tool**.

- See the fiwalk **Step-by-Step Guide**.

md5deep: Set of programs to compute MD5, SHA-1, SHA-256, Tiger, or Whirlpool message digests on an arbitrary number of files

nsrllookup: Query tool to check for a matching MD5 hash in the National Software Reference Library Reference Data Set

PhotoRec: File data recovery software designed to recover lost files including video, documents and archives from hard disks, CD-ROMs, and lost pictures from digital camera memory

RegRipper: Tool for extracting and parsing information (keys, values, data) from the Windows Registry

SDHash: File similarity tool using similarity digests

ssdeep: Fast hash generation

TestDisk: Data recovery software with focus on recovering lost partitions, making non-booting disks bootable again/partition table recovery

Packaging and Transfer

BagIt Python Library: Command line implementation of the BagIt specification

Grsync: GUI fronted for the rysnc command line tool to synchronize or transfer data between locations

Additional tools

Antiword: Converts the Microsoft Word 2, 6, 7, 97, 2000, 2002 and 2003 formats to plain text and PostScript

BitCurator Reports (command line): Command line implementation of the **BitCurator Reporting Tool**, see GUI entry under the *Forensic analysis tools* section

Bless Hex Editor: Hex editor to edit and view files as a sequence of bytes

ClamTK: Virus scanning

FIDO Format Identification: Command line tool to identify the file formats of digital objects, designed for integration into automated workflows

Fiwalk (command line): Fiwalk is part of The Sleuth Kit's collection of digital forensics tools and is used to produce a DFXML (Digital Forensics XML) report on the contents of a disk image within the **BitCurator Reporting Tool**.

- See the fiwalk **Step-by-Step Guide**.

GHex: A hex viewer/editor

GtkHash: A cryptographic hashing tool

Hashrat: Hashing tool supporting MD5, SHA1, SAH256, SHA512, Whirlpool, JH and HMAC versions of these. Includes recursive file hashing and other features.

HFS Explorer: Provides access to the legacy HFS file systems

- See the View and export information from HFS-formatted disk images **Step-by-Step Guide**.

Match BE Features to File Names: Command line implementation of the **BitCurator Reporting Tool** function

nwipe: Securely erase disks

Read Outlook PST File: A utility for reading and exporting the contents of PST files.

System Profiler and Benchmark: Link to the native system information tool

VLC media player: Multimedia player and framework that plays most multimedia files as well as DVDs, audio CDs, VCDs, and various streaming protocols.

If you would like to provide feedback for this page, please follow this link to the BitCurator Wiki Google Form for the Tools section.