

BlackBag Forensic Suite

Tools Description



Tool Name	Tool Description
Forensic Settings	Determine DiskArb setting, show hidden Unix folders and Multi-boot capacity
DCFLDD Assistant	Creates a GUI environment for using the dcfldd tool
PDisk Info	Obtain pdisk information of a device
PMap Info	Obtain pmap information of a device
IOReg Info	Obtain the ioreg information of a device
Directory Scan	Shows a complete directory listing of a selected volume or folder. Both visible and invisible files are present in the list. Obtain path, type and creator codes, File ID, Creation/Modified/Access/Backup/Attribute Modification dates. Select specific or all files that can be saved into a tab delimited report.
File Searcher	Enables an examiner to search the entire file system for a variety of different characteristics, including file names (extensions), file types, and creator codes. Once the needed files are found, an examiner can move the files or copy them to another location, generate a report of the found files, or simply verify file contents with GraphView.
Active File Searcher	Search active files for keywords or regular expressions throughout an entire volume or a single folder. Use dates to focus your search as well as filter out specific extensions.
Graph View	Enables an examiner to view graphic files or partial images. GraphView is especially useful when interesting data has been partially overwritten because an examiner can view whatever data is present. GraphView uses QuickTime to open hundreds of graphic file formats quickly and easily.
Phantom Search	Similar to FileSearch, enables an examiner to display the otherwise hidden files within a volume. In Mac OS X and other UNIX environments, malicious users are creating invisible files to hold nefarious data, and PhantomSearch enables examiners to find the files quickly.

Tool Name	Tool Description
Comment Hunter	Provides a quick snapshot of a subject's activity by gathering all comments from available files and displaying them in one central, easy-to-read location. By viewing the quick snapshot, an examiner can eliminate the need to open potentially thousands of files individually. Can also be useful in tracking down the original website of downloaded files because many websites include their locations in the comments field.
Header Builder	Enables the examiner to create a CRC of a header and then create an MD5 of the entire file (resource fork and data fork) for comparison to known sought files. HeaderBuilder is particularly useful when a group of known illegal images are hashed, then compared based on the hash, removing the need for an examiner to open and view each image.
MacCarver	Searches a system for specified header information and then locates matching headers within the file system. Once matching headers are discovered, MacCarver begins to "carve" a specific number of sequential sectors, which is useful when a suspect has changed the extension in an attempt to hide data. MacCarver searches the entire drive image, recovering both active files and files leftover in free space.
Image Buster	Provides the ability to search drive images for up to 128 key words. This tool is extremely useful in cases where classified information is found on systems where it was not authorized to be. ImageBuster can also search for web activity by scanning the entire drive image for URLs, providing an examiner with a quick snapshot of web activity, even if the URLs are in unallocated drive space.
Volume Explorer	Useful for an examiner who wants to view an HFS partition, see the files within it, and view the properties of each file, including the File ID field, which is especially useful when establishing a timeline around a specific file.
File Spy	A quick, all-purpose file browser that removes uncertainty about file contents by enabling an examiner to view the contents in ASCII format and navigate around the file easily.
Safari Cache Reader	Locate and view the cache of the Safari browser
Safari Cookie Reader	View the cookies received via the Safari browser; print to a text file if desired.
Safari Bookmark Reader	View the Safari bookmarks and meta data; print to a text file if desired.

Tool Name	Tool Description
Safari Download History Reader	View the Safari download history; print to a text file if desired.
Lock Master	An easy-to-use automation tool that locks or unlocks anywhere from one to hundreds of files to allow them to be edited or to prevent them from being edited.
Breakup	Simplifies the management of otherwise unruly folders that contain thousands of images by reducing a large directory or folder into smaller, more manageable sizes. Reducing a large directory can help in displaying files for analysis or in selecting a folder of files to burn a CD of evidence for discovery proceedings, for backup purposes, or upon request of the defense.
Device Checksum	Obtain the md5 or sha1 information of a device. If you are confirming the hash of a device be sure to set the block size to same number of blocks as the image.
DMG Rename	Rename images to the Macintosh supported .dmg naming convention