



# BlackBag Technologies, Inc.

## Macintosh Forensic Software Overview

BlackBag Technologies is a leading provider of computing forensic solutions. The BlackBag Macintosh Forensic Software (BlackBag MFS) is a suite of independent tools that give examiners the broadest level of flexibility available in the forensics field. Examiners can launch one or more of the applications during an examination to obtain as much evidence as possible from a suspect drive, all the while conducting thorough, efficient, and secure reviews of Macintosh file systems (HFS or HFS+), making the BlackBag software suite a valuable addition to the toolkit of any forensic examiner.

### Imaging

The imaging process is one of the most important aspects of computer forensics. At BlackBag we believe that examiners should have the flexibility of acquiring images with an open standard utility so that they can choose the best tool for analysis. For this reason, the BlackBag MFS supports several different methods of acquiring an image. While we recommend using `dd` given its flexibility and reliability, the BlackBag MFS is designed to work with any open imaging standard: `dd`, `i-Look`, `Disk Copy`, and `SafeBack`. Not all computer forensic analysis tools offer this flexibility, and some acquisitions done with proprietary tools cannot be analyzed using any other software, which limits examiners to the functionality of that application and might cause them to overlook valuable evidence. Therefore, BlackBag recommends imaging within Mac OS X to leverage powerful, built-in features, such as `dd`, to make the imaging process simple, fast, and flexible.

### Analyzing the Image

Analysis is best performed by using the same platform on which the original evidence was written. For example, the Macintosh formats, HFS and HFS +, contain information not readable by other operating systems. While performing analysis on a Macintosh operating system, an examiner can use built-in security features, such as turning off autodiskmounting, locking the device, etc., that will maintain the integrity of the suspect files throughout analysis, even when the examiner actually runs applications from the mounted file system. However, when imaging a drive, we recommend using the read-only BlackBag Firebox to maintain the integrity of the suspect files.

### BlackBag Macintosh Forensic Software

The following list represents the major features within the BlackBag MFS suite of independent tools.

*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.

*CommentHunter* provides a quick snapshot of a suspect'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. *CommentHunter* can also be useful in tracking down the original website of downloaded files because many websites include their locations in the comments field.

*DirectoryScan* shows a directory listing of a selected volume or folder. This listing can later be used as a guide for conducting analysis, or in many cases it might contain the incriminating information since both visible and invisible files are present in the list.

*FileSearcher* 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 GraphicView.

*FileSpy* is 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.

*GraphicView* enables an examiner to view graphic files or partial images. GraphicView is especially useful when interesting data has been partially overwritten because an examiner can view whatever data is present. GraphicView uses QuickTime to open hundreds of graphic file formats quickly and easily.

*HeaderBuilder* 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.

*HFS Extractor* provides the benefit of a Disk Copy file format (easily mounted so that the examiner can see things as the suspect did) and enables the examiner to review the active files when the initial image was acquired with another utility, such as SafeBack, dd, FWB, etc.

*ImageBuster* 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.

*ListBuilder*, used with ImageBuster, enables an examiner to prepare a list of keywords in any language that is supported by the operating system or any language created and mapped by a user. ListBuilder is useful when performing international investigations and when suspects attempt to conceal data by storing it in different languages or by mapping special alphabets to their equivalent ASCII characters.

*LockMaster* is 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.

*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.

*PhantomSearch*, 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.

*Typer* makes it possible for an examiner to reveal the type and creator code of a file by simply dragging and dropping any file onto the *Typer* tool.

*Volume Explorer* is 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.

BlackBag Technologies provides the most comprehensive suite of forensic software applications specifically built for the Macintosh operating system and will assist you in performing the best analysis of a Macintosh file system (HFS or HFS+). If you have any questions, suggestions, enhancement requests, or would like to receive product literature or purchase products, please visit us at [www.blackbagtech.com](http://www.blackbagtech.com)