BlackBag™ TECHNOLOGIES

BLACKLIGHT™

Mac OS X

iPhone and iPad (iOS)

BlackLight is a multi-platform forensic analysis tool that allows examiners to quickly and intuitively analyze digital forensic media. BlackLight is capable of analyzing data from Mac OS X computers, iOS devices (iPhone, iPad, iPod Touch) and Windows computers. It is compatible with all leading logical and physical forensic image formats.

Examiners may use BlackLight as a time-saving data triage tool, or as an advanced forensic examination tool depending on the circumstance. To learn more, please view the quick feature videos to the right, or use the drop down menus below which detail the many BlackLight features.

BlackLight Special Package Include:

- BlackLight
- MacQuisition
- SoftBlock

Latest Versions

BlackLight 2013 R1.1 was released April 30, 2013. Below are few of the new features you'll find in this release.

Operating System Specification

- Mac OS X Snow Leopard (10.6.0) or higher and Windows XP (SP3) or higher

Windows File System Support

- Import and process forensic images acquired from volumes and virtual machines formatted with the NTFS, FAT16, and FAT32 file systems.

Comprehensive Windows Registry Analysis

- Easily locate, analyze, and tag crucial MRU, and system, user, and application configuration Windows Registry keys. Search across all registry hives by key name, key value name, and/or key value content.

Enhanced Internet Artifacts Support

- Quickly and intuitively analyze Internet Explorer, Safari, Firefox, and Google Chrome Internet artifacts with the enhanced BlackLight Internet view.

Timeline Analysis

- View multiple Mac and Windows device files and communications chronologically to uncover important usage patterns. Drill down to isolate email, instant messages, voice communications, and files created or accessed within a specific time frame.

New File Filter Views

- Apply custom file filters independently within each BlackLight view to quickly pinpoint relevant media files, messages, email, contacts, and iOS device call data.

Key Features

The BlackLight Details view provides a visual device configuration and usage snapshot including:

- Device type, iOS / OS version, serial number, UDID, and IMEI.
- Artifact summary statistics for documents, emails, movies, calls, voice mail, and more.
- Device user account information and common Internet account information for applications such as Twitter and iCloud.
- Recent usage history including dialed phone numbers and associated contact information, last running applications, and most recent web-based location searches.

BlackLight's unique file filter includes preset and user-defined filter options to quickly pinpoint relevant date within large data sets. Filter criteria includes:

- File name, kind, size, or extension
- Date created, modified, or accessed
- Picture metadata attributes including GPS coordinates and camera (iOS device) type
- Positive and negative hash set filtering
- Users may apply any number of filters or inverse filters to quickly isolate important data from system files or base application files. BlackLight ships with several preset file filters including those that filter by file type, file attribute, geolocation coordinates, and source device type.

BlackLight acquires logical iOS device data and imports a number of third-party and industry-standard forensic image formats:

- Unix/Apple image formats: dd, .dmg
- Third-party image formats: EnCase® (EWF-E01), (EWF-L01), and SMART (EWF-S01) image files
- Third-party iOS physical and logical image formats: MPE+, ElcomSoft toolkit, Jonathan Zdziarski's Method, Cellebrite, and iXAM
- VMware® virtual machine files
- Automatic iOS backup folder recovery and import
- Time Machine and Time Capsule
- Individual files and folders

BlackLight supports a number of iOS and OS X messaging applications and message types including:

- iChat
- SMS
- MMS
- Skype
- iMessage

BlackLight has built-in support for many picture and video file types, and includes several helpful and unique media processing and analysis features such as:

- Video Frame Analysis: Triage multiple video files, displayed as 4x4 frame sequences, to quickly separate contraband from benign media.
- Proprietary Skin Tone Analysis Algorithm: Sort pictures and video by the skin tone percentage contained in the file.
- Built-in GPS Mapping: Media files containing GPS data display with a placemark badge. View media file geolocation data on a Mercator map (offline) or using Google Maps (online) directly from the built-in GPS view.

BlackLight is designed to be incredibly flexible. Examiners may export large data sets parsed in a human-readable format, and export examiner reports in a variety of formats to enable easy information sharing with both technical and non-technical interested third-parties.

- Easily tag evidence and include associated metadata in the examiner report. Report export formats include .pdf, .html, .docx, and .txt.
- Export eDiscovery data to a generic load file that is compatible with all major review platforms.
- Mask (blur) sensitive data contained in examiner reports that may be shared with non-authorized third parties.

BlackLight has extensive positive and negative hashing features and imports common third-party hash sets. BlackLight ships with a proprietary Mac OS X (10.0.0 through 10.8.3) system file hash set. Other file identification features include:

- Encase (6.19 and lower), NSRL, and custom text-based hash set import.
- Automated file hashing, known file analysis, and file signature analysis during OS X, iPhone, and iPad device acquisitions.

BlackLight has a powerful search feature that quickly isolates evidence contained in large data sets. Search in file names and/or file content.

- Search across multiple volumes and devices simultaneously.
- Search by keywords while including or ignoring specific file extensions.
- Easily search regular expressions such as MAC address, IP address, email address, URL, phone number, and postal code via a customizable drop-down menu.

BlackLight parses and displays Mac Mail application email accounts, several Internet log types, and chat logs.

- Full Safari, Firefox, and Chrome web browser support. View visited URLs and URL names stored by the web browser. View bookmarked websites, dates, times, and cookie contents (text strings and URLs).

- Full iChat and Skype chat application support. Display active chat files with text content, dates, names and file sizes. Export searchable chat conversations with examiner reports.
- Traverse the Mac Mail application directory structure for each user, and display all mail account names and email addresses associated with specific email message headers and content.

Several BlackLight features are designed to streamline workflow for individual examiners, and examiners working together in a larger agency. Features include:

- Custom Template Import and Export
    - Create and share standardized agency templates with preconfigured search criteria, file filters, evidence tags, and report elements.

- Side-by-side Evidence Analysis
    - Open multiple BlackLight window instances to simultaneously analyze and compare related evidence.

- Pause... Then Start Again
    - Built-in pause and crash recovery features. Pause work on a case, or restart after a system crash. BlackLight automatically picks up where the digital forensic investigator left off.

MacQuisition

MacQuisition™ is a powerful 3-in-1 live data acquisition, targeted data collection, and forensic imaging solution. Tested and used by experienced Mac forensic examiners for over 7 years, MacQuisition™ acquires data from over 185 different Macintosh computer models. Avoid complicated and time consuming take-aparts. MacQuisition™ runs on the Mac OS X operating system and safely boots and collects data from Xserve, Mac, iMac, Mac Mini, MacBook, and MacBook Air computers in their own native Mac OS X environment.

Key Features

Targeted Data Collection

- Target and forensically acquire files, folders, and user directories while avoiding known system files and other unresponsive data.
- Preserve valuable metadata by maintaining its association with the original file.
- Authenticate collected data using any or all MD5, SHA-1, or SHA-256 hash functions.
- Thoroughly log data acquisitions and source device attributes throughout the collection process.
- Selectively acquire email, chat, address book, calendar, and stickies on a per user, per volume basis.

Live Data Acquisition

- Capture important live data such as Internet, chat, and multimedia files in real time.
- Soundly acquire and save volatile Random Access Memory (RAM) contents to a destination device.

- Choose from 21 unique system data collection options including active system processes, current system state, and print queue status.
- Extensively log live data acquisition information throughout the collection process.

Forensic Imaging

- Avoid time consuming take-aparts. Use the source machine's own system to create a forensic image by booting from the MacQuisition USB swivel key.
- Image over 185 different Mac laptop, desktop, and OS X server models.
- Write-protect source devices while maintaining read-write access on destination devices.
- Extensively log forensic image acquisition processes, disk and volume attributes, and corresponding hash values.

SoftBlock

Now supports Mac OS 10.7 Lion! SoftBlock™ is a software-based forensic write-blocking tool. SoftBlock quickly identifies newly attached hardware devices, and mounts the device with read-only or read-write permissions according to user preference. This forensic software is built to handle the needs of both large-scale digital forensic labs and individual forensic practitioners. SoftBlock allows forensic examiners to quickly and safely preview data contained on evidentiary devices before data is imported. SoftBlock is built to run on a forensic examiner's analysis machine; no additional expensive or cumbersome hardware is needed.

Key Features

Support for Mac OS 10.7.x Lion

- SoftBlock™ runs on Mac OS 10.6.x and above.

Scalability

- SoftBlock™ handles as many hardware devices as a forensic analysis machine allows.

Mobility

- Avoid purchasing expensive write-blocking hardware. SoftBlock™ blocks data transfer at the kernel-level. No additional hardware is necessary.

Device Management

- A true timesaver. Quickly and safely mount and preview multiple external devices.

Seamless Workflow Integration

- SoftBlock™ features an intuitive user interface. Once installed, SoftBlock™ runs in the background and is available for use on demand.