Data Expert™ Technology Makes Possibility

Blacklight Analyze

One Tool • One Interface • All Four Major Platforms

BlackLight quickly analyzes computer volumes and mobile devices. It sheds light on user actions and now even includes analysis of memory images. BlackLight allows for easy searching, filtering and otherwise sifting through large data sets. It can logically acquire Android and iPhone/iPad devices, runs on Windows and Mac OS X, and can analyze data from all four major platforms within one interface. It's simply the best option available for smart, comprehensive analysis.

BLACKLIGHT®
ANALYZE

Windows Forensics:

Memory: Process hiberfil.sys (Vista and later), pagefile.sys, crash dumps (full, from Vista and 7) and live memory acquisitions (RAM) in seconds

Advanced Registry Analysis: Uniquely handles Volume Shadow Copies, Windows log and event files, and Registry artifacts (including customizable view of significant items, along with display of LNK files, Jumplist, shellbag, prefetch and superfetch data)

User-Specific Intelligence: User account information, recently opened documents and applications, Recycle Bin, USB device connection artifacts, automatic iOS backup detection, file filtering for all applications, event logs, and failed print jobs

Mac OS X Forensics:

Unparalleled OS X Recognition: Includes native recognition of Core Storage, FileVault 2 and Fusion Drives. Data Structure view color overlays to differentiate amongst data types

Robust Mac Analysis Features: User-specific .plist files, .fseventsd log parsing, device connections (including automatic iOS backup detection), network information (including location data for OS X 10.9 and later), user's look and feel, last file ID, Quarantine database parsing, Trash contents, and most recent documents, apps and servers

Mobile Forensics:

Device-Specific Information: Details view displays device type/OS, phone number, and device usage overview. Actionable intel displays registry artifacts, device connections and backups, recent file downloads, Trash and Recycle Bin, and user account information.

Versatile File Filtering and Analysis: Includes filters for user-created pictures, photos with EXIF information, GPS filter with KMZ export, and intuitive multi-device file hash comparison, as well as deleted SQLite recovery with custom tagging and reporting option

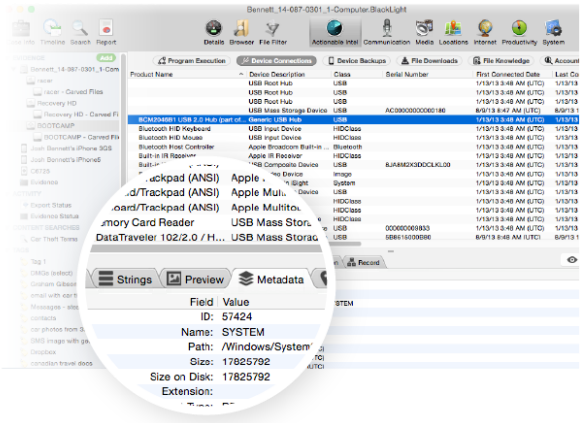
DataExpert (Thailand) Company Limited
Level 29, Suite No. 2986L, The Offices at Centralworld 999/9 Rama I Road, Pathumwan, Pathumwan, Bangkok 10330 (Thailand)
Website: www.dataexpert.co.th **Email:** info@dataexpert.co.th **Service Hotline: +66 2 207 8689**

Data Expert™ Technology Makes Possibility

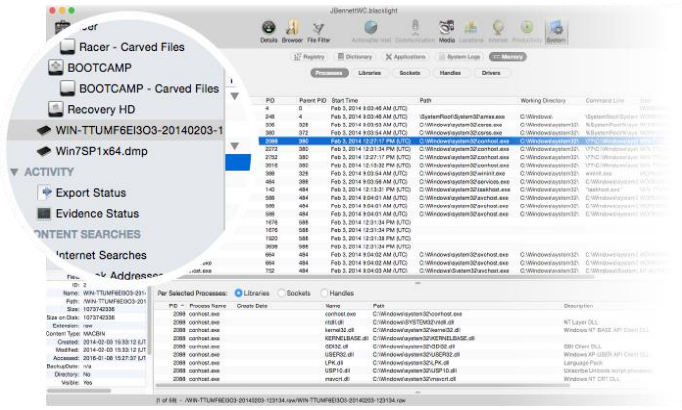
Features:

Easily Uncover User Actions

- Windows Registry artifacts - recently executed files and programs, link files, jumplists, Prefetch and Superfetch data
- Device connection data for all devices previously connected to the system, including USB device connection dates/times and the associated user account
- iOS device backups
- Recent file downloads
- Trash (for Mac OS X volumes) and Recycle Bin (for Windows volumes)
- Current and deleted user account info



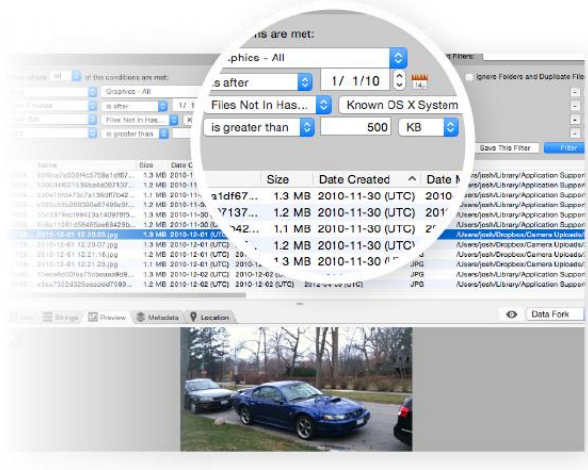
Analyze Windows Memory Files



- Analyzes several types of memory files, including raw dumps, Hibernation files (Windows Vista to Windows 10), pagefile.sys, and crash dumps (full, from Windows Vista or 7)
- Performs file carving and bulk extraction content searches (for numerous items such as URLs, addresses, phone numbers, etc.)
- Features a Memory subview for analyzing processes, libraries, sockets, handles, and drivers
- Processes memory files many times faster than traditional open-source forensic tools

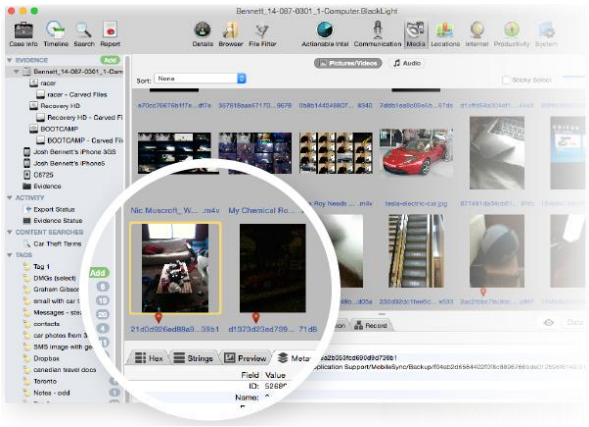
Efficiently Sift Through Large Data Sets

- File name, kind, size, or extension
- Date created, modified, or accessed
- Picture metadata attributes, including GPS coordinates and camera (iPhone/iPad device) type
- Positive and negative hash set filtering



DataExpert (Thailand) Company Limited
Level 29, Suite No. 2986L, The Offices at Centralworld 999/9 Rama I Road, Pathumwan, Pathumwan, Bangkok 10330 (Thailand)
Website: www.dataexpert.co.th **Email:** info@dataexpert.co.th **Service Hotline: +66 2 207 8689**

Find the Picture and Video Evidence You Need

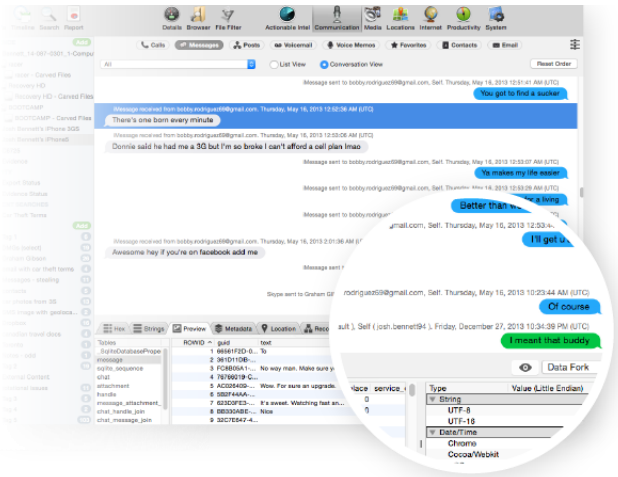


- Built-in GPS Mapping: All media files containing GPS data will be identified with a placemark badge. Examiners can view media geolocation data on a Mercator map (offline) or using Google Maps (online) directly from the built-in GPS view
- Proprietary Skin Tone Analysis Algorithm: Sort picture and video files by the skin tone percentage contained in the file
- Video Frame Analysis: BlackLight initially displays video files as 4x4 frame sequences, allowing examiners to quickly triage multiple video files in order to locate potential evidence

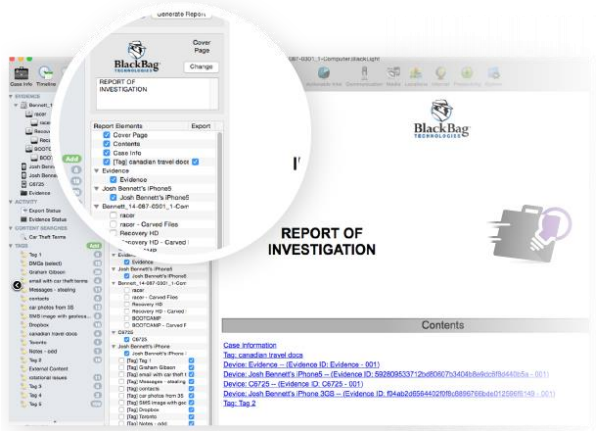
Recover Every Message from the Most Common Source

The Communication view in BlackLight allows examiners to see a full log of calls, voicemail, social media activity, and more. Most importantly, examiners can view messaging threads in list view or in their native format, with support for data from:

- Text Services (SMS/MMS, iMessage)
- Messaging Apps (Skype, Kik, TextPlus, TextFree, Tango)
- Social Media (Facebook, Twitter, LinkedIn, Foursquare/Swarm)



Customize Your Report



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

Data Expert™ Technology Makes Possibility

Files and Formats Supported

Operating System, Platform, Image Format and Hash Value Support	
Disk Image Support:	E01 (variants) / L01 / Raw (.dd) / DMG, VMDK/ .sparsebundle / .sparseimage / .img / .iso
Windows Memory Image Support:	Raw / hiberfil.sys (Vista and later) / pagefile.sys / Crash Dumps (Full) (Vista and 7)
Third-Party iOS Image Support:	MPE+ / Cellebrite / ElcomSoft / Lantern
Logically Acquires:	Android / iOS devices (iPhone, iPad, iPod touch)
Hash Value Support:	MD5 / SHA1 / SHA256 / PhotoDNA
Included Hash Sets:	Hashkeeper / Project VIC / Known OS X & Windows System Files (BlackBag Proprietary)
Comprehensive File Type Analysis	
Archives	.zip/ .sit/ .tar/ .gz/ .7z/ .rar/ .bz2
Databases	.db/ .sql/ .sqlit
Emails	.pst/ .ost/ general mbox / .olk15Message/ .eml/ .emlx/ .imapmbox
Graphics	.bmp/ .gif/ .jp2/ .jpg/ .jpeg/ .kdc/ .png/ .psd/ .tif/ .tiff/ .xbm
iWork	.numbers/ .pages/ .keynote
Movies	.3gp/ .avi/ .dv/ .flv/ .m4v/ .mov/ .mp4/ .mpeg/ .mpg/ .vob/ .wmv
Music	.mp3/ .aac/ .mpa/ .ogg/ .aiffff/ .wav/ .wma/ .m4a
Documents	.doc/ .docx/ .xls/ .xlsx/ .ppt/ .pptx/ .pdf
Platform Unique	.plist / .dat
Metadata Field Support	
Catalog Node ID / Size on Disk / Extension / Content Extension / Date Created, Modified, Accessed, Added / Attribute Modification Date / Visible / Locked/Root File Created, Modified, Backup, Accessed / Fork Count / Extended Attributes / Geolocation	
Custom File Filtering	
Path / Kind / Extension / Content Extension / Extension Matching / File Tagged State / Size / Date Created, Modified, Accessed / File ID / Hash Set / Hash Set Category / File Hash / List Duplicate Files / Suppress Duplicate Files / File Entropy / Locked / Resource Fork / Alternate Data Stream / Volume Shadow Copy / Visibility / Metadata Field / Metadata Value / Internal Filter	

Device Compatibility

IOS	iPhone 3G and newer with iOS 4.0 to 10.0
	All iPads with iOS 4.0 to 10.0
	iPod Touch 2G and newer with iOS 4.0 to 10.0
Android	Devices running Android 4.0.4 to 6.0
	Devices manufactured by: Samsung, Motorola, HTC, LG, Google Nexus

*Note: Additional devices running Android 4.0 or later may function properly if the appropriate USB driver for Windows OS is installed.

System Requirements

Operating System Specification	Mac OS X Yosemite (10.10) or higher / Windows 7 or higher
Compatibility	BlackLight runs on Intel® based systems only
	BlackLight requires the following additional software: • iTunes 12.6 or higher • QuickTime 7.6.9 or higher for Mac, and Windows Media Player 12 for Windows
Minimum Requirements	• Mac OS X Yosemite (10.10) or Windows 7 • 2.6 GHz Intel Dual Core i5 • 8 GB 1067 MHz DDR3 • 25GB of Disk Space • 1024 x 768 or higher screen resolution
Optimum Requirements	• Mac OS X macOS Sierra (10.12.5) or Windows 10 • 3.1 GHz 6-Core Intel Xeon E5 or better • 16 GB 1866 MHz DDR3 • 25GB of Disk Space • 1680 x 1050 or higher screen resolution

*Note: For Windows systems, BlackLight uses whatever the default app may be for playing media files. Windows Media Player 12 is recommended. If Windows examiners do not have QuickTime installed and they wish to play certain file types such as .AMR files (voicemail, etc.) they will need to install some non-default codecs, following the instructions found here: http://shark007.net/win8codecs.html

BlackBag TECHNOLOGIES