BLACKLIGHT 2019 R1 RELEASE NOTES

April 23rd, 2019

Thank you for using BlackBag Technologies products.

The Release Notes for this version include important information about new features and improvements made to BlackLight. In addition, this document contains known limitations, supported versions, and updated system requirements. While this information is complete at time of release, the information below is subject to change without notice and is provided for informational purposes only.

SUMMARY

To enhance our forensic analysis tool, BlackLight 2019 R1 includes:

- Built-in Image Categorization using Image Analyzer
- Smart Indexing - Initial Release
- Logical Evidence Files (EnCase© .L01 format) export option
- New Investigative Notes option
- Ability to ingest AFF4 evidence from MacQuisition 2019 R1 to support latest Apple systems with the T2 chip or APFS Fusion
- Time Capsule and Time Machine improved support
- Photo DNA and Project Vic updated support
- Windows 10 and Apple Mojave system artifacts improvements
- Added GoPRO LRV filetype support

NEW FEATURES

Image Categorization with Image Analyzer Integration

Image categorization reduces review time by revealing images and videos that may contain categories of interest. BlackLight now includes Image Analyzer's latest machine learning technology for image categorization. Image Analyzer is a proven solution with years of experience in categorizing images. Users can run image categorization across pictures and videos with no Internet connection.

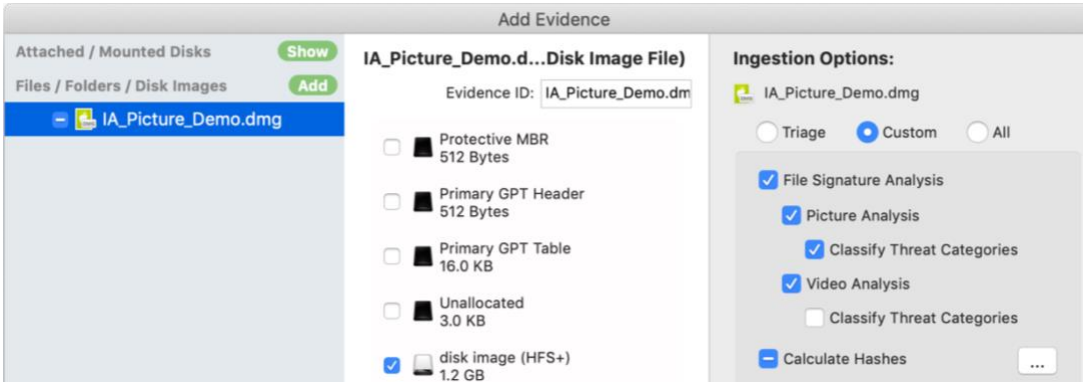
BlackLight will look for the following categories:

- Porn
- Weapons
- Drugs
- Extremism
- Gore
- Alcohol
- Swimwear/Underwear

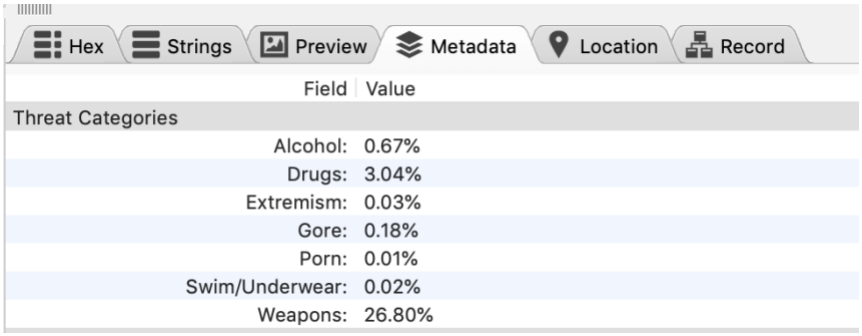
All available threat categories will run when Image Categorization is used in BlackLight.

Improvements to Image Analyzer, including new threat categories, will be provided with new releases of BlackLight. New image categories can be requested using the feedback form: https://www.blackbagtech.com/productfeedback.html.

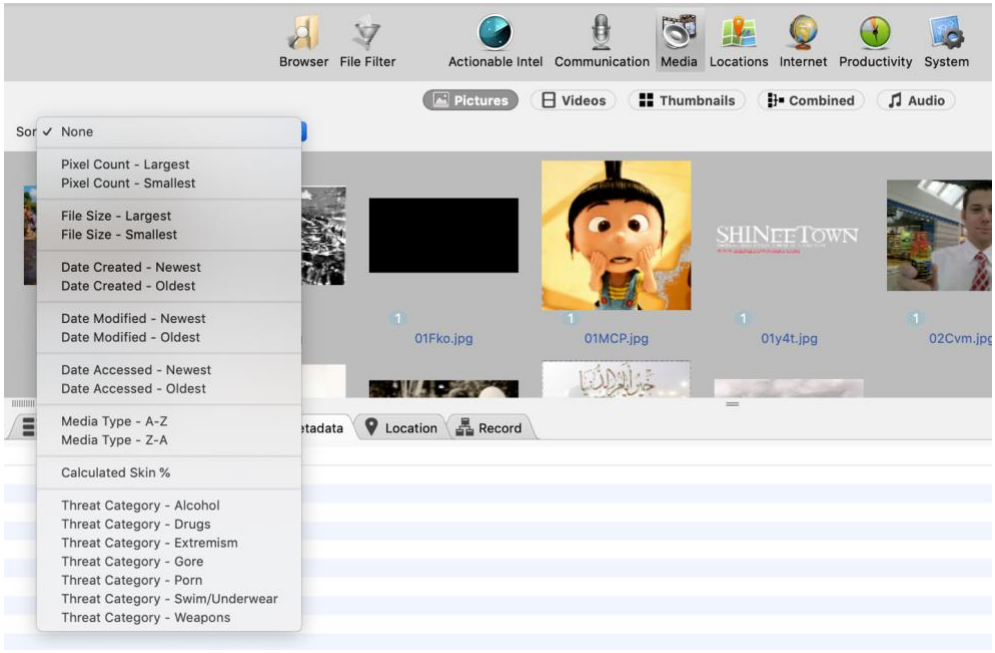
Image Analyzer can be run at the time evidence is added or later. To run during initial ingestion, check the **Classify Threat Categories** options under **Picture Analysis** and **Video Analysis**.



Threat Category results can be seen in the 'File Information Pane' or the **Metadata** tab in 'File Content Viewer.'



In ‘Media’ view, users can sort by Threat Category.



In the ‘Media’ view files can also be filtered by Threat Category. In addition to choosing the Threat Category of interest, using one of five modifier options: is less than, is greater than, is between, is less than or equal to, or is greater than or equal to.

For additional information on using Image Analyzer with prior cases and troubleshooting tips please see the User Guide “What’s New” section.

Smart Indexing - Initial Release

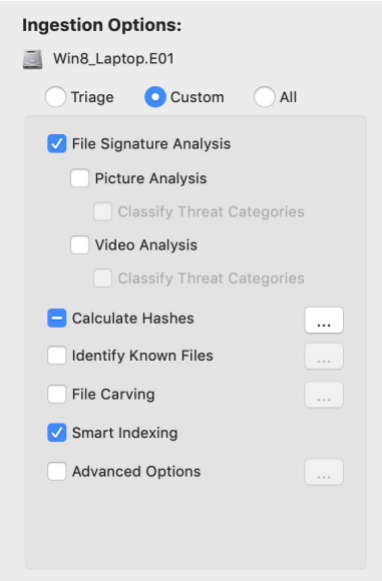
Creating an index of text documents on a device allows an examiner to quickly find if a particular topic or subject is mentioned within the evidence set. While the process of creating an index has historically been time consuming and resulted in bloated cases sizes, advancements around this field now allow BlackLight to provide users with a quick and efficient process to build the index. Once built, investigators can follow where the leads take them by making fast sequential queries of the index for words without waiting for a traditional search of the drive contents. Index searching also includes operations like proximity and Boolean logic to refine which files are most relevant.

With this initial release, BlackLight provides index capabilities only for allocated files on the file system. These are the files most relevant and likely to be useful for prosecution. Data extracted by BlackLight from inside

of container files like internet history, email, or archives as a result of processing are not included in the index in this initial release but will follow shortly. During this initial release we will be working with customers to refine the query interface and feature set.

Creating the Index

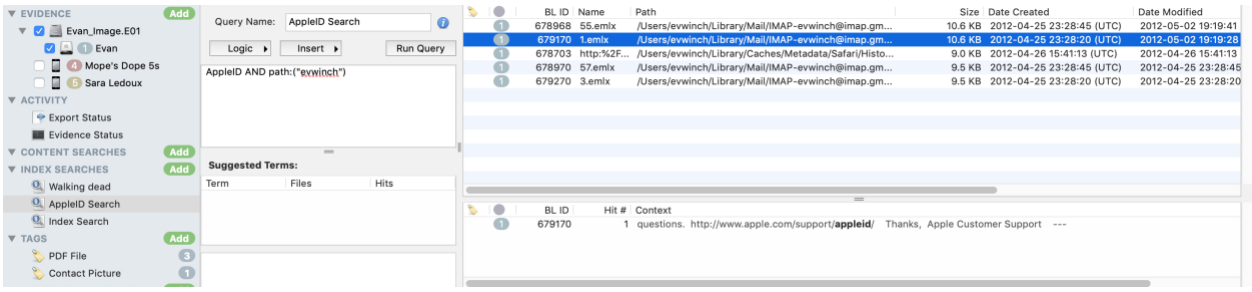
Indexing is a processing option that can be selected when the Evidence is added or after initial processing from the Evidence Status page.



Once an Index is created, users can search the index by creating a new Index Search in the left-hand pane. An Index search allows the examiner to search for specific words, combinations of words, pathnames, file size, date created, date modified, date accessed, and date changed using AND, OR, and NOT operators.

Searching the Index

BlackLight uses an implementation of Elastic search for smart indexing. By default searching the index, also called querying the index, will look across all the fields and documents that have been indexed. Additional functionality has been built in to allow examiners to further specify which files they are interested in. Common searching techniques and examples are summarized below.



When searching the index, users enter a **query string** that is interpreted by the index engine into a series of terms and operators.

A **term** can be a single word — quick or brown — or a phrase surrounded by double quotes — "quick brown" — which searches for all the words in the phrase in the same order. By default, entering only terms will search the index for any items that contain one or more of those words, exactly as you enter them in the search field. Index searching is not case sensitive.

Operators allow you to customize the search — the available options are explained below.

Query Options	Operator	Example query string	Result
AND Used to indicate both terms on either side of the AND must be present in the item	**AND**	quick AND brown	A file with the phrase “the quick brown fox” or “the brown fox is quick” would both be found by this query
OR Used to indicate at least one of the terms on either side of the OR must be present in the item	**OR**	quick OR brown	A file with the phrase “the quick fox” or “the brown mouse” would both be found by this query
NOT Used to the term after the NOT is not located in the item	**NOT**	quick NOT brown	Returns files with the word quick but that do not have the word brown in the file
Grouping Terms In order to build complex queries, users can group terms and operators	**()**	(quick AND brown) OR (slow AND steady)	Returns files with either the words quick and brown or the words slow and steady.
Wildcard Typically used at the end of a term to indicate find any words that start with these letters	*****	bro*	Both items with brown and browns would return a hit
Replace One Character Locate files with where the ? can be any single character.	**?**	qu?ck	Both quick and quack would have a hit, but not quaeck
Proximity Allows users to specify a maximum distance of words in a phrase. In addition, they can be in any order	**~distance number**	“fox quick” ~5	Items with “quick brown fox” or “fox is running very quick” would both return hits since they are within 5 words.
Date Searching Locates only items within the date or date range. Can be combined with other terms to find files within a date range and with terms	**date:[YYYY-MM-DD TO YYYY-MM-DD]**	created: [2000-01-01 TO 2020-12-31]	Locates files with a created date between January 1st, 2000 and December 31st 2020
Path Searching Locates only items specific terms in the path	**path:(“term”)**	path:(”SMS”)	Locates files where the Path field contains SMS
Metadata Field Searching For any other metadata fields, can search for specific values in that field	**“Metadata field: term”**	“Device Model: iPhone 4”	Locates files where the Device model metadata field matches iPhone 4 exactly

Date and Number Ranges

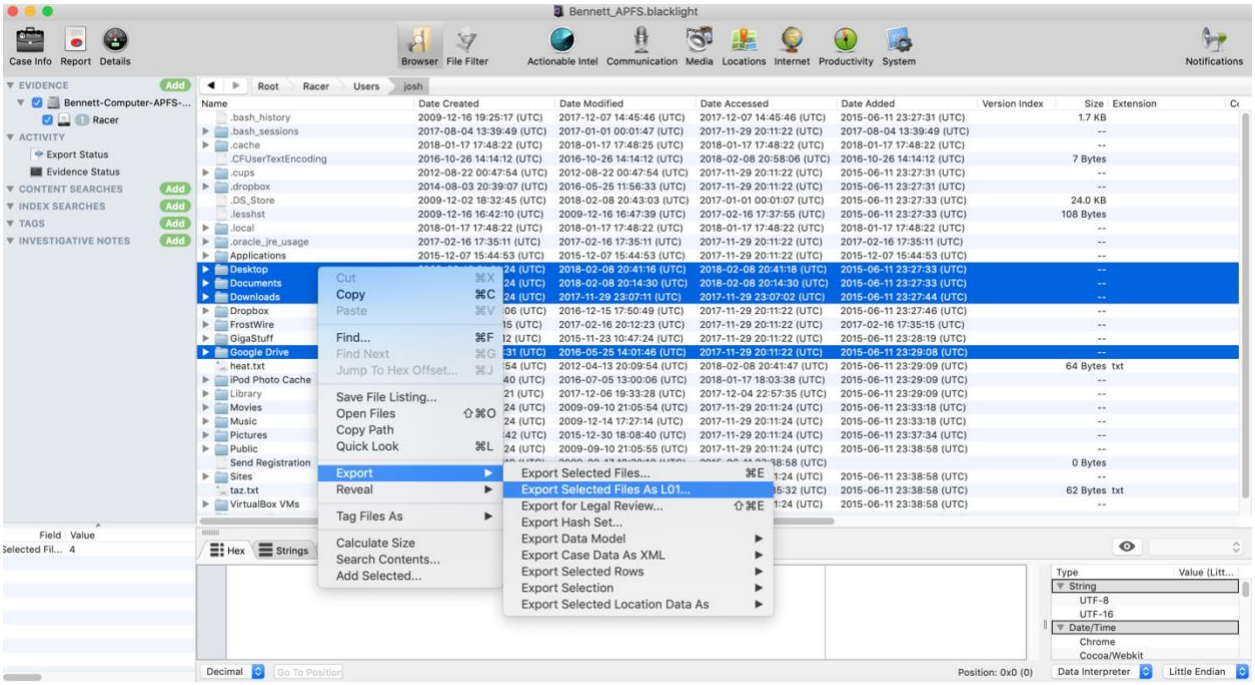
Ranges can be specified for date, numeric or string fields. Inclusive ranges are specified with square brackets `[min TO max]` and exclusive ranges with curly brackets `{min TO max}`.

Range option	Example Operator	Result
Date range inclusive All days in a range including the first and last specified	`created:[2019-01-01 TO 2019-12-31]`	All Files with a created date in 2019
Number Range All numbers in a range including the first and last specified	**Count: [1 to 5]**	Files where the metadata field "Count" has a value of 1, 2, 3, 4, or 5
Items Before a Specified Date Use the wildcard to indicate any time before a specific date	**`created`: {* TO 2019-01-31}**	All Files with a created date before January 31st 2019
Items After a Specified Date Use the wildcard to indicate any time before a specific date	**`created`: {2019-01-31 TO *}**	All Files with a created date after January 31st 2019

The index can also be searched using standard Lucene query syntax, along with most Lucene search operators and term modifiers. For more advanced options on Elastic search operators and term modifiers, see the Elastic Documentation.

Export files to EnCase© Logical Evidence Files (.L01) format

The EnCase Logical Evidence File Format (L01) is widely supported by Forensic and eDiscovery tools and preferred as a forensic container for logical files as it preserves file content, metadata, and folder structure. BlackLight now allows you to create Logical Evidence Files directly as an export option. Logical evidence files can be created using the **[Export]** menu. Metadata and folder structure is maintained for the files and folders exported in logical evidence files. Select the files and folder to include in the logical evidence file. Access the **[Export]** by right (contextual) clicking or from the **[Action]** menu.



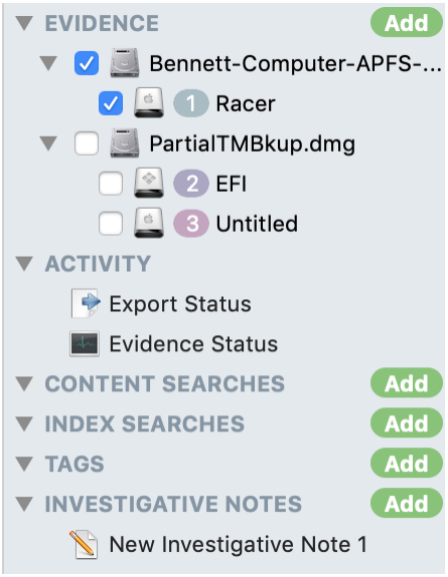
Once **[Export Selected Files as L01...]** is selected a 'Save' dialog window appears. Select (or create) a destination folder.

AFF4 Images of Apple systems with T2 chips or APFS Fusion drives

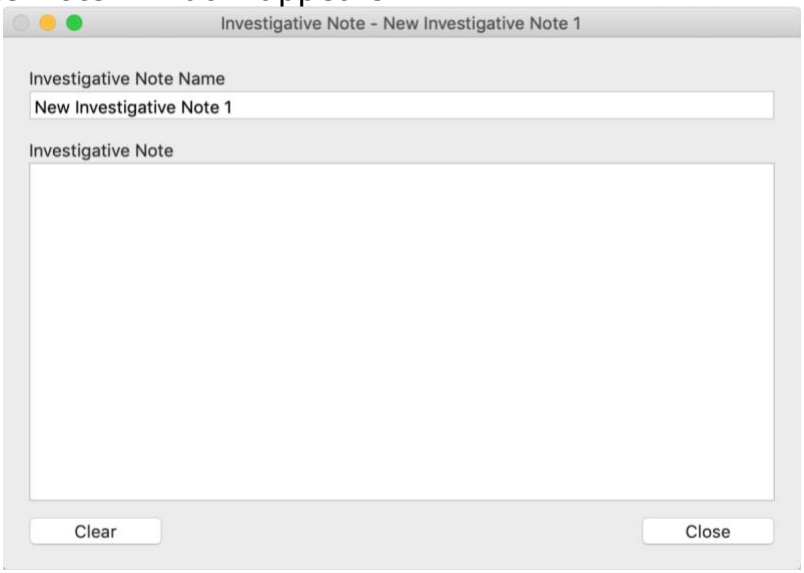
MacQuisition 2019 R1 will be able to create a decrypted physical image of Apple systems with T2 chips as well as for APFS Fusion drives. When MacQuisition creates these images, they will be in the AFF4 evidence file format. BlackLight 2019 R1 has been updated to ingest and process the AFF4 evidence files.

New Investigative Notes

Investigative Notes are accessible in the Tag area of the component view. The Investigative Notes provide and area for the examiner to copy and paste or type in information they wish to note during the analysis. To add an Investigative Note, in the 'Component List' select the green **Add** button to the right of 'Investigative Notes.'



An ‘Investigate Note’ window appears.



The window provides and area to give the Investigative Note a name and then the area to paste or type in content. Investigative Notes are saved in the case file but are not included in the analysis report.

Export Unique Files from Time Machine Backups

Time Machine backups, including the backups stored on a Time Capsule, contain incremental backups of a macOS system. These backups are stored in the folder Backups.backupdb, which stores date/time folders for each backup. On Time Capsule, the Backups.backdb folder is stored in a sparsebundle. Time Machine backups are incremental but use Hard Links to give the appearance of full backups in each date/time folder. Once the first backup is created, Time Machine creates Hard Links in subsequent date/time folders that serve as pointers to the original files. When the next backup is made, only the files that have changed are copied into the backup and Hard Links are created for files that are not changed.

When BlackLight processes a Time Machine backup, all the files and Hard Links are processed. Consequently there can be millions of files and Hard Links in each Time Machine backup. When a folder is Exported from a Time Machine backup, the Hard Links are resolved, exporting the same file multiple times.

Examiners may now choose to export only unique files from a Time Machine backup.

Operating System Improvements

BlackLight has also improved support for data structures related to macOS and Windows operating systems.

- Support has now been added for macOS Mojave (10.14).
- Windows improvements include:
  - Parsing file size in **Actionable Intel** for files in the Recycle Bin ($I records)
  - Improved $MFT, $Logfile support, improved $USNJRNL parsing.
- Support has also been added for parsing ExFAT volume boot records.

Additional Updates

BlackLight now processes GoPRO LRV files.
Updates were made to support newer versions of Photo DNA and Project Vic.

KNOWN LIMITATIONS

Use of ExFAT for storage media is NOT recommended.

Due to issues with the Apple file system driver use of exFAT formatted storage media may cause serious performance issues when using BlackLight. We highly recommend that you DO NOT use exFAT for storage of your case or image files on macOS and highly recommend the use of NTFS, HFS, or APFS for storage.

RESOLVED ISSUES

BL-12983	Ingesting Cellebrite iOS physical images are now parsed and added to the case
BL-14822	Improved performance of Media view when scrolling
BL-14703	$USNJRNL entry MFT and parent MFT reference numbers are parsed properly
BL-14643	Improved Report when exporting tagged files
BL-14627	Dongle license for EWMounter is properly detected
BL-14605	Picture processing completes on some image where it previously would not finish
BL-14550	Improved Android SMS messages
BL-14489	Improved SMS database parsing
BL-14486	Specific evidence that could not be parsed is now added properly
BL-14427	Specific APFS images that were unable to be parsed now complete properly
BL-14147	Processing now completes on images that previous reported temp out of space
BL-14137	Add Evidence no longer deselects processes when user clicks on unallocated partition
BL-14129	When using Search Criteria view and clicking on + to expand Skipped Files there is no longer an error
BL-13859	System -System Logs: $USNJRNL data view has been improved
BL-13812	APFS unallocated space from pool is properly labeled
BL-13726	Media view is now available when Unallocated partition is selected after carving
BL-13474	PhotoDNA processing now completed more quickly
BL-13470	Windows - Export Log Created and Modified timestamps are properly adjusted
BL-12686	Restore Case Archive: restored case with iPhone backup import no longer shows the device as "<Unavailable>"
BL-14652	Tagged emails now show up in proper order
BL-14638	Improved UI responsiveness on Windows when working with GrayKey extraction
BL-14565	On some evidence Internet Logs are now parsed, where prior parsing did not complete
BL-14501	C4all export has been updated to properly support ingestion for tools like Griffeye
BL-14139	Improved Exporting Time Machine data at parent folder to include all child folders and files properly
BL-14102	Updated deleted recovered messages from Chat.db to locate additional items
BL-13888	Attached Disk can now add attached unlocked FV2 volume from mounted E01 or DMG image
BL-13373	Improved Outlook 2016 for Mac emails rendering
BL-11766	Exports Specific Selected Files from Browser view on Windows no longer errors
BL-11635	Improved View filter date conditions on System-Systems logs content view
BL-11393	Improved viewing Shellbags
BL-10973	Properly updated Evidence Status: Hashes column after adding additional hash processes
BL-14876	Improved support for Graykey extraction to link .m4a files in Voice memo view
BL-14029	Improved support for Graykey extraction to support displaying Kik messages
BL-14893	iPhone XR/iPad Pro now display device icon in Details view
BL-14656	Improved L01 parsing to support logical evidence files over 2G
BL-14423	Communication-Contacts - Contact Details pane: Font is now red italic for deleted records
BL-10767	Communication-Email view: all mbox emails are now displayed properly
BL-14888	System-> System Logs-> FSEvents Identifier column now sorts numerically

SYSTEM REQUIREMENTS

OPERATING SYSTEM SPECIFICATION	Mac OS X 10.11.4 or newer*‡ Windows® 7 or newer Windows® Server 2016 or newer
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 • Windows Media Player 12 for Windows
MINIMUM REQUIREMENTS	• Mac OS X El Capitan (10.11.4) or Windows 7 • 2.7 GHz Intel Dual Core i7 • 16 GB DDR3 • 5GB of Disk Space (Installation) • 25GB of Disk Space (Temp Space) • 1024 x 768 or higher screen resolution
OPTIMUM REQUIREMENTS	• MacOS Sierra (10.12.6) or Windows 10 • Intel Xeon E5, 6-Core, or better • 32 GB DDR3 or higher • 5GB of Disk Space (Installation) • 25GB of Disk Space (Temp Space) • 1680 x 1050 or higher screen resolution

‡ We recommend strongly against using macOS versions .0 and .1 in all cases. For example (10.13.0 or 10.13.1)

**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.

For information about downloading iTunes and QuickTime, please visit http://www.apple.com/quicktime/download/

SOFTWARE DOWNLOADS

The BlackLight® macOS installer is delivered as a package file (.pkg) while the Windows installer is delivered as a setup executable.

In addition to the BlackLight installers, installers for offline maps, operating system hash sets, and memory symbols will need to be installed in order for BlackLight to take advantage of those. All installers can be found on the BlackBag software downloads page here: https://www.blackbagtech.com/resources/software-downloads.html

SUPPORTED DEVICES

IOS

- iPhone 3G and newer with iOS 4.0 to 12.2
- All iPads with iOS 4.0 to 12.2
- iPod Touch 2G and newer with iOS 4.0 to 11.4.1

ANDROID

- Devices running Android 4.0.4 to 8.1
- 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

SUPPORT

If you need support, we are here to help.

Please use the form at https://www.blackbagtech.com/support.html to submit your request for support and someone for our technical support will respond.

FEEDBACK REQUESTS

As we grow and perfect new features and functionality within our products we need you to continue to provide the insightful feedback that has allowed us to develop the tool we are proud to offer today. If you would like to submit feedback or suggestions, https://www.blackbagtech.com/productfeedback.html. Through your feedback, we can continue to provide investigators with the solutions they need to solve the critical issues they face every day.