MACQUISITION 2020 R1 RELEASE NOTES

February 20, 2020

Thank you for using BlackBag Technologies products.

The Release Notes for this version include important information about new features and improvements made to MacQuisition. In addition, this document contains supported versions and 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 Mac forensic imaging tool further, the new features and enhancements of MacQuisition 2020 R1 include:

- Triage before collection in both live and booted mode
- New Browser View to preview file content prior to acquisition
- New Search View to locate files using filters or keywords before acquisition
- While triaging in the Browser and Search views, files and folders can be added to the data collection
- Ability to stored data collection in the .L01 logical evidence file format
- Added capabilities to decrypt unallocated space on T2 drives
- Added hashing for AFF4 images as the data is collected
- Restructured MacQuisition log files
- Capture RAM and targeted collections live on macOS 10.15 (Catalina)
- Support added to boot newer hardware

Triaging with MacQuisition

Imaging multiple macOS computers and external media that may or may not contain data relevant to an investigation can be time consuming and waste precious time, storage space, and other resources. MacQuisition's new capabilities allow users to focus available resources with effective and efficient triage functionality.

Triaging can be performed in both live and booted mode to determine whether further analysis of a system or device is warranted. Two new tabs were added to MacQuisition to provide triaging capabilities. The **Browser** and **Search** tabs both have a preview feature providing the examiner an opportunity to see the contents of a file prior to acquisition.

Browser View

The **Browser** view permits navigation through the file system of connected volumes. As files are highlighted, a preview of the file is displayed in the preview pane of the **Browser** view. File metadata is also displayed. File previews work on file types supported by macOS QuickLook: pictures, videos, office files, pdfs, etc.

Search View

The **Search** view permits filtering data and searching for data by keyword. Filter criteria includes: **Location** (path), **Name** (file name), **Extension**, **File Size**, and **Date** (created, accessed, and modified). The **Content** field is provided to search the connected media for data using a keyword. Options are provided to **Search Binary Files** and to **Search Documents**. By combining the filter methods and searching the content for a keyword, relevant data is displayed in the **Search** view. As files are highlighted, a preview of the file is displayed in the preview pane of the **Search** view. File metadata is also displayed. File previews work on file types supported by macOS QuickLook: pictures, videos, office files, pdfs, etc.

Adding Triaged Data to the Collection

Once data of interest is located using the triage features it can be added to the **Additional Files** section of the **Collection** view. After highlighting the folders or files, **right-click** (**control-click**) and choose **Add Selected Items to Collection**. Navigate to the **Collection** view and see the items added to the collection from the **Browser** and **Search** views listed in **Additional Files**.

Logical Evidence (.L01) Collection Format

The option is now provided to stored collections in the .L01 logical evidence file format. Within the logical evidence file data is stored in the same structure as a collection saved to a folder. The **Files** folders contains subfolders for each data type collected (System Data, User Files, etc.). The **Logs** folder contains the comma-separated value log files. If there are collection errors the **Logs** folder will also be created outside the .L01 file in the folder where the .L01 file is stored. *Case_Details.log* is stored in the folder with the .L01 and inside the .L01.

Collection Log Files

Log files documenting a Collection have been simplified. The file *Case_Details.log* documents the start and stop time of the collection as well as any case data entered on the **Case** Details tab. A **Log** folder containing two comma-separated value log files is created in the collection container (folder, sparse image, or .L01). If there are collection errors they are stored in *errors.log*. All information about files and folders in the collection (including path, extension, hash values, etc.) is stored in *report.csv*.

Capturing RAM and data collections live on Catalina 10.15

Apple continues to restrict what an application can access while the Mac is running live. MacQuisition 2020 R1 has been updated to support Catalina 10.15; examiners can capture RAM and perform data collections while the Mac is running live.

COMPATABILITY

TYPE	EARLIEST COMPATIBLE SYSTEM*	MOST RECENT COMPATIBLE SYSTEM
IMAC	iMac (Late 2012) Model Identifiers: iMac13,1 / 13,2	iMac (2019) Model Identifiers: iMac19,1
IMAC PRO	iMac Pro (2017) Model Identifier: iMacPro1,1	iMac Pro (2017) Model Identifier: iMacPro1,1
MAC MINI	Mac mini (Late 2012) Model Identifier: MacMini6,1 / 6,2	Mac mini (2018) Model Identifiers: Macmini8,1
MAC PRO	Mac Pro (Late 2013) Model Identifier: MacPro6,1	Mac Pro (2019) Model Identifier: MacPro7,1
MACBOOK	MacBook (Early 2015) Model Identifier: MacBook8,1	MacBook (2017) Model Identifier: MacBook10,1
MACBOOK AIR	MacBook Air (Mid 2012) Model Identifier: MacBookAir5,1 / 5,2	MacBook Air (2019) Model Identifiers: MacBookAir8,2
MACBOOK PRO	MacBook Pro (Mid 2012) Model Identifier: MacBookPro9,1 / 9,2	MacBook Pro (2019) Model Identifiers: MacBookPro16,1

* Certain older 2007-2009 models that are not supported by the MacQuisition 2020R1 partition may be bootable by the MacQuisition Secondary partition. Having trouble identifying a Mac OS X system? We recommend the MacTracker App, available for free at the App Store.

LEGACY MACS

Trouble booting older Mac systems? Within each MacQuisition dongle, there is a legacy version of the software that can boot Intel-based Mac systems that predate the compatibility table above. For even older systems, including those running OS 9 (Classic), all MacQuisition customers have access to an ISO boot disk. ISO downloads are available within MacQuisition customers' individual account pages on BlackBag's website.

KNOWN LIMITATIONS

When using an 8GB MacQuisition dongle on some T2 systems, if the dongle is plugged in to a USB port on the system *after* reaching the Startup Disk selection screen, the system will boot to the OS on the internal drive not to 'MacQuisition 2020R1.' Either plug the MacQuisition dongle into a USB hub, or plug the MacQuisition dongle into a USB port on the system before powering it on.

At this time, MacQuisition only allows searching for non-English characters in the **Search** view when running on a live system in restricted mode.

RESOLVED ISSUES

MQ-2498	Able to image T2 system created with encrypted APFS partition then macOS install
MQ-2336	Correctly detect FileVault is off on T2 systems where FileVault was previously enabled
MQ-2323	Able to image T2 system with two APFS containers
MQ-2307	Unlocks APFS on system connected via TDM without supplying specific user
MQ-2303	AFF4 images created with MacQuisition can be ingested into other tools
MQ-2254	Can collect data from TDM connected system with same volume name
MQ-2231	Segment size recorded correctly for multiple images created in one session
MQ-1799	By default, MacQuisition prevents erasing internal disks and TDM connected devices

SUPPORT

If you need support, we are here to help.

Search our Knowledge Base articles for instant answers or Submit a Request at https://www.blackbagtech.com/support.html. When you submit your request for support, someone from our technical support will respond.
s