



MacQuisition™

QUICK START GUIDE

VERSION 2020 R1

INTRODUCTION

MacQuisition 2020 R1 is officially supported on macOS 10.11 (El Capitan), 10.12 (Sierra), 10.13 (High Sierra), 10.14 (Mojave), and 10.15 (Catalina) systems, although 10.10 (Yosemite) and lower may potentially work. MacQuisition also boots into a forensically sound environment directly from the dongle.

This QuickStart guide provides a brief explanation to get the examiner started. See the *MacQuisition User Guide* located on the 'Application' partition for more detailed information.

Welcome to the MacQuisition Quick Start Guide

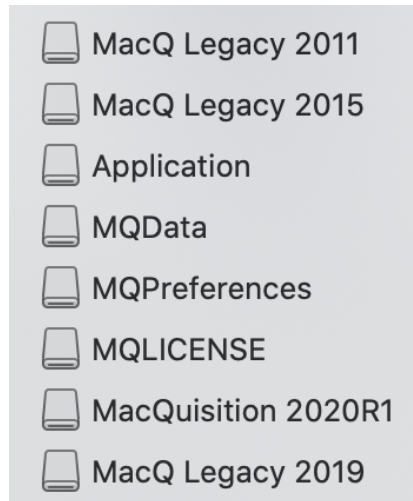
MacQuisition™ is designed for triaging and imaging Mac computers. MacQuisition can be used to image Mac computers, including those with T2 chips, and also to collect data from live running Mac computers. This Quick Start guide will walk through live data collection with MacQuisition, booting a target system with MacQuisition for imaging, and running MacQuisition from an analysis Mac to acquire the target system via Target Disk Mode. Other factors that have to be considered when determining your approach, such as firmware passwords, FileVault2, T2 security chips, the file system used, and fusion drives will also be explored.

The MacQuisition Device

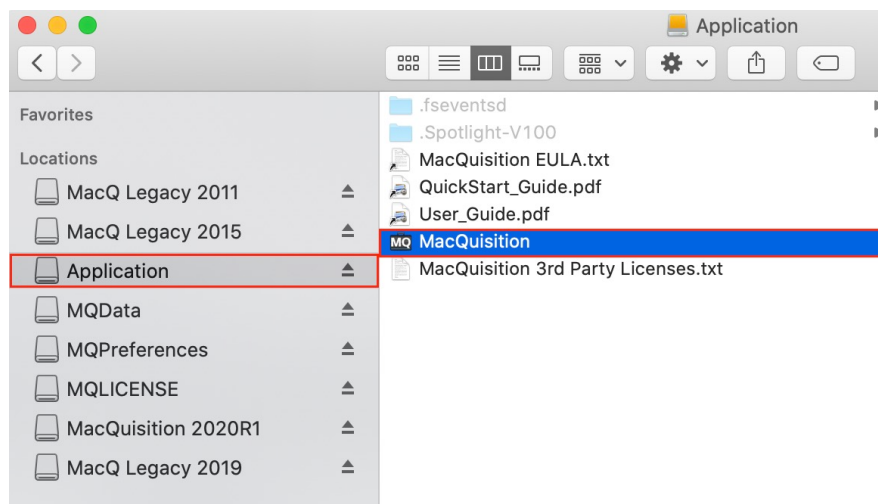
MacQuisition devices are setup up with multiple boot partitions, an application partition, a preferences partition, a license partition, and a data partition. The size of the data partition varies, depending on which MacQuisition device is purchased. Currently, there are two device sizes to choose, 1 TB or 120 GB. The devices connect via USB or USB-C cables shipped with the device.



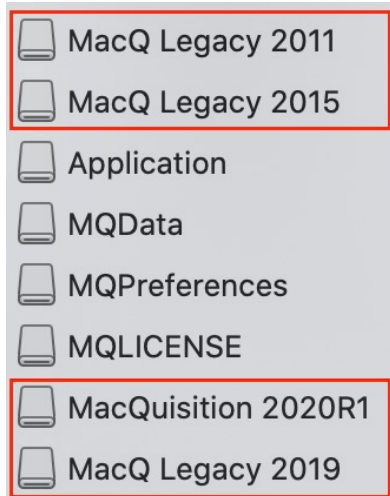
In Finder, the following partitions will appear when MacQuisition is connected:



The Application partition contains the MacQuisition application, used to collect data from live systems and when running MacQuisition from an analysis Mac to acquire a target system. The application partition also contains a link to the MacQuisition User Guide.



Multiple boot partitions are included, providing support for a variety of Macintosh hardware. The boot partitions are used to boot a target system for imaging. The most recent boot code will reside on the partition named with the MacQuisition version number.



The remaining partitions serve the following purposes:

- MQData: a storage partition that can be used as a destination drive during data collections
- MQPreferences: contains MacQuisition settings preferences
- MQLICENSE: stores the MacQuisition license



What Do I Need to Consider?

Before an acquisition occurs, there are some things you need to consider.

Triage

Before collecting data or an image of a device, MacQuisition can be used to triage the device to determine if data of relevance exists on the machine. Features now built in to MacQuisition allow you to Browse and Search the file system, previewing files encountered. File previews work on file types supported by macOS QuickLook: pictures, videos, office files, pdfs, etc.

Note: Triage on a Live system will result in changes to the system. For more information refer to Appendix B of the MacQuisition User's Guide.

Live Acquisition

When a computer is up and running, MacQuisition can be used to collect live data. There are circumstances where gathering data from the running system is imperative. The increasing use of FileVault2 encryption requires immediate acquisition of the logical data available. Once the system is shutdown, if a user login password or Recovery Key are not available the data will no longer be accessible.

Note: Live Acquisition will result in changes to the system. For more information refer to Appendix B of the MacQuisition User's Guide.

Cold Box

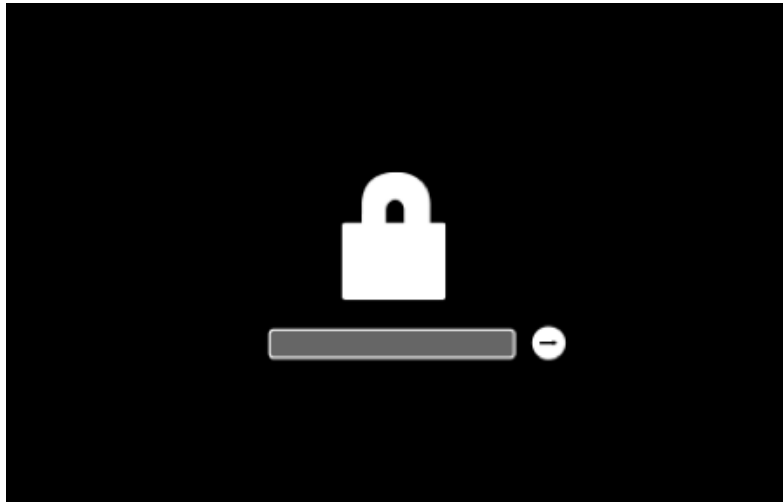
If the system is not running, there are two ways to use MacQuisition. The first is to boot the target system directly using MacQuisition. The second is to boot an analysis machine with MacQuisition and connect to the target via Target Disk Mode (TDM). Determining which method to use depends on several variables.

Firmware Password

A Firmware password on a Mac prevents starting up from any internal or external storage device other than the selected startup disk. This includes booting to the Recovery partition, Target Disk Mode, and MacQuisition. To determine if a

firmware password is set on a target system, press and hold the **Option** key immediately after turning on or restarting the Mac.

If no Firmware password is set, the bootable volumes on the device will be seen. At a minimum this includes the volume containing macOS. When a Firmware password is set, the following screen will appear:



If the Firmware password is not known, the system cannot be booted into Target Disk Mode nor can MacQuisition be used to boot the system. **No imaging can occur without this password.**

Model

Mac with T2 chips have additional startup security features embedded in the T2 chip. Determine if the Mac is a model with a T2 security chip. The serial or model number can be used.

One of the functions of the T2 chip is to restrict boot process preventing the computer from booting to external devices, including MacQuisition. This setting can be changed in the **Startup Security Utility**, accessible in the Recovery partition. To boot the Recovery partition, press **Command (⌘) - R** while booting.

Note: An admin password is needed to access the **Startup Security Utility**. For additional information refer to <https://support.apple.com/en-us/HT208198>.



BlackBag®

300 Piercy Road • San Jose, CA 95138 • 408.844.8890 • <https://www.blackbagtech.com>

If the Secure Boot settings have not been changed and the admin password is not known, the system cannot be booted directly using MacQuisition.

Recommendation

When a Mac with a T2 chip is encountered, boot the system to Target Disk Mode (TDM) and attach it to an Analysis system booted to MacQuisition for imaging. A physical image can be obtained without modifying the SecureBoot settings.

Ports, Cables, and Write Blockers

When connecting a target system to an analysis machine for imaging, ports, cables and write blockers all must be considered.

Target Disk Mode (TDM) is a Mac feature designed essentially to turn the computer into an external hard drive. The initial use for this feature was file transfer. Consequently, when a computer is in TDM it will be written to when connected to another system. Thus, the need for write blocking.

The ports and cables needed to connect a target system to an analysis system depends on the Mac models. The TDM interface allows connection via FireWire for older Macs. Newer Macs allow access via Thunderbolt and USB. Apple has exhaustive information on TDM at <https://support.apple.com/en-us/HT201462>.

After determining which ports to use on both systems, the proper cables and any necessary adapters must be obtained. Keep in mind that all cables and adapters are not created equally. Genuine Apple cables and adapters tend to work better.

If a source device has only one USB port, an examiner may use a (preferably powered) USB hub. If the source device only has USB-C port(s), a USB-C to USB-A type adapter will be needed.

Hardware write blockers add a layer of complexity. The hardware write blocker must be considered when determining the cables and adapters required. If there are difficulties, the hardware write blocker, connections to and from the write blocker, present additional items for trouble shooting.

The other option is to install a software write blocker on the analysis Mac. BlackBag's SoftBlock™ is a software-based forensic write blocking tool. When installed on the analysis system, the user can choose to mount newly attached hardware devices with read-only or read-write permissions. SoftBlock is a viable alternative when hardware write blocking tools are unavailable or the require cables to connect through the write blocker are unavailable.

Keep in Mind...

An analysis system can be booted to MacQuisition to create a forensically sound environment for connecting and imaging other devices. Devices connected to a system booted with MacQuisition will be write-blocked automatically.



LAUNCHING MACQUISITION

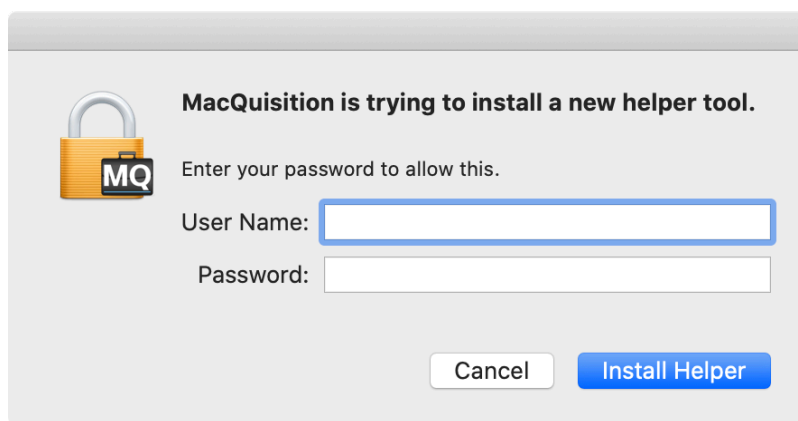
For live acquisition of a target, or to use MacQuisition for acquisition from an analysis system, plug the MacQuisition dongle into the Mac. The partitions previously listed in *The MacQuisition Device* section of this guide will appear on the system.

Keep in Mind...

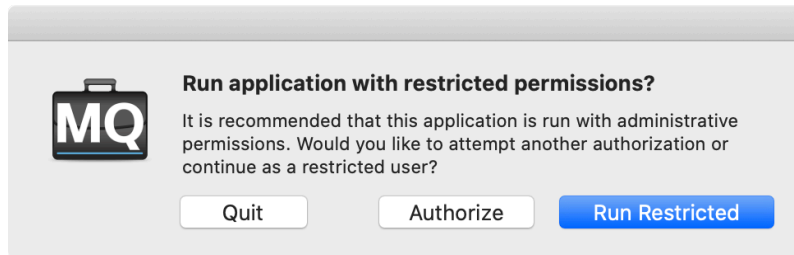
Running MacQuisition on a live computer will make changes to the computer. Artifacts will be changed when running MacQuisition live. In some cases, this may be the only way to get data from the target Mac.

Note: For more information about possible changes refer to Appendix B of the MacQuisition User's Guide.

Navigate to the *Application* volume and click on the *MacQuisition* application. The following window appears:



An admin password is needed. If the password is known, enter it, otherwise click **Cancel**. If you click cancel the following prompt will appear:



Clicking **Quit**, closes MacQuisition. **Authorize** takes you back to the previous prompt. **Run Restricted** allows MacQuisition to start with restricted user permissions.

Recommendation

Launch MacQuisition from an administrator account when possible so the software runs with admin-level permission. Once an administrator password is successfully entered, MacQuisition runs with root privileges.

Once **Continue** is clicked, the user will see the main display for MacQuisition. Relevant case information can be entered, and the time zone settings can be set for logs and reporting.



MacQuisition™

Case Details

Browser Search Collection Image Tools

Case Identification

Case Name:

Case Number/ID:

Location:

Exhibit ID/Evidence #:

Description:

Examiner Information

Examiner:

Agency/Company:

Section/Department:

Comments

Display Time Zone

For display, logs and reporting use:

America/New_York

Current machine time:

2020-02-07 13:49:24 (EST)

TRIAGING

Browser and **Search** tabs provides the ability to navigate through the file system and search for data before any data collection or imaging is performed. Triaging a device can help determine whether data needs to be collected from the device and whether the device needs imaged.

WARNING

*Using the Triage features (**Browser** and **Search**) in Live mode (on a running computer), will change data on the system.*

Note: For more information about possible changes refer to Appendix B of the MacQuisition User's Guide.

The **Browser** and **Search** tabs operate then MacQuisition running on a Live system and when a system is booted with MacQuisition or connected via TDM to a system boot with MacQuisition. The major differences are on a Live system data will be changed on the system, on a Live system data protected by FileVault 2 is still accessible without providing a user login password or the FileVault 2 recovery key.

Triaging After Shutdown

*The Triage features (**Browser** and **Search**) work when a system is booted with MacQuisition. If the system has FileVault 2 activated, a user login password or the Recovery Key are required to access the data.*

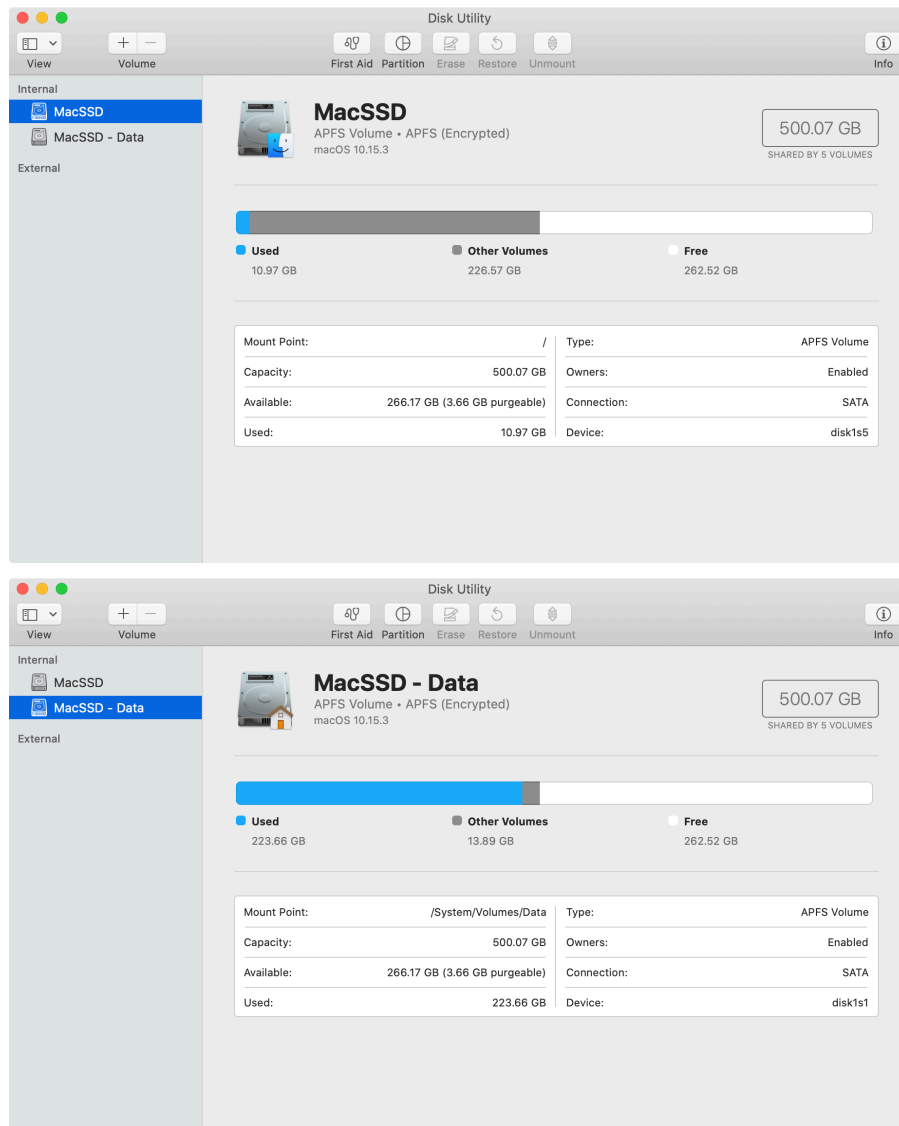
Note: When using **Browser** or **Search** on a system booted with MacQuisition or connected via TDM to an analysis system booted with MacQuisition, FileVault2 encrypted volumes must be unlocked before they can be triaged. A dialog box will appear indicating: **Full Disk Encryption Detected. To unlock an encrypted disk, go to the 'Tools → Mount Device' view.** On Live systems, FileVault 2 will already be unlocked.



A Note About macOS 10.15 (Catalina)

When Apple® release macOS 10.15 (Catalina), increased system protection was added to macOS. macOS Catalina runs in a read-only system volume, separate from other files. When a system is upgraded to Catalina, a second volume is created, and some files may move to a Relocated Items folder.

The boot volume was split into two pieces. On the Desktop it appears as one volume, but looking at it via Disk Utility, it is readily apparent there are two volumes:

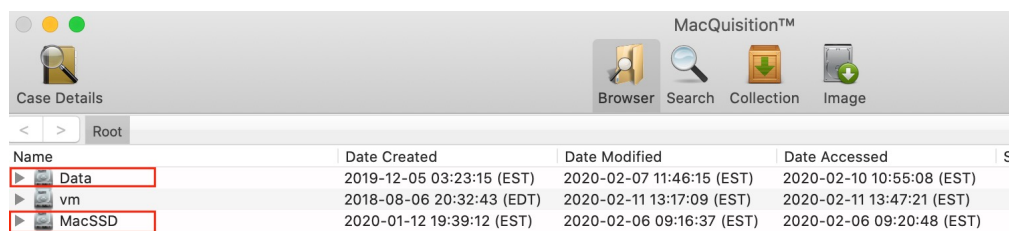


The volume name that appears on the Desktop appears in both volumes, the second volume has ' - Data' appended to the volume name. To read more about this is refer to <https://support.apple.com/en-us/HT210650>.

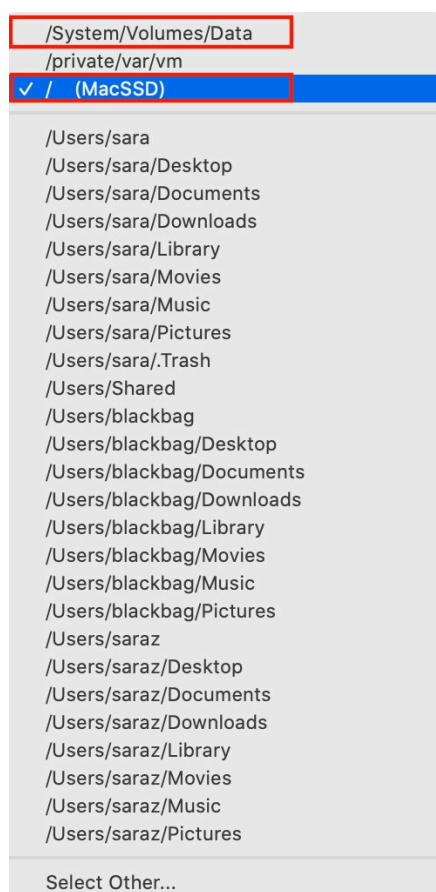
If FileVault 2 is enabled, the same credentials will unlock both volumes in MacQuisition.

Different views in MacQuisition will display these volumes differently:

- **Browser:** Both volumes appear. The system volume appears with the volume name, the second volume appears as **Data**.



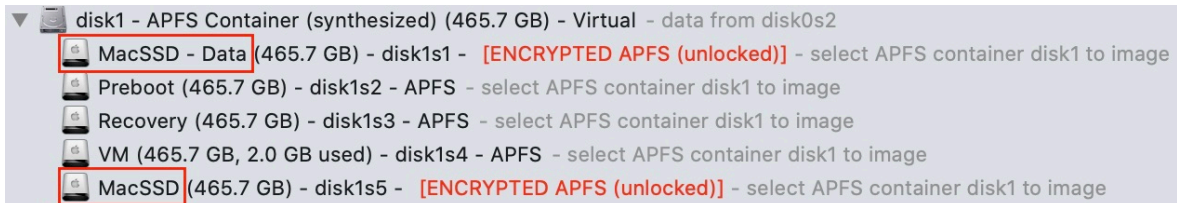
- **Search:** Both volumes appear in the Location drop-down menu. The system volume appears as / (**VolumeName**), the second volume appears as /System/Volumes/Data



- **Collection:** Both volumes appear in the 'System Files → OS X Volumes' area. The system volume appears with the volume name, the second volume appears as **Data**.

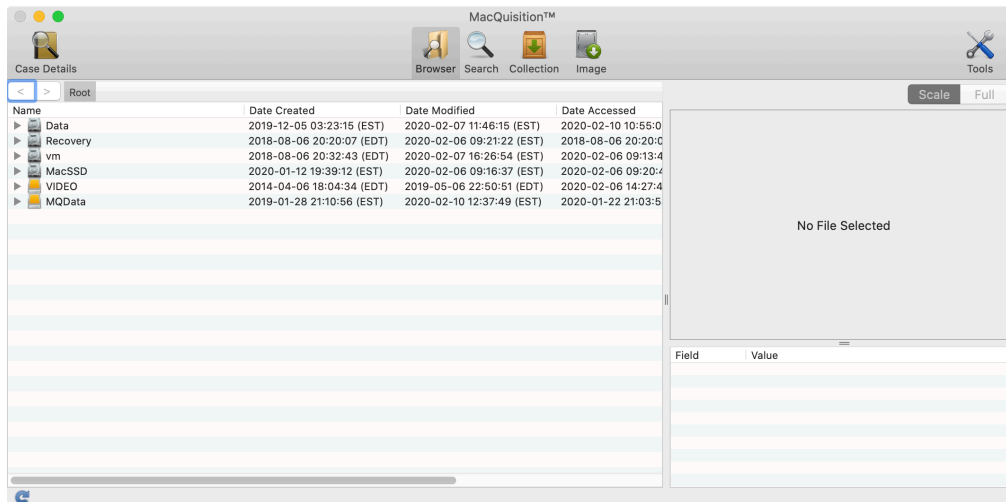


- **Image:** Both volumes appear as two separate slices. The names shown in Disk Utility correspond to the names seen in **Image**.

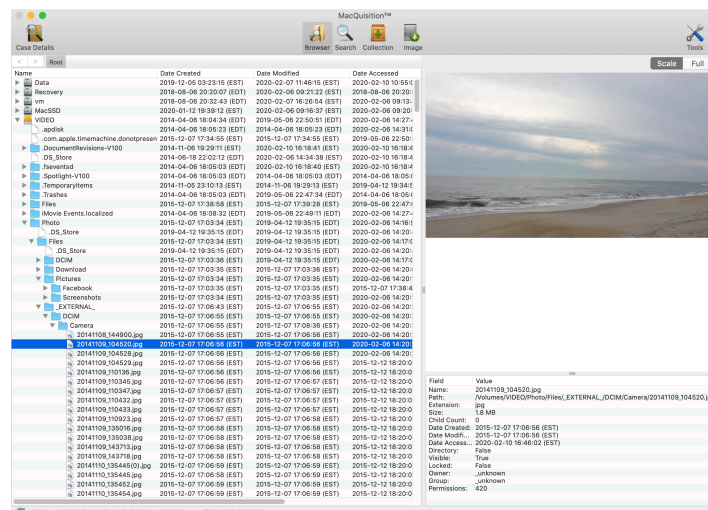


Browser

The 'Browser' window allows navigation through the file systems of the devices connected. Click on the **Browser** button to see the volumes connected.



Navigate through the directory structure of connected devices. Previews of the file selected on the left side of the 'Browser' window will appear on the right side along with file metadata.



File previews work on file types supported by macOS QuickLook: pictures, videos, office files, pdfs, etc.



BlackBag®

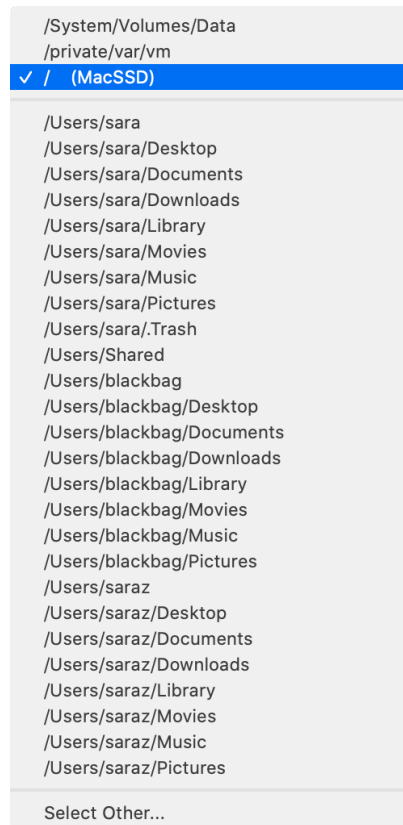
300 Piercy Road • San Jose, CA 95138 • 408.844.8890 • <https://www.blackbagtech.com>

Search

The 'Search' window allows searches for data based one or more of the following criteria:

- Location - Volume or specific path
- Name - Filename using the operators *contains*, *does not contain*, or *exact match*.
- Extension - File extension using the operators *is* or *is not*.
- File Size - File size using the operators *greater than*, *less than*, or *between*.
- Date - Date Created, Date Modified, or Date Accessed using the operators *is between*, *is before*, *is after*, or *is exactly*.
- Content - Content contained within either binary files or documents.

Location provides a drop-down menu that automatically lists the following:



From the drop-down list, choose one of the locations listed, or select the **Select Other...** option. By default, the location is / (*VolumeName*).

Searching for files by name, the options are:

- ✓ any file name
- contains
- does not contain
- exact match

Searching for files by extension, the options are:

- ✓ any extension
- is
- is not

Searching for files by file size, the options are:

- ✓ any size
- greater than
- less than
- between

Once greater than, less than, or between is chosen, file sizes can be specified by KB, MB, or GB.

Searching for files by data, the options are:

- ✓ any date
- date created
- date modified
- date accessed

- ✓ is between
- is before
- is after
- is exactly

Once the desired date type and range are selected, specifies the dates of interest. Dates can be typed in, changed using the arrows, or selected via the calendar.

Note: When searching by file extension, multiple extensions can be searched for at the same time. Separate each file extension by a colon. For example:

jpg:gif:png



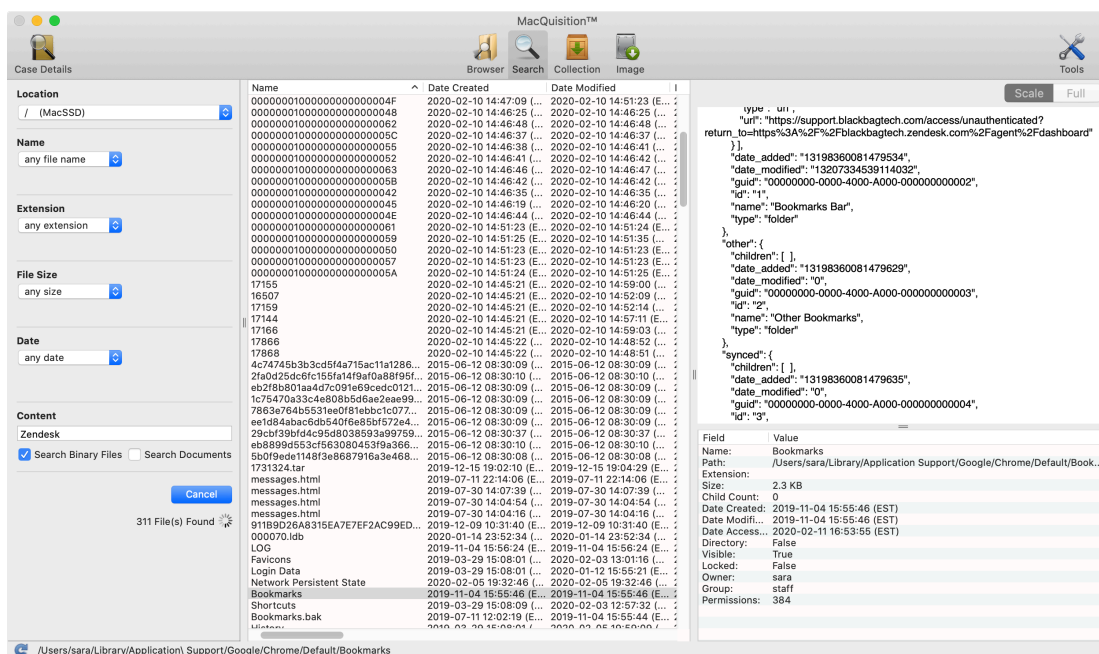
Searches can be conducted for files containing specific data. A search can be conducted for data within binary files, documents, or both. Type the content to search for and check either **Search Binary Files**, **Search Documents**, or check them both.

Content

☐ Search Binary Files ☒ Search Documents

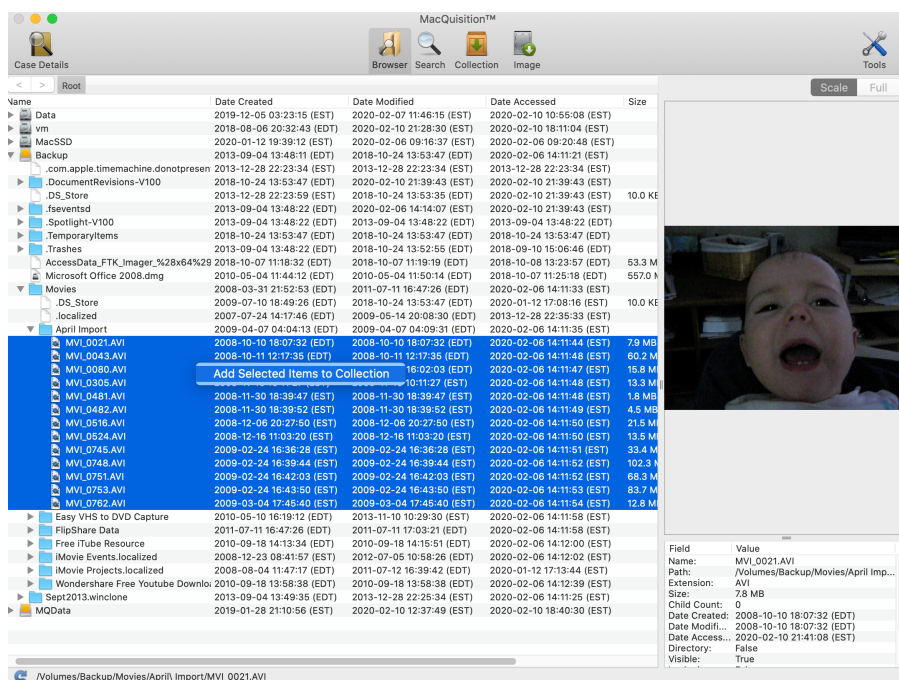
Multiple search criteria can be combined to create a more complex search, filtering data down to items that are relevant to the investigation. Searches can also be used to determine if a device contains information of interest. If no items are returned from searches for data of interest, further processing of the device may not be necessary.

Once a search completes, the items returned are listed in the middle portion of the 'Search' window. Items highlighted in the middle portion of the 'Search' window, a preview and file metadata is shown on the right side of the 'Search' window.

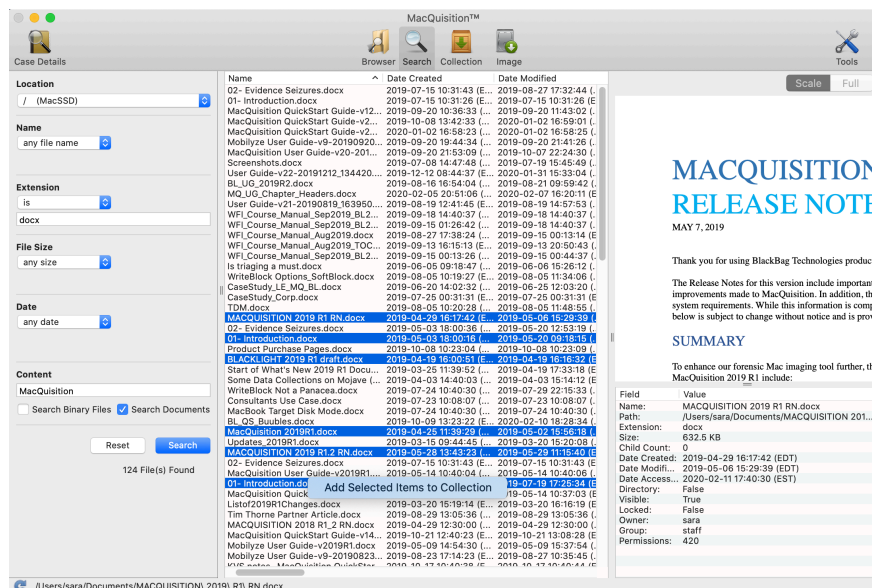


Adding Files to the Collection

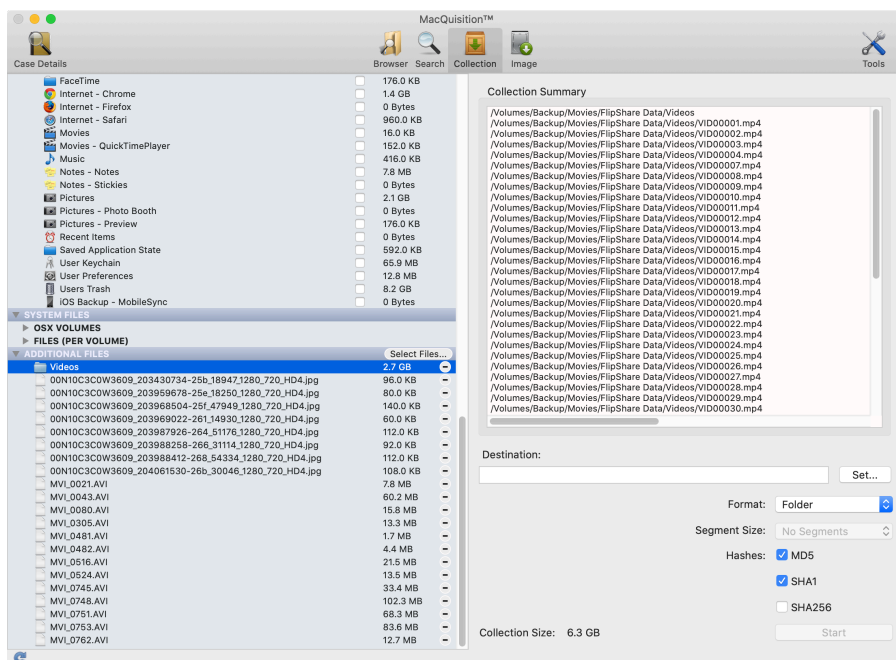
In addition to browsing and searching through the volumes and previewing files, files and folders can be added to **Additional Files** section in the 'Collection' window from **Browser** and **Search**. Browsing and searching through the files and folders, data may be located for collection. Files can be added to the collection one at a time, multiple files can be selected for addition, or folders can be added. To select multiple files or folders listed sequentially, select the first file, hold down the shift key, click the last item. **Right-click (control-click)** on any selected file and select **[Add Selected Items to Collection]**.



To select multiple files or folders that are not listed sequentially, hold down the command key and click on the desired files. Right-click (control-click) on any selected file and select [Add Selected Items to Collection].

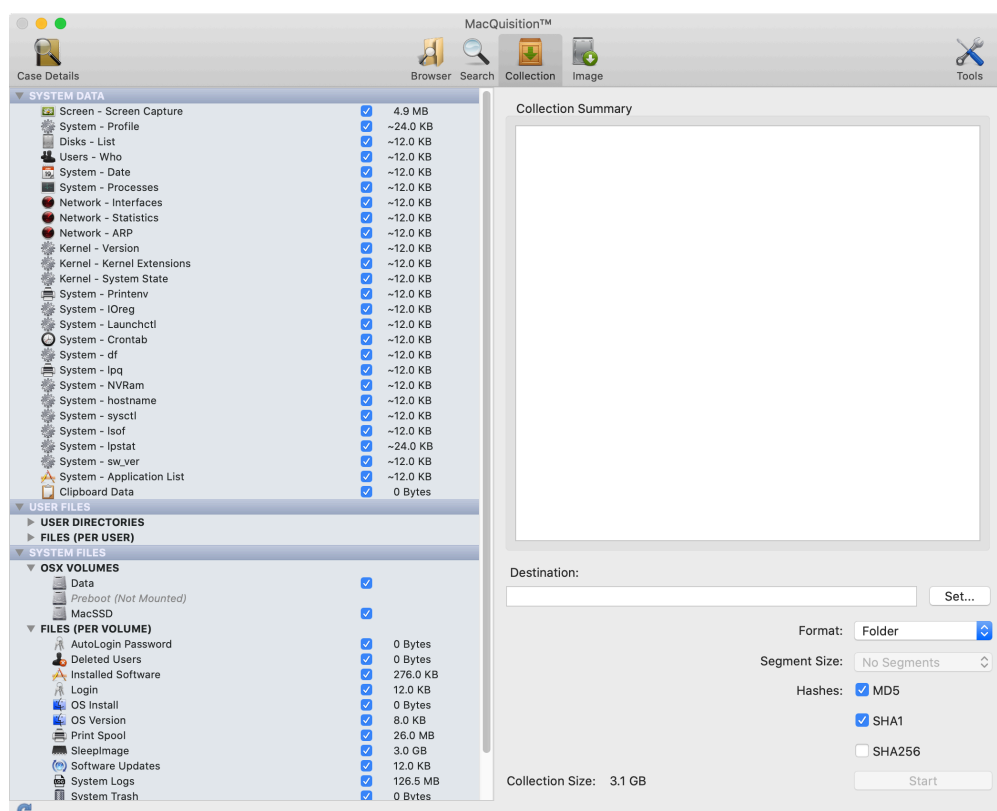


Files added to the collection appear in the 'Collection' window in the **Additional Files** section. For folders added, the contents of the folder will be listed in the **Collection Summary** when folder is highlighted in the 'Collection' listing.



LIVE DATA COLLECTION

Once MacQuisition is launched on a target system, data can be collected from the live system via the **Collection** tab. The data collected can be sent to the **MQData** partition on the MacQuisition dongle or a separate destination collection device. Click on the **Collection** tab.



This tab shows locations pre-defined in MacQuisition available for collection. It is organized by the following categories:

- **System Data:** data related to the system including network and macOS information
- **User Files:** allows collection of data from specific user profiles on the system
- **System Files:** files from selected volumes including Deleted Users, OS Version, and sleepimage
- **Additional Files:** an area to specify other files for collection



BlackBag®

300 Piercy Road • San Jose, CA 95138 • 408.844.8890 • <https://www.blackbagtech.com>

As information is selected for collection, the approximate size of the collection is calculated and displayed.

Destination: Set...

Format: Folder

Segment Size: No Segments

Hashes: ☒ MD5
☒ SHA1
☐ SHA256

Collection Size: 53.0 GB

Start

The information that will be collected by MacQuisition is displayed in the **Collection Summary**. Highlight an item listed for collection, and review the information displayed in **Collection Summary**. Highlighting an item listed for collection provides one of the following:

- A preview of the data that will be collected. This is common for items listed under **System Data**.

MacQuisition™

Case Details

Browser Search Collection Image Tools

SYSTEM DATA

- Screen - Screen Capture 4.9 MB
- System - Profile ~24.0 KB
- Disks - List 4.0 KB**
- Users - Who 4.0 KB
- System - Date 4.0 KB
- System - Processes 96.0 KB
- Network - Interfaces 4.0 KB
- Network - Statistics 48.0 KB
- Network - ARP 4.0 KB
- Kernel - Version 4.0 KB
- Kernel - Kernel Extensions 24.0 KB
- Kernel - System State 48.0 KB
- System - Printenv 4.0 KB
- System - IOREG 1.3 MB
- System - Launchctl 12.0 KB
- System - CronTab 4.0 KB
- System - df 4.0 KB
- System - lprq 4.0 KB
- System - NVRam 12.0 KB
- System - hostname 4.0 KB
- System - sysctl 44.0 KB
- System - lsof 64.0 KB
- System - lprstat 20.0 KB
- System - sw_ver 4.0 KB
- System - Application List 4.0 KB
- Clipboard Data 0 Bytes

USER FILES

SYSTEM FILES

OSX VOLUMES

- Data
- Preboot (Not Mounted)
- MacSSD

FILES (PER VOLUME)

- AutoLogin Password 0 Bytes
- Deleted Users 0 Bytes
- Installed Software 92.0 KB
- Login 4.0 KB
- OS Install 0 Bytes

Collection Summary

/dev/disk0 (internal, physical):

#:	TYPE NAME	SIZE	IDENT
0:	GUID_partition_scheme	+500.3 GB	disk0
1:	EFI EFI	209.7 MB	disk0
2:	Apple_APFS Container disk1	500.1 GB	disk0

/dev/disk1 (synthesized):

#:	TYPE NAME	SIZE	IDENT
0:	APFS Container Scheme - Physical Store disk0s2	+500.1 GB	disk1
1:	APFS Volume MacSSD - Data	213.1 GB	disk1
2:	APFS Volume Preboot	85.1 MB	disk1
3:	APFS Volume Recovery	523.5 MB	disk1
4:	APFS Volume VM	3.2 GB	disk1
5:	APFS Volume MacSSD	11.0 GB	disk1

/dev/disk2 (external, physical):

#:	TYPE NAME	SIZE	IDENT
0:	GUID_partition_scheme	+1.0 TB	disk2
1:	EFI EFI	209.7 MB	disk2
2:	Apple_HFS MacQuisition 2020R1	2.1 GB	disk2
3:	Apple_HFS MacQ Legacy 2019	2.0 GB	disk2
4:	Apple_HFS MacQ Legacy 2015	1.3 GB	disk2
5:	Apple_HFS MacQ Legacy 2011	926.9 MB	disk2

Destination: Set...

Format: Folder

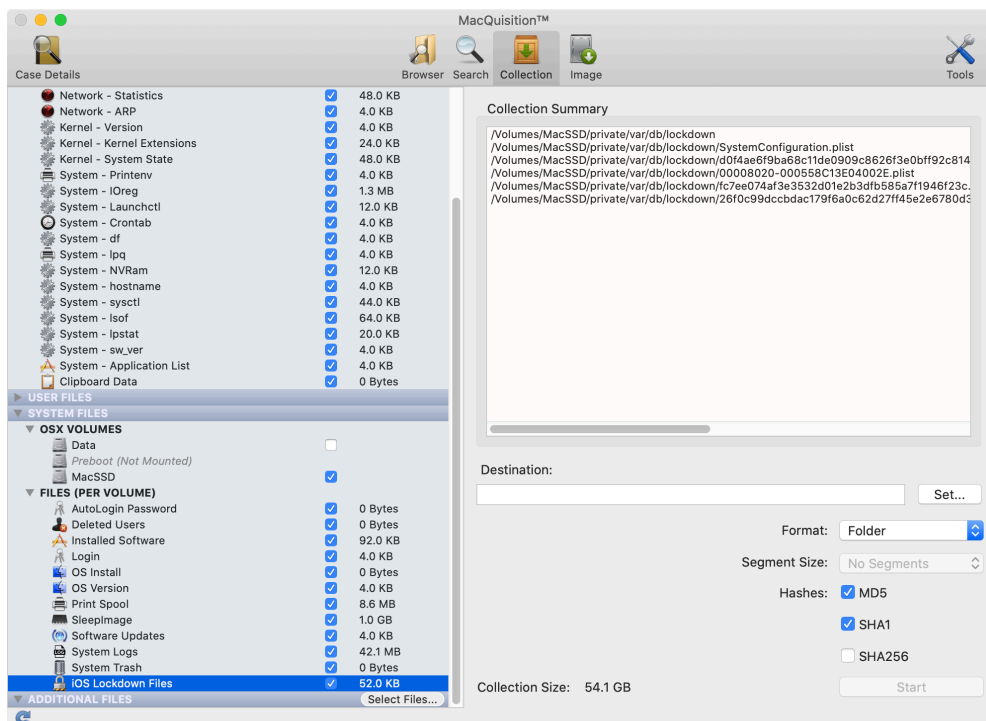
Segment Size: No Segments

Hashes: ☒ MD5
☒ SHA1
☐ SHA256

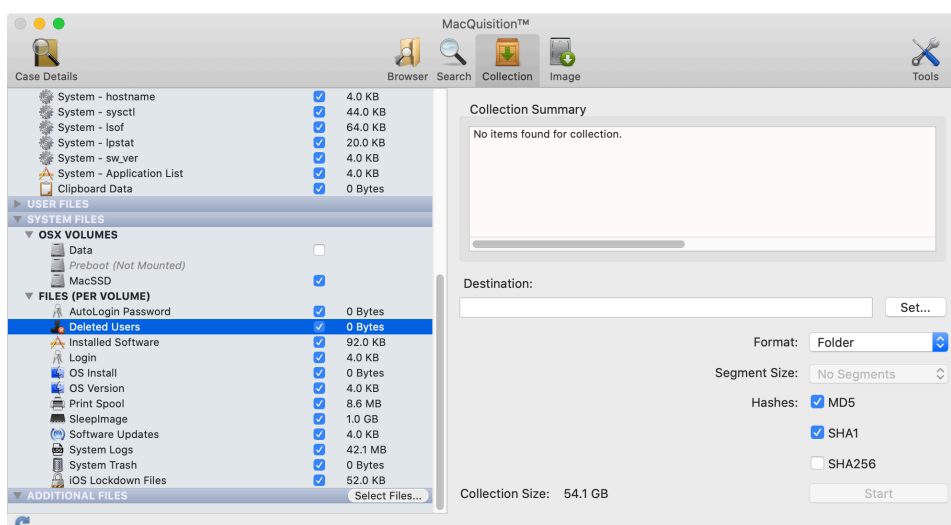
Collection Size: 53.0 GB

Start

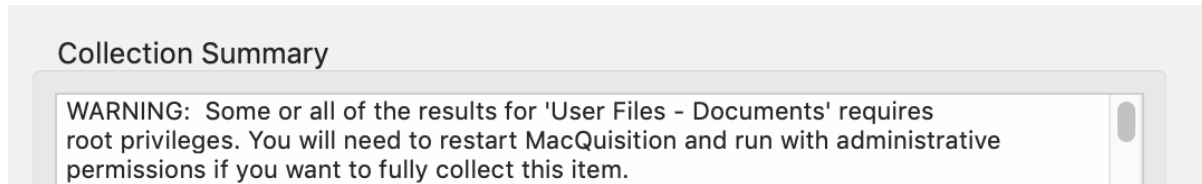
- A listing of the files that will be collected. This is common for both **User Files** and **System Files**.



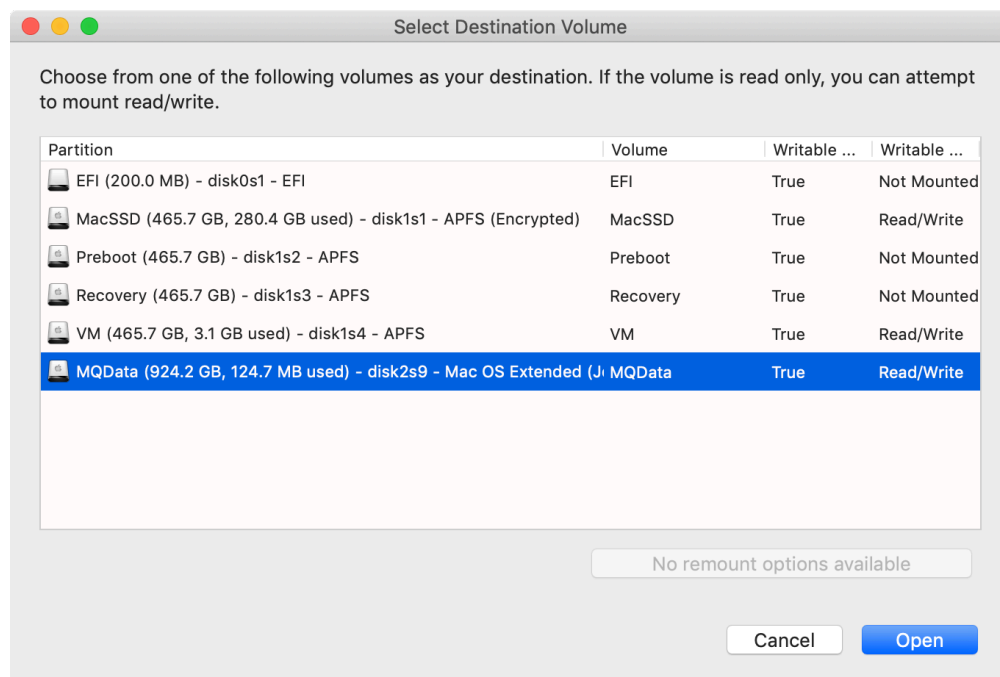
- A message indicating there are no items to collect for that data.



Note: When running in restricted mode, a warning will appear in the **Collection Summary** box if admin permissions are required to collect the data selected.

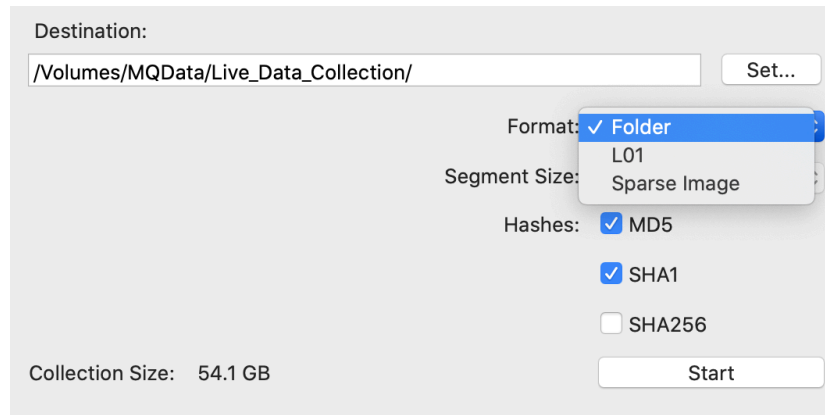


After all items for the collection are selected, a destination, hash types, and format of the collection all must be specified. Click **Set...** to choose the destination for the collection. The **Select Destination Volume** window appears.



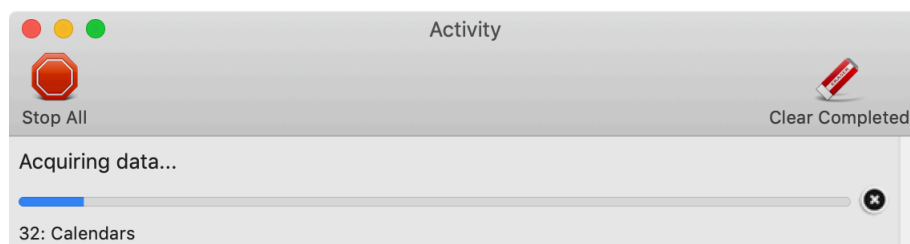
All of the Volumes with storage space currently attached to device are listed. In the example shown, EFI, MacSSD, Preboot, Recovery, and VM are all volumes on the internal hard drive. MQData is the data partition on the MacQuisition dongle. You can see in the window which drives are writeable, which drives are mounted and if they are mounted Read Only or Read/Write. Any external media connected will also be displayed and available to select as the collection destination. Select the destination volume, then click **Open**. A folder can be created on the destination volume for the collection.

Once the Destination volume has been selected, set the other collection options. By default, MD51 and SHA1 are both selected. SHA256 is also a hash type option. Check or uncheck the boxes to select or deselect the corresponding hash type. The collection can be stored in a folder or a sparse image. The drop-down menu can be used to change from Folder to either L01 or Sparse Image.

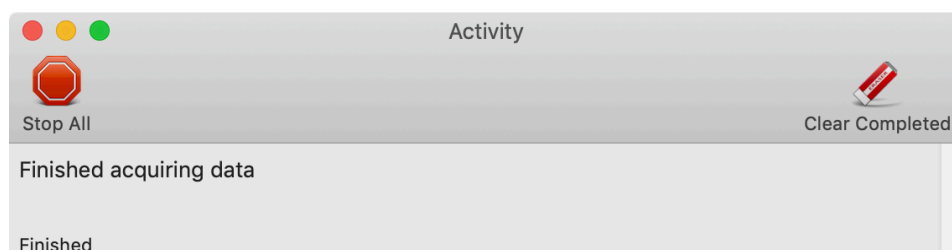


Once all collection preferences are set, click **Start**.

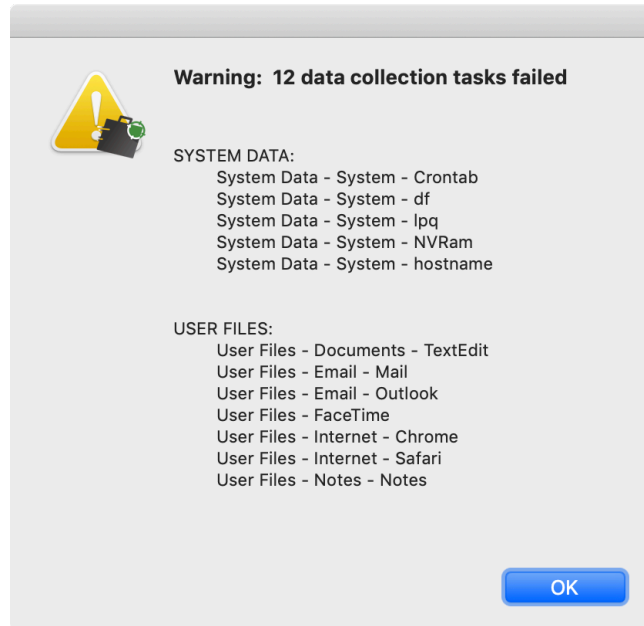
Once the collection begins the **Activity** window will appear showing the status of the collection. MacQuisition immediately begins acquiring data.



When the collection finishes, if all items specified for collection were copied, the **Activity** window displays the following message:



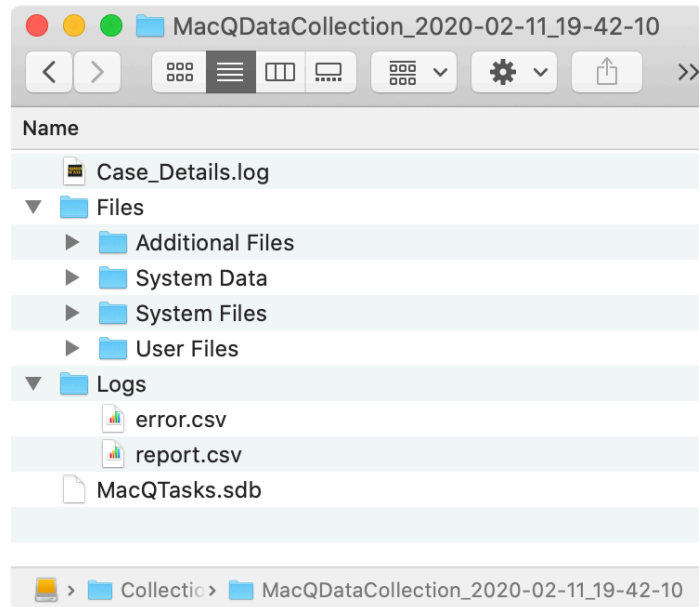
If problems were encountered, a pop-up window appears listing the tasks that failed by collection category.



Once **OK** is clicked, the following message appears in the **Activity** window.



Navigating to the collection destination the following folder structure can be seen.



Files collected are organized in the *Files* folder by collection category (Additional Data, System Data, System Files, and User Files) and by volume name. Folder structure from the system is maintained for Additional, System, and User Files.. *Logs* contains files documenting information about the files collected and the MD5 values.



BlackBag®

300 Piercy Road • San Jose, CA 95138 • 408.844.8890 • <https://www.blackbagtech.com>

report.csv		Open with Numbers	
Name	Path		
Volumes	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes		
MacSSD	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD		
Users	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users		
sara	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users/sara		
Library	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users/sara/Library		
Application Support	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users/sara/Library/Application\ Support		
AddressBook	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users/sara/Library/Application\ Support/AddressBook		
Metadata	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users/sara/Library/Application\ Support/AddressBook/Metadata		
.info	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users/sara/Library/Application\ Support/AddressBook/Metadata		
FA5EEA6C-E36F-47F3-8E80-3DD6FD2AD70/ABInfo.abcdi	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users/sara/Library/Application\ Support/AddressBook/Metadata		
Sources	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users/sara/Library/Application\ Support/AddressBook/Sources		
715F5C13-0CDF-41C4-BBE5-8BAFD8BDF23D	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users/sara/Library/Application\ Support/AddressBook/Sources/		
Metadata	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users/sara/Library/Application\ Support/AddressBook/Sources/		
.info	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users/sara/Library/Application\ Support/AddressBook/Sources/		
SyncOperations.plist.lockfile	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users/sara/Library/Application\ Support/AddressBook/Sources/		
.AddressBook-v22_SUPPORT	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users/sara/Library/Application\ Support/AddressBook/Sources/		
_EXTERNAL_DATA	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users/sara/Library/Application\ Support/AddressBook/Sources/		
AddressBook-v22.abcdadb-wal	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users/sara/Library/Application\ Support/AddressBook/Sources/		
AddressBook-v22.abcdadb-shm	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users/sara/Library/Application\ Support/AddressBook/Sources/		
AddressBook-v22.abcdadb	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users/sara/Library/Application\ Support/AddressBook/Sources/		
Images	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users/sara/Library/Application\ Support/AddressBook/Sources/		
78E57FCB-984C-4F35-8721-B464CA888BEF	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users/sara/Library/Application\ Support/AddressBook/Sources/		
.AddressBook-v22_SUPPORT	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users/sara/Library/Application\ Support/AddressBook/.Address		
_EXTERNAL_DATA	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users/sara/Library/Application\ Support/AddressBook/.Address		
AddressBook-v22.abcdadb-wal	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users/sara/Library/Application\ Support/AddressBook/AddressE		
ABAssistantChangelog.acicadb-wal	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users/sara/Library/Application\ Support/AddressBook/ABAssist		
ABAssistantChangelog.acicadb-shm	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users/sara/Library/Application\ Support/AddressBook/ABAssist		
AddressBook-v22.abcdadb-shm	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users/sara/Library/Application\ Support/AddressBook/AddressE		
ABAssistantChangelog.acicadb	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users/sara/Library/Application\ Support/AddressBook/ABAssist		
AddressBook-v22.abcdadb	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users/sara/Library/Application\ Support/AddressBook/AddressE		
Images	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users/sara/Library/Application\ Support/AddressBook/Images		
Migration 20200112201300-502.abbu.tbz	/Volumes/MQData/Collection/MacQDataCollection_2020\02\11_19\42\10/Files/User\ Files/Volumes/MacSSD/Users/sara/Library/Application\ Support/AddressBook/Migration		

USING MACQUISITION TO BOOT A SYSTEM

There are several reasons to boot a system with the MacQuisition dongle and what you can accomplish depends on whether you boot the target system with MacQuisition, or you boot an analysis system. When booting a target system with MacQuisition, you can use MacQuisition to image the target system, collect RAM, or carry out a logical data collection. Booting an analysis system with MacQuisition creates a forensically sound environment for imaging devices attached including other Macs in Target Disk Mode. An analysis system booted with MacQuisition provides a forensically sound environment for imaging attached devices. Devices attached to a system booted with MacQuisition are attached as read-only so write-blockers are not needed.

A Mac that is powered off can be booted from the MacQuisition dongle. MacQuisition can then be used to image the Mac to an external collection device. MacQuisition boots to a forensically sound environment, all devices are accessed by default as read-only. No write blocking hardware or software is required.

The Collection Device:

- *A collection device can be formatted with ANY Apple file system (APFS, HFS+, etc.).*
- *Using a collection device formatted with exFAT is NOT recommended.*
- *A collection device CAN be formatted with NTFS.*
- *On a collection device formatted with FAT32 the largest supported acquisition segment size is 3.9 GB.*



How to Start...

Before beginning...

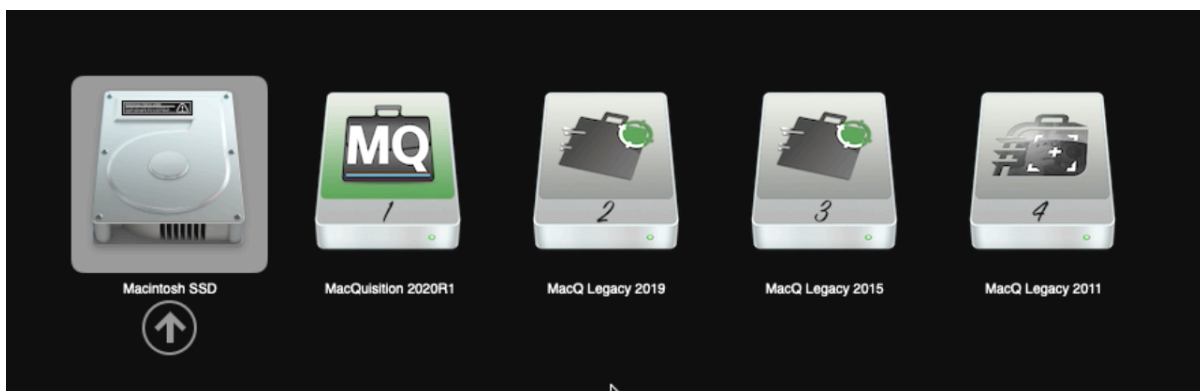
- *Check the model – if it has a T2 chip consider TDM*
- *Do not use a wireless keyboard – keystrokes on wireless keyboard may not be transmitted in time*

Boot Process

How to Boot:

1. *Insert the MacQuisition dongle into the USB port.*
2. *Attach the collection device for storing the image.*
3. *Press the power button and immediately hold down the **Option** key.*

A screen similar to the following appears:



Any internal volume on the device are listed with the bootable partitions on the MacQuisition dongle.

Note: If Bootcamp is installed, the Bootcamp partition is also displayed here.

Reminder

If a firmware password is enabled a lock icon will appear. The firmware password must be entered. If the firmware password is unknown or entered incorrectly the MacQuisition boot process will fail.

Select the appropriate version of MacQuisition to run based on the source Mac architecture.

The 'MacQuisition 2020R1' boot partition boots most newer Apple hardware. If this fails, attempt to boot from other MacQuisition boot partition in numerical order (1, 2, 3, then 4).

An arrow appears below the icon of the selected partition. Click the arrow to begin the boot process. The BlackBag logo appears and shortly after a progress bar.



BlackBag®

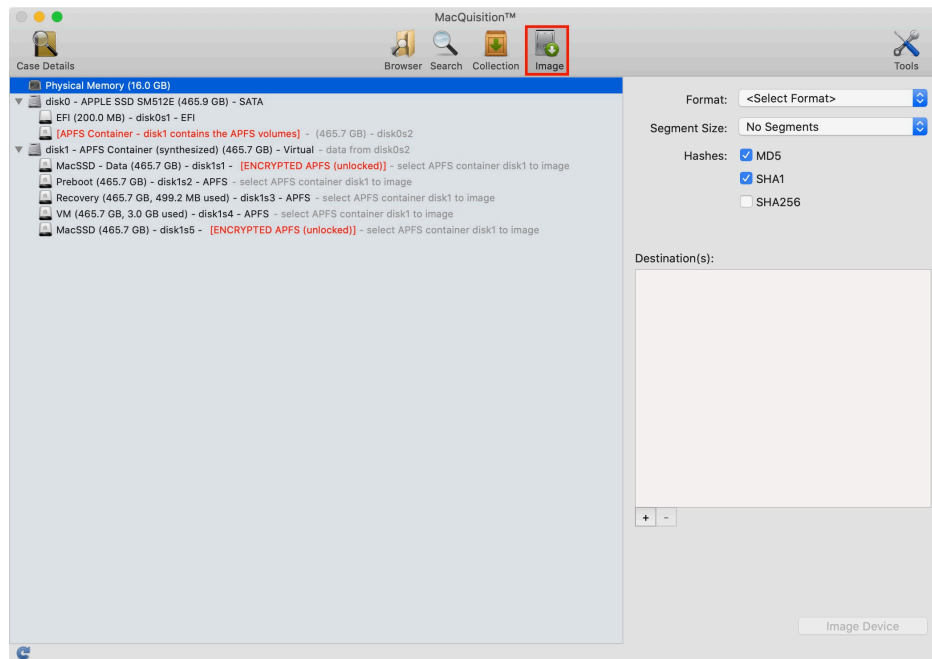
300 Piercy Road • San Jose, CA 95138 • 408.844.8890 • <https://www.blackbagtech.com>

IMPORTANT: If the Apple logo appears BEFORE the BlackBag logo IMMEDIATELY shutdown the computer with the power button – it is booting to a drive or other device NOT to MacQuisition.

A gray screen with a slashed circle will appear if the system fails to boot to the selected MacQuisition boot partition. Shutdown the system by pressing and holding the power button and attempt to boot with the next MacQuisition partition until all options are exhausted.

FORENSIC IMAGING

To image a computer booted to MacQuisition or to image a target system attached to an analysis system via TDM, select the **Image** button.



At this point, what you image depends on several factors including:

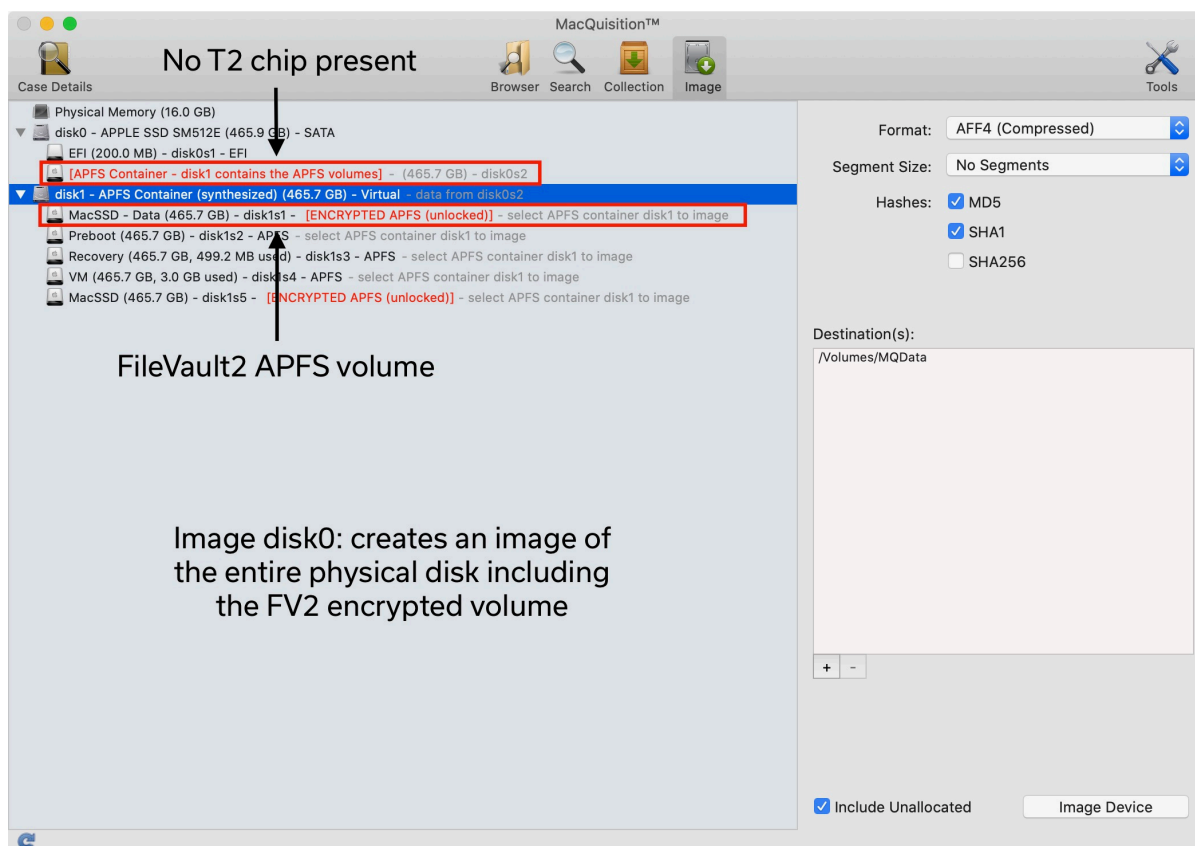
- FileVault2 enabled
- File system (APFS or HFS+)
- Fusion drives
- Bootcamp enabled
- T2 chip present

MacQuisition provides labels indicating exactly what hardware is present (T2 or multiple drives using Fusion) which file system is in use (APFS or HFS+), if there is a Bootcamp partition, and if FileVault2 is enabled.

So, let's walk through some of the different labels MacQuisition uses. This is by no means an exhaustive list.



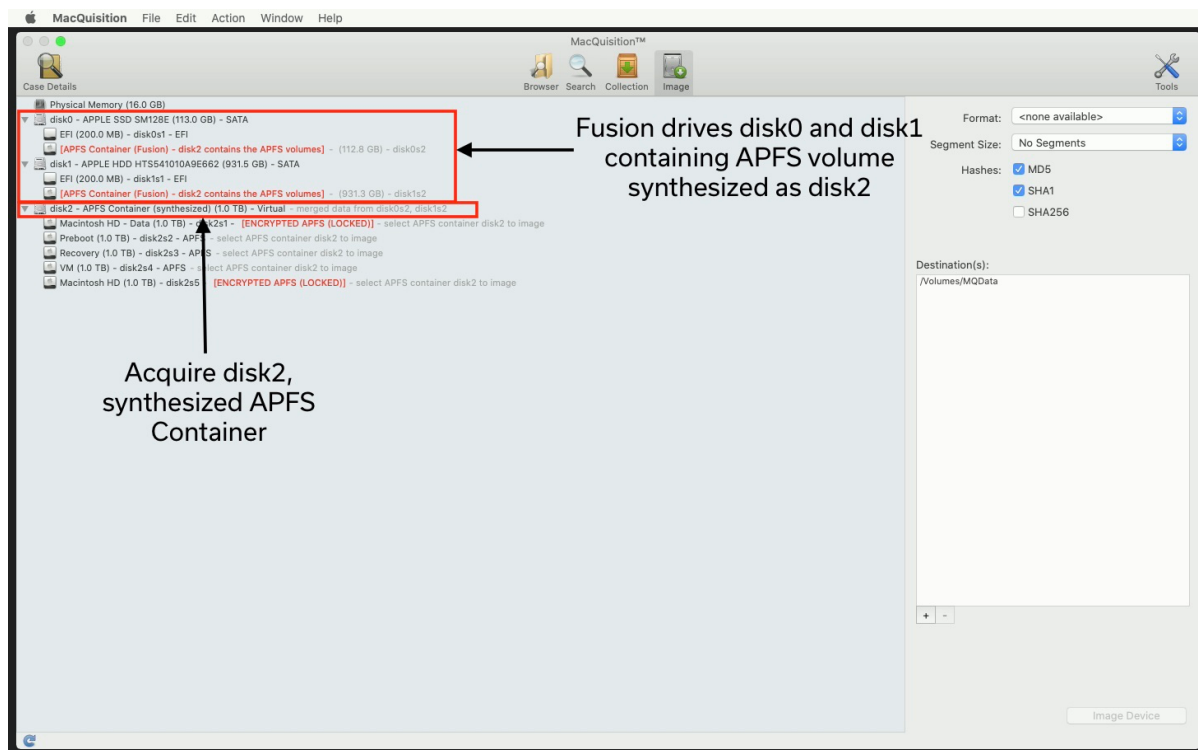
APFS and FileVault2



MacQuisition identifies an APFS volume on disk0 with FileVault2 enabled. In the example above, a user password or Recovery Key have already been entered, unlocking the FileVault2 encryption. There are two options for imaging:

- Image disk0: Creates a bit-by-bit copy of the entire physical disk. FileVault2 can be decrypted during analysis with BlackLight.
- Image disk1: Creates an image of the APFS Container with the FileVault2 encrypted data. FileVault2 can be decrypted during analysis with BlackLight.

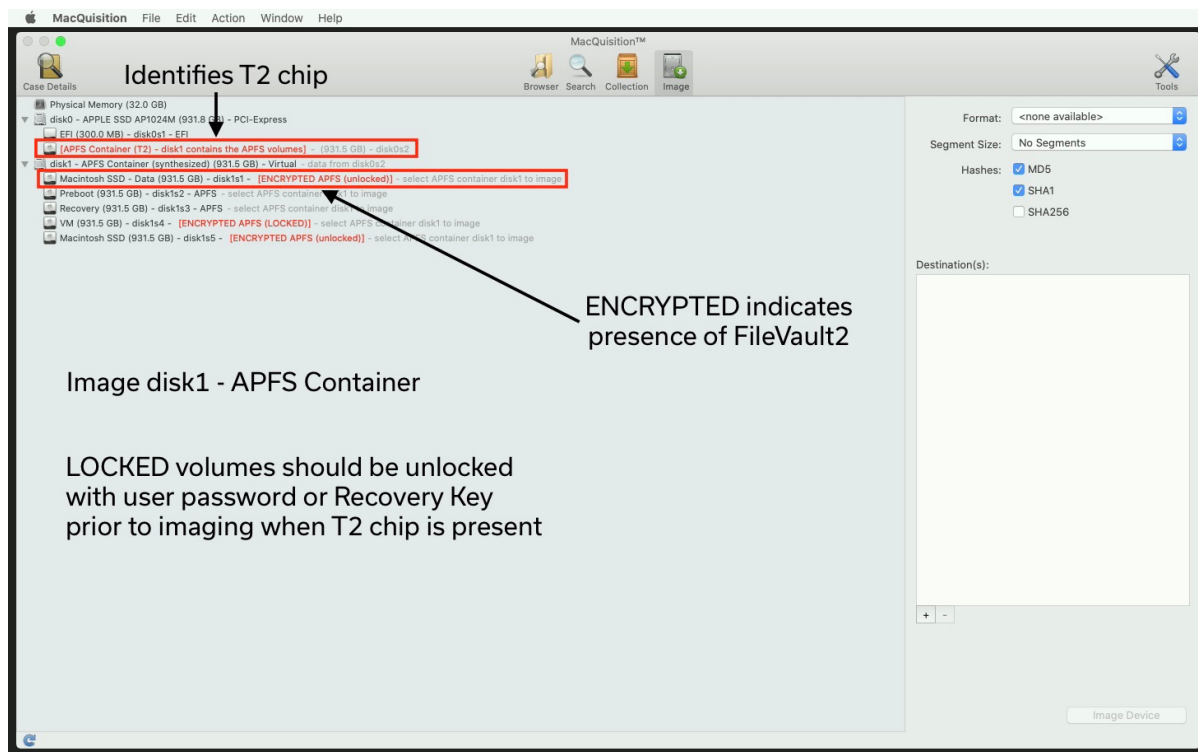
APFS and Fusion



MacQuisition identifies an APFS volume (disk2) on a Fusion drive using disk0 and disk1. The APFS Container is synthesized as disk2. Image disk2, the synthesized APFS container.



APFS, T2 and FileVault2



MacQuisition identifies and APFS volume with FileVault2 on a system with a T2 chip on disk0. The APFS container is synthesized as disk1. Image disk1 after unlocking the volume using a user login password or the Recovery Key. Since this system has a T2 chip, FileVault2 must be decrypted during acquisition. An image of disk0 will contain encrypted data that cannot be decrypted.

Take a Closer Look

In the examples shown, the systems were boot to MacQuisition. If a target system is attached to an analysis system via Target Disk Mode, the disk numbers will be different. The internal disk on the analysis system and any external hard drives connected will also be listed in MacQuisition.

Other Possibilities

If any of the above configurations also included a Bootcamp partition, it would be listed. An image of the APFS Container and a separate image of the Bootcamp partition may be required.

For systems with HFS+, if FileVault2 is enabled a user login password or Recovery Key are needed to unlock the volume before imaging.

Quick Reference Chart

Below is a quick reference chart to help determine when FileVault2 must be unlocked before imaging and which device should be imaged. The disk numbers referenced will change if TDM is used to connect a target system to an analysis system running or boot to MacQuisition.

File System/T2	Fusion	FileVault2 Enabled	Imaging Options
HFS+	No	No	Image physical drive (disk0)
HFS+	Yes	No	Image logical drive containing merged data (disk2)
HFS+	No	Yes	Unlock encrypted FileVault2 data before imaging, image decrypted logical drive
HFS+	Yes	Yes	Unlock encrypted FileVault2 data before imaging, image decrypted merged fusion logical drive
APFS	No	No	Image physical drive (disk0) (Do this if Bootcamp is present) or Image APFS Container (disk1)
APFS	Yes	No	Image APFS Container (disk2) merged data from disk0 and disk1
APFS	No	Yes	<i>FileVault2 data can be decrypted during analysis by BlackLight</i> Image physical drive (disk0)
APFS	Yes	Yes	<i>FileVault2 data can be decrypted during analysis by BlackLight</i>



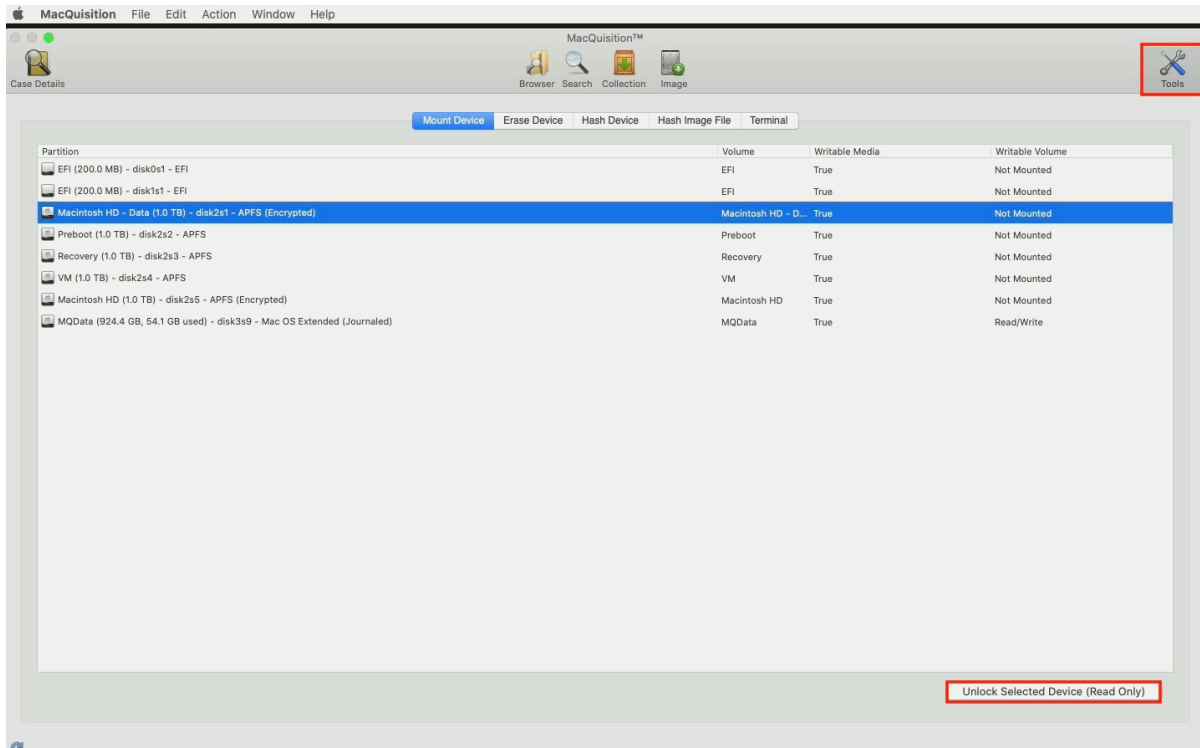
File System/T2	Fusion	FileVault2 Enabled	Imaging Options
			Image APFS Container (disk2) merged data from disk0 and disk1 (can unlock encrypted data before imaging to get decrypted image)
APFS T2 chip	No	No	Image APFS Container (disk1)
APFS T2 chip	Yes	No	Image APFS Container (disk2) merged data from disk0 and disk1
APFS T2 chip	No	Yes	Unlock encrypted FileVault2 data before imaging, image APFS Container (disk1)
APFS T2 chip	Yes	Yes	Unlock encrypted FileVault2 data before imaging, image APFS Container (disk2) merged data from disk0 and disk1

Takeaway

On APFS systems with no T2 chip, FileVault2 encrypted data can be decrypted during analysis. On systems with T2 chips, a user login password or Recovery Key are required during acquisition.

Unlocking FileVault2 Volume

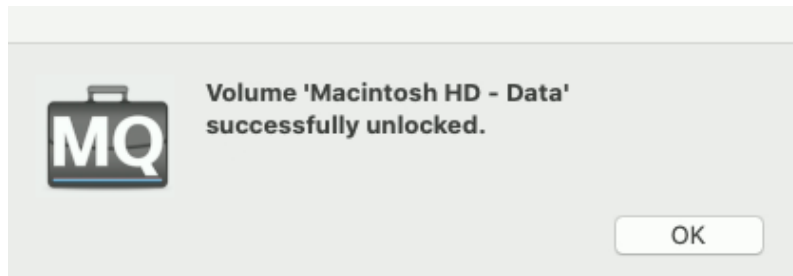
To unlock a volume, on the MacQuisition toolbar, select the **Tools** button. Select the **Mount Device** tab then locate and select the Locked volume. In the bottom right corner of the 'Tools' window, select the **Unlock Selected Device (Read Only)**.



A password/recovery key prompt appears.



Enter a user login password, the FileVault2 Recovery Key or click **Select Keychain File...** (*FileVaultMaster.keychain*). Click **Unlock**. If an incorrect decryption credential is entered, a dialog box appears indicating failure. If correct decryption credentials are entered, a dialog appears indicating the volume was successfully unlocked.



On the MacQuisition toolbar, select the **Image** button. The encrypted APFS volume should now be unlocked in the 'Image Device' view.

Mount Device Tab

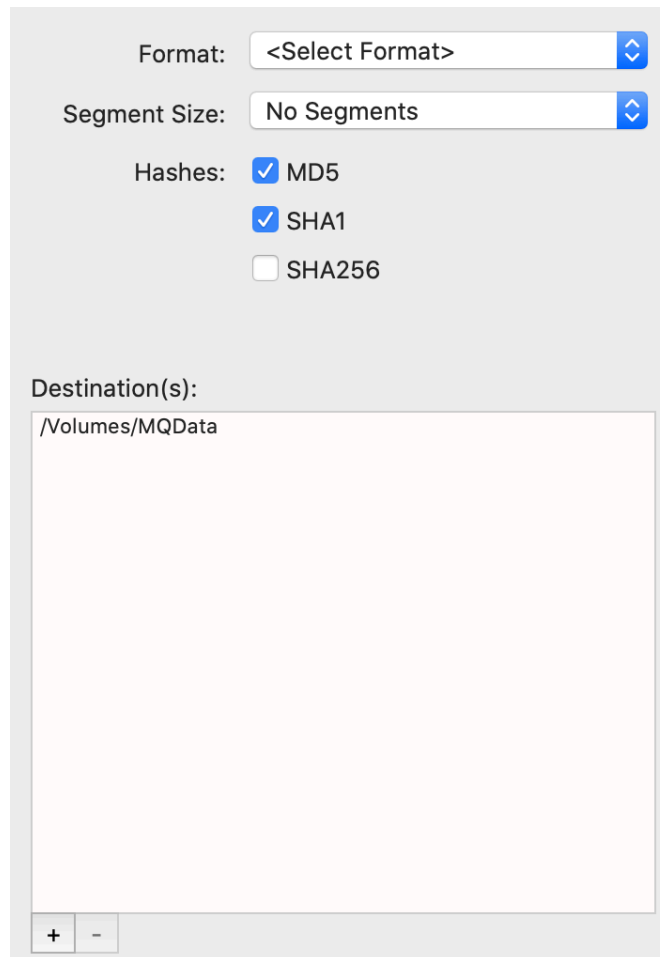
When booting a device with MacQuisition, by default only the MQData is mounted Read/Write. To save an image to another location on external media, mount the volume as Read/Write here.

Imaging

Options

Before imaging begins, the following information must be provided to MacQuisition:

- Image Format
- Segment Size
- Hashes
- Destination(s)
- Include Unallocated (AFF4 format only)



The image shows a software dialog box titled "Options" for MacQuisition. It contains several configuration fields:

- Format:** A dropdown menu currently showing "<Select Format>".
- Segment Size:** A dropdown menu currently showing "No Segments".
- Hashes:** A section with three checkboxes:
 - ☒ MD5
 - ☒ SHA1
 - ☐ SHA256
- Destination(s):** A large text area containing the path "/Volumes/MQData".

At the bottom left of the dialog box, there are two small buttons: a "+" button and a "-" button.



Image Format

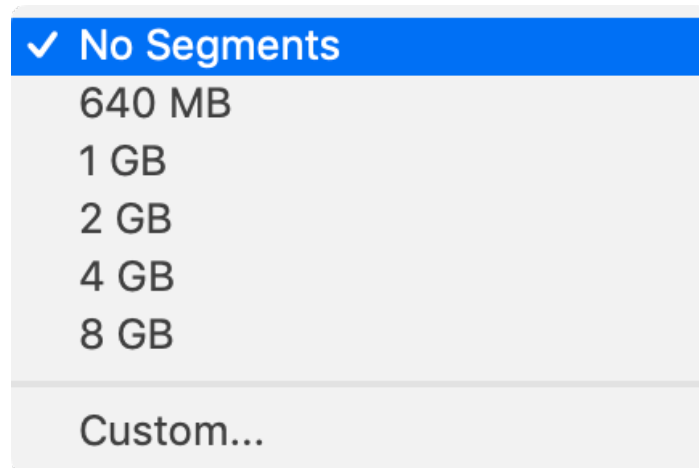
The following image formats are available:

- ✓ <Select Format>
- AFF4 (Compressed)
- AFF4 (Uncompressed)
- Raw
- DMG
- E01 (Uncompressed)
- E01 (Empty Block Compression)
- E01 (Fast Compression)
- E01 (Best Compression)

AFF4 format option will only be available for APFS containers. AFF4 must be selected for APFS Fusion drives and devices with T2 chips.

Segment Size

With the exception of AFF4, images can be segmented. Choose the segment size from the drop-down menu or manually enter a customized segment size. By default, **No Segments** is selected, creating a one large image.



✓ No Segments

640 MB

1 GB

2 GB

4 GB

8 GB

Custom...

✓ **Quick Tip: Forensic Image Sizes**

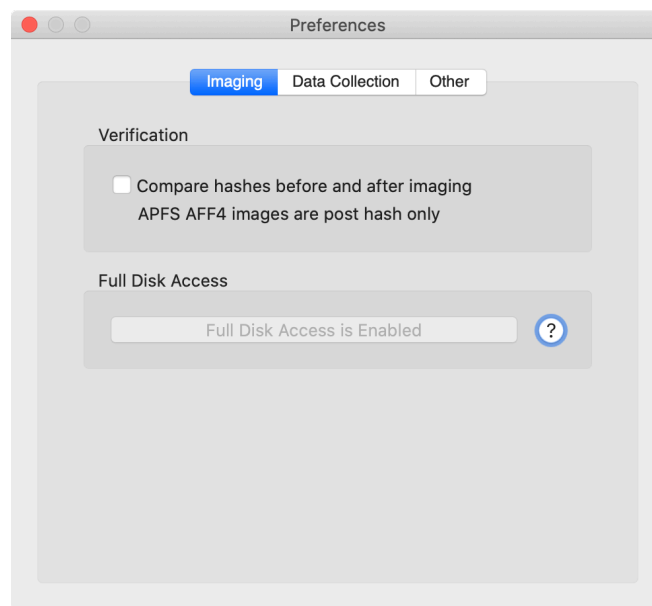
It is important to format the acquisition destination device appropriately. For instance, if the destination device is formatted with a FAT32 file system, **the largest supported acquisition segment size is 3.9 GB**. As AFF4 images cannot be segmented they cannot be stored on devices formatted with FAT32.



Hashes

MacQuisition has three imaging hashing options: MD5, SHA1 and SHA256. An E01 image will contain the MD5 and SHA1 hash value within the image if these hash options are selected. AFF4, Raw and DMG image formats do not store the hash values within the image.

Pre-image hashing is a preference that can be set in MacQuisition. When selected, hashing will occur before and after imaging.



Note on Pre-Image Hashing...

The AFF4 image format was integrated into MacQuisition primarily for imaging APFS Fusion and systems with T2 chip. Pre-image hashing is not valid for APFS Fusion drives since they are synthesized containers. Pre-image hashing on systems with T2chips would result in a hash of encrypted data that could never be decrypted and is therefore also not valid.

Destination(s)

Destination(s) indicate where the created image and MacQuisition log files will be stored. For segmented images, more than one destination drive can be selected.

Include Unallocated

Once the AFF4 format is selected, an **Include Unallocated** check box will appear next to the **Image Device** button. MacQuisition 2020 R1 is able to decrypt unallocated space on devices with T2 chips. Testing has shown collecting data from unallocated space, especially on systems with SSDs, does not provide useful data. To decrease overall imaging time, uncheck the box next to **Include Unallocated** to decrease overall imaging time.



Include Unallocated

Image Device



BlackBag®

300 Piercy Road • San Jose, CA 95138 • 408.844.8890 • <https://www.blackbagtech.com>

Image Device

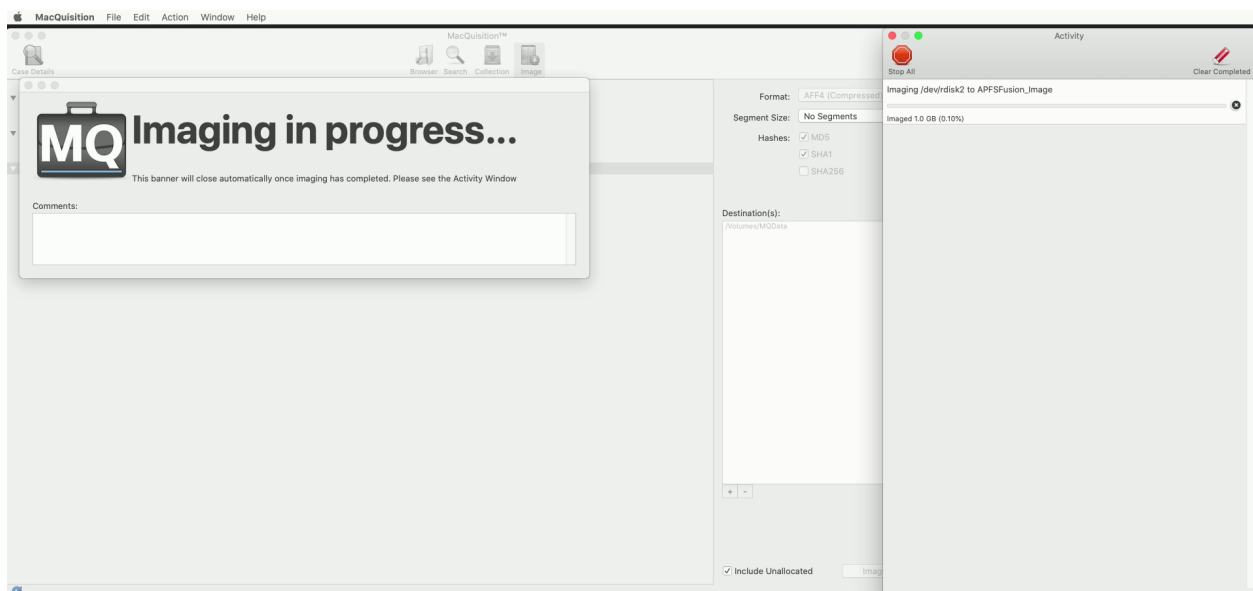
Once all options are set as desired select the **Image Device** button. An image name prompt appears. Enter a name in the text box and select the **Continue** button.

Destination Drive Warnings

If RAW, DMG, E01 (Uncompressed), or AFF4 (Uncompressed) are selected and the destination drive capacity is insufficient, a warning appears to indicate how much space is available on the destination drive and the space required to successfully acquire the source device image.

MacQuisition does not estimate the size of a compressed image. Therefore, if AFF4 or E01 with compression is selected and the destination drive capacity is insufficient for an uncompressed image, a warning appears to indicate how much space is available on the destination drive. Take this in consideration and proceed with caution.

Click **Image Device**. The **Image in Process** and **Activity** windows appear.

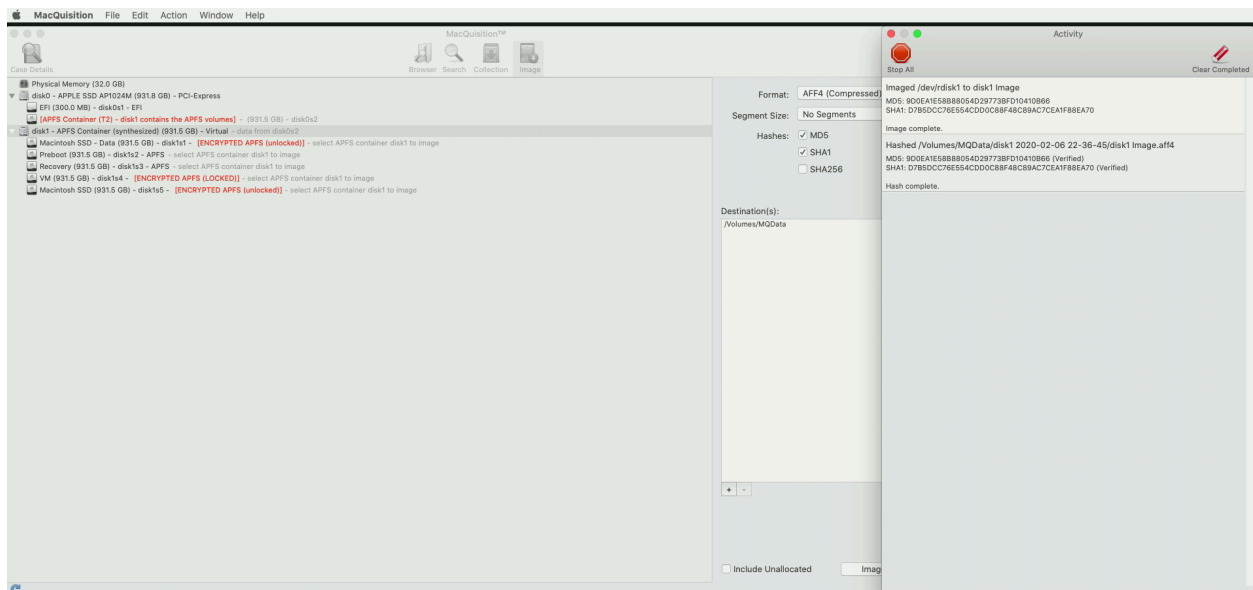


Activity Window

During the acquisition process, MacQuisition displays an **Activity** window. A progress bar appears to indicate bytes complete, percentage complete, and estimated time remaining.

Hashes selected on the **Image Device** window will be computed after the image is created. The hash values will appear in the **Activity** window and will also be stored in the *Acquisition Log.txt* file created in the image destination folder.

For AFF4 images, once imaging completes the **Activity** window will appear similarly to the following:



ADDITIONAL INFORMATION

For additional information on using MacQuisition, refer to the MacQuisition User's Guide. If you have any other questions or issues, search the BlackBag support portal <https://support.blackbagtech.com> or reach out to tech support via email support@blackbagtech.com.