MACQUISITION 2019 R1.2 RELEASE NOTES

MAY 30, 2019

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.

RESOLVED ISSUES

MQ-2204	Fixed booting on T2 Macs, previously was booting to internal Recovery partition.
MQ-2278	Fixed Target Disk Mode on MacBook Pro 2018 systems that previously resulted in error message.

MacQuisition 2019 R1 NEW FEATURES

Imaging Devices with T2 Chips

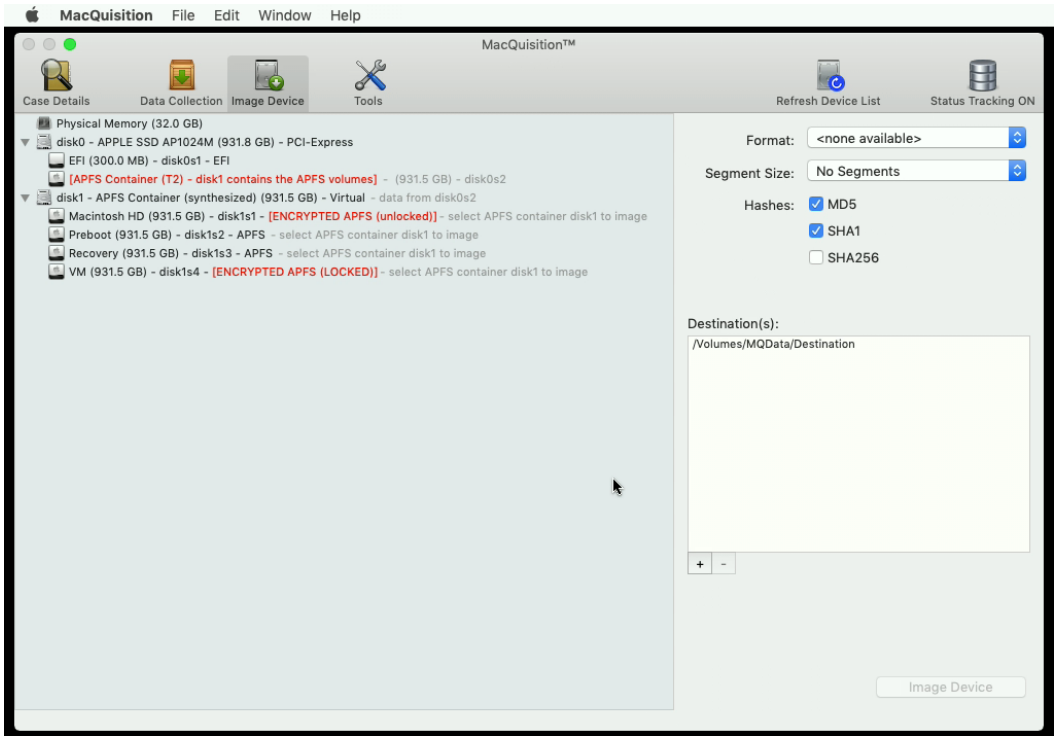
Starting in 2018, Mac computers have Apple's T2 security chip providing hardware-assisted encryption for data stored on the system. T2 chips are embedded into the disk controller and contain unique encryption keys. By default, all APFS volumes that contain user data on T2 protected systems are encrypted. The only way to decrypt the data is to use information embedded in the specific T2 chip from a given T2 protected system. Currently, it is not possible to extract encryption keys from the T2 chip. If the T2 chip is damaged, data can never be recovered from the drive.

The encryption provided by the T2 chip works in conjunction with FileVault 2. When FileVault 2 is enabled, the Recovery Key or password from any of the user accounts on the system is required to decrypt the data. Credentials to access the FileVault 2 encryption keys are required at the time of acquisition to decrypt the data.

MacQuisition 2019 R1 is the only solution that interfaces with the T2 chip to decrypt the filesystem at collection time, providing a physical image. MacQuisition 2019 R1 performs a physical acquisition that attempts to collect data as it exists on the disks including data not available via the file system interfaces providing more options for analysis and recovery of historical or deleted data. As analysis techniques evolve, the physical images created may lead to recovery of even more data. Currently, the physical images will provide access to APFS "Free Queue" blocks, APFS Snapshots, and data hidden in file slack.

Since the T2 chip is responsible for all encryption all data must be decrypted during acquisition; it is not possible to decrypt the data at analysis time. Because of the way encryption is implemented with the T2 chip, unallocated space cannot be decrypted at this time. To save time, since the unallocated space cannot be decrypted, there is an option to skip imaging unallocated space.

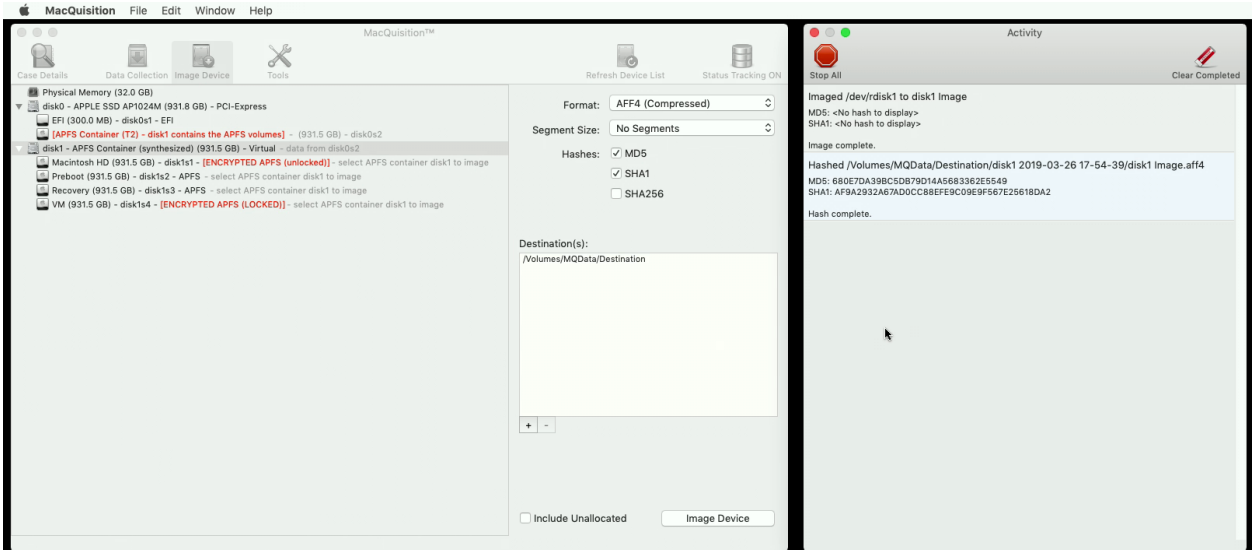
When a T2 system is booted, MacQuisition identifies the T2 device on the physical disk with the label APFS Container (T2).



If the physical disk is imaged, disk0 in the example shown above, the resulting image would be encrypted. The information needed for decryption is resident on the T2 chip and the decryption must occur during

acquisition. For MacQuisition to decrypt the data, the synthesized APFS container needs to be imaged. If the physical disk contains other volumes, such as a Bootcamp volume, they must be imaged separately.

As the APFS Container on the T2 system is acquired, MacQuisition interfaces with the T2 chip to decrypt the T2-protected data creating a decrypted physical image. Pre-image hashing would not be valid as the data is decrypted during the acquisition process. In order to create the physical image, MacQuisition creates an image using the open standard Advanced Forensic File Format (AFF4) image format. AFF4, supported by a number of popular forensic tools including BlackLight, provides modern compression algorithms and the flexibility required to efficiently image non-linear data, the APFS container, while optionally skipping data that cannot be decrypted, such as the unallocated space.



For additional information please see the User Guide Chapter 6.

Imaging APFS Fusion Drives

With the release of macOS 10.14 (Mojave), Apple provided an implementation for APFS Fusion. In macOS 10.14 (Mojave), the APFS logical container pool may consist of blocks that span across multiple physical volumes. APFS logical containers allow all volumes in the container to share a common pool of extents, data from all volumes is interspersed and volumes are not contiguous. This necessitates an imaging tool that is able to handle imaging non-contiguous APFS containers. Since synthesized APFS

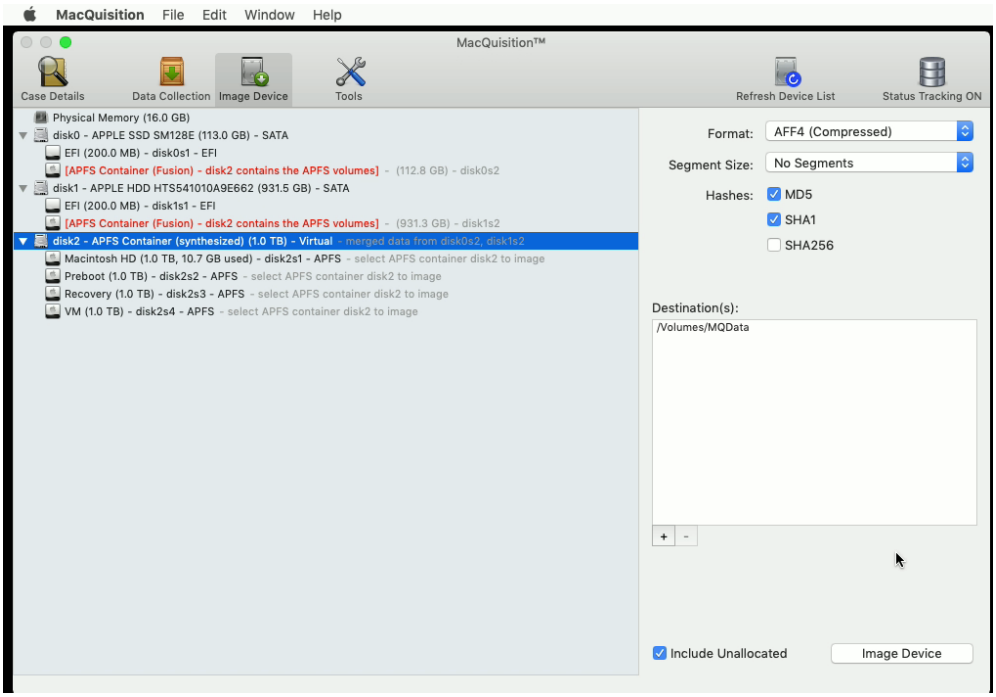
containers do not have a limit on the size or location of the volumes within it, creating a bit-by-bit physical image is not realistic.

Versions of MacQuisition prior to 2019 R1 allowed the acquisition of logical files only from APFS Fusion drives, copying files from the APFS container. Only information available via the file system interfaces was available. MacQuisition 2019R1 performs a physical acquisition that attempts to collect data as it exists on the disks including data not available via the file system interfaces providing more options for analysis and recovery of historical or deleted data.

In order to image non-contiguous APFS containers, MacQuisition creates an image using the open standard Advanced Forensic File Format (AFF4) image format. AFF4 is supported by a number of popular forensic tools, including BlackLight, provides modern compression algorithms and the flexibility required to efficiently image non-linear data found on APFS Fusion drives.

When loaded in MacQuisition, the partitions on the physical drives used to create the APFS logical containers will be identified as APFS Container (Fusion). The label will also indicate the disk MacQuisition assigns to the synthesized APFS container. The APFS container will indicate the disks and partitions used to create the synthesized container.

To create a physical image of an APFS Fusion device, select the disk that represents the synthesized **APFS Container**.



For additional information please see the User Guide Chapter 6.

Additional APFS Imaging Options

Examiners are increasingly encountering Apple File System (APFS) formatted Mac computers with FileVault 2 encryption. MacQuisition 2019 R1 provides the capabilities to acquire the encrypted data or decrypt the data at the time of acquisition.

For additional information please see the User Guide Chapter 6.

Capturing RAM and data collections live on Mojave 10.14

Apple continues to restrict what an application can access while the Mac is running live. MacQuisition 2019 R1 has been updated to support Mojave 10.14; examiners can capture RAM and perform data collections while the Mac is running live. The Data Collection pre-selected categories are also improved to better support the files on Mojave.

COMPATABILITY

TYPE	EARLIEST COMPATIBLE SYSTEM*	MOST RECENT COMPATIBLE SYSTEM
IMAC	iMac (Late 2009) Model Identifier: iMac10,1 / 11,1	iMac (2017) Model Identifiers: iMac18,1 / 18,2 / 18,3
IMAC PRO	iMac Pro (2017) Model Identifier: iMacPro1,1	iMac Pro (2017) Model Identifier: iMacPro1,1

TYPE	EARLIEST COMPATIBLE SYSTEM*	MOST RECENT COMPATIBLE SYSTEM
MAC MINI	Mac mini (Mid 2010) Model Identifier: Macmini4,1	Mac mini (2018) Model Identifiers: Macmini8,1
MAC PRO	Mac Pro (Mid 2010) Model Identifier: MacPro5,1	Mac Pro (Late 2013) Model Identifier: MacPro6,1
MACBOOK	MacBook (Late 2009) Model Identifier: MacBook6,1	MacBook (2017) Model Identifier: MacBook10,1
MACBOOK AIR	MacBook Air (Late 2010) Model Identifier: MacBookAir3,1 / 3,2	MacBook Air (2018) Model Identifiers: MacBookAir8,1
MACBOOK PRO	MacBook Pro (Mid 2010) Model Identifier: MacBookPro6,1 / 6,2 / 7,1	MacBook Pro (2018) Model Identifiers: MacBookPro15,1 / 15,2 / 15,3

* Certain older 2007-2009 models that are not supported by the MacQuisition 2019R1 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.

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.