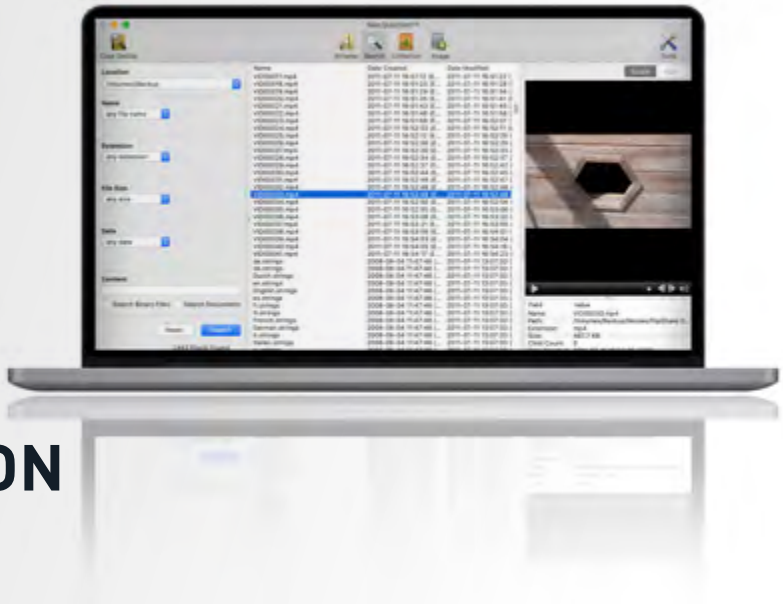
Cellebrite Digital intelligence for a safer world

PRODUCT OVERVIEW



Cellebrite
MACQUISITION

Triage and acquire forensic images from Apple's latest computers

The field of computer forensics investigation is growing, especially as law enforcement and legal entities realize that valuable data stored on computers can help reveal the full picture when conducting corporate and criminal investigations. As Apple's Mac computers continue to grow in popularity among users within organizations, today's forensic examiners need powerful and proven solutions to help them perform live data acquisition, targeted data collection, and forensic imaging from these computers.

MacQuisition® is the first and only solution to create physical decrypted images of Apple's latest Mac computers utilizing the Apple T2 chip. Apple's T2 encryption methodology is unique to each Mac, and critical data can only be decrypted using the keys stored in that systems T2 chip. BlackBag has built the only solution that works with the chip to decrypt the filesystem at collection time, empowering examiners to capture the entire physical blocks that hold vital information and not just logical files. In cases where multiple machines and devices are involved, MacQuisition® provides the option to browse and search through data, and preview file contents before any data is collected or devices are imaged.

Tested and used by experienced examiners for over a decade, MacQuisition® runs on the macOS operating system and safely boots and acquires data from hundreds of different Macintosh computer models in their native environment – even Fusion Drives.

Key Benefits of MacQuisition®

Carry Out On-scene Content Triage

With leading triage capabilities, users can browse files based on metadata or keyword hits prior to collection to verify the device system is relevant.

Perform Targeted Data Collection with Selective Extraction

Speed up the time to extraction by targeting and forensically acquiring files, folders, and user directories while avoiding known system files and other unnecessary data. Selectively acquire email, chat, address book, calendar, and other data on a per-user, per-volume basis. Thoroughly log data acquisitions and source device attributes throughout the collection process and preserve valuable metadata by maintaining its association with the original file. Easily authenticate collected data through hashing.

Collect Data from Live Systems

With live data acquisition, you can soundly acquire and save volatile Random-Access Memory (RAM) contents to a destination device. Capture important live data such as Internet, chat, and multimedia files in real time. Choose from 26 unique system data collection options, including active system processes, current system state, and print queue status. Capture RAM and targeted collections live on Catalina. Gain automatic log information of live data acquisition throughout the collection process.

Easily Create Forensic Images

MacQuisition provides the flexibility to collect macOS images of the whole drive, partial drive, or live RAM from the same tool depending on what the circumstance dictates. It is the only tool to create physical decrypted images of Apple's T2 chip systems, including unallocated and APFS Fusion drives.

If File Vault 2 exists, the examiner can, with the use of a password, Keychain file or recovery key, mount the volume in a read-only fashion, allowing for either a triage or collection of the files. Use the source machine's own system to create a forensic image by booting from the MacQuisition® USB dongle. Write-protect source devices while maintaining read-write access on destination devices.