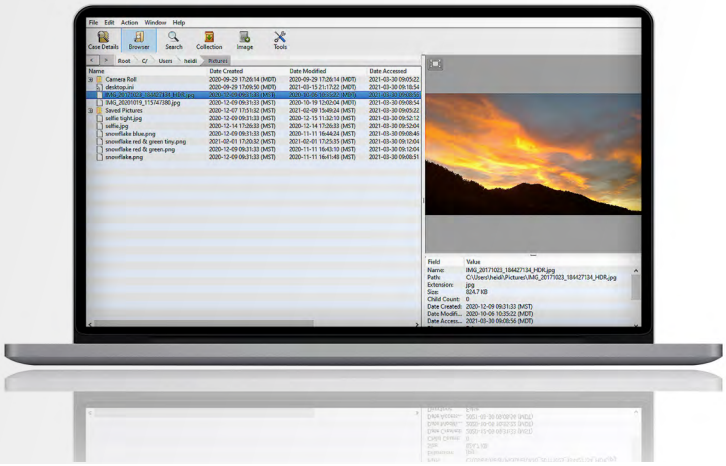
Cellebrite

Digital Collector.



Triage and acquire forensic images from Windows PC and Apple macOS computers

The field of computer forensics continues to grow, especially as public safety agencies, eDiscovery practitioners and internal investigators realize that valuable data stored on computers can help reveal the full picture when investigating computer-based or computer facilitated crimes.

With the ever-increasing rate of cybercrimes, computers may constitute a scene of a crime. Computers may hold evidence in the form of emails, internet history, documents, or other files relevant to crimes. Even metadata can help shed light on cases such as murder, kidnap, fraud, and drug trafficking. To better address these digital investigations, forensic examiners and analysts need powerful and proven solutions to detect and prevent crime where evidence is stored digitally.

Agencies and corporations need reliable computer forensic solutions to help them acquire, analyze, and report on digital evidence in a way that is both legally admissible and protects an organization.

Cellebrite Digital Collector is a powerful forensic imaging hardware-based software solution to perform triage, live data acquisition, and targeted data collection for Windows PC and macOS computers. As the only forensic solution on the market today that does live and dead box imaging for both Windows and macOS, Digital Collector is a must have tool in every digital forensic toolbox.

Used by experienced forensic examiners for over a decade, Cellebrite Digital Collector runs on both Windows and macOS operating systems, and safely boots and acquires data from hundreds of different macOS computer models in their native environment – even those with Fusion Drives, Apple T2 chips, or Apple Silicon M1-M4 systems. The solution is available on a self-contained, portable USB device with a choice of solid state drive (SSD) storage capacity to meet your needs.

Key Benefits of Cellebrite Digital Collector

Carry Out On-scene Content Triage

With leading triage capabilities, examiners can browse files based on metadata or advanced keyword search hits prior to collection or imaging to verify that the computer is relevant to the investigation.

File previews of images (e.g. JPG, PNG, GIF) and Microsoft Office files on Windows computers are available during triage, as well as all file types supported by Quick Look on macOS.

Perform Targeted Data Collection with Selective Extraction

Speed up the time of 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 throughhashing (MD5, SHA-1, SHA-256).

Collect Data from Live Systems

With live data acquisition, you can soundly acquire and save volatile Random-Access Memory (RAM) contents from macOS computers to a destination device or the Cellebrite Digital Collector SSD itself. Capture important live data such as Internet, chat, and multimedia files in real time. Choose from up to 26 unique system data collection options, including active system processes, current system state, and print queue status. View automatic log information of live data acquisition throughout the collection process.

Easily Create Forensic Images

Cellebrite Digital Collector provides the flexibility to collect macOS images of the whole drive, partial drive, or live RAM with the same tool depending on the circumstance. It is the only tool to create decrypted physical images of Apple T2 chip systems, including unallocated and APFS Fusion drives, as well as APFS volumes in the latest Apple Silicon M1-M4 systems. Advanced Forensic Format 4 (AFF4) format is supported for the imaging of APFS volumes.

On FileVault 2 systems, the examiner can provide a password, Keychain file, or recovery key, and then mount the volume as read-only to conduct triage and to collect files. Using the source machine's own system to create a forensic image by booting from the Cellebrite Digital Collector SSD USB dongle is possible. Write protection of source devices while maintaining read-write access on destination devices is fully implemented.

Windows PC computers can be easily imaged using Cellebrite Digital Collector in various AFF4, E01, and RAW formats. Cellebrite Digital Collector can acquire an image of an encrypted disk on Windows; however, Digital Collector cannot decrypt data during imaging or unlock encrypted disks for data collection from Windows PC computers. If the encryption is a variant supported by Cellebrite Inspector, such as BitLocker, TrueCrypt, or VeraCrypt, the image can be readily decrypted during ingestion using the password or recovery key.

Connect with one of our experts

to learn how you can streamline your investigations and accelerate your time to case resolution with Cellebrite Digital Collector.