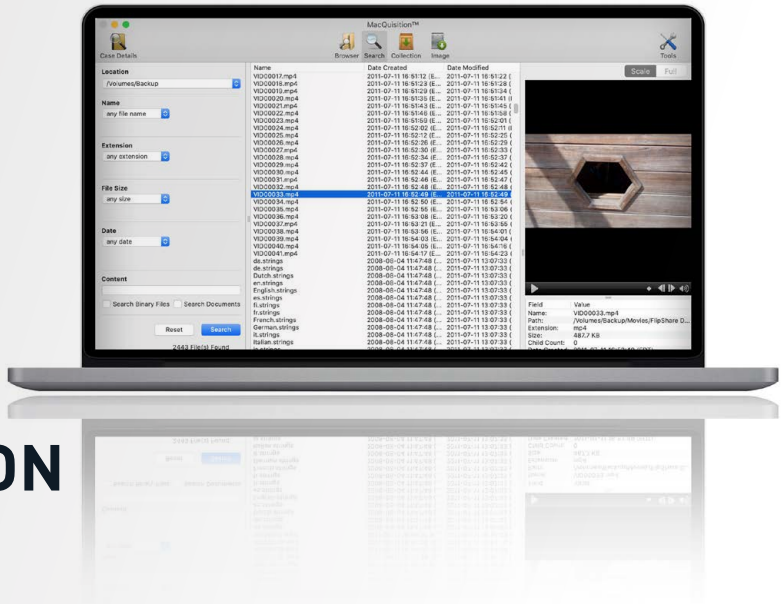
Cellebrite Digital intelligence for a safer world

PRODUKTÜBERSICHT



Cellebrite MACQUISITION

Sichtung und Erfassung forensischer Images von Apples neuesten Computern

Der Bereich der computerforensischen Ermittlungen wächst, insbesondere da Strafverfolgungsbehörden und juristische Personen erkennen, dass wertvolle Daten, die auf Computern gespeichert sind, bei der Durchführung von Unternehmens- und strafrechtlichen Ermittlungen helfen können, ein vollständiges Bild zu vermitteln. Da die Mac-Computer von Apple bei Anwendern innerhalb von Unternehmen immer beliebter werden, benötigen die heutigen forensischen Prüfer leistungsstarke und bewährte Lösungen, die sie bei der Live-Datenerfassung, der gezielten Datenerfassung und der forensischen Bildgebung von diesen Computern unterstützen.

MacQuisition® ist die erste und einzige Lösung, die physisch entschlüsselte Images der neuesten Mac-Computer von Apple mit dem Apple T2-Chip erstellt. Die T2-Verschlüsselungsmethode von Apple ist für jeden Mac einzigartig, und kritische Daten können nur mit den Schlüsseln entschlüsselt werden, die im T2-Chip dieses Systems gespeichert sind. BlackBag hat die einzige Lösung entwickelt, die mit dem Chip zusammenarbeitet, um das Dateisystem bei der Abholung zu entschlüsseln, sodass die Prüfer in der Lage sind, die gesamten physischen Blöcke zu erfassen, die wichtige Informationen enthalten, und nicht nur logische Dateien. In Fällen, in denen mehrere Maschinen und Geräte beteiligt sind, bietet MacQuisition® die Möglichkeit, Daten zu durchsuchen und eine Vorschau der Dateiinhalte zu erstellen, bevor Daten gesammelt oder Geräte abgebildet werden.

MacQuisition® wird seit über einem Jahrzehnt von erfahrenen Prüfern getestet und verwendet. Es läuft unter dem Betriebssystem macOS und bootet und erfasst Daten von Hunderten verschiedener Macintosh-Computermodellen in ihrer nativen Umgebung – sogar von Fusion-Laufwerken.

Die wichtigsten Vorteile von MacQuisition®

Inhaltssichtung vor Ort durchführen

Mit den führenden Sichtungsfunktionen können Benutzer Dateien vor der Erfassung auf der Grundlage von Metadaten oder Stichworttreffern durchsuchen, um zu überprüfen, ob das Gerätesystem relevant ist.

Gezielte Datenerfassung mit selektiver Extraktion durchführen

Verkürzen Sie die Zeit bis zur Extraktion, indem Sie Dateien, Ordner und Benutzerverzeichnisse gezielt und forensisch erfassen und dabei bekannte Systemdateien und andere unnötige Daten vermeiden. Erfassen Sie selektiv E-Mail-, Chat-, Adressbuch-, Kalender- und andere Daten auf Benutzer- und Volume-Basis. Protokollieren Sie die Datenerfassung und die Attribute der Quellgeräte während des gesamten Sammelprozesses gründlich, und bewahren Sie wertvolle Metadaten, indem Sie die Zuordnung zur Originaldatei aufrechterhalten. Authentifizieren Sie die gesammelten Daten problemlos durch Hashing.

Daten von Live-Systemen sammeln

Mit der Live-Datenerfassung können Sie flüchtige RAM-Inhalte (Random-Access Memory) zuverlässig erfassen und auf einem Zielgerät speichern. Erfassen Sie wichtige Live-Daten wie Internet, Chat und Multimediadateien in Echtzeit. Wählen Sie aus 26 einzigartigen Systemdatenerfassungsoptionen, einschließlich aktiver Systemprozesse, des aktuellen Systemstatus und des Status der Druckwarteschlange. Erfassen Sie RAM und gezielte Sammlungen live auf Catalina. Sie erhalten während des gesamten Erfassungsvorgangs automatische Protokollinformationen der Live-Datenerfassung.

Forensische Images einfach erstellen

MacQuisition bietet die Flexibilität, MacOS-Images des gesamten Laufwerks, eines Teils des Laufwerks oder des Live-RAMs mit demselben Tool zu sammeln, je nachdem, was die Umstände erfordern. Es ist das einzige Tool zur Erstellung physisch entschlüsselter Images von Apples T2-Chipsystemen, einschließlich nicht zugeordneter und APFS-Fusionslaufwerke.

Wenn File Vault 2 vorhanden ist, kann der Prüfer das Volume mit Hilfe eines Kennworts, einer Keychain-Datei oder eines Wiederherstellungsschlüssels schreibgeschützt mounten, sodass entweder eine Sichtung oder eine Sammlung der Dateien möglich ist. Verwenden Sie das eigene System des Ausgangsrechners, um ein forensisches Image zu erstellen, indem Sie vom MacQuisition®-USB-Dongle booten. Schreibschutz für Quellgeräte bei gleichzeitiger Aufrechterhaltung des Lese- und Schreibzugriffs auf die Zielgeräte.