

ÜBERSICHT ÜBER DIE LÖSUNG



Cellebrite MACQUISITION



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 T2-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. Dies wird dabei helfen, Prioritäten zu setzen, was gesammelt werden soll.

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.

Wichtigste Vorteile

- Inhaltssichtung vor Ort durchführen
- Gezielte Datenerfassung mit selektiver Extraktion durchführen
- Daten von Live-Systemen sammeln
- Forensische Images einfach erstellen



ÜBERSICHT ÜBER DIE LÖSUNG



Cellebrite BLACKLIGHT



Eine marktführende Lösung für die schnelle und umfassende Analyse von Computerextraktionen, mit der forensische Prüfer und Analysten Licht in die Benutzeraktivitäten bringen und verwertbare Erkenntnisse gewinnen können. Mit einer einfach zu bedienenden Schnittstelle, die einfaches Suchen, Filtern und Durchsuchen großer Datensätze ermöglicht, ist BlackLight® die beste verfügbare Option für die Durchführung intelligenter Datenanalysen.

BlackLight® unterstützt laufende forensische Toolkit-Integrationen, um Daten in einen Fall zu bringen; dazu gehören Produkte wie Berla, Semantics 21, PhotoDNA, Project Vic, APOLLO und mehr.

Wichtigste Vorteile

 Windows-Unterstützung	 Mac-Unterstützung	 Unterstützung für iOS und Android
<ul style="list-style-type: none"> Überprüfung der Gerätehistorie von Microsoft Volume Shadow Copies 	<ul style="list-style-type: none"> Volle Unterstützung für Apple Latest Systems APFS; einschließlich T2-Chip, Fusion und verschlüsselte Geräte 	<ul style="list-style-type: none"> Einfaches Anzeigen von Nachrichtengesprächen
<ul style="list-style-type: none"> Integrierte Analyse des Windows-Speichers und der Windows-Registrierung 	<ul style="list-style-type: none"> Überprüfung der Gerätehistorie von APFS-Snapshots und Time Machine-Sicherungen 	<ul style="list-style-type: none"> Überprüfung von Statusdaten, Wallet-Transaktionen und Kalenderaktivitäten
<ul style="list-style-type: none"> Automatisches Parsen von Kontoinformationen, aktuellen Dokumenten, Downloads, Papierkorb, USB-Verbindungen und mehr 	<ul style="list-style-type: none"> Anzeigen und Suchen von vereinheitlichten Protokoll-, Spotlight- und KnowledgeC-Daten 	<ul style="list-style-type: none"> Integration vieler Cellebrite-Extraktionen
<ul style="list-style-type: none"> Unterstützung von Benutzeraktivitäten und Registrierungsartefakten wie: Jump-Listen, Shell-Bags, Prefetch, Ereignisprotokolle, Superfetch, Windows 10-Zeitleistenaktivität, Srum und mehr 	<ul style="list-style-type: none"> Überprüfung von Downloads, WLAN-Verbindungen, aktuellen Dokumenten und Benutzeraktivitäten 	<ul style="list-style-type: none"> Integrierte SQLite- und Plist-Anzeige zur Überprüfung von Anwendungsdaten

