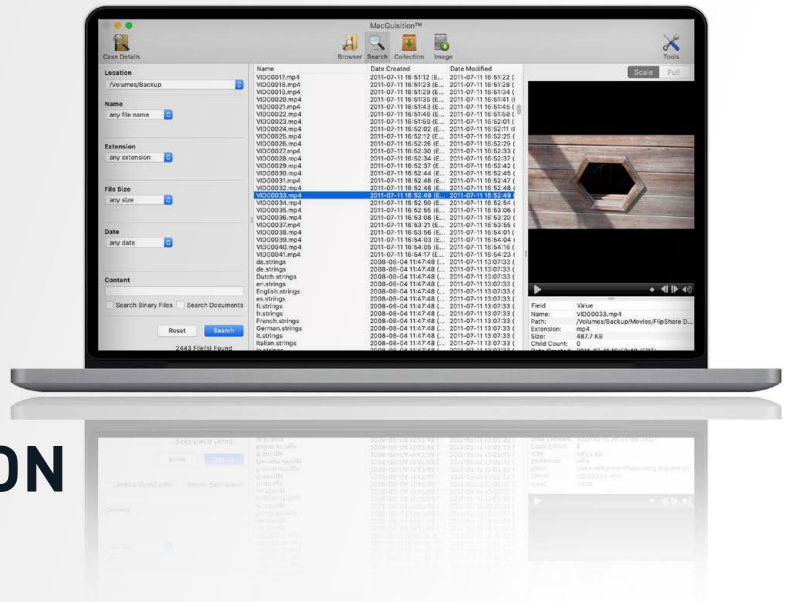


PRÉSENTATION DU PRODUIT



Procédez au triage et à l'acquisition d'images extraites des ordinateurs Apple dernière génération

Le domaine des renseignements et enquêtes numériques est en plein essor, d'autant plus que les forces de l'ordre et entités juridiques se rendent compte à quel point les données précieuses stockées sur les ordinateurs peuvent s'avérer utiles pour révéler le tableau complet lors d'enquêtes corporatives et criminelles. Tandis que les ordinateurs Mac d'Apple continuent de croître en popularité parmi les utilisateurs au sein des organisations d'aujourd'hui, les experts en renseignement numérique ont besoin de solutions performantes et éprouvées pour les aider à effectuer des acquisitions de données en temps réel, des collectes de données ciblées et de l'imagerie judiciaire depuis ces ordinateurs.

MacQuisition® est la première et la seule solution permettant de créer des images décryptées physiques des ordinateurs Mac dernière génération en utilisant la puce Apple T2. La méthode de cryptage T2 d'Apple est unique à chaque Mac, et les données critiques ne peuvent être déchiffrées qu'en utilisant les clés stockées dans la puce T2 de ce système. BlackBag a développé la seule solution qui fonctionne avec la puce pour décrypter le système de fichiers au moment de la collecte, permettant aux examinateurs de capturer l'ensemble des blocs physiques qui détiennent les informations indispensables et pas seulement des fichiers logiques. Dans les cas où plusieurs machines et appareils sont impliqués, MacQuisition® offre la possibilité de parcourir et de rechercher parmi les données, d'afficher un aperçu du contenu avant que des données ne soient recueillies ou que les appareils soient imagés.

Testé et utilisé par des examinateurs chevronnés depuis plus de dix ans, MacQuisition® fonctionne avec le système d'exploitation macOS et amorce et acquiert sûrement des données depuis des centaines de différents modèles d'ordinateurs Macintosh dans leur environnement natif - y compris Fusion Drives.



Les principaux avantages de MacQuisition®



Procéder au triage de contenu sur les lieux

Grâce à des capacités de triage de premier ordre, les utilisateurs peuvent parcourir des fichiers sur la base de métadonnées ou d'entrées de mots clés avant de procéder à la collecte pour vérifier que le système de l'appareil est pertinent.



Effectuer la collecte de données ciblées avec l'extraction sélective

Accélérer le temps nécessaire à l'extraction en ciblant et en acquérant de manière juridiquement recevable des fichiers, dossiers et répertoires utilisateurs tout en évitant les fichiers systèmes connus et autres données inutiles. Procéder à des acquisitions sélectives de mails, chats, carnet d'adresses et autres données sur une base par utilisateur, par volume. Minutieusement enregistrer les acquisitions de données et attributs des périphériques source tout au long du processus de collecte et préserver des précieuses métadonnées en maintenant leur association avec le fichier d'origine. Facilement authentifier les données recueillies via le hachage.



Recueillir des données à partir de systèmes actifs

Avec l'acquisition de données en temps réel, vous pouvez en toute quiétude acquérir et sauvegarder les données de mémoire vive (RAM) sur un appareil de destination. Capturer des données « vivantes » comme des fichiers multimédia, chat ou Internet en temps réel. Sélectionner parmi 26 options uniques de collecte de données du système, y compris les processus de système actif, l'état actuel du système et l'état de la file d'attente d'impression. Capturez des collectes ciblées et RAM en temps réel sur Mojave. Obtenez automatiquement des informations relatives au journal d'acquisition de données en direct tout au long du processus de collecte.



Créer facilement des images judiciaires

MacQuisition offre la souplesse nécessaire à la collecte d'images macOS de l'ensemble du disque, du disque partiel ou de RAM en direct depuis le même outil, en fonction de ce que les circonstances exigent. C'est le seul outil qui permet de créer des images décryptées physiques des systèmes de puce T2 d'Apple, y compris les disques non attribués et APFS Fusion.

Si File Vault 2 existe, l'examineur peut, avec un mot de passe, un fichier du Trousseau ou une clé de récupération, monter un volume en lecture seule, permettant soit un triage, soit une collecte des fichiers. Utiliser le système même du dispositif source pour créer une image judiciaire en amorçant depuis le dongle USB MacQuisition®. Protéger des appareils contre l'écriture tout en conservant un accès en lecture/écriture sur les appareils de destination.

