

MOBILedit Cloud Forensic

Obtenez l'empreinte numérique
complète d'un suspect

Les gens interagissent dans l'univers numérique d'aujourd'hui par le biais de leurs téléphones et de leurs applications. Laisant des empreintes numériques partout. Pour une enquête numérique complète et réussie, il est nécessaire d'analyser toutes les traces. La criminalistique des téléphones est extrêmement importante, mais ce qui est stocké dans un appareil mobile n'est qu'un instantané de l'ensemble des données. Les preuves trouvées dans le Cloud, les plateformes de messagerie et les réseaux sociaux apportent un éclairage complet sur la vie d'une personne.

Comprendre son style de vie, ses activités, personnalité, goûts et aversions, préférences et activités sociales grâce à des services tels que Facebook, Instagram, LinkedIn, Twitter, Slack ou les applications Google.

Avec un examen de téléphone réussi fourni par MOBILedit Forensic PRO, vous avez presque tout ce qui est nécessaire pour une extraction réussie du Cloud. En effet, les applications téléphoniques contiennent des informations de connexion précieuses pour la plupart des services Cloud. Même sans téléphone, vous pouvez toujours accéder aux données des services Cloud qui sont utilisées par des millions de personnes plusieurs fois par jour.

MOBILedit Cloud Forensic est un outil complet d'extraction de données dans le Cloud et un générateur de rapports pour les services les plus populaires. Il peut immédiatement débiter les téléchargements lorsque des informations d'authentification sont trouvées dans un téléphone, et il peut exécuter plusieurs extractions simultanément lorsque le temps est compté.

CLOUD FORENSICS EST DISPONIBLE EN DEUX OPTIONS POUR RÉPONDRE À LA FOIS AUX BESOINS DES SPÉCIALISTES DE L'INTERCEPTION JUDICIAIRE DES RÉSEAUX ET AUX CONTRÔLEURS DE DISPOSITIFS MOBILES.

Intégration avec MOBILedit Forensic PRO

Avec cette option, vous pouvez extraire des données du Cloud via un appareil mobile connecté à MOBILedit Forensic Pro.

Les informations d'identification sont extraites de l'appareil, et l'extraction du Cloud est lancée dans le cadre du processus d'examen du téléphone. Ces informations d'identification sont également enregistrées afin qu'un enquêteur puisse utiliser le jeton (token) ou les détails de connexion du compte à une date ultérieure.

MOBILedit Cloud Forensic comme produit autonome

Pour enquêter sur le stockage dans le Cloud et les services en Cloud sans avoir besoin d'examiner les appareils mobiles. L'accès au Cloud en utilisant cette méthode nécessite un mot de passe et un nom d'utilisateur ou un jeton (token) importé d'une autre source. Dans les deux cas, vous pouvez enquêter sur plusieurs clouds à la fois, et les extractions s'exécutent simultanément pour vous aider à travailler plus rapidement et à récupérer plus de preuves. La quantité de données extractibles est aussi grande que le compte cloud. Par conséquent, vous devez prendre en compte la capacité de stockage ou filtrer par période de temps au moment de l'extraction. En outre, les jetons (token) ont une date d'expiration qui dépend du fournisseur de services.



FONCTIONNALITES

- Téléchargement automatique des Cloud en utilisant soit un jeton d'autorisation soit un nom d'utilisateur et un mot de passe d'identification. Ceux-ci peuvent être trouvés, extraits et sauvegardés à partir d'un téléphone pendant l'extraction et l'analyse avec MOBILedit Forensic Pro.
- L'accès par jeton d'autorisation et l'accès par nom d'utilisateur et mot de passe sont tous deux pris en charge. Un jeton d'autorisation est un fichier enregistré sur un ordinateur ou un appareil mobile. Il reconnaît un appareil et un compte pour permettre à un utilisateur de se connecter à un service sans avoir à saisir à chaque fois un nom d'utilisateur et un mot de passe.
- Accès manuel en saisissant un nom d'utilisateur et un mot de passe.
- Des téléchargements immédiats et simultanés qui permettent à un enquêteur de travailler efficacement tout en extrayant le maximum de données dans le temps le plus court possible. Le temps est essentiel car un utilisateur peut effacer toutes les données, un jeton peut expirer ou un mot de passe peut être modifié.
- Rapports professionnels et exportations dans les formats suivants: pdf, html, xml, ufd, et Excel.
- Téléchargement de la structure complète du fichier.

SERVICES SOUTENUS

- Box
- Dropbox
- Google Drive
- Microsoft OneDrive
- FTP
- Facebook
- Facebook Messenger
- Google Contacts, Calendar, Keep
- Instagram
- LinkedIn
- Slack
- Twitter
- Emails tels que Gmail, Outlook, et bien d'autres via POP3, protocoles IMAP
- et autres

POURQUOI LES CLOUD?

- D'ici 2025, on estime que la moitié des données mondiales se trouveront dans le cloud, ce qui représente 100 zettaoctets. Cela représente 100 milliards de téraoctets de données. (Cybercrime Magazine - Page One For The Cybersecurity Industry)
- Un utilisateur moyen stocke 500 Go de données dans son espace personnel pour les documents texte uniquement, l'utilisateur moyen stocke 130 Go dans le Cloud, ce qui équivaut à 10 millions de papiers. Imaginez maintenant la quantité potentielle de preuves qui s'y cachent. (pCloud - The Most Secure Cloud Storage)
- Facebook Messenger est l'une des principales plateformes de messagerie aux États-Unis, avec plus de 2 millions de téléchargements mensuels. Plus de 20 milliards de messages sont échangés entre entreprises et utilisateurs chaque mois sur Facebook Messenger. (Accueil - Review42)

