cellebrite
delivering mobile expertise

RELEASE NOTES

Version 5.2 | August 2016

UFED CLOUD ANALYZER

HIGHLIGHTS

Cloud data sources represent a virtual goldmine of potential evidence for digital forensic investigators. Together with digital device data, they often capture the details and critical connections investigators need to solve crimes. However, access remains a challenge. Roadblocks and red tape add time and significant cost to investigations. Cellebrite continues to deliver the most innovative and up-to-date Cloud-data solutions. UFED Cloud Analyzer's latest release – Version 5.2 – is no different. This unique and powerful investigative tool continues to dive deeper and deeper into the Cloud. With Version 5.2, you can:

- Access treasure trove of subjects' backed up data stored on multiple Apple devices – even when devices are locked or unobtainable.
- Reveal user's credentials to expand access to critical evidence located on user's account, as webpages and additional cloud services.
- Enhance investigations with insights extracted from WhatsApp conversations held on Android mobile devices, including chat history, call log history and contacts.

GAIN ACCESS TO SUBJECT'S DATA STORED ON APPLE DEVICES

Use subject's user credentials and login information from PC to reveal critical evidence and insights from a multitude of user's iPhone devices – even when the device remains locked or remains with the user.

REVEAL USER'S CREDENTIALS AND GAIN ACCESS TO CRITICAL INSIGHTS

Gain access to username and password for websites and cloud servers that may contain the 'smoking gun' needed for an investigation.

ENHANCE INVESTIGATIONS WITH CRITICAL EVIDENCE EXTRACTED FROM WHATSAPP BACKUP

On an Android device the backup is stored on Google Drive and thus is now accessible using UFED Cloud Analyzer – version 5.2. Enhance investigations today – with access to critical evidence stored in the backup.

GAIN ACCESS TO TREASURE TROVE OF SUBJECT'S DATA STORED ON MULTIPLE APPLE DEVICES

Apple users have various options to backup their devices, including via iTunes or iCloud. In this context, iTunes is a local backup of the device done when the user connects their device to a trusted PC; iCloud is a remote backup of the device stored on Apples servers – if the user decides to backup the information to iCloud, the backup may be initiated when the user is connected to Wi-Fi – anytime and anywhere.

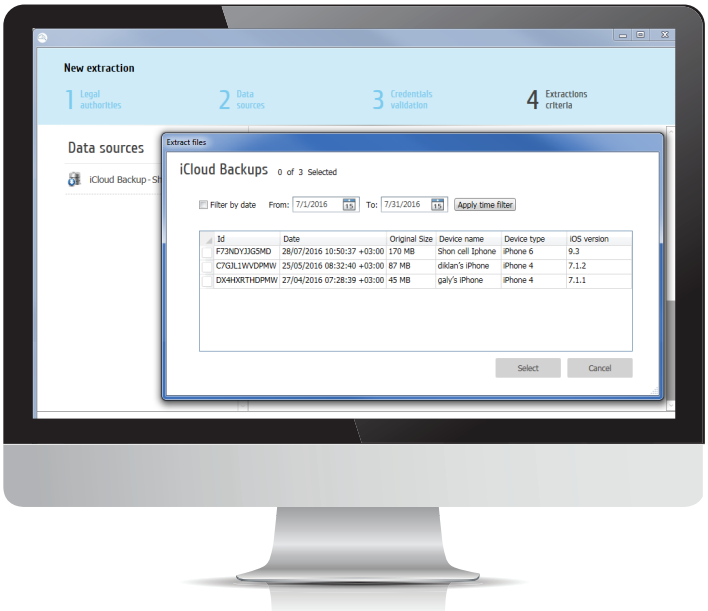
REVEAL CRITICAL MOBILE INSIGHTS WITH CREDENTIALS GAINED FROM SUBJECT'S PC

With UFED Cloud Analyzer 5.2, you may now use the iCloud username and password or login information from a PC to gain access to any subject's device backup stored on Apple's iCloud, which contains a treasure trove of critical information needed for investigations. This includes nearly all data and settings stored on the device, particularly text messages, call logs, application information, device settings and much more.

By combining this powerful backup extraction capability with the iCloud data extraction capability introduced in version 5.1, examiners can be sure that they are collecting the majority of data related to the subject's devices and are not leaving any Apple device behind.

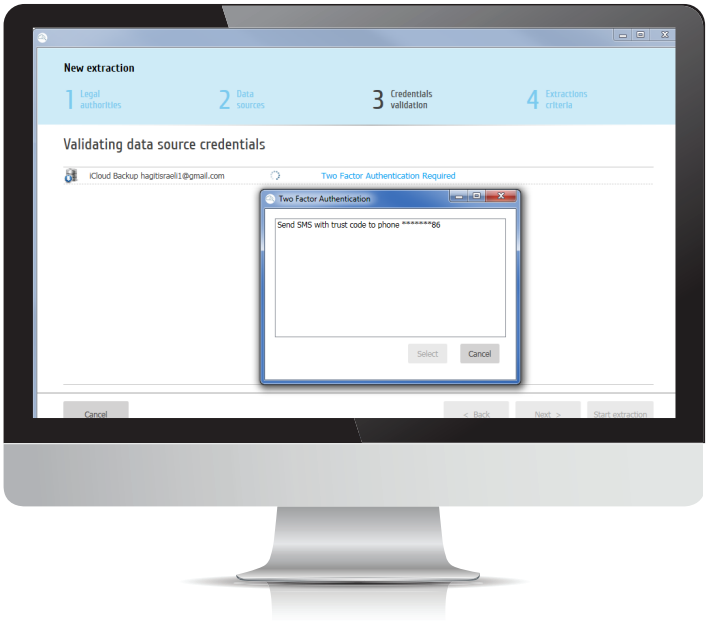
EXPOSE DELETED DATA WITH SNAPSHOT GAINED FROM SUBJECT'S iCLOUD BACKUPS

In addition, Apple stores data in the cloud in several incremental snapshots. This means that the examiner may have access to the last three backups performed by the user and can look for information that was subsequently deleted in between those snapshots.



EFFECTIVELY COUNTER TWO-FACTOR AUTHENTICATION WITH iCLOUD CREDENTIALS

UFED Cloud Analyzer – version 5.2 – further enables you with the ability to access the device backup – even when the user has applied the two-factor authentication. When using the iCloud credentials to access the backup, the examiner may select if they would like to send the second factor of authentication and to which device. The device may be selected from a list of authorized devices previously defined by the user. This gives the examiner better control of the process and lowers the amount of alerts sent to the user and their other devices.



REVEAL USER'S CREDENTIALS AND GAIN ACCESS TO CRITICAL INSIGHTS

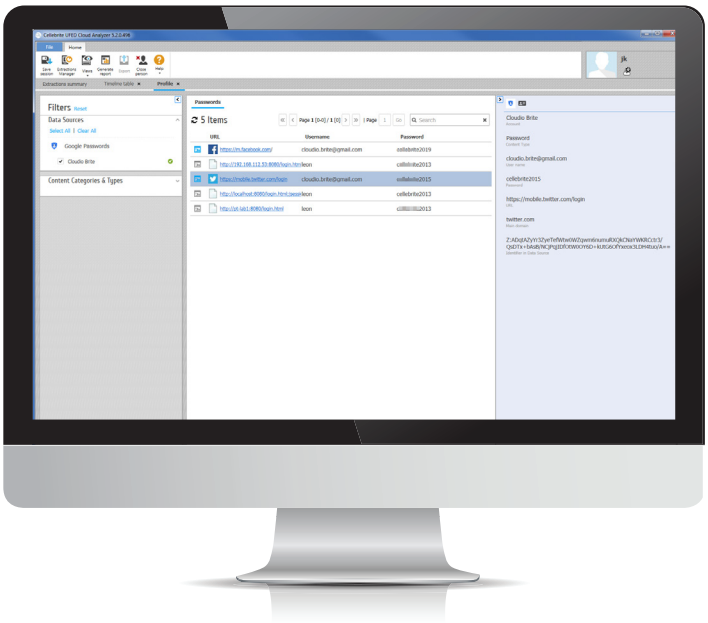
With UFED Cloud Analyzer's latest release, extract credentials (usernames and passwords) the user saved from their chrome browser or from their Android device. With this in mind, Version 5.2 allows you to gain access to username and password for websites and cloud service that may contain information needed for the investigation. It further enables you to identify a lexicon of the subject's password that might be handy when trying to reveal a credential to a website or cloud service the user was using. These new and innovative capabilities significantly accelerate investigations by providing you with the most information as possible.

How does it work? Google offers its users a service that stores username(s) and password(s) for a multitude of websites and cloud services – located in the Google Cloud. This information may be accessed from the user's Google account if either of the following are true:

- The user is signed into Chrome and are syncing passwords
- The user is using Google Smart Lock for passwords on Android

Once user credentials are available, the examiner may use this information to download additional content using UFED Cloud Analyzer. Alternatively, the examiner may decide to manually access the cloud service.

To gain access to the Google password service, the examiner may either use the Google credentials or Google login information taken from the mobile device.



OBTAIN CRITICAL EVIDENCE AND INSIGHTS FROM SUBJECT'S WHATSAPP CONVERSATIONS

WhatsApp is the leading instant messaging application in the world. The application provides 1 billion users with the ability to communicate via text messages, photos, videos and calls. While the conversations are stored locally on the device, a WhatsApp user may backup their content to the cloud and later restore it on new devices. On an Android device, the backup is stored on Google Drive and thus is accessible using UFED Cloud Analyzer. The backup contains all relevant information, including chat history and call log history. With this in mind, the frequency of the backup is user dependent.