Release Version 7.7: UFED Cloud Analyzer

March 2019

HIGHLIGHTS

As people around the world migrate their professional communication onto mobile and cloud business apps, richer data profiles and activity histories become available to digital investigators that legally access both the personal and professional lives of suspects and victims. Having the ability to extract all conversations generated by a mobile device can become vital evidence in an investigation.

With this version, Cellebrite delivers access to shared files and instant messaging data from Slack, the popular communication tool of the business community.

As 40% of US citizens are likely to use a ride-hailing app, it has become important for investigators to be able to account for the transportation activity of passengers and drivers involved in a crime. UFED Cloud Analyzer now supports Lyft, the second biggest ridesharing app to UBER, which is already also supported in version 7.6.

With the constant expansion of Google apps, come an increased variety of digital data a suspect or victim can spread across several applications. With support for Google Keep and Google My Activity, come the possibilities to gain insight into the notes and search logs of criminals or victims.

Slack App: For professional communication in the workplace and on the go

Slack, the business community messaging app for organizational communication has 10M+ daily active users in 150+ countries. With the average user spending 10 hours per weekday on the platform, Slack is quickly becoming the identity layer of enterprises. With this functionality, Slack can act as a provider of identity to login into other apps.

The communication ecosystem that Slack data retrieval covers consists of instant messages, files, user data and more.

Lyft App: Ridesharing

Operating in over 300 cities in the US and Canada, Lyft is the second largest ridesharing contender next to UBER, offering the similar service of matching private drivers with passengers needing one-off rides to specified destinations. With 4 billion rides completed in 2018, Lyft accounts for 22% of the ridesharing market.

As 35% of Generation Z and 31% of Millennials in the US use ride-hailing apps, crimes that involve this demographic could benefit from tapping into the digital data contained in the Lyft app. The supported data extraction will include passenger and driver profile data, travel logs and payment details.

Google Keep: Checklist and note-taking app

Google Keep users save notes, create reminders and store their to-do lists on the app that features Google Docs integration. Retrievable data includes notes, lists, photos and more.

Google My Activity: Activity logs recording Google app engagement

Personal activity from a range of Google apps is stored in the form of time-stamped logs which is valuable to investigations and only exists in the cloud. Investigators will be able to track activity from multiple devices attributed to one user such as searches, applications opened, websites visited, and videos watched.

With full data access to Google My Activity history, examiners will have a comprehensive view of a suspect's or victim's digital behavior on multiple devices leading up to, during and after a crime is commited.

General Enhancements:

2FA support for Instagram:

UFED Cloud Analyzer now overcomes two-factor authentication for Instagram users who have chosen to receive a text message (SMS) code to their mobile phone to log in.

Facebook activity log extraction is now supported by PC collector

Sources:

Slack:

- https://techcrunch.com/2016/04/01/rocketship-emoji/
- https://expandedramblings.com/index.php/slack-statistics/
- https://slack.com/about

Lyft:

- https://www.statista.com/topics/4919/lyft/
- https://www.statista.com/statistics/934529/ride-hailing-usage-in-the-past-year-united-states-by-generation/

Google Keep:

- https://www.tech21century.com/google-keep-update-includes-two-new-features/
- https://9to5google.com/guides/google-keep/