

Release Version 7.6: UFED Cloud Analyzer

January 2019

HIGHLIGHTS

Investigators and examiners are now benefiting from comprehensive access to a wide range of digital evidence as smartphones become the personal gateway to other digital devices and online accounts in the cloud.

With the release of UFED Cloud Analyzer 7.6, forensics examiners can retrieve digital evidence from routers, the UBER app, mobile web browsers and more.

Consumer demand is being driven by cutting-edge experiences as a result of innovative cameras, sensors, and apps. Unfortunately, criminals have begun to exploit this user-friendly remote-piloted technology that allows them to easily engage in espionage, smuggling and drug delivery at borders, prisons and city neighborhoods.

With 3M drivers and 75M passengers**, UBER is driving past the 600 city mark in 65 countries as it expands its service territory. With high user engagement comes valuable travel data for both passengers and drivers.

And due to popular request from Germany, we added data retrieval from T-Mobile's MagentaCloud app that offers phone data backup services to their 75M customers***. Potential digital evidence residing in the cloud can be retrieved by investigators needing historical data from the mobile device of a suspect or victim.



UBER App: Passenger & Driver Profile Data, Travel logs and Payment Details

Uber, the #1 ride-sharing app², allows its users to enjoy an easy and economical way to travel by car to their destination of choice. With the addition of Uber as a data source in UFED Cloud Analyzer 7.6, investigators gain valuable data including passenger and driver profile data, pick-up and drop-off location logs, and the last 4 digits of a user's credit card.

UFED Cloud Analyzer 7.6 supports retrieval of tokens from a mobile device to access the account, and credit card details that new users are required to fill in on their first login. As the passenger chooses their pickup location, desired destination, and available driver, each journey is well documented. Recorded routes are aggregated and then categorized by favorite destinations.

The driver's information includes the name and photo identification.

With the user tokens, examiners can capture forensically sound evidence which can be relevant when faced with a possible missing person case, or when attempting to place a suspect or victim at a certain location in time.



Password Collector: Mobile Web Browser

UFED Cloud Analyzer 7.6 extends its password collector functionality to include passwords saved on mobile web browsers. Examiners can now retrieve password logins from various sites using the password collector to collect the maximum amount of data about a suspect or victim.

This is accomplished by leveraging a person's login details which have been saved in their browser when they access their online accounts.



Capturing Router Data

Up until now, collecting data from routers has been a very manual process as investigators had to browse and collect information screen by screen. This inefficient method was not always forensically sound.

With the WebCapture, capture user and device details from routers by the most popular brands. WIFI passwords, as well as a list of connected devices, are now retrievable in a forensically sound manner.





MagentaCloud App

The MagentaCloud App from Telekom (T-mobile) Germany delivers storage and backup services to their customers' for phone data backup that includes sent and received files.

Telekom customers receive 25GB of free online storage to upload photos, videos, and documents. Users access their account with their Telekom login, as well as an optional four-digit PIN.

Law enforcement officials can often wait weeks to get requested data back from service providers, and when the data does finally arrive it is not the full amount. With this version, examiners who already have a subpoena can immediately access the MagentaCloud app data using tokens retrieved from the mobile device or user credentials.

Enhancements

Amazon Captcha verification is now supported for both Amazon shopping and Alexa services. This means that if a user is presented with a popup or page to be completed, during the login process, the popup screen is now displayed within UFED Cloud Analyzer 7.6.

This version now supports two-factor authentication for the cryptocurrency app, Coinbase.

Sources:

**<https://expandedramblings.com/index.php/uber-statistics/>

***<https://expandedramblings.com/index.php/t-mobile-statistics/>

1 [https://en.wikipedia.org/wiki/DJI_\[company\]](https://en.wikipedia.org/wiki/DJI_[company])

2 <https://blog.secondmeasure.com/2018/12/17/rideshare-industry-overview/>

