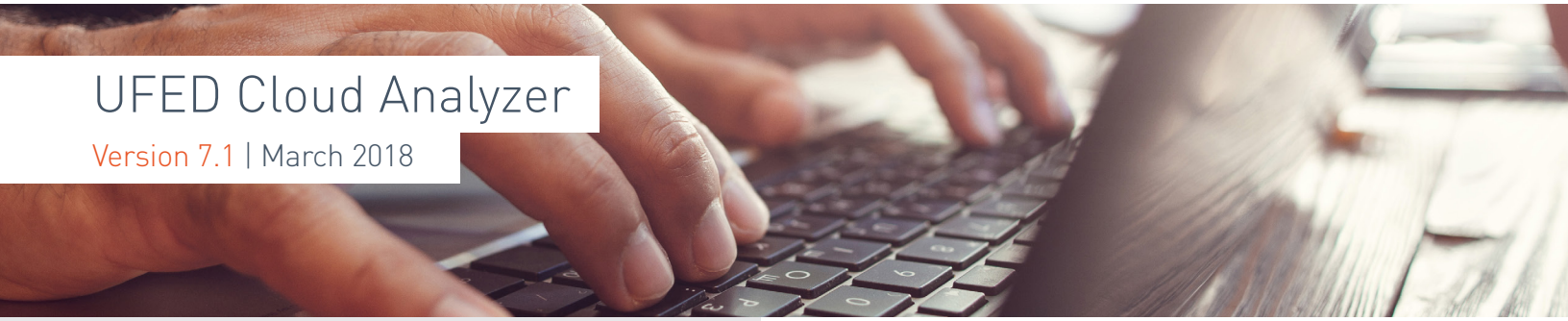
Cellebrite Digital intelligence for a safer world

Release notes



UFED Cloud Analyzer

Version 7.1 | March 2018

Highlights

UFED Cloud Analyzer 7.1 presents Web Capture

Generate new leads and quickly corroborate statements and findings with evidence collected from any HTML-based web page using UFED Cloud Analyzer's new Web Capture function. Using the Web Capture, you can collect digital evidence from many data sources, even those not yet supported by UFED Cloud Analyzer.

Web Capture enables you to:

- Automatically collect and hash digital evidence such as media files, recover data and take snapshots of entire web sites.
  - > Supported technologies include: WebM / ogg, chat sites, YouTube Videos, Render Style in JavaScript, vBulletin 5, and more
- Focus web searches with customizable capture settings, such as depth level, page downloads and specific URLs
- Easily produce PDF reports that contain screenshots and comments - can be further analyzed with other data

Note: An update on The PC Cloud Collector

The PC Cloud Collector is now supported for Mac and Windows 10. The PC Cloud Collector is an independent tool that creates tokens from a suspect's PC using the cookies in the browsers and the applications that are installed on that PC.

How to recover critical data from data sources and websites using Web Capture

Identify data source

- Select the website you want to recover data from
- Some website's may require user credentials to access private data

Start using Web Capture

- Open UFED Cloud Analyzer
- Select Person Web Capture
- Enter the website / data source
- Select prefered capture settings
- Start capturing

Analyze

- Review the captured data and screen shots using any of the two views: Files or Pages

Share

- Share your findings and generate a PDF report and proceed with your investigation

Example using FitBit app

Identify data source:

FitBit products are activity trackers, wireless-enabled wearable technology devices that measure data such as the number of steps walked, heart rate, quality of sleep, steps climbed, and other personal metrics involved in fitness. FitBit has a user base of over 10 million people, and is popular among a variety of ages. You can view Fitbit information online, on a mobile device, or through the desktop application.

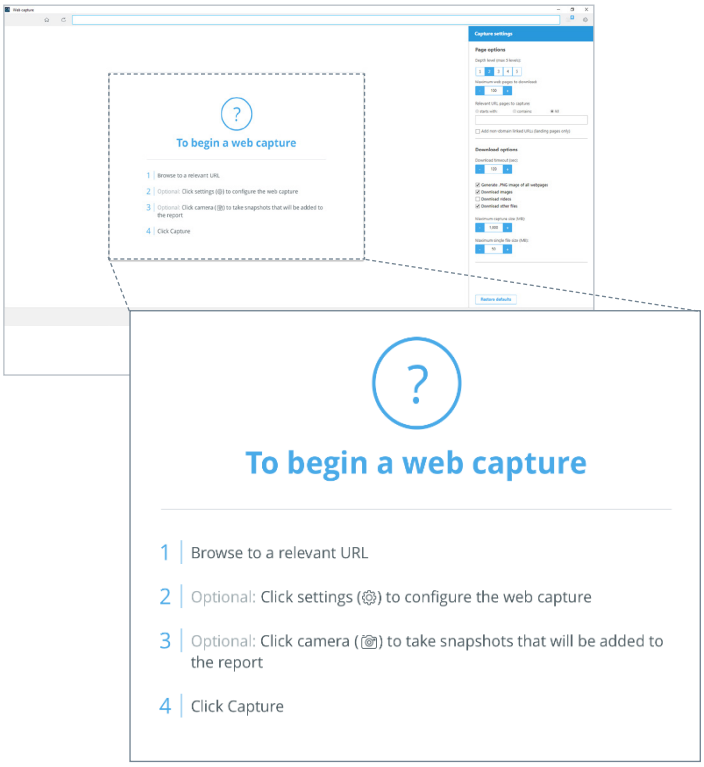
Up to date FitBit devices have been involved in several case investigations. Analyzing the artifacts generated by the applications are important.

Assuming that you have a case involving a FitBit device, you can use Web Capture to capture data from the FitBit user's account.

Example using FitBit app (cont...)

Start using Web Capture:

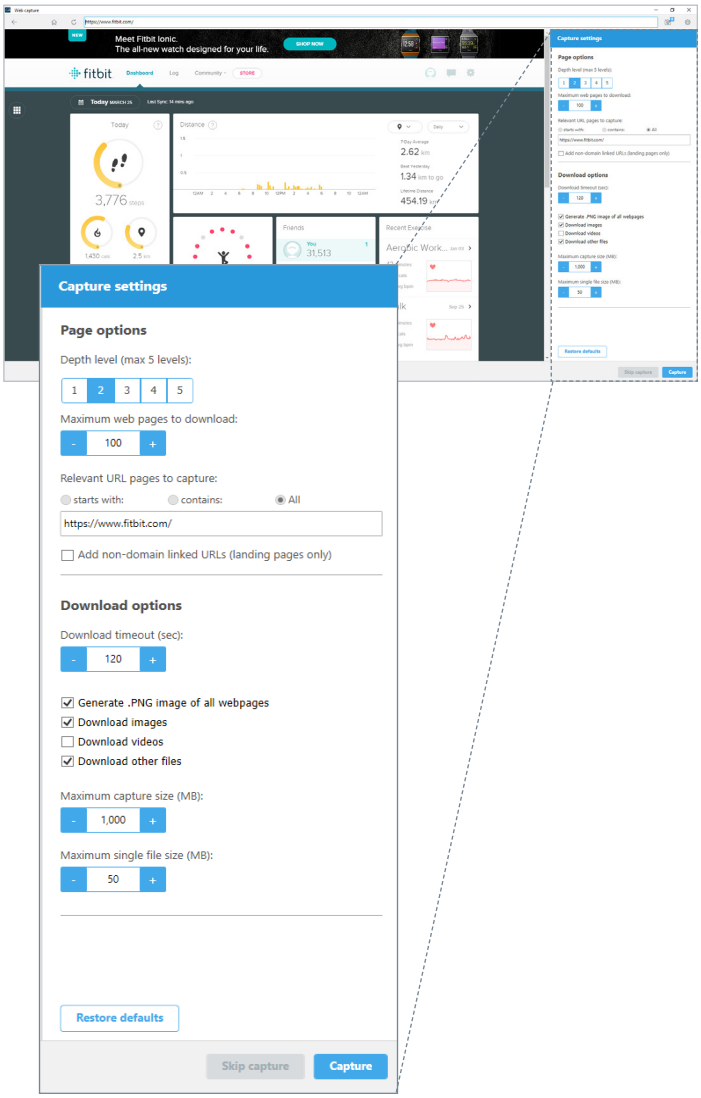
You will need credentials to the FitBit website to capture private user data.



Select preferred capture settings:

Now you can start the capturing process and the preservation of all activities data.

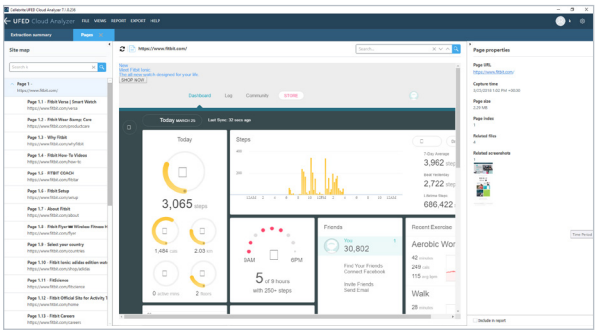
Select the desired capture settings such as page depth (Number of levels within the website page to include), maximum number of pages, set a maximum wait time for download per page before timing out etc. You can even take snapshots during the capture process. These snapshots can be added to the web capture report.



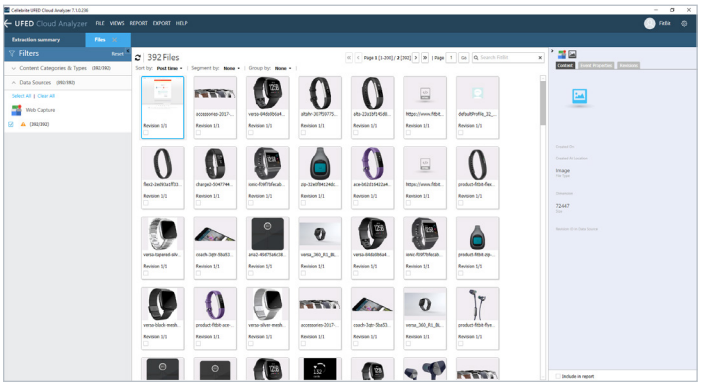
Analyze:

Review the captured data and screen shots. You can see below that the user's personal activities have been captured including Timestamps, Locations etc. This information can be of great value to your investigation.

Pages:



Files:



Share:

Generate a PDF report and share your findings with other team members and proceed with your investigation.