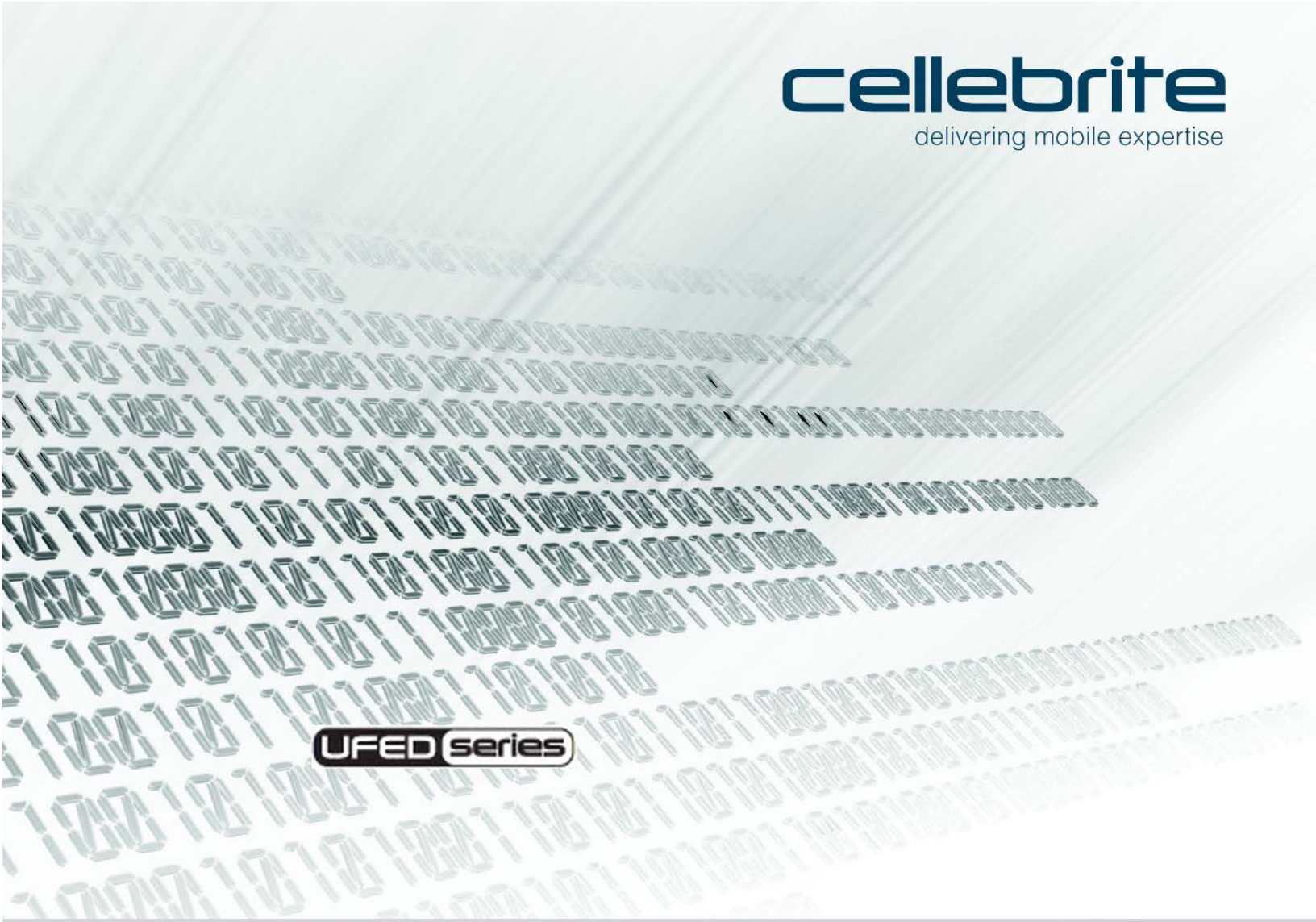



# UFED Touch/4PC and UFED Physical/Logical Analyzer version 4.2

## Release Notes

May 2015

# Contents

# Release highlights

## Decoding

### Apps support

New and updated applications for Android devices:

- 9 new apps: BeeTalk, ChatOn, Path, Nimbuzz, Tango, textPlus, Tumblr, UC Browser, and Whisper.
- 40 updated Android apps.
- Waze locations for Android devices – Location information is now decoded for Android devices and displayed as part of the device's locations.

New and updated applications for iOS devices:

- 10 new apps: BeeTalk, ChatOn, Nimbuzz, Path, Tango, textPlus, Threema, Tumblr, UC Browser, and Whisper.
- 63 updated iOS apps.

New and updated applications for Windows Phone devices:

- 9 new apps: Facebook, Facebook Messenger, Skype, Kik, Waze, Voxer, ooVoo, Odnoklassniki, and Whatsapp.

### General

- Decryption of KeepSafe and WeChat applications.
- Decoding support for WhatsApp VOIP call logs on Android and iOS devices.
- New WhatsApp timestamps for iOS, Android and BlackBerry 10 devices. View the Read, Delivered and Played timestamps of outgoing WhatsApp message.
- Twitter group chat messages are now presented as part of Chats in the project tree.

### Device support

- Physical extraction while bypassing lock, and decoding from 58 LG Android devices, including:
  LG GSM LG-H810 G4, LG-H811 G4, LG-D850 G3, LG-F300K Optimus Vu III, LG-F350S G Pro 2
  LG CDMA LG-VS985 G3, LG-VS415PP Optimus Zone 2, LS995 G Flex, LS660 Tribute 4G

  **Note:** Support for LG Android devices that were released with Android version 4.2.x and above.

- Disable user lock for 57 LG Android devices including:
  LG GSM LG-H810 G4, LG-H811 G4, LG-D850 G3, LG-F300K Optimus Vu III, LG-F350S G Pro 2
  LG CDMA LG-VS985 G3, LG-VS415PP Optimus Zone 2, LS995 G Flex, LS660 Tribute 4G

  **Note:** Support for LG Android devices that were released with Android version 4.2.x and above.

- Disable user lock for 159 Samsung Android devices (using SPR and SPM methods), including:
  Samsung GSM SM-G900F Galaxy S5, SM-G9009D GALAXY S5, SM-G800A Galaxy S5 Mini, GT-S7582 Galaxy S Duos 2, GT-i9506 Galaxy S4, SHV-E300K Galaxy S4, GT-I9192 Galaxy S4 Mini Duos, GT-S7560 Galaxy Trend, SCH-P709E Galaxy Mega Plus, SHV-E300K Galaxy S4, SM-N910A Galaxy Note 4, SM-N900 Galaxy Note 3
  Samsung CDMA SCH-I535 Galaxy S III
  Samsung Tablet SM-T330NU Galaxy Tab 4 8.0

  Note: Supported for selected models, depending on the device's firmware version. Not all firmware versions are supported.

- Decryption of encrypted physical extractions from Android devices 4.2 and below, with a known password. This includes generic Android and Samsung devices.
- File system extraction and decryption of BlackBerry 10.x Backup with known BlackBerry ID credentials. Retrieve the key via BlackBerry backup server and decrypt the backup file.
- Decoding of BlackBerry 10 device information. Username, device model, PIN, IMEI, device name etc.
- Decoding of Windows Phone device information – IMEI, IMSI, MEID, mobile operator ID, country, Mac address, OS version etc.
- Physical extraction and decoding for BB5 RAPUv21 family: Asha 300 (RM-781), Asha 302 (RM-813), Asha 311 (RM-714), 700 Benji (RM-670), and 701 (RM-675).
- JTAG decoding for Samsung SPH-M270 devices.
- Data decoding from additional UMX devices: MXC-450, MXC-560, MXC-570, MXC-628, MXE-635a.
- Data decoding from additional Samsung E1200 series.
- Decoding of EnCase iTunes backup extractions.

For more information on decoding capabilities, see UFED Physical/Logical Analyzer – Decoding (page 7).

## Functionality

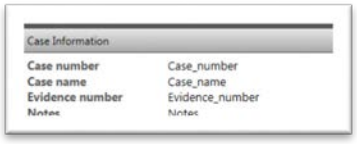
- Offline maps – View extracted locations using offline maps even without an Internet connection. The locations are presented with an icon displaying the location type. The maps function is free of charge. The maps package installation is required and it is available to UFED Physical/Logical Analyzer users with a valid license.
- View event information per location on the map – Zoom in for locations on the map and view related events on the right pane. Map view for all location types under device locations.

### Data file improvements

- Filtering of attachments – Enhanced ability to view and filter attachments within data files, locate the associated attachment event and view its metadata and location information on the right pane.

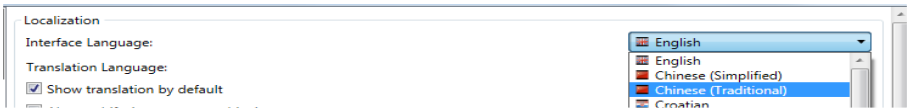
- **Right pane for data files** – View the file, its metadata and location information on the right pane.
- **Video Thumbnails –** View a frame of all video files in video table view. To view the video, you can double-click on the video or play it from the right pane.
- **Control images thumbnails –** You can now control the size of image thumbnail in thumbnail view.


- **Sort unknown file formats** – All unknown file formats or undefined file extensions will be displayed in the Uncategorized node in the tree.
- **Link between analyzed data, timeline and locations** – Easily jump from an event in any of the analyzed data tables, to its place in the timeline table, and from location information to its source event or timeline.
- **Timeline improvements** – Indication and filtering of location and attachments per data entry in the timeline view.
- **Export account package –** UFED Physical Analyzer can extract user account information (account package), which can then be imported into UFED Cloud Analyzer.
- **Case Information** – Case information settings are saved with the project or set when generating reports. You can now view case information extracted from UFDR reports in the "Extraction Summary" page.



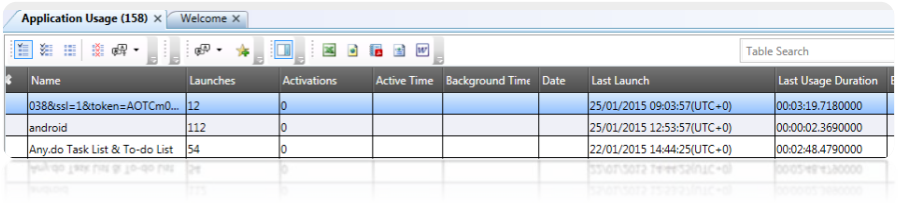

- **Create bookmarks for multiple items** – An entity bookmark is a quick reference pointer that you can create for individual items. Now enhanced with the ability to create, delete or remove multiple bookmarks.
- **Number of chat messages in the project tree –** View the number of messages per chat in the project tree


- **Traditional Chinese support** – New interface language for Traditional Chinese.



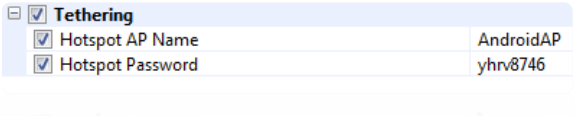
- **Enable/disable daylight saving time** – Ability to enable/disable the daylight saving time adjustment.


- **Application usage enhancements** – View Last Launch time stamp (indication of the latest usage time of the application) and Last Usage Duration (duration of application usage) as part of application usage data under Analyzed data.




- **Decoding of unsorted block image file system for Android devices –** As part of the physical decoding process, the user data partition in a new flash file system (UBIFS) is now decoded.

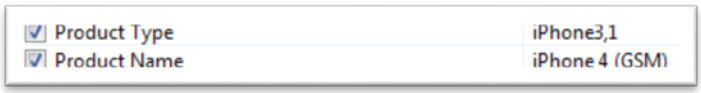
- **Tethering ID decoding for Android devices –** View the decoded Tethering ID and password under Device info.




- **Extract IPs of VoIP calls oriented applications for Android and iOS devices –** View the IPs used for calls as part of the device information and call log model view. In the reports output, the IP will be displayed in the Parties column.

- **Installed applications enhancements for Android and Windows Phone devices –** View the version number of installed Android applications.

- **Product name indication for iOS devices –** You can view the product name, in addition to product type information under Device info.




- **Wireless networks for Windows Phone 8 devices** – Wireless information is now located in Wireless Networks under Analyzed data.

- **New files suffix (Data files settings) -** Audio: .amr, .ogg; Video: .caf, .mp4; Configuration: .conf, and .config

For more information on functionality, see *UFED Physical/Logical Analyzer – Functionality* (page 11).

## Reporting

- **UFED Reader application when generating UFDR** – Easily share UFDR reports with authorized persons using the UFED Reader. You can now include the UFED Reader executable within the report output folder.

- **Entity bookmark table includes bookmark and item information** – In all report formats, the entity bookmark section now includes the bookmark itself and also the related item/record.

- **Locations info of chat messages in UI reports –** You can view the number of locations per chat and also export location data for chat messages in all report formats.

## Python API

- Improved Python API documentation by providing more information on the SQLite parser. Learn how to access and read the tables and their content for SQLite databases, including the sample codes for several applications.

# UFED Physical/Logical Analyzer – Decoding

- **Decryption of encrypted physical extractions from Android devices 4.2 and below with a known password** - the raw extraction is encrypted by default. You have the option to encrypt the devices (encryption is enabled by default). Cellebrite has the ability to decrypt encrypted extractions, remove the encryption and decode the data from the mobile device.

- **Extraction and decryption of BlackBerry 10 Backup with known BlackBerry ID credentials** – The ability to extract backup data of BlackBerry devices as part of file system extraction. Via UFED Physical Analyzer, retrieve a known BlackBerry ID credentials and decrypt the backup data from BlackBerry devices.
  **How to use:** Open a file system extraction of a BlackBerry 10 device, during the decoding process, a window is displayed:

  Enter the BlackBerry ID credentials and select **Get Backup key** (to retrieve a key, an Internet connection is required). You can save the key for future usage by selecting the **Save** button.
  If an Internet connection is not available, you can retrieve a key on any instance of Physical Analyzer connected to the Internet. Go to **Tools** and select **Retrieve BlackBerry 10 Backup Key**. Enter the BlackBerry ID credentials and select **Get Backup key**. Click **Save** and load the key from the UFED Physical Analyzer disconnected from the network to continue with the decoding process.

# New and updated apps for Android devices

## 9 New Android apps

- **BeeTalk -** Decoding of Chats, Contacts and User Accounts
- **ChatOn -** Decoding of Chats, Contacts and User Accounts
- **Nimbuzz -** Decoding of Contacts
- **Path -** Decoding of Contacts, Instant Messages and User Accounts
- **Tango -** Decoding of Chats, Contacts and User Accounts
- **textPlus -** Decoding of Chats, Contacts and User Accounts
- **Tumblr -** Decoding of Chats, Contacts and User Accounts
- **UC Browser -** Decoding of Bookmarks and Web History
- **Whisper -** Decoding of Chats, Contacts and User Accounts

## 40 Updated Android apps

Any.DO 3.0.3, 3.1.5, 3.2.5, 3.26; Badoo 2.53.7, 2.55.8, 2.56.9, 4.0.4; BBM 2.6.0.30, 2.7.0.23;
Chrome 39.0.2171.59, 39.0.2171.93, 40.0.2214.109, 41.0.2272.96;
Dropbox 2.4.6.8, 2.4.7.14, 2.4.7.18, 2.4.9.00; Evernote 6.2, 6.3.2.2, 6.3.3.1, 7.0.1;
Facebook 22.0.0.15.13, 24.0.0.30.15, 26.0.0.22.16, 29.0.0.23.13;
Facebook Messenger 17.0.0.16.14, 18.0.0.27.14, 24.0.017.13; Firefox 33.1, 34.01, 35.01;
Gmail 5.0, 5.0.1; Google Maps 9.1.0, 9.2.0, 9.3.0, 9.6.0;
Google+ 4.7.1.79583515, 4.8.0.81189390, 4.9.0.84567213, 5.1.1.88991728;
Hangouts 2.5.81636427, 2.5.83281670, 3.0.87531466; ICQ 5.8, 5.11, 5.12;
Instagram 6.10.1, 6.12.1, 6.14.1, 6.18.0; KakaoTalk 4.6.9, 4.7.1, 4.7.6, 4.8.0;
Kik Messenger 7.8.1.141, 7.9.0.1.143, 7.10.1.176, 8.1.0.4; LINE 4.7.1, 4.9.1, 4.9.2, 5.0.4;
LinkedIn 3.4.4, 3.4.5, 3.4.7; Mail.Ru 2.5.0.8258, 2.5.2.8498, 2.5.3.8500, 3.0.1.9598;
mypeople 4.8.3, 4.8.4; Navfree 2.3.68; Odnoklassniki 4.1.4, 4.1.5; ooVoo 2.2.5, 2.2.6, 2.2.8, 2.3.1;
Opera Mini 7.6.2, 7.6.3, 7.6.4; Opera Mobile 26.0.1656.87080, 27.0.1698.88647;
QQ 5.2.1, 5.3.1, 5.4.1; Skype 5.1.0.56619, 5.1.0.58677, 5.2.0.61097, 5.2.0.62296;
Snapchat 8.0.0, 8.1.2, 9.1.0.0, 9.4.1.0; Sygic 14.6.8, 14.7.4, 14.7.7;
Telegram Messenger 2.0.5, 2.3.2, 2.4.1, 2.6.1; TigerText 5.0.119, 5.0.121; Truecaller 4.5.1, 5.01, 5.1;
Twitter 5.35.0, 5.40.0, 5.45.0; Viber 5.1.1.42, 5.2.1.36; Vkontakte 3.9.1, 3.10.1;
Voxer 2.2.3.014121, 2.4.1.014238, 2.4.5.014299; Waze 3.9.3.0; WeChat 6.0.0.68, 6.02, 6.1.0.65;
WhatsApp 2.11.476, 2.11.505, 2.12.5; Yahoo Mail 4.8.4

# New and updated apps for iOS devices

## 10 new iOS apps

- **BeeTalk -** Decoding of Chats, Contacts and User Accounts
- **ChatOn -** Decoding of Chats, Contacts and User Accounts
- **Nimbuzz -** Decoding of Contacts
- **Path -** Decoding of Contacts, Instant Messages and User Accounts
- **Tango -** Decoding of Chats, Contacts and User Accounts
- **textPlus -** Decoding of Chats, Contacts and User Accounts
- **Threema -** Decoding of Chats, Contacts and User Accounts
- **Tumblr -** Decoding of User Accounts
- **UC Browser -** Decoding of Bookmarks and Web History
- **Whisper -** Decoding of Chats, Contacts and User Accounts

## 63 updated iOS apps

iOS 7x updated apps:

Any.DO 2.02, 2.1.3, 2.3.0; Badoo 3.15.1, 3.17.0, 3.19.0; BBM 2.7.0.69;
Chrome 39.0.2171.50, 40.0.2214.69; Dropbox 3.8; Evernote 7.6.3, 7.6.4, 7.6.6; Facebook 21, 23.1, 27;
Facebook Messenger 18, 19.1, 23.1; Foursquare 8.5.1, 8.9.1; Gmail 4; Google Maps 4.1.1, 4.8.3;
Google+ 4.7.4.46151, 4.8.0.48043, 4.8.3; Hangouts 2.6.0, 3.1.0; HeyTell 3.2.5; Instagram 6.4.1, 6.5.3, 6.8.0;
KakaoTalk 4.4.0, 4.5.2, 4.6.1; KeepSafe 5.3.3, 5.3.6; Kik Messenger 7.9.0, 7.10.1; LINE 4.9.0, 4.9.2, 5.0.2;
LinkedIn 8.3, 8.4, 8.6; Mail.Ru 4.3.2; mysms 4.3.3; Odnoklassniki 4.4.2, 5.0.1, 5.1, 5.2;
ooVoo 2.2.7, 2.2.8, 2.2.9, 2.3.1; Opera Mini 9.0.0, 9.1.0, 9.2.0, 10.0.0; QQ 5.3.0.319, 5.4;
Skype 5.8.0.5.516, 5.11; Snapchat 8.0.1, 8.1.1, 9.1.1, 9.4.0; Telegram Messenger 2.6, 2.7.2, 2.8, 2.9, 2.11;
TextNow 5.2.3; TrueCaller 4.48, 5.1; Twitter 6.18, 6.21, 6.24.5; 5.7.6; Viber 5.2.1, 5.2.2; Vkontakte 2.2;
Voxer 3.5.5.4132; Waze 3.9.2; WeChat 6.0.1, 6.0.2, 6.1.1, 6.1.3; WhatsApp 2.11.16; Wickr 2.3.4, 2.4.0;
Yahoo Mail 3.2.10, 3.2.12, 3.2.14, 3.2.16

iOS 8x updated apps:

Any.DO 1.19.0, 2.1.0, 2.1.3, 2.2.0; Badoo 3.13.2, 3.14.1, 3.16.2; BBM 2.6.1.31, 2.5.0.26; Chrome 40.0.2214.73;
Evernote 7.6.3, 7.6.5; Garmin Connect 2.11; Instagram 6.1.4, 6.2.2, 6.4.1, 6.6.1; KakaoTalk 4.4.1, 4.5.6;
Kik Messenger 7.9.0, 7.10.1; LINE 4.9.0, 5.0.0; LinkedIn 8.3, 8.4; Nimbuzz 3.7.0, 4.0.0; Odnoklassniki 5.1.1;
ooVoo 2.2.8; Opera Mini 9.1.0; Skype 5.9, 5.10.0.371; Snapchat 8.1.1, 9.2.0; vBrowse 4.0;
Viber 5.2.1, 5.2.2; Vkontakte 2.2; Waze 3.9.1, 3.9.2; WeChat 6.1, 6.1.1; WhatsApp 2.11.14, 2.11.15.348;

# New and updated apps for Windows Phone devices

## 9 new Windows Phone apps

- Facebook - Decoding of Contacts and User Accounts.
- Facebook messenger- Decoding of Chats, Contacts and Locations.
- Kik- Decoding of Chats, Contacts, Passwords, and User Accounts.
- Odnoklassniki - Decoding of Chats, Contacts and User Accounts.
- OoVoo- Decoding of Calls, Chats, Contacts, and User Accounts.
- Skype- Decoding of Calls, Chats, Contacts, SMSs, and User Accounts.
- Voxer- Decoding of Chats, Contacts, Locations, and User Accounts
- Waze - Decoding of Locations and User Accounts.
- Whatsapp - Decoding of Chats, Contacts, Locations, and User Accounts.

# UFED Physical/Logical Analyzer – Functionality

- **Offline maps –** View locations on maps view even when an Internet connection is not available. You can choose to use online or offline maps when accessing the device location under Analyzed data. To change the default view, go to **Settings** > **General settings** > **Map** section and select the desired maps view (online or offline).

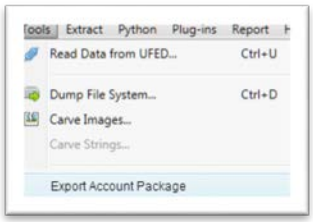
  **To download the offline maps package:** Login to MyCellebrite, then from the Download page, download the relevant Offline Maps Package (~40 GB).

  **To install the offline maps package:** In UFED Physical/Logical Analyzer, go to **Tools**, and select **Install Offline Maps Package**. In the installation window, load the Offline Maps Package. The loading process takes some time to complete. The offline maps are installed and ready.

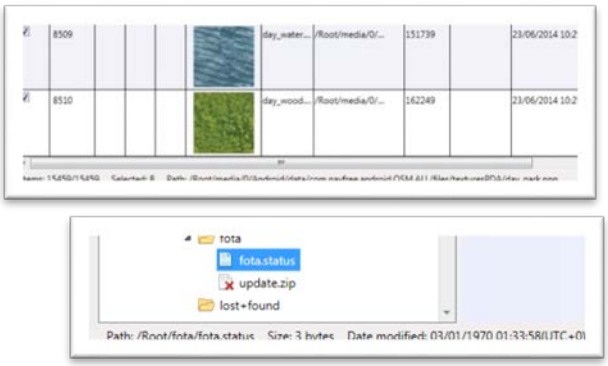
  **Note:** The offline maps feature uses a light Windows service that opens and listens to TCP port 3000. To use this feature, you need to select the **Install offline maps service** check box during the UFED Physical/Logical Analyzer installation process.

- **Indication and filtering of attachments** – Files (images, videos, audio, text, etc.) that were identified during the data analysis process are presented in the project tree under the Data Files category. You can now view and filter attachments within data files, locate the associated attachment event and view its metadata and location information on the right pane.

- **Export account package –** An account package is an export file that contains user account information. The account package can be imported into UFED Cloud Analyzer.




- **Status bar –** You can now view additional information in the status bar located below the file table, models table and thumbnail views. For example, the number of items presented, number of selected items and file path.




- **Access previous searches –** Your recent search activity, including "All projects search" and "table search" are now saved (up to 20), until you close the application.

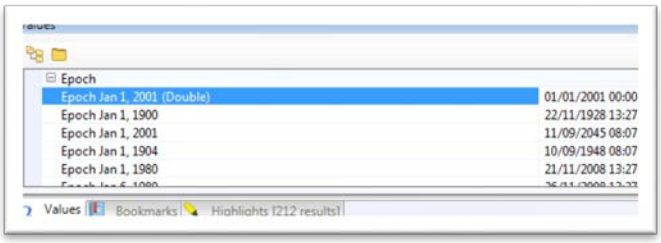
- **Maps and content presentation enhancements –** Zoom in for locations on the map view and view related event details on the right pane. View map view for all location types under Device locations.

- **Create bookmarks for multiple items** – An entity bookmark is a quick reference pointer that you can create for individual items. Now enhanced with the ability to create a single bookmark for multiple items. You can also delete/remove bookmark for multiple items.

  **To create a new bookmark for multiple items** – Select the items you want to bookmark, click the bookmark icon, complete the bookmark information and click OK. The bookmarked items records are marked with a bookmark icon.
  **To delete a bookmark from multiple items**: Select multiple items in the table, click **Delete bookmark**.

- **Hex View enhancements**:
  - The value base64 was added to values in Hex view (under Binary).


  - The value "Epoch Jan 1, 2001 (Double)" was added to values in Hex view (under Epoch) and also to the search options. This is a common representation of timestamps in iOS devices.



# Forensic methods

| Forensic methods | New | Total |
|---|---|---|
| Logical extraction | 191 | 7021 |
| Physical extraction* | 304 | 3447 |
| File system extraction | 331 | 3079 |
| Extract/disable user lock | 250 | 2008 |
| Total | 1076 | 15555 |

*Including GPS devices

# Supported devices

191 new devices supported for logical extraction

304 new devices supported for physical extraction

106 new devices supported for physical bypass

331 new devices supported for file system extraction

# Solved issues

- Fix for physical and file system extractions of Samsung Gusto 3 SM-B311V
- Fix for physical extraction of Samsung E1200R
- Decoding WhatsApp attachments for Android devices. When available, large images are now displayed instead of small thumbnails.

# Known limitations

- Due to the in-depth decoding process, it may take additional time to open iOS extractions.