Release Notes

UFED Physical Analyzer, UFED Logical Analyzer and Cellebrite Reader v7.19

May 2019

App support

- 139 updated application versions for iOS and Android devices
- Now supporting: 8,927 app versions

Get to more evidence on iOS devices

Upon access to the Apple iOS file system, which contains the KnowledgeC database, and following a full-file system extraction, you can now review data from three major sources that were previously inaccessible.

1. KnowledgeC – A key database which stores usage data and applications activities. Find valuable information about a user's activities on the device at any given time. Take a closer look at application activity – when was the app installed, opened, how was it invoked; all of the spotlight searches, when was the device locked and unlocked, when was it plugged into a charger or PC, and much more. This data is currently being decoded and presented under Device Events, and Application usage log models in UFED Physical Analyzer.

2. Health App – Apple's Health app (launched after iOS 8) tracks a user's physical activities and health based on data from a user's iPhone, Apple Watch and other apps. There were many cases where the Apple Health app data was used as evidence in many investigations.The health data is stored in the healthdb and healthdv-secure databases. This data is decoded and presented under Activities model, allowing you to track user activity such as body measurements, steps, running and walking and as well as location data.

3. Telegram support update (version 5.4.1 and later) – Telegram has made major database infrastructure changes. With UFED Physical Analyzer 7.19, you can now decode the following data:

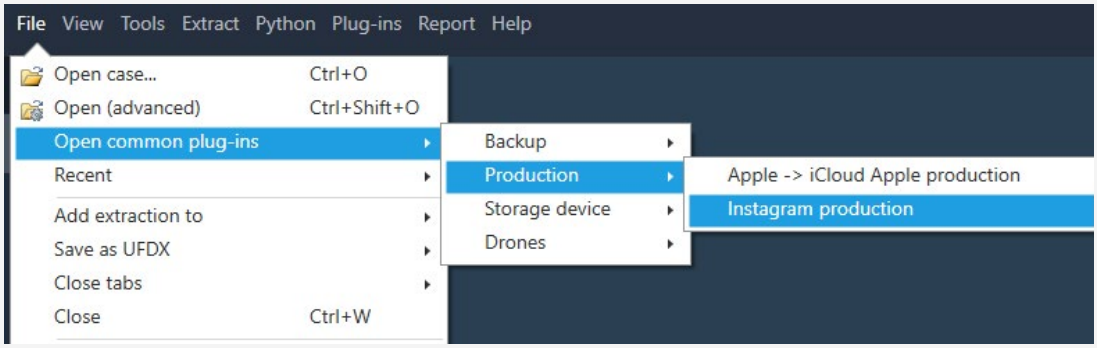
- User account (intact & deleted)
- Contacts (intact & deleted)
- Chat messages, including attachments, locations and system messages.
    - Message text
    - Message Attachments – partial support. Some attachments types are supported, for others there is only indication that there is attachment and its type
    - Message location
    - System message – partial support

Note: Data from KnowledgeC, the Health app and Telegram are only accessible via a full-file system extraction, usually performed with the help of Cellebrite Advanced Services or UFED Premium.

Uncover essential data from Instagram production sets to accelerate investigations

Instagram can produce a production set, that contains the same information that you may find in an Instagram application. Pending legal process, once examiners receive the Instagram production set back, it still needs additional handling to extract and decode all the information inside. In this version of UFED Physical Analyzer, you can process and decode an Instagram production set and gain access to images, messages and user account.

Use the "Open common plug-ins" to quickly decode Instagram production raw data.



Recover media files from the Snapchat feature, My Eyes Only (Memories)

Snapchat, the popular multimedia social application, has a feature called My Eyes Only (Memories). This feature allows its users to keep items private and hide content behind a passcode. The content is also encrypted.
Cellebrite has enhanced the support of this app for Android devices.
UFED Physical Analyzer 7.19 now enables decoding, decryption and recovery of media files kept in the 'My Eyes Only' gallery.

Additional enhancements

IMEI and IMSI from iOS devices

We now support the decoding of the IMEI and IMSI identifiers from an iPhone extraction (full file system).

SD Card E01

When performing SD card extraction in other tools, you can now decode the data in UFED Physical Analyzer.
To decode it, click on File / Open common plug-ins / Storage device / SD Card.

Solved Issues

- Failed to decode significant locations from a full file system extraction of iOS devices
- Manual screen capture/video presented in Timeline view
- When exporting emails into EML file format, subject and body include an extra prefix
- When exporting emails into EML file format, emails with no timestamp are mistakenly presented with current timestamp
- Failed to search two keywords with a space separator (global search)
- Missing user account information while decoding WeChat app for iOS devices
- Failed to decode data from QQ app for iOS devices
- Partial decoding of Quick Memo note app for Android devices
- Failed to decode Samsung E1200i device
- Failed to decode Alcatel 1050A device
- Failed to decode calls from the Nokia RM-607 device
- Failed to filter tags when running UFED Physical Analyzer on Win 10 in Turkish

New App versions

iOS: New and updated apps

62 updated apps	
Any.DO	4.29.6
Booking.com	19.0
Chrome	73.0.3683.68
Confide	8.3.1
Ctrip (Chinese)	8.2.2
DJI GO	3.1.54
Dropbox	136.2
Facebook	214.0
Facebook Messenger	208.0
Firefox	15.1
Flipboard	4.2.37
Gmail	6.0.190309
Google App	69.0
Google Docs	1.2019.12202
Google Drive	4.2019.12208
Google Duo	50.0
Google Maps	5.14
Google Translate	5.28.0
Google+	6.54.0
Grindr	5.5.0
GroupMe	5.29.2
Inbox	1.3.190212
Instagram	86.0
InstaMessage	3.1.3
Kakao Story	5.7.0
KakaoTalk	8.3.2
Keeper	14.3.0
KeepSafe	8.28.2
LinkedIn	9.1.125
Mail.Ru	9.18
MeetMe	13.14.0
Nike+ Run Club	5.23.0
Odnoklassniki	7.50.1
OkCupid	27.2.2
Pinterest	7.10
QQ Browser	9.1.1
Runtastic	9.2
Scruff	5.6027
Skout	6.6.0
Skype	8.42
Snapchat	10.53.5.9

Soma	2.0.14
Swarm	6.2.2
Tango	6.6.233830
Text Free Ultra Texting	11.37
Text Me!	3.16.6
Text Now	9.9.0
textPlus	7.4.8
Threema	4.1.3
TikTok	10.6.0
Tinder	10.9.1
Truecaller	10.7
Twitter	7.45
Viber	10.4
Vkontakte	5.12.2
Waze	4.49.2
Weibo	9.3.1
WhatsApp	2.19.31
Whisper	8.11.14
Yandex Browser	19.3.3.157
Zalo	190301
Zello	4.47

Android: New and updated apps

77 updated apps	
Android Messages	4.1.067 (Ettin_RC12_xxhdpi.arm64-v8a.phone)
Any.DO	4.15.1.5
AppLock	2.8.10
ASKfm	4.36.2
Azar	3.39.2-arm64
Booking.com	17.3
Chrome	73.0.3683.90
Dropbox	136.2.2
Facebook	214.0.0.43.83
Facebook Messenger	207.0.0.13.99
Fitbit	2.90
Flipboard	4.2.12
Gmail	2019.03.03.240577312.release
Google Calendar	6.0.26-238239064-release
Google Docs	1.19.112.02.45
Google Maps	10.12.1
Google Photos	4.12.0.238634345
Google Quick Search Box	9.46.5.21.arm64

Google Translate	5.27.0.RC04.237379852
Google+	10.27.0.235437929
Grindr	5.5.0
GroupMe	5.35.9
Hangouts	30.0.239887060
Hot or Not	5.110.1
imo	9.8.000000011641
Instagram	86.0.0.24.87
InstaMessage	3.1.2
Kakao Story	5.7.0
KakaoTalk	8.3.0
Keeper	14.2.0
KeepSafe	9.30.0
Kik Messenger	15.7.0.20120
LINE	9.4.2
Mail.Ru	9.0.0.26510
Mappy	6.1911.18005
MeetMe	13.12.2.1780
My Tracks	4.2.3
mysms	7.0.3
Nimbuzz	7.1.0
Odnoklassniki	19.3.26
OkCupid	27.1.1
One Drive	5.28
Opera Mobile	51.2.2461.137690
Outlook.com	3.0.34
Pokemon GO	0.137.2
SayHi	7.22
Scruff	5.6050
Skout	6.6.1
Skype	8.41.0.64
Snapchat	10.52.3.0
Soma	2.0.14
Swarm	6.2.1
Sygic	17.9.3
Tango	6.5.233394
Telegram Messenger	5.5.0
Text Free Ultra Texting	8.36.1

Text Me Up	3.17.3
Text Me!	3.17.3
Text Now	6.17.0.1
textPlus	7.4.7
Threema	3.63
TikTok	10.5.0
Truecaller	10.22.6
Tumblr	13.0.0.01
TunnelBear	v167
Twitter	7.88.0-release.41
Uber	4.254.10002
UC Browser	12.10.5.1171
Viber	10.3.0.8
VIPole	2.0.54
Vkontakte	5.30
Weibo	9.3.3
WhatsApp	2.19.81
Whisper	9.28.6
Yandex Browser	19.3.3.288
Zalo	19.03.01
Zello	4.52

Cryptographic Hash Values Information

You can validate the integrity of Cellebrite's UFED software files by verifying their cryptographic hash values. This can help you identify whether a file has been changed from its original state

Product	MD5	SHA-256 (Recommended)
UFED Physical Analyzer	d69e1434ef1ca951bbde44ac65af83a2	499ab81b67cfdfd91480c0f5d8bd567dc0d1f924162877c010db2b4126725d48
UFED Logical Analyzer	ad82c8edf6f669813bd62fe729642254	0483afd3163779b0ec19f1aaa212e489a0ea879e209a2fd1945a74ad5dd476be
Cellebrite Reader	58b9a87985d3324543fabcc7d0d624c2	a06346b971f82d52b23a808aebeacfab303777e8b4b0cf169c1ea6260d6faed7