

UFED Physical Analyzer, UFED Logical Analyzer and Cellebrite Reader v7.30

February 2020

App versions: 10,443

App support

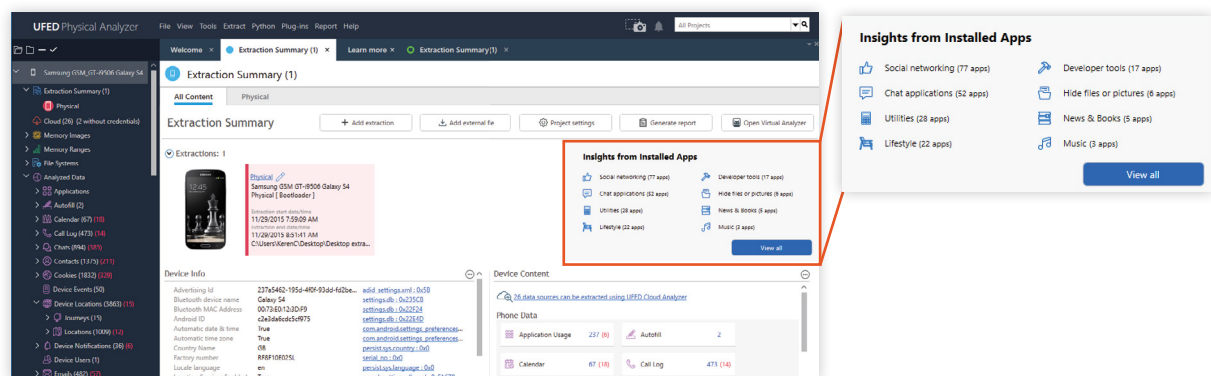
- **Signal Private Messenger (iOS)** – Updated decryption and decoding support for the latest version of Signal app on iOS devices surfaces user account details, contacts, chats and call logs.
- **WhatsApp support (KaiOS)** – New decoding support for the WhatsApp application on KaiOS devices surfaces contact details and chat messages.
- **225 updated applications** – Support for 225 new app versions for iOS and Android devices.

➔ New Dashboard Widget Shows Application Insights

This version of UFED Physical Analyzer introduces a new dashboard widget named “Insights from Installed Applications.” The purpose of the widget is to help examiners make insightful decisions around where to focus their examination efforts upfront, to optimize their examination process downstream.

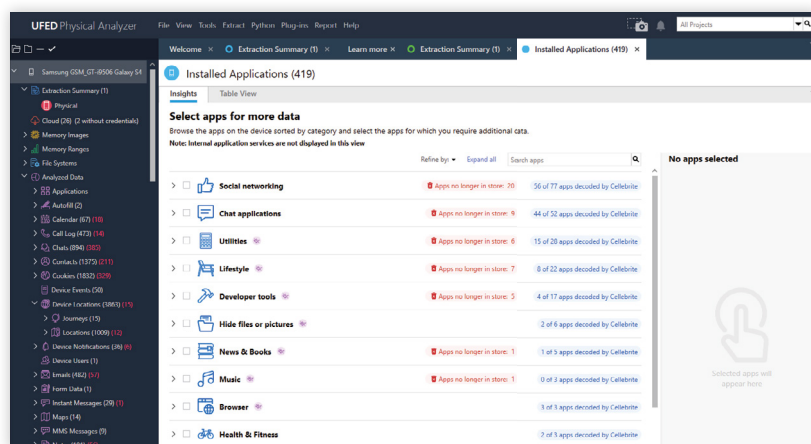
The dashboard widget shows a high-level overview of the applications installed on the extracted device, under their respective category. The widget is dynamic in nature and will display a list of categories based on the device extraction. Examiners can expand the application view by clicking on the dashboard widget, and later select one or more applications for further drill-down and review.

There are 30 categories listed. These are a combination of Cellebrite defined; hide files or pictures, fake GPS, Fake messages, Spoofing, Clean mobile etc, and industry accepted categories like social, finance, music, games and more.



This is the first step towards implementing a more intuitive design, with improved navigation, visuals and tools to optimize your use of UFED Physical Analyzer and to help you save valuable time.

You will notice that once you select the applications, and they are added to the right pane, you now have 2 additional options available for further review; App Genie and SQLite Wizard.

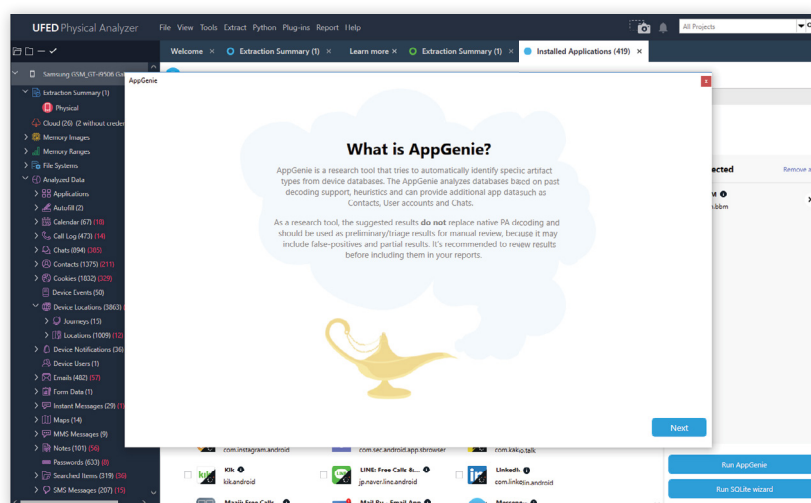


➔ Surface data from unsupported apps using AppGenie

AppGenie is a new and innovative research tool engine that surfaces data from 3rd party apps based on sophisticated heuristics. The AppGenie can perform automatic analysis of any application database, and decode chats, contacts, user accounts and location artifacts without any prior knowledge of the application.

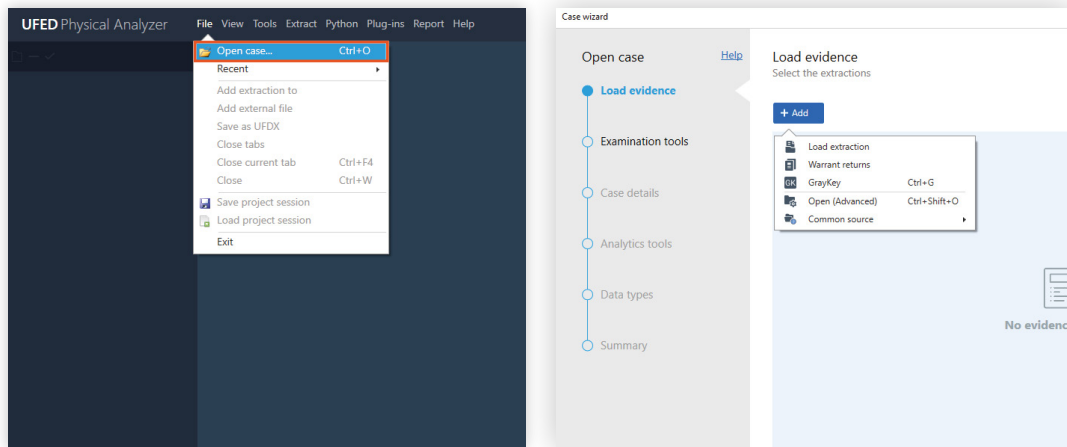
The AppGenie provides users of UFED Physical Analyzer with invaluable leads to evidence that was previously buried deep within the data, quickly making it legible, searchable and easy to incorporate into forensic reports.

The AppGenie tool comes as an addition to existing decoding capabilities in UFED Physical Analyzer to assist examiners that don't have the time or knowledge to write custom parsers to decode the data.



→ Unify the current Open Case flows under one tab

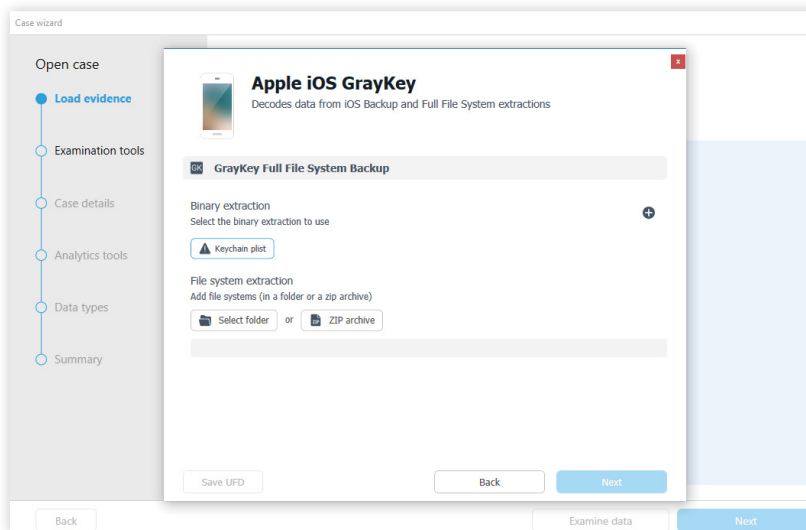
All open case options have now been unified under one tab. Users looking to open a new case from a UFED or Graykey extraction, load a warrant return or perform advanced open, can get to the various selections from one tab called Open Case. This is part of an ongoing effort to improve usability and streamline user workflow.



→ Open a GrayKey image through the new Open Case flow

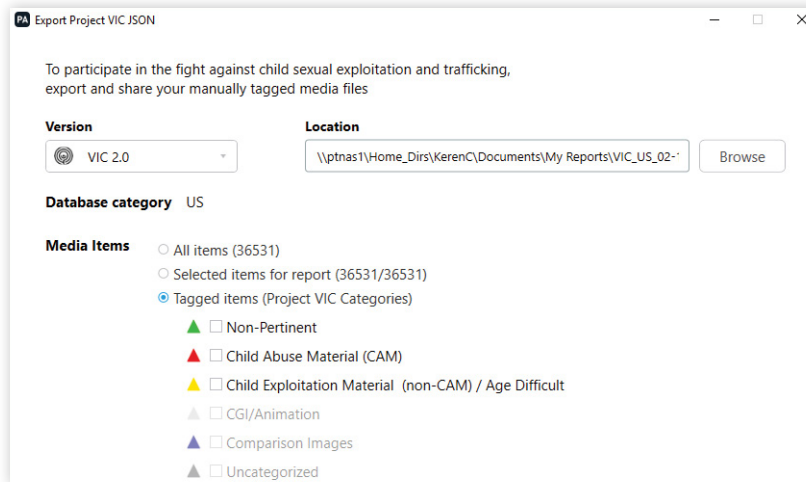
In the new Open Case flow, you can continue to ingest GrayKey files, but in a much simpler way. You can now import the GrayKey zip file and KeyChain plist file at one go, to allow UFED Physical Analyzer to parse both files simultaneously.

Note: GrayKey output contains 2 files; Full File System zip file (main image) and the KeyChain.plist as an external file (not part of the zip)



→ Updated Project VIC2.0 support

UFED Physical Analyzer now supports import and export of VICS 2.0 JSON data. Export in VIC/CAID format allows users to contribute back to the law enforcement community by sharing manually tagged suspicious media files. You can now include additional data into the exported file such as contact information and meta data.



→ Support for the InteractionC database in iOS

The InteractionC database (interactionC.db) on iOS stores important metadata generated from user interactions on the device. Such data includes call logs, SMS, chat messages and emails. Potential evidence deleted by the user may also leave traces in the interaction. The decoded data will be shown under the log entry model.

→ Seen and paired Bluetooth Devices

iOS device extractions will now include a list of the devices that were seen or paired via Bluetooth to the extracted device. The paired and seen Bluetooth connections are now decoded and presented under the DeviceConnectivity model, showing the type of connection.

Solved Issues – UFED Physical Analyzer

- Missing video thumbnails for iOS & Android devices
- CMS connection is lost after switching windows AD user
- Lost tagged data in a save session (pas file) of GK iOS extraction
- Missing tags in report when time range is selected
- Incorrect sender is decoded in Line apps chat messages for Android devices

Known Issues – UFED Physical Analyzer

- Tagged data of data files or attachments may be lost when loading a PAS file created in previous version



iOS: New and updated apps

101 updated apps	
Any.DO	4.39.5, 4.39.7
ASKfm	4.51
Azar	1.40.1
Badoo	5.148.0
Booking.com	22.0.2, 22.1.1
Calendar	13.3.1
Confide	9.2.4, 9.3.1
Contacts	13.3.1
Dropbox	174.2
Email	13.3.1
Facebook	251.0,254.0
Facebook Messenger	246.0, 249.0
Fitbit	3.13, 3.12.1
Flipboard	4.2.64, 4.2.65
Foursquare	11.16.2
Gmail/Inbox	6.0.191215
Google Docs	1.2019.49203, 1.2020.2203
Google Drive	4.2019.49206
Google Maps	5.34, 5.35
Google photos	4.35
GroupMe	5.3.6.1, 5.36.0
hike messenger	6.2.151, 6.2.161
Instagram	123.1, 126.0
KakaoTalk	8.7.0, 8.7.4
Keeper	14.8.2
Keepsafe	8.40.0
Kik Messenger	15.18.0
Life360	19.7.1, 19.8.0
Line	10.0.2, 9.19.0
Linkedin	9.1.159, 9.1.163
Locations	13.3.1
Mail.Ru	11.4, 11.5
Meet24	1.7.72, 1.7.74
MeetMe	14.8.0
Momo	8.21.5, 8.22.1
Nike+ Run Club	6.3.1, 6.4.0
Notes (iOS)	13.3.1
Odnoklassniki	8.30.3, 8.32.1



OKCupid	37.4.0
Reminder	13.3.1
SayHi	7.66
Scruff	6.1006
Signal Private Messenger / TextSecure	3.1.1, 3.2.1
SMS	13.3.1
SnapChat	10.72.5.69, 10.74.1.1
Swarm	6.4.3
Tango	6.15.240638
Taxify	Cl.4.14
Telegram	5.13.1, 5.14
TigerText	8.7
TikTok	14.2.0, 14.7.0
Tinder	11.6.0
Tumblr	14.9
Twitter	8.5, 8.6
Uber	3.382.10006
Viber	12.1, 12.2.1
Vkontakte	5.31.2, 5.32.1
Waze	4.58, 4.59
WeChat	7.0.10
Weibo	9.12.3
Whatsapp	2.19.124, 2.20.11
WhatsApp Business	2.19.124, 2.20.11
Whisper	8.17.0
Wicker	5.43.2, 5.46.5
Yandex Browser	19.12.0.263
Yubo	3.40.3
Zalo	19.12.02, 19.12.03
Zello	4.80

Android: New and updated apps

124 updated apps	
Any.DO	4.16.2.7, 4.16.3.6
ASKfm	4.53, 4.53.1
Automatic Call Recorder	6.03.5
Azar	3.50.0, 3.52.0
Booking.com	20.8
Chrome	79.0.3945.116, 79.0.3945.136
Ctrip	7.4.5



DJI Go 4	4.3.28
Dropbox	170.2.8, 172.2.2
Evernote	8.12.5
Expedia	19.49.0, 20.2.0
Facebook	251.0.0.31.111, 255.0.0.33.121
Facebook Messenger	246.0.0.9.353, 249.0.0.10.122
Firefox	68.4.1, 68.4.2
Fitbit	3.12.1
GG	4.16.1.20411
Glide	Glide.v10.359.502, Glide.v10.359.605
Gmail/Inbox	2019.12.3.289507923.release
Go SMS Pro	7.89
Google Calendar	2019.47.2-284533606-release , 2019.49.4-290591059-release
Google Docs	1.19.492.02.45, 1.20.022.05.45
Google Drive	2.19.492.02.45, 2.19.511.03.45
Google Maps	10.32.1, 10.33.1
Google photos	4.33.0.284040878, 4.35.0.290133535
Google Translate	6.4.RC11.286428534
Grindr	5.25.0, 6.1.0
GroupMe	5.41.3, 5.43.1
Hot or Not	5.153.0
imo	2019.9.51
Instagram	123.0.0.21.114, 126.0.0.25.121
Kakao Story	5.16.2, 5.16.3
KakaoTalk	8.7.1, 8.7.4
Keeper	14.5.10.4
Kik Messenger	15.19.0.22104
Life360	197.2, 19.8.1
Line	9.22.2, 10.0.2
Linkedin	4.1.395, 4.1.401
Mail.Ru	11.8.0.28653, 11.9.0.28705
Meet24	1.32.9, 1.32.12
MeetMe	14.8.4.2400, 14.9.0.2410
Nike+ Run Club	3.3.0, 3.4.0
Odnoklassniki	19.12.25, 20.1.28
OKCupid	36.1.4, 37.4.0
One Drive	5.45.1
Opera Mini	46.0.2254.145391, 55.2.2719.50740
Outlook.com	4.0.94
Pinterest	7.43.0
Pokemon GO	0.163.3



SayHi	7.58
Skout	6.16.0
SnapChat	10.72.5.0, 10.74.6.0
Swarm	6.5.1
Sygic	18.4.4
Tango	6.16.240967, 6.16.9538411
Telegram	5.13.1, 5.14.0
Text Me Up	3.21.2
Text Now	6.56.1.0, 20.1.1.0
TigerText	8.7.719
TikTok	14.4.5, 14.7.5
Tinder	11.6.0, 11.7.0
Truecaller	10.62.7
Tumblr	14.9.0.00
Twitter	8.25.0-release.00, 8.29.0-release.00
Uber	4.293.10007
UC Browser	12.14.0.1221
Viber	12.1.0.11, 12.2.2.1
Vkontakte	5.51.1, 5.52
Waze	4.58.0.1, 4.59.0.4
WeChat	7.0.9, 7.0.10
Weibo	10.1.2
Whatsapp	2.19.360, 2.20.11
WhatsApp Business	2.19.130, 2.20.5
Whisper	9.38.0
Wicker	5.43.2, 5.45.4
Yahoo Mail	6.2.4
Yandex Browser	19.12.1.121
Yandex Mail	4.44.1
YouTube	14.50.53
Zalo	19.12.02
Zello	4.80

