

UFED, UFED Physical Analyzer, UFED Logical Analyzer & Cellebrite Reader v.7.28

January 2020

App versions: 10,107

App support

- **WhatsApp message forwarding feature on iOS & Android devices** – Forwarded messages are indicated with a label (both in UI and the reports) helping you identify that this message originated somewhere else and was forwarded to this recipient.
- **Wickr App on Android** – Decryption and decoding support for the latest versions of the encrypted Wickr app running on devices with the latest Android versions.
- **Find My app for iOS devices** – Recover more locations data from the Find My app for iOS devices.
- **Attachments within the Reminders app on iOS devices** – Recover documents and photos, added as attachments, from the Reminders app on iOS devices.
- **Notes app for iOS devices** – Decode and view the list of participants involved in the note sharing process.
- **105 updated applications** – Support for 105 new app versions for iOS and Android devices.

UFED 4PC/Touch 2



Perform Full File System Extraction on iOS Devices with a Built-in Solution

Based on checkm8, examiners can now take advantage of a first-to market solution with UFED 7.28. This update allows you to quickly perform a forensically sound temporary jailbreak and full file system extraction within one streamlined workflow. The table below lists the supported devices and iOS versions.

Device (SoC)	Minimum iOS version	Latest iOS version*
iPhone 5S (A7)	12.3	12.4.4
iPhone 6 iPhone 6+ (A8)	12.3	12.4.4
iPhone 6S iPhone 6S+ (A9)	12.3	13.3
iPhone SE (A9)	12.3	13.3
iPhone 7 iPhone 7+ (A10)	12.3	13.3
iPhone 8 iPhone 8+ (A11)	12.3	13.3
iPhone X (A11)	12.3	13.3

DFU Mode

For your convenience, we have included instructions on how to insert the device into DFU mode [here](#). The blog will provide you a wealth of additional valuable information.

Our recommendation is to insert device into DFU mode while the device is on.

Important note: Checkm8 is not supported on Windows 7.

UFED Physical Analyzer

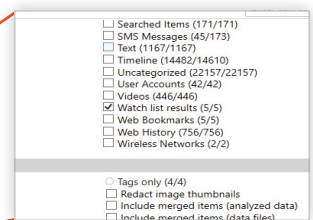
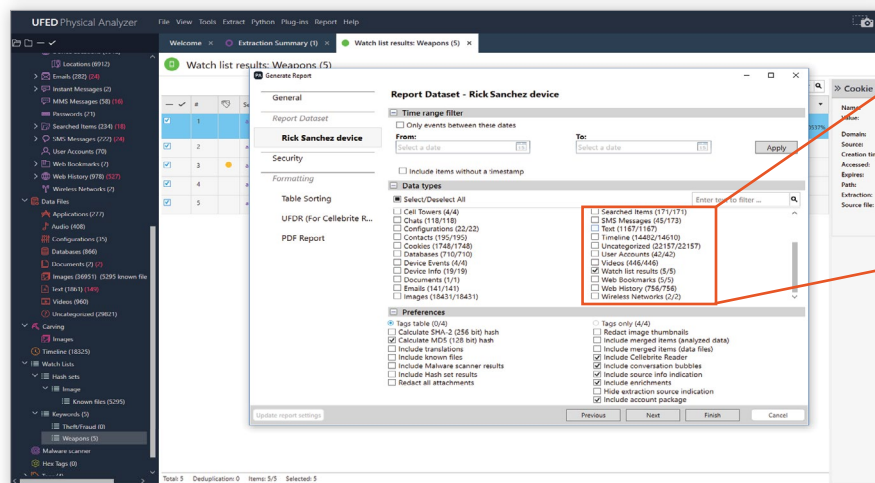
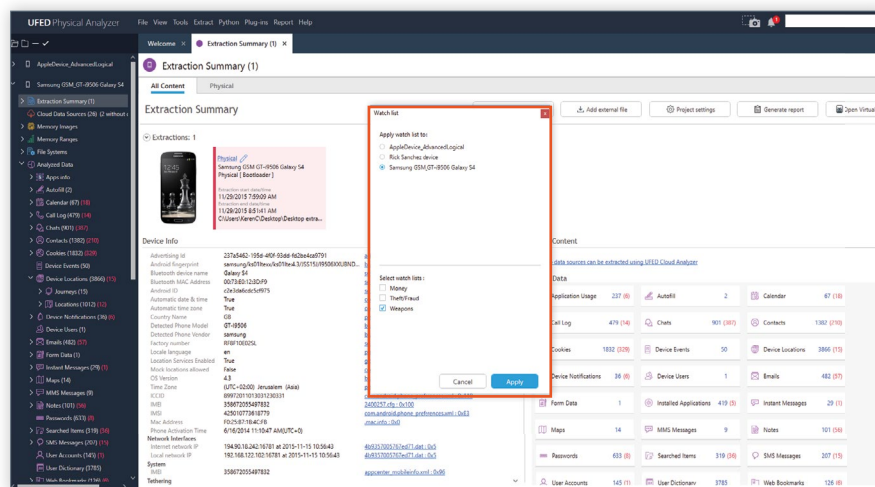


Watch lists enhancements

In UFED Physical Analyzer version 7.28 users can now run a watch list of keywords against your extracted data to identify and highlight important and relevant information in the Watch List capability.

This enhancement also allows users to:

- Run multiple watch lists on a selected project
- Receive notifications on the process run (progress bar)
- View the watch list results within a new and improved "search results" list
- Select, tag and incorporate watch lists results into your reports



UFED Physical Analyzer - Extraction Summary (1)

Extraction Summary

Extractions: 1

Device Info

Physical: Samsung SM-T800 Galaxy S4 Physical (Extraction 1)

Device Content

Phone Data

Application Usage: 237 (8)

Calendar: 67 (10)

Call Log: 479 (14)

Chats: 907 (887)

Contacts: 1382 (238)

Cookies: 1832 (329)

Device Events: 30

Device Locations: 3866 (10)

Device Notifications: 36 (8)

Device Users: 1

Emails: 461 (2)

Form Data: 1

Installed Applications: 479 (9)

Instant Messages: 29 (1)

Maps: 14

MMS Messages: 9

Notes: 101 (58)

Passwords: 613 (8)

Searched Items: 319 (26)

User Accounts: 145 (1)

User Dictionary: 3785

Watch lists in progress

NOTES

Watch lists in progress

Cancel

UFED Physical Analyzer - Watch list results: Weapons (5)

Watch list results: Weapons (5)

Q	#	Search Item	Matches count	Type	Fields	Content
1	1	ar15.com	1	Cookies	Domain	Cookie: sessionID (ar15.com)
2	2	ar15.com	1	Web History	URI	Shipping Firearms FAQ...
3	3	ar15.com	1	Web History	URI	Shipping Firearms FAQ...
4	4	ar15.com	1	Web History	URI	ar15.com/terms-and-conditions
5	5	ar15.com	1	Web History	URI	http://www.ar15.com/images/2016/Weapon.jpg

Total: 5 Enduplications: 0 Items: 5/5 Selected: 5

Cookie

Name	Value	Domain	Source	Creation Time	Expiration Time	Path	Extraction	Source File
sessionID	7878081811722975A12540C2D3030980337A70	ar15.com	Samsung Browser	5/18/2017 8:00:00 PM(UTC-5)	5/18/2017 8:00:00 PM(UTC-5)	/	Logical	Samsung SM-T800 Galaxy S4 Physical (Extraction 1)

Extraction Report

Participants

1541818182 OTDay Risk

Conversation - SMS Messages (42)

1541818182 OTDay Risk

Hey Risk, is OTDay are you around?

5/20/17 2:48:19 PM(UTC-5)

1541818182 OTDay Risk

For now, What's up?

5/20/17 2:48:33 PM(UTC-5)

1541818182 OTDay Risk

For now, What's up?

5/20/17 2:48:33 PM(UTC-5)

1541818182 OTDay Risk

Just checking in. In Florida now. Finally got out of Kern Valley. That was a mess, but that for the hook up.

5/20/17 2:52:56 PM(UTC-5)

1541818182 OTDay Risk

Anytime anyone, Im getting over to Australia today. Got a business meeting there. Might be good money. I'll get you some.

5/20/17 2:53:34 PM(UTC-5)





Unveil locations data anytime, anywhere using Cellebrite Reader

If an active internet connection exists, users of the Cellebrite Reader can now easily access locations data and view them in the map view.

The offline maps packages have been updated and are available for download from the MyCellebrite portal.



Now supporting the KaiOS operating system

Following customer demand, we are pleased to provide decoding support for devices running KaiOS. KaiOS is a mobile operating system based on Linux, and owned by KaiOS Technologies, with a global market share of 0.81% *

[*https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/](https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/)



New conversation view for faster discovery of evidence

UFED Physical Analyzer and Cellebrite Reader now display SMS, MMS, calls and emails in a bubble format in Word, PDF, HTML export, and reports.



Hide My Email for Sign in with Apple (iOS 13)

If you choose to hide your email when you create an account with an app or website using Sign in with Apple, a unique, random email address is created so your personal email can stay private. Any messages sent to this address are automatically forwarded to the user's personal email address, allowing them to read and respond directly while still keeping their personal address private.

UFED Physical Analyzer can now decode all these random email accounts and recover emails forwarded by them.

Additional Enhancements

- Following our previous support for Google production, we can now parse Gmail Contacts, Calendar, Locations (Json and csv format), My Activity (Search, Image search and locations), Google drive, Photos and Mobile backups.
- Now supporting iOS snapshot (KTX files) - when a user swipes up on the screen while using an application in an iOS device, or presses the home button, or if they receive a call while using an application, the active application is sent to the background. A "snapshot" of the current screen is taken in order to provide a smooth visual transition while changing screens. UFED Physical Analyzer can now recover all these snapshots under images data files. You can also filter by this file format.
- Enriched data in UFED Physical Analyzer is now indicated in blue color in both UI and reports.





End of life announcement for Windows 7

Following the announcement from Microsoft about the end of life for Windows 7 on January 2020, Cellebrite will continue to unofficially support UFED Physical Analyzer installations running on this platform until further notice. However, it is always recommended to run an officially supported platform.

Solved Issues

- Errors when generating PDF reports
- Decoding of iOS full file system extraction containing PaxHeaders
- Decoding of selected iMessages
- Decoding of snapchat database when performing APK downgrade
- Decoding of Safari for iOS
- Physical extraction of older iOS devices
- Slow decoding of WhatsApp data when performing APK downgrade
- Decoding of WhatsApp for selected Android devices

Known Issues

- Instagram call answer status is now indicated as unknown, presenting the most accurate data (previously selected calls may have been indicated as answered).

iOS: New and updated apps

36 updated apps	
Any.DO	4.15.9.12
AppLock	2.9.9
ASKfm	4.51.1
Azar	3.46.0
Blendr	5.143.2
Booking.com	20.1
Chatous	3.9.87
Chrome	78.0.3904.96
Dropbox	166.2.4
Evernote	8.12.3
Facebook	247.0.0.42.116
Facebook Messenger	241.0.0.17.116
Flipboard	4.2.27



Gmail	2019.10.20.278647676.release
Google Calendar	6.0.60-277466248-release
Google Docs	1.19.432.04.45
Google Drive	2.19.432.02.45
Google Maps	10.29.1
Google Photos	4.30.0.279188768
Google Quick Search Box	10.83.10.21.arm64
Google Tasks	1.7.275237227.release
Google Translate	6.3.0.RC06.277163268
Grindr	5.21.1
GroupMe	5.40.2
ICQ	7.7(823791)
imo	2019.6.31
Instagram	119.0.0.33.147
Kakao Story	5.14.6
KakaoTalk	8.6.2
Keeper	14.4.1.3
KeepSafe	9.46.1
Life360	19.6.0
LINE	9.20.1
LinkedIn	4.1.379
Mail.Ru	11.3.0.28239
MeetMe	14.7.3.2330
MobileVOIP Cheap Calls	7.29
Odnoklassniki	19.11.5
Pinterest	7.41.0
Pokemon GO	0.159.2
SayHi	7.55
Scruff	6.0019
Skout	6.15.0
Skype	8.54.0.91
Snapchat	10.70.0.0
Sygic	18.4.2
Tango	6.13.239299
Telegram Messenger	5.12.1
Text Me Up	3.20.1
Text Now	6.51.0.2
textPlus	7.6.2
Threema	4.2
TikTok	13.6.12
Tinder	11.3.0



Truecaller	10.56.7
Tumblr	14.7.0.00
Twitter	8.21.0-release.00
Uber	4.288.10001
UC Browser	12.13.5.1209
Viber	11.9.1.1
Vkontakte	5.48.3
WeChat	7.0.7
Weibo	9.11.0
WhatsApp	2.19.330
WhatsApp_Business	2.19.144
Whisper	9.37.0
Yandex Browser	19.10.1.81
Zalo	19.10.02
Zello	4.78

Android: New and updated apps

69 updated apps	
Any.DO	4.15.9.12
AppLock	2.9.9
ASKfm	4.51.1
Azar	3.46.0
Blendr	5.143.2
Booking.com	20.1
Chatous	3.9.87
Chrome	78.0.3904.96
Dropbox	166.2.4
Evernote	8.12.3
Facebook	247.0.0.42.116
Facebook Messenger	241.0.0.17.116
Flipboard	4.2.27
Gmail	2019.10.20.278647676.release
Google Calendar	6.0.60-277466248-release
Google Docs	1.19.432.04.45
Google Drive	2.19.432.02.45
Google Maps	10.29.1
Google Photos	4.30.0.279188768
Google Quick Search Box	10.83.10.21.arm64
Google Tasks	1.7.275237227.release
Google Translate	6.3.0.RC06.277163268



Grindr	5.21.1
GroupMe	5.40.2
ICQ	7.7(823791)
imo	2019.6.31
Instagram	119.0.0.33.147
Kakao Story	5.14.6
KakaoTalk	8.6.2
Keeper	14.4.1.3
KeepSafe	9.46.1
Life360	19.6.0
LINE	9.20.1
LinkedIn	4.1.379
Mail.Ru	11.3.0.28239
MeetMe	14.7.3.2330
MobileVOIP Cheap Calls	7.29
Odnoklassniki	19.11.5
Pinterest	7.41.0
Pokemon GO	0.159.2
SayHi	7.55
Scruff	6.0019
Skout	6.15.0
Skype	8.54.0.91
Snapchat	10.70.0.0
Sygic	18.4.2
Tango	6.13.239299
Telegram Messenger	5.12.1
Text Me Up	3.20.1
Text Now	6.51.0.2
textPlus	7.6.2
Threema	4.2
TikTok	13.6.12
Tinder	11.3.0
Truecaller	10.56.7
Tumblr	14.7.0.00
Twitter	8.21.0-release.00
Uber	4.288.10001
UC Browser	12.13.5.1209
Viber	11.9.1.1
Vkontakte	5.48.3
WeChat	7.0.7
Weibo	9.11.0



WhatsApp	2.19.330
WhatsApp_Business	2.19.144
Whisper	9.37.0
Yandex Browser	19.10.1.81
Zalo	19.10.02
Zello	4.78

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	fae4f70ce0a70e98ce2814f847ecd671	bff71e19597c7267c5b6228309c876e85596d55e053619d3594527a475653499
UFED Logical Analyzer	939c971c331905d63f93554a60965508	592f4cbfa3c1030ff810265d7d439d9601a53c6684e9331aa4868f68f41579d
Cellebrite Reader	2ee79efc67e292b33041393d14c33536	a79c0d4aaab3101fbda42d0cc22bba4f57dd89f73053dc5bfe56f7e3ab8e217d
UFED Touch2 (cpkg)	58dd79dca4cede45da5e8f9324d4ac1d	cfbe4d3d66fde8a63a60bbab544536d0e458ff88dddf7711b99cdd93097872f6
4PC (cpkg)	7bd2309b4b3adab44884fafa8626e834	9f0876e423ab91126fb0523a6d9da74cd1d53739f3b0c5da53c12ed5a80db451
4PC (exe)	140b5396668765abcf33dc88329ab979	b02b02ce4410a0dc7fdecf31d4737024afa5cd77ef86064b9241cb02593375db
Permission Manager (exe)	b33517d3e47537a1f8d7d019cb71830c	91bf6946b2b62c8c633499cc9fe6b330adb62ec969920dc8a829695941cfdb57

