NOTAS DE LA VERSIÓN

UFED, Cellebrite UFED Cloud, Cellebrite Physical Analyzer, Cellebrite Logical Analyzer y el Cellebrite Reader v7.34

Junio de 2020

Actualmente proporciona soporte para: 31.113 perfiles de dispositivos

Versiones de aplicaciones: 10.831

Métodos forenses	v. 7.34	Total
Extracción lógica	20	12.040
Extracción física*	20	7.722
Extracción del sistema de archivos	19	7.721
Extracción/desactivación del bloqueo de usuario	1	3.650
Total	60	31.113
*Incluidos dispositivos GPS		

El número de dispositivos móviles únicos con capacidades para contraseñas es de 5.545

Soporte de aplicaciones

- Aplicación de Instagram para Android: ahora proporciona soporte para la decodificación de actividades en redes sociales.
- Cuenta múltiple de la aplicación Wickr para Android: ahora proporciona soporte para varias aplicaciones/ cuentas de la aplicación Wickr instaladas en el mismo dispositivo y la indicación de eventos relacionados con la cuenta.
- WeChat - Controle los datos adicionales de WeChat iOS - La decodificación de fts_messages.db trae otra fuente de datos para la aplicación WeChat. Esto le dará la posibilidad de recuperar registros de WeChat eliminados/perdidos y, por otro lado, pueden surgir duplicaciones. Puede controlar la cantidad de duplicados desactivando la configuración "Parse FTS content from WeChat" en la ventana de configuración general.
- Descifrado de WeChat con número de IMEI: en versiones más recientes, el descifrado de WeChat se basa en el número IMEI. En esta versión, si el número IMEI no se encuentra en el dispositivo, los usuarios tendrán la opción de ingresar el número del IMEI manualmente, para permitir el total descifrado y la decodificación.
- **108 aplicaciones actualizadas:** soporte para 108 nuevas versiones de aplicaciones para dispositivos iOS y Android.

Cellebrite Physical Analyzer 7.34

Por primera vez, acceso a capacidades de extraccion de información publica y privada de la nube

Para un proceso de análisis continuo y simplificado, los usuarios de Cellebrite Physical Analyzer pueden revisar los datos del dispositivo y de la nube a través de una sola herramienta y con una experiencia unificada. Al agregar la licencia de Cellebrite UFED Cloud a Cellebrite Physical Analyzer, y al permitir una conectividad abierta a Internet, los usuarios tienen múltiples opciones para acceder a los datos en la nube;

- Credenciales de usuario proporcionadas bajo consentimiento de una víctima / testigo / sospechoso
- Tokens de dispositivo extraídos con UFED
- Cookies del navegador de un PC

Para festejar este logro, estamos extendiendo un descuento especial por tiempo limitado. Entre en contacto con el departamento de ventas para conocer el **descuento especial que puede aplicarse.**

Los clientes interesados en evaluar la solución Cellebrite UFED Cloud, ahora pueden hacerlo actualizando a la versión 7.34 y utilizando la prueba GRATUITA que está disponible hasta el 31 de julio.

Para ayudarlo a comenzar, hemos preparado este sencillo video Cómo Comenzar.

Mejoras de la interfaz de usuario

Para abordar los comentarios proporcionados por los usuarios después del lanzamiento de la versión 7.33, hemos realizado las siguientes mejoras:

- Barra de tiempo - Ahora está disponible una opción para acercar y alejar usando los botones (+) y (-), (además de la barra de desplazamiento). Además, siempre se presenta la barra de tiempo gráfica.
- La sección de archivos de datos ahora está separada en los datos analizados.
- Configuración de vistas: hay 2 vistas de color disponibles: oscuro y claro. Puede cambiarlo en la configuración.
- Seleccionar/ Deseleccionar elementos para el informe ahora está disponible en el menú global de kebab. También puede Seleccionar/ Deseleccionar elementos en la vista de línea de tiempo.
- El icono de captura de pantalla se ha movido a la barra de menú superior, para permitir una navegación más suave.

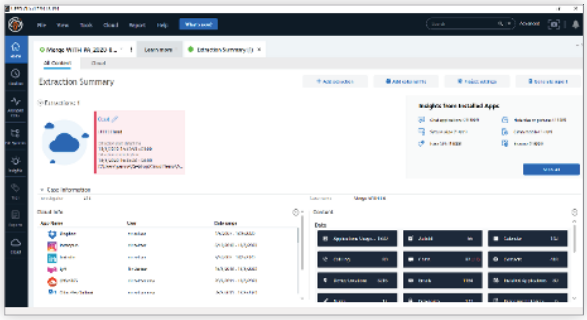
Cellebrite UFED Cloud 7.34

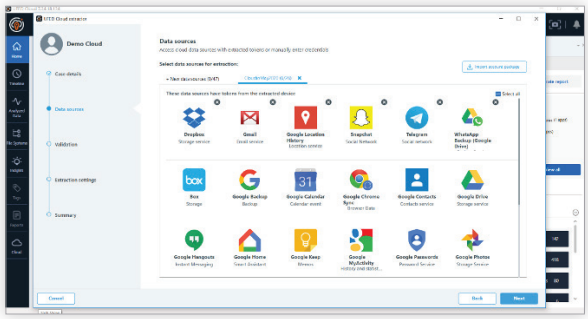
Revisión general de la interfaz de usuario

El video muestra los cambios programados en Cellebrite UFED Cloud. Los cambios sustanciales se producen como resultado de los comentarios directos que recibimos de ustedes, nuestros clientes, a medida que evolucionamos constantemente nuestras soluciones de inteligencia digital para brindarles un mejor apoyo en la realización exitosa de sus investigaciones.

Construida sobre las bases comprobadas de Cellebrite Physical Analyzer, Cellebrite UFED Cloud no solo trae una interfaz de usuario modernizada, sino que incorpora varias de las nuevas y existentes capacidades de Cellebrite Physical Analyzer, tales como listas de palabras claves, línea de tiempo gráfica, traducciones de texto, enriquecimiento de datos y más.

Para ayudarlo a comenzar, hemos preparado este sencillo video de Cómo Comenzar.





Diferencias de producto/ Limitaciones conocidas de Cellebrite UFED Cloud

- La capacidad de captura de páginas web no es compatible.
- Las capacidades de extracción pública directa no son compatibles.

UFED 7.34

Qualcomm Live

Nos complace anunciar el primer soporte para una extraccion genérica completa del sistema de archivos completo o una extracción física para dispositivos Android desbloqueados equipados con varias referencias de chips Qualcomm. La nueva capacidad de Qualcomm Live amplía el acceso a los últimos dispositivos de los principales proveedores chinos como Xiaomi, OPPO, OnePlus, VIVO, así como también en dispositivos Nokia, LG Motorola y otros, que ejecutan las versiones del sistema operativo 7 y 10.

Este método genérico, como la mayoría de los métodos genéricos en UFED, se ha desarrollado con el objetivo de admitir dispositivos de múltiples fabricantes y varias referencias de chips utilizando un único perfil genérico. El método genérico aborda la necesidad inmediata de un cliente de acceder a dispositivos con Sistema Operativo Android 8.1 o superior. Los usuarios no requieren técnicas o cables especiales para realizar la extracción.

Nota: El soporte para Samsung y Huawei llegará pronto.

Compatible con dispositivos VIVO basados en MTK

A medida que VIVO amplía su porción del mercado en varias áreas del mundo, hemos ampliado nuestra capacidad MTK Live, la primera en el mercado, para soportar dispositivos VIVO basados en procesadores MTK.

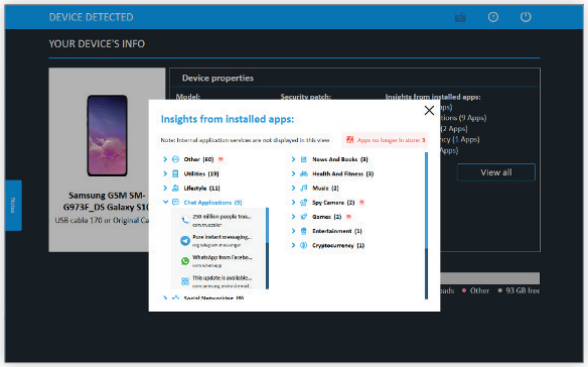
Una lista completa de los dispositivos recientemente compatibles está disponible en la sección Lista de teléfonos.

Soporte a nuevos dispositivos con Samsung Decrypting Exynos

Esta versión tiene soporte para dispositivos Samsung con cifrado de disco completo como el Samsung Galaxy S9 y el Samsung Galaxy Note 9 con Android 10.

Indicios de las aplicaciones instaladas

Esta versión de UFED también ofrece a los usuarios una vista general de los datos del dispositivo en la nueva sección con indicios de las aplicaciones instaladas. Los datos de aplicaciones instaladas serán presentadas antes de realizar la extracción de un dispositivo Android. Puede ubicar la información en la página Información del Dispositivo, donde se muestran las propiedades del dispositivo. La capacidad está diseñada para ayudar a los examinadores a tomar decisiones certeras sobre dónde enfocar sus esfuerzos de análisis por adelantado, a fin de optimizar su proceso de revisión posterior. También es una forma efectiva de detectar actividad sospechosa y mejorar el proceso de priorización de los dispositivos.



Cellebrite Physical Analyzer: Problemas resueltos

- Error de decodificación de la aplicación Signal para la extracción completa del sistema de archivos iOS.
- Decodificación de registros de llamadas del dispositivo Nokia RM-1172.
- Falla al decodificar la aplicación KeepSafe.
- Error de decodificación de las aplicaciones de Chrome versión 62.0.3202.84.
- Error al guardar un archivo UFDX para más de 2 fuentes de devolución de garantía combinadas.
- Error al guardar un depósito para imágenes.
- Error al ejecutar el escarbador de ubicaciones.
- Error de análisis de la agenda de direcciones para dispositivos iOS 3.0.

Cellebriter Physical Analyzer y Cellebrite UFED Cloud: Problemas conocidos

- El enriquecimiento con datos públicos no está funcionando actualmente. Estamos trabajando para solucionarlo en los próximos lanzamientos.
- Cancelar la extracción de datos en la nube durante el proceso de extracción solo es válido desde el Centro de Notificaciones.

iOS: Aplicaciones nuevas y actualizadas

Decodificación de 51 aplicaciones actualizada	
Any.DO	5.1.0
ASKfm	4.56
Azar	1.42.0
Badoo	5.162.1
Booking.com	23.3
Chrome	81.0.4044.124
Confide	9.4.1
Dropbox	186.2
Facebook	268.0
Facebook	266.0
Facebook Messenger	264.0
Facebook Messenger	263.0
Fitbit	3.20
Flipboard	4.2.73
Foursquare	11.16.8
Garmin Connect	4.30
Gmail/Bandeja de entrada	6.0.200412
Google Drive	4.2020.18204
Google Maps	5.42
Traductor de Google	6.7.0
Grindr	6.8.1
GroupMe	5.39.2
Hangouts	33.0.0
hike Messenger	6.2.230
Hot or Not	5.162.0
Instagram	142.0
Instagram	140.0
InstaMessage	3.3.7
KakaoTalk	8.8.2
Keeper	14.9.1
Keepsafe	10.0.10
Kik Messenger	15.22.1
Life360	20.2.0
Line	15.21.0.22201
Linkedin	9.1.177
Momo	8.23.4
Odnoklassniki	8.42.1
Signal Private Messenger / TextSecure	3.8.1

Skype	8.59
SnapChat	10.80.5.79
Telegram	6.1.2
TikTok	15.9.1
Twitter	8.18
Viber	12.8
Vkontakte	6.2.1
Whatsapp	2.20.51
Whatsapp	2.20.50
WhatsApp Business	2.20.51
WhatsApp Business	2.20.50
Wicker	5.53.11
Zalo	20.04.01

Android: Aplicaciones nuevas y actualizadas

Decodificación de 57 aplicaciones actualizada	
Any.DO	5.0.0.10
ASKfm	4.58.1
Azar	3.56.0
Badoo	5.167.1
Booking.com	22.0.5
ChatOn	1.0.23
Chrome	80.0.3987.149
Ctrip	7.6.6
DJI Go 4	4.3.36
Dropbox	186.2.6
Expedia	8.13.2
Facebook	270.1.0.66.127
Facebook Messenger	264.0.0.23.120
Firefox	68.7.0
Fitbit	3.19.2
Flipboard	4.2.41
GG	4.19.0.20437
Glide	Glide.v10.359.703
Gmail/Bandeja de entrada	2020.03.01.300951155.release
Calendario de Google	2020.14.1-306605106-release
Documentos de Google	1.20.122.06.45
Google Drive	2.20.101.12.45
Google Maps	10.37.2
Google Fotos	4.44.0.303191992

Google Tasks	2020.02.298557460.release
Google Traductor	6.6.1.RC09.302039986
Grindr	6.5.1
GroupMe	5.46.3
Growlr	11.13
Hangouts	33.0.303435107
HERE WeGo	2.0.14211
Hot or Not	5.167.1
Hushed	5.0.4
imo	2020.04.1031
Instagram	134.0.0.26.121
Keeper	14.5.40.3
Kik Messenger	15.21.0.22201
Life360	20.2.1
Line	10.4.2
Linkedin	4.1.444
Odnoklassniki	20.3.24
Signal Private Messenger / TextSecure	4.57.2
Skout	6.19.0
Skype	8.58.0.93
SnapChat	10.82.1.0
Devolución de garantía de Snapchat	10.78.6.0
Telegram	6.0.1
TextNow	20.15.0.0
TikTok	15.5.4
Twitter	8.38.0-release.00
Viber	12.8.0.19
Vkontakte	6.0
Whatsapp	2.20.89
WhatsApp Business	2.20.35
Wicker	5.50.4
Wicker	5.45.4
Zalo	20.03.01

Lista de teléfonos

Qualcomm Live y VIVO MTK Live

14 dispositivos recientemente compatibles	
Coolpad	YuLong C3701A Revvl Plus
LG CDMA	US998 V30
LG GSM	K550 Stylo 2 Plus, H860 G5
Motorola GSM	XT1925DL Moto g6 Prepaid, XT1766 Moto E4
OPPO	R11, PBAM00 A5, PBCM30 K1, PCGM00_DS K3
Xiaomi	M1810E5E Mi Mix, M1903C3EI_DS Redmi 7A, M1906F9SI Mi A3, M1808D2TG Mi 8 Lite

Extracción física con omisión del bloqueo

9 dispositivos recientemente compatibles	
HTC	6275, PB99400 Desire CDMA
Huawei	NMO-GT3, NMO-L31 GR5 Mini
Lenovo	S660_DS
Samsung GSM	SC-05G (Galaxy S6)
Tablets	Samsung GT-P3113TS Galaxy Tab 2 7.0
VIVO	Y55_DS, Y67L

Extracción física con omisión del bloqueo

20 dispositivos recientemente compatibles	
Asus	X017DA ZenFone 5Q, ZC600KL, X00TD Zenfone Max Pro, ZB602KL, X00QD Zenfone 5, ZE620KL, Z01MDA ZenFone 4 Selfie Pro, ZD552KL, X00RD ZenFone Live, ZA550KL, Z01BDC ZenFone 3, ZC551KL
HTC	6275, PB99400 Desire CDMA
Huawei	LLD-AL00 Honor 9 Lite, NMO-GT3, NMO-L31 GR5 Mini
Kyocera	KYF33(TORQUE X01)
Lenovo	S660_DS
LG CDMA	H790, bullhead Nexus 5x, LGM322 X Charge Xfinity, X Power 2
Meizu	M818H_DS C9
Motorola GSM	XT2013-4 One Action, XT2016-2 One Macro
Nokia GSM	TA-1041 7
Oppo	R11s Plus, R833T
VIVO	Y83A_DS, V1818CA_DS Y91, V1916A Iqoo Pro 5G, Y927, Y913_DS, V1938T X30 Pro, Y55_DS, V1921A_DS Z5, Y67L
Xiaomi	2014813_DS Redmi

Extracción del sistema de archivos con omisión del bloqueo

5 dispositivos recientemente compatibles	
HTC	6275, PB99400 Desire CDMA
Huawei	NMO-GT3, NMO-L31 GR5 Mini
VIVO	Y67L

Extracción del sistema de archivos

19 dispositivos recientemente compatibles	
Huawei	LLD-AL00 Honor 9 Lite
Kyocera	KYF33(TORQUE X01)
Lenovo	S660_DS
Meizu	M818H_DS C9
Motorola GSM	XT2013-4 One Action, XT2016-2 One Macro
Nokia GSM	TA-1041 7, Fake Nokia E79+
Oppo	R11s Plus, R833T
VIVO	Y83A_DS, V1818CA_DS Y91, V1916A Iqoo Pro 5G, Y927, Y913_DS, V1938T X30 Pro, Y55_DS, V1921A_DS Z5, Y67L

Extracción lógica

20 dispositivos recientemente compatibles	
Huawei	LLD-AL00 Honor 9 Lite
Kyocera	KYF33(TORQUE X01)
Lenovo	S660_DS
Meizu	M818H_DS C9
Motorola GSM	XT2013-4 One Action, XT2016-2 One Macro, XT2013-2 One Action
Nokia GSM	TA-1041 7
Oppo	R11s Plus, R833T
VIVO	Y83A_DS, V1818CA_DS Y91, V1916A Iqoo Pro 5G, Y927, Y913_DS, V1938T X30 Pro, Y55_DS, V1921A_DS Z5, Y67L
Xiaomi	2014813_DS Redmi