NOTAS DA VERSÃO

UFED, Cellebrite UFED Cloud, Cellebrite Physical Analyzer, Cellebrite Logical Analyzer e Cellebrite Reader v7.34

Junho de 2020

Agora compatível com: 31.113 perfis de dispositivos móveis

Versões do aplicativo: 10.831

Métodos de perícia digital	v. 7.34	Total
Extração lógica	20	12.040
Extração física*	20	7.722
Extração de sistema de arquivos	19	7.721
Extrair/desativar bloqueio do usuário	1	3.650
Total	60	31.113
*Incluindo dispositivos GPS		

O número de dispositivos móveis únicos com recursos de senha é 5.545.

Suporte do aplicativo

- Aplicativo Instagram para Android – agora compatível com a decodificação de atividades da rede social mais usada no momento.
- Conta múltipla do aplicativo Wickr para Android – agora compatível com vários aplicativos/contas do aplicativo Wickr instalado no mesmo dispositivo e a indicação de eventos relacionados à conta.
- WeChat – controle dos dados extras do iOS do WeChat – a decodificação do fts_messages.db traz outra fonte de dados para o aplicativo WeChat. Este recurso possibilitará a recuperação de registros do WeChat excluídos/ausentes e, por outro lado, poderão surgir duplicidades. Você pode controlar o número de duplicidades ao desativar a configuração "Analisar conteúdo FTS do WeChat" na janela de configurações gerais.
- Descriptografia do WeChat com número IMEI – nas versões mais recentes, a descriptografia do WeChat é baseada no número IMEI. Nesta versão, se o número IMEI não for encontrado no dispositivo, os usuários terão a opção de inserir o número IMEI manualmente e assim habilitar a descriptografia e decodificação completas.
- **108 aplicativos atualizados –** suporte para 108 novas versões de aplicativos para dispositivos iOS e Android.

Cellebrite Physical Analyzer 7.34

Acesso pela primeira vez a capacidades de nuvem pública e privada

Para um processo de análise integrado e simplificado, os usuários do Cellebrite Physical Analyzer podem analisar os dados do dispositivo e da nuvem por meio de uma única ferramenta e com uma experiência unificada. Ao adicionar a licença do Cellebrite UFED Cloud ao Cellebrite Physical Analyzer e habilitar a conectividade aberta à Internet, os usuários têm várias opções de acesso aos dados em nuvem;

- Permite a inserção de credenciais de usuário fornecidas mediante o consentimento de uma vítima/testemunha/suspeito
- Tokens de dispositivo extraídos usando o UFED
- Cookies do navegador para PC

Em comemoração desta conquista, estamos concedendo um desconto especial por tempo limitado. Entre em contato com a equipe de vendas para saber mais sobre o **desconto especial que pode ser aplicado.**

Os clientes interessados podem avaliar a solução Cellebrite UFED Cloud atualizando para a versão 7.34 e usando a demonstração GRATUITA que está disponível até 31 de julho.

Para ajudá-lo a começar, reunimos este vídeo com os primeiros passos simples.

Aprimoramentos na IU

Para tratar os feedbacks fornecidos pelos usuários após o lançamento da versão 7.33, fizemos os seguintes aprimoramentos:

- Barra de tempo – uma opção para aumentar e diminuir o zoom agora está disponível usando os botões (+) e (-) (além da barra de rolagem). Além disso, a barra de tempo gráfica estará sempre visível.
- A seção de arquivos de dados agora está separada nos dados analisados.
- Configurações de temas – existem dois temas de cores disponíveis: preto e branco. Você pode alterar o tema nas configurações.
- A opção de Marcar/desmarcar itens para o relatório agora está disponível no menu geral de três pontos. Você também pode marcar/desmarcar itens na visualização da linha do tempo.
- O ícone de captura de tela foi movido para a barra de menu superior, a fim de permitir uma rolagem mais suave.

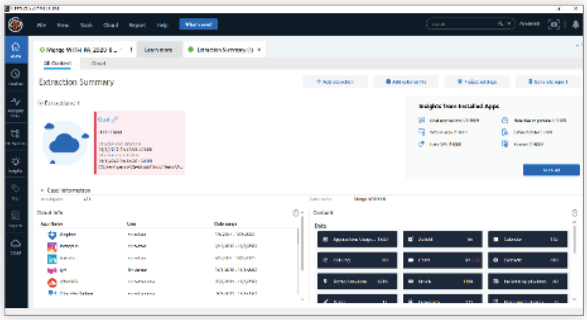
Cellebrite UFED Cloud 7.34

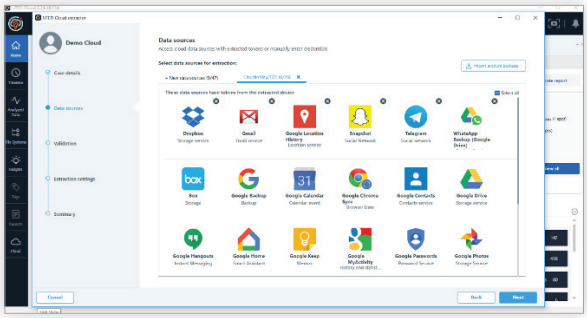
Renovação geral da IU

O vídeo mostra alterações tardias no Cellebrite UFED Cloud. As alterações substanciais são resultado do feedback direto que recebemos de vocês, nossos clientes, à medida que evoluímos constantemente nossas soluções de inteligência digital para melhor ajudá-los a realizar suas investigações com êxito.

Desenvolvido considerando as bases comprovadas em campo do Cellebrite Physical Analyzer, o Cellebrite UFED Cloud não apenas traz uma interface de usuário modernizada, como incorpora várias das capacidades novas e existentes do Cellebrite Physical Analyzer, incluindo favoritos, linha do tempo gráfica, tradução de textos, enriquecimento de dados e muito mais.

Para ajudá-lo a começar, reunimos este vídeo com os primeiros passos simples.





Defasagens do produto/limitações conhecidas do Cellebrite UFED Cloud

- A capacidade de captura de web não é compatível.
- As capacidades de extração pública direta não são compatíveis.

UFED 7.34

Qualcomm Live

É com satisfação que anunciamos o suporte pela primeira vez de uma genérica e completa extração dos arquivos de sistema, permitindo opcionalmente, extração física para dispositivos desbloqueados dos modelos Android equipados com chipset Qualcomm. A nova capacidade Qualcomm Live amplia o acesso aos dispositivos mais recentes dos principais fornecedores chineses, como Xiaomi, OPPO, OnePlus, VIVO, além de dispositivos da Nokia, LG e Motorola, entre outros, que executam as versões 7 até 10 do sistema operacional.

Esse método genérico, como a maioria dos métodos genéricos do UFED, foi desenvolvido com o objetivo de oferecer suporte a dispositivos de vários fornecedores e chipsets usando um único perfil genérico. O método genérico atende a uma necessidade imediata de clientes por acesso a dispositivos com Android 8.1 ou superior. Os usuários não precisam de cabos ou técnicas especiais para realizar a extração.

Observação: o suporte para Samsung e Huawei estará disponível em breve.

Suporte a dispositivos VIVO baseados em MTK

À medida que a VIVO amplia sua participação de mercado em várias áreas do mundo, expandimos nossa capacidade de MTK Live pioneira no mercado para incluir o suporte a dispositivos VIVO baseados em MTK.

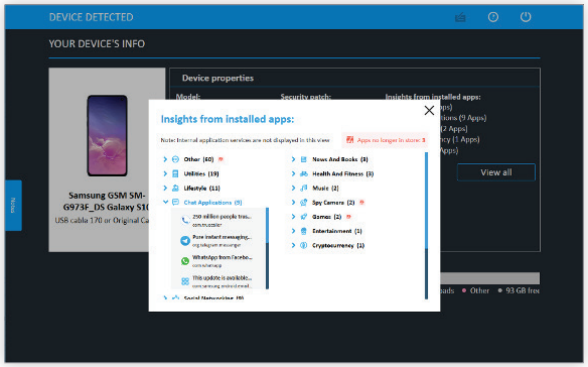
Uma lista completa dos dispositivos mais recentes com suporte pode ser encontrada na seção Lista de telefones.

Suporte a novos dispositivos com o Samsung Decrypting Exynos

Esta versão apresenta suporte para dispositivos Samsung que estiverem com criptografia de disco completo, como o Samsung Galaxy S9 e o Samsung Galaxy Note 9 executando o Android 10.

Informações de aplicativos instalados

Esta versão do UFED também oferece aos usuários uma visão geral dos dados do dispositivo com novas informações dos aplicativos instalados. Os dados do aplicativo instalado serão apresentados antes da extração do dispositivo Android. Você pode localizar as informações na página Informações do dispositivo, em que as propriedades do dispositivo são exibidas. A capacidade foi projetada para ajudar os examinadores a tomar decisões informadas e com antecedência sobre onde concentrar seus esforços de extração a fim de otimizar todo o processo de exame até a conclusão. É também uma maneira eficaz de detectar atividades suspeitas e aprimorar o processo de triagem do telefone.



Cellebrite Physical Analyzer: Problemas resolvidos

- Correção na falha na decodificação do aplicativo Signal para extração completa do sistema de arquivos do iOS.
- Decodificação de registros de chamadas do dispositivo Nokia RM-1172.
- Correção na falha na decodificação do aplicativo KeepSafe.
- Falha na decodificação dos aplicativos Chrome versão 62.0.3202.84.
- Erro ao salvar um arquivo UFDX para mais de duas fontes de retorno de garantia mescladas.
- Erro ao salvar um dump de imagens.
- Erros ao executar o escavador de localizações.
- Correção na falha da análise do catálogo de endereços para dispositivos iOS 3.0.

Cellebrite Physical Analyzer e Cellebrite UFED Cloud: Problemas conhecidos

- O enriquecimento de dados públicos não está funcionando no momento. Estamos trabalhando para corrigir isso nas próximas versões.
- O cancelamento da extração de dados na nuvem durante o processo de extração é aplicável apenas por meio do Centro de notificações.

iOS: Aplicativos novos e atualizados

51 aplicativos atualizados	
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/Caixa de Entrada	6.0.200412
Google Drive	4.2020.18204
Google Maps	5.42
Google Tradutor	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: Aplicativos novos e atualizados

57 aplicativos atualizados	
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/Caixa de Entrada	2020.03.01.300951155.release
Google Agenda	2020.14.1-306605106-release
Google Docs	1.20.122.06.45
Google Drive	2.20.101.12.45
Google Maps	10.37.2
Google Fotos	4.44.0.303191992

Google Tarefas	2020.02.298557460.release
Google Tradutor	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
Devoluções de mandados 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 telefones

Qualcomm Live e VIVO MTK Live

14 dispositivos recém-compatíveis	
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

Extração física com bypass de bloqueio

9 dispositivos recém-compatíveis	
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

Extração física com bypass de bloqueio

20 dispositivos recém-compatíveis	
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

Extração de sistema de arquivos com bypass de bloqueio

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

Extração de sistema de arquivos

19 dispositivos recém-compatíveis	
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

Extração lógica

20 dispositivos recém-compatíveis	
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