

Notes de version 7.13 : UFED Physical Analyzer, UFED Logical Analyzer et Cellebrite Reader

Améliorations : UFED 4PC/Touch2

Janvier 2019

- ★ Applis prises en charge : 27 141 profils d'appareils
- ★ Versions : 7 318

LES POINTS FORTS

Prise en charge des applications sur UFED Physical Analyzer

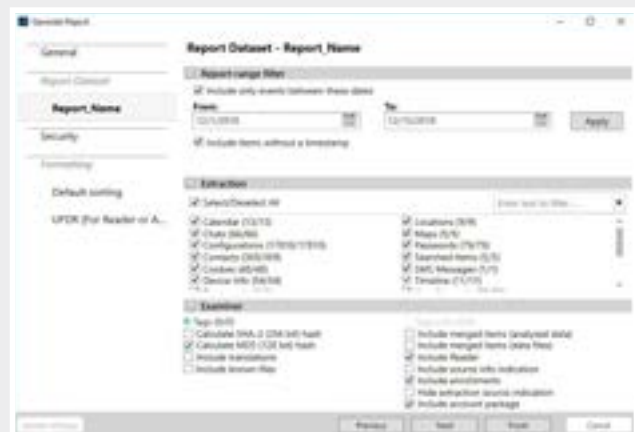
- Décodage des messages sur Snapchat pour les appareils iOS.
- 131 applications mises à jour pour les appareils iOS et Android.

Améliorations UFED 4PC/Touch 2

- **Nouveauté UFED 7.13 :** méthode de contournement d'écran de verrouillage générique sur tous les appareils Android.

Filtrage des données de rapport

Dans cette version, les utilisateurs disposent d'une fonctionnalité de filtrage des données de rapport qui leur permet de générer des rapports pour une période spécifique. Les enquêteurs et les magistrats peuvent ainsi analyser les données générées au cours d'une période spécifique et gagner du temps.



Décodage des messages de Snapchat sur les dispositifs iOS

UFED Physical Analyzer prend désormais en charge le décodage des messages de Snapchat sur les dispositifs iOS utilisant la dernière version de format de fichier « TSF ».



Méthode de contournement d'écran de verrouillage générique sur les smartphones Android

La nouvelle méthode de contournement d'écran de verrouillage générique ajoutée dans UFED 7.12 vous donne désormais accès aux preuves cruciales des smartphones Android les plus populaires comme le Samsung Galaxy S9, le Galaxy S8, etc. Cette méthode inédite fonctionne désormais sur différents modèles de grands fabricants (Samsung, LG, Motorola, Sony, Xiaomi et bien d'autres). Les dispositifs pris en charge doivent fonctionner sur Android 6 (ou version ultérieure) avec un cryptage complet du disque (FDE) et un patch de sécurité antérieur à août 2018.

Comment utiliser cette méthode :

1. Vous aurez besoin des câbles 500, 501 et 508.
2. Dans UFED 7.13, 64 périphériques LG sont désormais compatibles. Pour utiliser cette méthode, localisez le profil LG MP260 et sélectionnez l'option « Désactiver le verrouillage de l'écran » (dans Désactiver/Réactiver le verrouillage utilisateur).
3. Ensuite, suivez les instructions qui s'affichent à l'écran.



Attention :

- Cette méthode ne fonctionne que sur les dispositifs FDE « Full Disc Encryption » et non sur les chiffrements de système de fichiers. Suivez bien les instructions d'UFED (éteignez l'appareil à chaque tentative de déverrouillage).
- Si vous ne savez pas si l'appareil analysé est un dispositif FDE, vous pouvez :
 - Consulter le tableau de référence des appareils testés
 - Rechercher des périphériques similaires et exécuter la méthode ADB



Appareils testés :

Fabriqueur	Modèles testés
Samsung	SM-G955W, SM-J737VPP, SM-G950U, SM-J400F, SM-J810F\DS, SM-J510M, SM-J327T, SM-G950N, SM-G570F\DS, SM-G930F, SM-G920P, SM-G955N, SM-G9650, SM-G960U1
Motorola	XT1765, XT1625, XT1922-9, XT1767, XT1762, XT1641, XT1922-5, XT1766, XT1650-03, XT1644, XT1921-1
Xiaomi	Redmi 5 Plus, Redmi 5, Redmi Pro, Mi 5, Mi 5s Plus, Mi A1, Mi 5x, Redmi 4X
Sony	G3121 Xperia XA1, F5121 Xperia X, D6603 Xperia Z3
Meizu	M6 Note, Meilan M6, M621H Meilan Note
OnePlus	A3010 3T

Problèmes résolus sur UFED Physical Analyzer :

- Un problème de blocage de Cellebrite Reader lors de l'enregistrement de fichiers « PAS » lorsque le chemin d'accès est long.
- Décodage des appels sur les dispositifs Alcatel 1016G.
- Éléments sélectionnés pour le rapport lors du chargement de fichiers « PAS ».
- Un problème de tri dans le tableau de « tags ».
- Un problème de paramétrages de champs supplémentaires dans les rapports (listes).
- Un problème avec les éléments triés de la chronologie des rapports PDF, doc et excel.

iOS : Nouvelles applis et mises à jour

66 applis mises à jour	
Any.DO	4.27.0
ASKfm	4.28
Ctrip (chinois)	7.16.2
DJI GO	3.1.47
DJI GO 4	4.3.4
Dropbox	120.3
Facebook	198.0
Facebook Messenger	193.0
Flipboard	4.2.28
Gmail	5.0.181103
Google App	62.0
Google Docs	1.2018.44204
Google Drive	4.2018.44203
Google Duo	43.0
Google Maps	5.5
Google Tasks	4.9.13
Grindr	4.3.0
Hot or Not	5.88.0
Hushed	4.7.2



Inbox	1.3.181103
Instagram	72.0
InstaMessage	2.9.7
Kakao Story	5.4.0
KakaoTalk	8.20.0
Keeper	14.0.2
KeepSafe	8.20.0
Kik Messenger	14.9.0
LINE	8.16.1
LinkedIn	9.1.108
Mail.Ru	9.11
Meet24	1.7.63
MobileVOIP Cheap Calls	2.0.5
Momo	8.10.5
Musical.ly	9.2.0
Nike+ Run Club	5.20
Odnoklassniki	7.32
OkCupid	23.1.0
Pinterest	6.77
QQ	7.9.0
SayHi	7.15
Scruff	5.6022
Skype	8.34
Snapchat	10.45.1.0
Swarm	6.1
Taxify	Cl.3.61
Telegram Messenger	5.0.17
Text Me Up	3.15.3
Text Me!	3.15.3
Text Now	9.1.0
textPlus	7.3.9
Threema	4.0.1
TigerText	7.9.1
Tinder	10.2.1
Twitter	7.36
Uber	3.326.10002
Viber	9.8.5
Vkontakte	5.4
Waze	4.45
WeChat	6.7.4
Weibo	8.11.1
WhatsApp	2.18.102
Yandex Browser	18.10.3.114
Yandex Mail	3.71.1
Yandex Maps	10.5.6



Yubo	3.9
Zalo	181103

Android : Nouvelles applis et mises à jour

65 applis mises à jour	
ASKfm	4.29.2
Booking.com	16.4.1
Coco - Dorado (applis)	7.6.1
DJI GO 4	4.3.4
Dropbox	120.2.2
Expedia	18.46.1
Facebook	198.0.0.53.101
Facebook Messenger	192.0.0.31.101
Firefox	63.0.2
Fitbit	2.83
Flipboard	4.2.5
Gmail	Version 8.10.21,220187835
Google Calendar	Version 6.0.8-220605953
Google Docs	1.18.442,01.45
Google Drive	2.18.432,04.45
Google Maps	10.3.2
Google Photos	4.5.0,220874418
Google Translate	5.25.1.RC06.220517201
Grindr	4.5.1
Hot or Not	5.90.0
Instagram	71.0.0.18.102
Kakao Story	5.4.0
KakaoTalk	8.1.2
Keeper	14.0.0
KeepSafe	9.21.0
Kik Messenger	14.10.0,16873
LINE	8.17.1
LinkedIn	4.1.244
LOCX Applock	2.3.1.061
Mail.Ru	8.1.0,25690
MeetMe	13.6.1,1605



Odnoklassniki	18.11.14
OkCupid	23.0.0
One Drive	5.20
Opera Mini	37.2.2254,133143
Opera Mobile	48.2.2331,133274
Outlook.com	2.2.252
Pinterest	6.89.0
Pokemon GO	0.127.2
SayHi	7.06
Scruff	5.6021
Skout	6.1.0
Skype	8.34.0.72
Snapchat	10.45.5.0
Swarm	6.1.1
Sygic	17.4.22
Text Me Up	3.15.2
Text Now	6.2.0.3
textPlus	7.3.9
TigerText	7.9.2,626
Tinder	10.1.0
Tumblr	12.1.0.01
Twitter	7.71.1-release.15
Uber	4.236.10001
UC Browser	12.9.7,1153
Viber	9.8.5.13
VIPole	2.0.0
Vkontakte	5.22
Voxer	3.18.18,21046
Waze	4.45.0.8
Weibo	8.11.1
WhatsApp	2.18.341
Yandex Browser	18.10.0,1012
Yandex Mail	4.10.1
Zalo	18.10.04



Signature électronique des fichiers d'installation

Vous pouvez valider l'intégrité des fichiers UFED de Cellebrite en vérifiant leurs valeurs de hash. Cela peut vous permettre de savoir si un fichier a été modifié.

Produit	MD5	SHA-256 (Recommandé)
UFED Physical Analyzer	6cc710912528b9a6e8137c92020694ca	6f593bb3d46b28ebd165a6d6eaa9fbaa6d5431997c5c5746617dc3a1dd667df8
UFED Logical Analyzer	eff0ab5ed5c883055f22daf3a6ff3517	d0cf4c67bb1fd2fcfe1da21b18e9a7fc72fad2fd4132f7af1ee99a51d52d92ba
Cellebrite Reader	a3e547ff8b313b44c0d1abdce5591e4f	8c26df9b0b47fec598bc53326d1c16b336d569ecce0baa89ee5b9c3ba9b48558

