事案に関係するキーワードがスマホに 記録されていないか探したい

Ver. 1.0



Copyright © 2023 Cyber Defense Institute, Inc. All Rights Reserved

目次

1	事案に関係するキーワードがスマホに記録されていないか探したい2
1.1	主に利用する機能



1事案に関係するキーワードがスマホに記録されていないか探したい

解析の説明に使用しているデータの詳細は、当サポートページに掲載の資料「解析を始める前に…」の「1.1 解析に使用しているデータについて」をご覧ください。またこちらの資料はそのデータを元に解析したもの ですので、お客様の環境とは異なります。必要に応じて読みかえていただきますようお願い申し上げます。

1.1 主に利用する機能

事案に関係するキーワードを探す際に主に使用する機能は「Search」と「Apple Notes」です。

> Search

デバイス内のあらゆるデータに対して以下の検索機能を実行することが出来ます。

詳細は、当サポートページに掲載の資料「Search 機能 解説ガイド」をご覧ください。

機能名	機能説明
Text	文字検索
Keyword lists	キーワードリストに一致するデータを検索
Hash sets	ハッシュセットに一致するファイルを検索
RegExp	正規表現による検索
Face sets	フェイスセットに一致する顔写真を検索
Hex	16 進数検索
Hex lists	ヘックス(16 進数)リストに一致するデータを検索

i) Extraction info 🚹 Export 🏹	x Reset filters	T
Search history < 🕻	Text Keyword lists Hash sets RegExp Faces sets Hex Hex lists 🏹 Find text 🔨 💙 Details	
Select keywords	Select keywords V Keyword lists Search	
	 Advanced settings 	
	Case sensitive Whole words only	
	Search in	
	✓ Parsed data	
	File metadata	
	File content None Max number of matches within a file for	
	Image: Image: Source Type ∨ Description Time stamp (Tokyo) ∨	
	No data in this section	
Filters		
No information		
Version: 15.2.0.246 Total: 0 Filtered: 0		

> Apple Notes

iOS デバイスの場合、General sections に が表示されます。Apple Notes では、iOS デバイス本体(ローカル)に保存されたメモデータ、iCloud と同期されるメモ、同期設定を行ったメールやカレンダー等のアカウントのメモが表示されます。

まい鍵マークは抽出したデータの中に鍵付きのデータがある事を示している							
🔊 Oxvaen Forensic®	Detective						
Image: Apple Notes - iPhone X							
Extraction info	Export -	X Reset filt	Timeline	Maps Ge	eo data 👻 Enter passwo	ord	
✓ Categories	28 ^	Notes	Timeline	j find te	5		
✓ iCloud ✓ Notes	7		✓ Status	鍵付きデータ	Created (Tokyo		
📝 Notes	7		A	pw=7.	2017/04/25 11:	1 So	
✓ iPhone ✓ Notes	9		C	PWFXI 添付画:	2016/08/23 14: 2016/07/04 16:	So file	

上記のような鍵付きのデータは、以下の手順で解除する事が可能です。

- 1. 鍵付きのデータをクリックで選択
- 2. 「Enter password」をクリック
- 3. 表示される入力フォームにパスワードを入力し、[Apply]をクリック
- 4. [Decrypt data]をクリック
- 5. [Reload data]をクリック

👂 Oxygen Forensic® Detective — 🗌						- 0			
三 ŵ in Apple No	😑 🎧 🎲 Apple Notes - iTunes backu ×								
1 Extraction info	Export	\bigvee_{\times} Reset filters	i 📋 View	🗸 🔀 Map	🥦 Enter pa	ssword			
📝 Apple Notes	<: I	All data Files	Timeline		Find text		- AV	>> Details	
✓ Categories	16	Votes			S Appl	ecryption			×
✓ iCloud	7		✓ Status	Title		Enter pas	sword		
✓ Notes	7		8	新PWテスト		Entre provide			
📝 Notes	7		A	PW解I除テスト		Enter password to	o decrypt data		N
✓ iPhone	6		8	PWテスト	_				
✓ Notes	5			添付面像		Password hint:			ľ
📝 Notes	4					 いつもの4桁 			
Attachments	1	1000							Consul
✔ 仕事用	1	1.00		100				лрру	Cancel
📝 Notes	1	-	_	-	and the second se			(UTC)	02:14:45 (UTC-
Cached files	3		••	**				Text	a [Encrypted
		-	-						data]
	3	_					*	Password	e [Encrypt data] いつもの4桁

> Apple Note に関する補足

Apple Note には、iCloud 設定やアプリケーションのアカウント設定からメモへの同期を許可する事で「デバイス本体に保存されるメモ」以外のメモが追加されます。





改訂履歴

版数	発行日	改訂履歴
Ver. 1.0 2023年03月09日		初版発行