Oxygen Forensic (Detective/Device Extractor/Cloud Extractor) ログモードでの起動方法

Ver. 1.0



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

目次

1	ログモードの用途について	2
2	Detective ログモードの起動手順	2
3	Device Extractor ログモードの起動手順	3
4	Cloud Extractor ログモードの起動手順	4

1 ログモードの用途について

Oxygen Forensic(Detective/Device Extractor/Cloud Extractor)で何らかの問題が発生した際、トラブル シューティングのためにログのご送付をお願いする場合がございます。その際には、ログモードで起動いた だくと自動でログが作成されます。

本マニュアルでは、このログモードの起動手順について解説します。

2 Detective ログモードの起動手順

- 1. もし Oxygen を起動している場合は終了してください
- 2. タスクバーから検索を起動(もしくは Win+Qキー)し、[アプリ]タブを選択してください
- 3. 検索ボックスに『Detective』と入力してください
- 4. 複数件ヒットしますが、『Oxygen Forensic Detective (Log enabled)』を実行してください

•	すべて アプリ ドキュメント ウェブ その他 ▼ 	X		
	アプリとの最適な一致			
	Oxygen Forensic Detective (Log enabled) דידיו	Oxygen Forensic Detective (Log enabled)		
	アプリ			
	Detective data base import >	アプリ		
	• Oxygen Forensic Detective >			
	Oxygen Forensic Detective 12	□ m< □ 管理者として実行		
	Oxygen Forensic Detective 11	□ ファイルの場所を開く		
	 Oxygen Forensic Detective をアンイン フトールナス 	- ロ スタートにピン留めする		
	Ar-1090	─□ タスク バーにピン留めする		
	enabled)	値 アンインストール		
	Oxygen Forensic Detective 11 (Log enabled)			
	ストア			
	💼 Detective - Microsoft Store 内のアプリを検索する			
%				
A 😜				
10:21 金曜日				

- 5. Oxygen Forensic Detective が起動するので、調査したい問題が再現するように操作してください
- 6. 問題が再現されましたら、そのまま Detective を終了してください
- エクスプローラーで、ファイルパス『C:¥Users¥<ユーザ名>¥Oxygen Forensic¥Logs』を開くとログ が表示されますので、こちらを当社宛にご送付ください



		> Oxygen Forensic > Logs	✓ ひ Logsの検索	
ta ^	E	名前 ^	更新日時	種類
ロード先 🖈		LOG_OxyDetective_23 07 14 15 23 25 366.txt	2023/07/14 15:31	テキストドキュメント
*	1			

3 Device Extractor ログモードの起動手順

- 1. もし Oxygen を起動している場合は終了してください
- 2. タスクバーから検索を起動(もしくは Win+Qキー)し、[アプリ]タブを選択してください
- 3. 検索ボックスに『Detective』と入力してください
- 4. 複数件ヒットしますが、『Oxygen Forensic Detective (Log enabled)』を実行してください



- 5. Oxygen Forensic Detective が起動するので、Detective から Device Extractor を起動して抽出して ください(問題が再現する条件で抽出を実行してください)
- 6. 抽出が終了しましたら、Device Extractor のウィンドウを終了させてください
- う自動でエクスプローラーが起動しログファイルの保存先が表示されますので、こちらを当社宛にご送付 ください



I	< ユーザー > Oxygen Forensic > Logs	ې <mark>ن ب</mark>	Logsの検索
^	■ 名前	●更新日時	種類 サイズ
	LOG_DeviceExtractor_23 07 14 15 23 33 365.txt LOG_OxyDetective_23 07 14 15 23 25 366.txt	2023/07/14 15:23 2023/07/14 15:23	テキスト ドキュメント 5 KB テキスト ドキュメント 0 KB

4 Cloud Extractor ログモードの起動手順

- 1. もし Oxygen を起動している場合は終了してください
- 2. タスクバーから検索を起動(もしくは Win+Qキー)し、[アプリ]タブを選択してください
- 3. 検索ボックスに『Cloud Extractor』と入力してください
- 4. 2件ヒットしますが、『Oxygen Forensic Cloud Extractor (Log enabled)』を実行してください

پ	すべて アブリ ドキュメント ウェブ その他 ▼	X		
	アプリとの最適な一致	-		
	Oxygen Forensic Cloud Extractor (Log enabled) アプリ			
	アプリ	Oxygen Forensic Cloud Extractor (Log		
	Oxvgen Forensic Cloud Extractor >	enabled)		
	۶۶ ۲	r 2 Y		
	🔒 cloud extractor - Microsoft Store 内のアプリを検	□' 開<		
	索する	□ 管理者として実行		
		□ ファイルの場所を開く		
		-□ スタートにピン留めする		
		-□ タスク バーにピン留めする		
		値 アンインスト−ル		
>				
A 😜				
10:09 月曜日				

- 5. Oxygen Forensic Cloud Extractor が起動するので、抽出(問題が再現する条件で抽出を実行してくだ さい)
- 6. 抽出が終了しましたら、Cloud Extractor のウィンドウを終了させてください
- 7. 自動でエクスプローラーが起動しログファイルの保存先が表示されますので、こちらを当社宛にご送付 ください



> PC >	OS (C	:) > ユーザー > Oxygen Forensic > Logs	ٽ ~		
	^	■ 名前	更新日時	種類	サイズ
先	*	LOG_OxyCloudExtractor_23 07 10 10 08 51 737.txt	2023/07/10 10:13	テキスト ドキュメント	28 KB
	*	🗹 📙 OxyCloudExtractor_23 07 10 10 13 23 859.zip	2023/07/10 10:13	圧縮 (zip 形式) フォ	4 KB

改訂履歴

版数	発行日	改訂履歴
Ver. 1.0	2023年07月14日	初版発行