Cloud Extractor を用いた WhatsApp iCloud Backup の抽出手順

Ver. 1.0



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

目次

1	イントロダクション	. 2
2	抽出手順	. 2
3	メッセージの復号手順	. 8
4	インポート手順	11

1 イントロダクション

本ドキュメントは、以下の検証環境で実施した検証を書き起こしたものです。 環境が異なる場合は再現出来ない可能性がございますので、ご了承ください。

- Oxygen Forensic Detective v16.1.0.200
- Cloud Extractor v10.1.0.250
- WhatsApp iOS 版 v2.23.25.85
- 本手順を実行しますと、ログイン中のスマートフォン側の WhatsApp アプリケーションがログアウト される可能性がございます。あらかじめご了承ください。
- WhatsAppの認証コードは連続で取得すると、数分から数時間のロックが掛かる可能性がございます。
 あらかじめご了承ください。

2 抽出手順

2.1 Cloud Extractor を起動し、[New extraction]をクリックする





2.2 [Owner name]に何らかの名前を入力し、[Next]をクリックする

😯 Oxygen Forensic® Cloud Extractor - 10.1.0.250 — 🗆 🗙								
Oxygen Forensic® Cloud Extractor - 10.	Account owner Fill in the information about th Add photo	e account owner and the case Owner name Kana Tanash Owner email Owner phone number Evidence number Incident number Cloud backups folder C:¥Users¥	ts¥Clou	Extraction alias				
≅ 0 0			Back	Next	Cancel			

2.3 アプリー覧から[WhatsApp iCloud Backup]を選択し、[Add credentials]をク

リックする

Oxygen Forensic® Cloud Extractor - 10.		o x
Oxygen Forensic* Cloud Extractor	Image: Constraint of the state of the s	×
	Select all Add	credentials
≅ ? 0	Back Next	Cancel

2.4 認証ポップアップが表示されるので、iCloud の認証情報を入力して[Apply]をク

リックする

	WhatsApp QR	WhatsApp	WhatsApp	WhatsApp		whatsapp	
en Forensic® d Extractor		WhatsApp iClou Username/Password Username Password	d Backup Token Proxy .com Apply	Clos	••••••••••••••••••••••••••••••••••••••		
) () ()		•	Select	all Add	credentials

2.5 「Check iOS device connection」のポップアップが表示されるが、本手順書で

は[Skip]をクリックする

Oxygen Forensic® Cloud Extractor - 10.1.0.250				- 0 ×
	Services	Credentials		Validated
	WhatsApp iCloud Backup	Username Password	Bicloud.com	♥ ●
Cloud Extractor	 WhatsApp iCloud Backup Add cloud service Check iOS device connect Check iOS device connect WhatsApp iCloud Ba actions: Prepare any jailbro connection. Prepare any jailbro connection. Launch OxyAgent a Type the host and 0 click the "connect" Don't close the OxyA till the end of extract Read installation instru IP address or hostnam (e.g. 192.168.4.151 	ion tsApp iCloud Backup ckup service needs some addit ken device with iOS 12.3 or late pp on the device. pport from the app. button. Agent app or lock the device tions e Connect	ional er for e screen Port 8899	
			Back Ston	Cancel



2.6 スマートフォンを用いた認証方法が提案されるので、「Send verification code to

trusted device」をクリックする(この際、スマートフォンはロックを解除した状

態で手元にご用意ください)



2.7 スマートフォンに verification code がポップアップで表示されるので、Cloud



Extractor のポップアップに入力して[OK]をクリックする



2.8 無事に認証が完了すると、Validated に緑のチェックが付くので[Next]をクリッ

クする



2.9 抽出前の確認画面に遷移するので、抽出項目を確認して[Next]をクリックする

Oxygen Forensic® Cloud Extractor - 10.	1.0.250						
	Services			Categories			
Oxygen Forensic* Cloud Extractor	WhatsApp ICloud Backup -	₽icloud.com		Other files			
		Back		Next	C	Cancel	

2.10 抽出が開始される。完了したら[Next]をクリックする



3メッセージの復号手順

「Services decryption」画面に遷移する。チャットを復号する場合は、[Get 3.1

Oxygen Forensic® Cloud Extractor - 10.1	.0.250						D	
	Services decryption Decrypt encrypted data from services below							
	Encrypted services	~	Phone number	Confirmatio	n code		Statu	IS
Oxygen Forensic® Cloud Extractor	💽 WhatsApp ICloud Backup -		8:	Decryption 201	on via security code)
		Ple	ase review the WhatsApp	data extraction	manual			
			Get sec	curity code	Enter PIN	D	ecrypt)	
≣ 0 0					Skip	(Cancel	

security code]をクリックする

「Authentication parameters」 ポップアップが表示されるので、今回は[SMS] 3.2



を選択して[Apply]をクリックする



3.3 スマートフォン側に SMS でセキュリティコードが届くので、Cloud Extractorの

[Enter the security code here]をクリックし、セキュリティコードを入力して

[Decrypt]をクリックする







4 インポート手順

- Oxygen Forencie® Cloud Extractor 10.10.20
 • ×

 Extraction finished!
 Data is successfully extracted from the Cloud

 Extraction finished:
 Determine in F900822015(x69783247088966591E3

 Cocourt owner:
 Cocourt owner:

 Oxygen Forensic®
 Cloud services

 Cloud Extractor
 Cloud Services

 Image: Cloud Extractor
 Image: Cloud Backup Image: Point and the cloud Backup Image: Point an
- 4.1 「Extraction finished!」画面に遷移したら、[Next]をクリックする

4.2 [Open extracted data in Oxygen Forensic Detective]をクリックし、デー

タをインポートする





4.3 インポートすると、以下のように表示される

👽 Oxygen Forensic® Detective								
😑 🎧 ' 🙆 WhatsApp Messenger - Clo >	😑 🎧 诸 WhatsApp Messenger - Clo ×							
뉦 Extraction info 🚹 Export • 🏹 Reset filters 📋 View • 🛛 🖓 Maps 👷 Geo data • 🔊 Translations •								
🙆 WhatsApp Messenger 🛛 😽 🕻	All data Files	Contacts Chats Timeline	e Social Graph					
✓ Categories 10	🖸 🕁 🖉	🗠 🔄 🗠 Remote party	Remote party name	Time stamp (Tokyo)	Text			
✓ @icloud.com (Wh 10	🔽 🕁	81	佐井場攻太	2018/07/24 14:50:02 (UTC+9)	(tt)w			
Encrypted bases 6	- 🗠	2 81	佐井場攻太	2018/07/24 14:49:51 (UTC+9)	こっちも使えるようになったんだね			
✓ 81 6	2 🕁	(3 8:	佐井場攻太	2018/07/24 14:49:14 (UTC+9)	おっ			
🎦 BackedUpKeyValue.s 1	Solution	2 8:	佐井場攻太	2018/07/24 14:42:45 (UTC+9)	whatsappもインストールしてみました。			
ChatStorage.sqlite.enc 1								
🔓 current_wallpaper.jp 1								
Ranking.sqlite.enc 1								
🔓 Sticker.sqlite.enc 1								
UserDefaults.plist.enc 1								
✓ 81 4								
✓ Chats 4								
✓ Private 4								
佐井場攻太 4								

改訂履歴

版数	発行日	改訂履歴
Ver. 1.0	2023年12月25日	初版発行