OxyAgent を用いた LINE データ抽出ガイド

Ver. 1.1



内容

1	イントロダクション
1.1	対象デバイスの前提条件2
2	OxyAgent のインストール 2
2.1	USB ケーブル経由のインストール 2
2.2	メモリカード経由のインストール6
2.2	Wi-Fi 経由のインストール7
3	LINE データの抽出
3.1	EXTRACT THIRD PARTY APPLICATIONS DATA
3.2	LINE データ抽出作業11
4.	Oxygen Forensic Detective へのインポート
4.1	ADB を使用して、抽出したファイルを確認する15
4.2	ADB を使用して、抽出したファイルをデバイスから PC にコピーする 15
4.3	PC にコピーした抽出ファイルを Detective にインポートする16

1 イントロダクション

1.1 対象デバイスの前提条件

本ガイドで案内している手順を実施する前に、以下の条件を満たしているかをご確認ください。

- > ロック解除出来るデバイスであること
- ▶ 機内モードになっていること

2 OxyAgent のインストール

本手順では OxyAgent を使用します。以下では複数のインストール方法を紹介しています。お手元のご環境 に合った方法をお試しください。

2.1 USB ケーブル経由のインストール

① Oxygen Forensic Extractor を開き、[Android OxyAgent extraction]を押下します



② 注意書きを読み、デバイスの状態を確認してください。確認後、チェックを入れて[Connect]ボタンを押

下します

Oxygen Forensic® Extractor v.13.6.	0.47 –
Oxygen Forensic® Extr View connection instructions.	ractor
	Connection instructions パッテリーの残量 を確認してください。 デバイスがロックされていない ことを確認してください。 機内モード に設定してください。 USBデバッグモード であることを確認してください。 Android 4.2.2 以降のデバイスを使用している場合、RSAキー の受け入れを許可してください。 スリーブモードにしない 設定になっていることを確認してください。 USBモデム オブションを無効にしていることを確認してください。 USBモデム オブションを無効にしていることを確認してください。 ドライバが正しくインストールされている ことを確認してください。 If you stil have questions on device connection you can contact us by e-mail support@oxygen-forensic.com. Please always specify device model name and Android OS version.
	< Back Connect Cancel

③ デバイスの USB デバッグを許可した後、チェックを入れて[Connect]ボタンを押下します

Sxygen Forensic® Extractor v.14.3.1.0	-0		×
Oxygen Forensic® Extractor Androidデバイスが接続されていません。			
First Cardon Orabes Cive/Set and Code Set of Code Set			
Connect	Sear	ch new devic	e

- ④ デバイスが正常に接続されると、[Install agent]ボタンが表示されるので押下し、OxyAgent をデバイス にインストールします。
- ☞ OxyAgent のインストールが完了した後、Extractor は閉じてください
- 接続に失敗する場合は、ケーブルの挿し直しや、USB ポートの変更をお試しください

Oxygen Forensic® E 接続されたデバイス	Extractor		
Connected!	デバイスが正常に接続さ Device information Model: IMEI: Hardware Revision: Software Revision: Software Revision: Install agent Select sections to be extractor □ Take the snapshot of the file s 抽出するデータの保存先を選択して C:¥Users¥ ¥Document	hました! Google Pixel 3a N/A 10 DxyAgentをインストー/ しました。 ed from th Sevice ystem with してはの th になさい。 s¥Oxygen Forensicke	
		E	Cancel

- OxyAgent のインストールが完了すると、デバイス側でコンテンツのキャプチャ・記録に関するポップア ップが表示されますので、[今すぐ開始]をタップしてください。
 - ポップアップの表示内容はデバイスの環境によって異なります





⑥ [TERMINATE]をタップします



⑦ [EXTRACT OTHER DATA]をタップします

Image: Solution in the second sec
Extraction is finished, you can now remove agent from device and proceed with extracted data analysis
EXTRACT OTHER DATA
UNINSTALL
EXIT
Copyright © 2000-2021 Oxygen Forensics Version: 5.6.0.38

⑧ 「3. LINE データの抽出」に進んでください

2.2 メモリカード経由のインストール

① [Android manual OxyAgent extraction]を押下してください



② [Save]を押下して SD カードに APK ファイルを保存してください

Oxygen Forensic® Extractor v.13.6.0.47 –	
Oxygen Forensic® Extractor OxyAgent経由でデバイスを接続	
Data Agentの推出手順 * OxyAgent APKを5Dカードに保存するための保存先を指定してください Dx¥ 7.15 GB (OXYGEN) * 5Dカードを安全に取り外してください * デバイスに5Dカードを全様して、のxyAgentを全しストールしてください * OxyAgentを起動し、要求されたすべての確認を確認してください * OxyAgentを起動し、要求されたすべての確認を確認してください * SDカードを全に取り外してください * 5Dカードを全に取り外してください * SDカードを全に取り外してください * NEXT ボタンをクリックし、抽出されたデータがあるフォルダーを選択し、手順に従ってください。 * すでに抽出したデータがある場合は、このウィンドウをスキップして、次の画面で抽出したデータへのパスを指定してくだ	Save Č(\o
< Back Next >	Cancel

- ③ デバイス内で保存した APK ファイルを実行し、OxyAgent のインストールを行ってください
- ④ 「3. LINE データの抽出」に進んでください

2.2 Wi-Fi 経由のインストール

- ① PC とデバイスを同じネットワークに接続してください
- ② [Android OxyAgent over WiFi extraction]を押下してください



③ [インストールしてください]を押下すると、OxyAgent をインストールするためのリンクまたは QR コードが表示されます。表示される手順に従ってインストールを完了させてください



④ 「3. LINE データの抽出」に進んでください



3 LINE データの抽出

3.1 EXTRACT THIRD PARTY APPLICATIONS DATA

- ① OxyAgent を起動してください
- ② [EXTRACT THIRD PARTY APPLICATIONS DATA]を選択してください

🔤 🔤 🕷 😽 🛧 89% 🖹 午後 2::		
WHA	AT DO YOU WANT TO DO?	
Öö	EXTRACT TO INTERNAL/ EXTERNAL STORAGE	
Ĵ	TAKE SCREENSHOTS AND RECORD THE SCREEN	
Ì	EXTRACT THIRD PARTY APPLICATIONS DATA	
	EXTRACT DATA OVER Wi-Fi	
Cop	yright © 2000-2021 Oxygen Forensics Version: 5.6.0.38	

③ PREPARING 画面で、[Change folder]をタップしてください



- ④ デフォルトでは、`/storage/emulated/0`が Output folder(保存先)に選択されています。今
 回は、変更せずそのまま[NEXT]をタップします。
- ☞ Output folder を変更する場合は、[Select]をタップしてください



⑤ PREPARING 画面に戻り、[Go to settings]をタップしてください



⑥ ユーザー補助>サービスに遷移するので、[Oxygen Forensic Agent]を ON にしてください

く ユーザー補助
シングルタップモード アラーム、カレンダー、タイマーの通知の解 除、着信の応答や拒否を1回のタップで実行し ます。
ユーザー補助を管理 ユーザー補助設定をインポートおよびエクスポート、 または他の端末と共有します。
サービス
Lookout OFF
KakaoTalk ^{OFF}
Oxygen Forensic Agent OFF
他の機能をお探しですか?
かんたんモード SOSメッセージを送信
■ ※ % ■ 午前 9:56
< OXYGEN FORENSIC AGENT
OFF
Oxygen Forensics accessibility service provides a possibility to automate user actions and extract data from device by means of UI

- ⑦ Oxygen Forensic Agent から権限を要求するポップアップが表示されるので、[OK]をタップしてくださ
 - い(機種によって多少表示内容が異なる可能性があります)



⑧ デバイスの戻るボタンを押し、OxyAgent 画面に戻ってください

③ [Select destination folder for extraction] と[Turn on accessibility settings]にチェックを入れた後、
 [CONTINUE]ボタンをタップしてください



3.2 LINE データ抽出作業

- ① LINE アプリが起動している場合は、アプリを終了してください
- ② SELECT APPLICATION TO ACQUIRE 画面で[Line]を選択してください



Copyright © 2021 Cyber Defense Institute, Inc. All Rights Reserved

CyberDefense

③ 注意書きをご確認いただき、[CONTINUE]ボタンをタップしてください



和訳:

Note: 抽出が完了するまで、デバイス画面を操作しないでください。 画面上で発生する全ての着信通知とアクションを無視してください。 データ抽出を確実に成功させるために、下記を推奨します。 ・ 機内モード設定 ・ 充電器の接続 ・ データ抽出が終了するまで、バッテリー最適化アプリを停止する 上記を実施しない場合は、抽出プロセスが中断される可能性があります。

- ④ Oxygen Forensic Agent からコンテンツのキャプチャ・記録に関するポップアップが表示されるので、
 [今すぐ開始]をタップしてください
 - ポップアップの表示内容はデバイスの環境によって異なります



```
Copyright © 2021 Cyber Defense Institute, Inc. All Rights Reserved
```

⑤ SELECT DATA TO ACQUIRE 画面に遷移します。全てを抽出する場合は、[EXTRACT ALL DATA]を選択

してください



⑥ [START]をタップし、抽出を開始してください

	🔊 ¥ 🛧 89% ■ 午後 2:26
	SELECT DATA TO ACQUIRE
	Line
	Configure all data extraction
	Save avatars during extraction
Ex	tract all recent chats
_	
	START
c	Copyright © 2000–2021 Oxygen Forensics Version: 5.6.0.38

- ⑦ 自動で LINE アプリが起動したのち、LINE アプリ画面に遷移し、抽出が開始されます
 - LINE アプリ画面に遷移後、自動でトーク画面やプロフィール画面が展開され、自動操作が 実行されますが、仕様ですので触らずそのままお待ちください
 - ④ 途中、LINEの画面上でエラーが表示されても、触らずそのままお待ちください。

 ⑧ 個別に抽出した場合は、SELECT DATA TO ACQUIRE 画面に[FINISH]ボタンが表示されるので、タッ プしてください

PP.	🔝 💐 🛧 33% 🕯 午前 9:59
	SELECT DATA TO ACQUIRE
	Line
	8 EXTRACT USER INFO
	2 EXTRACT CONTACTS
	EXTRACT CHATS
	EXTRACT FILES
	EXTRACT ALL DATA
	Copyright © 2000-2021 Oxygen Forensics Version: 0.0.0.0

⑨ EXTRACTION IS COMPLETE 画面に遷移します。[EXIT]をタップして終了してください

🔝 👯 🛧 33% 🖹 午前 9:59
EXTRACTION IS COMPLETE
traction is finished, you can now move agent from device and proceed th extracted data analysis
EXTRACT OTHER DATA
UNINSTALL
EXIT

- 抽出に失敗した場合は、以下をご確認ください
 - > LINEを開いたまま抽出を実行すると、エラーが発生します
 - > 抽出実行中にデバイスを操作すると、エラーが発生します
 - > オンライン状態で抽出を実行すると、抽出に失敗する可能性があります

4. Oxygen Forensic Detective へのインポート

4.1 ADB を使用して、抽出したファイルを確認する

adb を使用しない場合は、デバイスの機種ごとのマニュアルを確認し、

デバイス内のフォルダアプリ等から3.1-④で設定した保存先ファイルパスをご確認ください。

- ① デバイスを PC に接続し、デバイス側で USB デバッグを許可する
- ② コマンドプロンプトを立ち上げ、下記のコマンドを入力し、抽出したファイルを確認する
- ③ adb.exe や抽出データの保存先ファイルパスは、お客様環境に合わせて書き換えてください。

"C:¥Program Files¥Oxygen Forensics¥Oxygen Forensic Detective¥DeviceExtractor¥adb¥adb.exe" ls /storage/emulated/0

☞ 上記の出力結果が多すぎる場合は、以下のようにファイル名で絞り込むことも可能です。

"C:¥Program Files¥Oxygen Forensics¥Oxygen Forensic Detective¥DeviceExtractor¥adb¥adb.exe" ls /storage/emulated/0 | findstr <LINE 抽出を実行した日付(YYYY-MM-DD 形式)>

③ 実行例(「2022-03-28」でファイル名を絞り込んだ場合)

4.2 ADB を使用して、抽出したファイルをデバイスから PC にコピーする

adb を使用しない場合は、デバイスの機種ごとのマニュアルを確認し、

3.1-④で設定した保存先ファイルパスから PC にデータを移動させてください

- ① デバイスを PC に接続し、デバイス側で USB デバッグを許可する
- ② コマンドプロンプトを立ち上げ、下記のコマンドを入力する
- ☞ adb.exeのファイルパスや保存先ファイルパスは、お客様環境に合わせて書き換えてください。

"C:¥Program Files¥Oxygen Forensics¥Oxygen Forensic Detective¥DeviceExtractor¥adb¥adb.exe" pull /storage/emulated/0/<4.1-②で確認し たファイル名> <PC の保存先ファイルパス>



☞ 実行例

ש בעאר לעסל אין איז איז איז פאר פאנער פ ער גער פאנער פאנ			×
C:¥Users¥ ndersen >"C:¥Program Files¥Oxygen Forensics¥Oxygen Forensic Detective¥De ¥adb¥adb.exe" pull /storage/emulated/0/2022-03-28_11-38-51 /storage/emulated/0/2022-03-28_11-38-51/: 170 skipped. 4.2 MB/s (32948127 byte	viceEx s in 7	(tract) 7. 428s)	or)
C:¥Users¥ Levenne >"C:¥Program Files¥Oxygen Forensics¥Oxygen Forensic Detective¥De ¥adb¥adb.exe" pull /storage/emulated/0/2022-03-28_11-38-51.manifest.xml /storage/emulated/0/2022-03-28_11-38-51.manifed, 0 skipped. 0.1 MB/s (847 byte	viceEx s in C	ktracto). 011s)	or

4.3 PC にコピーした抽出ファイルを Detective にインポートする

- ① Oxygen Forensic Detective を起動します
- ② [Home]>[Import]>[OxyAgent extraction]をクリックします
- ③ 4.1 で<PCの保存先ファイルパス>に指定したフォルダ配下から、XMLファイル(.manifest.xml)を選択
 - し、[開く] をクリックしてください



 ④ Import wizard が起動し、インポート時のオプションが表示されます。特に変更がない場合は、そのまま [Import]をクリックしてください

👽 Import wizard - Template: Default		— 🗆 X				
Extraction	Extraction	Save template				
i] Information about extraction						
🚯 General import settings	Add the extraction file to be imported into Oxygen $Forensic^{\circledast}$ Detective.					
Nested archives unzip	Path to the file					
dvanced analytics	C:¥Users¥user¥work¥0¥0¥2022-03-28_11-38-51.manifest.xml					
Q Search	Extraction type					
📃 Summary						
	Password					
	Default					
	Select an import settings template from the list					
	Default					
Templates						
	Back Next	Import Cancel				

⑤ Oxygen 上で正しくパースされていれば成功です

Oxygen Forensic	- 0	
= ☆		Ē
Cases (i) >	 OxyAgent extraction (0) Time zone (UTC+00:00) UTC OS Android OS 10 Incident number Evidence number Evidence number 	×
Considerat extraction (0)		
Signal Accounts and Passwords Q Contacts Piles Piles Signal Reports Snapshots Piles Piles	1 2785 2775 000000000000000000000000000000000000	<u>8</u>
(a) (ke) extended (b) (C.R. Q. Search (c) Social Graph (c) Statetics (c) Timeline (c) Applications (c) Line	180 Image: State of the sta	
u u e	Faces Key Evidence OCR 0.C.R. Q Search & Social Graph in Statistics (L) Timeline 100 Applications 1	
Find text		
Version: 14.3.1.0 Total extractions: 19		

Copyright © 2021 Cyber Defense Institute, Inc. All Rights Reserved



Oxygen Forensic [®] Determine	ective							- 0	×
😑 🎧 🧔 Line - OxyAgent extraction ×					Ŧ				
i Extraction info 🚹	Export 🗸	∇_{\times} Reset fil	ters 📒 View 🗸 🏹	Maps					< Þ
😋 Line		All data Files	Contacts Chats Timeline	Social Graph	Find text	~ ~	>> Details		
✓ Categories	938	Chats			1	80 ^	Source file	e ip.naver.line.a	nd
🔬 Account	1		🗸 😪 🗠 Remote 🗸	Time stamp (Tokyo)	Text		Source file	e 76.0 KB	
Q Contacts	5			2022/02/10 10:44:00 (LEC 10)		71	size	e	
44 Group chats info	1			2022/02/18 18:44:00 (UTC+9)	「ビイカスのスタンノを抽力するよく、気に入らたスタンノルのうたら、デエアクロ	νCα 107	Source table	ine_messages line_chats	, ,
✓ ♀ Chats	180		0 / 2 平 法	2022/02/17 13:50:00 (UTC+9)	[これはへにもとりやりい日前ことはの人タンクによ。ゆることの著者をタップ	07.			
✓ ^Q Private	168			2022/02/17 12:00:00 (UTC+9)	18年に9.		Direction	1 🕝 Incoming	
LINE	10		○ 251/18 ◎ 255/18	2022/02/17 12:00:00 (UTC+9)	20年2月11日90日12月11日		Demet	message - 夕照 抽	
LINEスタンプ	119		 ・しまいせ ・11NE7かご 	2022/02/17 12:50:00 (UTC+9)	「「フマーピー日棠ことば(茨聿きアート)」「銘碑の」みバスフないプロ新作フ	<i>b</i> 1	party	: ~습뢰/11함 V	
1056	2		 (ろさん) 	2022/02/16 18:01:00 (LTC+9)	「たいだはあれがとうございました!		Time stamp	2021/11/08	
佐开場大吉	1		▲ 4500	2022/02/16 18:00:00 (LTC+9)	あの後本 コロナだし、プレゼン小だけにしようかって話になって		(Tokyo)) 14:23:00 (UTC	+9)
1号能慶次	30		2 くろさん	2022/02/16 18:00:00 (UTC+9)	「スタンプ」		Text	1 やってるといえ	t
治野椿	6		2 名野椿	2022/02/16 17:59:00 (LTC+9)	※抑令のやつ				
V 4 Group	12		② 名野椿	2022/02/16 17:59:00 (UTC+9)	昨日言ってか話なんだけど		Key Ev	🖉 Add tag 🗋	Note
1等能慶/次, 治野 悟	12		CINEスタンプ	2022/02/15 19:50:00 (UTC+9)	LINE選抜クリエイター6名の新作スタンプが登場!1		<u> </u>	CP	_
Attachments	1		C LINEスタンプ	2022/02/15 12:50:00 (UTC+9)	「えびにゃんが動くスタンプになって登場!おいちそうな(?)にゃんこのスタン	プで			
Cache	750		C LINEスタンプ	2022/02/15 11:50:00 (UTC+9)	「「動く!えびにゃん」「うさぎ & くま100% 死語 うごく」新作スタンプ2種類	登北			
Suckers	/49		C LINEスタンプ	2022/02/14 19:50:00 (UTC+9)	- 「連休明け、がんばりましょう…]				
images	1		C LINEスタンプ	2022/02/14 13:50:00 (UTC+9)	[あなたにおすすめのスタンプ]				
			CALINEスタンプ	2022/02/04 18:46:00 (UTC+9)	[オススメのスタンプを紹介するよ! 気に入ったスタンプがあったら、チェック!	πa			
			(2) 名野 椿	2022/02/03 14:21:00 (UTC+9)	お久しぶりですー				
			(2) 名野 椿	2021/11/08 14:23:00 (UTC+9)	やってるといえばやってます◎				
			(3) LINEスタンプ	2021/11/01 17:50:00 (UTC+9)	[あなたにおすすめのスタンプ]				
			C LINEスタンプ	2021/11/01 13:50:00 (UTC+9)	[大人気「すこぶる動くウサギ」とユニクロ公式キャラクター「天使」の動くコラ	ボス			
			CALINEスタンプ	2021/10/09 11:50:00 (UTC+9)	[今週の人気クリエイターズスタンプはこちら!]				
			🙆 LINE	2021/10/08 17:18:00 (UTC+9)	他の端末でLINEにログインしました。 あなた自身がログインした場合は、	ເທະ			
			C LINE	2021/10/08 17:18:00 (UTC+9)	【重要】他の端末のLINEから、あなたの電話番号による認証が要求され				
		<				>			
		Group by: Yes	ar Month Day		2020年4月14-2022年3月25	\times			
						-			
Eind toyt			and the second sec		- <u> </u>				
Version: 14.3.1.0 Total: 938	^ ¥ Eiltered	2020年4月14 1:938 Selecter	: 1		20224	3月25			





改訂履歴

版数	発行日	改訂履歴		
Ver. 1.0	2021年06月25日	初版発行		
Ver. 1.1	2022年03月29日	v14.3 に対応		