

デバイス所有者が送受信したメッセージの内容を知りたい

Ver. 1.0



目次

1	デバイス所有者が送受信したメッセージ内容を知りたい.....	1
1.1	主に利用する機能.....	1

1 デバイス所有者が送受信したメッセージの内容を知りたい

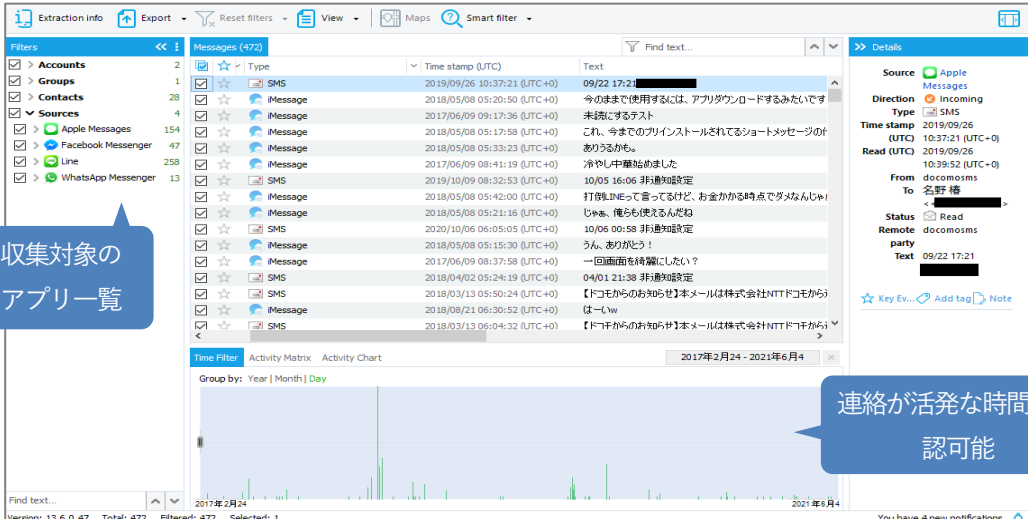
解析の説明に使用しているデータの詳細は、当サポートページに掲載の資料「解析を始める前に…」の「1.1 解析に使用しているデータについて」をご覧ください。またこちらの資料はそのデータを元に解析したもので、お客様の環境とは異なります。必要に応じて読みかえていただきますようお願い申し上げます。

1.1 主に利用する機能

デバイス所有者が送受信したメッセージの内容を知りたい時に主に使用する機能は「Messages」と「Applications」です。

➤ Messages

デバイス内のメッセージは、「Messages」から確認可能です

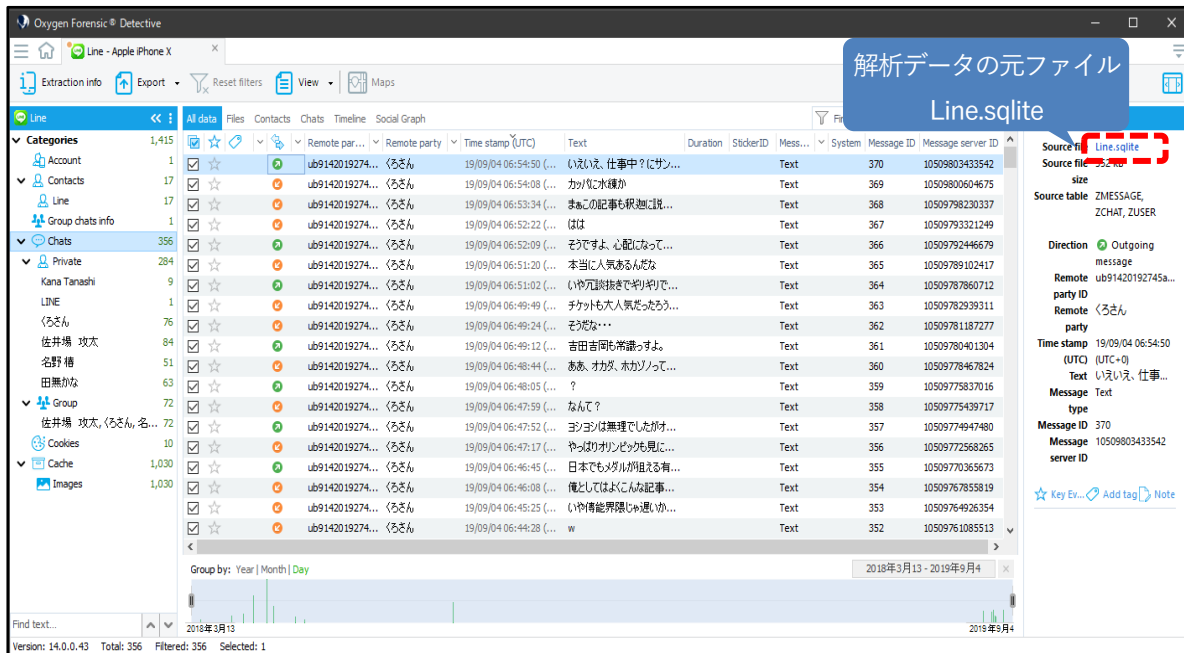


The screenshot displays the CyberDefense interface for analyzing messages. On the left, a 'Filters' sidebar shows a tree view with 'Sources' expanded to list various messaging apps like Apple Messages, Facebook Messenger, Line, and WhatsApp Messenger. The main area shows a table of messages with columns for 'Type', 'Time stamp (UTC)', and 'Text'. A 'Time Filter' section at the bottom includes an 'Activity Matrix' and an 'Activity Chart' showing message activity over time. Two blue callout boxes highlight key features: one points to the 'Sources' filter with the text '収集対象のアプリ一覧' (List of target applications), and another points to the 'Activity Chart' with the text '連絡が活発な時間を確認可能' (Possible to confirm active communication times).

➤ Applications

メッセージアプリごとの詳細な解析をしたい場合は「Applications」からLINE等のアプリケーションを選択します。
今回は例として「LINEの解析画面」、「Kakao Talkの解析画面」を掲載します。

➤ LINEの解析画面



The screenshot displays the Oxygen Forensic Detective application interface. The main window shows a list of chat messages with columns for 'Remote party', 'Time stamp (UTC)', 'Text', 'Duration', 'StickerID', 'Mess...', 'System', 'Message ID', and 'Message server ID'. A blue callout box with the text '解析データの元ファイル Line.sqlite' points to the 'Line.sqlite' file in the 'Source file' pane on the right. The 'Source file' pane also shows 'Source table' (ZMESSAGE, ZCHAT, ZUSER), 'Direction' (Outgoing), 'party ID', 'party', 'Time stamp (UTC)', 'Message', 'type', 'Message ID', and 'Message server ID'.

LINEの解析についての補足：

バックアップ抽出でのLINEの解析はiOSのみ可能です。

Androidの場合は、「Full file system」メソッドでの抽出や「OxyAgent」メソッドなどを使用する必要があります。

➤ Kakao Talk の解析画面

通話履歴がある場合は、Calls も表示される

解析データの元ファイル Message.sqlite

Oxygen がメッセージを自動的に復号している

Row ID	Remote party	Sent (UTC)	Read (UTC)	Content
457	佐井場攻太	19/08/27 09:42:06 (UTC+0)	19/08/27 09:42:07 (UTC+0)	そうですね。
456	佐井場攻太	19/08/27 09:41:45 (UTC+0)	19/08/27 09:41:45 (UTC+0)	暑さやらいできて、良いんだけど、明日は暑くなってほしいな。
455	佐井場攻太	19/08/27 09:41:08 (UTC+0)	19/08/27 09:41:08 (UTC+0)	だよな。
454	佐井場攻太	19/08/27 09:41:02 (UTC+0)	19/08/27 09:41:03 (UTC+0)	確かに、それほど暑くなくなったもんね。
453	佐井場攻太	19/08/27 09:40:19 (UTC+0)	19/08/27 09:40:19 (UTC+0)	そっか黒さんと電話で話したんだけど、最近暑さがやわらいでいる。
452	黒田三吉	19/08/21 03:32:03 (UTC+0)	19/08/21 03:32:03 (UTC+0)	ハロー
451	佐井場攻太	18/06/25 05:46:27 (UTC+0)	18/06/25 05:46:27 (UTC+0)	ばつり、消毒しましたって言っていました。
450	佐井場攻太	18/06/25 05:46:10 (UTC+0)	18/06/25 05:46:11 (UTC+0)	ありがたいね。
449	佐井場攻太	18/06/25 05:45:50 (UTC+0)	18/06/25 05:45:50 (UTC+0)	消毒しなきゃだから、掃除のおばちゃんにお熱いしました。
448	佐井場攻太	18/06/25 05:45:14 (UTC+0)	18/06/25 05:45:16 (UTC+0)	自分でそうしたの？
447	佐井場攻太	18/06/25 05:44:53 (UTC+0)	18/06/25 05:44:54 (UTC+0)	困りましたね
446	佐井場攻太	18/06/25 05:44:44 (UTC+0)	18/06/25 05:44:44 (UTC+0)	ちょっと焦った:(('...')):
445	佐井場攻太	18/06/25 05:44:32 (UTC+0)	18/06/25 05:44:32 (UTC+0)	コロコロしたのどうも落として、
444	佐井場攻太	18/06/25 05:44:15 (UTC+0)	18/06/25 05:44:15 (UTC+0)	はいw
443	佐井場攻太	18/06/25 05:44:06 (UTC+0)	18/06/25 05:44:06 (UTC+0)	朝掃除してやっつ？
442	佐井場攻太	18/06/25 05:43:54 (UTC+0)	18/06/25 05:43:54 (UTC+0)	うん、今日、俺の机にお土産を落としていました。
441	佐井場攻太	18/06/25 05:43:08 (UTC+0)	18/06/25 05:43:08 (UTC+0)	最近ねずみがやっつるよ、よね
440	佐井場攻太	18/06/25 05:42:28 (UTC+0)	18/06/25 05:42:28 (UTC+0)	はい
439	佐井場攻太	18/06/25 05:42:17 (UTC+0)	18/06/25 05:42:17 (UTC+0)	情報さん

📌 Kakao Talk の解析についての補足 :

Message.sqlite データベースの「Message」テーブルの「message」カラムは暗号化されていますが、Oxygen 側で復号しています。

改訂履歴

版数	発行日	改訂履歴
Ver. 1.0	2023年3月3日	初版発行