Oxygen データ抽出・解析ガイド

Ver. 7.0

目次

※データ抽出・解析の前に

本ガイド内のスクリーンショットは英語表記ですが、言語設定を日本語にしている方は一部()内の日本語に読み替えてご使用ください。

1　イントロダクション

本ガイドは、Oxygen Forensic® Detective v14 から採用されたインターフェイスを使用したデータの抽出と解析方法を記載しております。

1.1　解析対象デバイスの前提条件

データの抽出と解析を実行する前に、下記の前提条件を御確認下さい。これらの前提条件を満たしていない場合、Oxygen Forensic® Detective はデータの抽出及び解析をすることが出来ません。

デバイス種別	前提条件
Android デバイス	• USB デバッグモードが有効な状態、もしくは有効にできる。 ➢ 詳細は"2.1 USB デバッグモードの設定"を参照してください。
iOS デバイス	• パスコード等の認証機能が無効な状態、もしくは機能を解除できる。

1.2　フライトモード（機内モード）の設定

通信によるデータの上書きや削除、リモートワイプ等を防ぐために、解析対象デバイスの操作が可能な場合は、フライトモードに設定して通信を遮断します。フライトモード設定ができない場合は、他に通信を遮断する措置をおすすめします。

1.3　接続用ケーブルと解析対象デバイス用ドライバの準備

解析対象デバイスからデータを取得する際は、USB ケーブルを使用します。

Oxygen はデバイスからのデータ取得に際し、各デバイスのデバイスドライバのインストールが必要となります。

※ 解析対象デバイスの種類によってはドライバなしに接続できる場合があります。

デバイスドライバは、各製品ベンダーのサイトや、解析対象デバイス付属のメディア等から入手することが可能です。また、Oxygen Forensics 社から各種デバイスのデバイスドライバをまとめたドライバパックを提供しています。

※ 別紙「インストールガイド」を参照してください。

2　Android スマートフォンのデータ抽出

2.1　USB デバッグモードの設定

Oxygen で解析する Android スマートフォンデバイスは、USB 接続する際には ADB（Android Debug Bridge）を経由するため、「USB デバッグモード」になっている必要があります。

- **USB デバッグモードの設定方法**

  USB デバッグモード設定には解析対象デバイスを操作し、「設定」⇒「開発者向けオプション」⇒「USB デバッグ」にチェックを入れます。

  なお、この操作は、パスワードや暗証番号等による認証機能が無効なデバイスか、認証を解除したデバイスでないと設定できません。

  - データ取得前に使用者などから PIN コード又はパターン等を入手して下さい。
  - Android4.2 以降のデバイスはデフォルトで「開発者向けオプション」が表示されていません。

- **開発者オプションの表示方法**

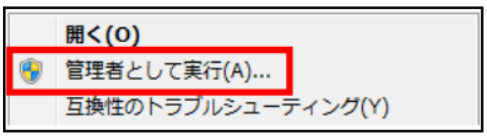
  「開発者向けオプション」が表示されていない場合、解析対象デバイスを操作し、「設定」⇒「デバイス情報」又は「タブレット情報」⇒「ビルド番号」の画面で、「ビルド番号」を 7 回以上タップします。

2.2　データ抽出

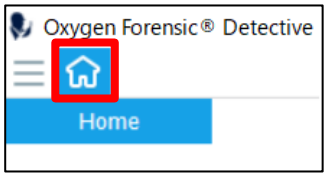
- **データ抽出の手順**

  - 解析対象デバイスの認証機能は、無効化もしくは解除しておいて下さい。

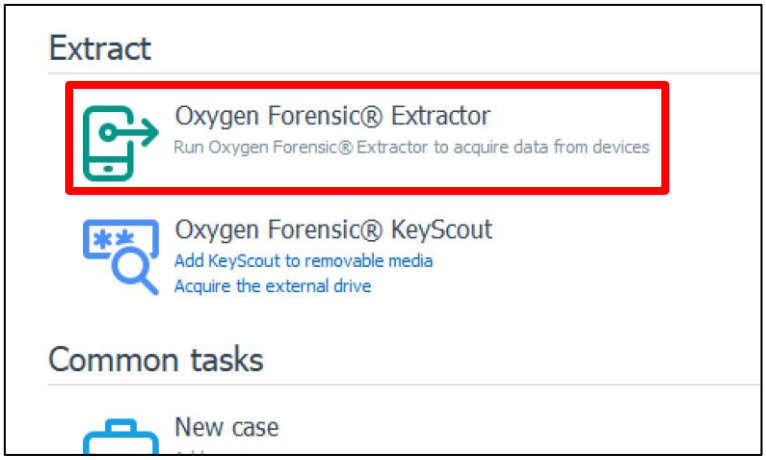
① Oxygen Forensic® Detective のデスクトップアイコンを右クリックし、「管理者として実行」を選択します。



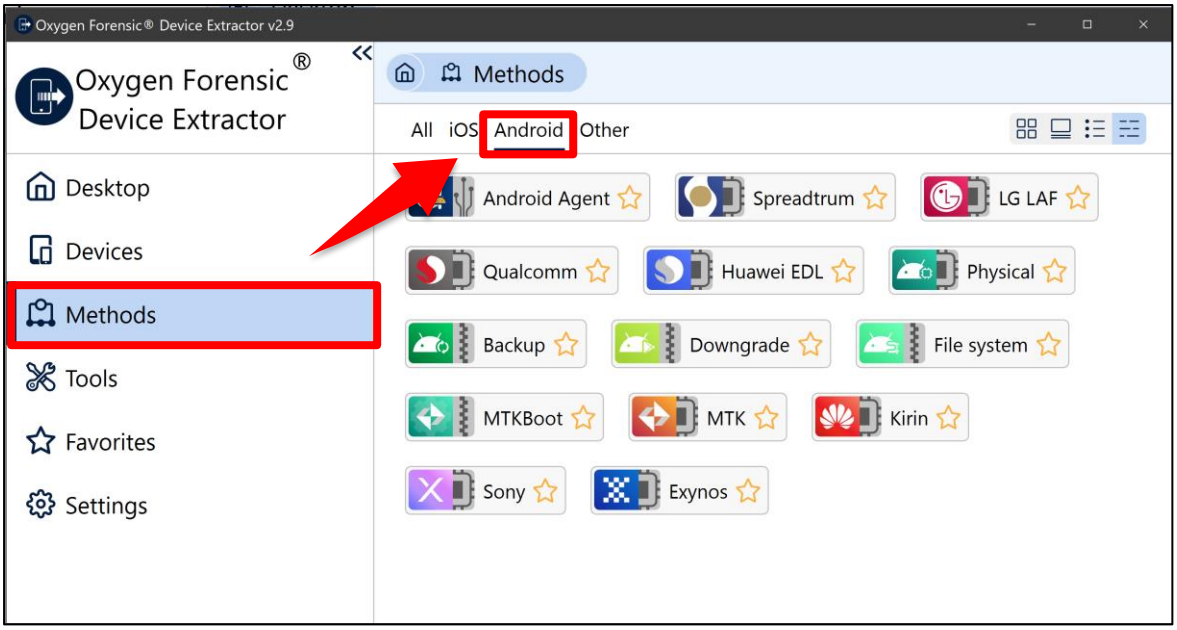
② 起動した Oxygen Forensic® Detective のホームタブをクリックします。



③ 表示されたメニューの中から「Oxygen Forensic® Extractor」をクリックします。



④ Oxygen Forensic® Extractor が起動します。「Methods」をクリックし、「Android」タブをクリックして Android デバイスの抽出方法一覧を表示します。調査対象端末に合わせて抽出方法を選んでください。



☞ Android の抽出は、以下の方法が用意されています。

- Android physical (via ADB): Android の物理抽出（ADB 経由）。
- Android backup (via ADB): Android のバックアップ（ADB 経由）。
- Android OxyAgent extraction: OxyAgent をデバイスにインストールして抽出。
- Android manual OxyAgent extraction: OxyAgent を SD カードに保存して抽出。
- Android OxyAgent over WiFi extraction: OxyAgent をデバイスにインストールして WiFi 経由で抽出。
- Android file system: Android OS の脆弱性を利用し root 化を試みる論理抽出。
- MTK Android: Media Tek 社製のチップセットを搭載した Android OS デバイスからの物理抽出。
- LG Android: LG 社製の Android デバイスからの物理抽出。
- Spreadtrum Android: Spreadtrum Communications 社製のチップセットを搭載した Android デバイスからの物理抽出。

  この方法はリスクがあります。それを踏まえた上で使用するかどうか検討してください。抽出中にパーティションテーブルを上書きします。また、デバイス内に非公式の ROM がある場合、ロードが中断する場合があります。ユーザデータが失われるため設定のリセットを行わないでください。

- Samsung Android: Samsung 社製の Android デバイスからの物理抽出。

  この方法はリスクがあります。それを踏まえた上で使用するかどうか検討してください。独自のリカバリイメージで上書きします。この時、以前のイメージは失われます。システムとユーザデータは影響を受けない様ですが、他にも KNOX カウンターへの影響や Samsung の公式サポート外になります。

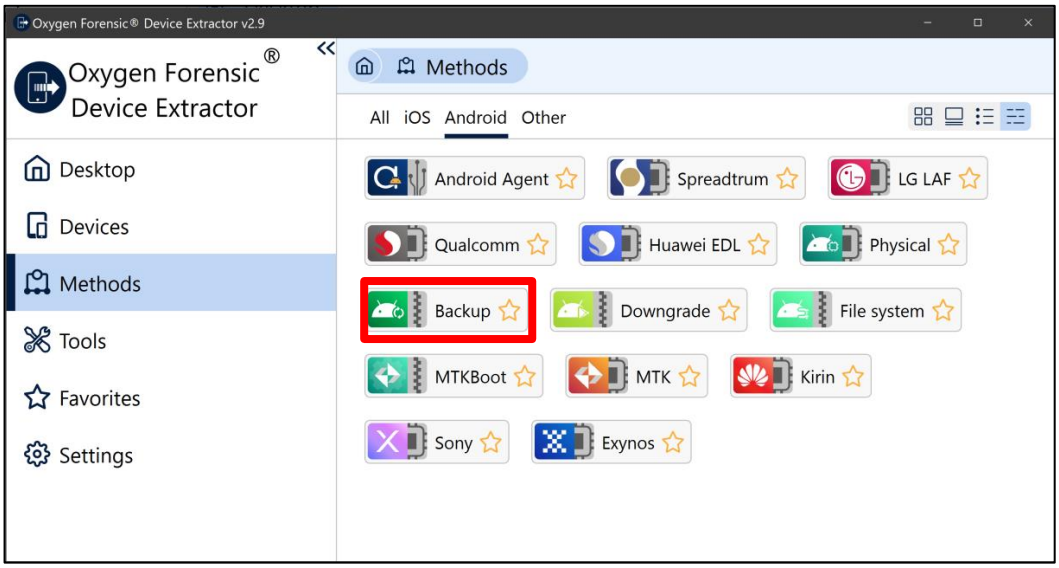
- Samsung Exynos: Samsung 社製の Exynos チップセット搭載 Android デバイスからの物理抽出。
- Motorola Android: Motorola Mobility LCC 製の Android からの物理抽出。
- Qualcomm EDL: Qualcomm 社製のチップセットからの物理抽出。
- Huawei Kirin: Samsung 社製の Kirin チップセット搭載 Android デバイスからの物理抽出。
- Sony MTK: Sony 社製の Mediatek チップセット搭載 Android デバイスからの物理抽出。
- Huawei Qualcomm: Huawei 社製の Qualcomm チップセット搭載 Android デバイスからの物理抽出。
- APK Downgrade: デバイス内のアプリケーションを一時的にダウングレードさせてから、ADB backup を試みる。
- LG Qualcomm: LG 社製の Qualcomm チップセット搭載 Android デバイスからの物理抽出。

  この方法はリスクがあります。それを踏まえた上で使用するかどうか検討してください。データの抽出

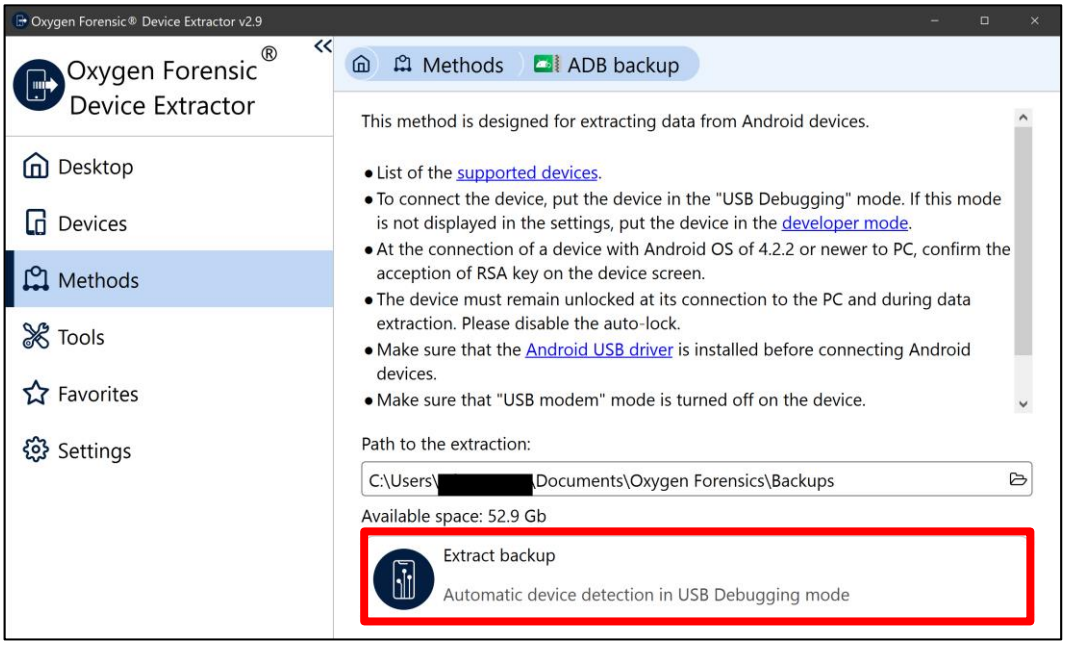
後にデバイスが通常モードで起動しない場合は、デバイスのパーティションをリストアします。

⑤ 今回は例として、ADB バックアップを使用したデータ抽出方法を選択します。

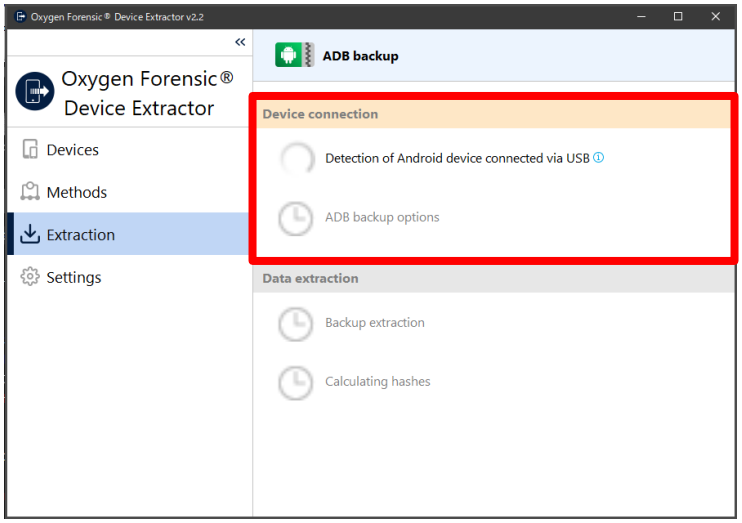
「Backup」（旧名：Android backup via ADB）をクリックします。



① Oxygen Forensic Device Extractor が起動します。ADB backup のメソッドが選択された状態の画面が展開されますので、そのまま「Extract backup」をクリックします。



⑥ 解析対象デバイスを USB ケーブルで PC と接続してください。「Device connection」セクションでは、Oxygen が解析対象デバイスとの接続を確認します。



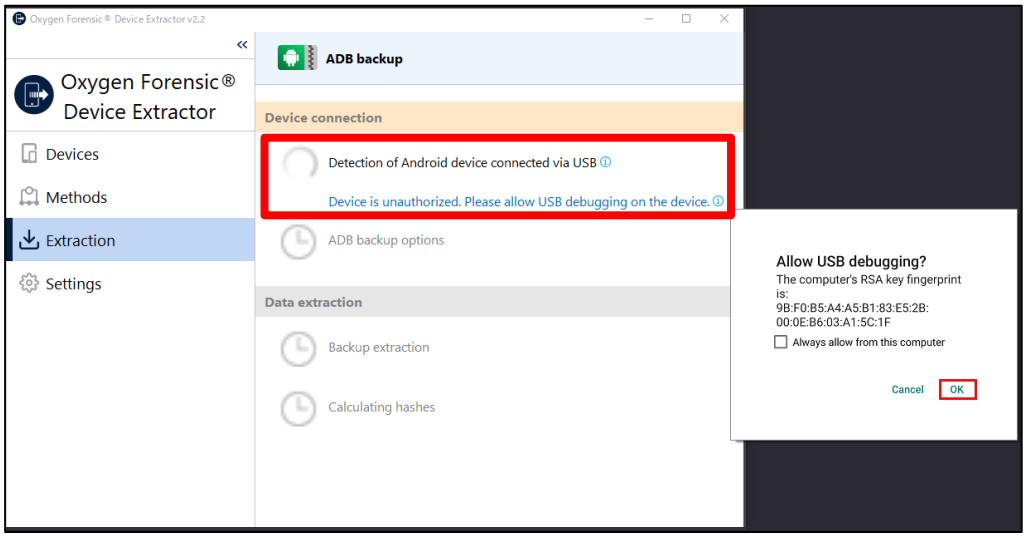
- 接続確認中はケーブルを抜かないでください。
- 接続に失敗した際は、次の条件を確認してください。

☞ 解析対象デバイスが「USB デバッグモード」になっていること。

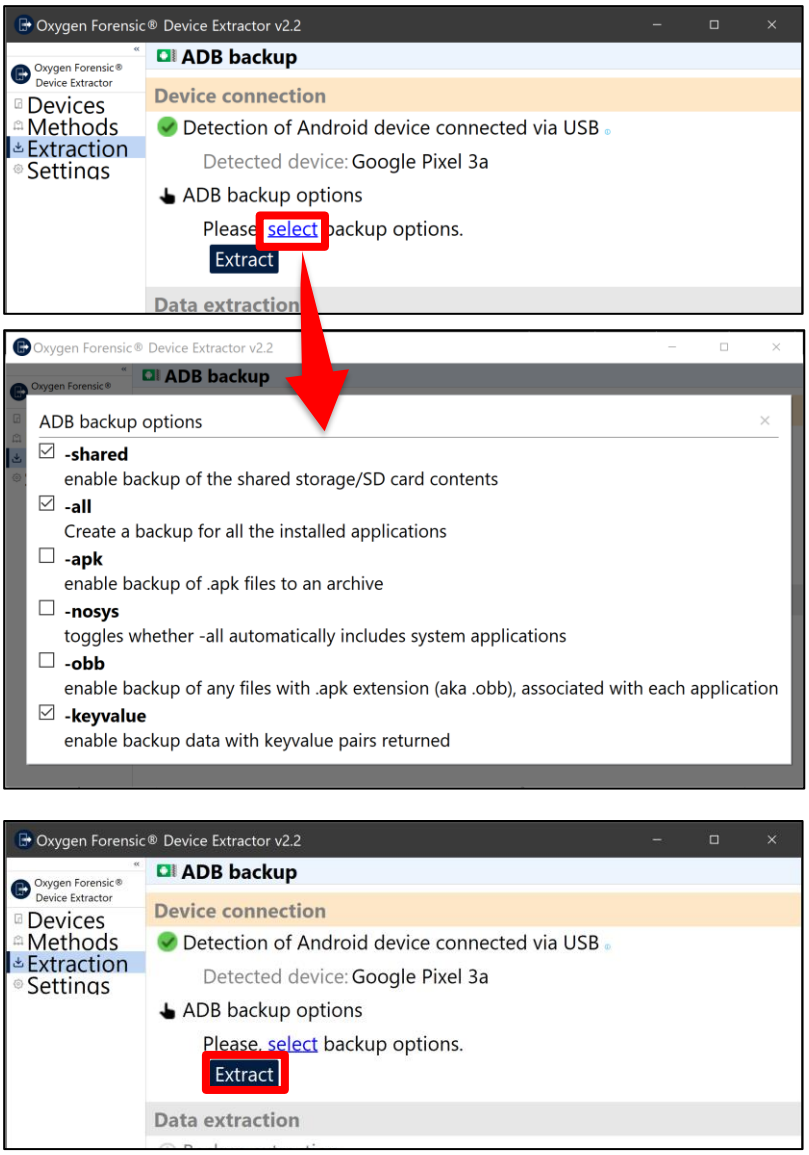
☞ 解析対象デバイスのデバイスドライバが、PC にインストールされていること。

☞ ケーブルが正しく接続されていること。

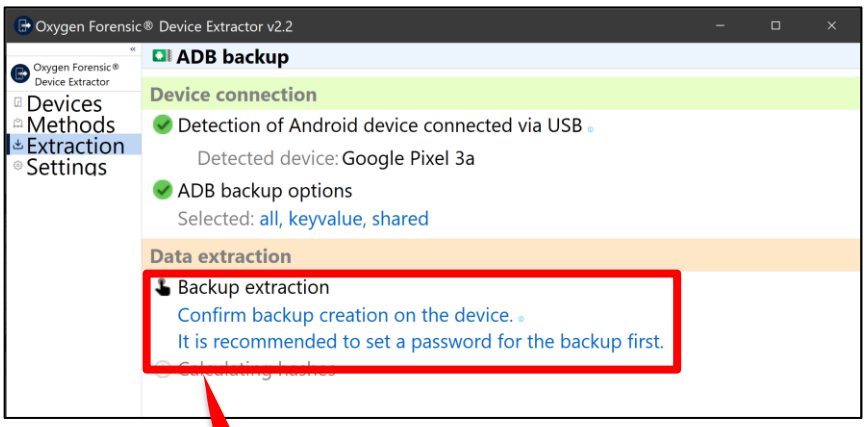
⑦ 「Device is unauthorized. Please allow USB debugging on the device.」と表示されたら、解析対象のデバイス画面で「OK」をタップしてください。



⑧ 接続に成功し、デバイス情報が確認できたら、「select」をクリックして抽出時のオプションを確認します。「ADB backup options」のポップアップを閉じて、「Extract」ボタンをクリックします。

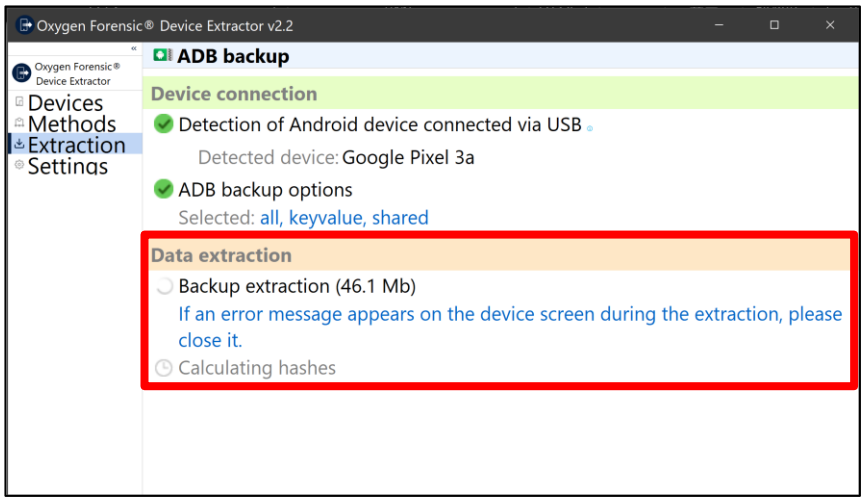


⑨ 「Data extraction」セクションに解析対象デバイスでの操作指示が表示されます。解析対象デバイスを操作して、「Back up my data(データをバックアップ)」をタップして下さい。

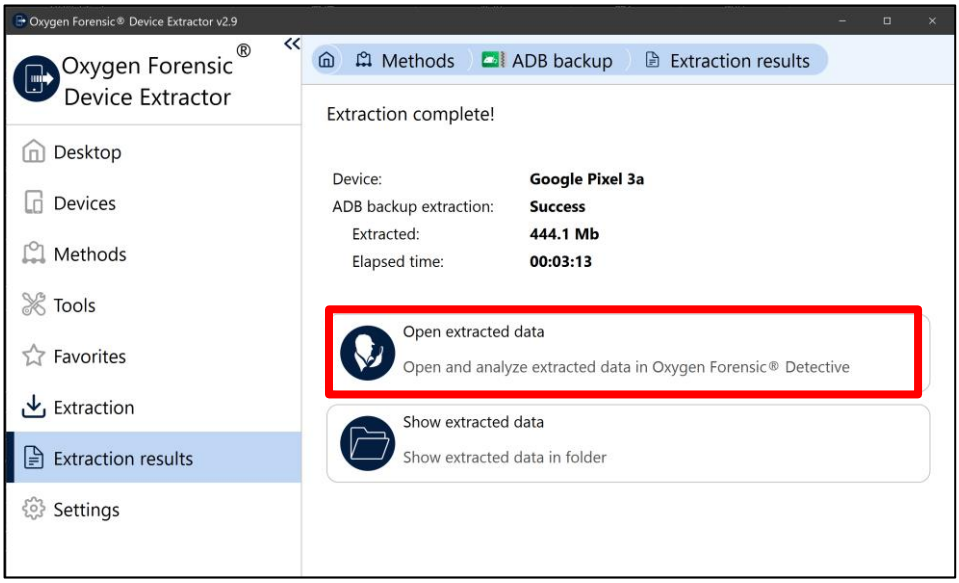


解析対象デバイスの画面

⑩　データ抽出の進捗が表示されるので、このまま抽出完了まで待ちます。



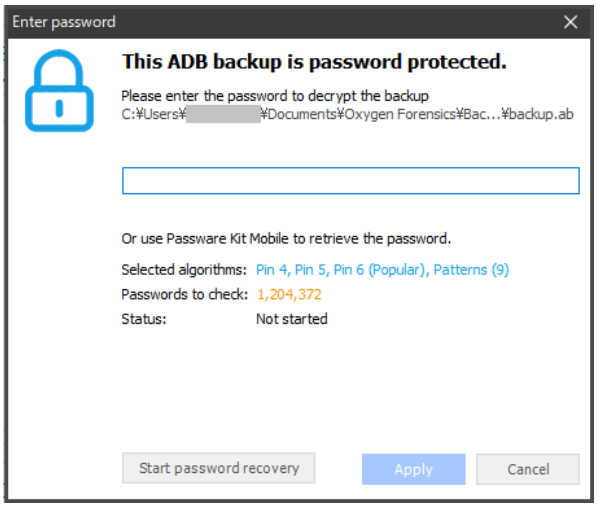
⑪ 抽出が完了すると、画面が切り替わり、抽出結果が表示されます。問題なければ「Open extracted data」をクリックします。



☞ 結果に「Success」と表示された場合、データの抽出に成功しています。

☞ 明らかにデータ数が少ない場合は抽出に失敗している可能性があります。これは再抽出することで改善される可能性があります。

⑫ 手順⑨でデータをバックアップする際に任意のパスワードを設定した場合、以下の画面が表示されます。この画面が表示された場合は、バックアップパスワードを入力してください。



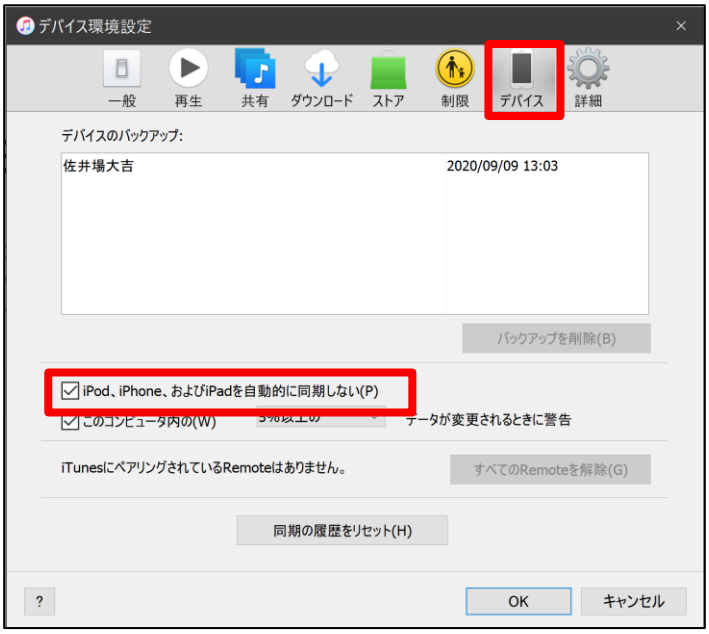
☞ Start password recovery を試す事で、パスワードを自動解析できる場合があります。

3　iPhone のデータ抽出

3.1　iTunes のインストール

Oxygen が iOS デバイスのデータへアクセスするためには、iTunes のバックアップ機能等で使用される AFC(Apple File Connection)サービスを使用するため、Oxygen を実行する PC に iTunes をインストールする必要があります。

- iOS デバイスのバージョンアップによって、iTunes についてもバージョンアップが必要となる場合があります。
- Oxygen を起動する前に必ず一度は iTunes を起動し、「編集」⇒「環境設定」より iTunes の自動同期設定を無効化してください。



3.2　iPhone の接続と「信頼」

iOS7.x 以降を搭載した iOS デバイスは、今まで接続したことがない PC またはデバイスに接続すると、接続されたデバイスを信頼するかどうかを確認するよう求められます。

- **「信頼」する方法**

  iOS7.x 以降を搭載したデバイスの画面に「信頼」に関するメッセージが表示されます。
  「信頼」をタップすると、PC または別のデバイスから iOS デバイスに保存されているファイルにアクセスすることが出来るようになります。

（Apple 社サポートページ：https://support.apple.com/ja-jp/HT202778）

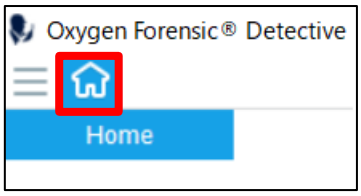
- 「このコンピュータを信頼しますか？」は、デバイスのスクリーンロックが解除されている状態でのみ表示されます。
- 解析をするには、「信頼」を選択し、PC からデバイスへの接続を許可する必要があります。
- iOS11.4.1 以降では、「USB アクセサリ」機能が追加されています。デバイスのロックを解除しても USB アクセサリが認識されない場合は、デバイスを再接続してください。

3.3 データ抽出

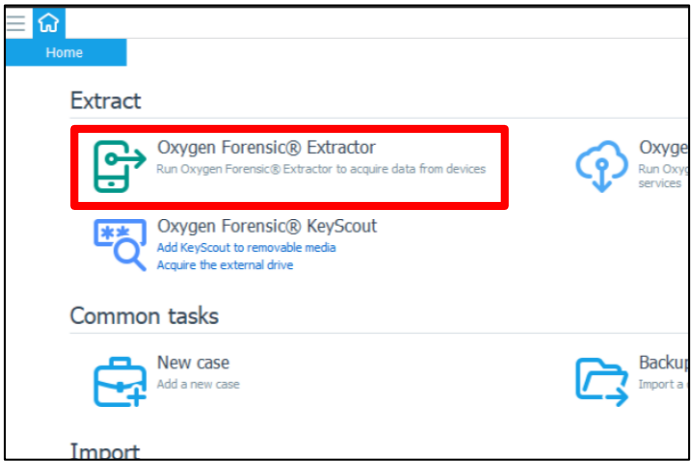
- **データ抽出の手順**

- 「このコンピュータを信頼しますか？」は、デバイスのスクリーンロックが解除されている状態でのみ表示されます。
- 解析をするには、「信頼」を選択し、PC からデバイスへの接続を許可する必要があります。

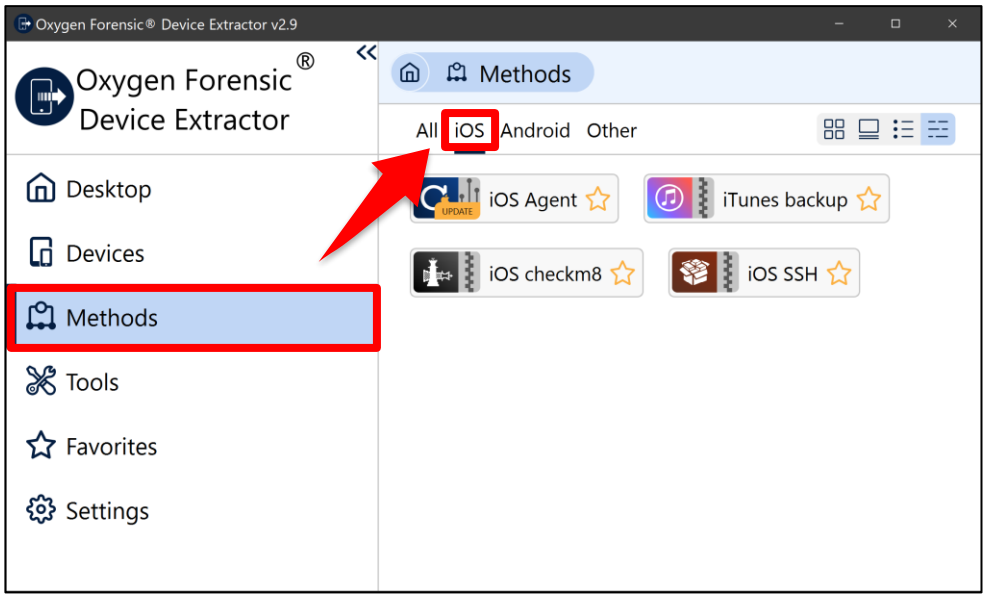
① Oxygen Forensic® Detective を管理者権限で起動し、ホームタブをクリックします。



② 表示されたメニューの中から「Oxygen Forensic® Extractor」をクリックします。

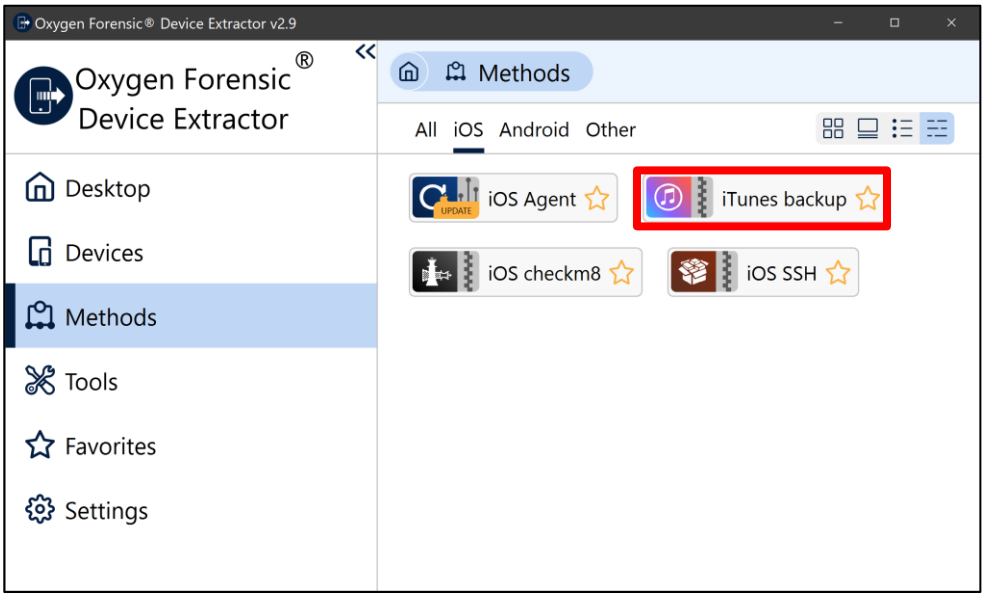


③ データ抽出を行う Oxygen Forensic® Extractor が起動します。Oxygen Forensic® Extractor の操作画面の「Methods」をクリックし、「iOS」タブをクリックで展開して抽出方法を選んでください。



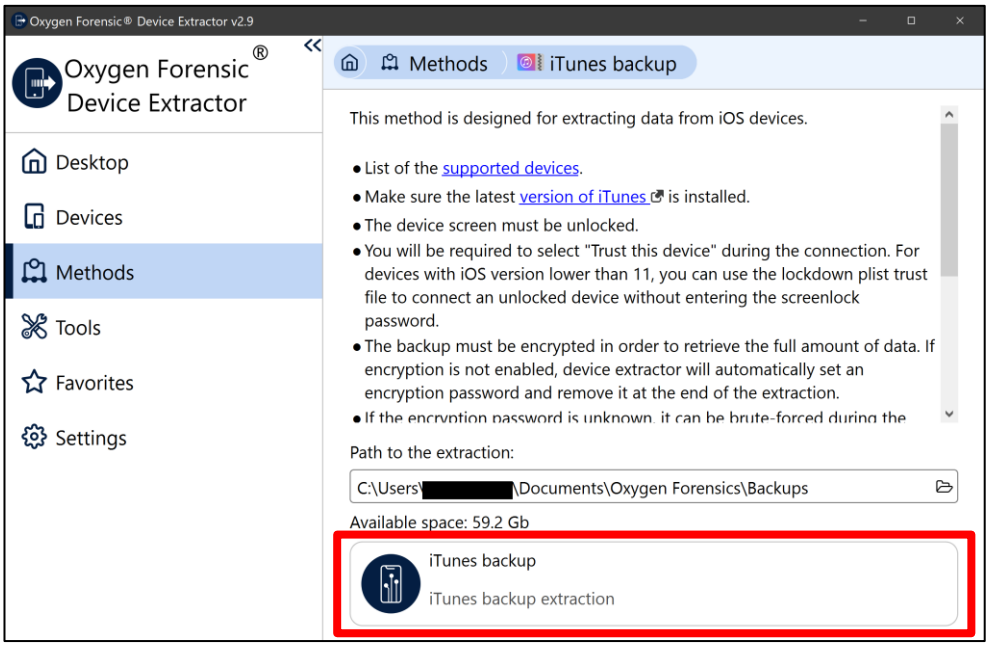
- ☞ iTunes backup: iTunes バックアップの仕組みを使用してデータを抽出します。
- ☞ iOS Advanced extraction: checkm8 や SSH を介した論理抽出を行います。
  - Oxygen で実行する checkm8 では Jail Break(JB)を行いません。
- ☞ Logical file structure：ファイルの構造を取得します。

④ 今回は例として、iTunes バックアップを使用したデータ抽出方法を選択します。
「iTunes backup」をクリックします。

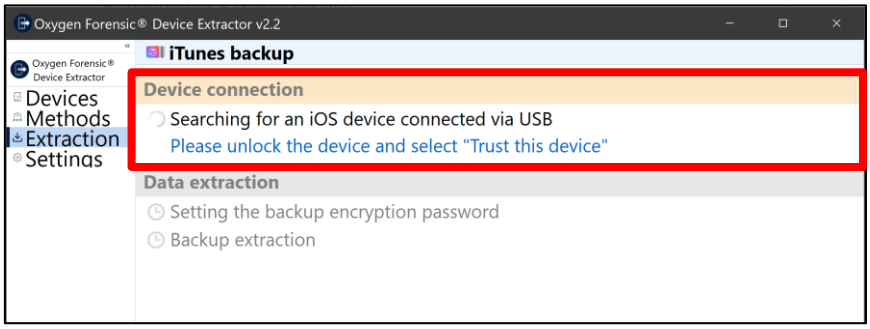


⑤ iTunes backup のメソッドが選択された状態の画面に遷移されるので、そのまま「iTunes backup」をクリックします。

この抽出方法では、より多くの領域をバックアップに含めるため、バックアップパスワードを設定する必要があります。事前に設定していない場合は、Oxygen が自動で設定し、抽出完了時にデバイスから削除します。



⑥ 解析対象デバイスを USB ケーブルで PC と接続してください。「Device connection」セクションでは、Oxygen が解析対象デバイスとの接続を確認します。デバイスのスクリーンロックを解除し、デバイスの画面に「このコンピュータを信頼しますか？」と表示されるので、「信頼」をタップします。



接続に失敗した際は、次の条件を確認してください。

- 解析対象デバイスに対応した iTunes がインストールされていること。
- Oxygen がサポートしているバージョンの iTunes であること(サポート対象外のバージョンがリリースされた場合は、弊社サポートページにてご案内致します)。

☞ iTunes がインストールされ、一回でも起動していること。

☞ ケーブルが正しく接続されていること。

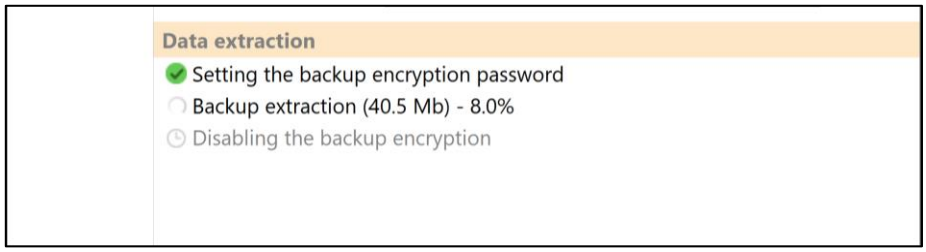
⑦ デバイスの接続に成功すると、デバイス情報が表示されます。また、デバイス側で再度パスコード入力が求められるので入力します。

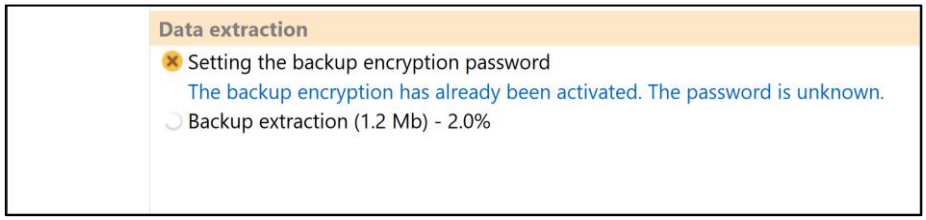
⑧ 抽出の準備が完了すると、「Start with encryption」ボタンと「Start without encryption」が表示されます。「Start with encryption」はより多くのデータが抽出出来る代わりに、バックアップファイルのパスワードがデバイスに保存されます。問題がなければ、「Start with encryption」ボタンをクリックで抽出を開始します。

- あらかじめバックアップパスワードが設定されていない場合のみ上記の画面が表示され、Oxygen が「123456」をバックアップパスワードとしてデバイスに自動設定します。
- 抽出が完了すると、Oxygen が自動設定したバックアップパスワードはデバイスから削除されます。
- 抽出途中で処理が中断した場合、Oxygen が自動設定したバックアップパスワードがデバイスに残る場合があります。

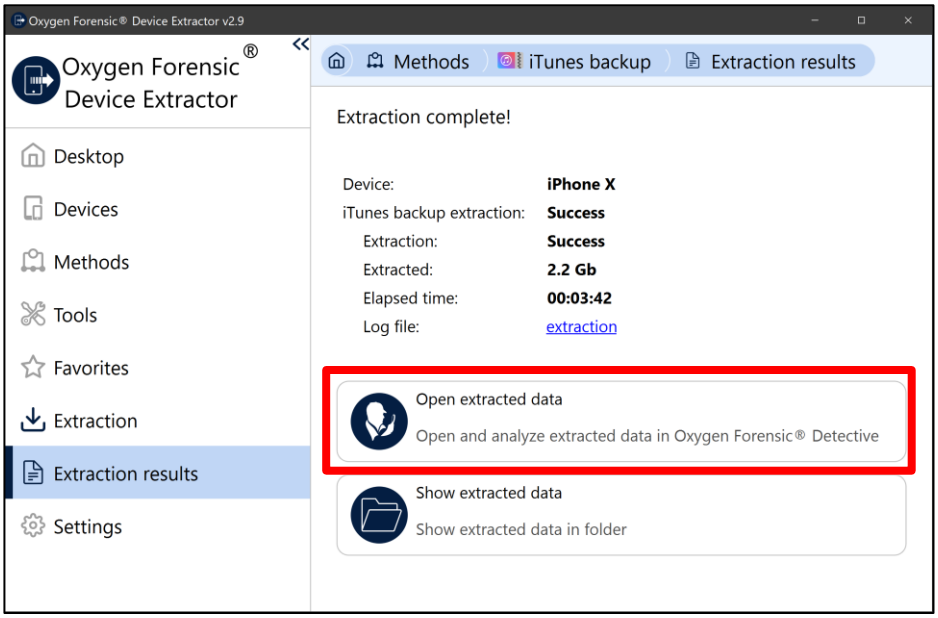
⑨ 抽出が始まります。あらかじめバックアップパスワードを設定している場合は、「Setting

the backup encryption password」に失敗しますが、抽出には影響ありません。

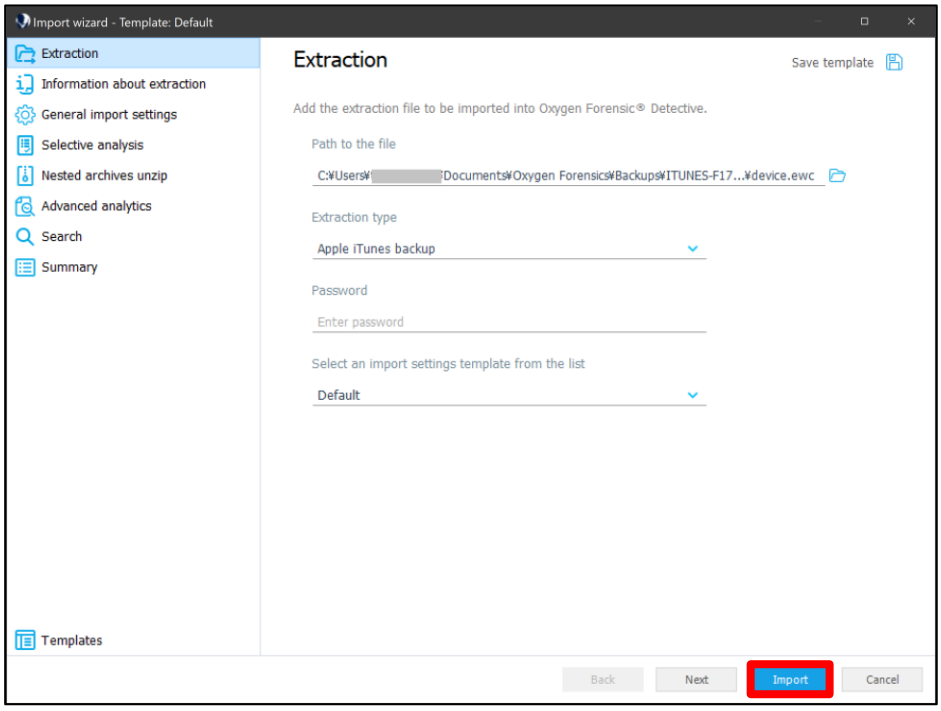




⑩ 抽出が完了すると、「Open extracted data」ボタンと「Show extracted data」ボタンが表示されます。抽出したデータを Oxygen Forensic® Detective で解析する場合は、「Open extracted data」をクリックします。



⑪ 抽出データを Oxygen Forensic® Detective に Import する際に Import wizard が表示されます。Import wizard では、抽出データに対するオプションを変更出来ます。特に変更がない場合は、このまま「Import」ボタンをクリックします。



- 解析対象デバイスが、過去に iTunes でバックアップの暗号化を設定していた場合、"パスワード"の入力を求められます。
- "パスワード"は、バックアップの暗号化を設定するときにユーザが任意に決定するものであり、iOS デバイスの認証用の"パスコード"ではありません。パスワードがかかっていた場合下記の様な画面が表示されますので、パスワードを入力してください。

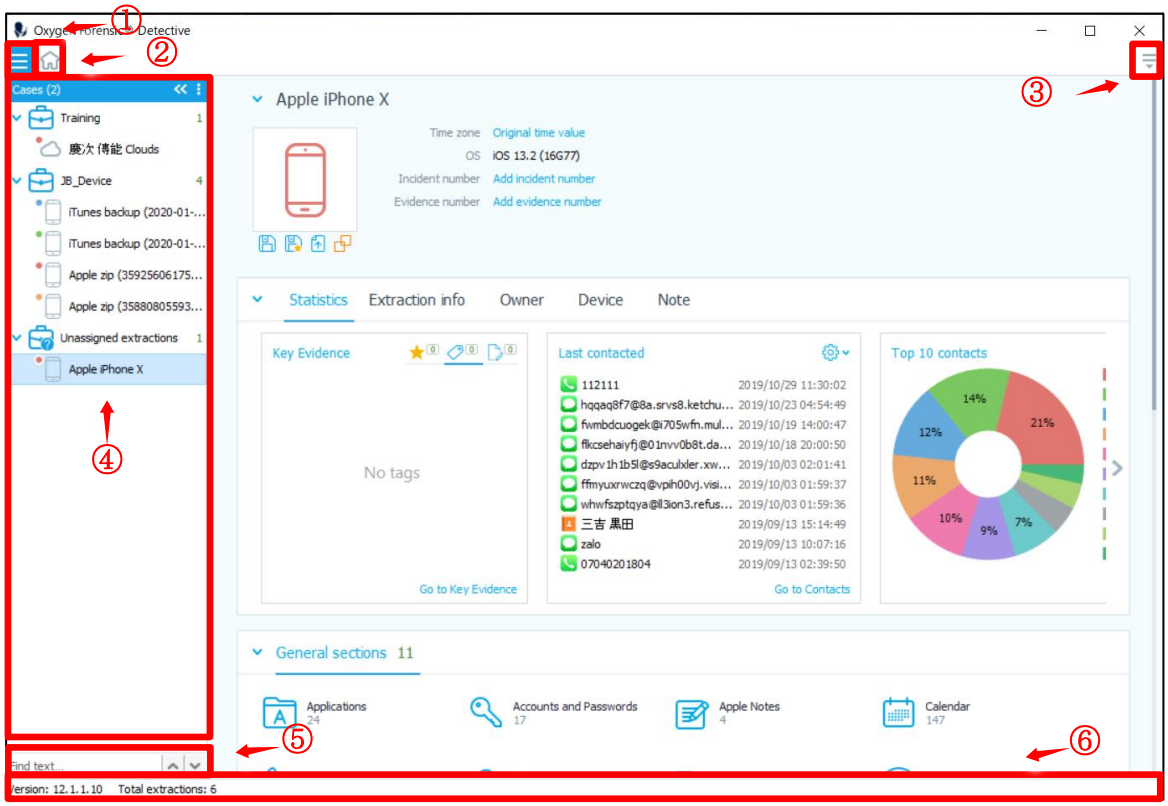
4　データ解析

本章では iOS を対象にした解析画面のスクリーンショットを用いて解説しています。Android の場合は本章の UI と異なる場合がございます。

4.1　インターフェイスについて

- **ケースタブの機能一覧**

Oxygen を起動すると以下の様な画面が開きます。



① ケースタブ： ケースパネルを表示します。

② ホームタブ： Export、Import、Tools などの各種ウィザードの起動が行えます。

③ メニュー：各種ウィザードの起動、言語の切替え、アップデートの確認などが行えます。

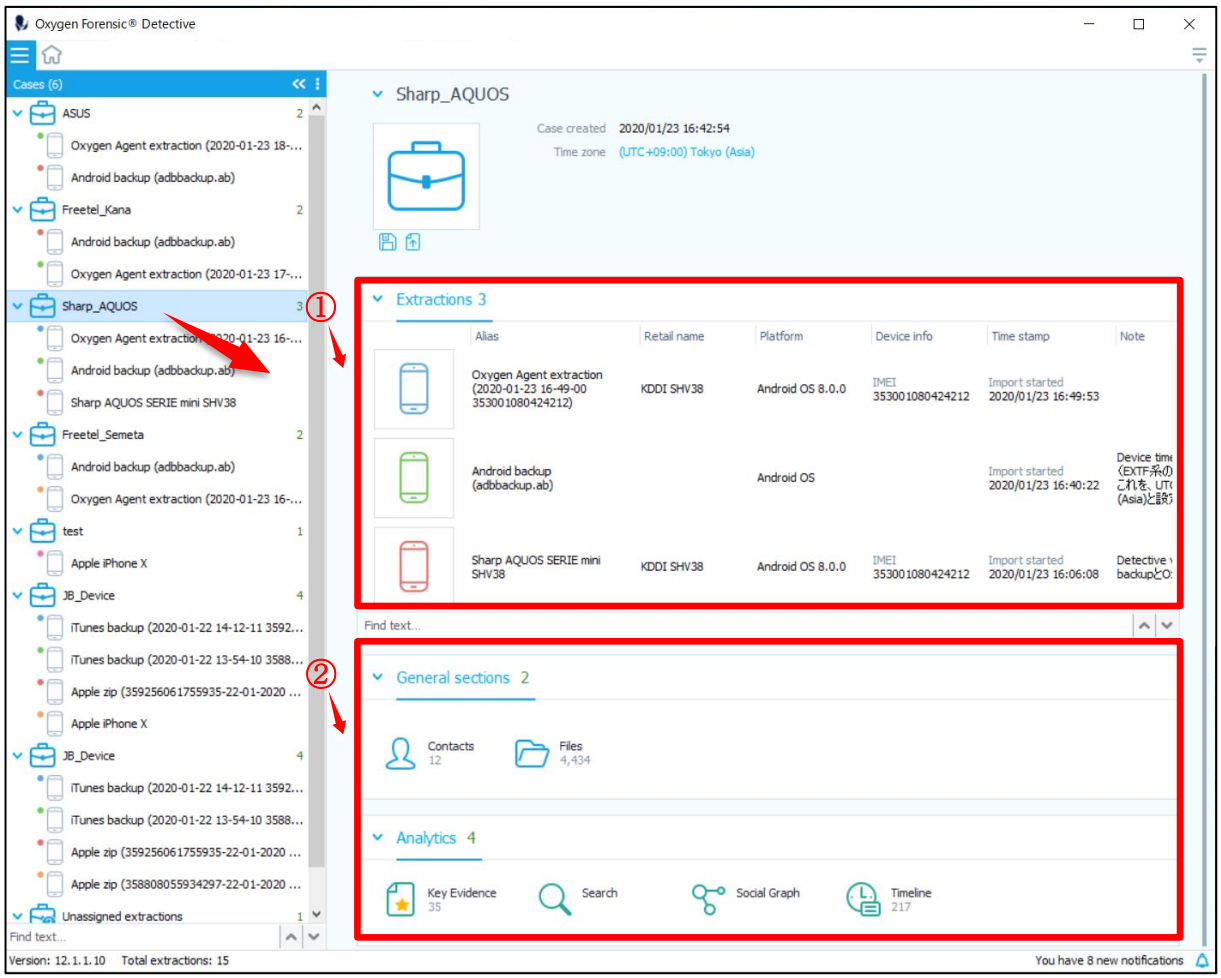
④ ケースパネル：ケース毎に抽出したデバイスの一覧を表示します。

⑤ 検索ボックス:ケースパネル内のデバイス名または Case 名を検索し、該当の文字列をハイライトします。

⑥ インフォメーションバー：Oxygen Forensic® Detective のバージョンや、取り込んでいるデバイス数が表示されます。

- **ケース毎の解析画面**

解析したいケースを選択すると画面が切り替わり、ケースに格納されているデバイスの情報と、解析のメニューが表示されます。

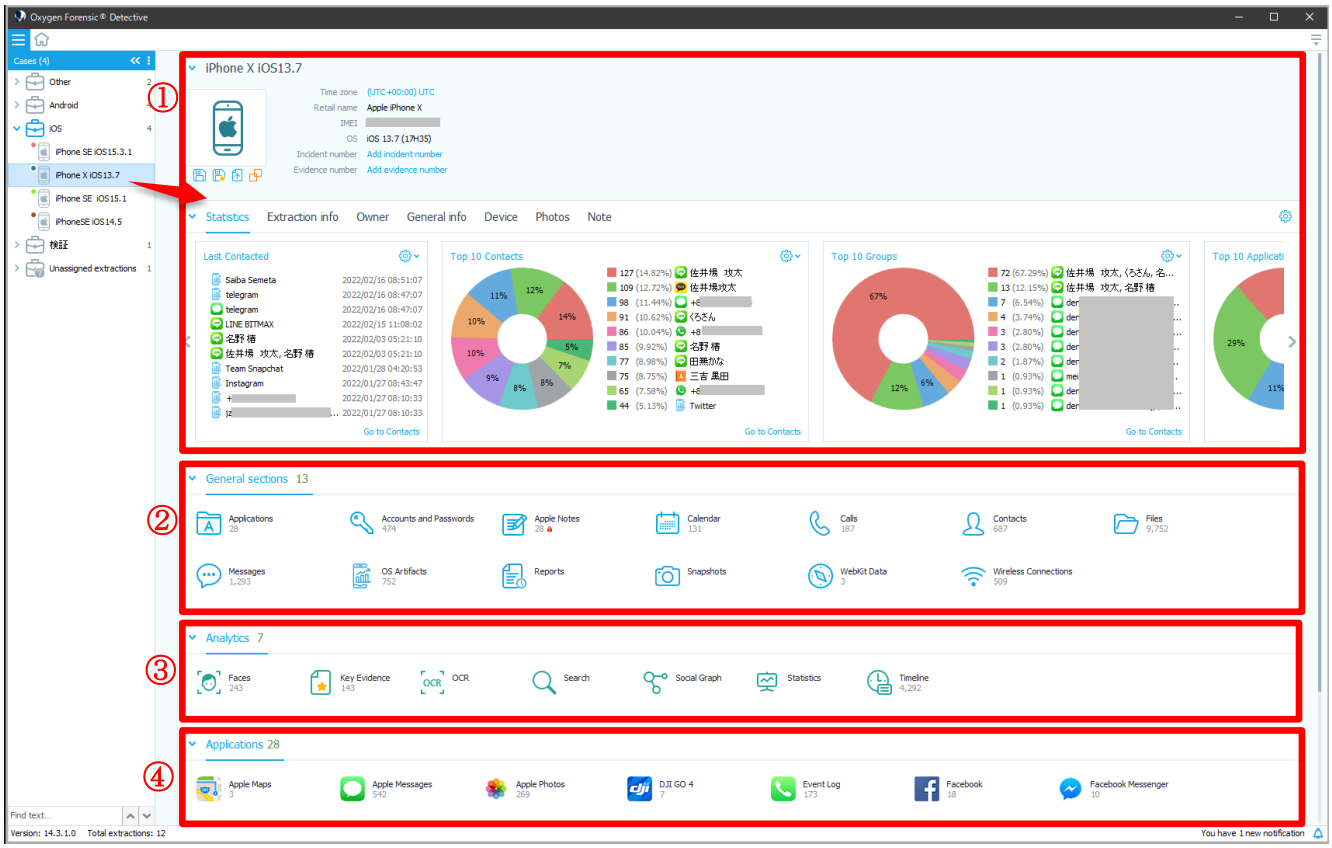


① デバイス情報：ケースに格納されているデバイスの情報が一覧で表示されます。

② 解析メニュー一覧：ケース単位で利用可能な解析メニューが表示されます。

- **デバイス毎の解析画面**

解析したいデバイスを選択すると画面が切り替わり、デバイスとシステムに関する詳細な情報と、解析のメニューが表示されます。



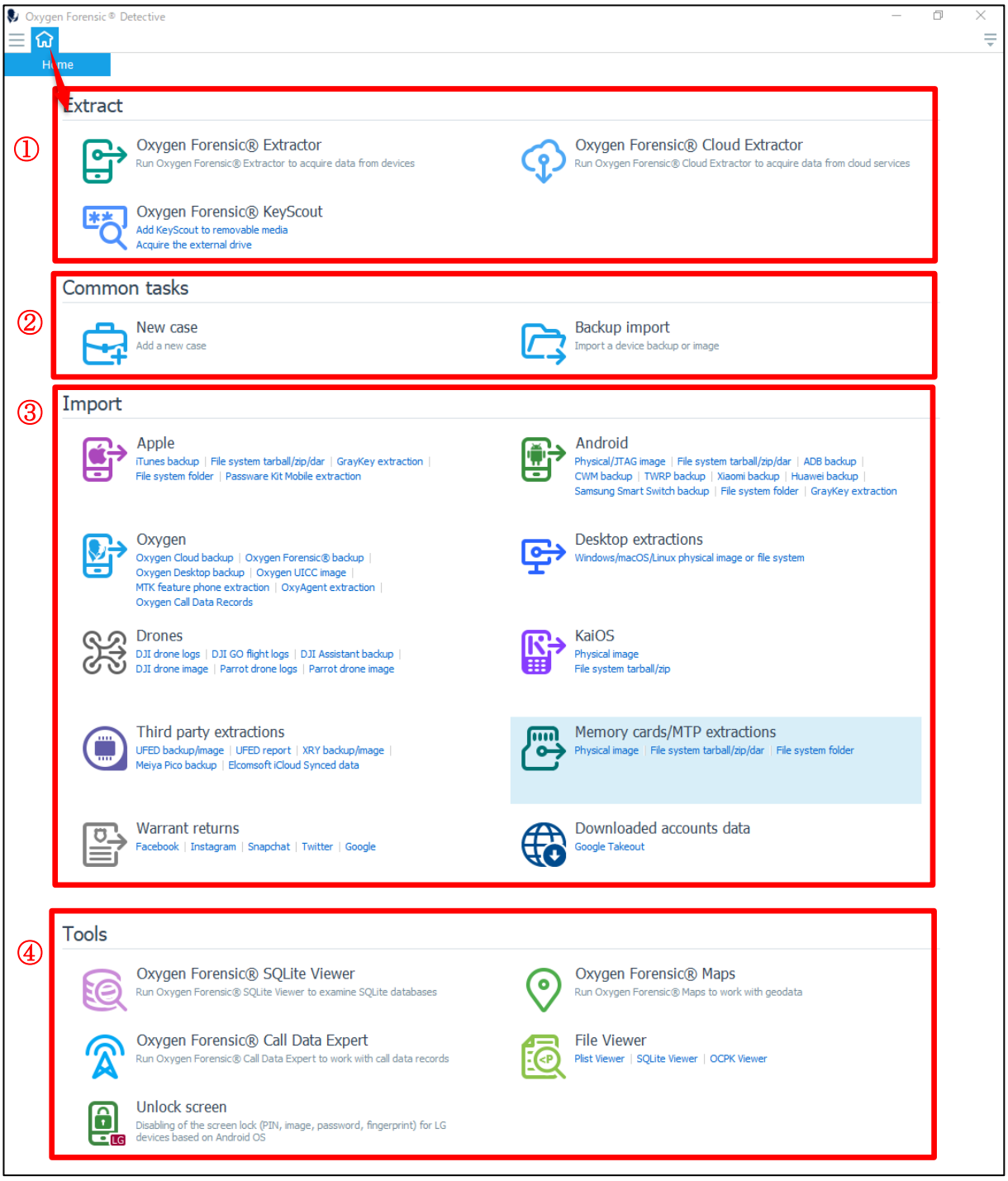
① デバイス情報：デバイス所有者やアカウントに関する情報、統計情報等が表示されます。

② General セクション：個別のアプリケーションに関係なく、すべての連絡先や発着信履歴等がまとめて表示されます。

③ 解析セクション：Faces(顔認識)、Key Evidence(ブックマーク)、OCR(光学文字認識)、Search、Social Graph、Statistics（統計情報）、Timeline の解析メニューが表示されます。

④ アプリケーションセクション：個別のアプリケーションの解析メニューが表示されます。

- **ホームタブの機能一覧**



① Extract：Extractor、Cloud Extractor、KeyScout の起動

	Oxygen Forensic® Extractor	データ抽出をするために Oxygen Forensic® Extractor を起動します。

	Oxygen Forensic® Cloud Extractor	クラウドサービスからデータを抽出するために Oxygen Forensic® Cloud Extractor を起動します。
	Oxygen Forensic® KeyScout	KeyScout を起動します。
		KeyScout をリムーバルメディアに保存します。

② Common tasks：ケースの作成やデバイスバックアップをインポートする機能

	ケースの作成 (New Case)	ケースを新規作成します。
	バックアップのインポート (Import backup file)	デバイスのバックアップやイメージをインポートします。

③ Import：Apple や Android、Oxygen などの各種バックアップファイルをインポート

Apple

	iTunes backup	iTunes backup ファイルをインポートします。
	File system tarball/zip	Apple の File system tarball/zip をインポートします。
	Graykey extraction	GrayKey で抽出した Apple デバイスのデータをインポートします。
	File system folder	Apple の File system folder をインポートします。
	Passware Kit Mobile extraction	Passware Kit Mobile で抽出した Apple デバイスのデータをインポートします。

Android

	Physical/JTAG image	Physical/JTAG image をインポートします。
	File system tarball/zip/dar	Android の File system tarball/zip/dar をインポートします。
	ADB backup	ADB backup ファイルをインポートします。
	CWM backup	CWM Nandroid backup をインポートします。
	TWRP backup	TWRP Nandroid backup をインポートします。
	Xiaomi backup	Xiaomi Android backup をインポートします。
	Huawei backup	Huawei Android backup をインポートします。
	Samsung Smart Switch	Samsung Smart Switch backup をインポートします。

	backup	
	File system folder	Android の File system folder をインポートします。
	GrayKey extraction	GrayKey で抽出したファイルをインポートします。

Oxygen

	Oxygen Cloud backup	Oxygen Forensic® Cloud Extractor backup ファイルをインポートします。
	Oxygen Forensic® backup	Oxygen Forensic® backup ファイルをインポートします。
	Oxygen Desktop backup	Oxygen Desktop backup ファイルをインポートします。
	Oxygen UICC image	Oxygen Forensic® UICC image ファイルをインポートします。
	MTK feature phone extraction	MTK feature phone ファイルをインポートします。
	Oxygen Agent extraction	OxyAgent で抽出したファイルをインポートします。
	Oxygen Call Data Records	Oxygen Call Data Records ファイルをインポートします。

Desktop extractions

	Windows/macOS/Linux physical image or file system	Windows/macOS/Linux の physical image もしくは file system をインポートします。

Drones

	DJI drone logs	DJI drone logs をインポートします。
	DJI GO flight logs	DJI GO の flight logs をインポートします。
	DJI Assistant backup	DJI Assistant backup をインポートします。
	DJI drone image	DJI drone の physical image をインポートします。
	Parrot drone logs	Parrot drone logs をインポートします。
	Parrot drone image	Parrot drone physical image をインポートします。

KaiOS

	Physical image	KaiOS physical image をインポートします。

	File system tarball/zip	KaiOS File system tarball/zip をインポートします。

Third party extractions

	UFED backup/image	UFED backup/image をインポートします。
	UFED report	UFED report をインポートします。
	XRY backup/image	XRY backup/image をインポートします。
	Meiya Pico backup	Meiya Pico backup をインポートします。
	Elcomsoft iCloud Synced data	Elcomsoft iCloud Synced data をインポートします。

Memory cards/MTP extractions

	Physical image	メモリーカードの physical image をインポートします。（FAT、EXT）
	File system tarball/zip/dar	メモリーカード/MTP 抽出の File system tarball/zip/dar をインポートします。
	File system folder	メモリーカード/MTP 抽出の File system folder をインポートします。

Warrant returns

	Facebook	Facebook warrant return archive をインポートします。
	Instagram	Instagram warrant return archive をインポートします。
	Snapchat	Snapchat warrant return archive をインポートします。
	Twitter	Twitter warrant return archive をインポートします。
	Google	Google warrant return archive をインポートします。

Downloaded accounts data

	Google Takeout	Google Takeout data をインポートします。

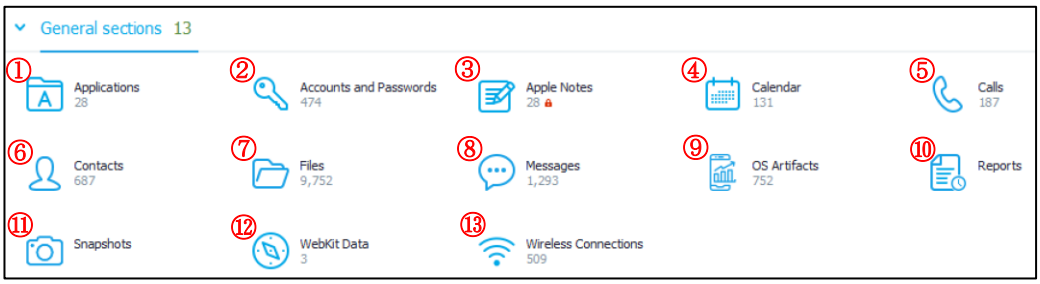
④ Tools： 各種ビューワや Maps、Unlock screen の起動

	Oxygen Forensic® SQLite Viewer	Oxygen Forensic® SQLite Viewer を起動して SQLite データベースを調査します。
	Oxygen Forensic® Maps	Oxygen Forensic® Maps を起動して geo データを調査します。
	Oxygen Forensic® Call Data Expert	Oxygen Forensic® Call Data Expert を起動して、call data records を調査します。※日本では使用不可
	Unlock screen	LG 製 Android デバイスのスクリーンロック(PIN, image, password, fingerprint)の解除ツールを起動します。

File Viewer

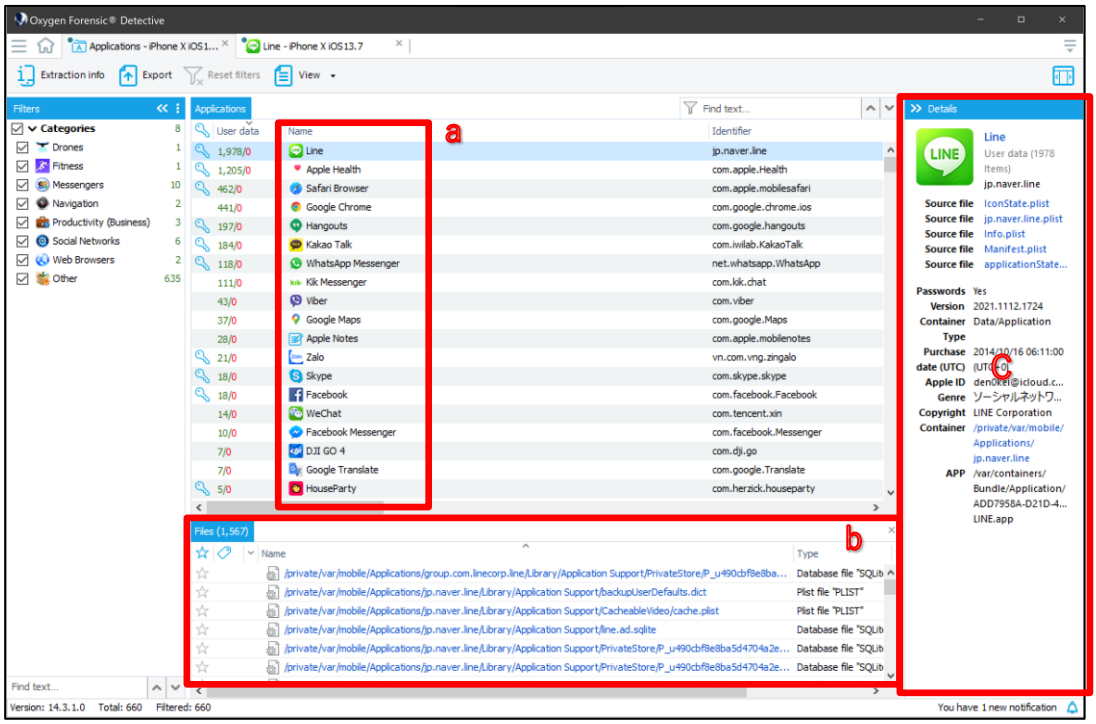
	Plist Viewer	.plist ファイルをインポートして、Oxygen Forensic® Plist Viewer で調査します。
	SQLite Viewer	SQLite データベースをインポートして、Oxygen Forensic® SQLite Viewer で調査します。
	OCPK Viewer	OCPK ファイルをインポートして、Oxygen Forensic® OCPK Viewer で調査します。

4.2 General セクションの主な解析機能



① Applications

抽出できたアプリケーションの情報を一覧で表示します。アプリケーションセクションにアイコンまたは名称が表示されていないアプリケーションも含まれる場合があります。



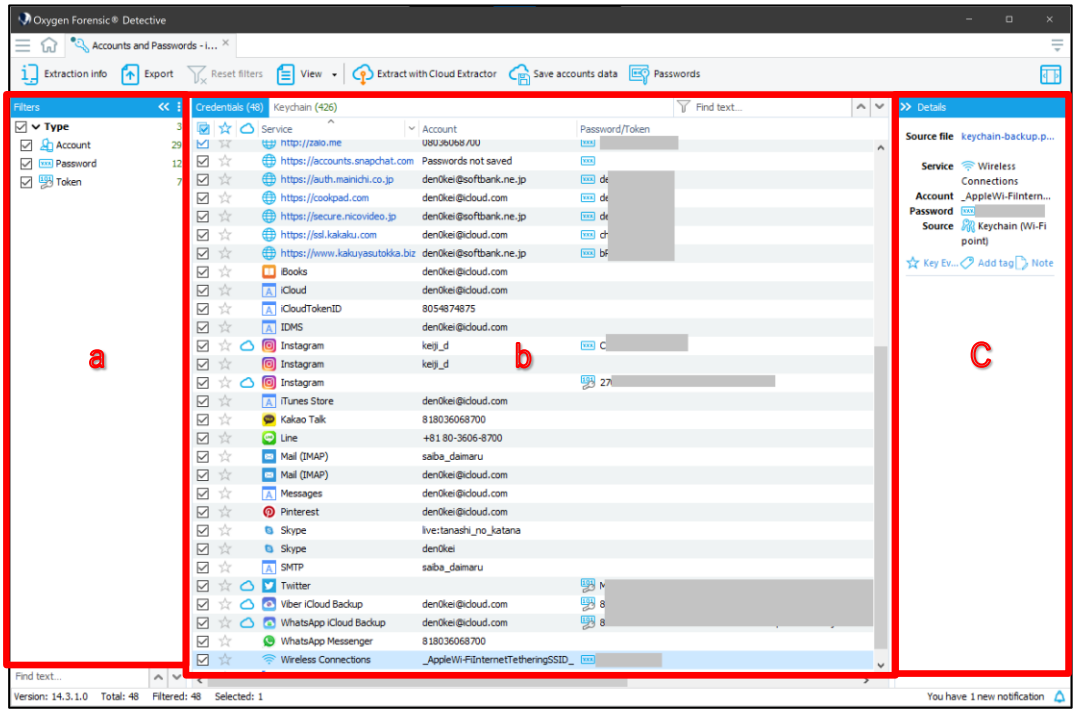
a : Name の列には、アプリケーションの一覧が表示されます。Oxygen が自動でデータを解釈できたアプリケーションは、アイコンが付与されます。アイコンが付与されていないアプリケーションは別途 SQLite Viewer などでの解析が必要となります。

b : Files には、a で選択したアプリケーションのファイルが表示されます。

c : a で選択したアプリケーションの詳細が表示されます。

② Accounts and Passwords

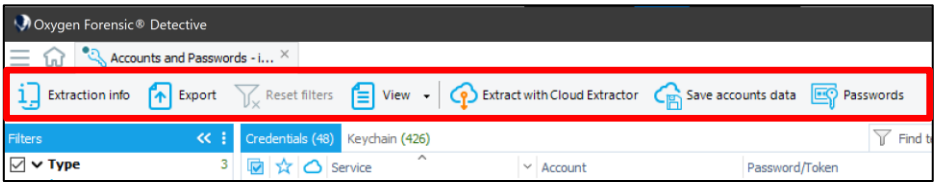
アカウントとパスワード セクションでは、アプリケーションのログインパスワード、またはトークン情報が表示されます。



a：フィルターパネルです。チェックを入れる事で Account、Password、Token などのタイプ毎にフィルターされ、b に表示されます。

b：a でチェックを入れたデータが一覧で表示されます。

C：b で選択したデータの詳細が表示されます。



Extraction info：ケースタブを表示します。

Export：レポートへの出力を行います。(詳細は、「6.1 レポートの出力」を参照してください。)

Reset filters：フィルターの設定をリセットします。

View：tag の表示/非表示

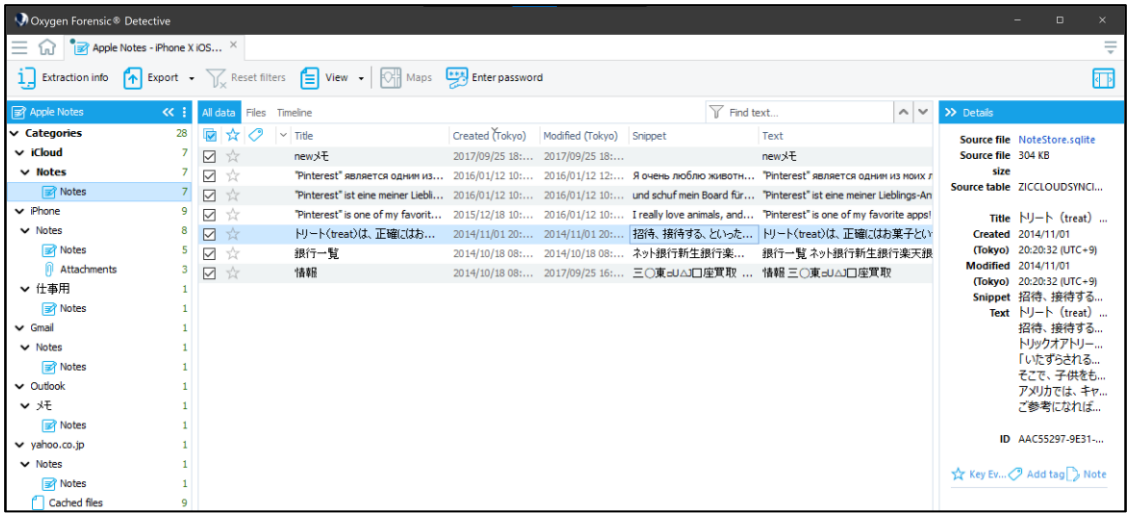
Extract with Cloud Extractor：選択した認証情報を使用して、クラウド抽出を試みます。

Save accounts data：アカウント情報を保存します。(.ocpk ファイル形式)

Passwords： Password Dictionary Builder が起動し、passwords dictionaries にアカウントとパスワード情報を追加することが可能です。

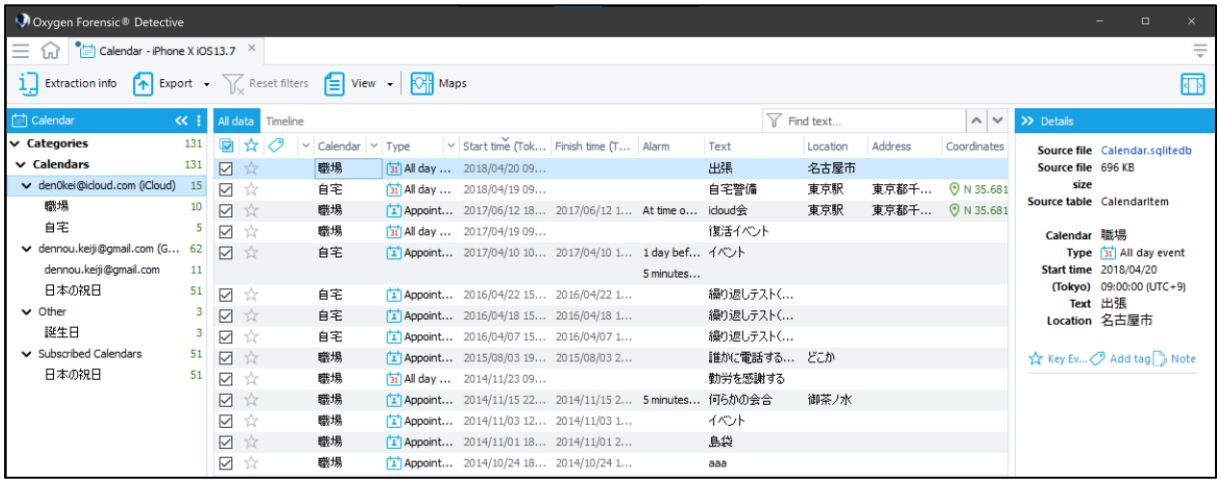
③ Apple Notes

iOS デバイス内のメモ帳機能内のメモを一覧表示します。また、メモ帳に連携されているサードパーティアプリケーションのメモ機能がある場合も表示されます。メモにロックが掛かっている場合は、パスワードを入力してロック解除することで中身が確認できます。



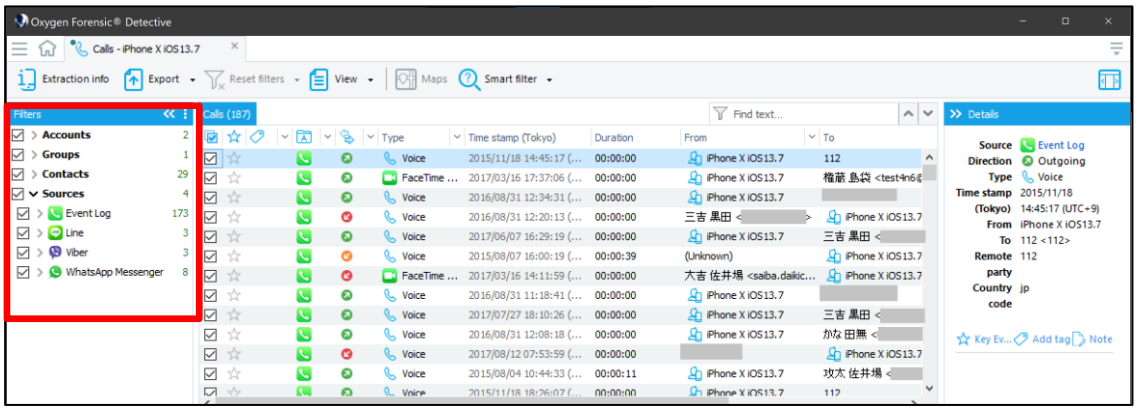
④ Calendar

デバイス内の標準カレンダーや Google カレンダー等のサードパーティのカレンダーデータを集約し一覧表示します。



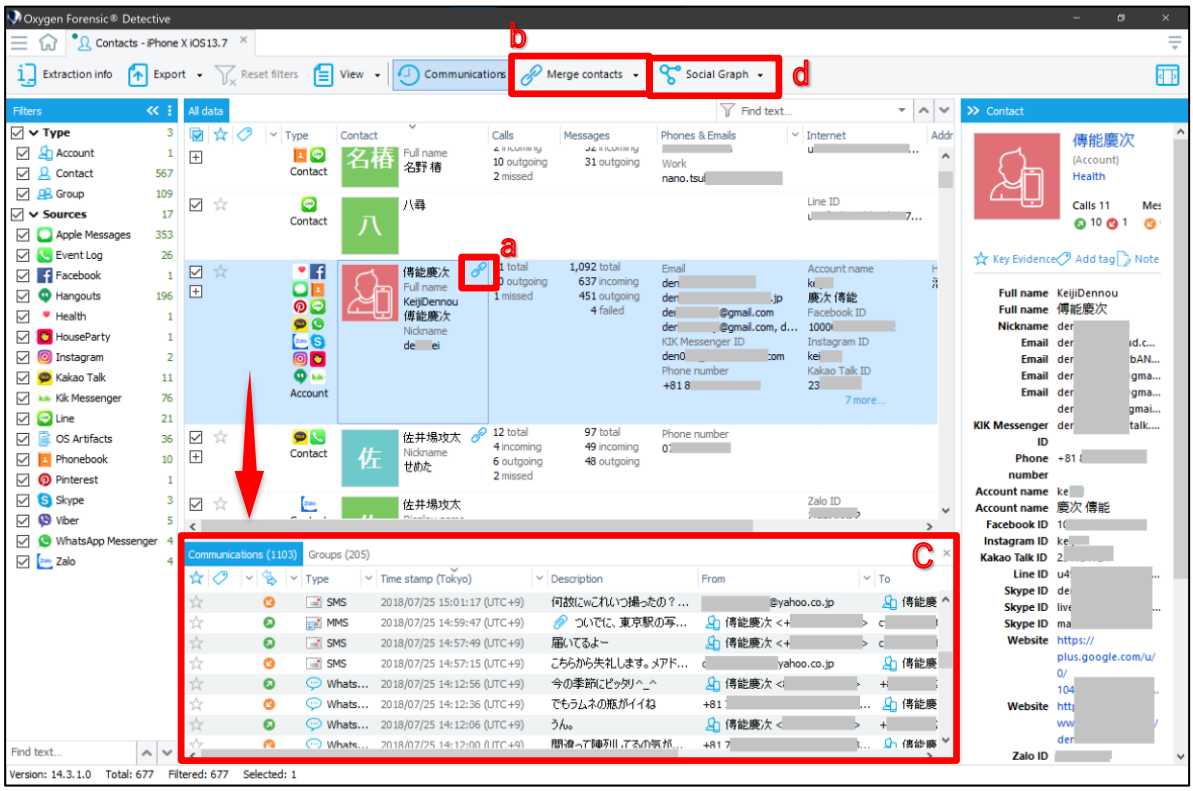
⑤ Calls

Calls セクションには、電話の通話履歴だけではなく、アプリの通話履歴もまとめて表示されます。例として、下の画像では Event Log（電話の通話履歴）および LINE、Viber、WhatsApp Messenger が表示されています。



⑥ Contacts

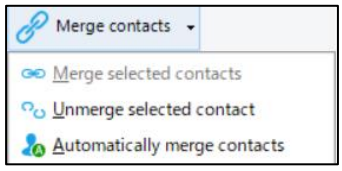
Contacts セクションには、標準機能の電話帳、通話記録、メッセージやアプリケーションなど様々なソースから取得した連絡先が表示されます。同じ連絡先は自動的に 1 つの連絡先にマージされます。



a：青色の鎖のマークは、連絡先がマージされている事を示しています。

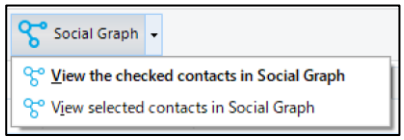
b：連絡先のマージおよび解除は Merge contacts から行えます。

- Merge selected contacts：選択した連絡先をマージします
- Unmerge selected contact：選択した連絡先のマージを解除します
- Automatically merge contacts：自動的に連絡先をマージします



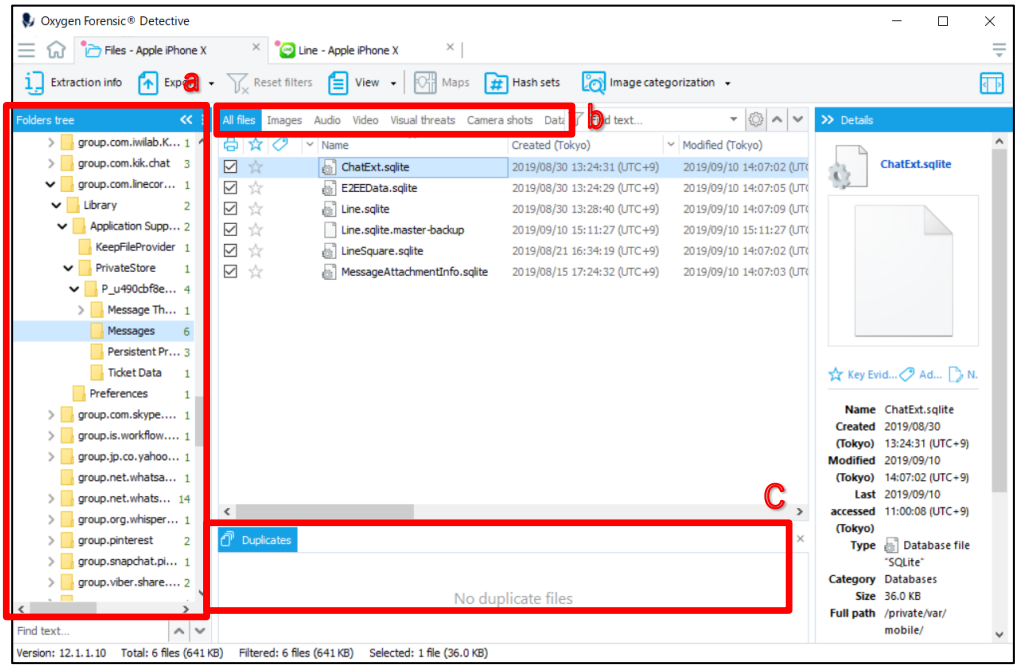
C : 選択した連絡先のコミュニケーション内容（やり取りしたメッセージや通話履歴等）が表示されます。

d : Contacts のデータを使用して Social Graph を作成します。



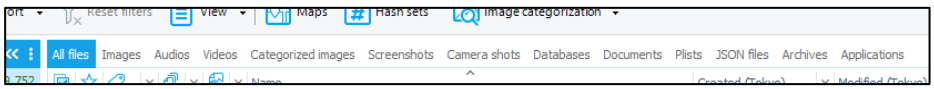
⑦ Files

Files セクションでは、取得したデータのフォルダ構造やファイルの中身をエクスプローラのように表示します。ユーザの写真、ビデオ、ドキュメントおよびデータベース情報が確認できます。



a : 端末から抽出したデータをツリー構造で表示します。取得方法によって表示される構成が異なります。主にパースしていないデータを調査する際に使用します。

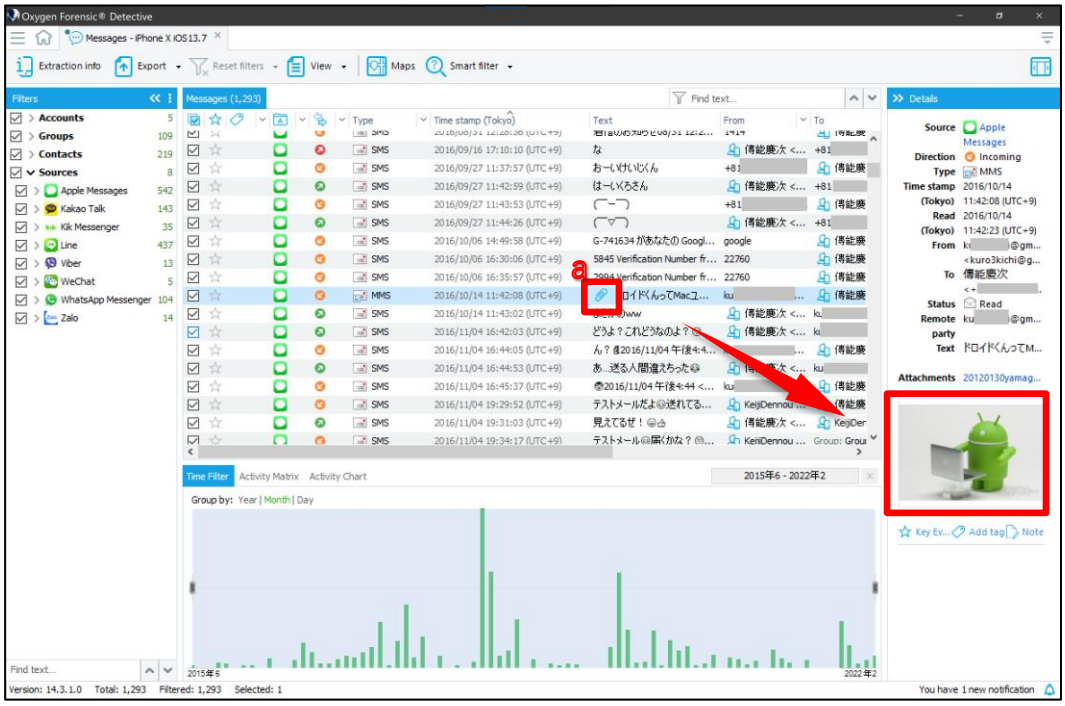
b : タブを切り替える事で、ファイルを種類別に表示する事ができます。



c : Duplicate（重複）したファイルの一覧が表示されます。

⑧ Messages

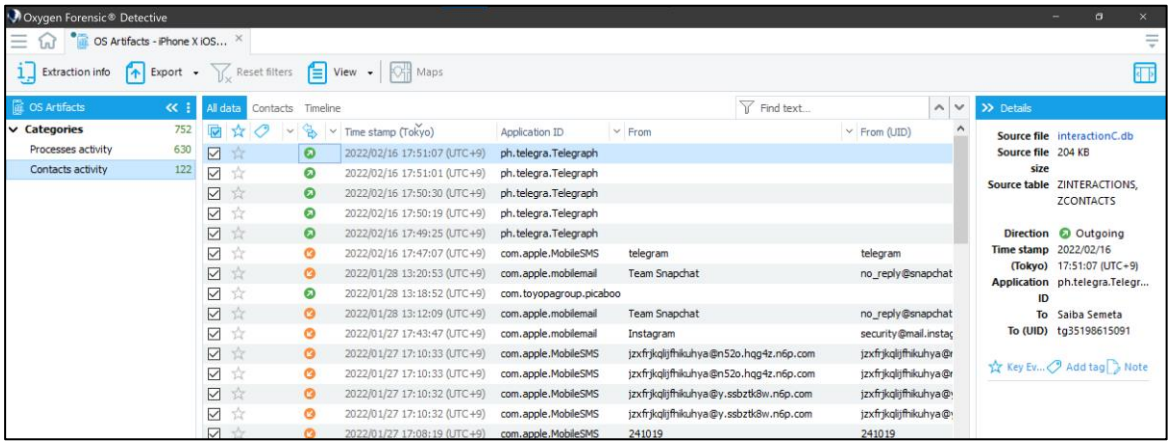
Messages セクションでは、SMS、MMS、iMessage、電子メール（添付ファイル含む）などを確認できます。



a：添付ファイルがある場合、テキスト列に青色のクリップマークが表示されます。また画面右側の Details を確認する事で Attachment されたファイル名等を確認できます。

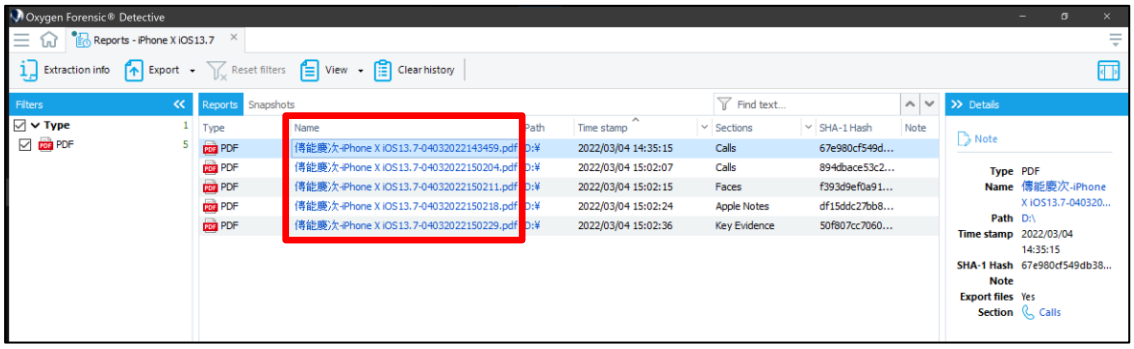
⑨ OS Artifacts

デバイス内のアクティビティなどを一覧として表示します。



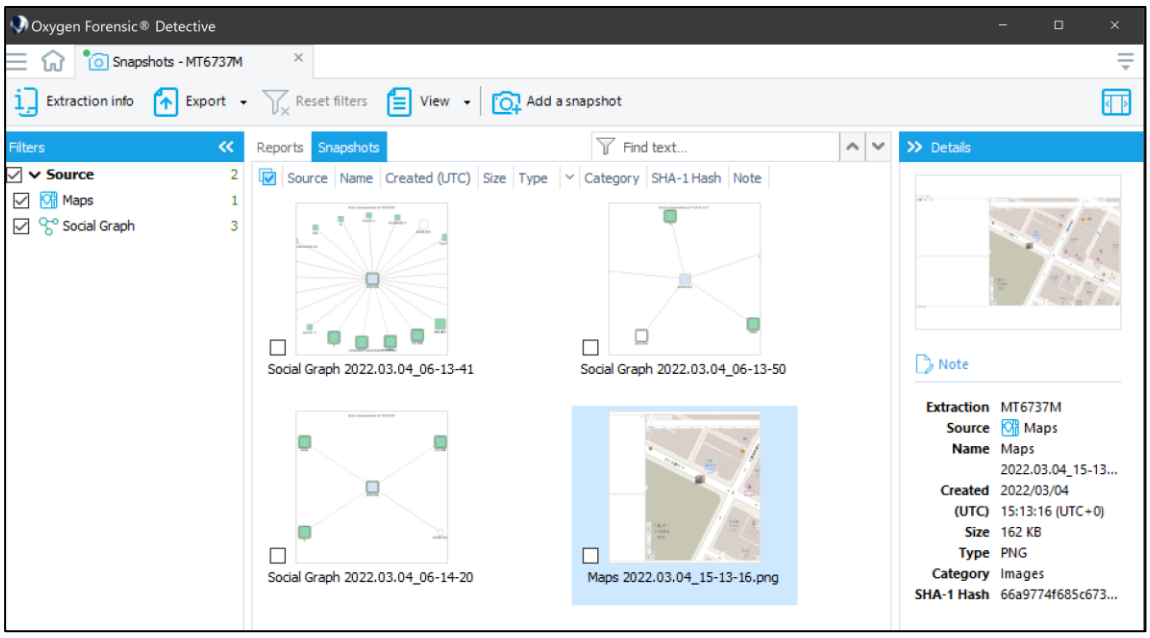
⑩ Reports

出力したレポートの一覧が表示されます。レポートが表示されているファイルパスにある場合、Name をクリックすることでレポートを表示させることが可能です。



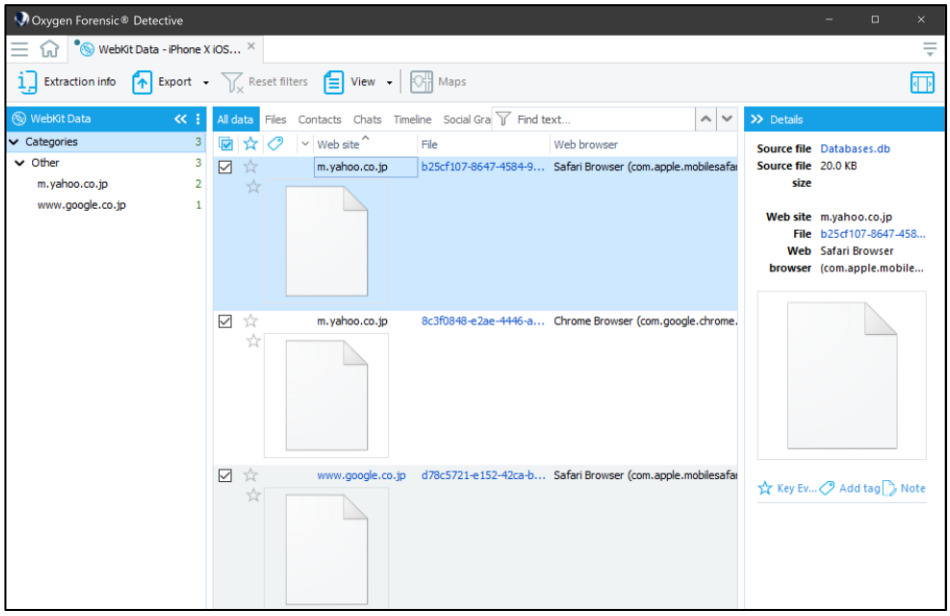
⑪ Snapshots

解析時にスナップショット機能を使用して撮影したスクリーンショットを一覧表示することが可能です。チェックボックスを有効化したデータは、レポートに含めることが出来ます。



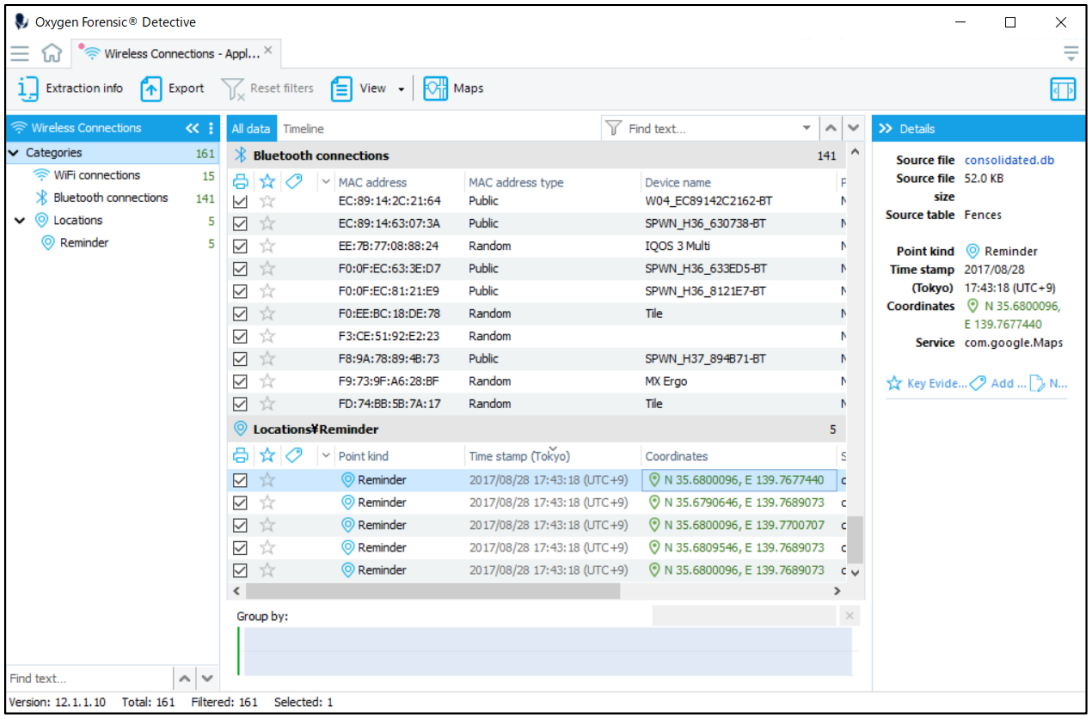
⑫ Webkit Data

iOS デバイスの場合、Apple が開発している HTML レンダリングエンジン「Webkit」のデータをパースすることで、Web メールや Web ページのコンテンツ履歴を解析することが可能です。

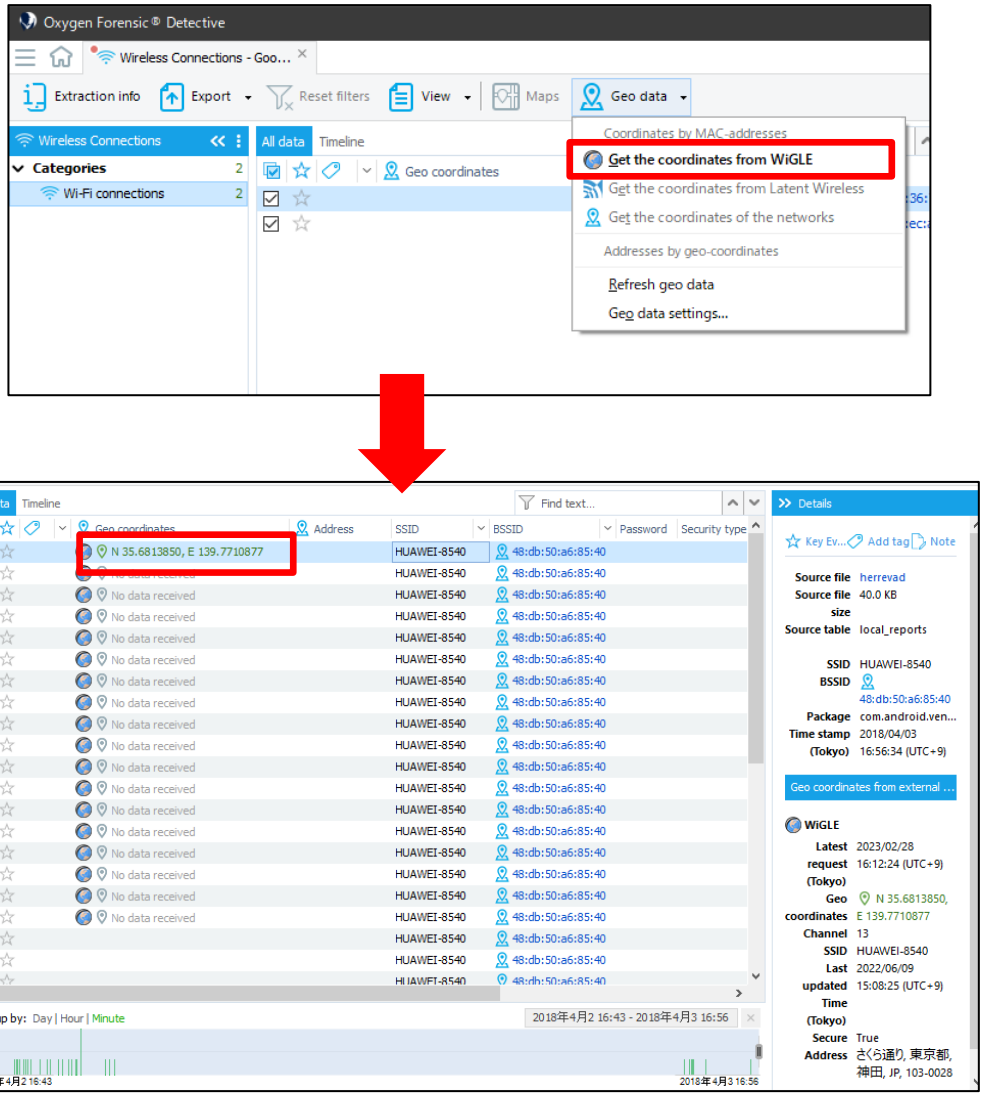


⑬ Wireless Connections

Wireless Connections セクションでは、Wi-Fi 接続の情報や、Bluetooth 接続、また GoogleMap などの地図アプリの位置情報も、取得できていれば確認できます。

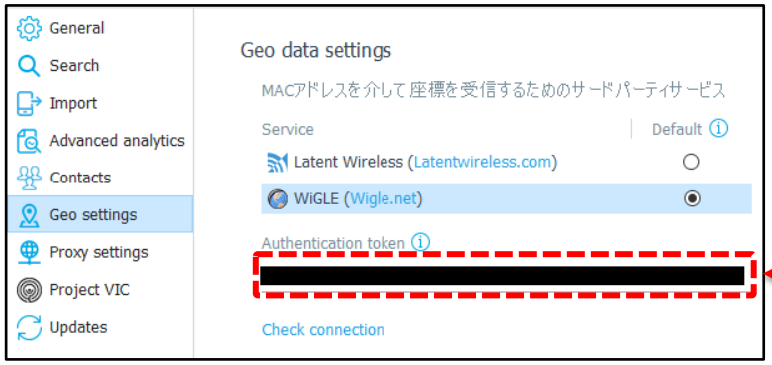


また、外部サービスである WiGLE を使用することによって、Wi-Fi の接続情報(BSSID)から位置情報を解析することも可能です。

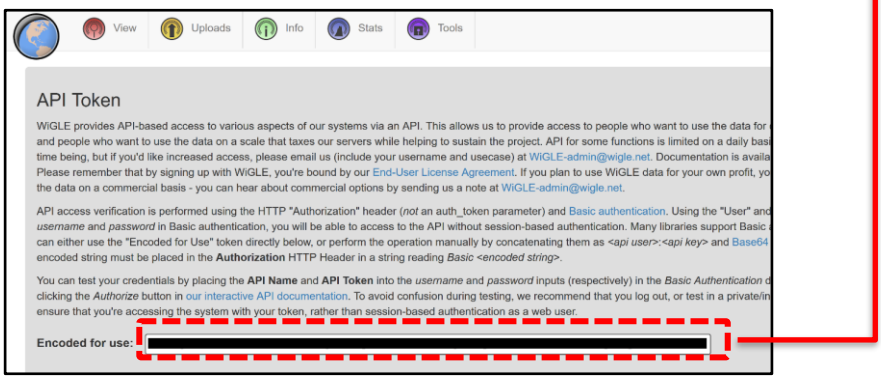


Detective 上で WiGLE を使用するには、事前に WiGLE の HP(https://wigle.net/)から無料会員登録を行い、Authentication key を発行する必要があります。

発行した Authentication key は、Detective 上の Options>Geo settings から登録出来ます。



↑Options>Geo settings 画面

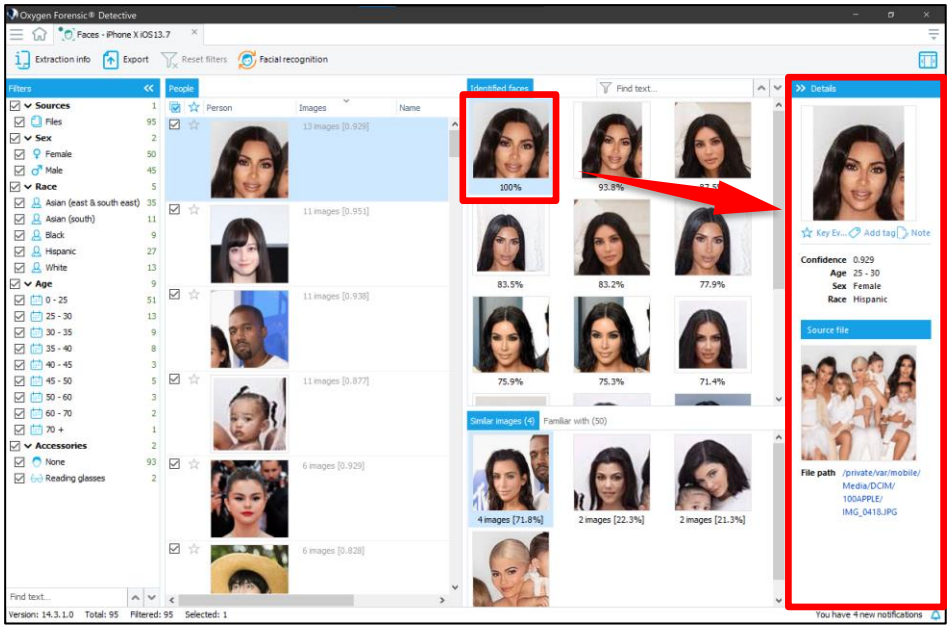


↑WiGLE の Web サイト

4.3 Analytics セクションの主な解析機能

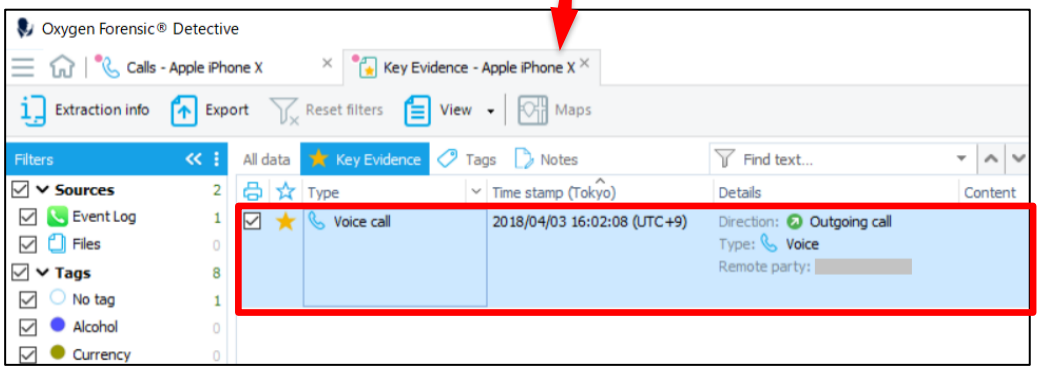
① Faces

Faces セクションでは、顔認識技術を使用して人の顔を分類できます。また、その画像から推測される年齢、性別、人種、感情などを表示します。



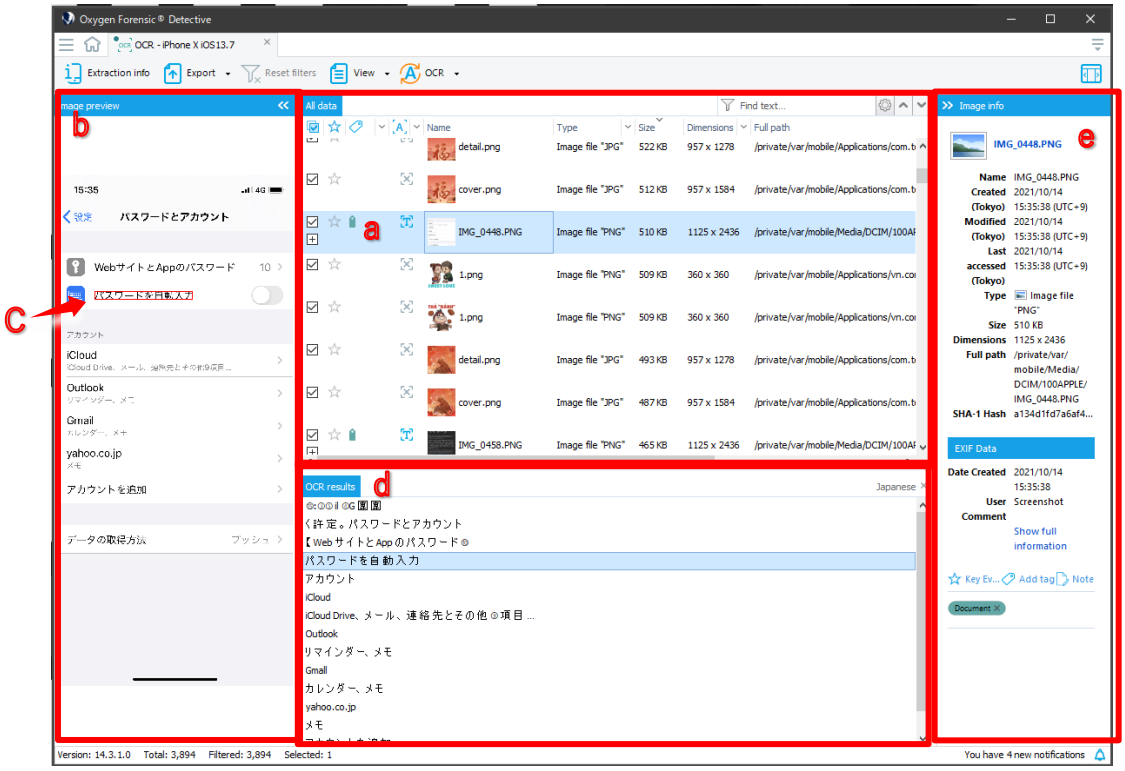
② Key Evidence

調査した情報をブックマークします。ブックマークしたい情報のフラグをクリックすることで、ブックマークした複数の情報をまとめて閲覧することが可能です。



③ OCR

OCR セクションでは、写真から文字を自動で書き起こすことが可能です。



a: 写真を選択します

b: 選択した写真のプレビューが表示されます

C: 対応している文字が赤枠で囲まれます

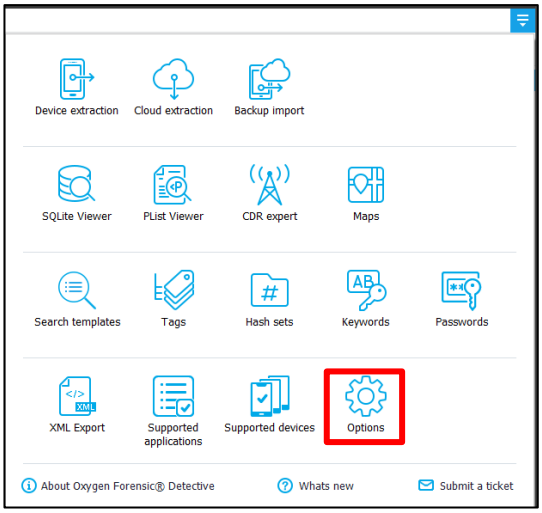
d: 選択した写真から書き起こされた文字列が表示されます

e: 選択した写真の詳細が表示されます

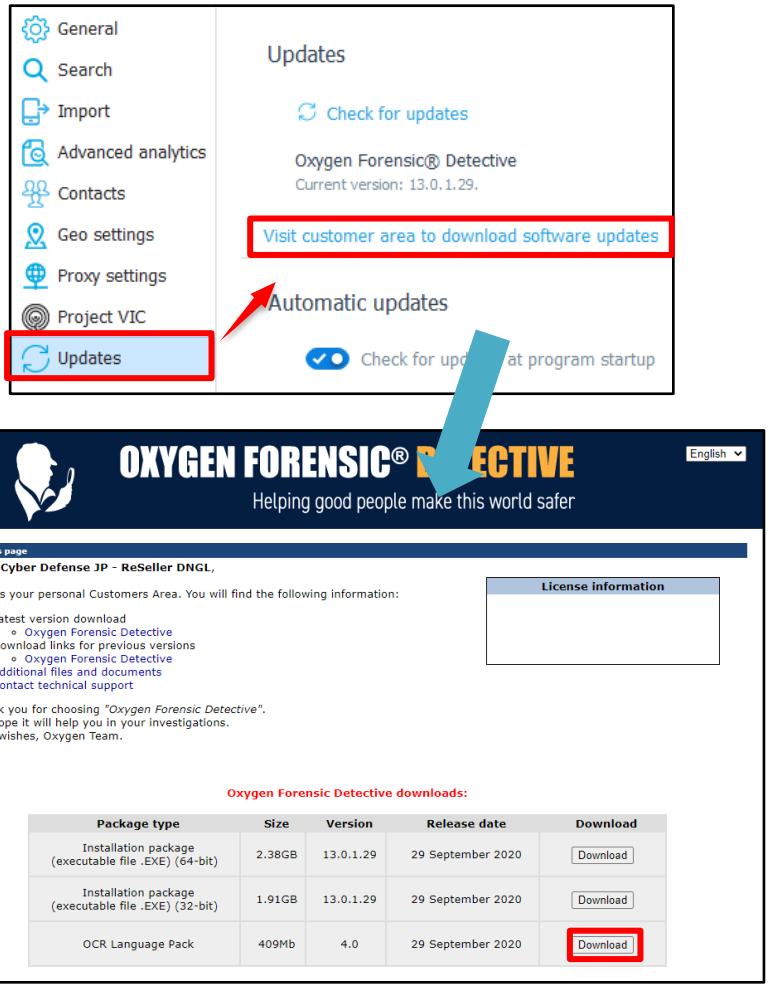
☞ 日本語を認識させるには：

1. ヘッダー右端にある menu アイコンをクリックします

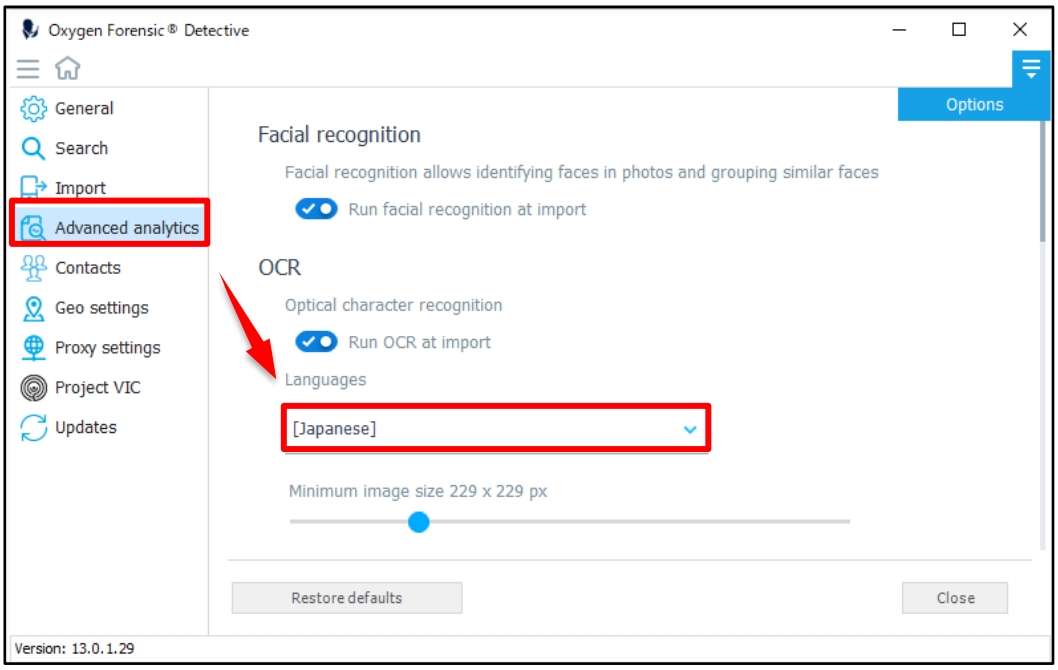
2. Options をクリックします



3. Updates タブを開き、「Visit customer area to download software updates」から Oxygen の公式ページに遷移後、OCR Language Pack の Download ボタンをクリックします。ダウンロードされた「OCR_Languages_Setup_x.x.x.exe」ファイルを展開し、インストールを完了してください

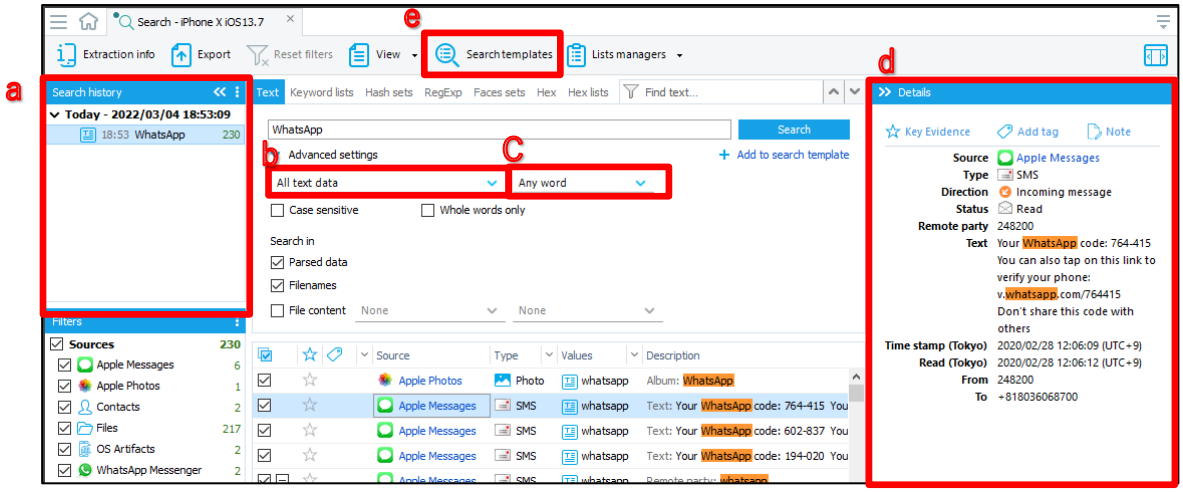


4. Oxygen Forensic® Detective を再起動し、再度 Options を開きます
5. Advanced analytics タブを開き、OCR の Languages を Japanese に設定します
6. Close ボタンを押して、OCR の言語設定は完了です



④ Search

キーワードよる検索はもちろん、探したい情報（電話番号、メールアドレス、クレジットカード番号等）を指定して検索することができます。



a：Search history では、検索履歴が確認できます。

b：探したい情報を指定できます。デフォルトでは All text data が設定されています。

C：テキスト入力欄に入力したキーワードのいずれかを含む情報の検索や、正確なフレーズでの検

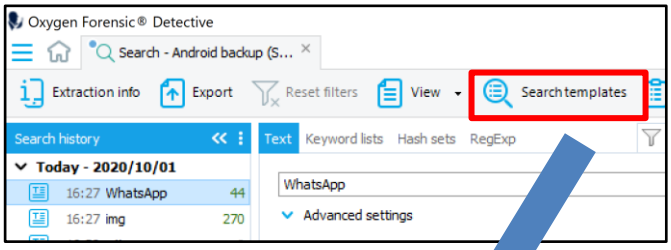
索等、検索方法の指定ができます。デフォルトでは Any words が設定されています。

d：Details 欄では、検索結果から選択した情報の詳細が確認できます。

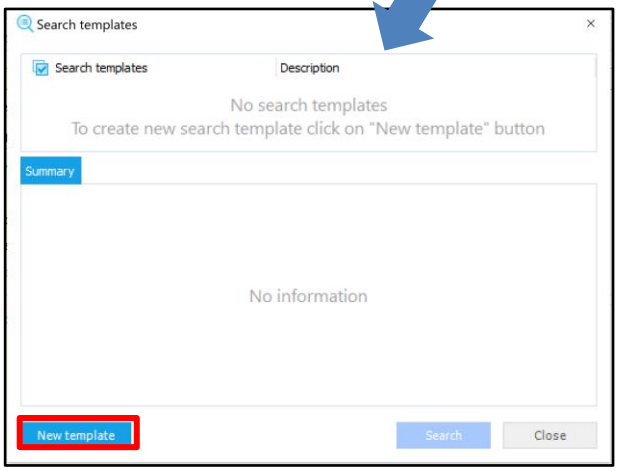
e：保存された検索テンプレートを用いてデータを検索できます。

☞ 検索テンプレートを追加するには：

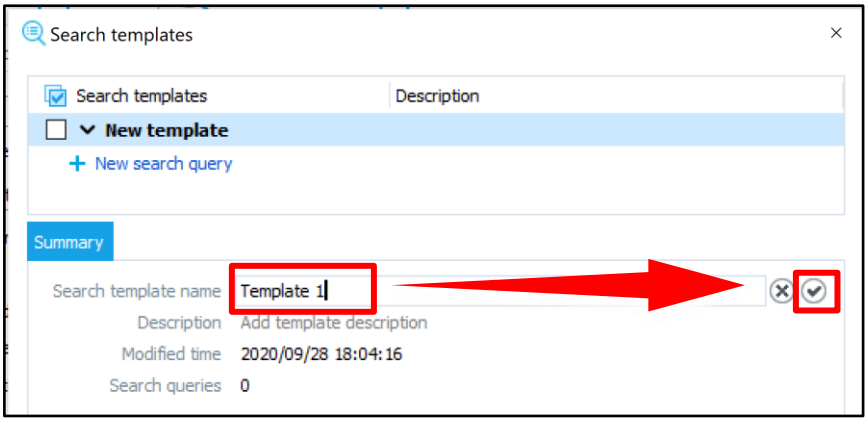
1. Search templates をクリックします



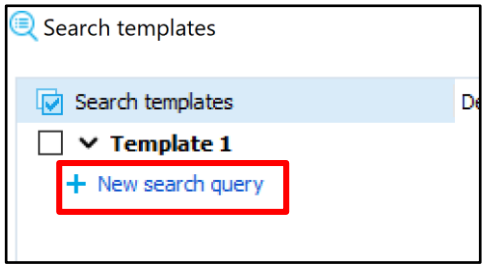
2. New template をクリックします



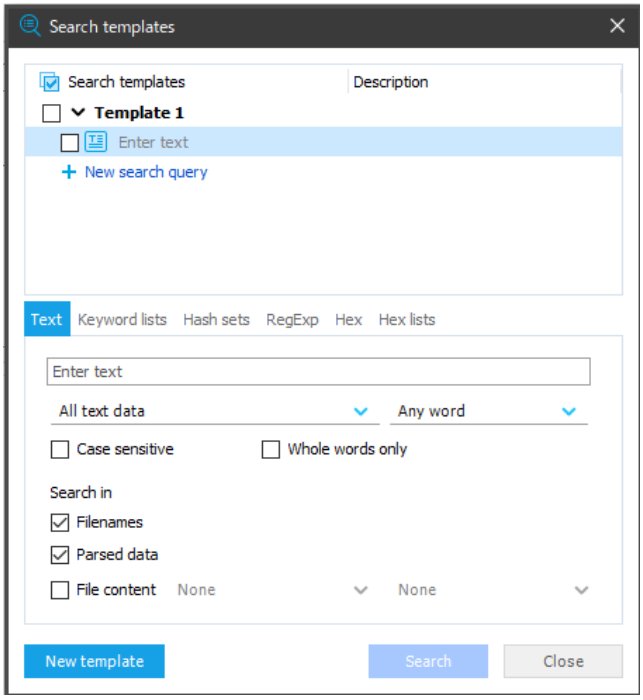
3. テンプレート名を入力し、✓ボタンをクリックして保存します



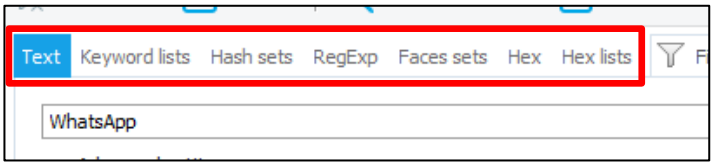
4. New search query をクリックします



5. 作成したテンプレートに検索条件を保存することが出来ます



その他にも、keywords、Hash sets、RegExp、Hex、Hex lists のタブを切り替える事で柔軟な検索が行えます。



⑤ Social Graph

a：コミュニケーション回数でフィルターします。

b：

	Rebuild graph	グラフの再読み込み
	Enable drag mode	ドラッグモードの有効化
	Full Screen	全画面へ切り替え

⑥ Statistics

Statistics セクションでは、ユーザアクティビティの全体的な統計セクションを確認することが可能です。各グラフは、クリックすると Timeline が表示され、詳細の確認が可能です。

a：ユーザアクティビティをチャート図で表示します。

b：ユーザアクティビティをマトリックス図で表示します。

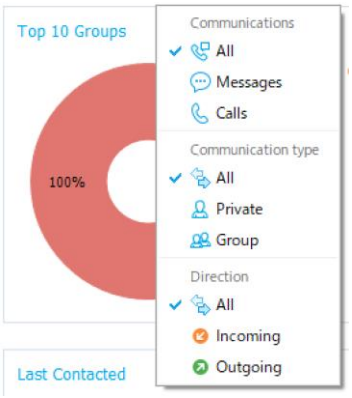
c：使用率の高いアプリケーション上位 10 位までを円グラフで表示します。

d：連絡頻度の高い連絡先上位 10 位までを円グラフで表示します。

e：連絡頻度の高いグループ上位 10 位までを円グラフで表示します。

f：最新 10 件の連絡履歴を表示します。

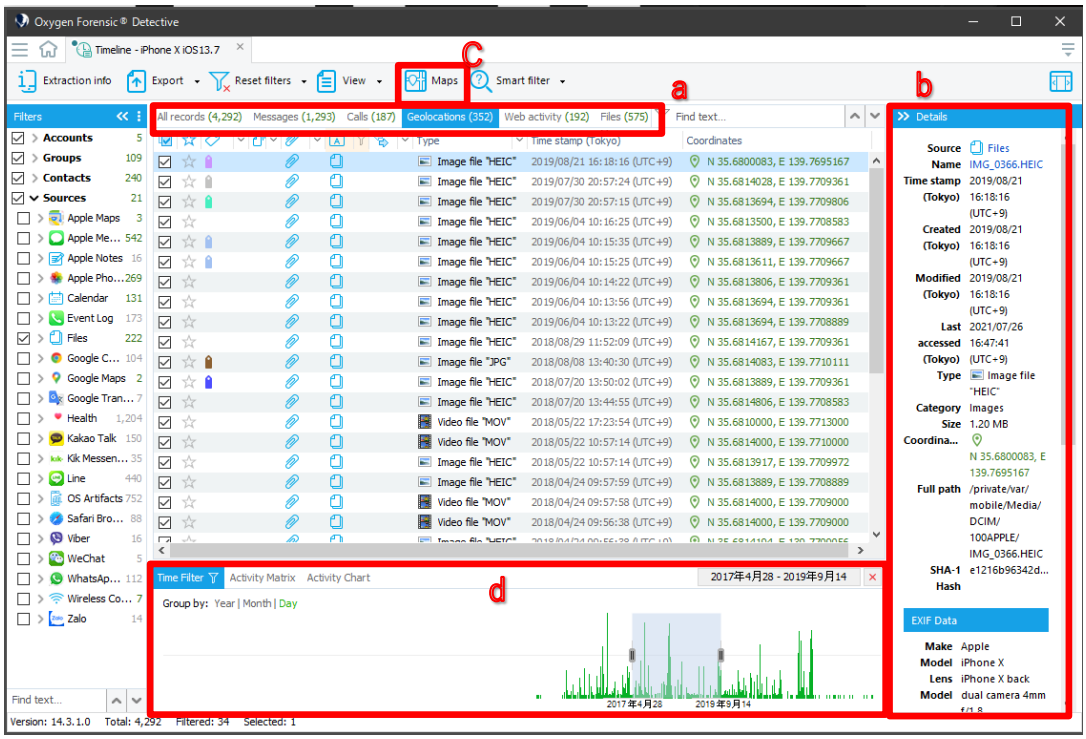
☞　歯車アイコンをクリックすると、ソートのオプションが表示されます。



g：ユーザアクティビティ内のデータ種別を表示します。

⑦　Timeline

様々なアクティビティを時系列で分析します。

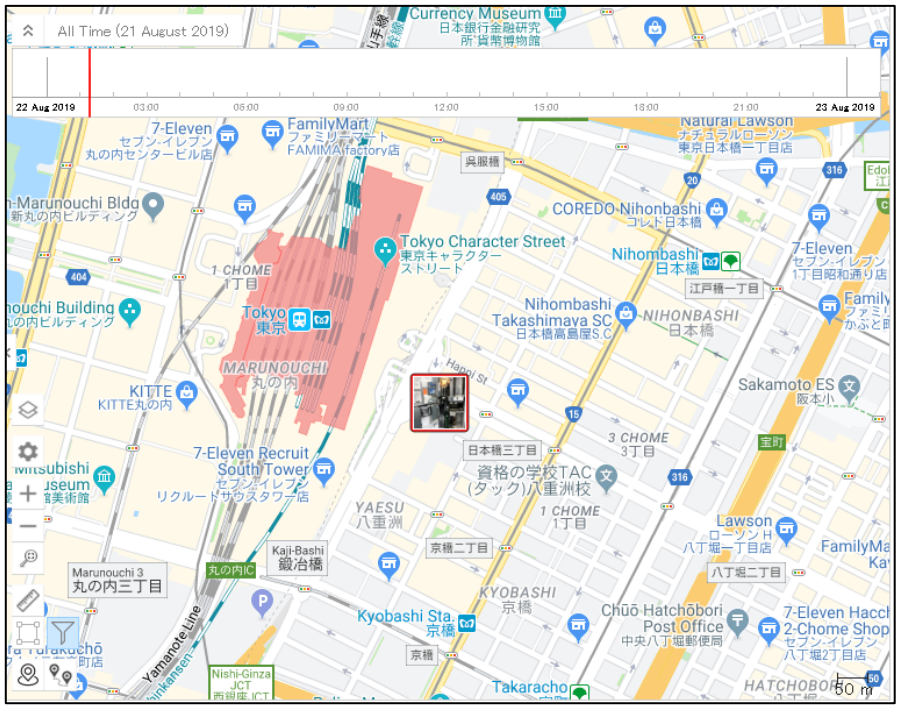


a：表示方法を選択できます。「All records」タブで全てのアクティビティを時系列で表示します。その他に、Messages、Calls、Geolocations、Web activity、Files にタブを切り替える事でアクティビティの種別毎に時系列で表示する事ができます。

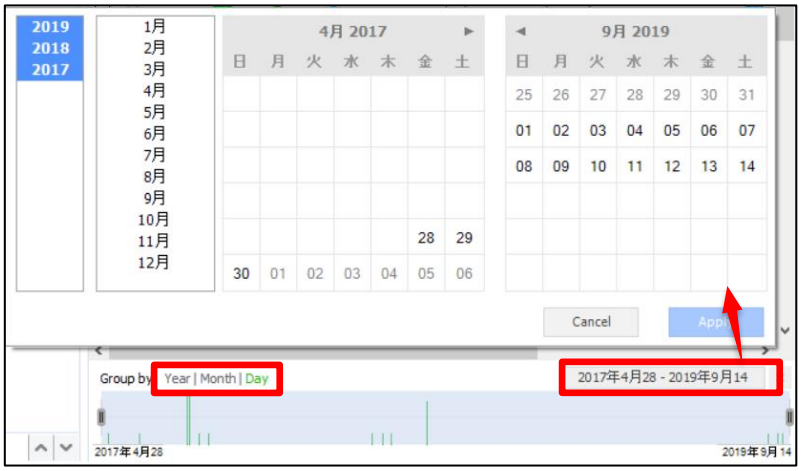
b：選択したデータに Exif 情報があれば、Details に表示されます。

c：位置情報を含んだデータは、ボタンパネルの「Maps」 から地図を開く事も可能です。

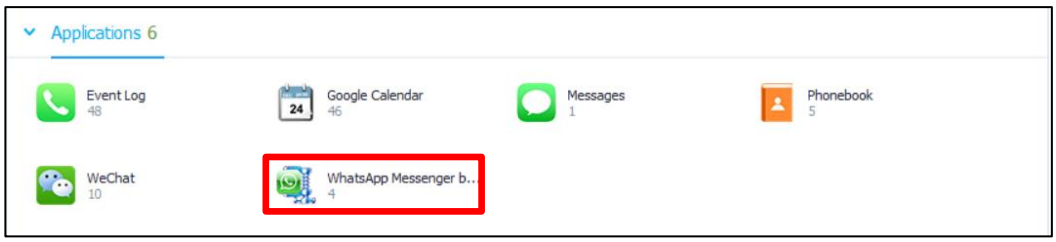
補足：Maps 機能は GoogleMaps、OpenStreetMap、BaiduMap 等のマップを選択できます。下図は、GoogleMaps を使用して表示した例です。



d：画面下には日付フィルターがあります。表示したい期間を設定することが可能です。また、Year、Month、Day に表示を切り替える事も可能です。

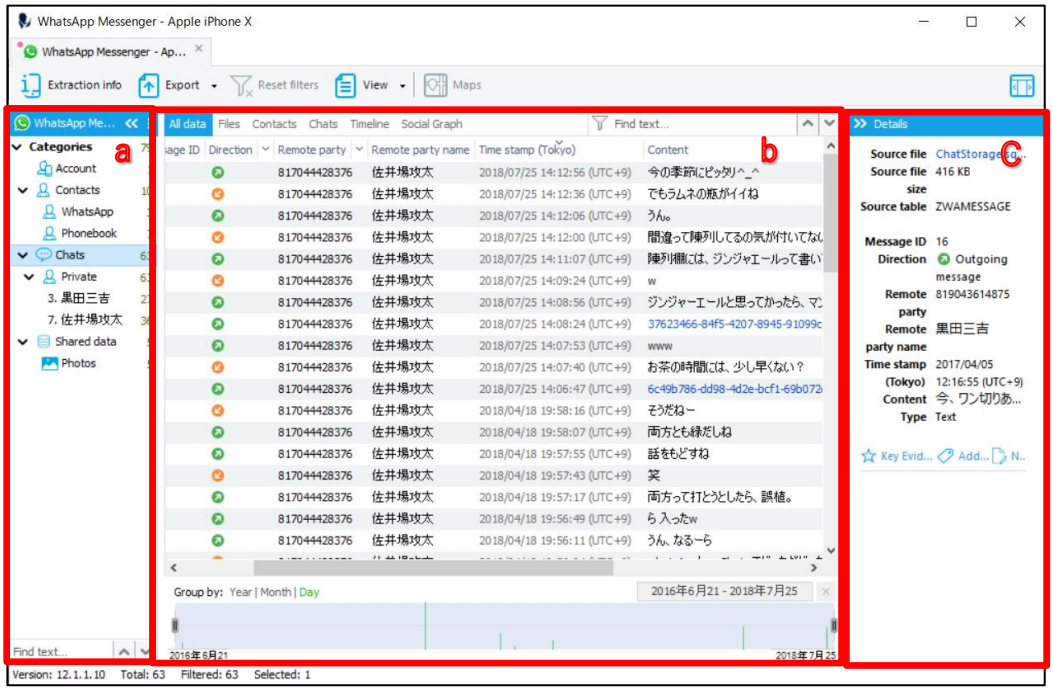


4.4 アプリケーションセクションの主な解析機能



抽出できたアプリケーションデータのうち、Oxygen が自動でデータを解釈し可視化できたアプリケーションのアイコンまたは名称が表示されます。アプリケーションアイコンまたは名称をクリックすることで該当するアプリケーションデータを個別に閲覧することができます。

個別のアプリケーションに対する解析方法は、どれも類似しているので、ここでは例として、WhatsApp Messenger について説明します。



a：カテゴリーでフィルター可能

b：a で選んだカテゴリーの内容が b に表示されます。

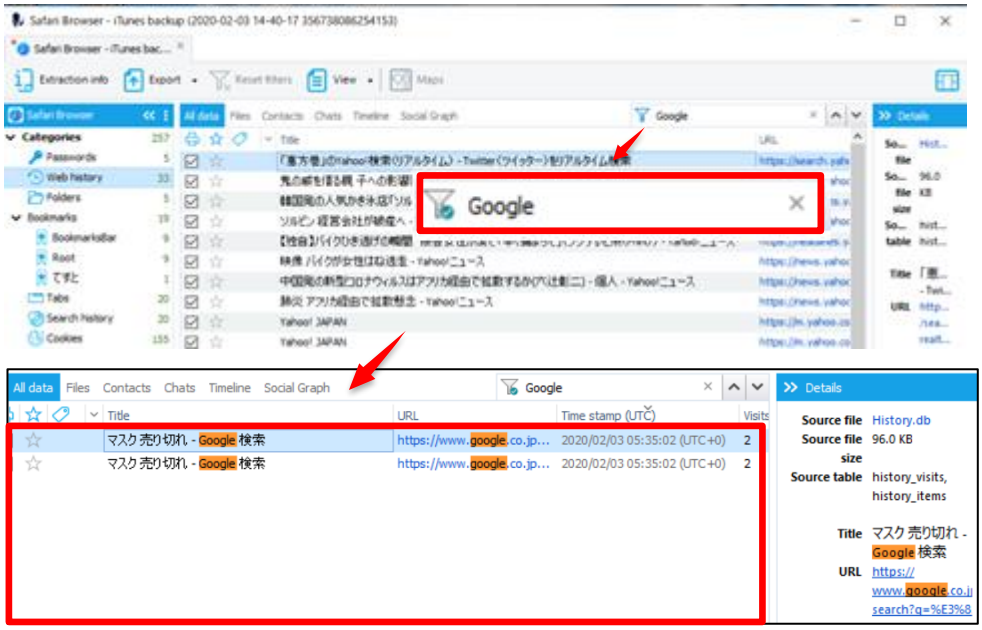
この例では、a で chats を選択しているので、chats の内容が b に表示されています。

c：ソースファイルへのリンクなどの詳細情報が表示されます。

4.5 基本的な解析機能の紹介

- **クイックフィルタ機能**

セクション内のデータに対して、meta データや拡張子、文字列などをクエリボックスに入力した文字列で検索し、ウィンドウに表示する機能です。

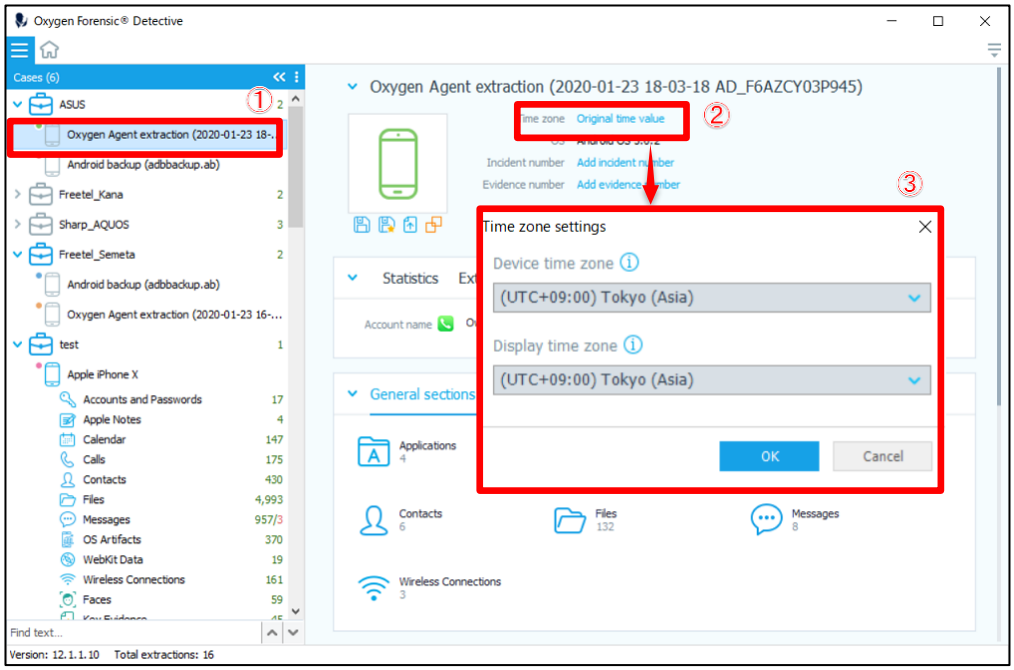


ここでは web ブラウザの閲覧履歴情報から「Google」の文字列を検索した結果を表示しています。

- **タイムゾーン設定**

Oxygen のタイムゾーンを設定します。

タイムゾーンの設定は、取り込んだデバイス毎に行う必要があります。



①：ケースパネルから対象のデバイスを選択します。

②：Time zone の項目、デフォルトは青い文字で「Original time value」と表示されている箇所をクリックします。

③：Time zone settings が表示されます。タイムゾーンをそれぞれ日本時間、(UTC+09:00) Tokyo (Asia)に設定します。

☞ Device time zone：デバイス内の非 UTC のタイムスタンプ（例えば、EXIF 等のメタデータ）です。こちらの設定を変更すると、タイムラインセクションの Details に反映されます。

☞ Display time zone：インターフェイスに表示されるタイムゾーンです。こちらの設定を変更すると、Detective のインターフェイスに反映されます。

デバイスやアプリによって保持する時刻情報に違いがある場合などは、
特に注意が必要です。

5　解析データのバックアップ

Oxygen のバックアップファイルには独自形式の拡張子が 3 種類あります。

各拡張子の特徴は以下をご確認ください。

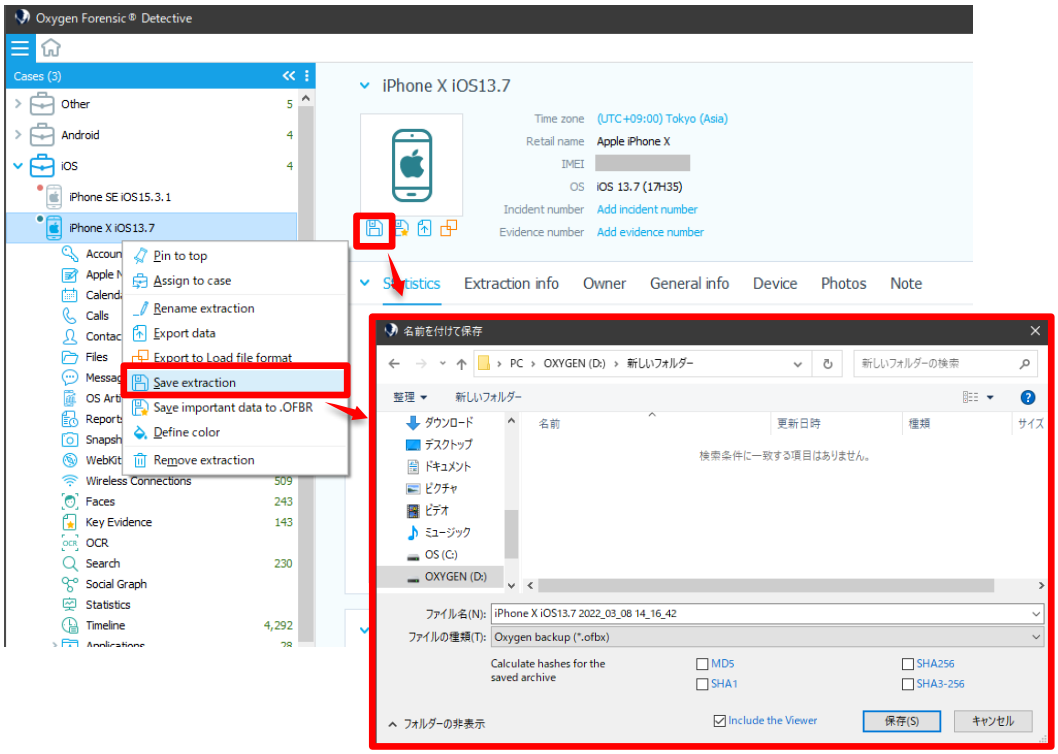
OFB 形式	Detective v11 以前のバックアップファイルの拡張子	
OFBX 形式	Detective v12 以降のバックアップファイルの拡張子	
OFBR 形式	Save important data only	Key Evidence を付けているデータ**のみを対象**にしたバックアップファイルの拡張子
	Exclude irrelevant data	「Not Relevant(重要ではないデータ)」としてマークしたデータ**以外を対象**にしたバックアップファイルの拡張子

5.1　OFBX バックアップの作成

- **OFBX バックアップの作成手順**

① 左のケースパネルからバックアップファイルを作成したいデバイスを選択し、右クリックして「Save extraction」を選択、もしくは、  アイコンをクリックします。

表示されたウィンドウ上で保存先を選択し、「保存」をクリックします。

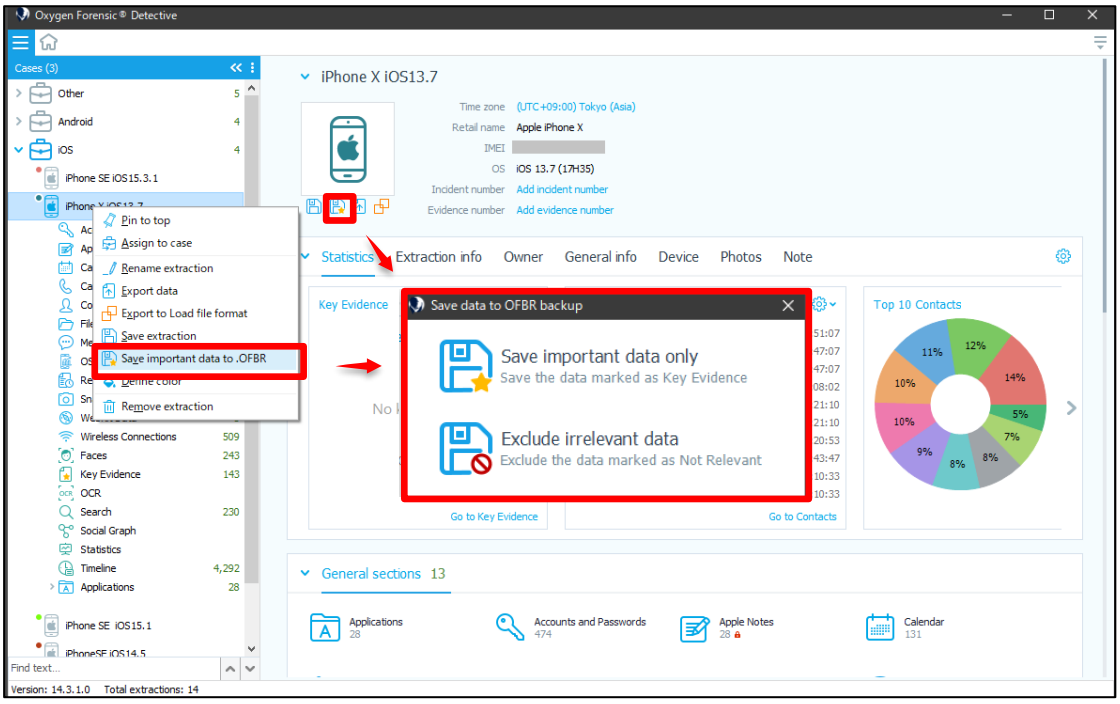


5.2 OFBR バックアップの作成

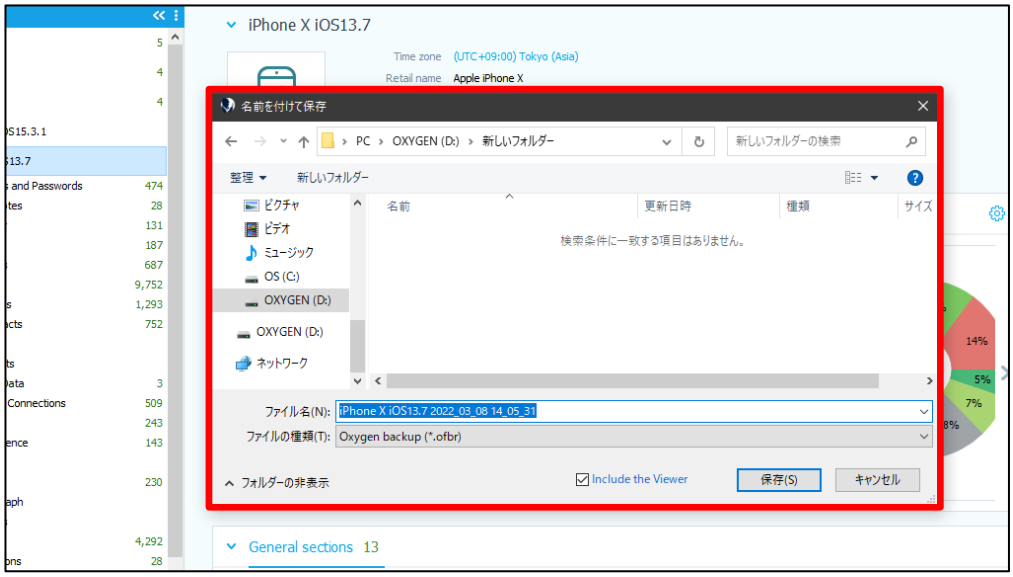
- **OFBR バックアップの作成手順**

① 左のケースパネルからバックアップファイルを作成したいデバイスを選択し、右クリックして「Save important data to .OFBR」を選択、もしくは、  アイコンをクリックします。

「Save data to OFBR backup」ポップアップが表示されるので、目的にあったメニューを選択してください。



② 保存先を選択して「保存」をクリックします。



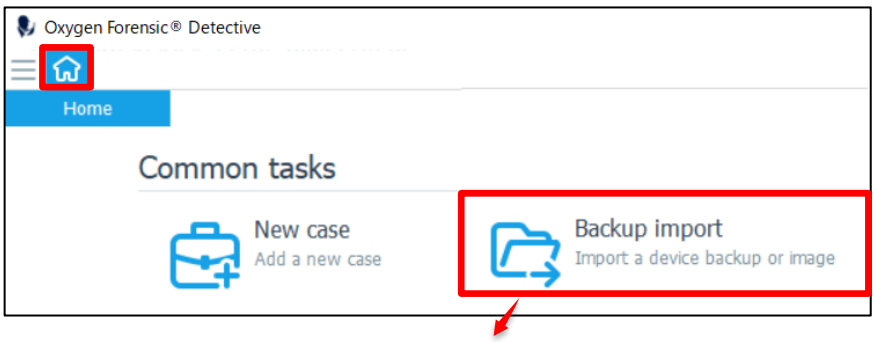
5.3 OFBX・OFBR バックアップの読み込み

OFBX・OFBR バックアップファイルは、Oxygen 同士であれば相互に読み込むことができます。

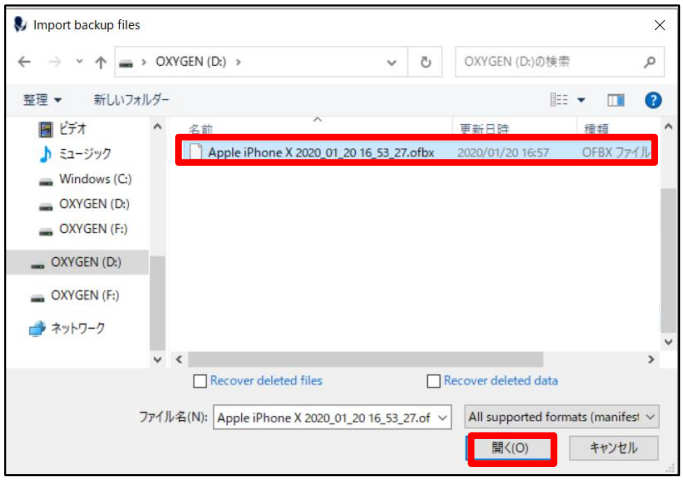
- **OFBX・OFBR バックアップファイルの読み込み手順**

① ホームタブをクリックし、Common tasks の項目の中から「Backup Import」をクリックします。

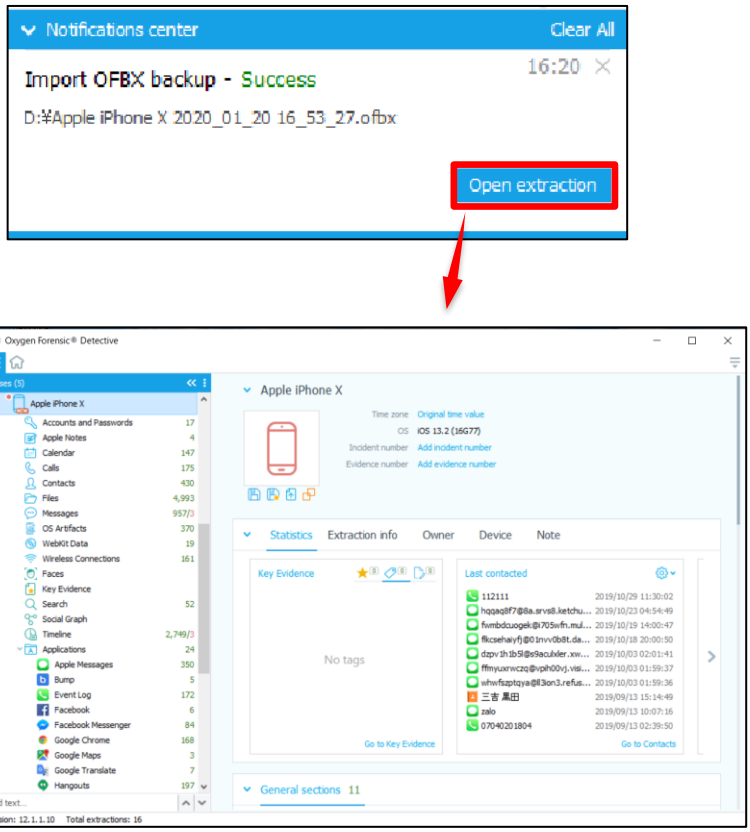
☞ 他にも、Import の項目の Oxygen の中から「Oxygen Forensic® backup」をクリックし、OFBX・OFBR ファイルを読み込むことも可能です。



② 任意の ofbx・ofbr ファイルを選択し、「開く」をクリックすることで読み込みが開始されます。



③ 読み込みに成功したら、「Open extraction」をクリックすると、インポートした情報が表示されます。



5.3 iTunes バックアップの読み込み

Oxygen は iTunes のバックアップファイルの解析に対応しています。

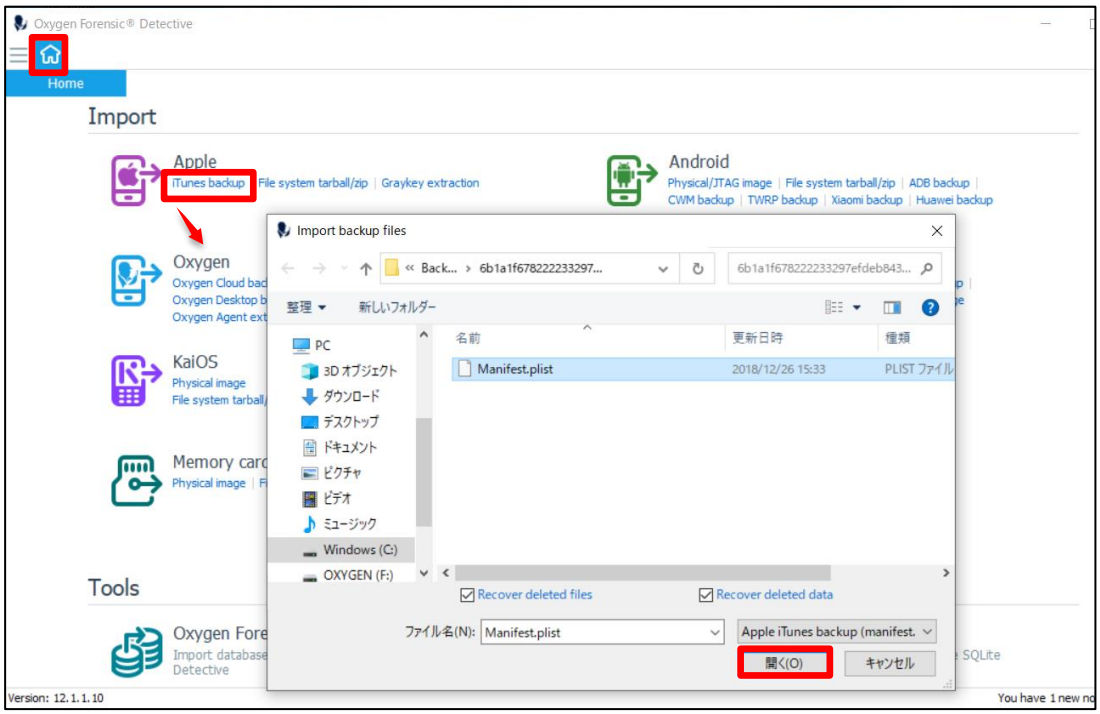
iTunes バックアップファイルが暗号化されている場合、パスワードの入手や解析が必要です。

iTunes バックアップファイルのデフォルトの保存場所は下記の通りです。

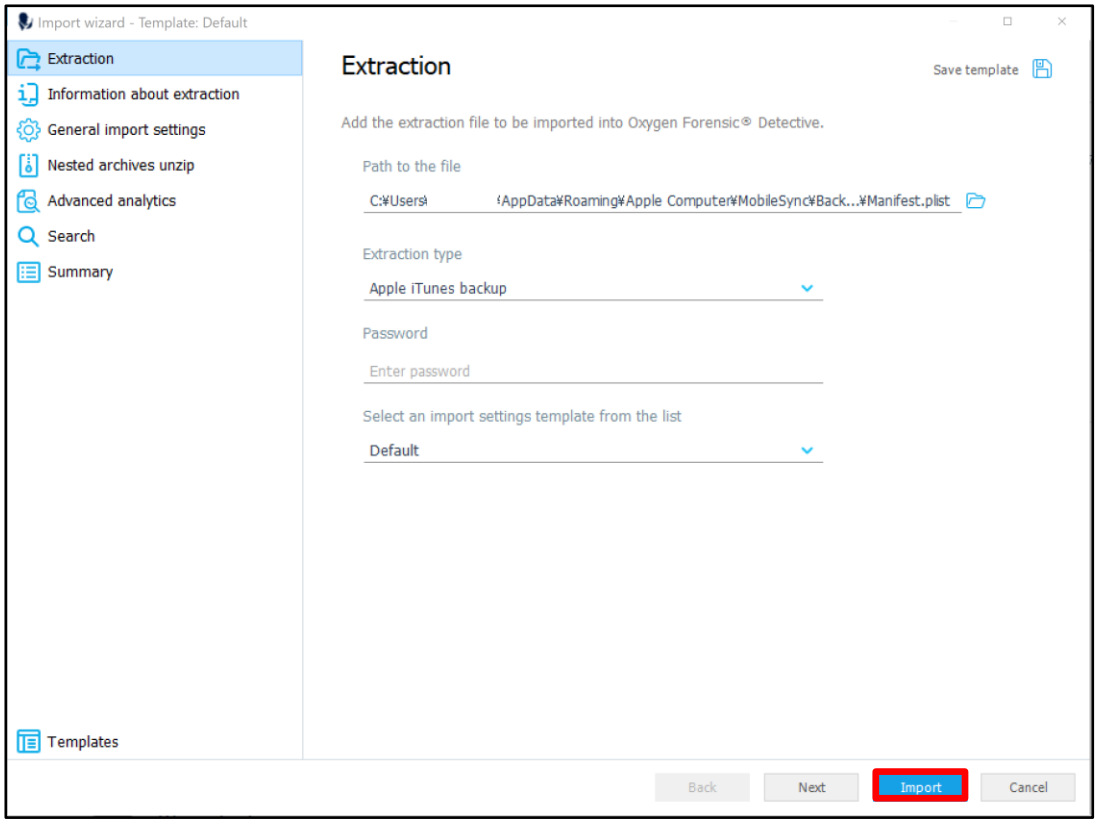
Windows XP	C:¥Documents and Setting¥(ユーザ名)¥Application Data¥Apple Computer¥MobileSync¥Backup¥(デバイス毎の UDID)
Windows Vista,7,8,10	C:¥Users¥(ユーザ名)¥AppData¥Roaming¥Apple Computer ¥MobileSync¥Backup¥(デバイス毎の UDID)
Mac	Users¥(ユーザ名)¥Library¥Application Support¥MobileSync¥(デバイス毎の UDID)

- **バックアップファイルの読み込み手順**

① ホームタブをクリックし、Import の項目の中の Apple の中から、「iTunes backup」をクリックします。バックアップデータのあるフォルダ内の plist ファイルを選択し「開く」をクリックします。



② Import wizard が表示されるので、特に変更がない場合は「Import」をクリックします。

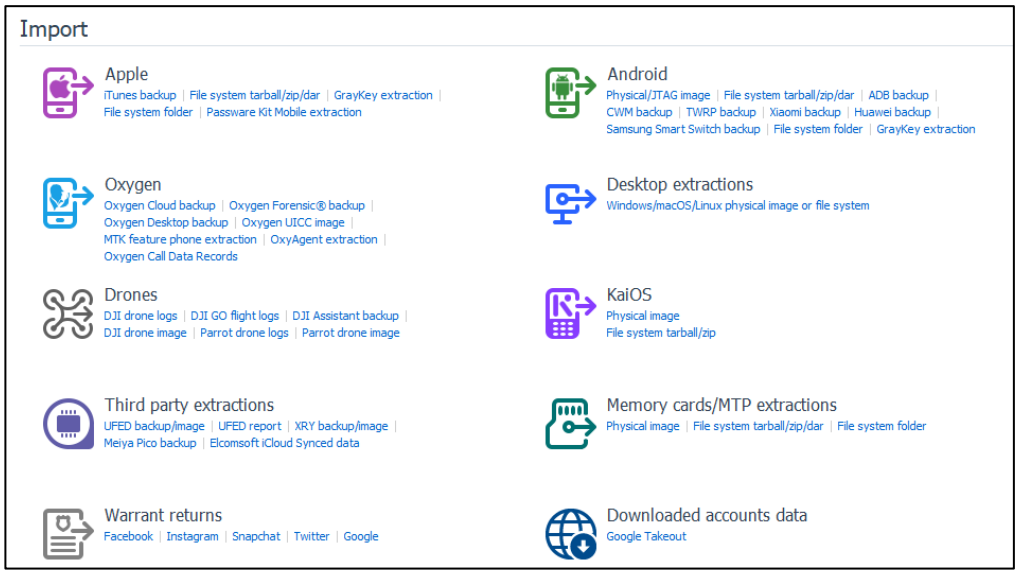


③ 以後の操作は、「5.2 OFBX・OFBR バックアップの読み込み」の③以降と同様です。

5.4　その他のバックアップ/イメージファイルの読み込み

Oxygen Forensic® Detective は、「ofbx・ofbr バックアップファイル」や「iTunes バックアップファイル」以外にも様々なバックアップファイルやイメージファイルの読み込みに対応しています。

各種バックアップファイルやイメージファイルを読み込むには、Import の中から、各項目を選択します。



6　レポートの出力

6.1　レポートの出力

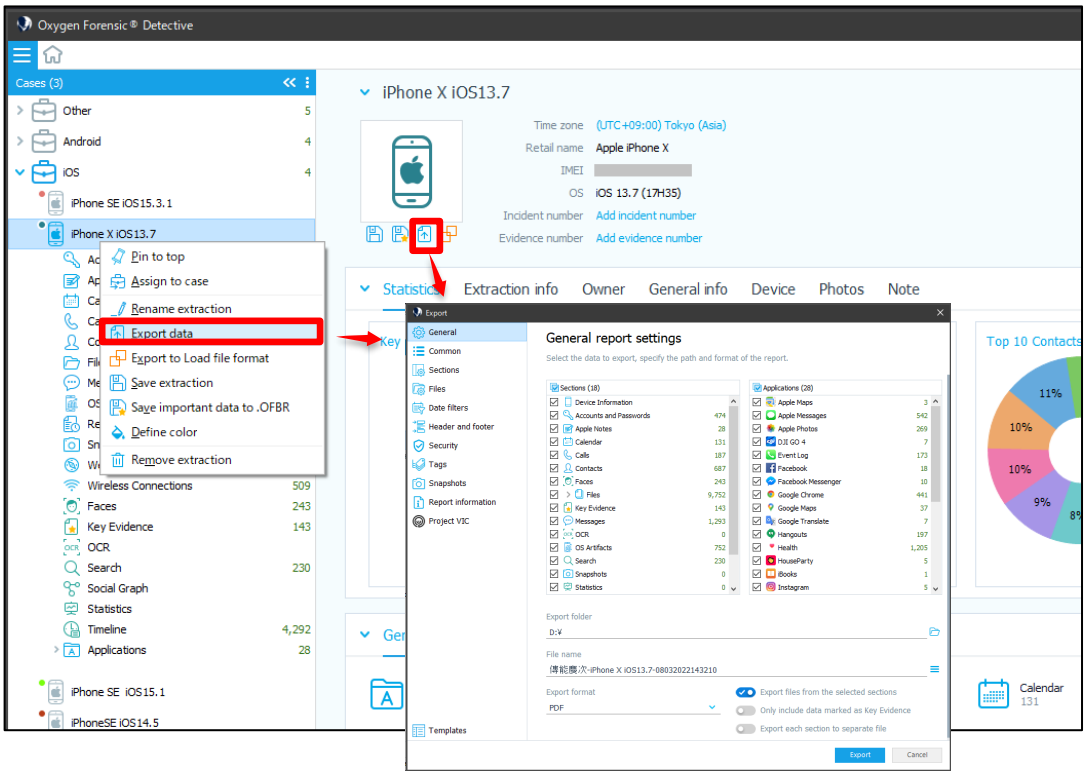
デバイスやバックアップファイル等から抽出したデータを、下記の種類の形式のレポートとして出力できます。

- **レポートの形式**

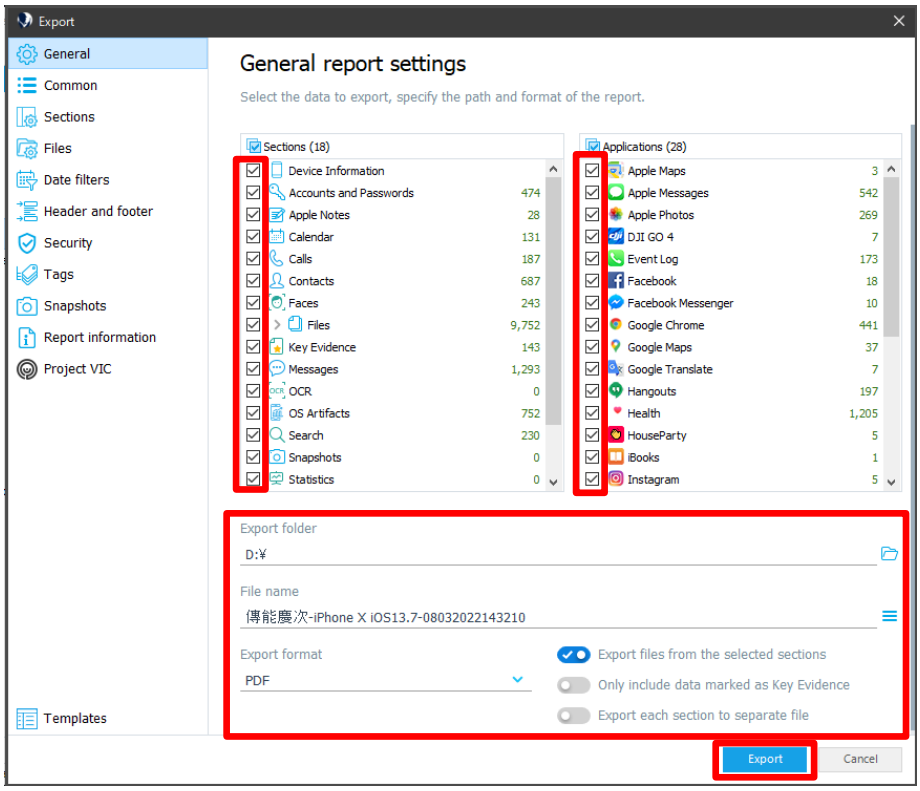
  - ☞ PDF 形式
  - ☞ RTX 形式
  - ☞ XLS – Formatted view 形式
  - ☞ XLS – Table view 形式
  - ☞ XLSX – Table view 2010 形式
  - ☞ HTML –Table view 形式
  - ☞ HTML – Formatted view 形式
  - ☞ XML export 形式
  - ☞ JSON Project VIC 形式

- **レポートの出力方法**

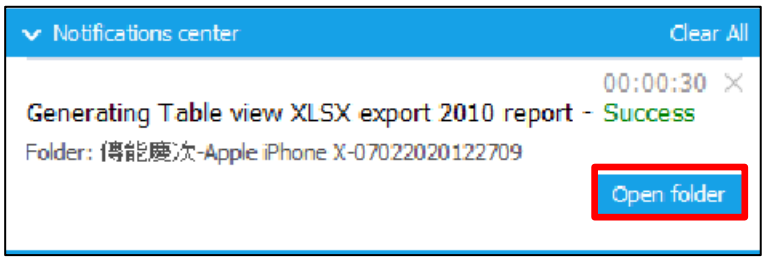
  レポートを出力したいデバイスを選択し、右クリックで出てきたメニューの「Export data」をクリックします。他にもデバイスのアイコンのすぐ下の上矢印のアイコン( )をクリックすると、レポートを出力するためのウィンドウが表示されます。



表示されたウィンドウ上でレポートとして出力したい項目を選択し、ファイル名やファイルの保存場所、出力形式を確認して「Export(エクスポート)」をクリックします。



レポートの出力が完了したら、「Open folder」をクリックすることで、レポートを確認できます。



改訂履歴

版数	発行日	改訂履歴
Ver. 1.0	2015 年 7 月 1 日	初版発行
Ver. 2.0	2016 年 8 月 1 日	第 2 版発行
Ver. 3.0	2018 年 3 月 19 日	第 3 版発行
Ver. 4.0	2020 年 2 月 18 日	第 4 版発行　(v12 対応)
Ver. 5.0	2020 年 10 月 7 日	第 5 版発行
Ver. 6.0	2022 年 3 月 23 日	第 6 版発行　(v14 対応)
Ver. 6.0	2023 年 1 月 23 日	フッターの更新
Ver. 6.1	2023 年 2 月 28 日	位置情報に関する機能の解説を追加
Ver. 7.0	2023 年 4 月 18 日	第 7 版発行(v15 対応) Extractor の UI 変更に対応