CyberDefense

Oxygen Forensic Viewer ガイド

Ver. 1.0

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

目次

1　イントロダクション 1

1.1　このガイドについて 1

1.2　OxyViewer とは 1

2　OxyViewer の入手方法 2

3　起動方法 4

3.1　バックアップファイルの取り込み 4

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

1 イントロダクション

1.1 このガイドについて

本ガイドでは「Oxygen Forensic® Viewer（以降 OxyViewer と記載）」製品の特長や入手方法、起動方法について解説します。

1.2 OxyViewer とは

OxyViewer は、Oxygen Forensic® Detective(以降 Detective と記載)で取得抽出したデバイスデータを他の担当者と共有できるようにするポータブルツールです。

特長として、Detective から作成されたバックアップファイル（OFBX バックアップファイル、または OFBR バックアップファイル）を OxyViewer で閲覧する事が可能です。データの検索や、重要な証拠としてのマーク付け、タグ付けをする事、データをレポートとして出力する事が可能です。また、Detective のライセンスを所持していないユーザでも使用できます。

☛ **機能制限：**

こちらはビューアですので、Detective の様なデバイスデータの抽出機能や解析機能はございません。解析機能(Timeline 機能など)を利用したい場合は、Detective をご検討ください。

☛ **OFBX と OFBR の違い：**

OFBX は対象デバイスの全データなのに対し、OFBR は KeyEvidence などにチェックを入れたものだけが出力されます。

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

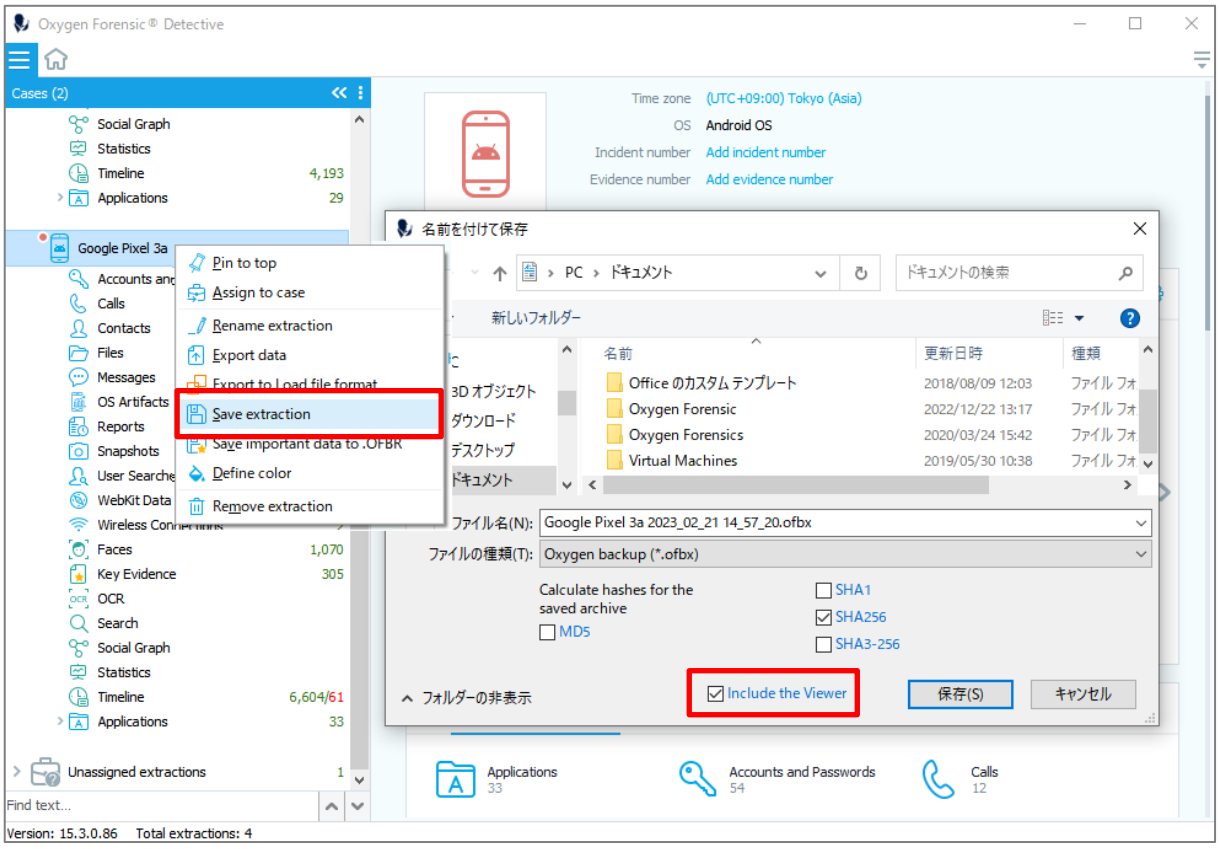
2　OxyViewer の入手方法

OxyViewer の入手方法は複数ありますが、その内 1 つの方法を例として掲示します。

Detective に取り込んだデータを、OFBX バックアップファイルとして保存する際に、「Include the Viewer」にチェックを入れる事で入手する事ができます。

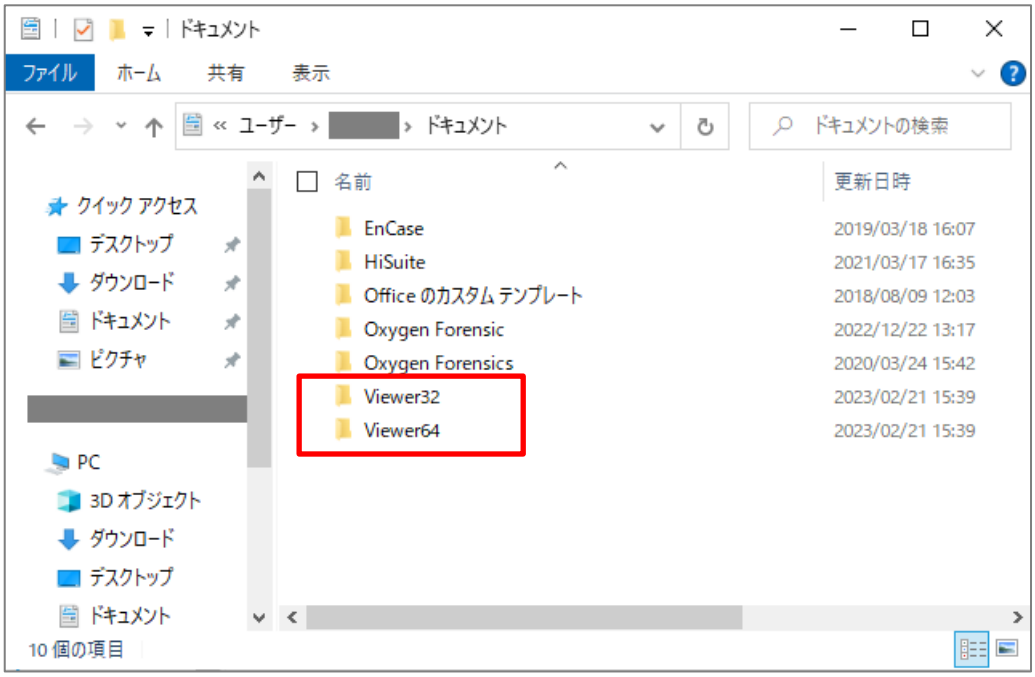
① Detective 上のデバイスデータを選択し右クリック、表示されたメニューから「Save extraction」をクリックします

② 表示されたファイルエクスプローラの下部ある「Include the Viewer」にチェクを入れて「保存」をクリックします

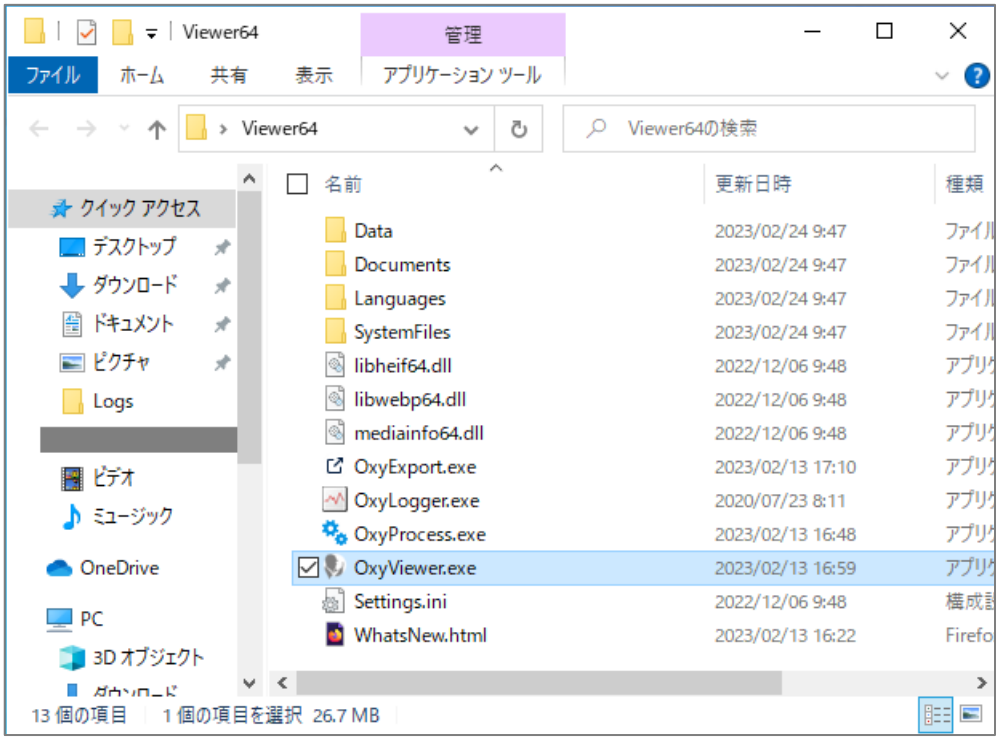


③ 保存先を確認すると「Viewer32」と「Viewer64」のフォルダが作成され、その中に「OxyViewer.exe」実行ファイルが格納されています

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



Viewer64 フォルダ配下は、下図のようになっており、「OxyViewer.exe」実行ファイルがあることが確認できます。



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

3　起動方法

OxyViewer を別の PC に配置する際は、「Viewer32」「Viewer64」フォルダごと移動します。中の実行ファイル「OxyViewer.exe」だけを移動すると起動できませんのでフォルダごと移動するようにお願いします。

☛ **Viewer32 と Viewer64 の違い：**

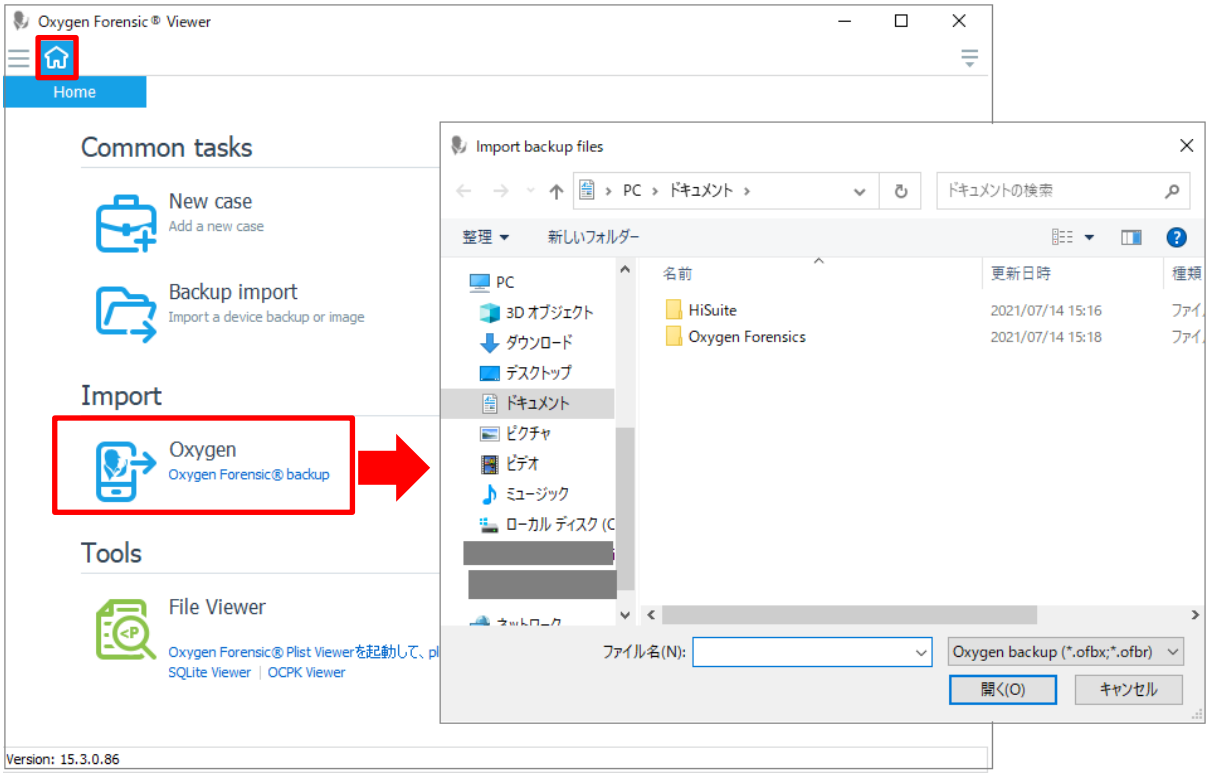
ご使用の Windows OS が 32bit の場合「Viewer32」を、64bit の場合「Viewer64」をご利用ください。

3.1　バックアップファイルの取り込み

① 「Viewer64」フォルダの中の「OxyViewer.exe」を実行します

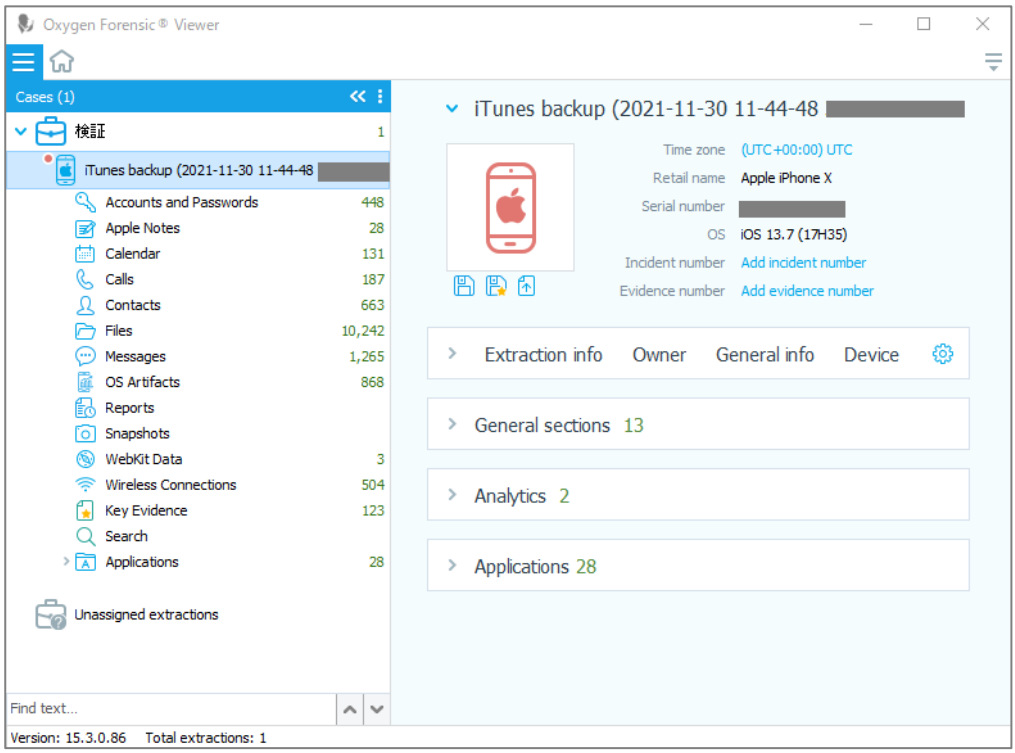
② ホームメニュー「」を開き、「Import」カテゴリの「Oxygen Forensic® backup」をクリックします

③ ファイル選択画面が表示されるので、対象のファイルを指定して「開く」をクリックすることで、バックアップファイルを OxyViewer に取り込むことができます。



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

④ 取込みが完了すると、下図の様に表示されます。



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

改訂履歴

版数	発行日	改訂履歴
Ver. 1.0	2023 年 2 月 27 日	初版発行

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