CyberDefense

解析をはじめる前に

Ver. 1.0

目次

1　解析を始める前に…

ユースケースは、以下の様なシチュエーションの解析方法を参考として公開します。

- デバイス所有者が使用するアカウントを知りたい
- デバイス所有者とあるグループとの繋がりを解明したい
- デバイス所有者の Web 閲覧履歴や検索履歴を知りたい
- 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
- デバイス所有者の行動履歴を知りたい
- デバイス所有者が撮影、収集した画像や動画を検索したい
- 事案に関係するキーワードがスマホに記録されていないか探したい

1.1　解析に使用しているデータについて

解析の説明に使用しているデータの詳細はこちらです。データの提供はございませんがユースケースの資料をご覧いただく際に、どんなデータを使ってどういう風にパースしている等のご参考になれば幸いです。

・ケース名： 2022_Training

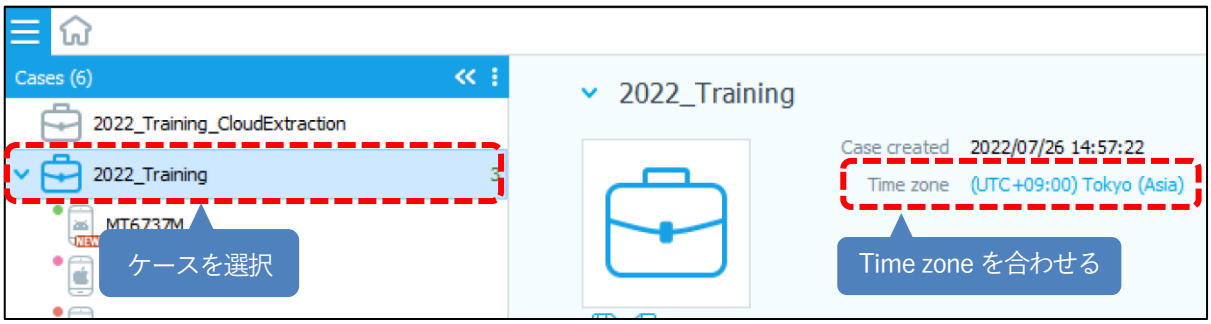
- iPhoneX
  機種名：iPhoneX
  所有者：傳能慶次
  OS：iOS13.7
  Oxygen の抽出方法：「iTunes backup」メニューを使用した論理抽出
- MT6737M
  機種名：Freetel Priori4
  所有者：田無かな
  OS：Android 7.0
  Oxygen の抽出方法：「MTK Android dump」メニューを使用した物理抽出
- Google Pixel 3a
  機種名：Pixel 3a
  所有者：佐井場 攻太
  OS：Android 10.0
  Oxygen の抽出方法：「Android full file system」メニューを使用した論理抽出

1.2 タイムゾーンの設定について

資料内のタイムゾーンは、以下の図の様に設定しています。解析を始める際は、最初にタイムゾーンが一致していることをご確認ください。

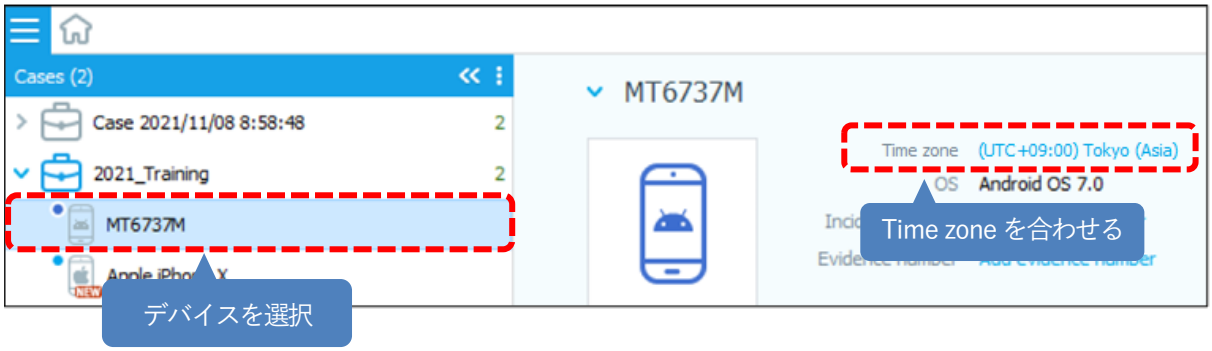
➢ ケースレベル

ケースに対してデータを解析する場合は、ケースを選択して Time zone を設定する必要があります



➢ デバイスレベル

各デバイスデータに対して、Time zone を設定します



改訂履歴

版数	発行日	改訂履歴
Ver. 1.0	2023 年 2 月 28 日	初版発行