Search 機能　解説ガイド

Ver. 1.0

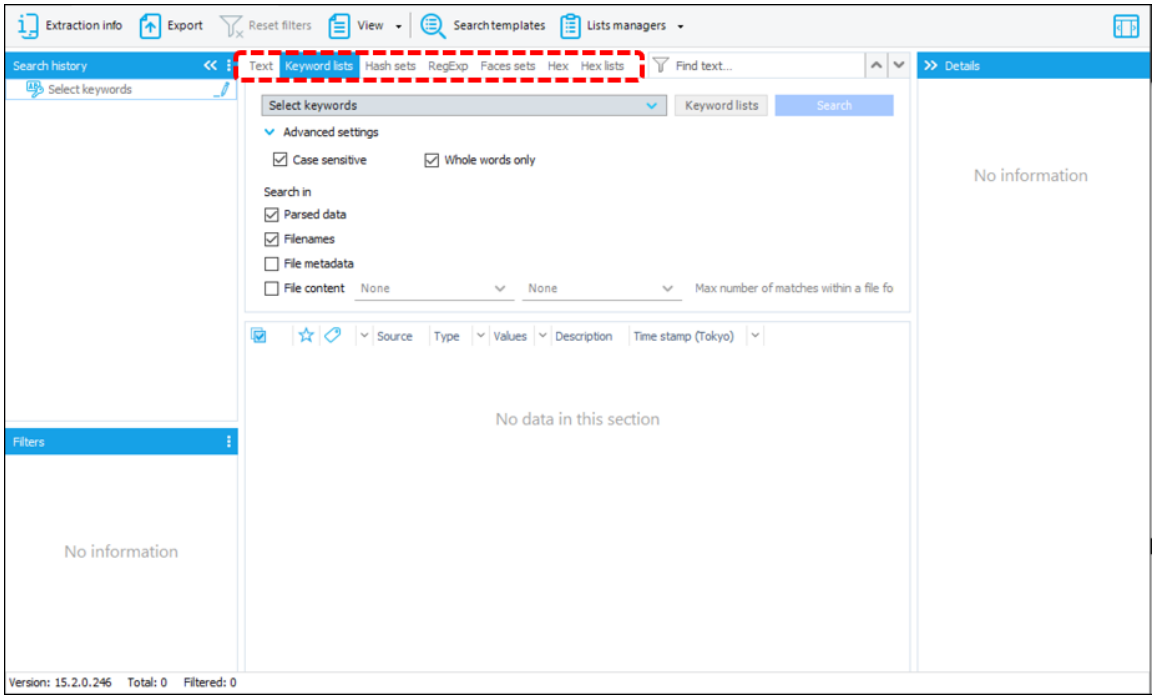
目次

1　Search 機能のカテゴリ

Search セクションでは、デバイス内のあらゆるデータに対して以下の機能を使用した検索が可能です。

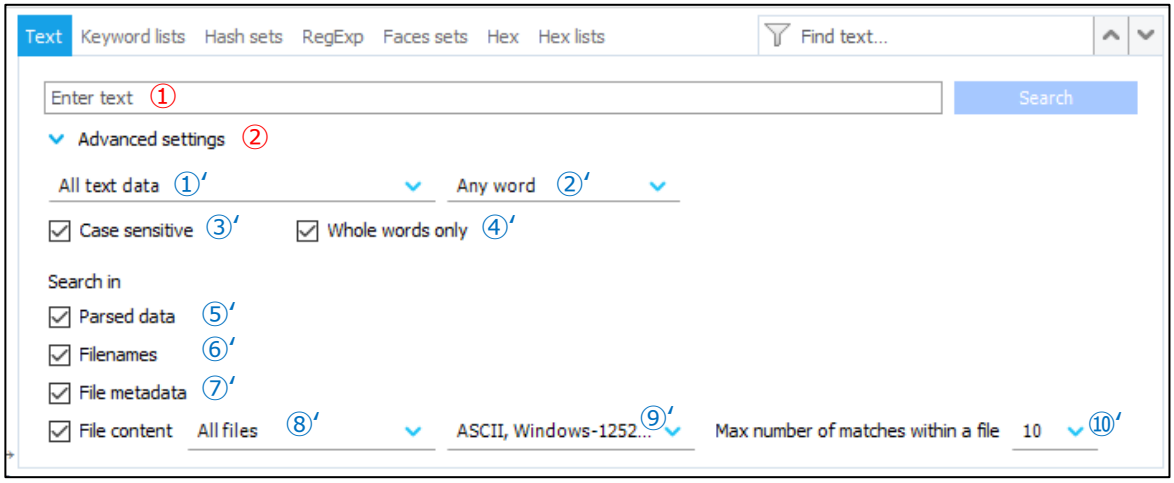
機能名	機能説明
Text	文字検索
Keyword lists	キーワードリストに一致するデータを検索
Hash sets	ハッシュセットに一致するファイルを検索
RegExp	正規表現による検索
Face sets	フェイスセットに一致する顔写真を検索
Hex	16 進数検索
Hex lists	ヘックス(16 進数)リストに一致するデータを検索

上記の機能は、下図の赤枠内のタブを切り替える事で選択可能です。



以降の章では、各機能の詳細を解説します。

2　Text 検索



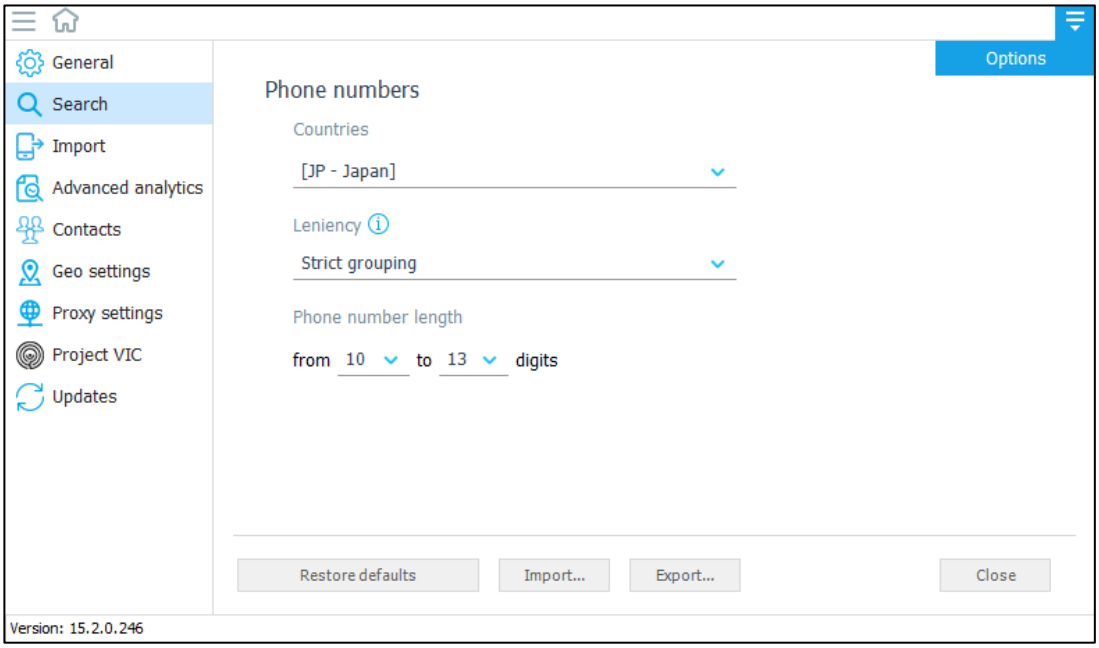
Text 検索タブでは、上図のように①テキスト入力ボックスと②Advanced settings(検索オプション)が用意されています。

Advanced settings では、上図①'～⑩'のオプションを設定することで、検索対象や検索範囲をユーザ自身で調整することが可能です。順番にオプションの詳細を解説していきます。

①'のオプション：クリックすると以下の項目が複数選択可能なチェックボックス形式で展開されます。選択した項目は検索対象に含まれます。

項目名	説明
All Text data	全ての文字列を検索対象にする
Phone number	電話番号を検索対象にする
Emails	メールアドレスを検索対象にする
Credit cards number	クレジットカード番号を検索対象にする
URLs	URL を検索対象にする
IP addresses	IP アドレスを検索対象にする
MAC addresses	MAC アドレスを検索対象にする
Geo coordinates	位置情報を検索対象にする

➤ Phone number については、Oxygen Forensic Detective アプリ上の menu>Options>Search からユーザ自身で電話番号の調整が可能です。



項目名	説明
Countries	検出対象の電話番号の国名を指定
Leniency	電話番号の精度 ➤ Strict grouping（電話番号のように見える数字の羅列） ➤ Exact grouping（電話番号に近い形式の数字の羅列） ➤ Possible（数字の羅列を全て電話番号とみなす） ➤ Valid（電話番号に似た数字の羅列）
Phone number length	電話番号と判定する数字列の長さ

②'のオプション： ①のテキスト入力ボックスに入力したキーワードのマッチタイプを選択出来ます。

項目名	説明
Any words	入力したキーワードのいずれか
All words	入力したキーワード全て
Exact Phrase	フレーズの完全一致

③'のオプション： Case sensitive にチェックを入れると、検索対象の文字列に対して大文字と小文字を区別するようになります。

④'のオプション： Whole words only にチェックを入れると、単語単位で検索するようになります。

⑤'のオプション： Parsed data にチェックを入れると、パース済みのデータを検索対象に含めます。

⑥'のオプション： Filenames にチェックを入れると、ファイル名も検索対象に含めます。

⑦'のオプション： File metadata にチェックを入れると、ファイルのメタデータも検索対象に含めます。

⑧'のオプション： クリックすると以下の項目が複数選択可能なチェックボックス形式で展開されます。選択した項目は検索対象に含まれます。

項目名	説明
All files	全ファイルを検索対象にする
Media files	メディアファイルを検索対象に含める
Images(OCR)	画像内の文字（OCR の書き起こし結果）を検索対象に含める
Databases	データベースを検索対象に含める
Documents	ドキュメントを検索対象に含める
Plist files	Plist ファイルを検索対象に含める
JSON files	JSON ファイルを検索対象に含める
Archives	アーカイブを検索対象に含める
Applications files	アプリケーションファイルを検索対象に含める
Other files	その他のファイルを検索対象に含める

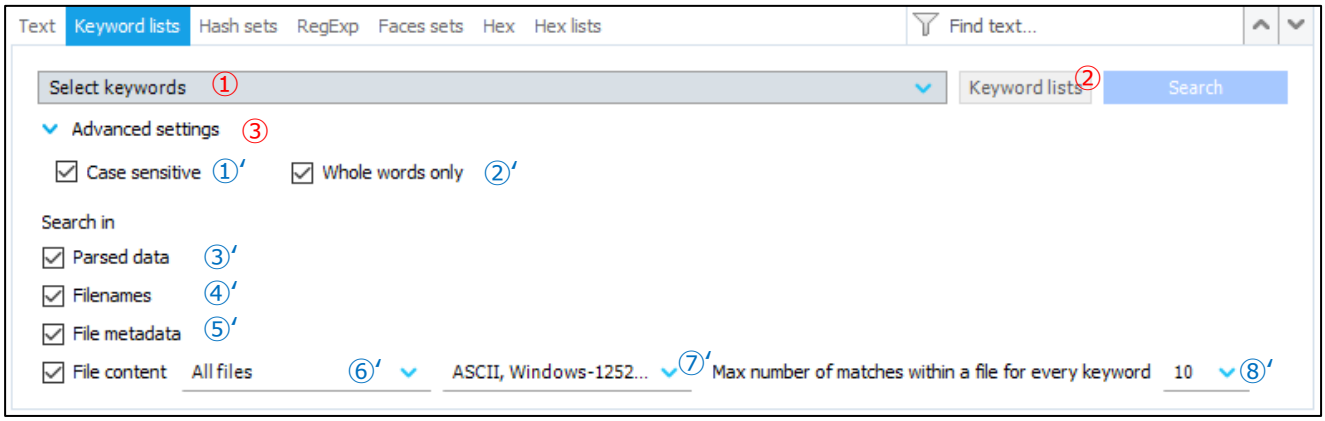
⑨'のオプション：クリックすると以下の項目が複数選択可能なチェックボックス形式で展開されます。選択した項目は検索対象に含まれます。

項目名
ASCII
Windows-1252
UTF-8
UTF-16LE
UTF-16BE
UTF-32LE
UTF-32BE

⑩'のオプション： ファイル内の最大一致数を 5~50 の間で選択可能。ただし、最大一致数までマッチを見るだけで、設定した数より多くワードが含まれていても一致とみなされる。

3 Keyword lists 検索

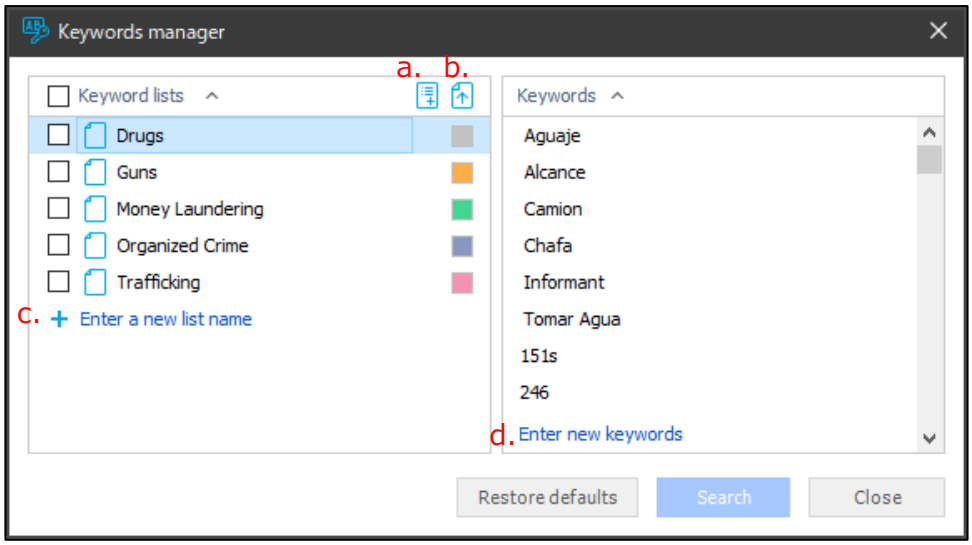
Keyword lists 検索タブでは、リストに登録済みのキーワードを一括検索することが可能です。



Keyword lists 検索タブでは、上図のように①Keyword list 選択フォームと②Keywords manager 展開ボタン、そして③Advanced settings(検索オプション)が用意されています。

Advanced settings では、上図①'～⑧'のオプションを設定することで、検索対象や検索範囲をユーザ自身で調整することが可能です。オプションメニューの解説は Text 検索機能タブと同様のため省略します。

②の Keywords manager 展開ボタンをクリックすると、下図の画面が展開されます。



a. Keyword list のインポート

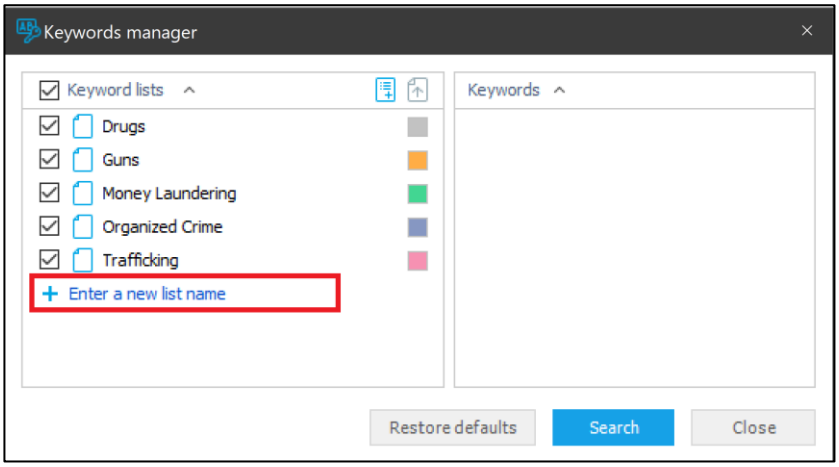
b. Keyword list のエクスポート

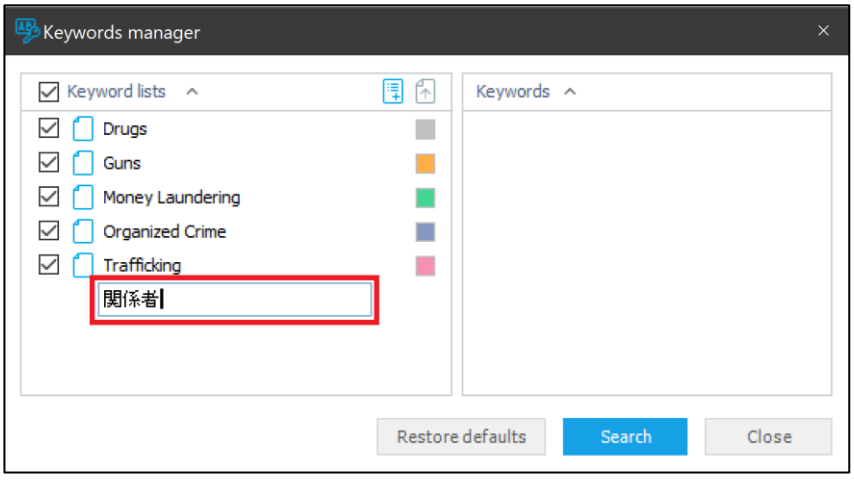
c. Keyword list の新規作成

d. Keyword list にキーワードを新規登録

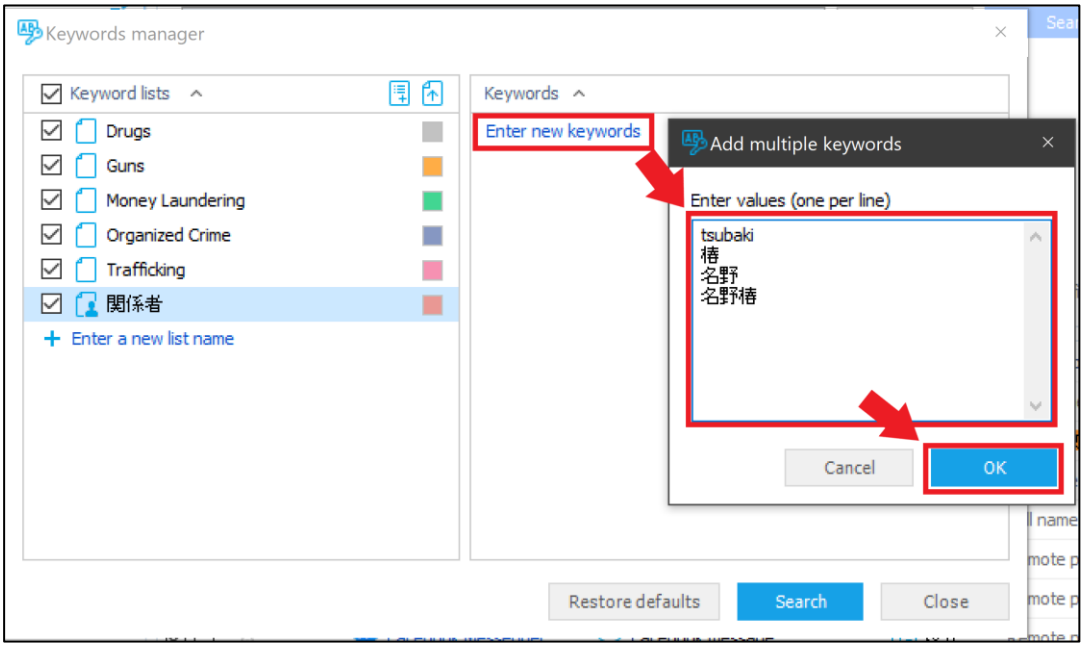
3-1. Keyword lists の追加方法

1. Keywords manager を開く
2. [+Enter a new list name]をクリックして、任意のリスト名を入力する

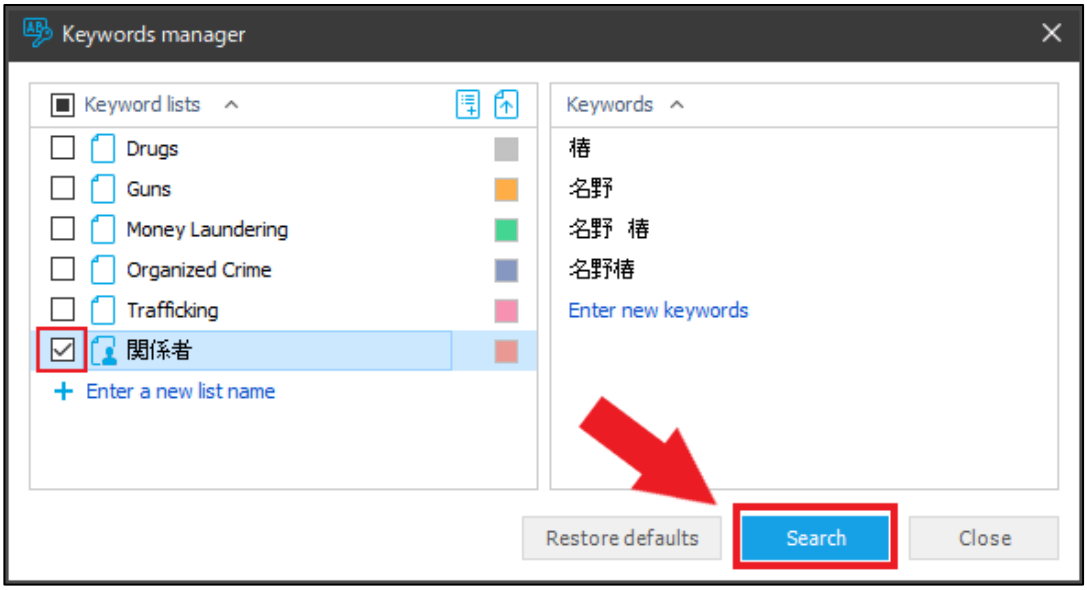




3. [Enter new keywords]をクリックし、キーワードを登録する。複数登録する場合は、改行で区切る。

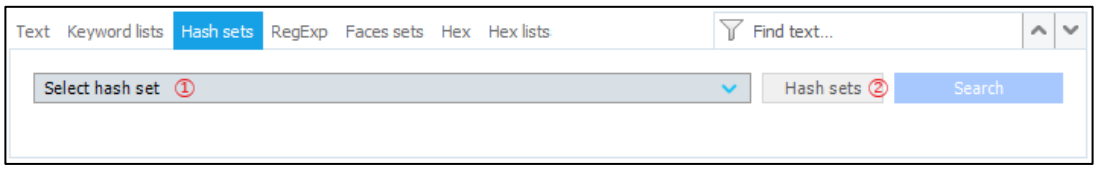


4. このまま検索する場合は、検索対象にしたいリストにだけチェックを入れて[Search]をクリックする



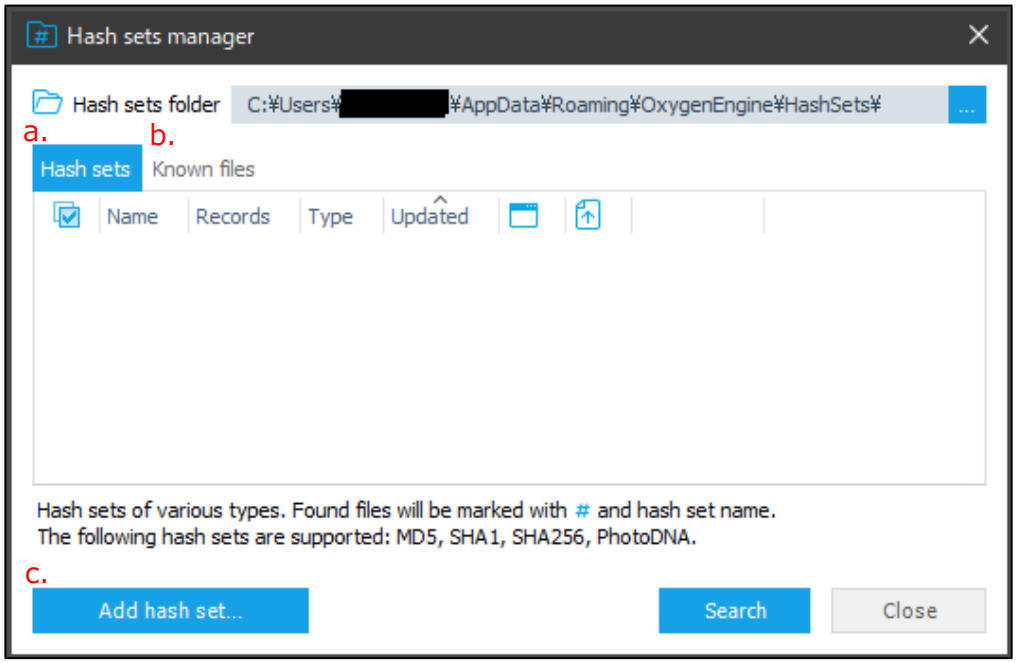
4 Hash sets 検索

Hash sets 検索タブでは、リストに登録済みの Hash sets を検索することが可能です。



Hash sets 検索タブでは、上図のように①hash set 選択フォームと②Hash sets manager 画面展開ボタンが用意されています。

②の Hash sets manager 展開ボタンをクリックすると、下図の画面が展開されます。



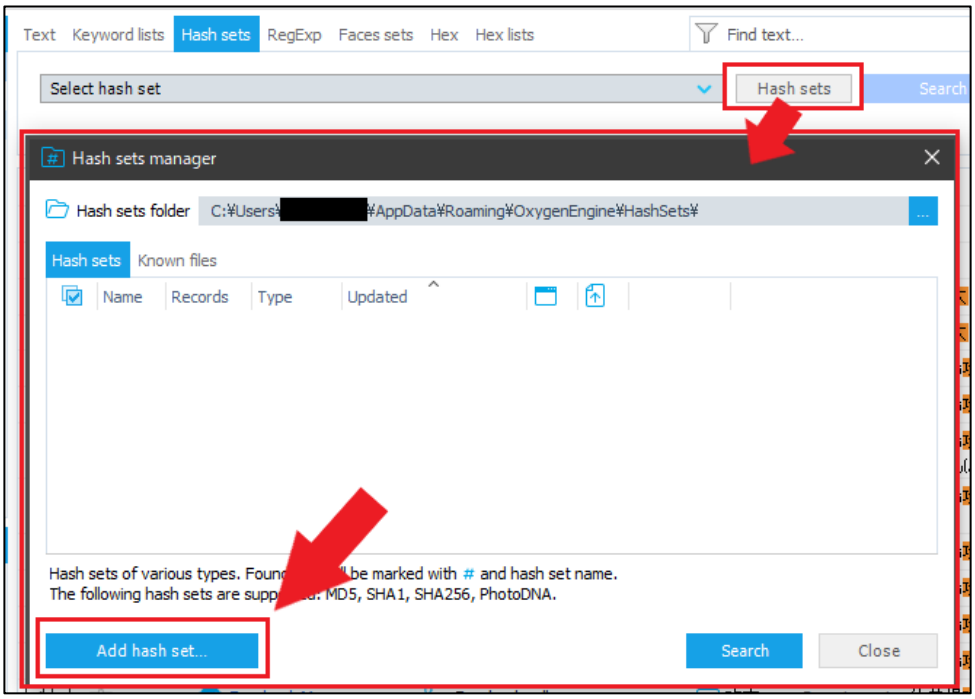
a. Hash sets タブ: 追加した Hash sets が表示されます

b. Known files タブ: iOS デバイスと Android デバイスの system file の Hash set がデフォルトで用意されています。これを検索時に除外することで、検索結果からユーザ固有でない system file データを除外することが可能になります.

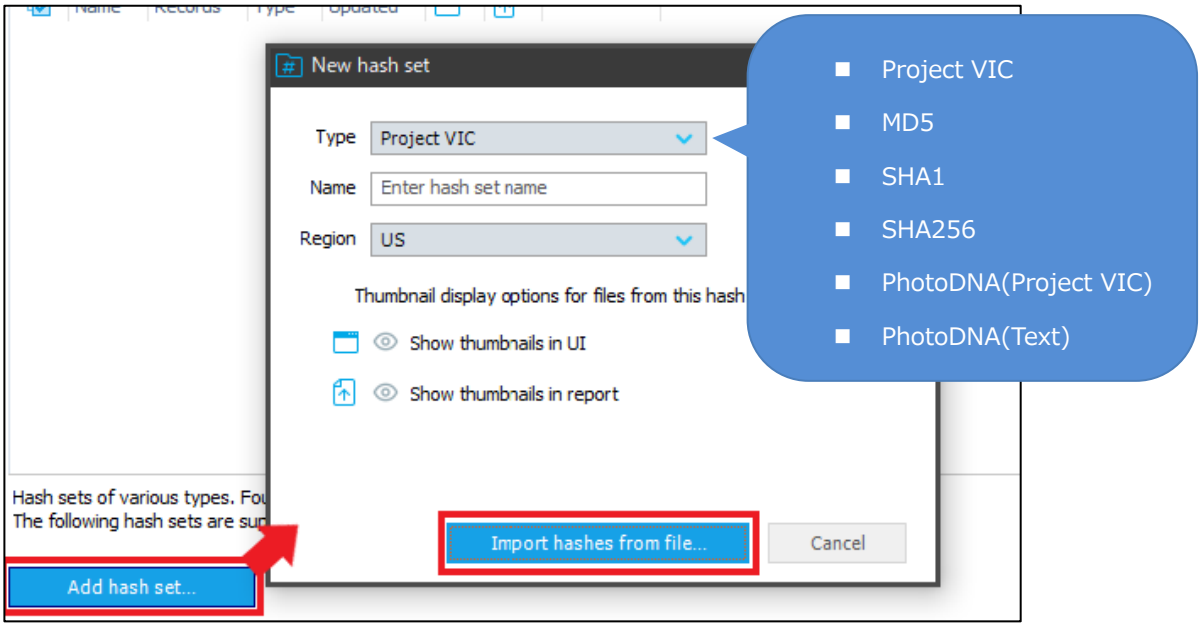
c. Hash set ファイルのインポート

4-1. Hash sets の追加方法

1. Hash sets manager 展開ボタンをクリックして、Hash sets manager を開く
2. [Add hash set…]をクリックする

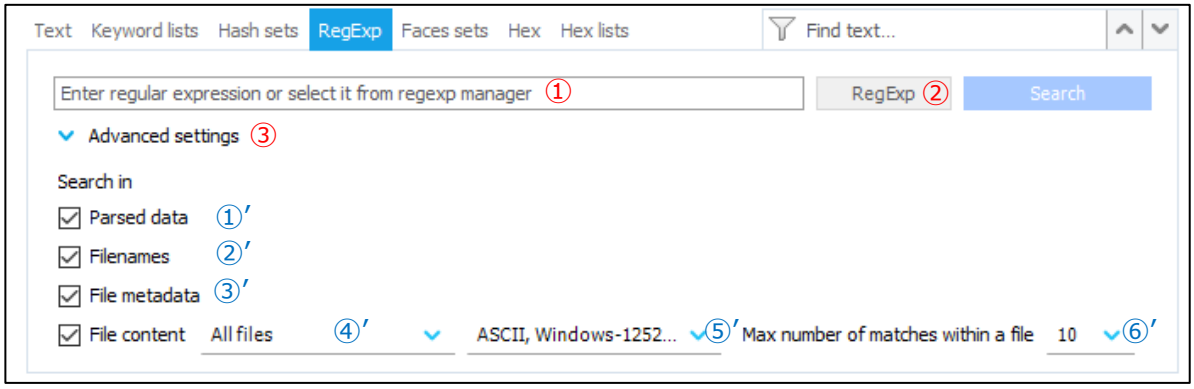


3. New hash set 画面が展開されるので、[Import hashes from file…]をクリックして Hash set ファイルをインポートする



5 RegExp 検索

RegExp 検索タブでは、入力フォームに直接入力、もしくはリストに登録した正規表現を使用して検索することが可能です。

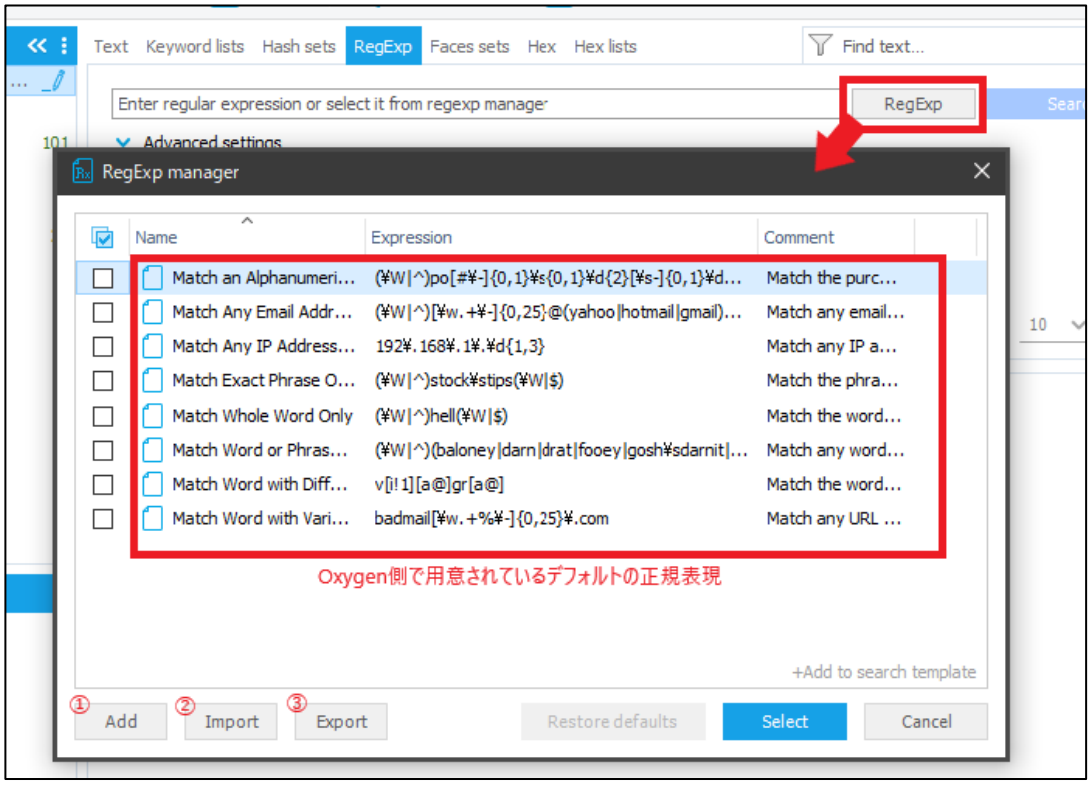


RegExp 検索タブでは、上図のように①正規表現(Regular expression)入力フォームと②RegExp manager 画面展開ボタン、そして③Advanced settings(検索オプション)が用意されています。

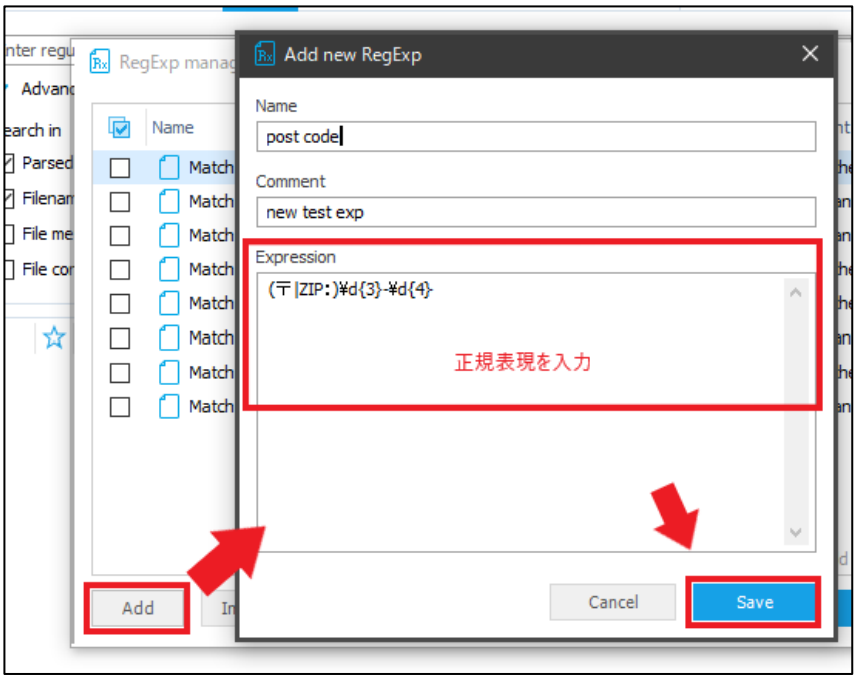
Advanced settings では、上図①′～⑥′のオプションを設定することで、検索対象や検索範囲をユーザ自身で調整することが可能です。オプションメニューの解説は Text 検索機能タブと同様のため省略します。

5-1. RegExp の登録の仕方

[RegExp]をクリックし、RegExp manager を展開します

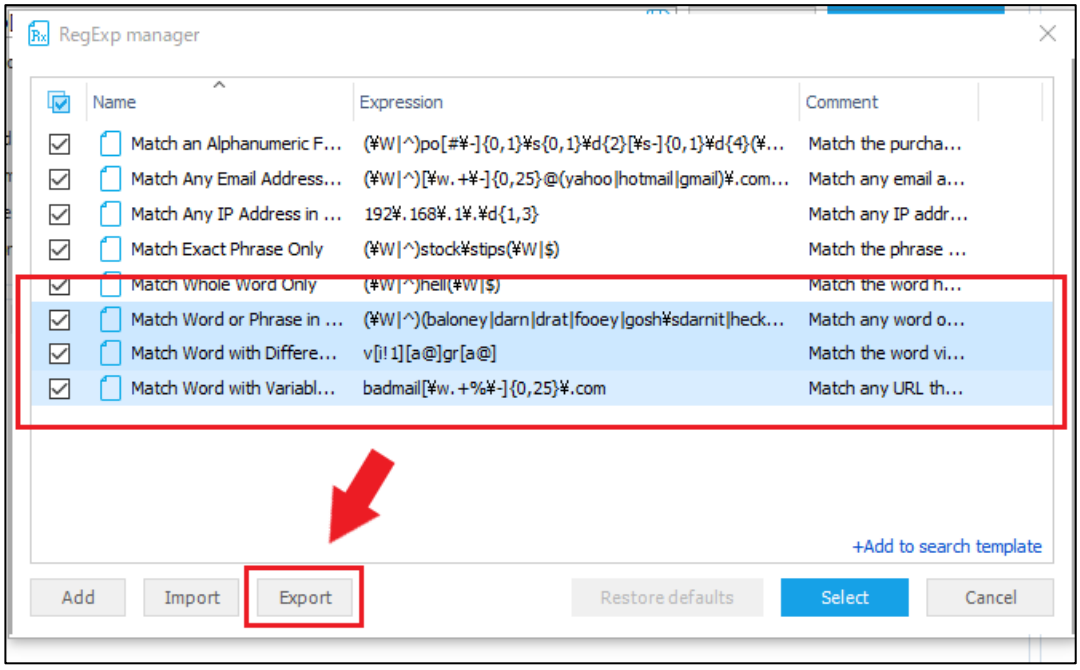


①Add： 正規表現を入力して保存したい場合は、[Add]をクリックして Add new RegExp 画面を展開し、登録したい正規表現を入力して[Save]をクリック



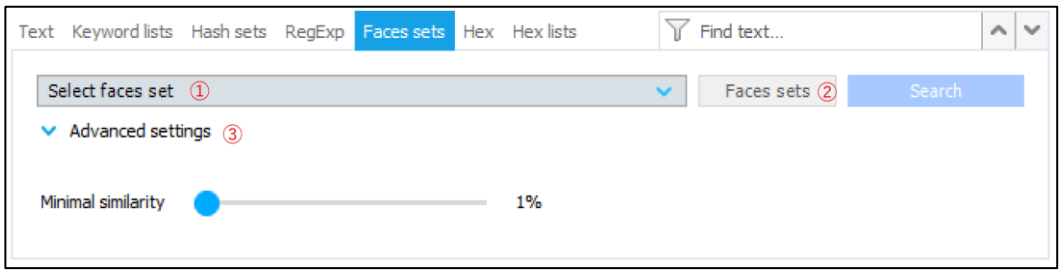
②Import: 正規表現を記述したファイルをインポートしたい場合は、[Import]をクリックしてファイルを選択

③Export: ファイルとして出力したい正規表現リストを選択し(選択したアイテムは背景が青になります)、
[Export]をクリックする。出力は CSV か text 形式が選択可能



6 Faces sets 検索

Faces sets 検索タブでは、リストに登録済みの顔写真を一括検索することが可能です。

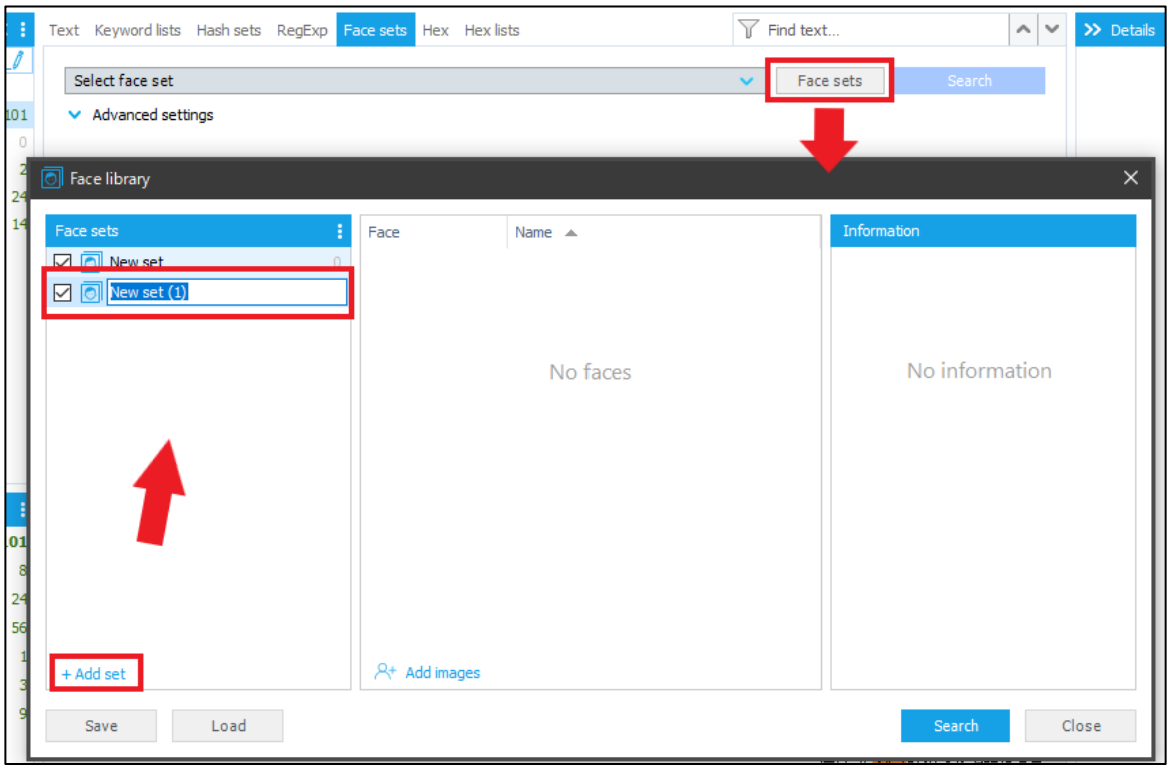


Faces sets 検索タブでは、上図のように①faces set 選択フォームと②Face library 画面展開ボタン、そして③Advanced settings(検索オプション)が用意されています。

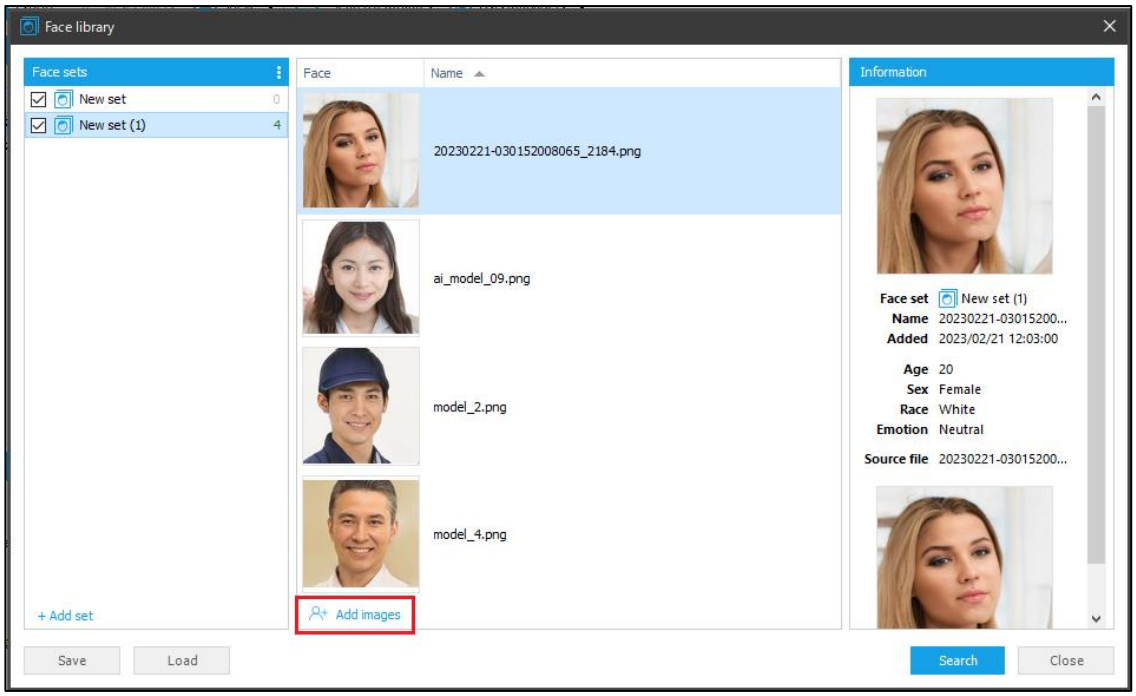
Advanced settings 内の Minimal similarity では、検索対象の顔写真との類似度(%)を調整する事が可能です。

6-1. Face library の追加方法

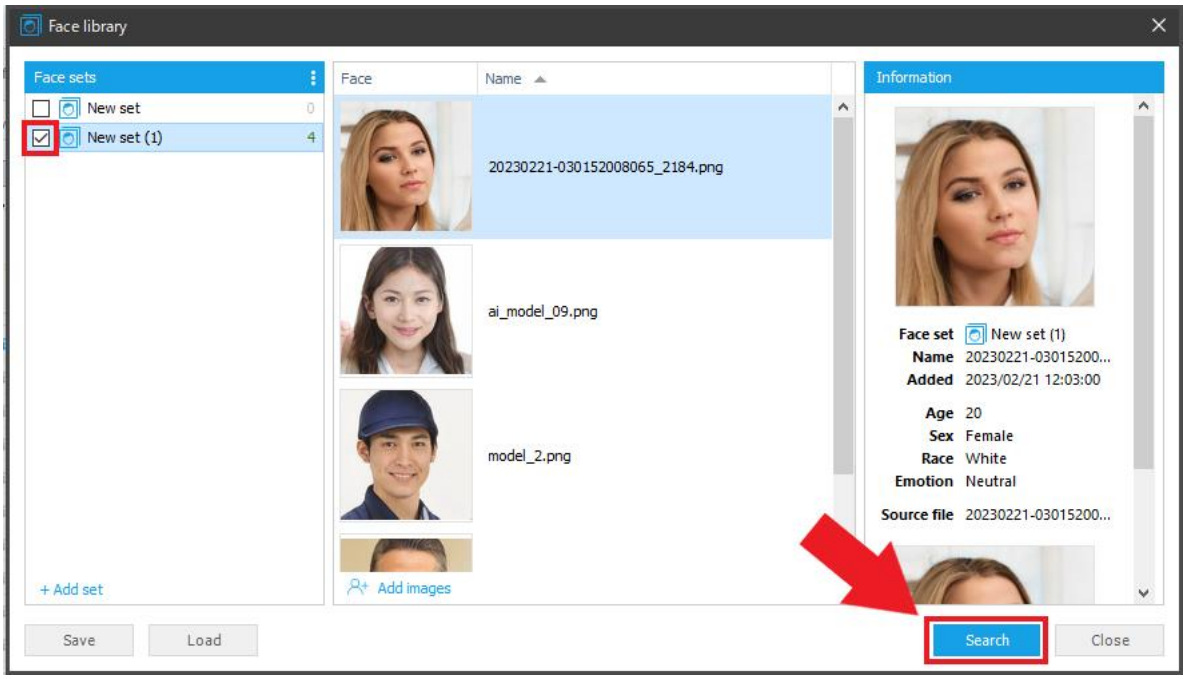
1. [Face sets]をクリックし、Face library を展開する
2. [+Add set]をクリックし、任意のリスト名を追加する



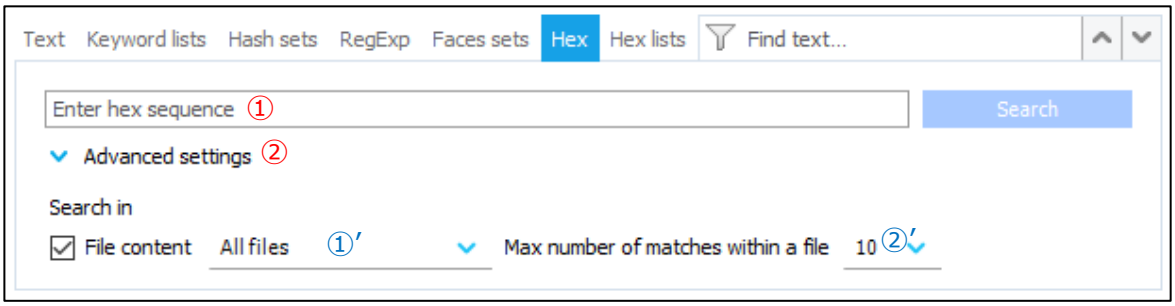
3. [Add images]をクリックして顔写真を追加する



4. このまま検索する場合は、検索対象にしたいリストのみにチェックを入れて[Search]をクリックする



7 Hex 検索

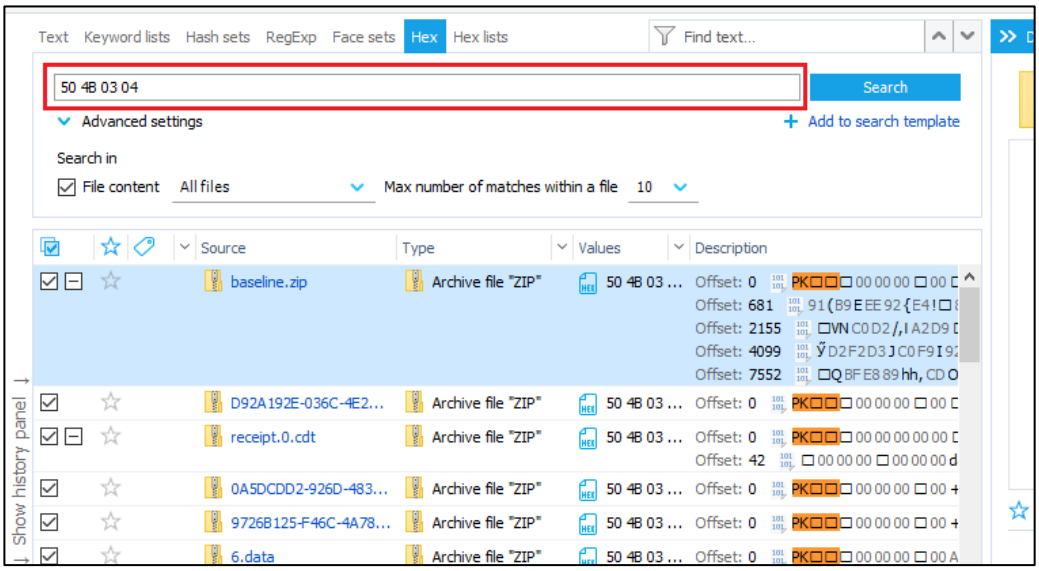


Hex 検索タブでは、上図のように①Hex(16 進数)入力フォームと②Advanced settings(検索オプション)が用意されています。

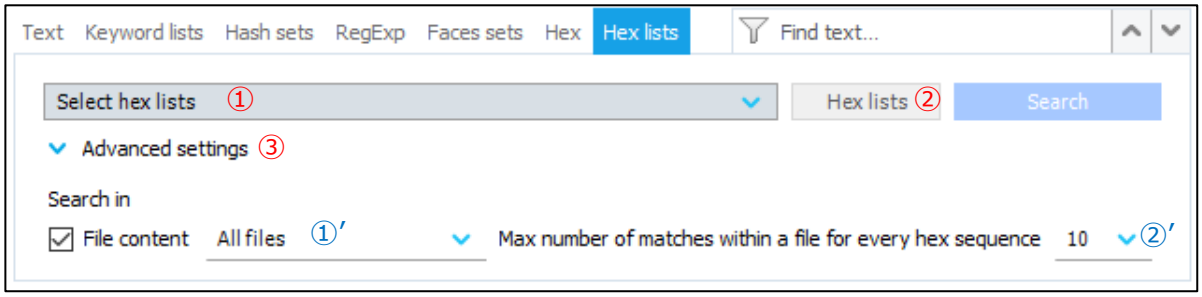
Advanced settings では、上図①′～②′のオプションを設定することで、検索対象や検索範囲をユーザ自身で調整することが可能です。オプションメニューの解説は Text 検索機能タブと同様のため省略します。

入力フォームに Hex(16 進数)を入力する際は、下図のように記述します。

下図は、例として ZIP ファイルのシグネチャ「50 4B 03 04」を検索したものです。



8 Hex lists 検索

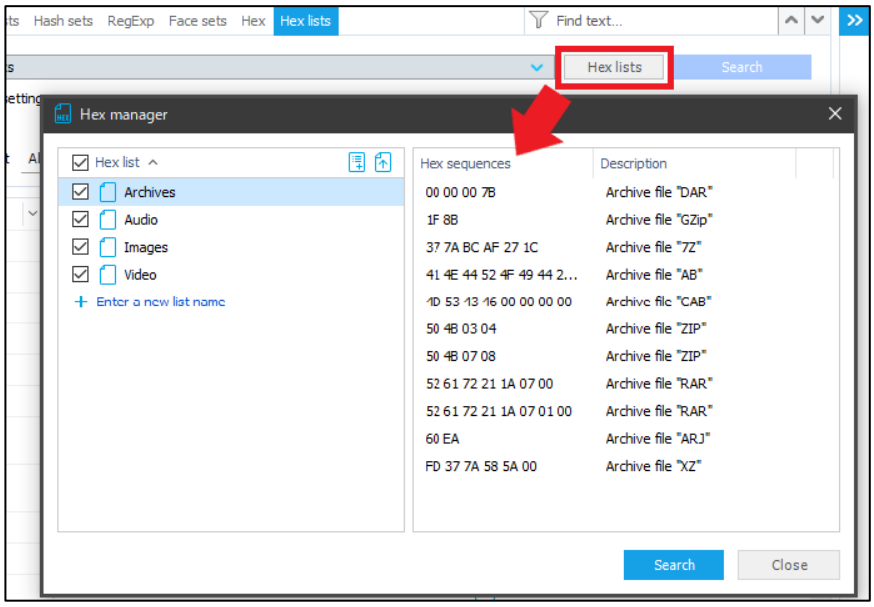


Hex lists 検索タブでは、上図のように①Hex lists 選択フォームと②Hex lists 編集画面展開ボタン、そして③Advanced settings(検索オプション)が用意されています。

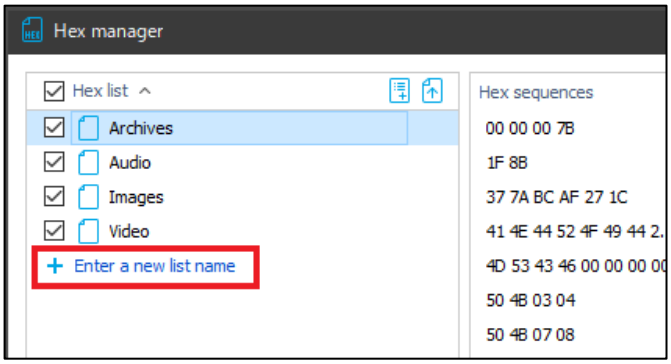
Advanced settings では、上図①′～②′のオプションを設定することで、検索対象や検索範囲をユーザ自身で調整することが可能です。オプションメニューの解説は Text 検索機能タブと同様のため省略します。

8-1. Hex lists の追加

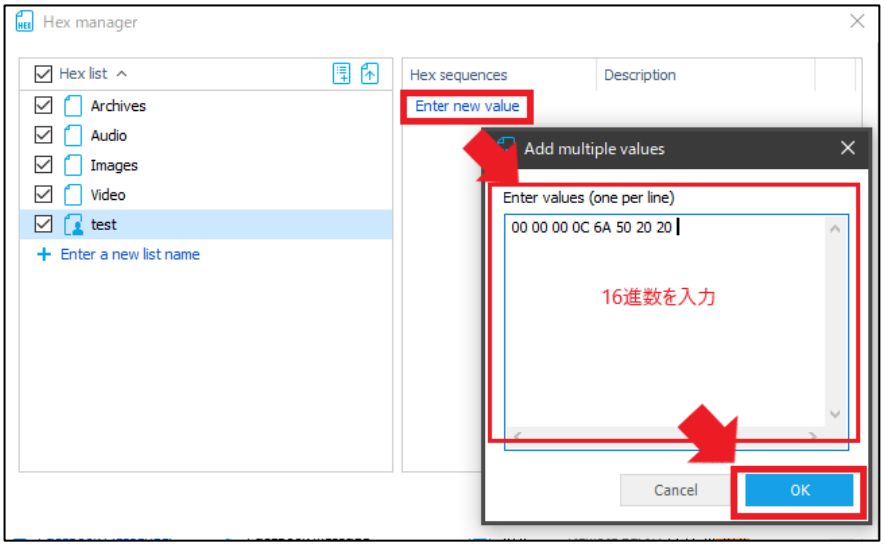
1. [Hex lists]ボタンをクリックして、Hex manager を展開する



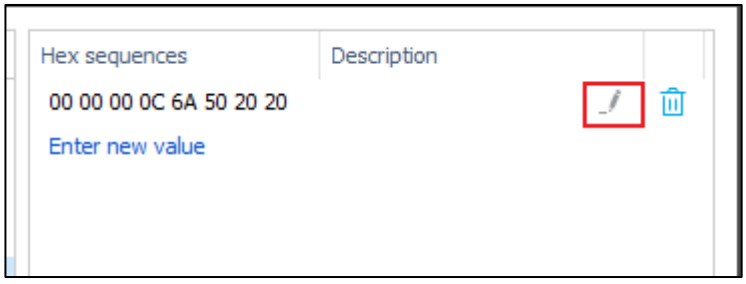
2. [+Enter a new list name]をクリックして、任意のリスト名を入力する

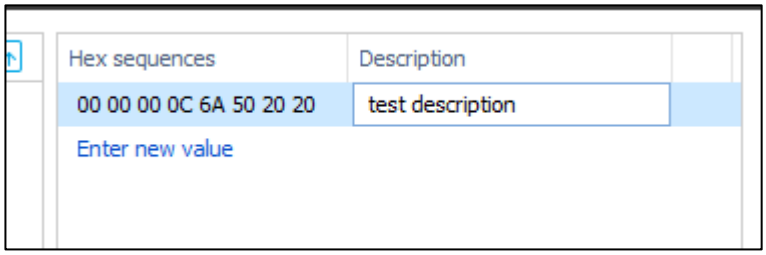


3. [Enter new value]をクリックして、Add multiple values を展開する
4. 入力フォームに 16 進数を入力して、OK ボタンをクリックする

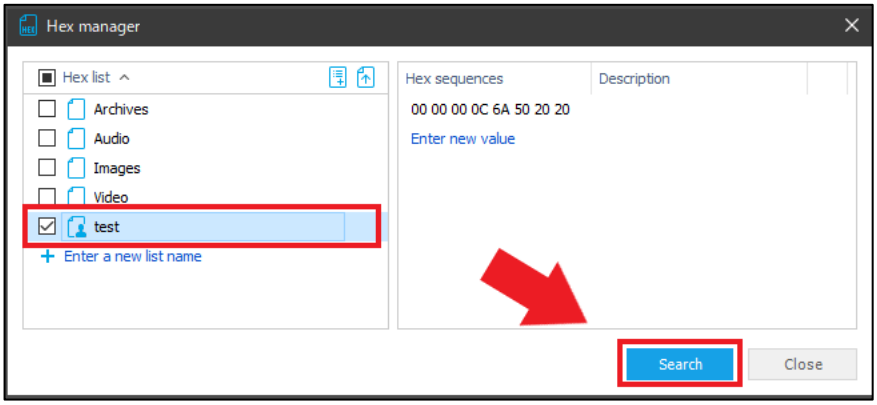


5. マウスを当てるとペンアイコンが表示されます。ペンアイコンをクリックすると、Description(説明)を入力するフォームが表示されます





6. このまま検索する場合は、検索対象にしたいリストのみにチェックを入れて[Search]をクリックする



改訂履歴

版数	発行日	改訂履歴
Ver. 1.0	2023 年 02 月 27 日	初版発行