X-Ways Forensics

トレーニングで紹介していないオプション

（対応バージョン 19.8）

Copyright©2019 dit Co., Ltd. All rights reserved.

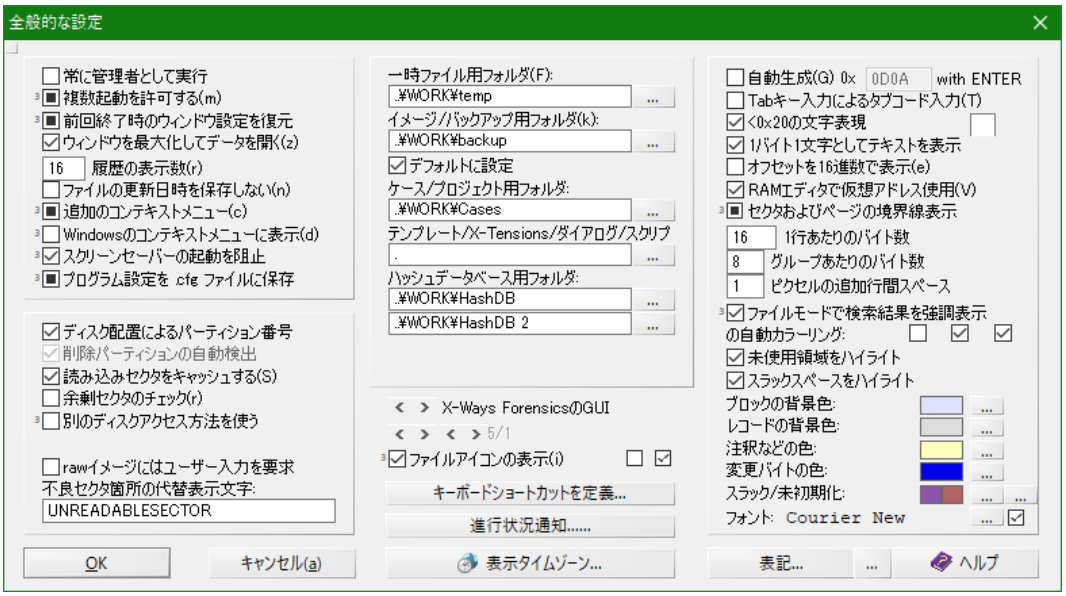
目次

Copyright©2019 dit Co., Ltd. All rights reserved.

Copyright©2019 dit Co., Ltd. All rights reserved.

1. 構成オプション

1.1. 全般的な設定



オプション	説明	推奨設定
常に管理者として実行	“管理者として実行”を指定して起動しなくても、管理者として実行される	☑
複数起動を許可する	☑：X-Ways が起動する ■：起動メニューを表示	■
起動時にクイックスタートを表示する	☑：クイックスタートメニューを表示	■
前回終了時のウィンドウ設定を復元（■時のみ）	■：前回終了時に開かれたケースやウィンドウの状態を復元して起動する	■
ウィンドウを最大化してデータを開く	(不明)チェック状態で変化なし	(任意)
履歴の表示数	[ファイル]メニューに表示される履歴の数	(任意)
ファイルの更新日時を保存しない	WinHex で開いたファイルを保存あるいは名前を付けて保存する際に、ファイルの更新日時を保存しない	☐
追加のコンテキストメニュー	☑：ケースウィンドウのディレクトリを右クリック時にコンテキストメニューを表示 ■：再帰的表示のオン/オフ [Shift]キーを押しながら右クリックでコンテキストメニューを表示	■
Windows のコンテキストメニューに表示	☑：Windows のコンテキストメニューに”Open in X-Ways Forensics”を表示（ディスク/フォルダ/ファイルに適用） ■：ディスク/フォルダに対してのみ適用	(任意)
スクリーンセーバーの起動を阻止	☑：常に起動を防止 ■：進捗バーが表示されているときのみ防止	☑
プログラム設定を.cfg ファイルに保存	☑：終了時に設定を保存 ■：ダイヤログで”OK”選択時に設定を保存	■

Copyright©2019 dit Co., Ltd. All rights reserved.

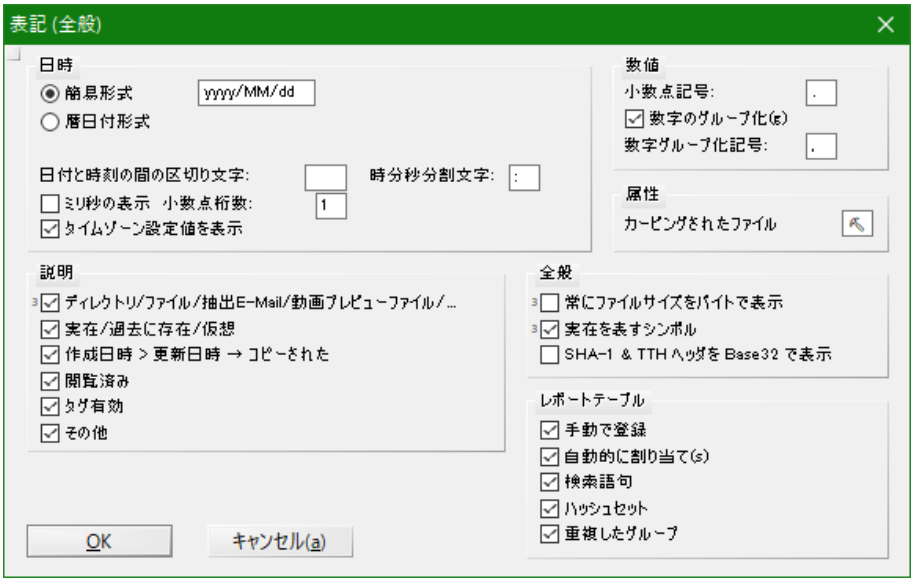
オプション	説明	推奨設定
ディスク配置によるパーティション番号	ディスクの物理的な配置によりパーティションに番号を振る	☑
削除パーティションの自動検出	常時☑(変更不可)	☑
読み込みセクタをキャッシュする	ディスクエディタによる連続的なディスクアクセスを高速化する(WinHex)	☑
余剰セクタをチェック	クラスタとして割り当てができない終端のセクタをチェックする	(任意)
別のディスクアクセス方法を使う	通常とは異なるセクタサイズでフォーマットされているハードディスクやその他のメディアへのアクセスを可能にする	☐
raw イメージにはユーザー入力を要求	raw イメージを追加する場合、常にイメージの種類、想定するセクタサイズ、続きのイメージファイルの置かれているパスを確認する	☐
不良セクタ箇所の代替表示文字	不良セクタ箇所に任意の文字を挿入	(デフォルト)
一時ファイル用フォルダ	解析時に作成される一時ファイルの保存先	(必須)
イメージ/バックアップ用フォルダ	イメージおよびバックアップファイル(.whx)のデフォルトの保存先	(必須)
ケース/プロジェクト用フォルダ	ケースの情報の保存先	(必須)
テンプレート、X-Tensions、ダイアログ、スクリプト	各種設定の保存先 通常".."のままで使用	(デフォルト)
ハッシュデータベース用フォルダ	内部ハッシュデータベースと PhotoDNA ハッシュデータベースの保存先	(デフォルト)
X-Ways Forensics の GUI	GUI のデザインの変更	(デフォルト)
ファイルアイコンの表示	ファイルに格納されているアイコンを表示	☑
Large icons	メニューアイコンを大きくする	☐
Alternative file selection dialog windows	(不明)	☑
自動生成	エディタ画面上で Enter キーを 押した際に指定した 16 進値を自動で入力(WinHex)	☐
Tab キー入力によるタブコード入力	Tab キーでモードの切り替え(hex⇔dec) (WindHEX)	☐
<0x20 の文字表現	0x00～0x19 の制御コードの文字表現を指定の文字で置き換えて表示	☑
1 バイト 1 文字としてテキストを表示	このオプションが無効な場合、Windows のアクティブコードページが 2 バイト文字セットの時、2 バイト 1 文字が適切なテキストは対応したテキストを表示	☑
オフセットを 16 進数で表示	バイナリ表示画面のオフセットを 16 進数で表示する(オプション無効の場合は 10 進数)	☐
RAM エディタで仮想アドレス使用	RAM エディタ利用時に基準としたオフセットではなく仮想アドレスを表示	☑
セクタおよびページの境界線表示	☑：セクタとページの境界線に線を表示 ■：セクタの境界線に線を表示	■
1 行あたりのバイト数	バイナリ表示で 1 行に表示するバイト数	16
グループあたりのバイト数	1 行内で指定バイトごとにスペースで区切る	8
ピクセルの追加行間スペース	行間のスペースのピクセル数	1

Copyright©2019 dit Co., Ltd. All rights reserved.

オプション	説明	推奨設定
ファイルモードで検索結果を強調表示の自動カラーリング	☑：常に表示 ■：検索結果リストが表示されているとき サブオプション(左から) FILE レコード FILETIME 編集	☑ サブオプション すべて☑
未使用領域をハイライト	空き領域/スラック領域を薄い色で表示 FAT, NTFS, Ext2/3 で有効	☑
スラック領域をハイライト		
ブロックの背景色	任意の色に指定	(任意)
レコードの背景色		
注釈などの色		
変更バイトの色		
スラック/未初期化		
フォント	バイナリ表示のフォントおよびサイズを指定	(任意)
サブオプション(フォントの右のチェックボックス)	GUI の他の部分で、標準の Windows GUI フォントを使用	☑

Copyright©2019 dit Co., Ltd. All rights reserved.

1.1.1. 表記

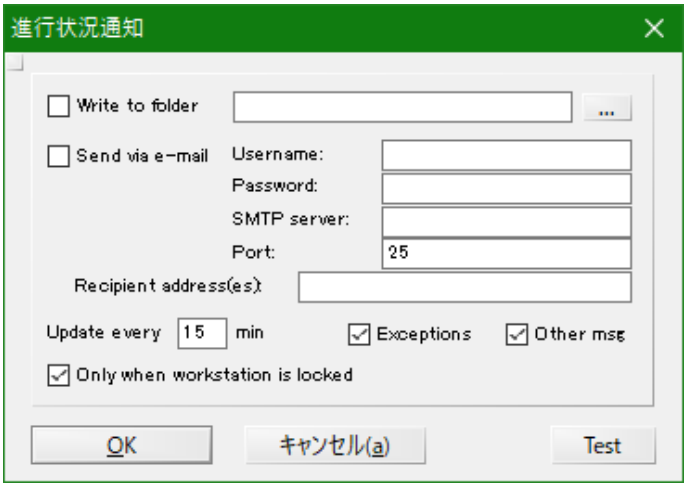


オプション	説明	推奨設定
簡易形式	“yyyy/MM/dd”等の表記	◉
暦日付形式	“yyyy‘年’M‘月’d‘日’”等の表記	○
日付と時刻の間の区切り文字	日付と時刻の間の区切り文字	スペース 2 つ
時分秒の分割文字	時、分、秒の分割文字	:
ミリ秒の表示 小数点桁数	ミリ秒以下の桁数	1
タイムゾーン設定値表示	タイムスタンプの後ろに”+9”等のタイムゾーン設定値を表示	☑
小数点記号	小数点の表示文字	.
数字のグループ化	(不明)	☑
数字グループ化記号	(不明)	,
カービングされたファイル	カービングされたファイルの表示文字	(デフォルト)
ディレクトリ/ファイル/抽出 E-Mail メッセージ/動画プレビューファイル	☑：“説明”カラムに左記内容を表示 ■：不明	☑
実在/過去に存在/仮想	“説明”カラムに左記内容を表示	☑
作成日時 > 更新日時 → コピーされた	“説明”カラムに左記内容を表示	☑
閲覧済み	“説明”カラムに左記内容を表示	☑
タグ有効	“説明”カラムに左記内容を表示	☑
その他	“説明”カラムに上記以外の説明を表示	☑
常にファイルサイズをバイトで表示	☑：常にバイト表示 ■：ボリューム内のアイテムのみ常にバイト表示	☐
実在を表すシンボル	(不明)	(任意)
SHA-1 & TTH ヘッダを Base32 で表示	ディレクトリブラウザで SHA- 1 および TTH192 のハッシュを Base32 表記で表示	(任意)
手動入力	(不明)	(任意)
自動的に割り当て	(不明)	(任意)

Copyright©2019 dit Co., Ltd. All rights reserved.

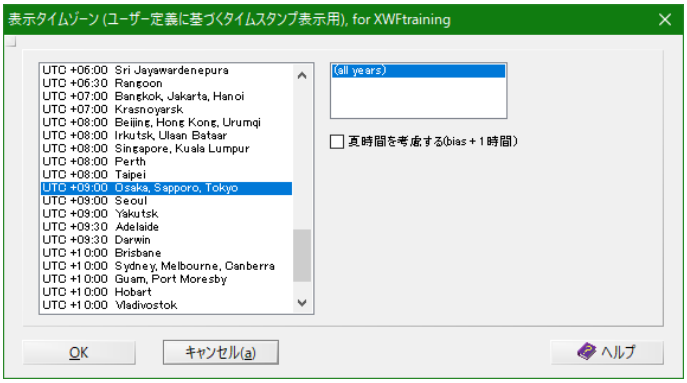
オプション	説明	推奨設定
検索語句	(不明)	(任意)
ハッシュセット	(不明)	(任意)
重複したグループ	(不明)	(任意)

1.1.2. 進行状況通知



解析の進行状況をファイル出力/メールで通知します。

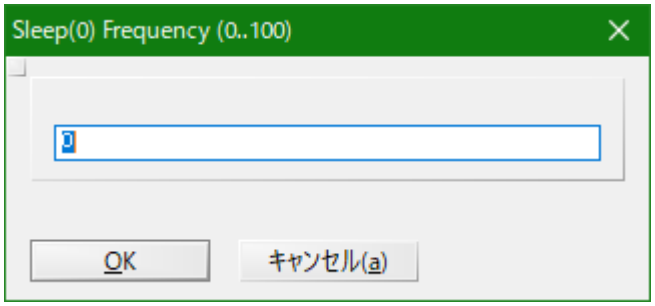
1.1.3. 表示タイムゾーン



X-Ways Forensics は、UTC タイムスタンプをディレクトリブラウザの表示、レポートテーブル、リストのエクスポートで使用する任意のタイムゾーンに変換するために、Windows の機能を使用せず、自身の中での設定を利用します。

Copyright©2019 dit Co., Ltd. All rights reserved.

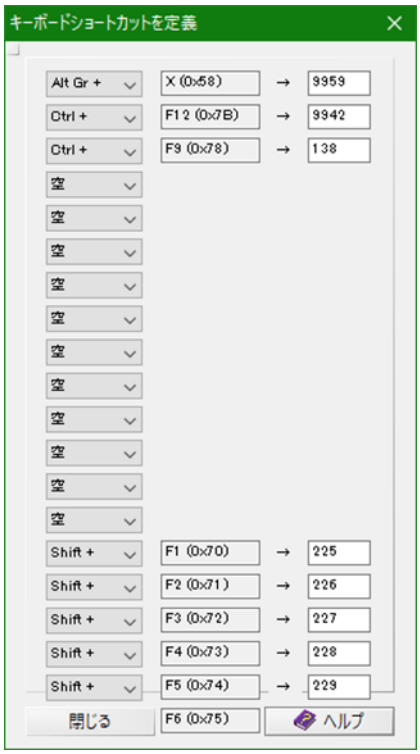
1.1.4. ... (Sleep(0) Frequency (0.. 100))



他のプロセスと CPU 時間を奪い合っている場合に、XWF が時間を要する操作の間、どれだけ協調的に振る舞うかを指定します。

- 0 (デフォルト)：協調しない
- 100：CPU 時間共有を最大限に行う

1.1.5. キーボードショートカットを定義



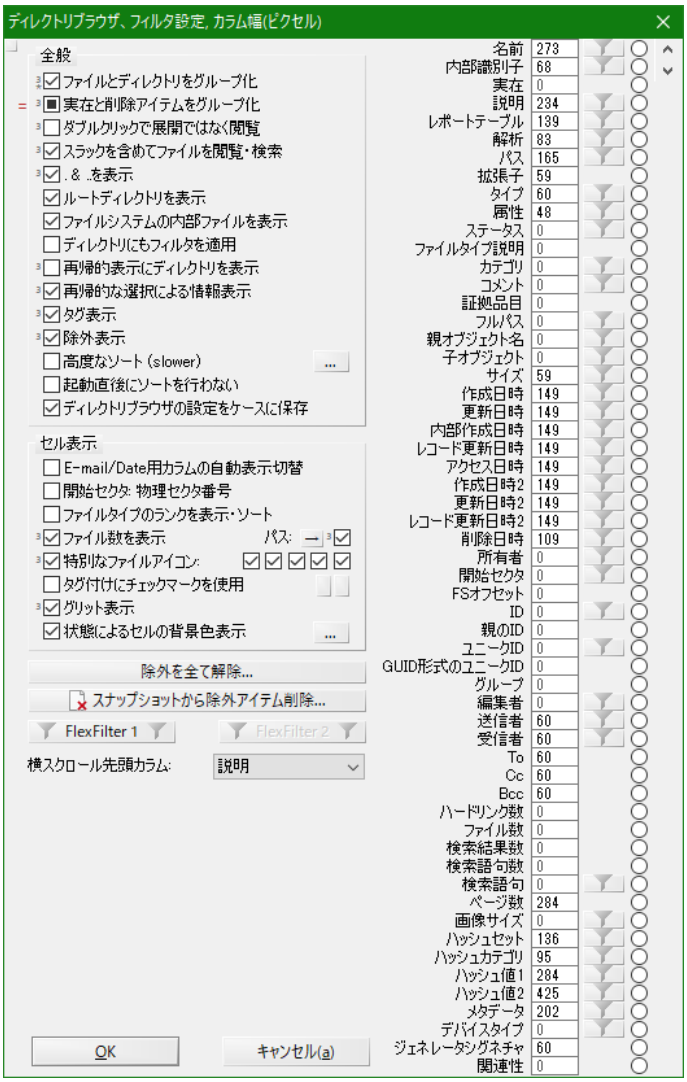
9800: 外部ビューアプログラム#1 で閲覧 9801: 外部ビューアプログラム#2 で閲覧 9802: 外部ビューアプログラム#3 で閲覧 ～ 9831: 外部ビューアプログラム#32 で閲覧 9919: ファイルタイプを定義 9920: 関連ファイルに移動 9921: 選択したファイルのボリュームスナップショットを更新 9927: 選択したファイルに対し X-Tension を実行	9955: ドライブレターとしてマウント(ディレクトリが 1 つだけ選択されている時のみ有効) 9956: 指定のビデオプレーヤーで再生 9957: 指定の HTML ビューアで閲覧 9958: 指定のテキストエディタで閲覧 9959: 関連付けられた外部プログラムで開く/実行 9960: 閲覧済みアイテムを選択 9961: 外部プログラムを選択して閲覧 9962: ハッシュに基づいて重複を削除 9963: 内部 ID に基づいてファイルを探す

Copyright©2019 dit Co., Ltd. All rights reserved.

9928: 外部ファイルをアタッチ 9931: メタデータを編集 9932: ファイルをディレクトリ内で表示 9933: ファイルをボリュームルートから表示 9934: 親オブジェクトを探す 9935: 選択したファイル内で論理検索 9937: 外部ディレクトリをアタッチ 9938: 安全な消去 9939: 特定ディレクトリの検索結果リストを残す 9940: 検索結果リストの重複を削除 9941: 除外アイテムを選択 9942: コメントを編集 9944: 除外を解除 9945: タグ付けされたアイテムを選択 9946: タグ付けされたアイテム以外を全て除外 9947: タグ付けされたアイテムを除外 9948: 証拠ファイルコンテナまたはスケルトンイメージ(バックグランドでアクティブなら)に追加 9949: 検索結果をリサイズ 9950: 検索結果をカービングファイルに変換 9951: カービングされたまたは仮想ファイルをリサイズ 9952: 検索結果を他の検索語句に割り当て 9953: 一連のビデオフレームを抽出 9954: 検索結果をレポートに含める	9964: 関連性評価によりソート 9965: 印刷 9966: リストのアイテム番号でアイテムを探す 9967: ソートしない 9968: すべて選択 9969: 選択したファイルのハッシュ値でフィルタ(重複検出のため) 9971: 展開 9972: 検索結果を重要とマーク 9973: 開く 9974: ファイルを定義しているファイルシステムデータ構造に移動 9975: Export list 9976: リストをエクスポート 9977: リカバー/コピー 9978: 展開/閲覧 9979: 選択を反転 9980: ハッシュデータベースに追加

Copyright©2019 dit Co., Ltd. All rights reserved.

1.2. ディレクトリブラウザ



オプション	説明	推奨設定
ファイルとフォルダのグループ化	☑：常にフォルダとファイルをグループ化 ■：通常表示(再起表示でない)のときにのみファイルとフォルダをグループ化	☑
実在と削除アイテムのグループ化	☑：実在と削除アイテムの 2 グループでグループ化(カラム上に”÷②”) ■：実在と復元できた可能性のある削除アイテム(“?”アイコン)と復元不能の削除アイテム(“×”アイコン)の 3 グループでグループ化(カラム上に”=③”)	■
ダブルクリックで展開ではなく閲覧	☑：ビューワーで閲覧 ■：閲覧と展開の選択画面を表示 ☐：子オブジェクトがある場合は展開	☐
スラックも含めてファイルを閲覧・検索	☑：ファイルを開く際や検索する際にファイルスラックも含め処理 ■：論理検索の時にのみ機能	☑

Copyright©2019 dit Co., Ltd. All rights reserved.

オプション	説明	推奨設定
. & .. を表示	☑：ディレクトリブラウザにカレントディレクトリ(“.”)と親ディレクトリ(“..”)のアイコンを表示 ■：ディレクトリブラウザに親ディレクトリ(“..”)のアイコンを表示	☑
ルートディレクトリを表示	ディレクトリブラウザにボリュームのルートディレクトリを表示	☑
ファイルシステムの内部ファイルを表示	NTFS が管理するシステムファイル(“$”から始まるファイル/ディレクトリ)を表示	☑
ディレクトリにもフィルタを適用	フィルタの対象にディレクトリを含める	(任意)
再帰的表示にディレクトリを表示	☑：再起表示時にディレクトリを表示 ■：フィルタリングの条件がディレクトリにもマッチする場合にのみディレクトリも表示	☐
再帰的な選択による情報表示	☑：選択したディレクトリのファイルの子オブジェクトを含むすべての子オブジェクトのファイル数と合計データサイズを表示 ■：選択したディレクトリの子オブジェクトのファイル数と合計データサイズを表示	☑
タグ表示	☑：親オブジェクトにタグ付けすると子オブジェクトにもタグ付けされる ■：タグ付けされたファイルに詳細なボリュームスナップショットで子オブジェクトが追加された場合、子オブジェクトにタグ付け ☐：選択したオブジェクトにのみタグ付け	☑
除外表示	☑：親オブジェクトを除外すると子オブジェクトも除外される ■：除外したファイルに詳細なボリュームスナップショットで子オブジェクトが追加された場合、子オブジェクトを除外 ☐：選択したオブジェクトのみ除外	☑
高度なソート（slower）	サブオプションの条件を使用したより高度なソートを実行	☐
起動直後にソートを行わない	☑：前回終了時のソートの状態を復元 ☐：ディレクトリブラウザ起動時にソートを行わない	(任意)
ディレクトリブラウザの設定をケースに保存	カラム幅、フィルタ、ソート順の設定状態をケースに保存し、次にケースをロードしたときに自動的に復元	☑
E-mail/Date 用カラムの自動表示切り替え	メールボックスから E-mail 抽出を実行した後、対象のディレクトリ以下をディレクトリブラウザ上で表示した際に、E-mail 用のカラム"送信者"と"受信者"を自動で表示	(任意)
開始セクタ：物理セクタ番号	☑：”開始セクタ”カラムの値を物理ディスクの先頭からのオフセット値で表示 ☐：”開始セクタ”カラムの値をパーティションの先頭からのオフセット値で表示	☐
ファイルタイプのランクを表示・ソート	“File Type Categories.txt”で定義されたファイルタイプのランクに従い並び替え	(任意)
ファイル数を表示	☑：ディレクトリブラウザのディレクトリと子オブジェクトを持つファイルおよびケースウィンドウのディレクトリの右に子オブジェクト数を表示	☑

Copyright©2019 dit Co., Ltd. All rights reserved.

オプション	説明	推奨設定
	■：ディレクトリブラウザのディレクトリと子オブジェクトを持つファイルの右に子オブジェクト数を表示	
パス	パスの表示を左揃えまたは右揃えに設定	→
部分パス(右のチェックボックス)	☑：再起表示時に部分パスを表示 ■：再起表示時に部分パス("...¥"付き)を表示	☑
特別なファイルアイコン	☑：サブオプションで有効にしたファイルタイプのアイコンを表示 ■：サブオプションで有効にしたファイルタイプのアイコンとシンボルを表示(クエスチョンマーク、矢印、ハサミ、ハンマー等) サブオプション(左から) Audio / Video / Picture / Document / Text	☑ サブオプション すべて☑
タグ付けにチェックマークを使用	タグにチェックマークを使用 (右のボタンでタグの色を任意に設定可能)	□
グリッド表示	☑：濃いグリッド線を表示 ■：薄いグリッド線を表示	(任意)
状態によるセルの背景色表示	設定したカラムの値の状態によってセルの背景色を任意に変更	(任意)
除外を全て解除	除外済みの設定をすべて解除	(任意)
スナップショットから除外アイテム削除	除外設定されているファイルをボリュームスナップショットから削除	(任意)
FlexFilter	プリセットされたフィルタと別に任意の条件でフィルタリング	(任意)
横スクロール先頭カラム	ディレクトリブラウザを横スクロールする際に、スクロールさせない固定のカラムを設定 プルダウンでスクロールさせるカラムの中で一番左に配置されているものを指定する	(任意)

Copyright©2019 dit Co., Ltd. All rights reserved.

1.3. ボリュームスナップショットオプション

オプション	説明	推奨設定
NTFS：スナップショットに EA を含める	ファイルが拡張属性を保つ場合、子オブジェクトに拡張属性の内容を含める ☑：すべての拡張属性が対象 ■：非レジデント属性のみが対象	(任意)
NTFS：スナップショットに LUS を含める	NTFS で利用される LUS (logged utility streams)を含める ☑：すべての LUS を含める ■：$EFS LUS 以外の LUS を含める	(任意)
NTFS：スナップショットに Zone.Id を含める	ファイルの代替データストリームにゾーン識別子が設定されている場合、子オブジェクトにファイルを追加	(任意)
FAT：削除ファイルは割り当て済みクラスタをスキップ	割り当て済みクラスタは、削除ファイルのデータを読むときにスキップ	☑
FAT32：削除オブジェクトを最大限復元	☑：全体に対して適用 ■：サブディレクトリに対してのみ適用	☑
ISO9600 形式も読込む(CD)	CD/DVD の読込みでエラーでファイルシステムのすべてのデータ構造を読めない場合、ディレクトリの対応するデータ構造が ISO9660 の読み取り可能なセクタに存在する場合、読み込みを試みる	(任意)
HFS+/APFS：EA の完全出力	EA(拡張属性)出力 ☑：バイナリ PList と普通の Security 属性も子オブジェクトとして出力 ■：firstlink 属性と quarantine 属性をメタデータ欄に出力	☐
RAM：モジュールのヘッダのみ	メインメモリ解析で、ハッシュ比較の際、ロードされたモジュールの不変のヘッダのみをリストする	☐
OS dir list：incremental completion	トップレベルのディレクトリの内容のみボリュームスナップショットに追加し、ユーザがアクセスしたディレクトリを順次追加する（非推奨オプション）	☐
コンテナのスナップショット更新状態を承認	証拠ファイルコンテナは、含まれるファイルのボリュームスナップショット更新の状態を記憶し、処理済みの更新をスキップ	☑

Copyright©2019 dit Co., Ltd. All rights reserved.

オプション	説明	推奨設定
すべての削除ファイルを含める	ボリュームスナップショットに削除されたファイルを含める	☑
削除状態の継承	パーティションごと削除されている場合、パーティションに含まれる全てのオブジェクトも削除されているものとみなす	☐
正味の空き領域計算	空き領域仮想ファイルを以前に存在したファイルに属すると判断されたクラスタのみに限定し、論理検索やインデックス作成の際に読まれるファイルシステム内の領域を最小化する	☑
OS を通してファイルを開く	Windows の先読みのメカニズムやファイルキャッシュのシステムを利用してファイルを開くことで読み込みを高速化する 対象メディアがライトプロテクトされている場合のみ利用すること	☐
未初期化部分をバイナリゼロとして読み込み	スラック領域をバイナリ値でゼロになっているとみなしてファイルを読み込む ☑：論理検索、インデックス作成、検索結果のプレビューを除くすべての操作が対象 ■：論理検索、インデックス作成、検索結果のプレビューを除くすべて読み取り操作が対象	☑
クラスタが得られないファイルも表示	メタデータが存在するが、クラスタからデータが得られないファイルも表示する ☑：メタデータから得られたファイルはすべて表示 ■：ファイル名やタイムスタンプ以上の何らかの情報が得られるもののみ表示	☑
クイックスナップショット(クラスタ配置無視)	セクタやクラスタの配置状況の情報を取得せずボリュームスナップショットを作成 ☑：全ファイルシステム対象 ■：Ext2/Ext3/ReiserFS 対象	☐
ボリュームのスナップショットの情報維持	オープンしたボリュームのファイルシステムの全情報を終了時に一時ファイル用のフォルダに保存	☑
より多くのデータをメモリに保持する	タイムスタンプによるソートが高速化される (オプション詳細不明)	☑
Convert RTF e-mail bodies to plain UTF-8	Outlook の電子メールアーカイブから、RTF フォーマットの電子メールボディを UTF-8 に変換	☑

Copyright©2019 dit Co., Ltd. All rights reserved.

1.4. ビューア設定

オプション	説明	推奨設定
セパレートビューアの使用	閲覧およびプレビュー機能を有効 パスに”.¥x64¥viewer”を指定	(デフォルト)
ビューア X-tensions をロード	ビューア用 X-tension を使用	☐
画像をビューアコンポーネントでも表示	セパレートビューアでなく、閲覧画面で画像を表示	(任意)
複数画像の同時表示	複数の画像をセパレートビューアを複数同時に起動して表示	☐
Auto update	複数画像の同時表示オプションがオフのとき、2 枚目以降の画像はシングルクリックでセパレートビューアの表示を更新	☑
別形式で.eml をプレビュー	☑：ディレクトリブラウザの表示形式に合わせた情報(送信者、受信者等)、ヘッダ情報を表示するプレビュー ☐：通常の From、To 等の情報をプレビュー	☑
.eml をヘッダなしで表示	上記オプションが有効の場合、プレビュー画面にヘッダを表示しない	☐
プレビュー/ディレクトリ	ディレクトリを選択したときに、プレビュー画面にディレクトリツリーを表示する	☐
クラッシュセーフなテキスト抽出(低速)	論理検索やインデックス作成の際、特定ファイルタイプからのテキストの抽出は、ビューアコンポーネントによって別プロセスで実行	(任意)
GDI フォントオブジェクトのリークをクリーンアップ	特定ファイルをロードするとき、稀にビューアコンポーネントで起こる GDI フォントオブジェクトのリークのクリーンアップを試みる	☑
ビューアでデコードしたテキストをバッファする	論理検索やインデックス作成で特定ファイルタイプから抽出されたテキストを次の検索/インデックス作成に備えてボリュームスナップ ショットに保存する	☑

Copyright©2019 dit Co., Ltd. All rights reserved.

オプション	説明	推奨設定
RAR 形式内の画像表示	RAR 形式アーカイブに保存された画像を解析しビューアに表示	☑
補助のサムネイルを許可する	埋め込みのサムネイルを持っている大きな JPEG ファイルですでにボリュームスナップショットに含まれているもの、あるいは画像処理の結果大きな画像に対する内部サムネイルが生成されているものは、オプションでそれを補助サムネイルとしてギャラリーの表示に使う ☑：補助サムネイルを循環表示 ■：循環表示しない	☑
ダブルクリックで展開でなく閲覧	ギャラリー画面でのサムネイルに対して ☑：ビューワーで閲覧 ■：閲覧と展開の選択画面を表示 ☐：子オブジェクトがある場合は展開	☐
ファイルサイズ	サムネイルにファイルサイズを表示	(任意)
シングルクリックで閲覧	ギャラリー画面でのサムネイルに対して、シングルクリックで閲覧	(任意)
サムネイルクリックでタグ付け	☑：サムネイルをクリックでタグ付け ■：サムネイルの左上の☐をクリックでタグ付け	☐
非画像ファイルもサムネイルとして表現	☑：サムネイル表示 ■：サムネイル表示 ☐：アイコン表示	☑
文書プレビューをサムネイルに縮小	☑：少し圧縮した圧縮サムネイル ■：強く圧縮した圧縮サムネイル ☐：標準サムネイル	☐
グレースケールのサムネイル	サムネイル画像をグレースケールで表示	(任意)
+x thread(s)	ギャラリーの描画処理に使用するスレッド数	+1
サムネイルサイズ指定	サムネイルのサイズを任意のサイズで指定	(任意)
タイムアウト(ミリ秒)	画像の読み込み中止までの時間	(デフォルト)
関連付けされたアプリケーションで閲覧	指定の拡張子のファイルを開いたときに、Windows に関連付けられたアプリケーションで開く	(デフォルト)
テキストエディタ	コンテキストメニューの"ビューア"に表示されるテキストエディタを指定	(任意)
HTML 出力ビューア	コンテキストメニューの"ビューア"に表示される HTML ビューア(ブラウザ)を指定	(任意)
MPlayer	MPlayer のパスを指定	(デフォルト)
Show console window (右のチェックボックス)	MPlayer 実行時にコンソールウィンドウを表示する	(任意)
動画用のビューア	動画を再生するビューアを指定	(デフォルト)
カスタムビューア	コンテキストメニューの"ビューア"に表示される任意のビューアを指定	(任意)
閲覧フラグを有効化	ビューアで閲覧したファイルに閲覧済みフラグを付ける	☑
... (閲覧フラグのオプション)	条件を満たす場合に閲覧済みフラグを付けるためのオプション	(デフォルト)

Copyright©2019 dit Co., Ltd. All rights reserved.

1.5. データインタープリタの設定

データインタープリタは、バイナリ表示内の値のカーソル位置のデータを変換する機能を提供するウィンドウです。

カーソル位置のバイトを先頭として、オプションで選択された項目の内容に従って単純に値を変換します。指定したカーソル位置からの値が、選択したオプションの項目の内容でない場合は、意味のない値が表示されます。

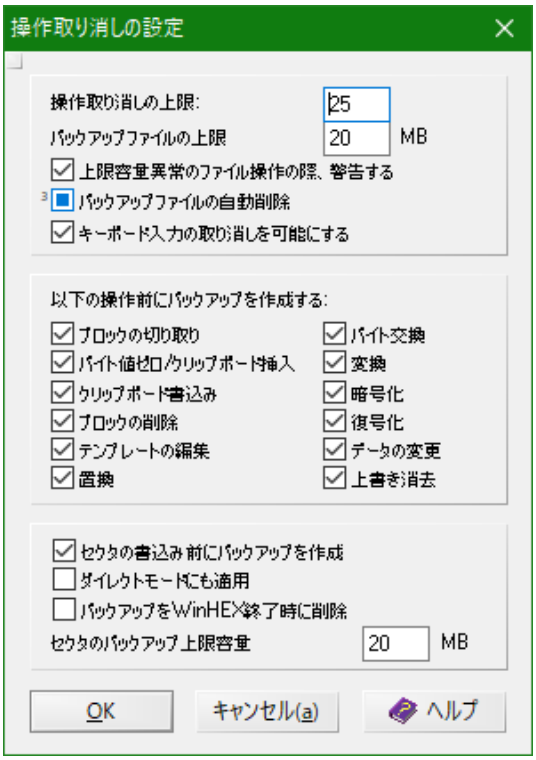
レジストリビューアで値を選択すると、バイナリ表示内の対応する値が選択された状態になります。このとき、データインタープリタを表示しておくと、レジストリビューア上では解釈できない表示の値の実際の値が確認できます。

データインタープリタのウィンドウを表示させるには、[ツール]－[表示画面]から”データインタープリタ”にチェックをします。

オプション	説明	推奨設定
Big Endian	ビッグエンディアンで計算して表示	☐
Hexadecimal / Octal	☑：16 進値で表示 ■：8 進値で表示 ☐：10 進値で表示	(任意)
10 進 ASCII タイムスタンプ	(不明)	☐
タイムゾーン:UTC +9:00	UTC +9:00 に基づくタイムスタンプ表示	☑
Transparency	半透明のウィンドウで表示	(任意)

Copyright©2019 dit Co., Ltd. All rights reserved.

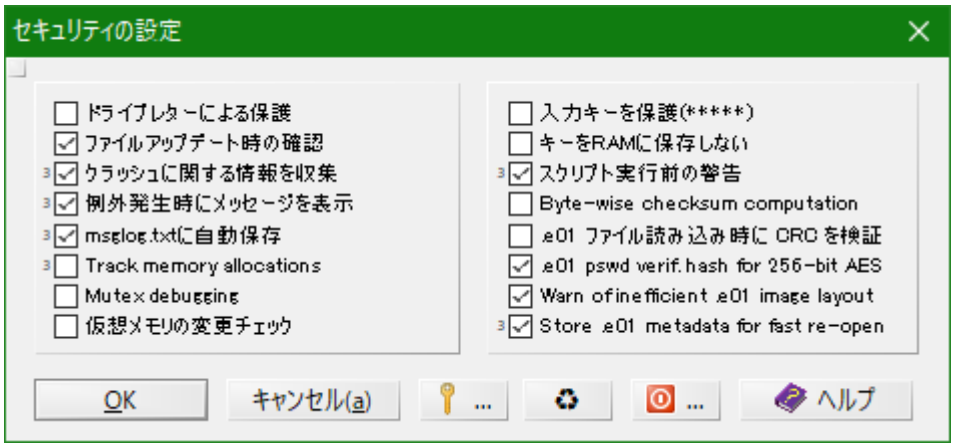
1.6. 操作取り消しの設定



オプション	説明	推奨設定
操作取り消しの上限	[編集]－[元に戻す]で戻ることのできる上限値	(任意)
バックアップファイルの上限	ディスクの容量や時間の節約のため設定されるバックアップファイルの上限値	(任意)
上限容量以上のファイル操作の際、警告する	バックアップファイルの上限を超えるファイル操作が行われた際に警告する	☑
バックアップファイルの自動削除	☑：ファイルを閉じたときにバックアップファイルを削除 ■：プログラムを閉じたときにバックアップファイルを削除	■
キーボード入力の取り消しを可能にする	(オプション項目の通り)	☑
以下の操作前にバックアップを作成する	チェックした項目の操作に対して、操作取り消しのためのバックアップを作成する	すべて☑
セクタの書き込み前にバックアップを作成	(オプション項目の通り)	☑
ダイレクトモードにも適用	ダイレクト編集モードを使用する際にも操作の取り消しを有効にする	(任意)
バックアップを WinHex 終了時に削除	(オプション項目の通り)	(任意)
セクタのバックアップ上限容量	セクタの編集操作でバックアップされる上限容量	(任意)

Copyright©2019 dit Co., Ltd. All rights reserved.

1.7. セキュリティの設定

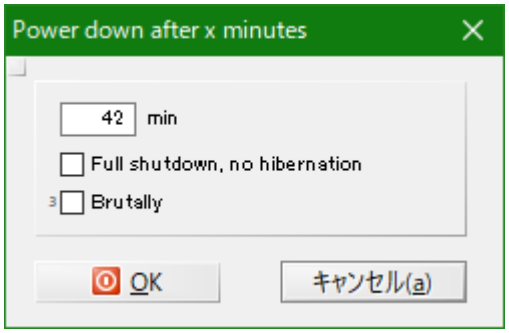


オプション	説明	推奨設定
ドライブレターによる保護	証拠品への書き込み防止のため、すべてのドライブに対してファイル出力保護が有効になる	☐
ファイルアップデート時の確認	実在ファイルへの変更を保存する前に確認画面を表示	☑
クラッシュに関する情報を収集	特定ファイル処理中にクラッシュした場合、XWF がプログラム再開時にクラッシュの原因と思われるファイルを通知 ☑：プログラムがクラッシュし再起動した際、クラッシュの原因となったファイルにどのサブオペレーションが実際に適用されていたのかも指摘 ■：プログラムがクラッシュし再起動した際、クラッシュの原因となったファイルを表示	☑
例外発生時にメッセージを表示	☑：破損したファイルに起因する解析結果に影響のないエラーもメッセージ出力 ■：関連する可能性のあるエラーをメッセージ出力 ☐：潜在的に深刻なエラーのみメッセージ出力	☑
msglog.txt に自動保存	Messages ウィンドウ内のメッセージをインストールディレクトリ内の"msglog.txt"に保存 但し、ケースを処理している場合は、ケースフォルダ以下の"_log"ディレクトリに保存	☑
Track memory allocations	(不明)	(任意)
Mutex debugging	(不明)	(任意)
仮想メモリの変更チェック	メモリエディタが仮想メモリの読み込み前または書き込み時、仮想メモリの構造が変わってもリードエラーを可能な限り防止	(任意)
入力キーを保護(*****)	暗号/復号時のキー入力内容を"*"表示	(任意)
キーを RAM に保存しない	プログラム実行中は入力したキーを暗号化した状態でメモリに保持	(任意)
スクリプト実行前の警告	☑：実行前に警告を表示 ■：コマンドラインからの実行に限定	(任意)
Byte-wise checksum computation	バイト単位のチェックサム計算 (詳細不明)	(任意)
.e01 ファイル読み込み時に CRC を検証	.e01 のチャンクの CRC をチャンクが読まれるたびに自動的にチェックし、不一致があればメッセージウィンドウにレポート	(任意)

Copyright©2019 dit Co., Ltd. All rights reserved.

オプション	説明	推奨設定
.e01 pswd verif.hash for 256-bit AES	256 ビット AES で生成された .e01 を開く際、入力されたパスワードが正しいかをチェック	(任意)
Warn of inefficient .e01 image layout	.e01 ファイルが非効率な構成(テーブルセクション当たり 32 チャンク以下、または圧縮チャンクで圧縮率が 0.1%以下)であることを検出するとユーザに通知	(任意)
Store .e01 metadata for fast re-open	.e01 ファイルのメタデータを作成し、次回開く際に高速化する ☑：イメージと同じディレクトリに保存 ■：現在のケースの証拠品目の内部メタデータディレクトリに保存	(任意)

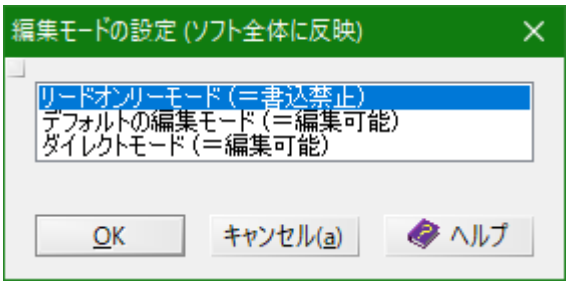
オプション	説明
鍵マークのボタン	詳細なボリュームスナップショットの圧縮ファイルのパスワード解析で使用するパスワードリストの編集(テキストエディタで password.txt が開かれる)
リサイクルマークのボタン	システムメモリを専有する (Windows 10 では権限不足で実行不可)
電源マークのボタン	指定時間後にマシンをシャットダウンまたはハイバネートする ようスケジュール



オプション	説明
Full shutdown, no hibernation	マシンをシャットダウンする
Brutally	☑：保存されていない作業に対してユーザに対処を促ししばらく待機 ■：強制シャットダウン

Copyright©2019 dit Co., Ltd. All rights reserved.

1.8. 編集モードの設定

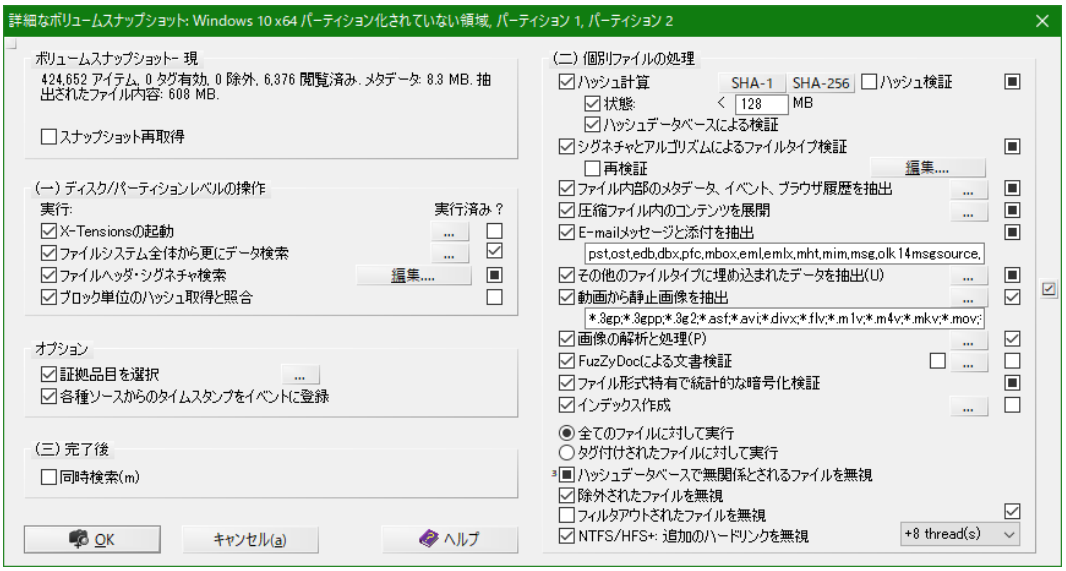


この編集方法が使えるのは WinHex のみで、X-Ways Forensics では使用できません。フォレンジック用途では、証拠品を編集することは禁止されているため、X-Ways Forensics では、ディスクやイメージを読み取り専用でファイルを開くようになっています。

オプション	説明
リードオンリーモード (=書込禁止)	フォレンジック調査時に必須のモード X-Ways Forensics ではこのモードのみ利用可能 このモードで開かれたファイルまたはディスクは、WinHex による編集や変更は一切できない。
デフォルトの編集モード (=編集可能)	ディスクやファイルに対する変更を一時ファイル用のディレクトリに保存 編集ウィンドウを閉じる、またはファイルメニューの保存を実行した時に、確認を取った上でオリジナルのディスクまたはファイルに変更を書き込む
ダイレクトモード (=編集可能)	すべての変更(キーボード入力、ブロック削除、クリップボードデータの書き込み、置換など)を確認なしにディスクやファイルに書き込む

Copyright©2019 dit Co., Ltd. All rights reserved.

2. 詳細なボリュームスナップショット



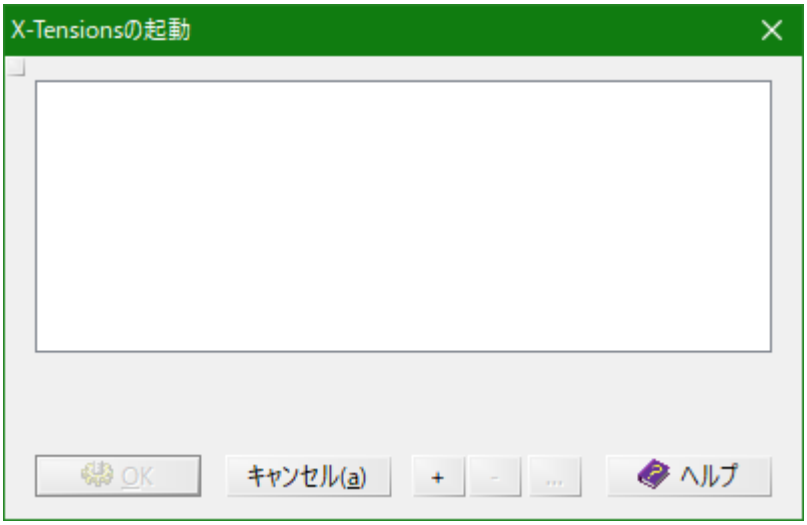
2.1. スナップショット再取得

詳細なボリュームスナップショットで実行した解析をすべて破棄し、ボリュームスナップショットを取得し直す。実行すると、最初に証拠品オブジェクトをケースに追加した時と同じ状態になります。

※ 解析で作成された仮想ファイルや、レポートテーブルの関連付け等の設定がすべて削除されます。

2.2. X-Tensions の起動

詳細なボリュームスナップショット実行時に X-Tensions を使用する。
チェックすると表示される[…]ボタンより、X-Tensions のコンポーネントを選択。

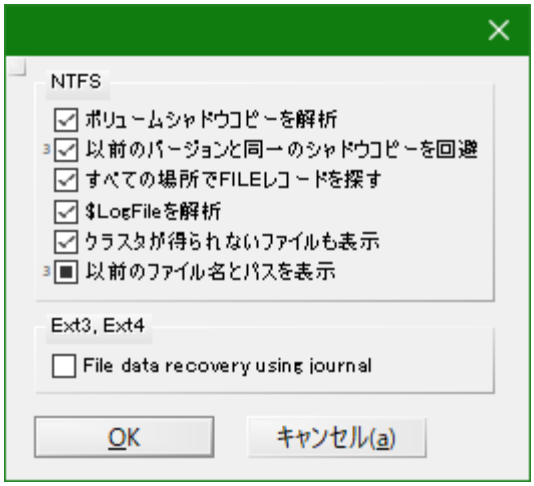


Copyright©2019 dit Co., Ltd. All rights reserved.

2.3. ファイルシステム全体から更にデータ検索

$LogFile およびボリュームシャドウコピーを解析し、MFT レコードからでは発見できない削除ファイルを調査、復元。

オプションで Linux 解析時、Ext3/4 ジャーナルからのファイル復元。



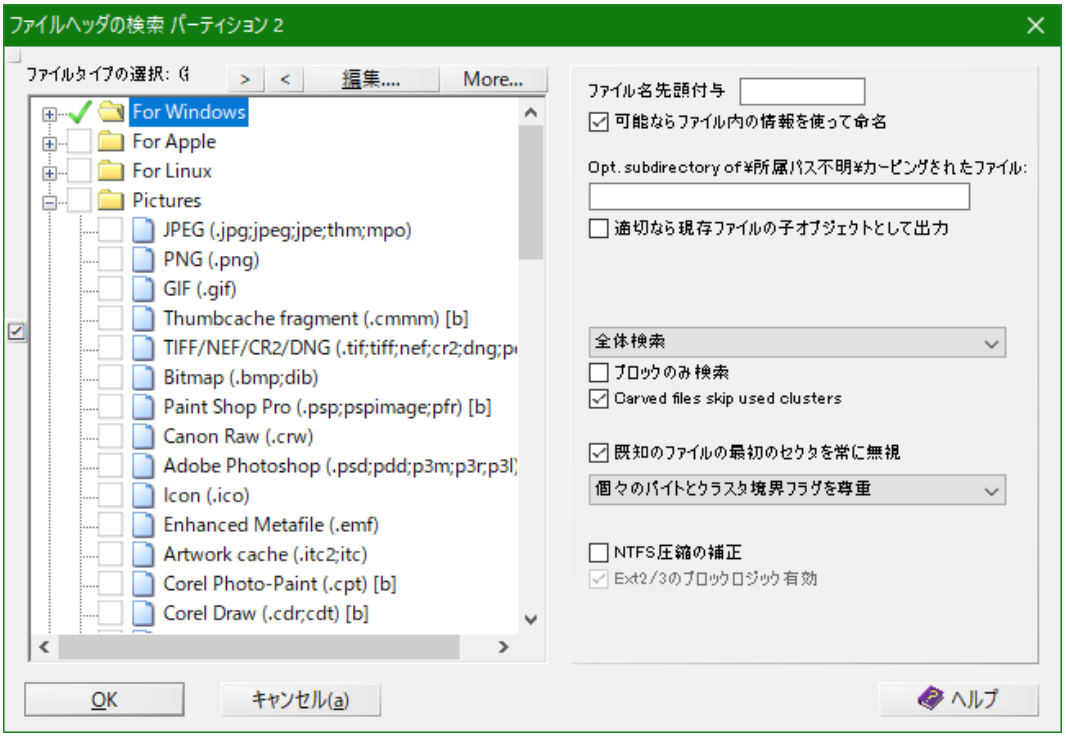
オプション	説明	推奨設定
ボリュームシャドウコピーを解析	ボリュームシャドウコピーが存在する場合、解析対象とする	☑ (必須)
以前のバージョンと同一のシャドウコピーを回避	複数のシャドウコピーが存在し、復元可能な同一のファイルが発見された場合に重複を回避するためのチェックを実施する ☑：128MB までのデータで比較 ■：16MB までのデータで比較	☑
すべての場所で FILE レコードを探す	ディスクの空き領域のセクタから、$MFT およびボリュームシャドウコピーに含まれていない MFT レコードを検索する	☑
$LogFile を解析	$LogFile を解析して削除されたファイルを探索する	☑
クラスタが得られないファイルも表示	データ部分が復元できないファイルも情報として表示する	☑
以前のファイル名とパスを表示	☑：以前のファイル名を名前カラムに、パスをパスカラムに表示 ■：以前のファイル名とパスをメタデータカラムに表示	■
File data recovery using journal	Ext3/Ext4 を使用した Linux システムの解析をする場合、ジャーナルを解析してファイルを復元	☐ (Windows の解析時)

2.4. ファイルヘッダ・シグネチャ検索

$MFT および「ファイルシステム全体から更にデータ検索」オプションで復元することができないファイルの復元を試みる。

空き領域または使用済み領域より、ファイル固有のヘッダ・シグネチャを探索し、指定のサイズで記録された情報を切り出してファイルとしてボリュームスナップショットに登録する。

Copyright©2019 dit Co., Ltd. All rights reserved.



オプション	説明	推奨設定
ファイルタイプの選択	ファイルヘッダ・シグネチャ検索を実行するファイルタイプを選択 **カテゴリ（フォルダのアイコン）**：カテゴリに含まれるファイルタイプをすべて選択 **ファイルタイプ**：選択したファイルタイプのみ選択 カテゴリ、ファイルタイプはカスタマイズ可能	(任意) すべてを選択すると意味のない不要なファイルが大量に追加されるため、必要最低限のファイルタイプを選択することを推奨します。
ファイル名先頭付与	ファイル名の先頭に任意の文字列を追加	(任意)
可能ならファイル内の情報を使って命名	JPEG やレジストリハイブファイル等、メタデータから情報を取得できたファイルにはオリジナルのファイル名を付与する	☑
Opt. subdirectory of¥所属パス不明¥カービングされたファイル:	カービングしたファイルの登録先サブディレクトリを指定	(任意)
適切なら現存ファイルの子オブジェクトとして出力	カービングしたファイルが現存する親オブジェクトの子オブジェクトであることが明確な場合、子オブジェクトとして登録する	☐
(検索対象)	・ 全体検索（デフォルト） ・ 未使用領域のみ検索 ・ 使用領域のみ検索	(任意) 削除されたファイルを検索する場合は、「未使用領域のみを検索」を選択
ブロックのみ検索	検索箇所を定義したブロックのみを検索	☐
Carved files skip used clusters	使用されているクラスタをスキップする	☑
既知のファイルの最初のセクタを常に無視	ボリュームスナップショットで既に把握されているファイルの開始セクタをカービングから除外する	☑

Copyright©2019 dit Co., Ltd. All rights reserved.

オプション	説明	推奨設定
(検索方法)	・ セクタ単位で検索 ・ 個々のクラスタ境界フラグを尊重 ・ 個々のバイトとクラスタ境界フラグを尊重 ・ バイト単位で検索（広範囲、要時間）	個々のバイトとクラスタ境界フラグを尊重
NTFS 圧縮の補正	NTFS 圧縮されたファイルのシグネチャを発見した場合、圧縮ファイルとしてマークし、圧縮解除されたファイルを登録	(任意)
Ext2/3 のブロックロジック有効	典型的な Ext2/3 のブロックロジックに従い復元	(任意) Ext2/3 以外の FS 処理時は無効

2.5. ブロック単位のハッシュ取得と照合

ディスクまたはパーティションの空き領域をブロックサイズごとにハッシュ値を計算し、ブロックハッシュのハッシュセットと照合をおこなう。ブロックサイズは固定で 512 バイト。

検索対象のファイルをブロックごとにハッシュ値を計算し検索を行うことで、空き領域にフラグメント化されて残存している情報と照合することが可能になる。

2.6. 証拠品目を選択

ケースに複数の証拠オブジェクトまたはパーティション等が登録されている場合、詳細なボリュームスナップショットを適用する対象を選択することができる。このオプションを使用しない場合、ケースに登録されているすべての証拠オブジェクトが対象になる。

[…]ボタンより、適用対象の証拠オブジェクトを選択する。

2.7. 各種ソースからタイムスタンプをイベントに登録

処理対象の様々なソースから抽出されたタイムスタンプをイベントリスト（タイムライン)に登録する。

2.8. 同時検索

詳細なボリュームスナップショットの処理終了後、すぐに同時検索を実行する。

2.9. ハッシュ計算

指定されたハッシュ関数でファイルのハッシュ値を計算する。同時に選択できるハッシュ関数は 2 つまでで、以下の関数から選択。

checksum (8bit)	checksum (16bit)	checksum (32bit)	checksum (64bit)
CRC (16bit)	CRC (32bit)	MD5 (128bit)	SHA-1 (160bit)
SHA-256 (256bit)	RipeMD-128 (128bit)	RipeMD-160 (160bit)	MD4 (128bit)
ed2k (128bit)	Adler32	TigerTree (192.bit)	Tiger128 (128bit)
Tiger160 (160bit)	Tiger192 (192bit)	Internal	

2.9.1. 状態

ハッシュ計算を行うファイルをファイルサイズで限定する。

Copyright©2019 dit Co., Ltd. All rights reserved.

2.9.2. ハッシュデータベースによる照合

予め登録したハッシュセットを使用して、計算したファイルのハッシュ値と比較・検証を行う。

ハッシュ計算で選択したハッシュ関数のハッシュデータベースが登録されている場合、詳細なボリュームスナップショット開始前に使用するハッシュセットの選択画面が表示される。

2.10. シグネチャとアルゴリズムによるファイルタイプ検証

「File Type Signatures Check Only.txt」に登録されたファイルのシグネチャを使用して、ファイルのファイルタイプを照合する。

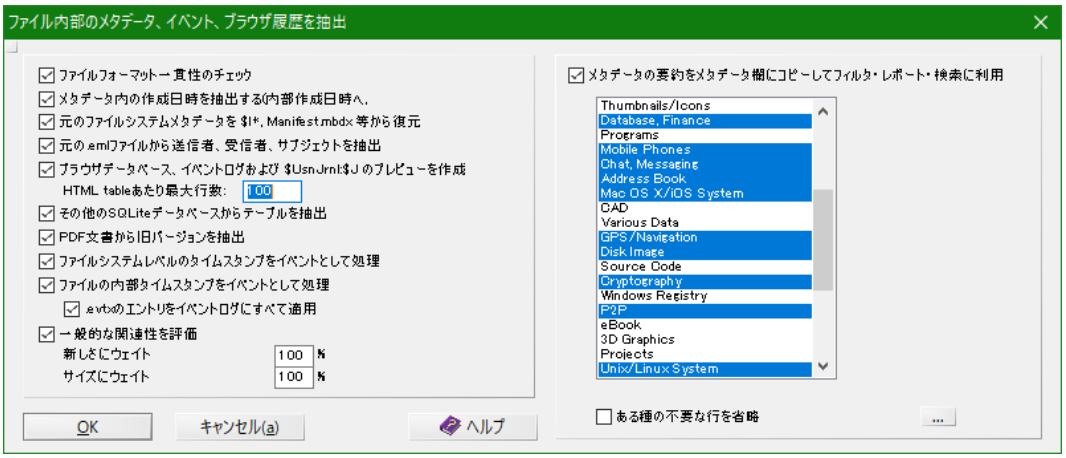
拡張子がないファイルや、シグネチャ情報と拡張子が異なるファイルは、タイプカラムに本来のファイルタイプを表示する。

詳細なボリュームスナップショットのこれ以降のオプションは、ファイルタイプを参照し、該当するファイルに対して処理を実行するため、予め正しいファイルタイプを検証しておく必要がある。

2.11. ファイル内部のメタデータ、イベント、ブラウザ履歴を抽出

ファイル内部に存在するメタデータ、イベントログやファイルシステムが持つ情報、ブラウザの履歴等を解析・抽出し、各種ファイルへの出力およびイベントリスト（タイムライン)への追加を行う。

2.11.1. オプション



オプション	説明	推奨設定
ファイルフォーマット一貫性のチェック	以下のファイルの一貫性をチェック ・ EXE, ZIP, RAR, JPEF, GIF, PNG, RIFF, PDF	☑
メタデータ内の作成日時を抽出する	以下のファイルから内部時刻を抽出 抽出した時刻は、「内部作成日時」カラムに登録 ・ EDB, TIFF, PNG, GZ, GHO, ETL, SQM, CAT, CER, CTL ・ OLE2 複合ドキュメント（2007 より前の Office ファイルなど) ・ PGP の .pkr キーリング	☑

Copyright©2019 dit Co., Ltd. All rights reserved.

オプション	説明	推奨設定
	・ IE の Cookies ・ SHD プリンタースプール ・ PF prefetch ・ LNK shortcut ・ DocumentSummary 代替データストリーム	
元のファイルシステムメタデータを$I*, Manifest.mbdx 等から復元	$I ファイル、iPhone mobile sync のバックアップインデックス（Manifest.mbdx)等より、元のファイルのメタデータを復元し登録 ファイル名が明らかな場合は、「名前」カラムのファイル名を抽出したファイル名で置換する	☑
元の.eml ファイルから送信者、受信者、サブジェクトを抽出	以下の単一のメールファイルから、送信者、受信者、件名の情報を抽出し、「送信者」、「受信者」カラムに登録、ファイル名を件名に置換 ・ .eml, .emlx, olk14msgsource	☑
ブラウザデータベース、イベントログおよび$UsnJrnl:$J のプレビューを作成	以下のブラウザの項目を SQLite データベースより抽出し、HTML プレビューを作成 **Firefox** ・ 閲覧履歴、ダウンロード、フォーム履歴、ログイン情報 **Google Chrome** ・ 閲覧履歴、archived history、Coockies、ログイン情報、Web データ、同期情報 **Safari** ・ キャッシュ、フィード **Internet Explorer 9 以前** ・ index.dat **Internet Explorer 10 以降** ・ WebCacheV01.dat **Microsoft Edge** ・ spartan.edb (お気に入りとリーディングリスト) **Skype** ・ main.db の contacts、ファイル転送履歴 **Opera** 以下のイベントログファイルを解析し、HTML プレビューを作成 ・ Windows イベントログ（.evt, .evtx) ・ Apple FS Event ログ $UsnJrnl:$J を解析し、$J.tsv ファイルを作成 システムリソース利用量モニタ（SRUM)を解析し、HTML プレビューを作成 ・ Application Resource Usage ・ Energy Usage ・ Energy Usage LT ・ Network Connectivity Usage ・ Network Data Usage ・ Windows Push Notifications	☑
その他の SQLite データベースからテーブルを抽出	各種 SQLite データベースを解析し、tsv ファイルを作成 iOS の netusage.sqlite を解析し、HTML プレビューを作成	☑

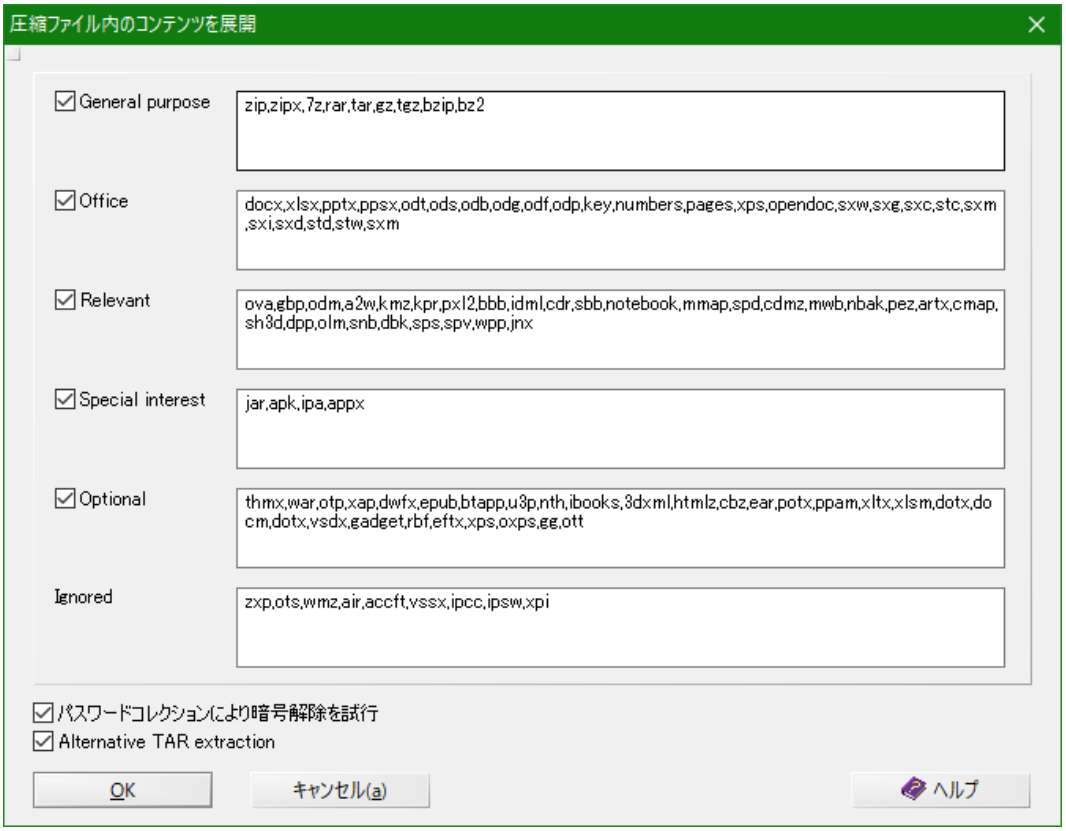
Copyright©2019 dit Co., Ltd. All rights reserved.

オプション	説明	推奨設定
PDF 文書から旧バージョンを抽出	編集された PDF ファイルを解析し、オリジナルを子オブジェクトとして追加	☑
ファイルシステムレベルのタイムスタンプをイベントとして処理	ファイルシステムの各種タイムスタンプを抽出し、イベントリスト（タイムライン)に追加	☑
ファイルの内部タイムスタンプをイベントとして処理	ファイルおよびイベントの内部タイムスタンプを抽出	☑
.evtx のエントリをイベントログにすべて適用	すべてのイベントログのイベントをイベントリスト（タイムライン)に追加	(任意)
一般的な関連性を評価	ファイルの一般的な関連性の評価 ウェイトは、0～255%で設定	☑
メタデータの要約をメタデータ欄にコピーしてフィルタ・レポート・検索に利用	詳細画面にデータが表示されるすべてのファイルおよび Windows ショートカット（.LNK)、プリフェッチファイル(.pf)より、メタデータを抽出し、「メタデータ」カラムに登録 メタデータカラムに追加するカテゴリを選択（任意)	☑

2.12. 圧縮ファイル内のコンテンツを展開

ZIP, RAR, ARJ, GZ, TAR, 7Zip, BZIP の圧縮ファイル内のファイルを圧縮ファイルの子オブジェクトとしてボリュームスナップショットに追加する。また、Office 2007 以降のドキュメント等 zip 圧縮が使用されているファイルを展開し、内部の構成ファイルを子オブジェクトとしてボリュームスナップショットに追加する。

2.12.1. オプション



Copyright©2019 dit Co., Ltd. All rights reserved.

オプション	説明	推奨設定
General purpose	記載の拡張子を持つ圧縮ファイルを展開する	☑
Office	Microsoft Office 2007 以降のドキュメント、LibreOffice、OpenOffice、iWork のファイルを展開する	☑
Relevant	その他圧縮ファイルの形式をとる記載の拡張子のファイルを展開する	(任意)
Special Interest	zip 関連ファイルを展開する	☑
Optional	その他圧縮ファイルの形式をとる記載の拡張子のファイルを展開する	(任意)
Ignored	記載の拡張を持つファイルを除外する	(デフォルト)
パスワードコレクションにより暗号解除を試行	パスワードコレクション（Password.txt)に記載の文字列を使用して、パスワードのかけられた圧縮ファイルの解除を試行する	(任意)
Alternative TAR extraction	代替の TAR 展開を使用する（詳細不明）	(任意)

2.13. E-mail メッセージと添付を抽出

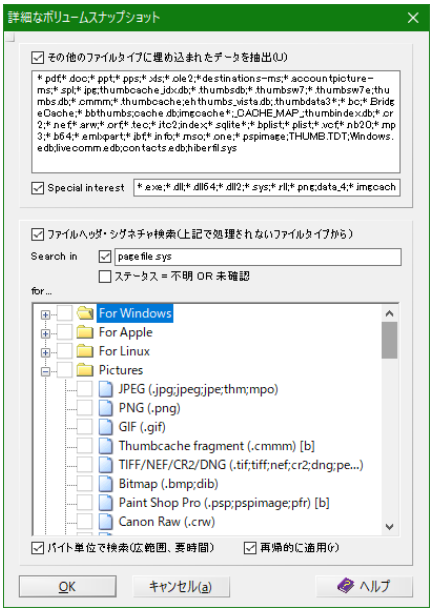
下記の E-mail アーカイブから、E-mail メッセージを.eml 形式で抽出し、ボリュームスナップショットに追加する。また、添付ファイルを抽出し、E-mail メッセージの子オブジェクトとして追加する。

- pst, ost, edb, dbx, pfc, mbox, eml, emlx, mht, mim, msg, olk14msgsource, olk14message, olk14msgattach, olk15msgattach, olk15msgsource, olk15message, oft ,mbs

2.14. その他のファイルタイプに埋め込まれたデータを抽出

以下のファイルタイプのファイルより、埋め込まれたデータを抽出し、子オブジェクトとしてボリュームスナップショットに追加する。

2.14.1. オプション



Copyright©2019 dit Co., Ltd. All rights reserved.

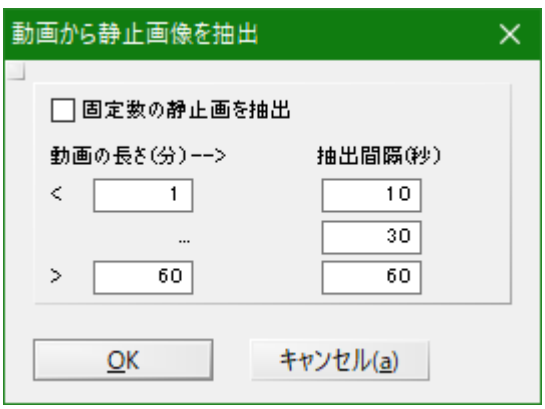
オプション	説明	推奨設定
その他のファイルタイプに埋め込まれたデータを抽出	記載の拡張子を持つファイルからデータを抽出 ・ *.pdf, *.doc, *.ppt, *.pps, *.xls, *.ole2, *destinations-ms, *.accountpicture-ms, *.spl, *.jpg, thumbcache_idx.db, *.thumbsdb, *.thumbsw7, *.thumbsw7e, thumbs.db,*.cmmm, *.thumbcache, ehthumbs_vista.db, .thumbdata3*, *.bc, *.BridgeCache, *.bbthumbs, cache.db, imgcache*, _CACHE_MAP_, thumbindex.db, *.cr2, *.nef, *.arw, *.orf, *.tec, *.itc2, index, *.sqlite*, *.bplist, *.plist, *.vcf, *.nb20, *.mp3, *.b64, *.emlxpart, *.jbf, *.info, *.mso, *.one, *.pspimage, THUMB.TDT, Windows.edb, livecomm.edb, contacts.edb, hiberfil.sys	☑
Special interest	記載の拡張子を持つファイルからデータを抽出 ・ *.exe, *.dll, *.dll64, *.dll2, *.sys, *.rll, *.png, data_4, *.imgcache	☑
ファイルヘッダ・シグネチャ検索（上記で処理されないファイルタイプから）	指定したファイルから、指定のファイルタイプのファイルをカービングする	(任意)
Search in	☑：右の欄に記載したファイルを対象とする	(任意)
ステータス=不明 OR 未確認	(詳細不明)	(任意)
for ...	ファイルヘッダ・シグネチャ検索を実施するファイルタイプを選択	(任意)
バイト単位で検索（広範囲、要時間）	埋め込まれたファイルで、オリジナルのファイル内の 512 バイト境界から始まっていないファイルを切り出す場合は、このオプションを使用する	☑ (ファイルヘッダ・シグネチャ検索を実施する場合)
再帰的に適用	カービングされたファイルを更に再帰的にカービングする	(任意)

2.15.動画から静止画像を抽出

下記ファイルタイプの動画より、動画プレビューとして指定の間隔で静止画像を抽出し、子オブジェクトとしてボリュームスナップショットに追加する。

・ *.3gp, *.3gpp, *.3g2, *.asf, *.avi, *.divx, *.flv, *.m1v, *.m4v, *.mkv, *.mov, *.mp4, *.mpeg, *.mpg, *.webm, *.nsv, *.nut, *.nuv, *.qt, *.rm, *.rmvb, *.vob, *.wmv, *.m2ts

2.15.1. オプション



Copyright©2019 dit Co., Ltd. All rights reserved.

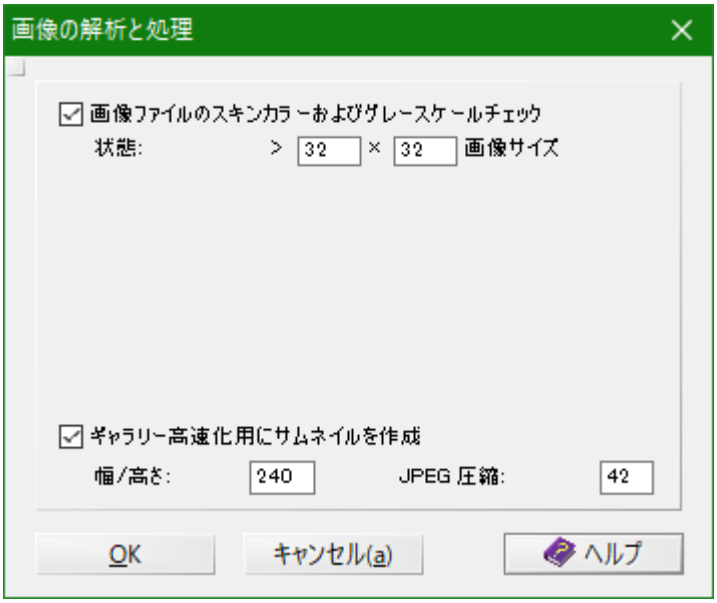
オプション	説明	推奨設定
固定数の静止画を抽出	☑：等間隔で指定した枚数の静止画を抽出する デフォルトは 10 枚 ☐：下記の設定で制し画像を抽出する	(任意)
動画の長さ ＜[○分]	指定した時間未満の場合、「抽出間隔（秒)」に指定した間隔で静止画像を抽出する	(任意)
動画の長さ ＞[○分]	指定した時間より長い場合、「抽出間隔（秒)」に指定した間隔で静止画像を抽出する	(任意)
…	上記で指定した長さの間になる動画の場合、「抽出間隔(秒)」に指定した間隔で静止画像を抽出する	(任意)

2.16.画像の解析と処理

下記ファイルタイプの画像に対して、画像内のスキンカラー(肌色)比率のチェックとグレースケール画像の検出を行う。

- JPEG, PNG, GIF, TIFF, BMP, PSD, HDR, PSP, SGI, PCX, CUT, PNM, PBM, PGM, PPM, ICO

2.16.1. オプション



オプション	説明	推奨設定
画像ファイルのスキンカラーおよびグレースケールチェック	画像ファイル内に占める肌色とグレースケールの割合を解析	☑
状態	指定した画像サイズより大きな画像だけを解析対象とする	(任意)
ギャラリー高速化用にサムネイルを作成	ギャラリー表示用のサムネイルを作成	(任意)
幅/高さ	サムネイル画像のサイズを指定	(任意)
JPEG 圧縮	サムネイルの JPEG 画像の圧縮率を指定	(任意)

Copyright©2019 dit Co., Ltd. All rights reserved.

2.17. FuzZyDoc による文書検証

FuzZyDoc™ により基準とする文書に対して、人の目で見て同じまたは似た内容の文書と判断できる下記タイプの文書を検索する。

- eml, ascii, txt, doc, docx, doc1, odt, pages, pdf, xps, rtf, ppt, pptx, odp, key, xls, xlsx, ods, numbers

2.17.1. オプション

オプション	説明	推奨設定
ハッシュセットに表されたテキストに基づく	「検索したファイルに基準とするファイルの文書が含まれるか」の割合を表示する	(任意)
処理された文書内のテキストに基づく	「検索した文書がどれだけオリジナルの文書に近似しているか」の割合を表示する	(任意)
Required	割合を指定する	(任意)
検証用のハッシュセット選択	FuzZy ハッシュデータベースに登録したハッシュセットを選択する	登録されたハッシュセットから選択

2.18. ファイル形式特有で統計的な暗号化検証

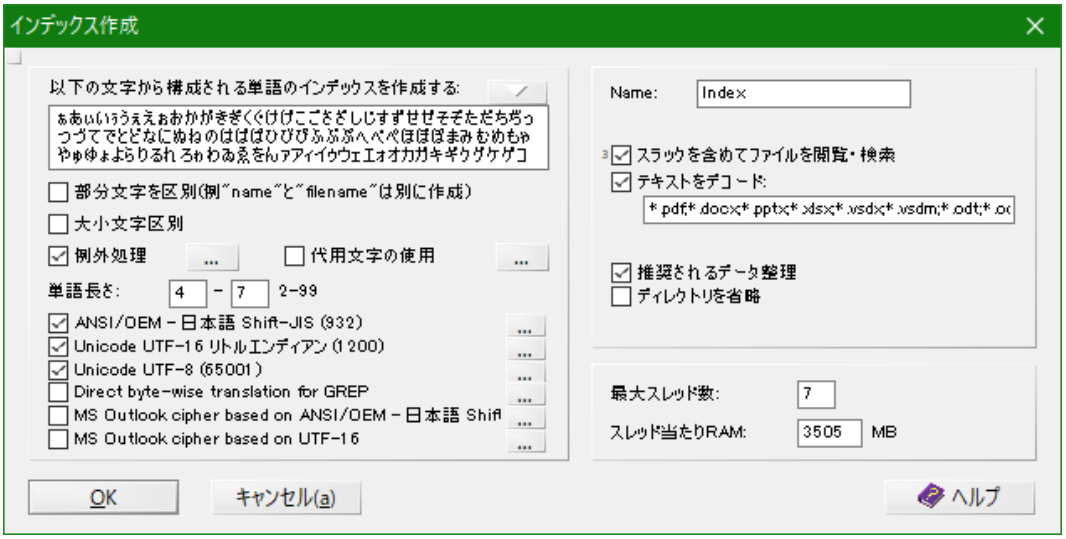
エントロピー検定により 255 バイト以上のファイルに対して暗号化の有無を実施する。結果は属性カラムに表示。

2.19. インデックス作成

ボリュームスナップショット内の全ファイルまたは特定ファイルから、ユーザ指定内容に従った全ての単語をインデックス化する。

Copyright©2019 dit Co., Ltd. All rights reserved.

2.19.1. オプション



オプション	説明	推奨設定
以下の文字から構成される単語のインデックスを作成する	右の「▽」ボタンから言語を選択	(任意)
部分文字を区別	単語内に含まれる別の単語も区別してインデックスを作成 日本語等の単語の区切りがない言語では、このオプション必須	☑
大文字小文字区別	大文字小文字を区別してインデックスを作成	(任意)
例外処理	「indexwds.txt」に記載された単語をインデックス作成から除外	(任意)
代用文字の使用	「indexsub.txt」に記載された代用文字を使用してインデックスを作成	(任意)
単語の長さ	インデックスとして作成する単語の長さを設定	(任意)
(文字コード選択)	インデックス作成に使用する文字コードを指定	(任意)
Name	ケースに出力するインデックスデータのフォルダ名を指定	(任意)
スラックを含めてファイルを閲覧・検索	☑：スラック領域の情報もインデックス作成 ■：(不明)	☑
テキストをデコード	下記ファイルタイプのファイルはデコードしてインデックス作成 ・ *.pdf, *.docx, *.pptx, *.xlsx, *.vsdx, *.vsdm, *.odt, *.odp, *.ods, *.pages, *.key, *.numbers, *.eml, *.wpd, *.vsd, *.onepkg	☑
ディレクトリを省略	ディレクトリをインデックス作成の対象としない	(任意)
最大スレッド数	インデックス作成に使用する最大スレッド数	(任意)
スレッド当たり RAM	スレッド当たりに使用するメモリサイズ	(任意)
(実行対象の選択)	詳細なボリュームスナップショットを実行する対象のファイルを選択 ◉ 全てのファイルに対して実行 ○ タグ付けされたファイルに対して実行	全てのファイルに対して実行
ハッシュデータベースで識別されるファイルを無視	ハッシュデータベースのハッシュ値と比較して、識別されたファイルを処理から除外する	☐

Copyright©2019 dit Co., Ltd. All rights reserved.

オプション	説明	推奨設定
ハッシュデータベースで無関係とされるファイルを無視	ハッシュ検証の結果、「無関係」とされるファイルを詳細なボリュームスナップショットの実行対象から除外する	☐
フィルタアウトされたファイルを無視	フィルタリングで除外されているファイルをボリュームスナップショットの実行対象から除外する	☐
NTFS/HFS+:追加のハードリンクを無視	ハードリンク数が 2 以上の場合、2 つ目以降のハードリンクを詳細なボリュームスナップショットの実行から除外する	☑
(スレッド数の選択)	詳細なボリュームスナップショットの処理で使用する最大スレッド数を選択 X-Ways Forensics 以外の用途で PC を使用していないなら、最大数を選択することを推奨 PC のスレッド数が上限 プログラム上の最大スレッド数は、16	(任意)

2.20.解析中に表示される状況画面

記号	説明
Hsh	ハッシング
Sig	ファイルタイプ検証
Met	メタデータ抽出
Arc	アーカイブ中のファイルのボリュームスナップショットへの追加
Eml	電子メール抽出
Emb	埋め込まれたデータの検出
Vid	動画からの静止画切り出し
Pic	その他の画像処理
Fuz	FuzZyDoc データベース照合
Enc	ファイルフォーマット固有の暗号化の検証
Idx	インデックス作成のための元ファイル内容の前処理
IdX	インデックス作成のためのデコードされたテキストの前処理
Dec	インデックス作成のためのテキストデコーディング
PDN	PhotoDNA データベース照合
Ent	エントロピーチェック

Copyright©2019 dit Co., Ltd. All rights reserved.

3. その他

3.1. XWF が自動的に設定するレポートテーブルの関連付け

英語メッセージ	日本語メッセージ(または和訳)
No detectable textual contents	検出可能なテキストコンテンツがない
Unable to decode text	テキストを解読できない
For error messages see Metadata	エラーメッセージはメタデータを参照
Unable to explore	調査できない
Empty archive?	空のアーカイブ？
Spanned archive	分割されたアーカイブ
No e-mails found	電子メールは見つからなかった
Path too long.	パスが長すぎる
Large non-resident $EA	大きな non-resident の$EA
Animated GIF	アニメーション GIF
Animated PNG	アニメーション PNG
Multi-page TIFF	マルチページの TIFF
Multi-page JPEG marker	マルチページの JPEG マーカー
Phone screenshot?	電話のスクリーンショット？
Zip bomb? Not fully processed	Zip 爆弾？ 完全には処理されていない
Unexpected tail (SFX?)	予期しない終端(SFX？)
Contains unknown segment (SFX?)	未知のセグメントを含む(SFX？)
FSG Packer	FSG Packer
PECompact	PECompact
UPX	UPX
英語メッセージ	日本語メッセージ(または和訳)
Unknown segment	未知のセグメント
Binder?	Binder?
Contains embedded document(s)	埋め込みドキュメントを含む
Contains embedded object(s)	埋め込みオブジェクトを含む
Contains embedded file	埋め込みファイルを含む
Contains hidden file	隠しファイルを含む
Hybrid MS Office document!	複合 MS Office ドキュメント
RAR hybrid	RAR hybrid
Contains embedded non-JPEG/non-PNG picture	埋め込み非 JPEG/非 PNG 画像を含む
Contains invisible old revisions	不可視の旧版を含む
Concatenated-PDF	結合された PDF
Contains private chunk	プライベートチャンクを含む
No pictures extracted	画像が抽出されない
Reason for crash?	クラッシュの原因？
Unsupported file type variant	未サポートのファイルタイプの変種
Omitted	省略された
Not copied	コピーされていない
Virus suspected	ウイルスの疑い
Unable to read	読み込み不能
Not decompressed	圧縮解除されていない

Copyright©2019 dit Co., Ltd. All rights reserved.