

Windows データ調査項目 (案)

- 削除ファイル内に機密情報が含まれていないかの調査 (キーワード検索)
 - 削除ファイルに保護されたファイルが無い確認
 - ゴミ箱フォルダの痕跡確認 (INFO2)
 - 削除ファイル・パーティションの復元
 - Volume Shadow
 - Copy内のゴミ箱フォルダ調査
- 未使用領域内に対するキーワード検索 (文字列・ファイル名痕跡の確認)
 - 未使用領域からのファイル復元 (パターンによる復元)
 - 未使用領域のキーワード検索
- アプリケーションログに対する、ファイル名などのキーワード検索
 - データ送信可能なアプリケーションの実行痕跡確認
 - 外部へのデータ送信痕跡の確認
 - データ送信可能なアプリケーションの履歴調査 (Skype等)
 - メモリーメージ内の外部との通信痕跡の調査
- 機密情報ファイルの確認
 - 圧縮ファイル内のファイルを含む既存ファイルに対するキーワード検索
 - ハッシュ値によるファイル検索
 - Volume Shadow Copy 内のファイル調査
 - 近似ファイルの検出
 - PDF画像ファイル(スキャン文書)の検出
 - Windows Search
 - インデックスにおけるファイル痕跡の確認
 - Office 文書のプロパティ情報に対するキーワード検索
 - オブジェクトIDを利用したOffice 文書のキーワード検索
- 隠蔽・保護ファイルの確認
 - OSインストール日時確認 (再インストール有無)
 - 保護ファイル (パスワード保護等) が設定されているファイルの検出
 - ファイル名変更痕跡の調査 (\$FILE_NAME 属性)
 - 隠し属性のファイル、拡張子が変更されたファイルを検出
 - 暗号化コンテンツ (ボリューム) の利用痕跡の調査
 - ステガノグラフィツールなどデータ隠蔽ツールの利用痕跡調査 (UserAssist)
- 印刷痕跡の確認
 - スワップファイル等から印刷ジョブ実行時のシャドウファイルスプールファイルを検出
- メモリーメージ内のファイル取り扱い情報 (オープンファイル) の調査
 - メモリーメージ内における文字列検索 (ファイル名・データ痕跡)
 - メモリーメージ内の文書ファイル痕跡調査
- Webメールの調査
 - Web履歴を利用したWebメール利用痕跡の確認 (URL文字列の確認)
 - レジストリ (TypedURLs) を利用したWebメール利用痕跡の確認 (URL文字列の確認)
 - アイコン画像を利用したWebメール利用痕跡の確認
 - Windows Search
 - インデックスにおけるWebメール利用痕跡の確認
 - Volume Shadow Copy内Web履歴の調査
 - 未利用領域におけるWeb履歴の復元と調査
 - 未使用領域におけるWebメール痕跡の調査 (文字列痕跡)
 - ブラウザセッションリカバリファイルの調査
- Webメール添付ファイルの調査
 - Web履歴ファイルに対する添付ファイル文字列痕跡の検索
 - 未使用領域におけるWeb履歴/添付ファイル文字列痕跡の検索
- メモリーメージ内のWebメール痕跡調査
 - メモリーメージ内のブラウザプロセス空間の抽出
 - ブラウザプロセスデータ内における文字列検索 (ファイル名痕跡)
 - ブラウザプロセスデータ内におけるファイル取り扱い情報の調査

文書ファイル

外付けデバイス

- USBデバイスの接続利用の調査
 - レジストリ (USBSTOR) の痕跡調査
 - Volume Shadow
 - Copy内レジストリ (USBSTOR) の痕跡調査
 - デバイス接続ログ (setup.dev.log) の調査
- ショートカットファイルの調査
 - ユーザのホームディレクトリのRecentフォルダを調査
 - LNKファイル内における外付けデバイス参照の痕跡調査
 - 未使用領域におけるLNKファイル内の痕跡調査 (ObjectID)
 - Volume Shadow
 - Copy内のLNKファイル調査
- ファイル名痕跡の調査
 - 外付けデバイス上を示す対象ファイル名文字列痕跡の検索
 - レジストリ (MRU) のファイル名痕跡の調査
 - Volume Shadow
 - Copy内レジストリ (MRU) の痕跡調査
- 携帯デバイスの調査
 - PC上のバックアップファイルの調査

電子メール

- 電子メールデータの調査
 - 削除メールの復元
 - Volume Shadow
 - Copy内メールボックスの調査
 - VSS内メールボックスと現メールボックスの差異調査
 - 未使用領域における削除メール痕跡の調査 (添付ファイル名)
 - 電子メールに対するキーワード検索
 - PST, DBX, mboxファイル内の
 - 未使用領域に対するキーワード検索
 - 欠落状態にあるメール (スレッド) の検出
- 電子メール添付ファイルの調査
 - 保護された添付ファイルの検出と抽出
 - 圧縮ファイルを含む添付ファイルに対するキーワード検索
 - 添付ファイルの抽出とファイルシグネチャ分析
 - ファイルタイプの識別と分類 (画像等の選別)
 - レジストリファイル (MRU) におけるファイル名痕跡の調査
- メモリーメージ内の電子メール痕跡調査
 - メモリーメージ内の電子メールプロセス空間の抽出
 - 電子メールプロセスデータ内における文字列検索 (ファイル名痕跡)
 - 電子メールプロセスデータ内におけるファイル取り扱い情報の調査