nuix Training

NUIX WINDOWS INVESTIGATIONS

nuix

Simple. Powerful. Precise.

NUIX WINDOWS INVESTIGATIONS

中級者向け　３日コース

「NUIX Windows Investigations」は、研修室内で行われる 3 日間のコースであり、Nuix Investigator を使用したことのある調査官の方向けです。Nuix Investigator やサードパーティ製のツールを使用して、Microsoft Windows に関連するデータの特定、分析、レポートを行うための先進的な内容を習得できます

本研修は、レジストリ、ゴミ箱、直近のアイテム、ユーザディレクトリ、システムフォルダに Windows（XP から 8 まで）がどのように情報を保存しているかを説明します。その内容には、電子メールを詳細に分析し、どのように特定、ソート、検索、重複除去するかも含まれています。また、Internet Explore が、履歴、Cookie、一時ファイルやユーザ設定をどのように保存しているかを学んだり、リンクファイル、プリフェッチファイル、ファイルのメタデータ、Word 文書やイメージの詳細な内容を学んだりします。

参加者は３日で以下のことを学びます

- Nuix Investigator のインタフェースと機能
- Windows 7、Windows 8 のディスク上のデータ構造やセキュリティ機能
- ゴミ箱、削除ファイルやメタデータのリカバリ方法
- Windows イベントログの閲覧、分析
- リンクやジャンプファイルの調査
- 電子メールの処理、ソート、検索、タグ付け
- Windows レジストリ調査、レジストリファイルから関連情報の抽出
- Internet Explore から履歴の抽出
- メタデータの定義、及び Nuix がどのようにメタデータを処理するのかの理解
- Windows 環境でのプリフェッチ機能やフォレンジックについて

本研修では、複数の実習ケースが含まれており、学んだことをすぐに実践に投入することができます。

参加の前提要件

本研修の内容を最大限に活用するためには、以下の要件を満たしている方を推奨します。

- PC の基本操作ができる方
- Microsoft Windows 環境に慣れている方
- フォレンジックの経験が 6 ヶ月以上ある方

コース概要

モジュール 1 ：イントロダクション

- 自己紹介
- コース概要
- Nuix の構成
- インストール

モジュール 2 ：Nuix の概要

- Nuix のケース作成
- シンプルケースとコンパウンドケース
- 検索、タグ、エクスポート、レポート

モジュール 3 ：Windows のフォルダ構造

- ファイルの配置
- シンボリックリンク
- セキュリティ機能
- Windows のライブラリ

モジュール 4 ：ゴミ箱

- ゴミ箱の機能や設定
- Windows XP の INFO2 ファイル
- $Recycle.Bin フォルダ
- レジストリの設定

モジュール 5 ：イベントログ

- イベントログのタイプ
- プロセシングログと内容の閲覧
- 特定のイベントタイプの調査

モジュール 6 ：リンクファイル/ジャンプファイル

- Windows ショートカットの概要
- リンクファイルとジャンプリスト
- 分散リンクトラッキングサービス
- ファイルシステム
- Windows 8 イマーシブアプリケーションのリンクファイル

モジュール 7 ：電子メール

- メールボックス処理
- 電子メールのメタデータ
- 添付の特定および処理
- 電子メールのソート、スレッド化、重複
- 電子メールの視覚化、レポート化

モジュール 8 ：レジストリの基礎

- レジストリの概要
- NT のレジストリファイル
- レジストリ解説
- SAM、システム、ソフトウェアとの関連

モジュール 9 ：Internet Explore

- Internet Explore のファイル配置
- キャッシュデータの調査
- ユーザ設定や履歴
- レジストリに関連するデータ

モジュール 10 ：メタデータ

- メタデータ概要
- ファイルシステムや MS Word のメタデータ
- EXIF データ
- Nuix でのメタデータ検索

モジュール 11 ：プリフェッチとスーパーフェッチ

- プリフェッチの概要と設定
- プリフェッチファイル
- Layout.INI ファイル

AOS リーガルテック株式会社

住所： 東京都港区虎ノ門 5-13-1 虎ノ門 40MT 森ビル 4F

電話： 03-5733-5790 FAX: 03-5733-7012

URL： http://www.aos.com/nuix_training/