nuix Training

NUIX FOUNDATIONS – INVESTIGATIONS

nuix

Simple. Powerful. Precise.

NUIX FOUNDATIONS-INVESTIGATIONS

中級者向け　３日コース

「NUIX Foundations - Investigations」は、研修室内で行われる 3 日間のコースです。Nuix Investigator を使用して、ケースの作成、データファイルのプロセシング、エビデンスの分析を行い、検査官にとってより実践的に Nuix の機能を習得することができます。

参加者は、調査ケースを作成するための全ての手順や、多様な非構造化データのフォーマットやフォレンジックイメージを抽出するための数多くの処理オプションを学びます。Nuix のツールで利用可能な検索、フィルター、タグ付け、ビジュアライゼーション、レポート出力の機能を学びます。先進的な内容として、シームレスにデータボリュームを間引くために使用される Ruby スクリプトの機能についても説明します。

本研修の最後には、Nuix Visual Analytics を使用して、タグ付け、エクスポート、レポート作成を行うためのタイムラインやジオタグの生成を行います。

参加者は３日で以下のことを学びます

- Nuix の構成オプションの理解
- Nuix Investigator のインストールと設定
- ケース生成オプションと MIME タイプの設定
- メタデータプロファイルとフィルタリング機能の定義
- メニューの機能とデータビューのオプション
- マイクロソフト系ファイル、画像ファイル、Web キャッシュ、Windows 上で扱われる典型的なファイルの分析
- ファイルデータやメタデータに対して基本的及び先進的な検索
- エンティティや近似機能について
- Nuix Visual Analytics を利用した What/Where/When/Who 分析
- Nuix のスクリプト機能の確認、及びケースデータに対して基本的なスクリプトの作成
- エクスポートのオプション及びレポーティング機能

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
- Nuix の歴史
- Nuix テクノロジーの概要
- エビデンスの抽出オプション
- 製品サポートチャネル
- インストールのオプション

モジュール２：データの処理-ケース作成

- Nuix の構成
- Nuix のケース作成
- シンプルケースとコンパウンドケース
- エビデンスファイルの追加
- ファイル抽出時のプレフィルタリング
- Nuix のログ

モジュール３：データの分析 – パート１

- カストディアンの管理
- Nuix デスクトップの概要
- Nuix タブ＆メニューの機能
- デスクトップのナビゲーション
- フィルタリングのビュー
- 検索結果ペイン
- レビューペイン

モジュール４：データの分析 – パート２

- データ分析およびデータの間引き（カリング）
- カスタムメタデータのプロファイル
- 対象外とするアイテムの選別
- アイテムのチェック
- アイテムのタグ付け
- コメントの追加
- データのエクスポート
- 組み込み済のフィルター機能
- ハッシュリストと重複排除

モジュール５：Windows 関連ファイルの処理

- レジストリ、画像、オフィス文書、メール、ゴミ箱

モジュール６：エンティティ

- エンティティの確認
- 正規表現の基礎
- 組み込み済のエンティティ
- エンティティの結果確認
- カスタマイズしたエンティティの作成

モジュール７：Nuix での検索

- 基本的なキーワード検索
- 先進的な検索方法
- 正規表現
- 近似 – シングル

モジュール８：Nuix でのスクリプト

- スクリプトとは
- スクリプトの適用範囲
- スクリプトの構成
- スクリプト API の紹介
- スクリプトの基本概念
- スクリプトの作成

モジュール９：Nuix Visual Analytics

- Nuix Visual Analytics の起動
- データセットの検索
- タグ付けやエクスポートのオプション
- NVA レポートのオプション

モジュール 10：エクスポート・レポート機能

- エクスポートするためのタグ付けされたアイテムの準備
- エクスポートのオプション
- メタデータプロファイルの適用
- レポートのオプション
- ケースの情報レポート
- Windows 関連ファイルのレポート
- MS-Office ドキュメントのレポート
- レジストリのレポート
- イベントマップのレポート
- ネットワーク図のレポート

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/