

Nuix Investigator Lab

巨大なボリュームのデジタル証拠を迅速に処理するために

Nuix Investigator Lab は、1日にテラバイト級のデータを迅速に抽出・処理し、解析しなければならないような専門調査機関向けの製品です。

国際カルテル調査など、多数の捜査官や調査の専門家が、実際に調査を行う際、Nuix Investigator Lab のセキュアなリモートアクセス機能、広範囲なレポートの機能を使用しています。

Nuix Investigation Lab は、証拠データのコレクション機能や、PC上で操作できる Nuix Investigator Workstation のライセンス、および 5 つの Reviewer のライセンスも含まれています。Nuix Web Review & Analytics のライセンスを追加することも可能です。

Nuix Investigator Lab の特長

豊富なフォレンジック機能

以下の機能を含む、パワフルなフォレンジック機能を提供します。

- Microsoft Windows レジストリの分析
- ログファイルやデータベースの解析
- 削除ファイルの復元、および、ファイル修復
- バイナリ形式のビューア (hex viewer) を使用した、より深いフォレンジック解析
- Windows, Mac OS HFS+, HFSX, Linux ファイルシステムの解析機能

Portable Collection

データの収集ツールを提供します。

- 各場所に散らばっているデジタル証拠を収集
- 収集したものをオフィスに持ち帰り、既存のケースにシームレスにマージ

全ての証拠データを即座に解析

以下のデータを抽出可能です

- ルースファイル (個別ファイル) やフォルダ
- シングルユーザ用 E-Mail データベース (PST, OST, NSF, mbox)

- マルチユーザ用 E-Mail データベース (EDB, Domino, Groupwise)
- dd, EnCase E01 および L01, Access Data AD1 を含むフォレンジックイメージ
- Mac OS Parallels, Microsoft Virtual Server および VMware virtual disk イメージ
- Microsoft SharePoint
- Cellebrite, Micro Systemation XRY, および Oxygen Forensic イメージ
- Gmail や Office365 のようなクラウドメールサービス
- Microsoft SQL Server

コンテンツベースのフォレンジック

複雑なデータマネージメント、分析およびフォレンジックのテクニックを支援し、重大な事実が浮かび上がるまで最もクリティカルな証拠データに焦点を絞ることができます。

機密情報の抜き出し、相互関連付け

複数のデータソースから、自動的に名前、会社、お金や他の個人情報のような機密情報を抜き出し、相互参照を行い、隠れていた関係性を浮かび上がらせます。

強力なビジュアル解析

ネットワークダイアグラム、タイムラインや、日付ごとのチャートを含んだツールを提供し、データをビジュアル化します。それにより、大量で複雑な証拠データから、容易にトレンドを発見したり、異常を特定したりすることができます。

法執行機関や政府機関向けの価格体系

Nuix Investigator Lab は、法執行機関や政府機関向けとして開発された経緯があり、大幅なディスカウント価格で提供しています。

お問い合わせ先

AOS リーガルテック株式会社

〒105-0001 東京都港区虎ノ門5-13-1 虎ノ門4 OMT森ビル 4F

URL: <http://www.aos.com>

Email: nuix@aos.com

Tel: 03-5733-5790 Fax: 03-5733-7012

Nuix Investigator Lab と Investigator の違い

Nuix Investigator と Lab は、強力な Nuix プラットフォームで動作するソフトウェアです。どちらも、非構造化データを事実上、無制限の容量に対して、より速く検索するためのインデックスを Nuix の特許取得済みの並列処理エンジンにより作成します。Lab を利用することで、一日あたりにテラバイト級の証拠データを処理することができ、複数の調査員が同時に利用できます。

Investigator の特長

- Nuix Workstation – Nuixエンジンのすべての機能を利用可能です
- スピードとスケール – 1 ライセンスで20ギガバイト/時のスピード。1 台のPCで最大4つのコアプロセッサで処理を行います。
- 100レベルまで検索可能なファイルを作成して抽出します。
- 複合ケース–複数のシンプルなケースから特定のケースの幅広い状況を把握するために、証拠を加えて、複合的なケースを作成することができます。
- ファイルタイプ–メジャーなメールソフトや他言語を含む400以上のファイルタイプをサポートしています。
- クラウドコレクション–クラウドやメールアーカイブからデータを収集し、処理できます。
- インテリジェント検索–シンプル、あるいは、複雑な検索でメタデータや個人データなどを調べることができます。
- ファイルタイプによる選択–最も関心の高いフォーマットにフォーカスするために、必要なファイルタイプを選択し、除外ファイルタイプを設定できます。
- レジストリ分析、削除ファイルの復元、破損ファイルの抽出、バイナリ表示、フォレンジックイメージの抽出など高度なフォレンジック機能を持っています。
- 証拠を抽出し、結び合わせる–名前や社名、金額、メールアドレス、IP アドレス、URL、クレジットカード番号などの情報を自動的に抽出し、相互に参照できます。
- ネットワークダイアグラムやタイムライン、チャートなどでビジュアルな分析ができます。
- 具体的な調査内容やディスカバリー情報が含まれるようにメタデータをカスタマイズすることができます。
- 不適切な画像を識別するために、肌の色調を分析。
- 地図上に位置をプロットするため写真に含まれるGPS情報やIPアドレスを使います。
- 文書ファイル、メールなどの中から、重複ファイルや重複ファイルに近いファイルを識別します。
- 通信記録を分析するため、CellebriteやMicro Systemation社のXRYからイメージデータを読み込むことができます。
- Mac OSのHFS+やHFSX、Linuxファイルシステムを分析できます。

Investigator Lab の特長

- スピードとスケール – 1 台のサーバで最大16コアのプロセッサまで処理を行え、1 ライセンスで85ギガバイト/時のスピード。
- 5つまでのレビューとエクスポートライセンス。同時に5人の調査官が同一の場所かセキュアな環境の遠隔地で共同レビューを行うことができます。
- 弁護士やその分野の専門家などが外部からアクセスすることができます。
- パソコンや共有ファイルから証拠データを収集するため、最小限のトレーニングで使えるNuix Collector portableを最大5ライセンスまで使用できます。このツールは、現場でデータ収集作業を行う前に、収集対象のデータを事前に設定することができます。
- ネットワーク上に分散している大量のデータから必要なデータを収集できるNuix Network collectorを最大5ライセンスまで使うことができます。
- マイクロソフトのSharePointから迅速、かつ、安全に証拠データを収集できるNuix SharePoint Collectorを利用できます。
- 現場やネットワーク経由で収集したデータは、ケースファイルに格納して、深い分析を行うことができます。
- 管理サーバー一つのサーバドングルで複数ユーザが利用できます。必要とするライセンスの種類を選択して、新規ユーザが必要とするライセンスを管理することができます。
- 同時に複数のユーザがアクセスできるように、Nuixサーバは、インデックス付きのケースを配置できます。
- ライセンスを管理するユーザとケースへアクセスできるユーザは、別々に管理することができます。