SUMURI

RECON LAB

FORENSIC SUITE

評判はすべてです。
私たちはあなたがそれを保つのを手助けします。
Reputation is everything.
We help you keep it.

RECON LABは、SUMURIのフラッグシップな法的解析スイートであり、macOS上で完全に構築され、Macのパワーを活用し、鑑識官が完全に新しいデータ領域にアクセスできるように設計されています。RECON LABは、ネイティブなmacOSライブラリを使用し、解析とレポート作成の両方に順次処理を行い、さまざまなオペレーティングシステムの完全自動処理など、21世紀のテクノロジーに合わせた多くの独自かつ革新的な機能を備えて、従来のコンピュータフォレンジックを活性化させています。

RECON LAB is SUMURI's flagship forensic analysis suite designed from the ground up on macOS to utilize Mac's power and give examiners access to an entirely new realm of data. RECON LAB takes traditional computer forensics and revitalizes it to be more in line with 21st century technologies through many unique and revolutionary features using native macOS libraries, sequential processing into both analysis and reporting, fully automated processing of many different operating systems, and much more.

SUMURIは、あらゆるタイプの鑑識官を考慮してRECON LABを設計しました。分析へのアプローチは3つの段階に分かれており、新人鑑識官から経験豊富なベテランまで、正確な結果を迅速に得ることができます。ステップ1は自動化された分析であり、macOS、Windows、iOS、Android、Google Takeoutからの数千のアーティファクトの自動解析をサポートしています。ステップ2は、高度なフォレンジックビューアを使用したセミ自動化された分析であり、macOSのプロパティリスト、SQLiteデータベース、Windowsレジストリ、および生データの解析と検査を支援します。ステップ3では、StoryBoardレポートを使用した順次処理とWYSIWYGレポート機能が含まれています。RECON LABには、数百もの革新的な機能が組み込まれており、手動分析を容易にします。

SUMURI designed RECON LAB with every type of examiner in mind. Our three-stage approach to analysis makes sure that brand new examiners and seasoned veterans alike can get accurate results fast. Step One is automated analysis that supports the automated parsing of thousands of artifacts from macOS, Windows, iOS, Android, and Google Takeout. Step Two is semi-automated analysis using our advanced forensic viewers that assist in parsing and examining macOS Property Lists, SQLite Databases, Windows Registry and Raw Data. Step Three includes Sequential Processing and WYSIWYG reporting features through the use of StoryBoard reporting. Hundreds of revolutionary features built into RECON LAB makes manual analysis easier.

- macOS固有の機能
  Native to macOS
- macOSネイティブライブラリを使用して、Appleの拡張属性とAppleのタイムスタンプを正しく利用します。
  Correctly Uses Apple Extended Attributes and Apple Timestamps with macOS Native Libraries
- macOS、Windows、iOS、Android、Google Takeoutの自動化された分析
  Automated Analysis of macOS, Windows, iOS, Android, and Google Takeout
- 順次処理（タイムライン分析）
  Sequential Processing (Timeline Analysis)
- StoryBoard - 画期的なWYSIWYGフォレンジックレポート
  StoryBoard - First of its Kind WYSIWYG Forensic Reports

SUMURI.COM