RECON LAB

SUMURI

Reputation is everything.
We help you keep it.

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 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.

- Native to macOS
- Correctly Uses Apple Extended Attributes and Apple Timestamps with macOS Native Libraries
- Automated Analysis of macOS, Windows, iOS, Android, and Google Takeout
- Sequential Processing (Timeline Analysis)
- StoryBoard - First of its Kind WYSIWYG Forensic Reports

RECON LAB

FORENSIC SUITE

NATIVE TO macOS

RECON LAB is developed natively on macOS and utilizes native Mac libraries to offer the most accurate representation of acquired data. These native features allow RECON LAB to display Apple Extended Attribute data with the proper macOS Timestamps missed by other forensic tools. Being designed on macOS allows RECON LAB to include a unique Hybrid Processing Engine, enabling images to be mounted and processed faster than other tools. Combining these attributes and our automated analysis functions creates one of the world's most powerful forensics suite.

CORRECT USE OF APPLE EXTENDED ATTRIBUTES

RECON LAB stands alone to integrate and support Apple Extended Attributes and proper macOS Timestamps fully. This unique and Mac-native form of metadata supports hundreds of extended attributes that can completely change a case's outcome and provide unparalleled information to examiners. Other forensic tools overlook this data, while RECON LAB makes these an essential part of the tool. RECON LAB utilizes Apple Extended Metadata, POSIX, and application-specific timestamps to give examiners as much information as possible.

AUTOMATED ANALYSIS OF macOS, WINDOWS, iOS, ANDROID, AND GOOGLE TAKEOUT

RECON LAB automates the analysis of thousands of supported artifacts, spanning macOS, Windows, iOS, Android, and Google Takeout! Simply by loading a forensic image, folder, or backup and selecting the plugin will pull all associated data and present it in an easy-to-understand format.

SEQUENTIAL PROCESSING (TIMELINE ANALYSIS)

RECON LAB features two unique ways to display information sequentially with Super Timeline and Artifact Timelines. Super Timeline generates global level timelines in a CSV or SQLite database to show all events as they transpired. Meanwhile, the Artifact Timeline visually represents events based on the timestamps collected through automated analysis. Both can provide a way to present the collected data visually to significantly reinforce case opinions.

STORYBOARD

RECON LAB's revolutionary reporting feature, StoryBoard, features many innovations to automate and enhance the reporting process. StoryBoard includes features to add bookmarked files in chronological order and include external files to help make the report more coherent. RECON LAB includes the first of its kind revolutionary WYSIWYG forensic report editor - StoryBoard. With StoryBoard's report editor, examiners can fully customize and tailor their reports to provide the most comprehensive, user-friendly, and coherent reporting experience of any tool on the market.

ABOUT SUMURI

SUMURI is a leading worldwide provider of solutions for digital evidence and computer forensic Training, Hardware, Software, and Services. SUMURI is also the developer of the industry standard PALADIN Forensic Suite, CARBON Virtual Forensic Suite, RECON *ITR*, RECON LAB, and TALINO Forensic Workstations.

sales@sumuri.com
+1 302.570.0015

Our Mailing Address:
P.O. Box 121 Magnolia,
DE 19962, USA