

UN SINFÍN DE INNOVACIONES





QUIENES SOMOS

SUMURI

SUMURI es una premiada empresa dedicada a la informática forense ubicada en el estado de Delaware en los Estados Unidos.

SUMURI comenzó a servir la comunidad de la informática forense en julio del 2010 al ser fundada por Steve Whalen, un Examinador Forense Certificado y policía estatal retirado, junto con su esposa Ailyn. SUMURI se destaca por su desarrollo de programas y equipos de informática forense innovadores y previsores y por ofrecer formación y servicios expertos de la informática forense.

Los valores fundamentales de SUMURI son el honor, la integridad, la lealtad, mantener una actitud positiva, la dedicación, y, por encima de todo, el altruismo; el deseo de ayudar, servir y cuidar a los demás antes que a uno mismo.

Consideramos que nuestros valores fundamentales, junto a nuestros conocimientos especializados, son el motor de nuestro éxito. Nuestro equipo está compuesto por expertos conocidos por sus continuas contribuciones a la comunidad de la informática forense.



La reputación lo es todo. Le ayudamos a protegerla.

RECON LAB es el paquete de análisis forense emblemático de SUMURI, diseñado desde cero en macOS para aprovechar el poder del Mac y dar acceso a los examinadores a un mundo de datos completamente nuevo. **RECON LAB** toma la informática forense tradicional y la revitaliza para así alinearla con las tecnologías del siglo XXI a través de muchas funciones únicas y revolucionarias utilizando librerías nativas macOS, el procesamiento secuencial para el análisis y la generación de informes, el procesamiento automatizado de muchos sistemas operativos diferentes, y mucho más.

SUMURI diseñó RECON LAB con todo tipo de examinador en mente. Nuestro planteamiento de tres fases al análisis asegura que tanto los nuevos examinadores como los veteranos experimentados puedan obtener resultados precisos rápidamente. La primera fase es el análisis automatizado que soporta al rastreo automático de miles de artefactos de macOS, Windows, iOS, Android y Google Takeout. La fase dos es el análisis semiautomatizado con nuestros visualizadores forenses avanzados que ayudan a rastrear e inspeccionar las listas de propiedades macOS, bases de datos SQLite, Windows Registry, y datos brutos. La fase tres incluye funciones de procesamiento secuencial y generación de informes WYSIWYG a través del uso de generación de informes StoryBoard. Los cientos de funciones revolucionarios incorporados a RECON LAB hace más fácil el análisis manual.



Nativo al macOS



Utiliza de forma correcta los atributos extendidos Apple y marcas de tiempo Apple con librerías nativas macOS



Análisis automatizado de macOS, Windows, iOS, Android, y Google Takeout



Procesamiento secuencial (Análisis de cronograma)



Storyboard: solución pionera de generación de informes forenses



RECON LAB

FORENSIC SUITE



Nativo al macOS

RECON LAB se desarrolló de forma nativa en macOS y usa librerías nativas Mac para realizar la representación más fiel de datos adquiridos. Estas funciones nativas permiten a RECON LAB presentar datos de Atributos Extendidos Apple con las marcas de tiempo de macOS correctos que escapan de otras herramientas forenses.

Ser diseñado en macOS permite a RECON LAB contar con un motor de procesamiento híbrido, lo cual permite montar y procesar las imágenes más rápidamente que con otras herramientas. Estos atributos, junto a nuestras funciones automatizadas de análisis crean uno de los paquetes de informática forense más potentes del mundo.

USO CORRECTO DE ATRIBUTOS EXTENDIDOS APPLE

RECON LAB se distingue por su capacidad de integrar y soportar los atributos extendidos Apple y las marcas de tiempo correctos macOS de forma completa. Este tipo único de metadatos Mac nativos soporta cientos de atributos extendidos que pueden cambiar completamente el resultado de un caso y proveer información sin igual a los examinadores forenses. Otras herramientas forenses hacen caso omiso a este tipo de datos; en cambio RECON LAB los hace una parte integral de la herramienta. RECON LAB utiliza metadatos extendidos Apple, POSIX, y marcas de tiempo específicas a las aplicaciones para proveer la máxima cantidad de información posible a los examinadores.

ANÁLISIS AUTOMATIZADO DE MACOS, WINDOWS, IOS, ANDROID Y GOOGLE TAKEOUT

RECON LAB automatiza el análisis de miles de artefactos soportados, abarcando macOS, Windows, iOS, Android y Google Takeout. Con simplemente cargar una imagen, archivo, o copia de respaldo forense y seleccionar el complemento, se podrá recoger todos los datos relacionados y presentarlos en un formato fácil de entender.

PROCESAMIENTO SECUENCIAL (ANÁLISIS DE CRONOGRAMA)

RECON LAB cuenta con dos formas únicas para presentar la información de forma secuencial con Super Timeline y Artifact Timelines. Super Timeline genera cronogramas a nivel global en una base de datos CSV o SQLite para mostrar todos los eventos según ocurrieron. Por otro lado, el Artifact Timeline representa los eventos de forma visual basado en las marcas de tiempo recogidas por el análisis automatizado. Las dos formas ofrecen un modo de presentar los datos recopilados visualmente para reforzar de forma significativa las opiniones sobre los casos.

STORYBOARD

Storyboard, el programa de generación de informes revolucionaria de RECON LAB, cuenta con muchas innovaciones para automatizar y mejorar el proceso de generación de datos. StoryBoard incluye funciones para añadir archivos marcados en orden cronológica e incluir archivos externos para hacer más coherente el informe. RECON LAB incluye el revolucionario editor de informes WYSIWYG-Storyboard. Con el editor de informes de StoryBoard, los examinadores pueden configurar sus informes a medida para lograr la experiencia de generación de informes más comprehensiva, más intuitiva, y más coherente que cualquier otra herramienta en el mercado.

CONTÁCTANOS

✉ info@hansgross.com.pe

🌐 www.hansgross.com.pe

📞 (+51) 971 596 045

☎ (044) 467335

📷 [f](#) [X](#) [in](#) /hansgrossperu

sales@sumuri.com

+1 302.570.0015

Nuestra Dirección de Correo:

P.O. Box 121 Magnolia,
DE 19962, USA