Análisis Forense con Autopsy

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético & Forense Digital

Sitio Web: https://www.reydes.com -:-: e-mail: reydes@gmail.com

Miércoles 27 de Octubre del 2021

Alonso Eduardo Caballero Quezada

EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator Certified, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures Pen Testing, Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist y OSEH.

Más de 18 años de experiencia como consultor e instructor independiente en las áreas de Análisis Forense con Autopsy y Forense Digital. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Análisis Forense con Autopsy, Forense Digital, GNU/Linux.

Redes Sociales

https://www.linkedin.com/in/alonsocaballeroquezada/

https://twitter.com/Alonso_ReYDeS

https://www.youtube.com/c/AlonsoCaballero

https://www.facebook.com/alonsoreydes/

https://www.reydes.com

reydes@gmail.com

+51 949 304 030

¿Qué es el Forense Digital?

Rama de la ciencia forense abarcando la recuperación e investigación de material encontrado en dispositivos digitales, frecuentemente relacionados con crímenes cometidos por computadoras.

El Forense de computadoras es una rama del forense digital, relacionado a la evidencia encontrada en computadoras y medios digitales de almacenamiento.

Su meta es examinar medios digitales de una manera “forense”, con el propósito de identificar, preservar, recuperar, analizar, y presentar hechos sobre la información digital.

El análisis forense es la etapa donde se realiza una investigación profunda, cuyo propósito es identificar objetivamente y documentar los culpables, razones, ruta y consecuencias de un incidente de seguridad, violación de las leyes, etc.

¿Cómo se Utiliza?

Debido a la variedad de las fuentes de datos, las técnicas del forense digital pueden ser utilizados para diversos propósitos.

- Investigar crímenes y violaciones a políticas internas
- Reconstruir incidentes de seguridad por computadora
- Resolver problemas operacionales
- Recuperar daños accidentales en los sistemas

Prácticamente toda las organizaciones necesitan tener la capacidad de realizar forense digital.

Autopsy

Autopsy es la principal plataforma de fuente abierta (open source) para forense digital. Construido por Basis Technology con las funcionalidades fundamentales esperadas de las herramientas forenses comerciales.

Autopsy es rápido, profundo, y eficiente para realizar investigaciones en dispositivos de almacenamiento (discos duros y dispositivos móviles), evolucionando conforme se tienen diversos requerimientos.

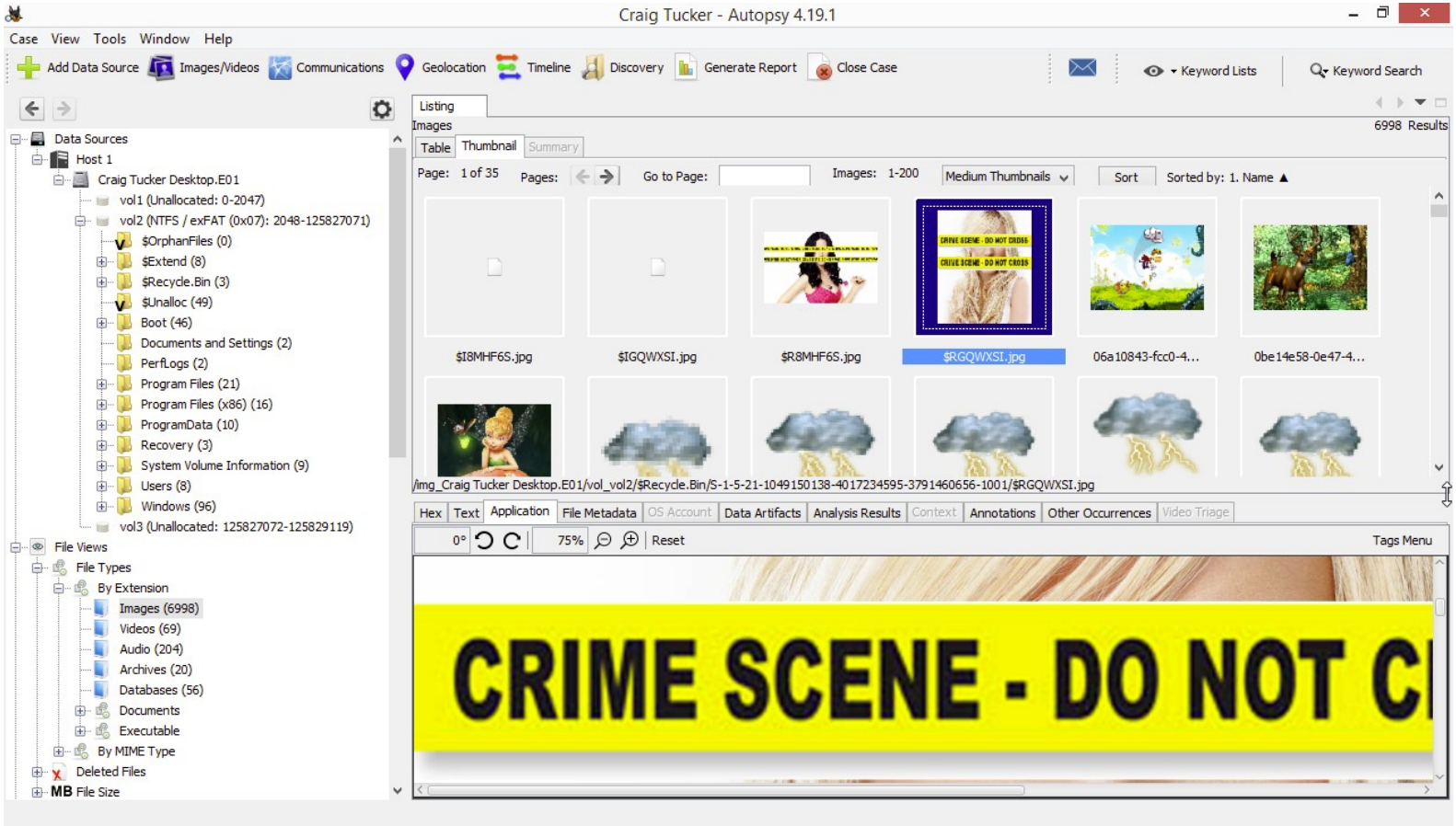
Autopsy es una interfaz gráfica para The Sleuth Kit, y otras herramientas del forense digital. Utilizado por fuerzas legales, militares, profesionales corporativos, con el propósito de investigar lo ocurrido en computadoras.

* https://www.autopsy.com/

Capacidades de Autopsy

- Actividad reciente
- Consulta de hashes
- Identificación por tipo de archivo
- Extracción de archivos
- Analizar imágenes
- Interpretar mensajes de correo electrónico
- Buscar palabras clave
- Detectar inconsistencias en la extensión de archivos
- Detectar archivos interesantes
- Reconstruir archivos
- Detectar encriptación
- Extraer máquinas virtuales
- Entre otras funcionalidades...

Demostración



Cursos Virtuales Disponibles Video

Curso Virtual de Análisis Forense con Autopsy
https://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Virtual de Hacking Aplicaciones Web
https://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web

Curso Virtual de Informática Forense
https://www.reydes.com/d/?q=Curso_de_Informatica_Forense

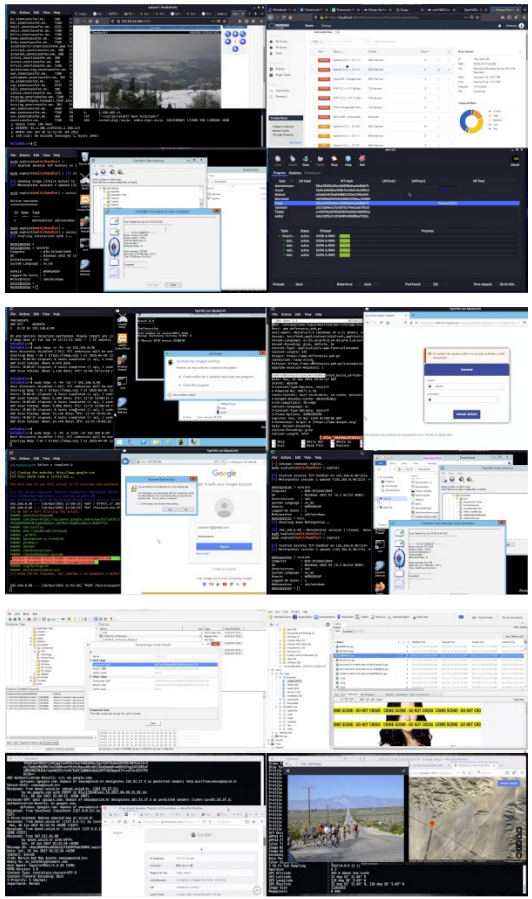
Curso Virtual Hacking con Kali Linux
https://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

Curso Virtual OSINT - Open Source Intelligence
https://www.reydes.com/d/?q=Curso_de_OSINT

Curso Virtual Forense de Redes
https://www.reydes.com/d/?q=Curso_Forense_de_Redes

Y todos los cursos virtuales:

https://www.reydes.com/d/?q=cursos



Más Contenidos

Videos de 70 webinars gratuitos

https://www.reydes.com/d/?q=videos

Diapositivas de los webinars gratuitos

https://www.reydes.com/d/?q=eventos

Artículos y documentos publicados

https://www.reydes.com/d/?q=documentos

Blog sobre temas de mi interés

https://www.reydes.com/d/?q=blog/1

Análisis Forense con Autopsy

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético & Forense Digital

Sitio Web: https://www.reydes.com -:-: e-mail: reydes@gmail.com

Miércoles 27 de Octubre del 2021