Forense con Autopsy

Domingos 16 y 23 de Julio del 2023. De 9:00 am a 12:00 pm (UTC -05:00)

Este curso virtual ha sido dictado a participantes residentes en los siguientes países:

Presentación

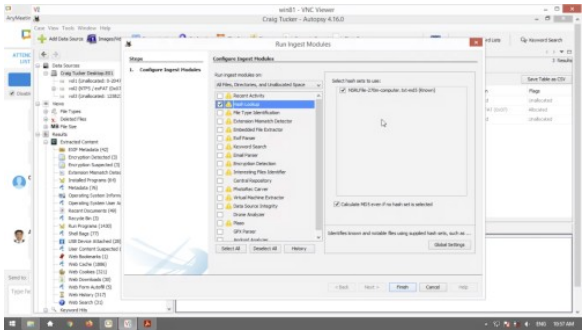
Autopsy es una plataforma forense digital de fuente abierta (Open Source) para sistemas Windows. La cual permite realizar investigaciones forenses contra dispositivos de almacenamiento como discos duros. Es utilizada por fuerzas del orden, militares, miles de investigadores y profesionales forenses alrededor del mundo. Autopsy ha sido diseñada para ser intuitiva, rápida, y ampliable, teniendo un gran apoyo de la comunidad open source. Autopsy es una plataforma constituida de módulos, los cuales proporcionan funcionalidades, como análisis de cronologías o líneas de tiempo, filtros por hashes, búsqueda de palabras clave, artefactos web, recuperación de datos, extractor multimedia, e indicadores de compromiso utilizando STIX.

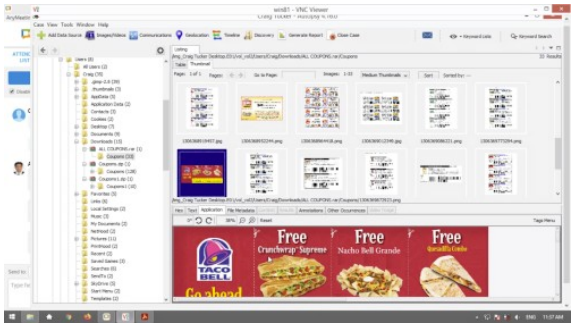
Objetivos

Este curso de Autopsy se basa en un caso forense práctico de estudio, mediante el cual se enseña la utilización de todas las funcionalidades incluidas en esta poderosa herramienta. Los participantes aprenderán a utilizar Autopsy para ejecutar una investigación forense sobre un dispositivo de almacenamiento de principio a fin, entendiendo las mejores prácticas forenses, utilizando la automatización y flujo de trabajo, aprovechando también los módulos de asimilación y búsqueda de palabras claves, como también las consultas de hashes, etiquetas, marcadores y finalmente la creación del reporte. Todo esto con el propósito de obtener los más óptimos resultados al utilizar Autopsy.

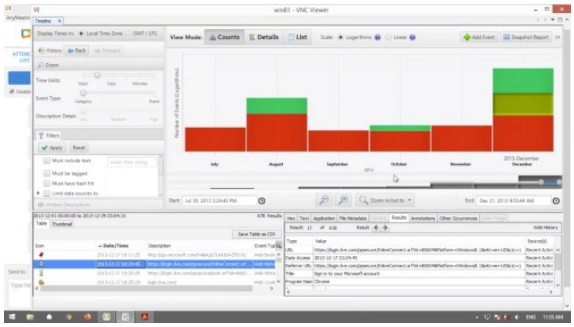
Temario

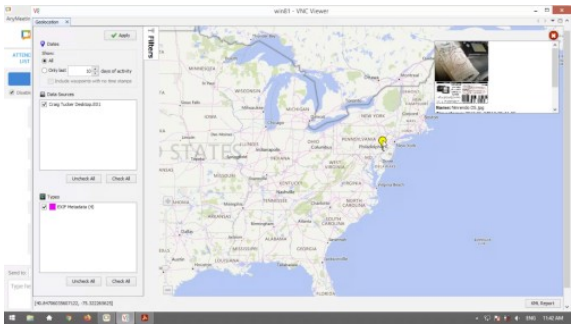
- Instalación de Autopsy
- Optimizar el Desempeño
- Guía de Inicio Rápido
- Casos y Añadir Fuentes de Datos
- Flujo de Trabajo de autopsy
- Casos
- Fuentes de Datos
- Ver Logs y Resultados del Caso
- Módulos de Asimilación
- Módulo de Actividad Reciente
- Módulo de Consulta en Base de Datos de Hash
- Módulo de Identificación por Tipo de Archivo
- Módulo de Extracción de Archivos Incorporados
- Módulo de Interprete EXIF
- Módulo de Búsqueda de Palabras Clave
- Módulo Interprete de Correo Electrónico
- Módulo Detector de Inconsistencia en Extensión
- Módulo de Integridad de Fuente de Datos
- Módulo Identificador de Archivos Interesantes

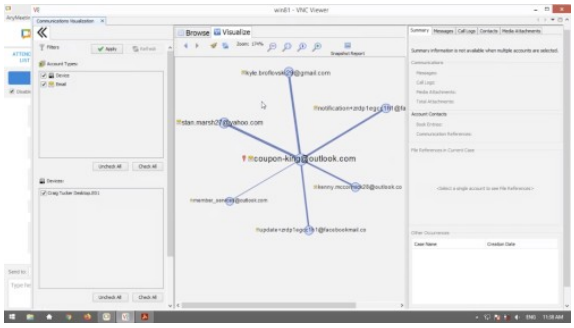




- Módulo de Reconstrucción con PhotoRec
- Módulo de Repositorio Central
- Módulo Detección de Encriptación
- Módulo Extractor de Máquina Virtual
- Plaso
- Revisar los Resultados
- Disposición de la Interfaz Gráfica
- Visor de Estructura de Árbol
- Visor de Resultados
- Visor de Contenidos
- Traducción de la Máquina
- Búsqueda
- Interfaz Gráfica para Búsqueda Rápida
- Búsqueda de Archivos
- Búsqueda de Palabras Clave Ad Hoc
- Búsqueda de Propiedades Comunes
- Buscar en todos los Casos
- Visores Especializados
- Módulo Galería de Imágenes
- Cronologías o Lineas de Tiempo
- Herramientas para Visualización de Comunicaciones
- Geolocalización
- Descubrimiento
- Personas
- Reportar
- Etiquetas y Comentarios
- Reportes
- Instalar Módulos de Terceros







Material

Todos los participantes al Curso Virtual Forense con Autopsy tendrán la posibilidad de descargar los videos de cada sesión, un día después de impartida la misma.

- **Autopsy 4.20.0**

  Enlace para Descarga: https://www.autopsy.com/download/

- **Data Leakage Case**

  Personal Computer (PC) - Imagen “DD”

  https://cfreds-archive.nist.gov/data_leakage_case/images/pc/cfreds_2015_data_leakage_pc.7z.001
  https://cfreds-archive.nist.gov/data_leakage_case/images/pc/cfreds_2015_data_leakage_pc.7z.002
  https://cfreds-archive.nist.gov/data_leakage_case/images/pc/cfreds_2015_data_leakage_pc.7z.003

Fechas y Horario

El Curso Virtual Fundamentos de Forense Digital tiene una duración total de seis (6) horas, las cuales se dividen en dos (2) sesiones de tres (3) horas cada una.

- **Fechas:**

  Domingos 16 y 23 de Julio del 2023

- **Horario:**

  De 9:00 am a 12:00 pm (UTC -05:00). 6 horas en total.

[*] El Curso se dicta sin ningún requisito mínimo en el número de participantes.

Inversión y Forma de Pago

Acceso a las sesiones en vivo, todos los videos y material:

S/. 175 Soles o $ 55 Dólares

Acceso a las sesiones en vivo, todos los videos, material, aula virtual por 30 días, evaluaciones, certificado de participación o certificado de aprobación.

S/. 260 Soles o $ 80 Dólares

El pago del curso se realiza mediante alguno de los siguientes mecanismos:

Residentes en Perú	Residentes en Otros Países
Deposito bancario o transferencia interbancaria en la siguiente cuenta: Scotiabank ScotiaBank Cuenta de Ahorros en Soles: 324-0003164 A nombre de: Alonso Eduardo Caballero Quezada CCI: 009-324-203240003164-58	Pago a través de PayPal. O también transferencia de dinero mediante Western Union y MoneyGram PayPal Escriba por favor un mensaje de correo electrónico a caballero.alonso@gmail.com para proporcionarle los datos pertinente para realizar el pago.

Confirmado el pago se enviará al correo electrónico del participante, los datos necesarios para conectarse hacia la plataforma, además de toda la información pertinente para su participación en el curso

El curso se realiza utilizando el sistema para video conferencias de nombre Anymeeting. El cual proporciona transmisión de audio y video HD en alta calidad, tanto para el instructor y los participantes, entre otras características ideales para el dictado de cursos virtuales o en línea.

INTERMEDIA ANYMEETING

Más Información

Para obtener más información sobre este curso virtual, tiene a su disposición los siguientes mecanismos de contacto.

Correo electrónico: caballero.alonso@gmail.com

Teléfono: +51 949 304 030

Sitio Web: https://www.reydes.com

Instructor

Alonso Eduardo Caballero Quezada. EXIN Ethical Hacking Foundation Certificate, 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, Ransomware Techniques, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS), OPEN-SEC Ethical Hacker (OSEH), Codered Certificate of Achievement: Digital Forensics Essentials (DFE) y Ethical Hacking Essentials (EHE). He sido instructor, expositor y conferencista en el OWASP LATAM Tour, OWASP Perú Chapter Meeting, OWASP LATAM at Home, PERUHACK, PERUHACKNOT, 8.8 Lucky Perú, Ekoparty University Talks Perú. Cuento con más de diecisiete años de experiencia en el área y desde hace trece años laboro como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital. Pertenecí por muchos años al grupo internacional RareGaZz y grupo Peruano PeruSEC. He dictado cursos para España, Ecuador, México, Bolivia y Perú, presentándome también en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux y Software Libre.