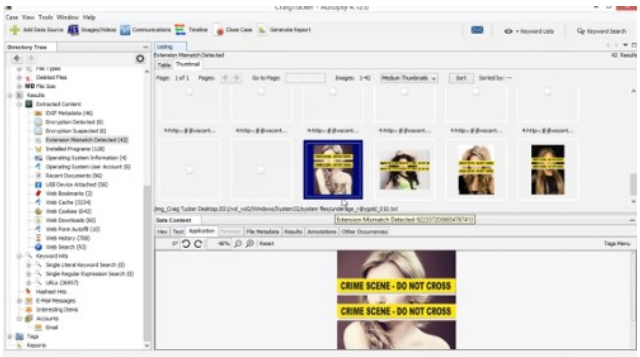
Forense con Autopsy

Curso Virtual - 2020



Único Curso del Año 2020

Fechas:

Sábados 19 y 26 de Setiembre del 2020

Horario:

De 9:00 am a 12:15 pm (UTC -05:00)

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

1. 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.

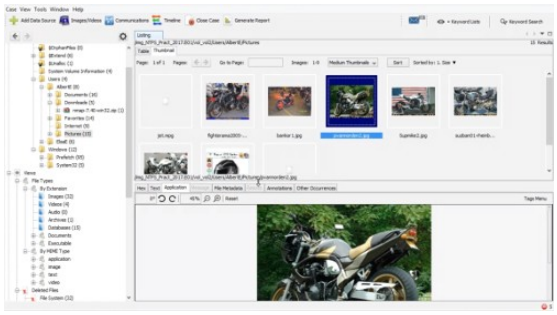
Autopsy es una plataforma constituida de módulos, los cuales proporcionan funcionalidades, como análisis de cronologías o líneas de tiempo, filtros por hashes, búsqueda de palabras clave, artefactos web, recuperación de datos, extractor multimedia, e indicadores de compromiso utilizando STIX.

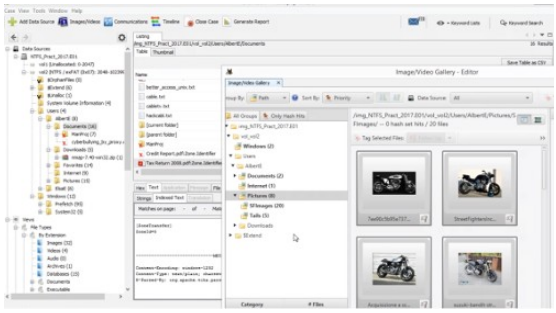
2. Objetivos:

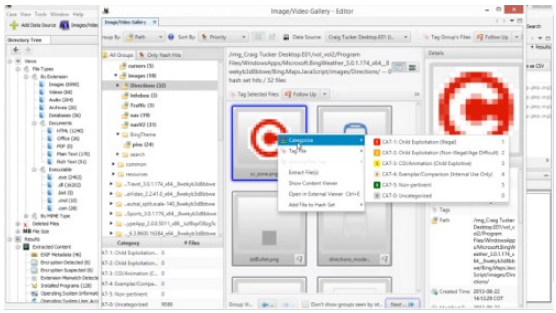
Este curso de Autopsy se basa en un caso forense práctico de estudio, mediante el cual se enseña la utilización de todas las funcionalidades incluidas en esta poderosa herramienta. Los participantes aprenderán a utilizar Autopsy para ejecutar una investigación forense sobre un dispositivo de almacenamiento 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.

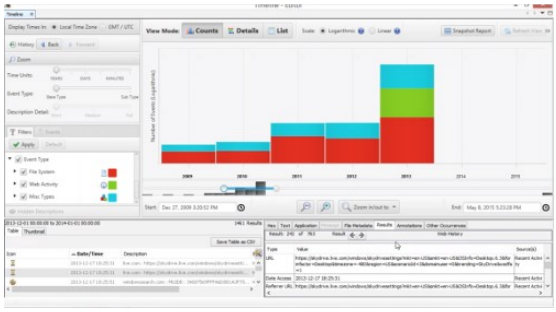
3. Temario:

- 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 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 Detección de Encriptación
- Módulo Extractor de Máquina Virtual
- 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
- STIX
- 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









4. Material:

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

Adicionalmente el participante tiene la opción de adquirir por S/. 50 Soles adicionales, Un (1) DVD conteniendo las máquinas virtuales utilizadas durante el desarrollo del curso. Este costo incluye los gastos de envío a cualquier lugar del Perú.

En caso el participante no adquiera el DVD, se le sugiere tener instalada la versión más reciente de Autopsy, además de descargar la imagen forense para desarrollar el curso.

- **Autopsy 4.15.0**

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

- **Data Leakage Case**

  Personal Computer (PC) - Imagen "DD"
  https://www.cfreds.nist.gov/data_leakage_case/images/pc/cfreds_2015_data_leakage_pc.7z.001
  https://www.cfreds.nist.gov/data_leakage_case/images/pc/cfreds_2015_data_leakage_pc.7z.002
  https://www.cfreds.nist.gov/data_leakage_case/images/pc/cfreds_2015_data_leakage_pc.7z.003

5. Día y Horario:

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

- **Fechas:**
  Sábados 19 y 26 de Setiembre del 2020

- **Horario:**
  De 9:00 am a 12:15 pm (UTC -05:00). 6 Horas en total.

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

6. Inversión y Forma de Pago:

El Curso Virtual Forense de Autopsy tiene un costo de

S/. 165 Soles o $ 50 Dólares

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

Residentes en Perú	Residentes en Otros Países
Deposito Bancario en la siguiente cuenta: ScotiaBank Cuenta de Ahorros en Soles: 324-0003164 A nombre de: Alonso Eduardo Caballero Quezada También puede realizar el depósito en un Agente Scotiabank. Encuentre el más cercano utilizando la siguiente página: https://intl.scotiabank.com/es-pe/locator/Default.aspx Una vez realizado el depósito, enviar por favor el voucher escaneado o sencillamente detallar los datos al siguiente correo: **caballero.alonso@gmail.com**	Transferencia o pago mediante Western Union o Moneygram, También mediante Paypal. Paypal: Escríbame por favor un mensaje de correo electrónico para detallarle los datos necesarios para realizar la transferencia o el pago. Una vez realizada la transferencia o el pago, enviar por favor el documento escaneado al siguiente correo: **caballero.alonso@gmail.com**

Confirmado el depósito o la transferencia se le enviará al correo electrónico del participante los datos necesarios para conectarse al sistema, además del material utilizado durante el desarrollo del curso.

El curso se realiza utilizando el sistema de video conferencias Anymeeting. El cual proporciona la transmisión de audio y video en tiempo real de alta calidad, tanto para el instructor como también para los participantes, entre otras características ideales para impartir cursos de manera virtual.

http://www.anymeeting.com

7. Más Información

Si requiere más información sobre el Curso Virtual Forense de Autopsy tiene a su disposición los siguientes mecanismos de contacto:

Correo electrónico: caballero.alonso@gmail.com

Vía Web: http://www.reydes.com

Celular: +51 949 304 030

8. Instructor

Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator, 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, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS) y OPEN-SEC Ethical Hacker (OSEH). Ha sido instructor en el OWASP LATAM Tour Lima, Perú del año 2014, expositor en el 0x11 OWASP Perú Chapter Meeting 2016 y OWASP LATAM at Home 2020, además de Conferencista en PERUHACK 2014, instructor en PERUHACK2016NOT, y conferencista en 8.8 Lucky Perú 2017. Cuenta con más de dieciséis años de experiencia en el área y desde hace doce años labora como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital. Perteneció por muchos años al grupo internacional de seguridad RareGaZz y al grupo peruano de seguridad PeruSEC. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux y Software Libre. Su correo electrónico es ReYDeS@gmail.com y su página personal está en: http://www.ReYDeS.com.