Curso Virtual Informática Forense 2021

Domingos 7, 14, 21 y 28 de Marzo del 2021. De 9:00 am a 12:15 pm (UTC -05:00)

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

Presentación

En la actualidad todas las empresas y organizaciones deben estar preparadas para enfrentar exitosamente diversos tipos de crímenes cibernéticos, los cuales se suscitan y afectan sus sistemas de cómputo y redes. Consecuentemente se ha incrementado la demanda por profesionales forenses debidamente entrenados y experimentados, quienes estén en la capacidad investigar crímenes cibernéticos relacionados a fraudes, amenazas internas, espionaje industrial, inadecuado uso de los empleados, e intrusiones hacia computadoras y redes Las agencias del gobierno a nivel mundial también requieren profesionales forenses debidamente entrenados y con amplia experiencia en el ámbito del forense digital.

Objetivos

Este curso enseña a los participantes a desarrollar un profundo conocimiento sobre forense digital aplicado al sistema operativo Microsoft Windows. Es fundamental comprender las capacidades forenses y artefactos en estos sistemas. Aprender a identificar, capturar, autenticar, y analizar datos forenses. Entender como se puede rastrear detalladamente la actividad realizada del usuario a través de la red, además de como organizar sus hallazgos para ser utilizado en una respuesta de incidentes, investigaciones internas, y litigios civiles o penales. Utilizar los nuevos conocimientos adquiridos para validar las herramientas de seguridad, mejorando las evaluaciones de seguridad, identificar amenazas internas, rastrear atacantes, y mejorar las políticas de seguridad. Aunque se conozca o no, el sistema operativo Windows silenciosamente registra una gran cantidad de datos sobre el propio sistema y los usuarios. Este curso enseña una metodología para forense de computadoras con etapas de identificación, preservación, análisis y documentación. Se exponen técnicas y procedimientos de investigación manuales, también se utilizan herramientas forenses.

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, expositor en OWASP Perú Chapter Meeting y OWASP LATAM at Home , además de Conferencista en PERUHACK, instructor en PERUHACKNOT, y conferencista en 8.8 Lucky Perú. 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 RareGaZz y PeruSEC. Ha dictado cursos 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: **https://www.ReYDeS.com**

Fechas & Horarios

Duración: Catorce (14) horas. Una (1) sesión previamente grabada de dos (2) horas, y cuatro (4) sesiones en vivo de tres (3) horas de duración cada una.

Fechas:

Domingos 7, 14, 21 y 28 de Marzo 2021

Horario:

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

Más Información

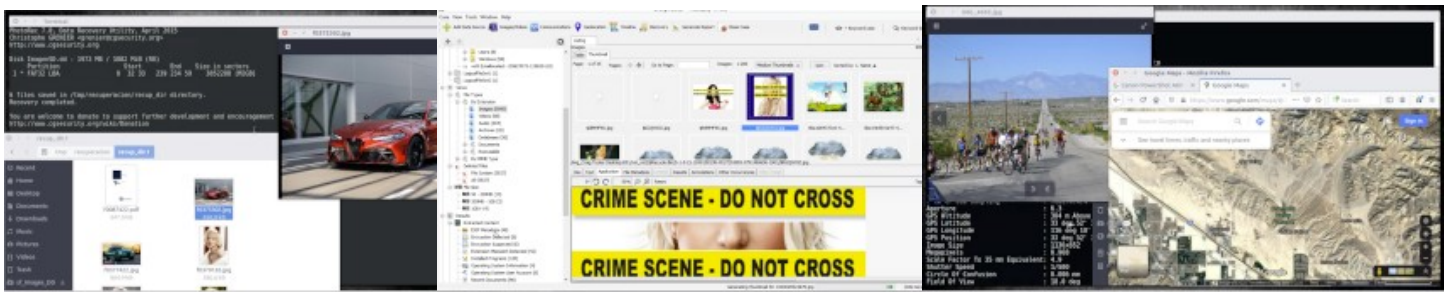
Para obtener más información sobre este curso virtual, tiene a su disposición los siguientes mecanismos de contacto.

Correo electrónico:

caballero.alonso@gmail.com

Teléfono: (+51) 949 304 030

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



Temario: (Actualizado)

- Proceso Investigación Forense
- Evolución del Sistema de Archivos Windows
- FTK Imager
- Adquisición de la Memoria RAM
- Evidencia Encriptada
- Obtener Archivos Protegidos
- Imagen con Contenidos Personalizado
- Discos de Estado Sólido (SSD)
- Nivelación de Uso y SSD Trim
- Artefactos Forenses en SSD
- Adquisición de un Disco Duro
- Adquisición de un USB
- Montar una Imagen
- Visualización Previa de una Unidad
- Recuperar Archivos Borrados
- The Sleuth Kit (TSK)
- Autopsy 2
- Autopsy
- Búsqueda de Cadenas
- Reconstrucción de Datos
- Análisis Forense a la Memoria RAM
- Volatility Framework
- Forense de Correos Electrónicos
- Forense al Registro de Windows
- Lo Esencial del Registro
- Análisis de Información de Usuarios y Grupos
- Análisis de la Configuración del Sistema
- Análisis de la Actividad del Usuario
- Análisis de la Actividad USB
- Archivos de Enlace
- Metadatos en Documentos Office
- Metadatos en Documentos PDF
- Metadatos en Archivos de Medios (EXIF)
- Análisis de Miniaturas
- Análisis de la Papelera de Reciclaje
- Análisis de Archivos Prefetch
- Fundamentos del Registro de Eventos
- Análisis del Registro de Eventos (Logs)
- Registro de Eventos en Windows
- Forense al Navegador Web
- Fundamentos de los Navegadores
- Internet Explorer
- Archivos del Historial Cache / Archivos Temporales
- Cookies, Historial de Descarga

Material:

- SIFT Workstation
- Imágenes Forenses Windows
- Herramientas Windows

Inversión y Forma de Pago

Este curso tiene un costo de:

S/. 350 Soles o $ 110 Dólares

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

Residentes en Perú

Depósito bancario en la siguiente cuenta:

Scotiabank

Scotiabank Perú SAA
Cuenta de Ahorros en Soles: 324-0003164
A nombre de: Alonso Eduardo Caballero Quezada
Código de Cuenta Interbancario (CCI): 009-324-203240003164-58

Residentes en otros países

Transferencia de dinero mediante Western Union y MoneyGram o pago por Paypal

Escribir por favor un mensaje de correo electrónico caballero.alonso@gmail.com para indicarle los datos necesarios para realizar el pago.

Confirmado el depósito o la transferencia se enviará al correo electrónico del participante, los datos necesarios para conectarse a la plataforma, además de la información pertinente para su participación en el curso.

INTERMEDIA ANYMEETING

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.