



5
Sesiones

14
Horas

En vivo,
Virtual, o
Personalizado



Alonso Eduardo Caballero Quezada

Tengo más de veintidós años de experiencia, y desde hace dieciocho años realizo capacitaciones y consultorías en Hacking, Forense, OSINT, CiberSeguridad, y GNU/Linux

Redes Sociales

[LinkedIn](#)

[X \(Twitter\)](#)

[YouTube](#)

[Facebook](#)

[Sitio Web](#)

[e-mail](#)

[WhatsApp](#)

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 profundo conocimiento sobre forense digital aplicado a Microsoft Windows. Es fundamental comprender sus capacidades forenses y artefactos. Aprender a identificar, capturar, autenticar, y analizar datos forenses. Entender como rastrear detalladamente la actividad realizada del usuario a través de la red, además de organizar hallazgos para ser utilizado en una respuesta de incidentes, investigaciones internas, y litigios civiles o penales. Utilizar los conocimientos adquiridos para validar las herramientas 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.



Temario

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 USB y Disco Duro
Montar una Imagen
Visualización Previa de una Unidad
Recuperar Archivos Borrados
The Sleuth Kit (TSK)
Flujos de Datos Alternativos
Volume Shadow Copy
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

Beneficios

- Acceso al aula virtual por 60 días
- Acceso a las sesiones en vivo
- Video de las cinco (5) sesiones
- Acceso libre a las sesiones en vivo de los siguientes cursos a dictarse
- Material utilizado durante el desarrollo del curso
- Dos (2) horas de asesoría personalizada en vivo por videoconferencia
- Libro "Fundamentos de Forense Digital" escrito por el instructor
- Certificado digital de participación
- Certificado digital de aprobación por una duración total de 24 horas

Inversión

Perú: S/. 450 Soles

- Depósito o transferencia interbancaria a Scotiabank
- Pago mediante YAPE o PLIN

Otros países: \$ 140 Dólares

- Pago mediante PayPal

Escriba un mensaje al WhatsApp
<https://wa.me/51949304030> para
proporcionarle los datos pertinentes.

Información

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

WhatsApp: <https://wa.me/51949304030>

Correo electrónico: reydes@gmail.com