



CMIF: Certificado MILE-SEC Informática Forense

14 Horas 30 Días Aula Virtual 2 Certificados

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 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

Presentación

En la actualidad todas las empresas y organizaciones deben estar preparadas para enfrentar exitosamente diversos tipos de crímenes cibernéticos, los cuales 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.

CM
CERTIFICADO MILE-SEC

IF
INFORMÁTICA FORENSE

Objetivos

Este curso enseña a los participantes a desarrollar un profundo conocimiento sobre forense digital aplicado al sistema operativo Windows. Es fundamental comprender sus capacidades forenses y artefactos. 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.