EDUCACIÓN IT

Informatica Forense

Programa de Estudio

Informatica Forense

Domina las herramientas de trabajo de un Analista Forense Informático. Incorpora metodologías para poder formar parte de un equipo dentro de una Causa Judicial.

Contenido del curso

El curso comienza con una introducción a la Informática Forense, en donde se presentará al asistente la disciplina, interiorizándolo en la metodología y en las herramientas utilizadas. Una vez adquirido el vocabulario se comenzará por la siguientes etapas del proceso, en donde se iniciará desde la Adquisición, pasando por la Preservación, el Análisis, hasta llegar a la redacción del Informe.

Durante el curso se verá cómo realizar una copia bit a bit sin perder de vista que no se altere la integridad de los artefactos a adquirir. Asimismo, se analizarán distintas técnicas para recuperar archivos y/o particiones eliminadas. Con respecto a las acciones del usuario en el equipo se analizarán los navegadores, los clientes de correo electrónico, la memoria RAM, el archivo de paginación y el de hibernación.

Se cerrará el curso con la redacción de un Informe final con las labores realizadas.

PRÁCTICAS EN CLASE ::

A lo largo del curso realizaremos distintas prácticas basadas en casos reales. Se llevarán a cabo ejercicios que permitan al asistente comprender la metodología que debe utilizar un Informático Forense al momento de realizar la labor. Poniendo en práctica diversas herramientas realizará la adquisición del disco rígido a peritar, recuperará archivos y particiones eliminadas, trazará una línea de tiempo a partir de los artefactos recolectados, investigará el historial de navegación, el caché y las descargas desde los diversos navegadores Web. Del mismo modo que analizará los correos electrónicos involucrados, la memoria RAM del equipo en cuestión, junto con los archivos de paginación y de hibernación. Se establecerán los lineamientos para el armado del Informe final, ya sea para presentar internamente en la Organización como para ser presentada en una causa judicial.

Público

Este curso está orientado, a cualquier persona sea un profesional de ciberseguridad, pentester, desarrollador, implementador ISO, auditor, así como para entusiastas de la tecnología.

Salida Laboral

Al finalizar el curso, te convertirás en Analista Forense informático. Podrás utilizar tus nuevas aptitudes para trabajar en las distintas fuerzas de la Ley como Especialista Informático Forense, trabajar como Consultor Técnico y/o en organizaciones donde sea una prioridad saber qué es lo que sucedió en sus activos informáticos.

Requisitos

Conocimientos previos: Tener conocimientos de seguridad informática o haber realizado el curso de Introducción a la seguridad Informática Tener conocimientos de criptografía o haber realizado el curso de Criptografía y Blockchain

Modalidad de cursado

Puedes tomar este curso en modalidad presencial o modalidad online - en vivo

¿Qué aprenderás?

- Fundamentos de la Informática Forense
- Procesos involucrados en una Causa Judicial
- Metodologías y herramientas de trabajo
- Tipos de adquisición
- Cadena de Custodia
- Análisis Forense
- File Carving / Data Carving
- Metadata de archivos
- Trabajando en Browsers y Correos electrónicos
- Uso de Nirsoft y Sysinternals Tools
- Técnicas de investigación con correos
- Cómo recuperar archivos y particiones eliminadas
- Análisis de Memoria e Informe Pericial
- Presentación de datos en un proceso judicial

Plan de Estudios

1. Introducción Informática

Ciencias Forenses
Informática Forense
Metodología
Marco legal
Consultor Técnico, Perito de Oficio y Perito de Parte
LiveCDs Forenses
Artefactos
Prueba Digital
Evidencia Digital
Criptografía aplicada a la Informática Forense
Registro de Windows
Buenas prácticas

2. Adquisición Forense

Conceptos
Adquisición física
Adquisición lógica
Adquisición directa
Adquisición indirecta
Adquisición por hardware
Adquisición por Software
dd como herramienta
GUYMAGER
FTK Imager
Preservación
Cadena de Custodia

3. Análisis Forense

Conceptos
Slack Space
Recuperación de archivos borrados

Recuperación de particiones eliminadas
File Carving / Data Carving
foremost
photorec
Línea de tiempo
Autopsy
Análisis de metadata de archivos

4. Browser y Correo electrónico

Conceptos
Historial
Cache
Descargas
Nirsoft
Sysinternals Tools
Distintos Browsers
SQLite
Cabeceras de correos
Distintos clientes de correo electrónico
Técnicas de investigación con correos

5. Análisis de Memoria e Informe Pericial

Conceptos
Memoria RAM
Archivo de Paginación
Archivo de Hibernación
Dump de memoria
FTK Imager
DumpIt
Análisis de RAM
Volatility
Informe final

EDUCACIÓN IT

Centro de Capacitación y Desarrollo Profesional

Lavalle 648 Piso 8, Microcentro, CABA
0810-220-8148
info@educacionit.com