EC-COUNCIL



EC-COUNCIL · PROGRAMA DE INVESTIGACIÓN FORENSE DIGITAL

Computer Hacking Forensic Investigator (C|HFI) v11

Investigue incidentes, preserve la evidencia digital y lleve a su organización a un estado de preparación forense

¿Por qué debería asistir?

El programa C|HFI de EC-Council prepara a los profesionales de ciberseguridad con los conocimientos y habilidades para realizar investigaciones forenses digitales efectivas y llevar a su organización a un estado de preparación forense: establecer el proceso forense, el laboratorio, los procedimientos de manejo de evidencia y las técnicas de investigación necesarias para validar incidentes y orientar a los equipos de respuesta.

Es un programa intensivo y práctico, con 68 laboratorios forenses sobre más de 70 GB de evidencia preparada. Cubre la nube, dispositivos móviles e IoT, ataques web, malware y la dark web, con un enfoque metodológico que garantiza evidencia admisible en un tribunal.

5 días	15	68	600+	70+ GB
DURACIÓN	MÓDULOS	LABORATORIOS	HERRAMIENTAS	EVIDENCIA



¿Quién debería participar?

Respuesta a incidentes y DFIR
Analistas SOC, equipos de respuesta a incidentes y de DFIR que deben validar, contener e investigar incidentes.

Investigación forense
Analistas y peritos forenses digitales que adquieren, preservan y analizan evidencia en distintos entornos.

Seguridad y TI
Profesionales de TI y ciberseguridad con conocimientos básicos de forense, respuesta a incidentes y vectores de amenaza.

Cumplimiento e investigación
Responsables de cumplimiento, auditoría y áreas legales o de investigación que requieren evidencia admisible.

Objetivos de aprendizaje

- Aplicar una metodología forense estructurada: documentar la escena, búsqueda e incautación, preservación, adquisición, examen y reporte
- Adquirir y examinar datos volátiles y no volátiles en Windows, Linux y Mac, incluido el análisis de memoria RAM
- Detectar y contrarrestar técnicas antiforenses, y analizar ShellBags, archivos LNK y Jump Lists de Windows
- Realizar análisis forense de malware, estático y dinámico, incluido ransomware reciente como BlackCat (ALPHV)
- Investigar ataques a aplicaciones web, tráfico de red, redes inalámbricas, correo electrónico y redes sociales
- Aplicar metodologías forenses en la nube (AWS, Azure y Google Cloud), dispositivos móviles, IoT y la dark web
- Automatizar tareas de investigación con scripts en Python
- Mantener la cadena de custodia y los procedimientos legales para que la evidencia sea admisible en un tribunal

Metodología forense del programa

Documentar la escena del crimen | Búsqueda e incautación | Preservación de evidencia | Adquisición de datos | Examen de datos | Reporte | Forense con Python

- Desarrollado por expertos y profesionales de forense digital de todo el mundo.
- Se basó en un análisis riguroso de las tareas del puesto (JTA) y en ofertas de empleo de empresas multinacionales, lo que lo alinea con lo que pide el mercado.

Programa del curso

Duración: 5 días

Módulo	Contenido
Módulos 1–3 Día 1	**01 La informática forense en el mundo actual:** fundamentos, tipos de ciberdelitos y su investigación, regulaciones y estándares aplicables. **02 Proceso de investigación forense:** fases del proceso de investigación, del primer respondedor al reporte. **03 Discos duros y sistemas de archivos:** tipos de discos, arranque y sistemas de archivos de Windows, Linux y Mac, RAID, NAS/SAN y análisis de formatos de archivo.
Módulos 4–6 Día 2	**04 Adquisición y duplicación de datos:** fundamentos y metodología de adquisición, eDiscovery y preparación de imágenes para el examen forense. **05 Cómo vencer las técnicas antiforenses:** técnicas antiforenses usadas por los atacantes, formas de detectarlas, herramientas y contramedidas. **06 Análisis forense de Windows:** datos volátiles y no volátiles, memoria y registro, aplicaciones Electron, navegadores, ShellBags, LNK, Jump Lists y logs de eventos.
Módulos 7–9 Día 3	**07 Análisis forense de Linux y Mac:** adquisición de datos volátiles y no volátiles, y análisis forense de memoria. **08 Análisis forense de redes:** correlación de eventos, IoC en logs de red, investigación de tráfico y detección de ataques inalámbricos. **09 Análisis forense de malware:** análisis estático y dinámico, comportamiento en el sistema y la red, y análisis de ransomware.
Módulos 10–12 Día 4	**10 Investigación de ataques web:** amenazas a aplicaciones web, logs de IIS y Apache, detección e investigación de ataques. **11 Análisis forense de la dark web:** funcionamiento del navegador Tor y proceso forense de Tor. **12 Análisis forense en la nube:** conceptos y desafíos, e investigación en AWS, Microsoft Azure y Google Cloud.
Módulos 13–15 Día 5	**13 Análisis forense de correo y redes sociales:** componentes del correo, investigación de delitos por correo y forense de redes sociales. **14 Análisis forense de dispositivos móviles:** arquitectura y arranque de Android e iOS, redes celulares, sistema de archivos SIM y adquisición lógica y física. **15 Análisis forense de IoT:** amenazas, vulnerabilidades y superficies de ataque, y proceso forense de IoT (Android Wear, Amazon Alexa).



Examen

Duración: 4 horas

Título	EC-Council Computer Hacking Forensic Investigator (C|HFI) – Versión 11		
Código	312-49	**N.º de preguntas**	150
Formato	Opción múltiple	**Duración**	4 horas
Aprobación	60 % – 85 %, según la forma del examen	**Plataforma**	ECC Exam Portal

Requisitos de elegibilidad

- **Requisitos recomendados:** profesionales de TI o forense con conocimientos básicos de TI y ciberseguridad, informática forense, respuesta a incidentes y vectores de amenaza.
- **Con capacitación oficial de EC-Council:** puede presentar el examen sin proceso de elegibilidad. **Sin capacitación oficial:** al menos dos años de experiencia en seguridad de la información, solicitud de elegibilidad aprobada y una cuota de US$100.

Demanda de profesionales forenses

Más del 90 % de los delitos tienen hoy un componente digital, y la Oficina de Estadísticas Laborales de EE. UU. proyecta que el empleo de técnicos forenses crecerá un 13 % entre 2022 y 2032. Según el Salary Survey 75, C|HFI es la única certificación forense digital con un salario de seis cifras, de hasta US$117.950.

Información general

- Manual del estudiante de más de 2.100 páginas y manual de laboratorio de más de 1.550 páginas; 40 % del tiempo de formación en laboratorios
- Credencial acreditada por ANAB (ISO/IEC 17024) y reconocida por el DoD 8570/8140, y alineada al 100 % con el marco NICE 800-181
- Cubre conocimientos para cumplir estándares como ISO 27001, PCI DSS, SOX y HIPAA