CURSO

INFORMÁTICA FORENSE

Plan de estudio

educación IT

Nuestro propósito

Transformar positivamente la vida de las personas.

Queremos que seas protagonista en la transformación que estamos viviendo. Por eso, nos comprometemos a capacitarte para que estés al día con las necesidades digitales actuales.

Te invitamos a trabajar en conjunto para que descubras tu mejor versión y la potencies. Anímate, toma las riendas de tu futuro.

Code your future!

Contenido del curso

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

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.

¿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.
- Trabajo con browsers y e-mails.
- Uso de Nirsoft y Sysinternals Tools.
- Técnicas de investigación con correos.
- Recuperación de archivos eliminados.

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

Modalidad del Curso

Duración
4 semanas / 15 h

Frecuencia semanal
2 encuentros de 2 h

Modalidad
Online en vivo

Grupos reducidos
Promedio 15 personas

Nivel: Avanzado

- [ ] Principiante
- [ ] Intermedio
- [x] Avanzado
- [ ] Experto

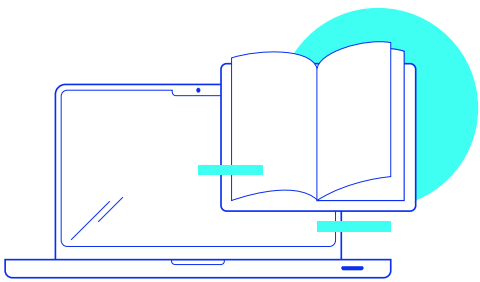
Requisitos

Es recomendable tener una base sobre:

- **Introducción a la Ciberseguridad**
- **Criptografía y Blockchain**

Dedicación fuera de clase

Además de las horas de clase, recomendamos que inviertas 4 h semanales extras para realizar los desafíos complementarios, estudiar el material de lectura y completar los exámenes del Alumni.



¿Cómo será tu experiencia?

Aprender haciendo

Ejercita y pon en práctica lo estudiado.

Trabajo en equipo

Une esfuerzos y potencia los resultados.

Clases grabadas

Consúltalas las veces que quieras.

Profesores expertos

Aprende de gigantes de la industria.

Asistente académico

Recibe soporte dentro y fuera de clase.

Plataforma Alumni

Encuentra recursos, materiales y clases.

¿Por qué Educación IT?

IT Créditos

Gana puntos al aprobar los exámenes de los cursos. Luego, podrás canjearlos por nuevos cursos sin costo alguno. Los IT Créditos que acumules no vencen ni se devalúan.

Garantía de aprendizaje

Si necesitas reforzar conceptos, recuperar clases o no estás satisfecho, ¡vuelve a tomar el curso sin ningún costo! Puede ser de forma total o parcial.

Comunidad en Discord

Mantente en contacto con la comunidad de EducaciónIT a través de nuestro servidor de Discord. Podrás hablar con tus compañeros, profesores, asistentes académicos y soporte.

Preguntas frecuentes

Si me pierdo una o más clases, ¿puedo recuperarlas?

Todas las clases quedan grabadas de por vida en tu plataforma Alumni. ¡Siempre podrás volver a verlas cada vez que lo necesites!

¿Cómo voy a aprender?

Te enfrentarás a situaciones de trabajo reales, en donde tendrás que aplicar lo aprendido de forma individual y en equipo. Por medio de la prueba y el error, irás superando desafíos y obteniendo nuevas habilidades que luego podrás aplicar en el ámbito laboral.

¿Cómo son las clases online en vivo?

Las clases duran entre 2 y 3 horas de lunes a viernes (sábados 3 o 4 hs) y se desarrollan de forma online en vivo en aulas virtuales, donde vas a poder interactuar con el instructor y tus compañeros.
Manejamos cupos reducidos para que puedas tener un seguimiento más personalizado durante tu aprendizaje.

educación IT

Plan de estudio

Code your future

www.educacionit.com

@educacionit