GUÍA DOCENTE

Curso de Experto en Análisis Informático Forense

EEN002

Alejandra Miguel López

Fecha de aprobación

NOMBRE DEL CURSO	Curso de Experto en Análisis Informático Forense
CÓDIGO	EEN002
MODALIDAD	Formación eLearning
TIPOLOGÍA DE LA TITULACIÓN	Cursos de experto +150 horas
ÁREA DE CONOCIMIENTO	Criminalística
PROFESORADO	Alejandra Miguel López
CORREO DE CONTACTO CON EL PROFESORADO	formacion.amiguel@ciberin.es
TUTORÍAS	Concretar cita con los profesores
IDIOMA EN EL QUE SE IMPARTE	Español
ADAPTADO A PERSONAS CON DISCAPACIDAD	Sí, a petición

ÍNDICE

1. Resumen del Curso y Objetivos

1.1. Resumen del Curso

El curso de experto en análisis informático forense está diseñado para proporcionar a los estudiantes una comprensión profunda de las principales herramientas para el análisis digital de cualquier dispositivo tecnológico, con el objetivo de obtener evidencias que permitan esclarecer delitos informáticos o preservar la seguridad de infraestructuras objeto de ataques. A lo largo de este curso, los estudiantes adquirirán las competencias necesarias para realizar distintos tipos de análisis informáticos de cara a cualquier servicio forense.

1.2. Objetivos del Curso

- Dominio avanzado de las principales herramientas de análisis forense informático, adaptadas a diversos dispositivos y entornos de infraestructura.
- Profundización en el proceso metodológico seguido por un perito forense informático durante la investigación de casos.
- Desarrollo de habilidades para la elaboración de informes periciales de análisis forense informático, con enfoque en la precisión y rigurosidad técnica.

2. Competencias

2.1. Competencias Generales

- Capacidad de realizar una investigación informática forense, utilizando las principales herramientas de adquisición de evidencias digitales.
- Capacidad para la elaboración de informes periciales informáticos forenses.
- Dominio de los distintos dispositivos e infraestructuras informáticas para la aplicación de distintos tipos de análisis.

2.2. Competencias Específicas

- Conocimiento de todas las fases del proceso de análisis forense informático dependiendo del tipo de evidencia.
- Capacidad para realizar la adquisición y preservación de evidencias digitales.
- Dominio de herramientas para el análisis forense de sistemas Windows, Linux, dispositivos móviles, infraestructura Cloud, red.
- Capacidad para la elaboración de informes periciales informáticos forenses y mantenimiento del proceso de la cadena de custodia hasta su ratificación.
- Conocimiento especializado de ataques informáticos y respuestas ante ellos.

3. Contenidos

3.1. Contenidos Teóricos

- Tema 1. Introducción al análisis informático forense: fases que se llevan a cabo para un análisis informático forense dependiendo de los distintos escenarios posibles y evidencias, elaboración de informes periciales e importancia de la cadena de custodia y recogida, preservación, proceso de clonación y hashing de evidencias digitales.

- Tema 2. Adquisición de evidencias en Windows: antecedentes, arquitectura, suites, software y herramientas nativas para adquisición de datos, logs, procesos y eventos.

- Tema 3. Adquisición de evidencias en Linux: antecedentes, arquitectura, suites, software y herramientas nativas para adquisición de datos, logs, procesos y eventos.

- Tema 4. Análisis forense de dispositivos móviles: historia y conceptos, sistemas operativos, arquitectura, herramientas nativas y software principal para su análisis y extracción.

- Tema 5. Análisis forense en Cloud: concepto e historia, funcionamiento y seguridad, tipos de infraestructura Cloud, riesgos, seguridad, y herramientas para su análisis.

- Tema 6. Análisis forense de red: Internet, protocolos, estructura y funcionamiento de la red, modelos de arquitectura, análisis de tráfico de red, firewalls, routers y correos electrónicos.

3.2. Contenidos Prácticos

3.2.1. Ejercicios Teórico-Prácticos

- Ejercicio 1: Hashing
- Ejercicio 2: Práctica de comandos/suite/herramienta Windows
- Ejercicio 3: Práctica de comandos/suite/herramienta Linux
- Ejercicio 5: Búsqueda de ataques a distintas infraestructuras Cloud
- Ejercicio 6: Análisis online cabeceras correo electrónico y análisis tráfico de red

3.2.2. Actividad Práctica

Análisis de una imagen forense utilizando las herramientas aprendidas a lo largo del curso. Se proporcionará al alumno un archivo a analizar y el alumno realizará la recuperación, búsqueda y estudio de las evidencias mediante la herramienta que considere más adecuada según las cuestiones a resolver en el caso forense planteado.

3.3. Trabajo final

Realización de un informe pericial informático forense sobre la actividad práctica siguiendo la estructura proporcionada y estudiada, aportando la metodología llevada a cabo junto con las capturas y la documentación necesaria para justificar las conclusiones finales.

Resumen contenido teórico	Total de horas
TEORÍA	20h

EJERCICIOS TEÓRICO-PRÁCTICOS	22h
ACTIVIDAD PRÁCTICA	30h
TRABAJO FINAL	30h

4. Estrategias Metodológicas, Materiales y Recursos Didácticos

4.1. Estrategias Metodológicas

- Clases teóricas:
  - Clases virtuales con presentación PPT en las que se explicará cada tema y se expondrán ejemplos y casos.
  - PDFs con la teoría vista en las clases, de forma desarrollada.
- Discusiones y aportaciones en el foro: planteamiento de temas y cuestiones a resolver y debatir en el foro.
- Ejercicios teórico-prácticos individuales: ejercicios con cuestiones para poner en práctica lo estudiado en cada tema utilizando distintas herramientas para resolver casos forenses
- Tests: parciales de cada tema y uno general del curso

4.2. Materiales y Recursos Didácticos:

- Lecturas recomendadas: material complementario para ampliar lo visto en las clases y guías para aprender a utilizar otras herramientas forenses.
- Artículos científicos: estudios para la preparación del trabajo final y complementar los temas presentados.
- Videos educativos: ejemplos de las explicaciones para facilitar la realización de las prácticas, charlas y otros vídeos de interés acerca de los temas estudiados.
- Software especializado: aportación de las herramientas estudiadas en cada tema para cada práctica.

5. Evaluación

5.1. Criterios de Evaluación

- **Comprensión Teórica:** Se evaluará la capacidad del estudiante para entender y explicar los conceptos teóricos presentados en el curso. Esto incluye la precisión en las respuestas y la claridad en la exposición de ideas.
- **Aplicación Práctica:** Se valorará la habilidad del estudiante para aplicar los conocimientos teóricos a situaciones prácticas y resolver problemas específicos relacionados con el contenido del curso.
- **Participación Activa:** Se tendrá en cuenta la participación del estudiante en las actividades del curso, incluyendo su contribución en los foros de discusión, la formulación de preguntas pertinentes y la interacción con sus compañeros y el profesor.
- **Calidad del Trabajo Final:** Se evaluará la profundidad del análisis, la originalidad, la estructura y la presentación del trabajo final del curso. Esto incluye la correcta aplicación de la metodología y el rigor científico.
- **Resolución de Ejercicios Prácticos:** Se valorará la precisión y la eficacia en la resolución de los ejercicios prácticos propuestos, así como la capacidad para seguir las instrucciones y aplicar los procedimientos adecuados.
- **Desempeño en Pruebas y Exámenes:** Se evaluará el rendimiento del estudiante en las pruebas y exámenes realizados durante el curso, teniendo en cuenta la exactitud de las respuestas y la demostración de un conocimiento sólido de los temas tratados.
- **Autonomía y Responsabilidad:** Se considerará la capacidad del estudiante para gestionar su propio aprendizaje, cumplir con los plazos de entrega y demostrar responsabilidad en la realización de las tareas asignadas.

5.2. Criterios de Calificación

- **1.- Exámenes de cada tema:** 10%
  2.- Examen Final de Curso: 15%
- **3- Ejercicios de diferentes unidades/temas:** 30%
- **4.- Participación activa en el foro (cuestiones moderadas por el tutor, participación en resolución de dudas, feedback varios, etc):** 10%
- **5.- Ejercicio práctico tutorizado (Actividad práctica):** 15%

- **6.- Trabajo final:** 20%

(Necesario superar 50% de puntos 1, 2, 3, 5 y 6, y 100% punto 4).

6. Cronograma

Semana 1 – Tema 1 (15h)

- PPT presentación (15 min)
- PPT tema (30 min)
- PPT explicación práctica (15 min)
- Lecturas recomendadas (3 horas)
- Foro (3 horas)
- Test (1 hora)
- PDF (3 horas)
- Ejercicio práctico (3 horas)
- Vídeos (1 hora)

Semana 2 – Tema 2 (18h)

- PPT 1 (30 min)
- PPT 2 (15 min)
- PPT explicación práctica (15 min)
- Lecturas recomendadas (3 horas)
- Foro (3 horas)
- Test (1 hora)
- PDF (4 horas)
- Ejercicio práctico (5 horas)
- Vídeos (1 hora)

Semana 3 – Tema 3 (18h y 15 min)

- PPT 1 (30 min)
- PPT 2 (30 min)
- PPT explicación práctica (15 min)
- Lecturas recomendadas (3 horas)
- Foro (3 horas)
- Test (1 hora)
- PDF (4 horas)
- Ejercicio práctico (5 horas)
- Vídeos (1 hora)

Semana 4 – Tema 4 (11h y 30 min)

- PPT (30 min)
- Lecturas recomendadas (3 horas)
- Foro (3 horas)
- Test (1 hora)
- PDF (3 horas)
- Vídeo (1 hora)

Semana 5 – Tema 5 (15h y 45 min)

- PPT (30 min)
- PPT explicación práctica (15 min)
- Lecturas recomendadas (3 horas)
- Foro (3 horas)
- Test (1 hora)
- PDF (3 horas)
- Ejercicio práctico (4 horas)
- Vídeos (1 hora)

Semana 6 – Tema 6 (17h y 15 min)

- PPT 1 (30 min)
- PPT 2 (30 min)
- PPT explicación práctica (15 min)
- Lecturas recomendadas (3 horas)
- Foro (3 horas)
- Test (1 hora)
- PDF (3 horas)
- Ejercicio práctico (5 horas)
- Vídeos (1 hora)

Semana 7 (17h y 45 min)

- PPT explicación actividad práctica (15 min)
- PPT repaso test final (30 min)
- Actividad práctica (15 horas)
- Test final (2 horas)

Semana 8 (15h)

- Actividad práctica (15 horas)

Semana 9 (16h y 15 min)

- PPT explicación trabajo final (15 min)
- Lecturas recomendadas (1 hora)
- Trabajo final de curso (15 horas)

Semana 10 (15h)

- Trabajo final de curso (15 horas)

Semana	Clases Grabadas (teoría + explicación prácticas)	PDFs teoría	Lecturas recomendadas	Foro	Ejercicios Prácticos	Trabajo final del curso	Documentales /videos	Test	Actividad práctica	**Total**
1	1h	3h	3h	3h	3h		1h	1h		**15h**
2	1h	4h	3h	3h	5h		1h	1h		**18h**
3	1h y 15 min	4h	3h	3h	5h		1h	1h		**18h y 15 min**
4	30 min	3h	3h	3h			1h	1h		**11h y 30 min**
5	45 min	3h	3h	3h	4h		1h	1h		**15h y 45 min**
6	1h y 15 min	3h	3h	3h	5h		1h	1h		**17h y 15 min**
7	45 min							2h	15h	**17h y 45 min**
8									15h	**15h**
9	15 min		1h			15h				**16h y 15 min**
10						15h				**15h**
Total	**7h**	**20h**	**19h**	**18h**	**22h**	**30h**	**6h**	**8h**	**30h**	**160 h**

7. Bibliografía

7.1. Lecturas Obligatorias

- INCIBE, Glosario de términos de ciberseguridad, 2020
- Arellano, L.E., La cadena de custodia informático-forense, 2012

- Jaramillo, G., Técnicas de análisis forense digital aplicadas a dispositivos y sistemas móviles, 2011
- Rodríguez, F., La informática forense: el rastro digital del crimen
- Alemán, A., Análisis forense digital en dispositivos móviles, 2024

7.2. Lecturas Recomendadas

- Contreras, C.A., Buenas prácticas en informática forense para el procesamiento de evidencia digital o información electrónicamente almacenada, 2021
- Kamble, D., Jain, N, Cybercrimes Solutions using Digital Forensic Tools, 2015
- Arif, M., Hazwam, I., Hafiz, M., Mohd, N., Digital Forensic Investigation of Trojan Attacks in Network using Wireshark, FTK Imager and Volatility
- Rathod, D., Mac OSX Forensics
- Brys, C., Martínez, D.L., Obregón, J., San José, G., GobLin: El Sistema Operativo GNU/Linux para los Gobiernos
- Satya, A., Sulistyo, W., Anti-Forensic Investigation Model Using Live Forensic Method on Private Web Browsing, 2023
- Chavarría, R., Uso de GnuPG como herramienta para la confidencialidad de la información, 2023
- Huerta, M., Julio, M., Marco de trabajo y herramientas para el análisis forense en la atención de los delitos informáticos de Cibergrooming bajo los dispositivos móviles Android, 2022
- Martínez, M.A., Robo de identidad y clonación de tarjetas de crédito y débito utilizando cajeros automáticos alterados, 2021
- Aprilliansyah, D., Riadi, I., S., Analysis of Remote Access Trojan Attack using Android Debug Bridge, 2021

8. Información Adicional

8.1. Requisitos Previos

- Este curso está dirigido a aquellos estudiantes o graduados en informática, criminalística, criminología o cualquier otra titulación relacionada con el ámbito informático forense.
- En caso de no disponer de una titulación relacionada con este ámbito, será necesario que el estudiante posea conocimientos básicos de informática

8.2. Políticas del Curso

Al inscribirse en este curso, los participantes reconocen haber leído, entendido y aceptado las políticas siguientes:

- El participante acepta que utilizará las herramientas y conocimientos adquiridos en el curso únicamente para fines legales y éticos, por lo que exonera a la institución, al profesor y a cualquier entidad asociada de cualquier responsabilidad derivada del uso inapropiado de dichos conocimientos.
- Si el estudiante necesita adaptaciones especiales o tiene dificultades de aprendizaje, deberá informar al profesorado al inicio del curso para proporcionar el apoyo necesario y adecuar el contenido y los materiales.
- Los documentos propios del curso deben de manejarse con uso restringido, es decir, que no se permite compartir material propio de Ciberin Security S.L. con terceros o difundirlo públicamente (manuales de estudio, videos, clases grabadas, etc.).

Ciberin Security S.L. no se hace responsable por el uso inadecuado o ilegal de las herramientas y técnicas enseñadas en este curso, siendo los participantes los únicos responsables de sus acciones y de las consecuencias legales que puedan derivarse del uso inadecuado de la información y habilidades adquiridas.

Por lo que, cualquier actividad que implique la violación de la privacidad de terceros, la infiltración en sistemas o cuentas sin autorización y cualquier otro acto que contravenga la ley, será considerado una violación grave de los términos de este curso y resultará en la expulsión inmediata y en la notificación a las autoridades competentes."