23-24

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

GUÍA DE ESTUDIO PÚBLICA

ANÁLISIS FORENSE

CÓDIGO 3110903-

UNED

23-24

ANÁLISIS FORENSE

CÓDIGO 3110903-

ÍNDICE

Nombre de la asignatura	ANÁLISIS FORENSE
Código	3110903-
Curso académico	2023/2024
Título en que se imparte	MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD
Tipo	CONTENIDOS
Nº ETCS	6
Horas	150.0
Periodo	SEMESTRE 1
Idiomas en que se imparte	CASTELLANO

PRESENTACIÓN Y CONTEXTUALIZACIÓN

PRESENTACIÓN

Esta guía presenta las orientaciones básicas que requiere el estudiante para el estudio de la asignatura de Análisis Forense, asignatura optativa del segundo semestre del Máster Universitario en Ciberseguridad. Por esta razón es muy recomendable leer con atención esta guía antes de iniciar el estudio, para adquirir una idea general de la asignatura y de los trabajos, actividades y prácticas que se van a desarrollar a lo largo del curso.

El número de incidentes relacionados con la ciberseguridad crece cada año más. Y no sólo se incrementa en número sino también en el impacto que reciben las organizaciones y la sociedad. Dentro de estos incidentes, su análisis forense juega un papel fundamental para poder aprender de los errores cometidos y llevar ante la justicia a los perpetradores. El análisis forense es el proceso de identificar, preservar, analizar y presentar las evidencias de que un sistema informático ha sido comprometido de forma legal y aceptable. Mientras que la respuesta ante incidentes tiene como objetivo el volver el sistema a un estado operativo con un mínimo de garantías, el análisis forense por su parte tiene el objetivo de lograr analizar cómo se ha producido un ataque y localizar a sus responsables, sin tener en cuenta el tiempo que lleve esta búsqueda.

En esta asignatura se explorará el análisis forense, las normativas asociadas y se comparará con la respuesta ante incidentes.

Por tanto, los conocimientos y habilidades prácticas que el estudiante adquiera al cursar esta asignatura le servirán de cara a mejorar su perfil profesional dentro del contexto del análisis forense dentro de un equipo de respuesta ante incidentes o el role de perito judicial, incluyendo la adquisición de evidencias, el análisis de evidencias y la elaboración de informes periciales.

CONTEXTUALIZACIÓN

La asignatura de Análisis Forense se trata de una asignatura de 6 créditos ECTS, obligatoria, impartida en el primer semestre del Máster Universitario en Ciberseguridad. Guarda relación con las siguientes asignaturas también disponibles en el mismo Máster:

- *Análisis de Malware.* El Malware es una de las principales herramientas asociadas a los incidentes. Comprender mejor el funcionamiento de estos programas facilita luego su posterior análisis.
- *Auditoria y Monitorización de la Seguridad*. Un analista forense podrá determinar o no la ocurrencia de un evento en base a los mecanismos de monitorización disponibles en un

sistema. Por lo tanto, que existan mecanismos que registren la actividad antes de un incidente son fundamentales para su uso posterior.

•*Gestión de Incidentes de Seguridad.* Como ya hemos comentado la respuesta ante incidentes tiene como objetivo volver a un sistema a un estado operativo tras la detección de incidente. Luego es un paso previo al análisis forense, aunque a veces ambos procesos se mezclan: se debe determinar la fuente del incidente para poder mitigarlo o eliminarlo del sistema.

REQUISITOS Y/O RECOMENDACIONES PARA CURSAR ESTA ASIGNATURA

Para cursar adecuadamente esta asignatura es recomendable tener los siguientes conocimientos previos:

•Estar familiarizado con las redes computadores, los servicios de redes y los protocolos de red.

•Estar familiarizado con los sistemas operativos y su funcionamiento.

•Saber programar scripts de configuración.

•Conocer (leer y escribir) el inglés técnico.

EQUIPO DOCENTE

Nombre y Apellidos	MARIA DE LOS LLANOS TOBARRA ABAD
Correo Electrónico	llanos@scc.uned.es
Teléfono	91398-9566
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	SISTEMAS DE COMUNICACIÓN Y CONTROL

Nombre y Apellidos	ROBERTO HERNANDEZ BERLINCHES (Coordinador de asignatura)
Correo Electrónico	roberto@scc.uned.es
Teléfono	91398-7196
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	SISTEMAS DE COMUNICACIÓN Y CONTROL

Nombre y Apellidos	JUAN CARLOS LAZARO OBENSA
Correo Electrónico	jclo@scc.uned.es
Teléfono	91398-7163
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	SISTEMAS DE COMUNICACIÓN Y CONTROL

COLABORADORES DOCENTES EXTERNOS

Nombre y Apellidos	JESUS SALVADOR CANO CARRILLO
Correo Electrónico	jcano@scc.uned.es

HORARIO DE ATENCIÓN AL ESTUDIANTE

Las consultas sobre los contenidos y funcionamiento de la asignatura se plantearán principalmente en los foros del curso virtual, que serán atendidas por el Equipo Docente de la asignatura.
Para contactar directamente con el Equipo Docente se utilizará preferentemente el correo electrónico, pudiéndose también realizar consultas telefónicas y entrevista personal en los horarios establecidos.

Datos del equipo docente:
María de los Llanos Tobarra Abad
Horario: miércoles lectivos de 10:00 a 14:00 horas
Email: llanos@scc.uned.es
Tfno: 913989566
Dirección postal:

Escuela Técnica Superior de Ingeniería Informática
C/ Juan del Rosal, 16
28040 - Madrid

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE

COMPETENCIAS BÁSICAS

CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio

CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios

CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades

CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

COMPETENCIAS GENERALES

CG1 - Analizar métodos y técnicas de ciberataques.

CG3 - Conocer la normativa y la legislación en materia de ciberseguridad, sus implicaciones en el diseño y puesta en marcha de sistemas informáticos.

COMPETENCIAS TRANSVERSALES

CT1 - Ser capaz de abordar y desarrollar proyectos innovadores en entornos científicos, tecnológicos y multidisciplinares.

CT2 - Ser capar de tomar decisiones y formular juicios basados en criterios objetivos (datos

experimentales, científicos o de simulación disponibles).

COMPETENCIAS ESPECÍFICAS

CE5 - Analizar e identificar técnicas de ocultación de ataques a sistemas de comunicaciones y aplicaciones.

CE7 - Analizar sistemas para encontrar evidencias de ataques en los mismos y adoptar las medidas precisas para mantener la cadena de custodia de dichas evidencias.

CE8 - Conocer las técnicas y herramientas para la realización de un análisis forense con la preservación de pruebas digitales.

RESULTADOS DE APRENDIZAJE

Los resultados de aprendizaje más relevantes que se pretenden alcanzar con el estudio de esta asignatura son los siguientes:

- Diseñar estrategias de recopilación de eventos para distintos elementos de un sistema y analizar los eventos observados en un ataque concreto para distinguir cuáles son de interés.
- Identificar las características de los distintos tipos de ataques sobre un sistema informático e identificar las fuentes más probables.
- Reunir las evidencias de un ataque sobre un sistema informático, garantizando la cadena de custodia necesaria.
- Justificar las medidas necesarias para mantener la cadena de custodia de las evidencias obtenidas de un sistema atacado.
- Describir la normativa legal y técnica de aplicación en el marco del análisis forense.

CONTENIDOS

Unidad 1: Introducción al Análisis Forense

Contenidos:

1. Introducción
2. ¿Qué es el análisis forense digital?
3. Caso ejemplo: el salón de té.
4. Modelos de investigación digital.
5. El método científico.

Unidad 2: Normativa legal vigente

Contenidos:

1. Normativas y estandares para el análisis forense
2. El rol del perito judicial

3. Fases peritaje judicial

Unidad 3: Adquisición y gestión de evidencias

Contenidos:

1. Principios básicos de adquisición de evidencias.
2. Cadena de custodia.
3. Representación de la información y sistemas de ficheros.
4. Herramientas necesarias.

Unidad 4: Análisis forense de sistemas

Contenidos:

1. El laboratorio forense.
2. Análisis forense en sistemas operativos Windows.
3. Análisis forense en otros sistemas operativos.
4. Análisis forense en red.

Unidad 5: Respuesta ante incidentes

Contenidos:

1. Incidentes.
2. Respuesta ante incidentes.
3. Integración del análisis forense en la respuesta ante incidentes.
4. Herramientas

Unidad 6: Informe pericial

Contenidos:

1. Estructura del informe pericial.
2. Redacción del informe.

METODOLOGÍA

Esta asignatura ha sido diseñada para la enseñanza a distancia. Por tanto, el sistema de enseñanza-aprendizaje estará basado en gran parte en el estudio independiente o autónomo del estudiante. Para ello, el estudiante contará con diversos materiales que permitirán su trabajo autónomo y la Guía de Estudio de la asignatura, que incluye orientaciones para la realización de las actividades prácticas. Asimismo, mediante la plataforma virtual de la UNED existirá un contacto continuo entre el equipo docente y los/as estudiantes, así como

una interrelación entre los propios estudiantes a través de los foros, importantísimo en la enseñanza no presencial.

El estudio de esta asignatura se realizará a través de los materiales que el Equipo Docente publicará en el curso virtual.

Esta asignatura de 6 créditos ECTS está planificada en 150 horas. El tiempo de las actividades formativas, siguiendo la anterior metodología, se han distribuido de forma orientativa de la siguiente manera:

- Estudio de los contenidos teóricos-prácticos utilizando la bibliografía y los materiales complementarios: 60 horas.
- Tutorías: 15 horas.
- Actividades en la plataforma virtual, incluyendo la participación en los debates propuestos en los foros de debate: 15 horas.
- Prácticas informáticas, de carácter individual y/o colectivo, que incluyen la resolución de casos prácticos, así como supuestos: 50 horas
- Otros trabajos/prácticas, de carácter individual y/o colectivo así como cuestionarios de autoevaluación: 10 horas.

Por otra parte, cada una de las actividades propuestas formativas en la asignatura constarán de una parte de trabajo individual, otra colectiva (si fuera el caso) y la utilización de la plataforma virtual, además de ser eminentemente prácticas. Todo ello de manera conjunta, por lo que la división de horas realizada en el apartado de actividades formativas es orientativa.

Tanto los trabajos individuales como los colectivos, además de las prácticas se podrán basar en el uso de software libre, así como de máquinas virtuales o simuladores disponibles que permitan emular diversos casos de estudio asociados con los objetivos propuestos en la asignatura.

Por otra parte, los medios necesarios para el aprendizaje son los siguientes:

1. **Materiales teórico-prácticos** preparados por el Equipo Docente para cubrir los conceptos básicos del temario.
2. **Bibliografía complementaria**. El estudiante puede encontrar en ella información adicional para completar su formación.
3. **Curso Virtual** de la asignatura, donde el estudiante encontrará:

- Una **guía de la asignatura** en la que se hace una descripción detallada del plan de trabajo propuesto.
- Un **calendario** con la distribución temporal de los temas propuesta por el Equipo Docente y con las fechas de entrega de las actividades teórico-prácticas que el estudiante tiene que realizar para su evaluación.
- Enunciado de las **actividades teórico-prácticas** propuestas y zona donde depositar los entregables asociados a dichas actividades.

Los foros de debate por medio de los cuales el Equipo Docente aclarará las dudas de carácter general y que se usarán también para comunicar todas aquellas novedades que surjan a lo largo del curso. Éste será el principal medio de comunicación entre los distintos participantes en la asignatura.

SISTEMA DE EVALUACIÓN

TIPO DE PRUEBA PRESENCIAL

Tipo de examen	Examen tipo test
Preguntas test	10
Duración del examen	90 (minutos)

Material permitido en el examen

Ninguno

Criterios de evaluación

La prueba presencial se tratará de un cuestionario de 10 preguntas teórico-prácticas que versarán sobre los contenidos de la asignatura. Cada cuestión tendrá un máximo de cuatro respuestas posibles, siendo sólo correcta una. Cada cuestión tendrá un valor de un punto en caso de contestar de forma correcta. Y restaran 0.45 puntos en caso de contestarse de forma errónea. El estudiante dispondrá de 90 minutos para la realización de este examen. Además de que no se permite ningún material durante su realización.

% del examen sobre la nota final	70
Nota del examen para aprobar sin PEC	
Nota máxima que aporta el examen a la calificación final sin PEC	7
Nota mínima en el examen para sumar la PEC	4

Comentarios y observaciones

CARACTERÍSTICAS DE LA PRUEBA PRESENCIAL Y/O LOS TRABAJOS

Requiere Presencialidad	No

Descripción

La práctica informática es **OBLIGATORIA** y consistirá en un trabajo que el estudiante deberá elaborar a lo largo del curso de manera incremental. El trabajo consistirá en resolver un caso práctico de análisis forense mediante las técnicas aprendidas a lo largo del curso.

No será necesario que el estudiante acuda al Centro Asociado para realizar esta práctica, ya que éste podrá realizarse de forma online en su totalidad a través de la plataforma de aprendizaje del curso.

Este trabajo se presentará a través del curso virtual.

Criterios de evaluación

El equipo docente publicará una guía para su realización, especificando los criterios de evaluación. Se debe obtener al menos un 5 en esta práctica para que se haga media para la nota final.

Ponderación de la prueba presencial y/o los trabajos en la nota final	25% de la nota final (2.5 puntos de la nota final)
Fecha aproximada de entrega	Debe entregarse antes del comienzo de la prueba presencial ordinaria, la fecha concreta se detallará en el curso virtual con la suficiente antelación.

Comentarios y observaciones

Se podrá entregar además en la convocatoria extraordinaria, con la fecha que indique el equipo docente.

En caso de haber aprobado la práctica pero no haber aprobado el examen, la nota de la práctica se guardará para la convocatoria extraordinaria de septiembre en el curso presente.

PRUEBAS DE EVALUACIÓN CONTINUA (PEC)

¿Hay PEC?	No
Descripción	
Criterios de evaluación	
Ponderación de la PEC en la nota final	
Fecha aproximada de entrega	
Comentarios y observaciones	

OTRAS ACTIVIDADES EVALUABLES

¿Hay otra/s actividad/es evaluable/s?	Si,no presencial

Descripción

Se considerarán también otros tipos de actividades evaluables (Trabajos), como puede ser los cuestionarios de los módulos, actividades teórico-prácticas y los debates propuestos por el equipo docente a lo largo del curso.

Criterios de evaluación

Estas actividades deben realizarse de **manera obligatoria** durante el cuatrimestre lectivo asociado a la asignatura y no se podrán entregar, en ningún caso, con posterioridad a la finalización del cuatrimestre docente.

Las otras actividades evaluables cuentan un 5% de la nota final de la asignatura.

Ponderación en la nota final	5% de la nota final de la asignatura.
Fecha aproximada de entrega	
Comentarios y observaciones	

¿CÓMO SE OBTIENE LA NOTA FINAL?

La calificación máxima será de 10 puntos. Para calcular la nota final de la asignatura se sumarán las notas obtenidas en la prueba presencial y en las pruebas teórico-prácticas con los siguientes pesos:
Examen presencial —70%
Prácticas informáticas —25%
Otras actividades— 5%
Para aprobar la asignatura se exigirá una nota mínima de 5 puntos y haber obtenido al menos 4 puntos en la prueba presencial antes de ponderarla. Las prácticas informáticas y otras actividades son OBLIGATORIAS. La calificación final de la asignatura se calculará de la siguiente forma:
En caso de que la nota de la prueba presencial antes de ponderarla sea inferior a 4, entonces la nota final será la nota de la prueba presencial sin ponderación.
En otro caso, se calculará la nota final sumando las diferentes pruebas de evaluación ponderadas con los porcentajes descritos arriba.

BIBLIOGRAFÍA BÁSICA

La bibliografía básica será proporcionada al estudiante dentro del curso virtual, estará compuesta por materiales teórico-prácticos propuestos por el equipo docente.
Gran parte de la bibliografía, así como los recursos proporcionados al estudiante en el curso virtual pueden estar únicamente en inglés, debido a la novedad de algunos de los contenidos propuestos para la asignatura.

BIBLIOGRAFÍA COMPLEMENTARIA

ISBN(13):
Título:NETWORK FORENSICS (7 agosto 2017)
Autor/es:Ric Messier ;
Editorial:JOHN WILLEY & SONS

ISBN(13):9780124171572
Título:WINDOWS FORENSIC ANALYSIS TOOLKIT, 4TH EDITION (11 Marzo 2014)
Autor/es:Harlan Carvey ;
Editorial:SYNGRESS

ISBN(13):9780128019498
Título:OPERATING SYSTEM FORENSICS (12 Noviembre 2015)
Autor/es:Ric Messier ;
Editorial:SYNGRESS

ISBN(13):9781118824993
Título:THE ART OF MEMORY FORENSICS: DETECTING MALWARE AND THREATS IN WINDOWS, LINUX, AND MAC MEMORY (28 Julio 2014)

Autor/es:Aaron Walters ; Michael Hale Ligh ; Andrew Case ; Jamie Levy ;
Editorial:JOHN WILLEY & SONS

ISBN(13):9781785887109
Título:PRACTICAL DIGITAL FORENSICS (26 Mayo 2016)
Autor/es:Richard Boddington ;
Editorial:Packt Publishing

La bibliografía complementaria de la asignatura se puede consultar en la sección de "Libros electrónicos" de la biblioteca de la UNED**,** desde donde se tiene acceso a gran cantidad de recursos online, como puede ser "O'Reilly for High Education". A fecha de edición de esta guía la dirección de acceso es la siguiente:
http://portal.uned.es/portal/page?_pageid=93,26012339&_dad=portal&_schema=PORTAL

RECURSOS DE APOYO Y WEBGRAFÍA

Los/as estudiantes dispondrán de los siguientes recursos de apoyo al estudio:

- **Guía de la asignatura.** Incluye el plan de trabajo y orientaciones para su desarrollo. Esta guía será accesible desde el curso virtual.
- **Curso virtual.** A través de esta plataforma los/as estudiantes tienen la posibilidad de consultar información de la asignatura, realizar consultas al Equipo Docente a través de los foros correspondientes, consultar e intercambiar información con el resto de los compañeros/as.
- **Documentación de la asignatura.** El equipo docente publicará recursos adicionales que faciliten o profundicen los contenidos desarrollados en la asignatura, además de los contenidos ya ofrecidos.
- **Biblioteca.** El estudiante tendrá acceso tanto a las bibliotecas de los Centros Asociados como a la biblioteca de la Sede Central, en ellas podrá encontrar un entorno adecuado para el estudio, así como de distinta bibliografía que podrá serle de utilidad durante el proceso de aprendizaje.

IGUALDAD DE GÉNERO

En coherencia con el valor asumido de la igualdad de género, todas las denominaciones que en esta Guía hacen referencia a órganos de gobierno unipersonales, de representación, o miembros de la comunidad universitaria y se efectúan en género masculino, cuando no se hayan sustituido por términos genéricos, se entenderán hechas indistintamente en género femenino o masculino, según el sexo del titular que los desempeñe.