Guía Docente

DATOS DE IDENTIFICACIÓN

Titulación:	Diploma en Ciberseguridad y Hacking Ético (Título Propio asociado a Ingeniería Informática)
Rama de Conocimiento:	Ingeniería y Arquitectura
Facultad/Escuela:	Escuela Politécnica Superior
Asignatura:	Informática Forense
Tipo:	Propia Obligatoria
Créditos ECTS:	1,50
Curso:	2
Código:	56414
Periodo docente:	Tercer semestre
Tipo de enseñanza:	Presencial
Idioma:	Castellano
Total de horas de dedicación del alumno:	37,50

Equipo Docente	Correo Electrónico
Jorge Antonio Cisneros González	j.cisneros.prof@ufv.es

DESCRIPCIÓN DE LA ASIGNATURA

El objetivo de esta asignatura es enseñar los conceptos básicos en torno a la informática forense y el uso de algunas de sus herramientas principales.
En concreto, los grandes bloques del curso serán:
1. Tecnicas de ocultacion o anonimato.
2. Navegacion anónima.
3. Análisis forense de sistemas.

Para ello usaremos una distribución Linux creada expresamente para el Análisis forense de sistemas, llamada Caine.
Esta distribución permite la toma de evidencias electrónicas con validez judicial.
Esta asignatura corresponde al título propio de Ciberseguridad y Hacking Ético que complementa los estudios de

Grado en Ingeniería Informática. Se imparte en el primer semestre del segundo curso. Requiere una dedicación de 35 horas por parte del alumno.

OBJETIVO

El objetivo final es que cada alumno tenga un conocimiento básico del uso de herramientas forenses

Los fines especficos de la asignatura son:

Recopilación de evidencias: se recopila información digital de dispositivos electrónicos, como computadoras, teléfonos móviles, servidores, etc. Esto implica la extracción de datos, ya sea de almacenamiento local o en la nube, y su preservación para evitar alteraciones.

Análisis forense: se examinan los datos recopilados para identificar y recuperar información relevante. Esto puede incluir la recuperación de archivos eliminados, el análisis de registros de actividad, la búsqueda de palabras clave, el análisis de metadatos, entre otros.

Investigación de delitos informáticos: se utiliza la informática forense para investigar delitos cibernéticos como fraude, robo de información, extorsión, acoso cibernético, espionaje industrial, entre otros. La evidencia digital obtenida puede ser utilizada en juicios y procedimientos legales.

Seguridad de la información: la informática forense también juega un papel importante en la prevención y detección de amenazas cibernéticas. Ayuda a identificar vulnerabilidades en sistemas informáticos y a tomar medidas para proteger la información sensible.

CONOCIMIENTOS PREVIOS

Haber cursado las asignaturas Hacking Ético y Pentesting I y II
Es recomendable que el alumno haya aprobado las asignaturas del primer curso del título propio así como las asignaturas de Introducción a la Programación y Programación Orientada a Objetos

CONTENIDOS

Tema 1 Introducción a la informática forense:

- Definición y conceptos básicos de informática forense.
- Importancia y relevancia de la informática forense en la sociedad actual.
- Principios y estándares éticos en la informática forense.

Tema 2 Delitos y amenazas informáticas:

- Tipos de delitos informáticos (fraude, robo de información, ciberacoso, etc.).
- Amenazas cibernéticas y técnicas de ataque comunes.
- Legislación y marco legal relacionado con los delitos informáticos.

Tema 3 Procedimientos y técnicas forenses:

- Procesos y pasos para llevar a cabo una investigación forense digital.

- Métodos de recolección y preservación de evidencia digital.
- Análisis de sistemas y recuperación de datos.

Tema 4 Herramientas y tecnologías forenses:

- Introducción a las herramientas forenses digitales utilizadas en la investigación.
- Análisis de registros y archivos de registro.
- Uso de técnicas de recuperación de datos y análisis forense de memoria.

Tema 5 Investigación de redes y análisis forense de dispositivos móviles:

- Investigación de redes y análisis de tráfico.
- Investigación forense en dispositivos móviles y sistemas operativos móviles.
- Técnicas de extracción y análisis forense de datos en dispositivos móviles.

Tema 6 Informática forense en entornos empresariales:

- Aspectos de seguridad y respuesta a incidentes en organizaciones.
- Políticas y mejores prácticas de informática forense empresarial.
- Análisis forense en entornos de nube y virtualización.

Tema 7 Aspectos legales y testimonio experto:

- Preparación de informes y documentación forense.
- Preparación para testificar como experto forense en el tribunal.
- Marco legal y jurisprudencia relacionada con la informática forense.

ACTIVIDADES FORMATIVAS

Se combinan lecciones expositivas con clases prácticas de manera que se favorezca la participación y la interacción alumno/profesor y alumno/alumno como vía para fomentar el aprendizaje colaborativo y la capacidad de autoaprendizaje, todo ello mediante estrategias de resolución de situaciones y metodologías de intervención. Las actividades no presenciales, que pueden ser tanto de tipo individual como colectivo, serán supervisadas por el profesor en clases y tutorías estando encaminadas a favorecer el aprendizaje autónomo y colaborativo. Se complementa la lección expositiva, por una parte, con las clases prácticas para la asimilación y aplicación de los conocimientos adquiridos y, por otra, con laboratorios que permitan realizar prácticas para la resolución de problemas y casos, con la supervisión directa del profesor y el enriquecimiento del trabajo en grupo.
Con el fin de facilitar al alumno el acceso a los materiales y la planificación de su trabajo, así como la comunicación con el profesor y el resto de alumnos, se empleará el Aula Virtual de la Universidad.
Las actividades formativas, así como la distribución de los tiempos de trabajo, pueden verse modificadas y adaptadas en función de los distintos escenarios establecidos siguiendo las indicaciones de las autoridades sanitarias.

El alumno resolverá una serie de prácticas forenses con la distribución Caine

En clase se resolverán conjuntamente algunas de ellas para que sepan cómo funciona y cómo se utilizan las herramientas más comunes de análisis forense.

Además, para apoyar el trabajo individual del alumno, en el Aula Virtual de la Universidad (Canvas) los alumnos cuentan con una serie de vídeos que muestran el uso de las herramientas más frecuentes en análisis forense.

Las actividades de carácter no presencial previstas incluyen el estudio individual, que permitirá trabajar en la fijación de los conceptos teóricos abordados en las clases expositivas correspondientes a todas las materias del

módulo y adquirir la destreza práctica que se persigue con las clases prácticas y los laboratorios, que aplicarán el aprendizaje por descubrimiento. El estudio y trabajo realizado por el alumno será supervisado y guiado por el profesor mediante tutorías, individuales o en grupo. En algunos casos, el alumno tendrá que realizar en clase la exposición de las principales conclusiones de su estudio o trabajo, lo que permitirá el intercambio de conocimientos y experiencias entre alumnos

DISTRIBUCIÓN DE LOS TIEMPOS DE TRABAJO

ACTIVIDAD PRESENCIAL	TRABAJO AUTÓNOMO/ACTIVIDAD NO PRESENCIAL
19 horas	18,50 horas
Lección expositiva 15h Tutorías 2h Evaluación 2h	Estudio y trabajo individual 11,50h Trabajo en grupo 7h

COMPETENCIAS

Uso de herramientas de análisis forense de sistemas

RESULTADOS DE APRENDIZAJE

Recopila información digital de dispositivos electrónicos, como ordenadores, teléfonos móviles, servidores, etc.

Examina los datos recopilados para identificar y recuperar información relevante.

Utiliza la informática forense para investigar delitos cibernéticos como fraude, robo de información, extorsión, acoso cibernético, espionaje industrial, entre otros.

Ayuda a identificar vulnerabilidades en sistemas informáticos y a tomar medidas para proteger la información sensible.

SISTEMA DE EVALUACIÓN DEL APRENDIZAJE

El sistema de evaluación contempla cuatro tipos de pruebas:
•[1] Práctica obligatoria sobre análisis forense básico: presenta un peso del 30% en la nota final.
•[2] Práctica voluntaria sobre análisis forense avanzado: presenta un peso del 35% en la nota final.
•[3] Examen tipo test: presenta un peso del 30% en la nota final.
•[4] Participación en clase e implicación en la asignatura: presenta un peso del 5% en la nota final, siendo requisito imprescindible haber asistido como mínimo al 80% de las sesiones. En caso contrario este tipo de prueba se calificará con 0 puntos.
En la prueba [1] es necesario obtener un mínimo de 5 puntos sobre 10 para poder aprobar la asignatura.
En la prueba [2] NO es necesario obtener un mínimo de 5 puntos sobre 10 para poder aprobar la asignatura.
En la prueba [3] es necesario tener un mínimo de 5 puntos para poder aprobar la asignatura.
Aquellos alumnos que estén exentos de la obligación de asistir a clase, bien por segunda matrícula en la

asignatura o sucesivas, bien por contar con autorización expresa de la Dirección del Grado, serán evaluados por el mismo tipo de pruebas. El 5% de la participación en clase podrán obtenerlo asistiendo al menos a tres tutorías con el profesor responsable de la asignatura o entregando las tareas asignadas por el profesor para evaluar este item.

Recuperación en convocatoria extraordinaria: Los alumnos que no hayan alcanzado la nota mínima en el examen, habiendo suspendido por tanto en la convocatoria ordinaria, podrán optar a una recuperación en la convocatoria extraordinaria.

En extraordinaria el alumno se presentará solo a las partes que tenga evaluadas por debajo de 5. La nota ponderada de la evaluación continua será un valor entre 0 y 10 y se calculará como sigue: 0,30*[1] + 0,35*[2] + 0,30* [3] + 0,05*[4].

A efecto de cómputo de convocatorias en una asignatura, solamente se contabilizarán como consumidas aquellas en las que el alumno se haya presentado a todas las pruebas de evaluación, o a una parte de las mismas, siempre que su peso en la nota final supere el 50%, aunque no se presente al examen final. Se entenderá que un alumno se ha presentado a una prueba aunque la abandone una vez comenzada la misma. La condición de No Presentado en la convocatoria extraordinaria estará ligada a la no asistencia o entrega de ninguna prueba, práctica o trabajo que esté pendiente.

Cualquier tipo de fraude o plagio por parte del alumno en una actividad evaluable, será sancionado según se recoge en la Normativa de Convivencia de la UFV. A estos efectos, se considerará "plagio" cualquier intento de defraudar el sistema de evaluación, como copia en ejercicios, exámenes, prácticas, trabajos o cualquier otro tipo de entrega, bien de otro compañero, bien de materiales o dispositivos no autorizados, con el fin de hacer creer al profesor que son propios.

_____

[1] Grabación de la resolución de una práctica de Análisis Forense.
[2] Grabación de la resolución de varias prácticas de Análisis Forense.
[3] Examen tipo test sobre la teoría alojada en Canvas. Preguntas tipo test, sólo una respuesta correcta a elegir entre varias, restan las incorrectas.
[4] Participación e implicación: 5% de la calificación final. Se evaluarán los ejercicios y otras actividades en grupo, el interés mostrado por el alumno, concretamente se computará el índice de asistencia a tutorías tanto individuales o grupales, el grado de participación activa en las clases mediante la respuesta a preguntas del profesor, el estudio de temas avanzados no vistos en clase, la recopilación de noticias aparecidas en los medios de comunicación relacionadas con la asignatura, etc. La calificación de este apartado será un valor numérico entre 0 y 10. Aunque esta nota sea inferior a 5, no se podrá optar a recuperación.

BIBLIOGRAFÍA Y OTROS RECURSOS

Básica

Nanni Bassetti Caine Forensics
https://www.caine-live.net/