DESCRIPCIÓN DE LA ASIGNATURA

Grado/Máster en:	Master Universitario en INGENIERÍA INFORMÁTICA por la Universidad de Málaga
Centro:	Escuela Técnica Superior de Ingeniería Informática
Asignatura:	INFORMÁTICA FORENSE
Código:	201
Tipo:	Optativa
Materia:	ESPECIALIDAD EN CIBERSEGURIDAD
Módulo:	COMPLEMENTOS EN TECNOLOGÍAS INFORMÁTICAS
Experimentalidad:	
Idioma en el que se imparte:	Español
Curso:	2
Semestre:	1
Nº Créditos	4,5
Nº Horas de dedicación del estudiante:	112,5
Nº Horas presenciales:	33,8
Tamaño del Grupo Grande:	
Tamaño del Grupo Reducido:	
Página web de la asignatura:	

EQUIPO DOCENTE

Departamento: LENGUAJES Y CIENCIAS DE LA COMPUTACIÓN

Área: INGENIERÍA TELEMÁTICA

Nombre y Apellidos	Mail	Teléfono Laboral	Despacho	Horario Tutorías
Coordinador/a: FRANCISCO JAVIER LOPEZ MUÑOZ	fjlopezm@uma.es	952131327	3.2.14 - E.T.S.I. INFORMÁTICA	

RECOMENDACIONES Y ORIENTACIONES

It is recommended that the student be familiar with the basic principles about the different architectures of operating systems and how these works in general terms to understand more quickly technical concepts inherent to the content of this course. In addition, some security solutions may negatively affect to the digital evidence collection while others can reinforce it. Therefore, being used to the security mechanisms included in network elements can facilitate learning.

CONTEXTO

During this course of specialisation, the student will acquire the technical skills to carry out computer forensic analysis and those methodologies that are fundamental for the successful training of a forensic computer practitioner.
In particular, the course covers in a horizontal manner the different phases of identifying, obtaining, analysing and presenting electronic evidences. These skills will be consolidated through a complete use case.

COMPETENCIAS

1 Competencias generales y básicas.

Competencias básicas

1.1 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

1.2 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

1.3 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

1.4 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

1.5 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

2 Competencias específicas.

2.2 ETI2 - Capacidad de comprender y saber aplicar el funcionamiento y organización de Internet, las tecnologías y protocolos de redes de nueva generación, los modelos de componentes, software intermediario y servicios.

2.3 ETI3 - Capacidad para asegurar, gestionar, auditar y certificar la calidad de los desarrollos, procesos, sistemas, servicios, aplicaciones y productos informáticos.

2.4 ETI4 - Capacidad para diseñar, desarrollar, gestionar y evaluar mecanismos de certificación y garantía de seguridad en el tratamiento y acceso a la información en un sistema de procesamiento local o distribuido.

2 Competencias específicas.

2.5 ETI5 - Capacidad para analizar las necesidades de información que se plantean en un entorno y llevar a cabo en todas sus etapas el proceso de construcción de un sistema de información.

3 Competencias transversales.

3.2 CT2 - Capacidad para identificar estrategias, herramientas y métodos que responden a situaciones de éxito que pueden ser abordadas con los recursos disponibles.

CONTENIDOS DE LA ASIGNATURA

Part I. Computer Forensics Fundamentals

Chapter1. Past, Present and Future of Digital Forensics

- History of Digital Forensics
- Digital forensics principles
- Challenges for Digital Forensics

Chapter2. Anti-Forensics

- Artifact wiping
- Tail ofuscation
- Attacks against forensic tools and methods
- Data Hiding

Chapter3. International Standards and Practices

- Standards for digital evidence management
- Standards for digital forensics
- Standards for reporting digital evidence

Part II. Gathering Digital Evidence

Chapter4. Sources of Digital Evidence

- Storage media
- Operating system
- Networks
- Others (e.g. mobile, cloud, etc.)

Chapter5. Tools and procedures for Gathering Digital Evidence

- Classification of tools for acquiring digital evidence
- Selection and configuration of tools for acquiring digital evidence

Part III. Analysing Digital Evidence

Chapter 6. Tools and procedures for Analysing Digital Evidence

- Classification of tools for analysing digital evidence
- Selection and configuration of tools for analysing digital evidence

Chapter 7. Interpretation and Correlation

- Choosing relevant data
- Interpretation of data and timeline
- Identification of manipulations

ACTIVIDADES FORMATIVAS

Actividades presenciales

Actividades presenciales

Actividades expositivas

Lección magistral

ACTIVIDADES DE EVALUACIÓN

Actividades de evaluación presenciales

Actividades de evaluación del estudiante

Realización de trabajos y/o proyectos

Otras actividades eval.del estudiante

RESULTADOS DE APRENDIZAJE / CRITERIOS DE EVALUACIÓN

It is expected that, at the end of the course, the student has acquired the following skills:

- Broad knowledge of the different contexts of digital forensics and open problems.

- Rich overview of fundamental concepts within the different digital forensic disciplines and scenarios (e.g. Differences between platforms, systems and devices).

- Develop technical skills using realistic (and flexible) use cases. It is through the context of the use cases that the student will learn to choose the best tools to face the specific needs of the investigation.

- Nourish the creativity and the independency of the student, making him/her participant in the decision making process of the digital investigation.

- Achieve a high degree of student autonomy so that he/she can carry out their professional work with confidence.

PROCEDIMIENTO DE EVALUACIÓN

Evaluation of the contents of the course will be mainly based on a final report about the practical assignments developed by the student along the semester, where the evaluation criteria will be based on the methodology followed to achieve the objectives, the clarity and quality of the report, between others.

Should the student need to pass the course in September or further, he/she will have to obtain 5 out of 10 points in the exam.

BIBLIOGRAFÍA Y OTROS RECURSOS

Básica

Barrett, Diane, and Greg Kipper. Virtualization and forensics: A digital forensic investigator¿s guide to virtual environments. Syngress, 2010.

Graves, Michael W. Digital archaeology: the art and science of digital forensics. Pearson Education, 2013.

Ho, Anthony TS, and Shujun Li, eds. Handbook of digital forensics of multimedia data and devices. John Wiley & Sons, 2015.

Philipp, Aaron, David Cowen, and Chris Davis. Hacking exposed computer forensics. McGraw-Hill, Inc., 2009.

Shavers, Brett. Placing the suspect behind the keyboard: using digital forensics and investigative techniques to identify cybercrime suspects. Newnes, 2013. - Casey, Eoghan. Handbook of digital forensics and investigation. Academic Press, 2009.

Complementaria

Altheide, Cory, and Harlan Carvey. Digital forensics with open source tools. Elsevier, 2011.

Carbone, Fernando. Computer forensics with FTK. Packt Publishing Ltd, 2014.

Carvey, Harlan. Windows forensic analysis toolkit. Syngress, 2018.

Easttom, Chuck. CCFP Certified Cyber Forensics Professional All-in-One Exam Guide. McGraw-Hill Education Group, 2014.

Widup, Suzanne. Computer Forensics and Digital Investigation with EnCase Forensic v7. McGraw-Hill Education Group, 2014.

DISTRIBUCIÓN DEL TRABAJO DEL ESTUDIANTE

ACTIVIDAD FORMATIVA PRESENCIAL

Descripción	Horas	Grupo grande	Grupos reducidos
Lección magistral	33,8	☑	☐
TOTAL HORAS ACTIVIDAD FORMATIVA PRESENCIAL	**33,8**		
TOTAL HORAS ACTIVIDAD FORMATIVA NO PRESENCIAL	**67,45**		
TOTAL HORAS ACTIVIDAD EVALUACIÓN	**11,25**		
TOTAL HORAS DE TRABAJO DEL ESTUDIANTE	**112,5**		