Teaching Guide				
Identifying Data				2024/25
Subject (*)	Forensic Analysis of Devices		Code	614530112
Study programme	Máster Universitario en Ciberseguridade			
Descriptors				
Cycle	Period	Year	Type	Credits
Official Master's Degree	2nd four-month period	First	Optional	3
Language	SpanishGalician			
Teaching method	Face-to-face			
Prerequisites				
Department	Ciencias da Computación e Tecnoloxías da InformaciónComputación			
Coordinador	Vázquez Naya, José Manuel	E-mail	jose.manuel.vazquez.naya@udc.es	
Lecturers	Vázquez Naya, José Manuel	E-mail	jose.manuel.vazquez.naya@udc.es	
Web	moovi.uvigo.es			
General description	Digital forensics consists in the application of scientific and analytical techniques to identify, preserve, analyze and present data that are valid within a legal process. The subject "Forensic Analysis of Devices" has a strong practical component. It will begin with an introduction to this field, explaining key concepts. Next, foundations and methodologies of forensic analysis will be studied from a generic applicable to new cases point of view, but concrete examples, based on real cases will also be studied. In the laboratory practices, the student will learn to handle different tools of forensic analysis and will perform practices simulating real problems.			

Study programme competences / results	
Code	Study programme competences / results
A32	HD-12 - Identificar, preservar y analizar evidencias, realizar análisis forense de un sistema de información, y generar informes que sean claros, concisos e inteligibles tanto por expertos como por personas ajenas al ámbito de la seguridad informática
B28	K-12 - Conocer las técnicas y herramientas para la preservación y análisis de evidencias, así como las metodologías adecuadas para la realización de trabajos forenses con validez legal
C11	C-06 - Identificar vulnerabilidades en un sistema real, así como variar sus parámetros y configurarlo para su protección frente a ellas; limitando así la exposición a amenazas conocidas
C13	C-08 - Realizar test de intrusión en entornos prácticos complejos para la identificación de vulnerabilidades, así como para realizar ataques en entornos controlados con juicio crítico y ético
C14	C-09 - Aplicar métodos de investigación forense para el análisis de incidentes o riesgos de ciberseguridad mediante técnicas científicas y analíticas para identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal

Learning outcomes			
Learning outcomes	Study programme competences / results		
Knowledge of the appropriate methodologies for carrying out forensic work with legal validity	AJ32	BJ28	CJ14
Ability to perform forensic analysis of the different elements that constitute an information system, on multiple platforms and operating systems	AJ32	BJ28	CJ11 CJ13
Ability to generate reports as a result of forensic analysis that are clear, concise and intelligible to both experts and outsiders in the field of computer security	AJ32		

Contents	
Topic	Sub-topic

1. Introdución á Análise Forense	- Definición e obxectivos da análise forense - Importancia no contexto da ciberseguridade - Marco legal e ético - Casos de estudo e exemplos prácticos
2. Proceso de Análise Forense	- Estándares e boas prácticas - Principais fases
3. Adquisición de evidencias	- Fundamentos - Creación de imaxes forenses - Adquisición de memoria
4. Análise de evidencias	- Análise da memoria do sistema - Análise do sistema de almacenamento
5. Forense en Sistemas Operativos	- Windows - Linux

Planning				
Methodologies / tests	Competencies / Results	Teaching hours (in-person & virtual)	Student?s personal work hours	Total hours
Guest lecture / keynote speech	A32 B28 C14	10	15	25
Laboratory practice	A32 B28 C11 C13 C14	10	20	30
Practical test:	A32 B28 C14	2	10	12
Objective test	A32 B28 C14	1	5	6
Personalized attention		2	0	2
(*)The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.				

Methodologies	
Methodologies	Description
Guest lecture / keynote speech	Clases expositivas de presentación dos coñecementos teóricos de cada un dos temas. Fomentarase a participación do alumnado.
Laboratory practice	Sesións prácticas en computador, nas que se deben resolver unha serie de boletíns de exercicios prácticos propostos polo profesor. Os exercicios buscan consolidar os coñecementos presentados nas sesións maxistrais e tamén fomentar a aprendizaxe autónoma do alumnado. Por cada boletín, o alumnado debe entregar unha memoria detallada indicando os pasos seguidos para resolver os exercicios, achegando evidencias. Valorarase: a calidade da memoria; a corrección do proceso descrito, dos comandos empregados e das opcións probadas; a xustificación dos pasos seguidos e a proposta de solucións alternativas. Os boletíns de exercicios publicaranse a través da plataforma de formación da Universidade da Coruña. Imporase unha data máxima de defensa para cada boletín, co obxectivo de fomentar o estudo continuo.
Practical test:	Ao remate da realización das prácticas de laboratorio, realizarase unha proba na que el alumnado deberá demostrar as competencias adquiridas, resolvendo unha serie de exercicios prácticos e respondendo a unha seria de preguntas.
Objective test	Proba mediante a que se valorarán os coñecementos e capacidades adquiridos polo alumnado.

Personalized attention	
Methodologies	Description
Laboratory practice	Resolución de dúbidas. O horario de titorías pode consultarse en https://www.udc.es/es/centros_departamentos_servizos/centros/titorias/?codigo=614

Assessment

Methodologies	Competencies / Results	Description	Qualification
Laboratory practice	A32 B28 C11 C13 C14	Several practices will be proposed throughout the course, related to the forensic analysis of equipment, in which the student will work with different tools and must perform cloning processes, information retrieval, report writing, etc. In the statement of each practice will be specified the deadline for completion of it, as well as the methodology of evaluation, which may be through the delivery of a report, a computer test, or both.	40
Objective test	A32 B28 C14	Final exam, multiple-choice or short-answer, through which the knowledge and abilities acquired by the student will be evaluated, both in the theory sessions and in the practical sessions.	40
Practical test:	A32 B28 C14	Ao remate da realización das prácticas de laboratorio, realizarase unha proba na que o alumno deberá demostrar as competencias adquiridas, resolvendo unha serie de exercicios prácticos e respondendo a unha serie de preguntas.	20

Assessment comments
Será necesario obter como mínimo o 50% da nota para aprobar a materia. Ademais, para aprobar a materia será preciso (en calquera oportunidade) obter un mínimo dun 40% da nota na proba obxectiva. En caso contrario, a nota máxima que se poderá obter é de 4.5. A nota da proba obxectiva NON SE CONSERVA en ningunha convocatoria. O resto de notas consérvanse para o resto de oportunidades do curso académico. 1. CONVOCATORIA DA PRIMEIRA OPORTUNIDADE - CONVOCATORIA ORDINARIA Ao longo do curso realizaranse unha serie de prácticas de laboratorio, unha proba práctica e unha proba obxectiva, coas características e peso indicados no cadro anterior. 2. RESTO DE CONVOCATORIAS Realizarase unha proba obxectiva, coas características e peso indicados no cadro anterior. A nota de prácticas de laboratorio poderá recuperarse mediante a realización das prácticas que se determinen para esta convocatoria. A presentación das prácticas nesta convocatoria implica a renuncia á nota obtida na primeira oportunidade, se a houbera. A nota da proba práctica poderá recuperarse mediante a realización dunha nova proba práctica. A presentación á proba práctica nesta convocatoria implica a renuncia á nota obtida na primeira oportunidade, se a houbera. No caso de querer recuperar a nota dalgunha parte nesta convocatoria, o alumnado deberá contactar co coordinador da materia, cunha antelación mínima de 20 días naturais antes da data do exame da correspondente convocatoria. 3. PLAXIO Se se detectara plaxio en calquera das probas de avaliación, a cualificación final da materia será de "suspenso (0)", feito que se comunicará á coordinación do título para adoptar as medidas oportunas. 4. CONDICIÓN DE "NON PRESENTADO" Considerarase como "non presentado" ao alumnado que non se presente a ningunha das actividades avaliables nunha convocatoria dada. 5. ESTUDANTES CON MATRÍCULA A TEMPO PARCIAL OU CON DISPENSA ACADÉMICA DE EXENCIÓN DE DOCENCIA Deberán poñerse en contacto cos profesores da materia para posibilitar a realización das tarefas fóra da organización habitual da materia.

Sources of information

Basic	Casey, Eoghan. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd ed., San Diego: Academic Press, 2011.Casey, Eoghan. Handbook of Digital Forensics and Investigation. Academic Press, 2009.Carrier, Brian. File System Forensic Analysis. Upper Saddle River: Addison-Wesley, 2005.Vila, Pilar. Técnicas de Análisis Forense Informático para Peritos Judiciales Profesionales. Madrid: 0xWord, 2018Farmer, Dan, and Wietse Venema. Forensic Discovery. Upper Saddle River, NJ: Addison-Wesley, 2005.McKemmish, Rodney. What is Forensic Computing?. Canberra: Australian Institute of Criminology, 1999.Sammons, John. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. Elsevier, 2012.Nelson, Bill, et al. Guide to computer forensics and investigations. Course Technology Cengage Learning, 2010.Johansen, Gerard. Digital forensics and incident response. Packt Publishing Ltd, 2017.Caballero, Juan Garrido, Juan Luis G. Rambla, and José Maria Alonso Cebrián. Análisis forense digital en entornos Windows. Informática 64, 2009.
Complementary	

Recommendations
Subjects that it is recommended to have taken before
Subjects that are recommended to be taken simultaneously
Subjects that continue the syllabus
Other comments

(*)The teaching guide is the document in which the URV publishes the information about all its courses. It is a public document and cannot be modified. Only in exceptional cases can it be revised by the competent agent or duly revised so that it is in line with current legislation.