Teaching Guide				
Identifying Data				2023/24
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	Rivera Dourado, Martiño Vázquez Naya, José Manuel	E-mail	martino.rivera.dourado@udc.es 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	
Code	Study programme competences
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		
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. Forensic Analysis Fundamentals	Introduction Fundamentals Normative Cloning
2. Windows Forensic Analysis	Artifacts Memory Tools Advanced Forensic Analysis
3. Mac OS Forensic Analysis	Artifacts Memory Tools Advanced Forensic Analysis
4. Mobile Devices Forensic Analysis (Android)	Artifacts Tools Advanced Forensic Analysis
5. Mobile Devices Forensic Analysis (iOS)	Artifacts Tools Advanced Forensic Analysis

Planning				
Methodologies / tests	Competencies	Ordinary class hours	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	1	0	1
Supervised projects	A32 B28	1	7	8
Objective test	A32 B28 C14	1	0	1
Personalized attention		10	0	10
(*)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	Expositive classes for the presentation of the theoretical knowledge of each one of the subjects. The participation of students will be encouraged.
Laboratory practice	Practical sessions in computer, in which a series of practical exercises bulletins proposed by the professor must be solved. The exercises seek to consolidate the knowledge presented in the lectures and also encourage the student's autonomous learning. Once the exercise bulletin is completed, the teacher will evaluate the work done by the student through a computer session. The exercise bulletins will be published through the Master's training platform. A maximum defense date will be imposed for each newsletter, with the aim of encouraging continuous study.
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.
Supervised projects	Proposta de traballos para a súa resolución individual por parte do alumnado. Estes traballos serán opcionais e permitiranlles ao alumnado interesado afondar en aspectos do temario que lles interesen especialmente e que non se puideran tratar co detalle suficiente durante as sesións maxistrais.
Objective test	Test through which the knowledge and skills acquired by the student will be assessed.

Personalized attention	
Methodologies	Description

Laboratory practice	Resolution of doubts

Assessment			
Methodologies	Competencies	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.	10
Supervised projects	A32 B28	Os traballos tutelados serán opcionais e sobre algún tema a convir entre o alumno e o coordinador da materia.	10

Assessment comments
1. FIRST OPPORTUNITY CALL Throughout the course, a series of laboratory practices will be carried out, with the characteristics and weight indicated in the table above. At the end of the course, an objective test will be carried out, with the characteristics and weight indicated in the table above. 2. SECOND OPPORTUNITY CALL AND EXTRAORDINARY CALL There will be an objective test, with the characteristics and weight indicated in the previous table. The grade of the objective test will NOT be retained in any call. With respect to the laboratory practices, the student will be able to keep the grade obtained in the first opportunity (if it is the case). In case of not having presented the practices in the first opportunity, the student must contact the coordinator of the subject, at least 20 calendar days before the date of the exam. 3. PLAGIARISM If plagiarism is detected in any of the evaluation tests, the final grade of the subject will be "failed (0)", a fact that will be communicated to the master?s coordination in order to take the appropriate measures. 4. CONDITION OF "NOT-TAKEN" Students who do not take the objective test will be considered as "not-taken".

Sources of information	
Basic	- Eoghan Casey (2009). Handbook of Digital Forensics and Investigation. Academic Press - Pilar Vila Avendaño (2018). Técnicas de Análisis Forense informático para Peritos Judiciales profesionales. Madrid : 0xWORD
Complementary	- Juan Garrido Caballero, Juan Luis García Rambla, Chema Alonso (2012). Análisis forense digital en entornos windows. Móstoles: Informática64

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.