Teaching Guide				
Identifying Data				2022/23
Subject (*)	Forensic Analysis of Devices		Code	614530012
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	
Code	Study programme competences
A6	CE6 - To develop and apply forensic research techniques for analysing incidents or cybersecurity threats
B1	CB1 - To possess and understand the knowledge that provides the foundations and the opportunity to be original in the development and application of ideas, frequently in a research context
B2	CB2 - Students will be able to apply their knowledge and their problem-solving ability in new or less familiar situations, within a broader context (or in multi-discipline contexts) related to their field of specialization
B3	CB3 - Students will be able to integrate diverse knowledge areas, and address the complexity of making statements on the basis of information which, notwithstanding incomplete or limited, may include thoughts about the ethical and social responsibilities entailed to the application of their professional capabilities and judgements
B7	CG2 - Ability for problem-solving. Ability to solve, using the acquired knowledge, specific problems in the technical field of information, network or system security
C4	CT4 - Ability to ponder the importance of information security in the economic progress of society

Learning outcomes			
Learning outcomes	Study programme competences		
Knowledge of the appropriate methodologies for carrying out forensic work with legal validity	AJ6	BJ1	CJ4
Ability to perform forensic analysis of the different elements that constitute an information system, on multiple platforms and operating systems	AJ6	BJ2 BJ7	CJ4
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	AJ6	BJ3 BJ7	CJ4

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	A6 C4	11	22	33
Laboratory practice	A6 B1 B2 B3 B7 C4	10	20	30
Objective test	A6 B1 B2 B3 B7 C4	2	0	2
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.
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	A6 B1 B2 B3 B7 C4	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.	50
Objective test	A6 B1 B2 B3 B7 C4	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.	50

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	- Pilar Vila Avendaño (2018). Técnicas de Análisis Forense informático para Peritos Judiciales profesionales. Madrid : 0xWORD - Eoghan Casey (2009). Handbook of Digital Forensics and Investigation. Academic Press
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.