UNIVERSIDADE DA CORUÑA

Teaching Guide				
Identifying Data				2019/20
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	faitic.uvigo.es			
General description	The forensic analysis consists of 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" 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 point of view, and they will applicable to new cases, but concrete examples, based on real cases will also be studied. In parallel, 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
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 / results		
Coñecemento das metodoloxías adecuadas para a realización de traballos forenses con validez legal	AJ6	BJ1	CJ4
Capacidade para a realización de análise forense dos diferentes elementos que forman un sistema de información, en múltiples plataformas e sistemas operativos	AJ6	BJ2 BJ7	CJ4
Capacidade para xerar informes como resultado da análise forense claros, concisos e intelixibles tanto por expertos como por persoas alleas ao ámbito da seguridade informática	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 / Results	Teaching hours (in-person & virtual)	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	Written 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 / Results	Description	**Qualification**

Laboratory practice	A6 B1 B2 B3 B7 C4	Realization and defense of the practices in computer, during the hours of practices and before the established deadline. It is a necessary condition (but not sufficient) to obtain a minimum score of 4 out of 10 in the practices in order to overcome the subject	40
Objective test	A6 B1 B2 B3 B7 C4	At the end of the semester, there will be a written test that will assess the knowledge and skills acquired by the student. It is a necessary condition (but not sufficient) to obtain a minimum score of 5 out of 10 in the objective test in order to overcome the subject	60

Assessment comments

1. FIRST CALL

Students may decide to be evaluated according to a continuous or single assesment model. It will be understood that a student chooses a continuous evaluation when defending the first of the practices of the subject. Once students choose the continuous assessment model, their grade can never be "No Show".1.a) Continuous assesmentIt consists in the realization and defense of a series of laboratory practices, during the entire period in which the subject is taught, and in the performance of an objective test, whose characteristics are described above.

The qualification will be the result of applying the weighted average between the results: (i) Objective test (60%) and (ii) laboratory practices (40%).

2.a) Single assesmentIt consists in carrying out an objective test, with the same characteristics as that corresponding to continuous assesment. And, in addition, another written test, which will be done next, on the practical part, and that will have the same weight as this part in the continuous evaluation.The evaluation of laboratory practices is only kept during the academic year.

The theory exam mark is not preserved.

3. PLAGIARISM

If plagiarism is detected in any of the evaluation tests, the final grade of the subject will be "failed (0)", which will be communicated to the faculty's direction to take the appropriate measures.

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 - Mattia Epifani, Pasquale Stirparo (2016). Learning iOS Forensics, 2nd Edition. Packt Publishing - Rohit Tamma, Donnie Tindall (2015). Learning Android Forensics. Packt Publishing

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.