



## Teaching Guide

| Teaching Guide           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |        |                                 |           |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|---------------------------------|-----------|
| Identifying Data         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |        |                                 | 2018/19   |
| 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               | Computación                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |        |                                 |           |
| 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                      | www.munics.es                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |        |                                 |           |
| General description      | <p>A análise forense de equipos consiste na aplicación de técnicas científicas e analíticas para identificar, preservar, analizar e presentar datos que sexan válidos dentro dun proceso legal.</p> <p>A materia "Análise Forense de Equipos" ten unha forte compoñente práctica. Comezarase con unha introdución a este campo, explicando conceptos clave. A continuación, estudiaranse fundamentos e metodoloxías de análise forense dende un punto de vista xenérico e aplicable a novos casos, pero tamén se estudiarán exemplos concretos baseados en casos reais. Paralelamente, nas prácticas de laboratorio o/a alumno/a aprenderá a manexar diferentes ferramentas de análise forense e realizará prácticas simulando problemas reais.</p> |        |                                 |           |

## 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 |            |     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|------------|-----|
| 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<br>BJ7 | CJ4 |
| Capacidade para xerar informes como resultado da análise forense claros, concisos e intelixibles tanto por expertos como por persoas ajeas ao ámbito da seguridade informática | AJ6                         | BJ3<br>BJ7 | CJ4 |

## Contents

| Topic                              | Sub-topic                       |
|------------------------------------|---------------------------------|
| 1. Fundamentos                     | Fundamentos                     |
| 2. Metodoloxía de Análisis Forense | Metodoloxía de Análisis Forense |



|                                                             |                                                          |
|-------------------------------------------------------------|----------------------------------------------------------|
| 3. Ferramentas de Análise Forense: Entornos Linux e Windows | Ferramentas de Análise Forense: Entornos Linux e Windows |
| 4. Casos                                                    | Casos                                                    |

| 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 | 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 maxistras e tamén fomentar a aprendizaxe autónoma do alumno.<br>Unha vez completado o boletín de exercicios, o profesor avaliará o traballo realizado polo alumno mediante unha sesión de traballo en computador.<br>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. |
| Objective test                 | Proba escrita mediante a que se valorarán os coñecementos e capacidades adquiridos polo alumno.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Personalized attention |                        |
|------------------------|------------------------|
| Methodologies          | Description            |
| Laboratory practice    | Resolución de dúbidas. |

| Assessment          |                   |                                                                                                                                                                                                                                                                                              |               |
|---------------------|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Methodologies       | Competencies      | Description                                                                                                                                                                                                                                                                                  | Qualification |
| Laboratory practice | A6 B1 B2 B3 B7 C4 | Realización e defensa das prácticas en computador, dentro das horas de prácticas e antes da data límite establecida.<br>É condición necesaria (pero non suficiente) obter unha puntuación mínima de 4 sobre 10 nas prácticas para poder superar a materia.                                   | 40            |
| Objective test      | A6 B1 B2 B3 B7 C4 | Ao finalizar o cuadrimestre, realizarase unha proba escrita mediante a que se valorarán os coñecementos e capacidades adquiridos polo alumno.<br><br>É condición necesaria (pero non suficiente) obter unha puntuación mínima de 5 sobre 10 na proba obxectiva para poder superar a materia. | 60            |

| Assessment comments |
|---------------------|
|---------------------|



## Alumnos a tempo parcial

Alumnado con recoñecemento de dedicación a tempo

parcial e dispensa académica de exención de asistencia, segundo establece a

"NORMA QUE REGULA O RÉXIME DE DEDICACIÓN AO ESTUDIO DOS ESTUDANTES DE GRAO NA UDC (Art. 2.3; 3.b e 4.5)(29/5/2012)".

Os alumnos que cursen a materia a tempo parcial deben

realizar as mesmas probas de avaliación que os alumnos que as cursen a tempo completo, coas seguintes consideracións:

Quedan exentos da asistencia a

clase. En canto á defensa das prácticas,

se o alumno non puidese asistir á defensa no horario de prácticas, convírase

con el un horario alternativo. O alumno deberá notificar ao coordinador da materia a

súa condición de estudante a tempo parcial tan pronto como lle sexa recoñecida,

de xeito que o profesor poida realizar unha correcta planificación das

actividades docentes.

Segunda oportunidade e oportunidade adiantada de

Decembro

Aspectos a ter en conta:

En caso de non presentar (ou non

superar) as prácticas de laboratorio en primeira oportunidade, o/a alumno/a deberá

someterse a un (novo) exame de prácticas, con computador. Para iso, o/a alumno/a

debe contactar co coordinador, como mínimo 15 días antes da data do exame

oficial da asignatura para a convocatoria en cuestión (Xullo ou Decembro), e

convir con el unha data e hora para a realización do exame de prácticas. Condición de

"Non Presentado"

Consideraranse como "non presentados" aos

alumnos que non realicen a proba obxectiva.

## Sources of information

|                      |                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Basic</b>         | <ul style="list-style-type: none"><li>- Pilar Vila Avendaño (2018). Técnicas de Análisis Forense informático para Peritos Judiciales profesionales. Madrid : 0xWORD</li><li>- Eoghan Casey (2009). Handbook of Digital Forensics and Investigation. Academic Press</li></ul>                                                                                                                       |
| <b>Complementary</b> | <ul style="list-style-type: none"><li>- Juan Garrido Caballero, Juan Luis García Rambla, Chema Alonso (2012). Análisis forense digital en entornos windows. Móstoles: Informática64</li><li>- Mattia Epifani, Pasquale Stirparo (2016). Learning iOS Forensics, 2nd Edition. Packt Publishing</li><li>- Rohit Tamma, Donnie Tindall (2015). Learning Android Forensics. Packt Publishing</li></ul> |

## 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.