**Syllabus of Module 5: Digital Forensics Fundamentals**

**Workload and ECTS**

Video classes: 8 hours

Autonomous work: 67 hours

ECTS: 3

**Learning Outcomes (Knowledge, Skills and Competences)**

The Comprehensive Digital Forensics Fundamentals module provides the theoretical and practical use of this knowledge in the collection, analysis and preservation of evidence, resulting in its constitution as evidence in court. The contents present in the program of this module, allow to consolidate the aim of this module. The skills to be developed are as follows:

1. The student knows the models of digital forensic analysis;

2. The student knows the relationship between clues, evidences and crime;

3. The student performs forensic reports;

4. The student in the scene, identifies, collects, acquires and preserves digital clues, using different techniques, protecting the integrity of the evidence;

5. The student uses the best practices and procedures in the acquisition and handling of digital evidence;

6. The student is familiar with various computer forensics techniques in the collection and analysis of various types of digital evidence using specific techniques and tools.

**Contents**

1. Concepts, definitions and Models

2. Preservation and collection of digital evidence at the scene of the crime

3. Acquisition procedures for digital evidence

3.1. Sterilization Procedures

3.2. Acquisition Techniques

4. Acquisition and analysis of volatile information

5. Identification and analysis of points of interest of information in Operating Systems

6. Use of OpenSource analysis tools

7. Digital Forensics Case Studies

7.1 Case Study 1: Hacking with windows SO tools

**Demonstration of the Contents Coherence with the Course Unit’s Learning Outcomes**

The objectives of this module are the theoretical knowledge of computer forensics concepts, and the use of this knowledge in the collection, analysis and preservation of evidence, resulting in its constitution as evidence in court. The contents present in the program of this module, allow to consolidate this objective of this module.

**Teaching Methodologies**

Theoretical and practical videos, which includes the presentation of subjects supported by teacher demonstrations, followed by quizzes to assess the student evolution and the analysis of real-world case studies. According to student performance on the quizzes, different videos should be provided to the students to reinforce the subjects where the assessment does not achieve the minimum stated level to procced to next subject. So, each student could have its own path on the videos prepared for the module, according to his performance.

**Demonstration of the Teaching Methodologies Coherence with the Course Unit’s Learning Outcomes**

The skills to be achieved of this module are divided into two areas: the theoretical domain of the procedures in collection, analysis and preservation of evidence. The teaching methodology adopted is divided into two types of videos: theoretical and practical lecture videos focused on achieving the objective related to the theoretical knowledge of forensic computer techniques and laboratory classes oriented to learning the use of tools; Demonstration videos focused on achieving the objective of the efficient use of tools to analyze digital forensics clues.

**Evaluation Methods**

The assessment is based on a set of quizzes, that focus on important aspects of each of the contents. Each student must achieve a preconfigured percentage of correct answers to proceed to next topic on the contents.

**Main Bibliography**

[1] BUNTING, Steve, The Official EnCE: EnCase Certified Examiner Study Guide, 2012.

[2] GRUNDY, Barry J., The Law Enforcement and Forensic Examiner's Introduction to Linux (http://www.linuxleo.com/Docs/linuxintro-LEFE-4.31.pdf), 2017.

[3] CASEY, Eoghan, Digital Evidence and Computer Crime, Academic press, 2011.

[4] BROWN, Christopher L. T., Computer Evidence: Collection and Preservation, 2nd Edition, 2009.

[5] CARVEY, Harlan, Investigating Windows Systems, 1st Edition, 2018.

[6] HALE LIGH, Michael, The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory 1st Edition, 2014.

[7] ENISA, Identification and handling of electronic evidence Toolset, September 2013.

[8] ENISA, Identification and handling of electronic evidence Handbook, September 2013.

[9] NIST, Computer Security Incident Handling Guide, Special Publication 800-61r2.