Computer Forensics

Academic Year: (2019 / 2020) **Review date: 02-05-2019**

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: PERIS LOPEZ, PEDRO

Type: Electives ECTS Credits : 6.0

Year : 4 Semester :

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

Operating Systems.
Computer Networks.
Cryptography and Computer Security.
Security Engineering.

OBJECTIVES

The course covers forensics tools, methods, and procedures used for investigation of computer crime, techniques of data recovery, protection and gathering of evidences, and expert witness skills.

Upon successful completion of this course, the student will be able to:
(PO a, b, c, d, e, f, g, j, k)

1. Know and use the methodology commonly used in computer forensics investigations.
2. Know and use methods for evidence gathering.
3. Use and evaluate various techniques for evidence analysis in file systems, memory and networks.
4. Install, configure and use forensics tools.
5. Get acquainted with hardware devices used in computer forensics investigations.
6. Retrieve, manipulate and organize evidences systematically.
7. Work in team, write forensics reports and present them in public.
8. Know and use standards and legal regulations linked with computer forensics investigations.

DESCRIPTION OF CONTENTS: PROGRAMME

1. Module 1
   a. Introduction
   b. Key technical concepts

2. Module 2
   a. Labs and Tools
   b. Evidence collection and archiving

3. Module 3
   a. Anti-forensics tools and techniques
   b. Internet and email

4. Module 4.
   a. Network forensics
   b. Mobile device forensics

5. Module 5.
   a. Standards and regulations
   b. Legal aspects

LEARNING ACTIVITIES AND METHODOLOGY

Lectures, where the main theoretical concepts of the subject will be described and explained. The students will be able to follow these lectures using the appropriate course material as well as the corresponding intranet tools and bibliography. References will help the students to further elaborate on any topic of their interest.

Lab sessions in computer labs where the students will work with forensics tools. Real forensics cases will be introduced and the students will have to solve several exercises that will help them to strengthen their theoretical knowledge and get acquainted with forensics tools.

ASSESSMENT SYSTEM

The final mark will depend on the following criteria:

The resolution, during the lab sessions, of lab assignments (forensic exercises): 50% of the final mark. These lab exercises are compulsory and are collectively marked by assessing each of the individual assignments and submitted reports. (PO a, b , c, d, e, f, g, j, k)

Final exam: 50% of the final mark.   Attending the final exam is compulsory and the student must get at least 50% of the maximum marks in the exam to be able to pass the course. (PO a, b, c, d, e, f, g, j, k)

Students who do not follow the continuous assessment scheme will be examined of the whole content of the subject. This exam will be different to the one done by students who followed the continuous assessment.

There will be a special examination session where the student who has not followed or has failed the continuous assessment scheme described above will be able to hand-in, if he so whishes, all the related coursework (including lab assignments), to get a mark along the lines described above. He can, alternatively, chose to seat the final exam and in this case the exam will account for 100% of the final marks.

% end-of-term-examination:	50
% of continuous assessment (assigments, laboratory, practicals…):	50

BASIC BIBLIOGRAPHY

- Brian Carrier File System Forensic Analysis, Addison-Wesley.
- Cory Altheide and Harlan Carvey Digital Forensics with Open Source Tools, Syngress Media.
- John Sammons The Basics of Digital Forensics. , Syngress.
- Nelson et al. Guide To Computer Forensics and Investigations. , Cengage Learning.

ADDITIONAL BIBLIOGRAPHY

- Eoghan Casey Handbook of Digital Forensics and Investigation, Academic Press Inc.
- Harlan Cavey Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry, Syngress Media.