Computer Forensic

Academic Year: (2022 / 2023) **Review date: 19/01/2023 12:49:03**

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: PERIS LOPEZ, PEDRO

Type: Electives ECTS Credits : 3.0

Year : 1 Semester : 2

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

Does not apply

OBJECTIVES

This subject leads to the following set of basic competences:

CB6: Master the knowledge required to propose original designs or developments, often in a research process within the area of cyber security.
CB7: Ability to apply acquired knowledge to solve problems under novel or almost novel situations or within broader (multidisciplinar) contexts related with cyber security.
CB8: Ability to state critical opinions and judgements having incomplete or limited information in the field of cyber security. These judgements must take into account include considerations about social and ethical responsibilities
CB9: Discuss in a public audience about their acquired knowledge, and the conclusions from the work. Students will be able to give their foundational and most convincing reasons to a specialized and non specialized audience in a clear way, without ambiguities.
CB10: Students should have the learning skills required to continue studying in a autonomous or self-directed way.

Concerning general and specific competences, students will be able to:

CG2: Create, design, deploy and maintain a cyber defense global system in a given context.

CG3: Create and refine concise and comprehensively documents, plans and projects in the scope of cyber security.
CG4: Know the relevant technique part of the legal regulation in cyber security and its implications in the design of systems and security tools.
CE4: Analyze systems to find attack evidences and to adopt the required measures to maintain the custody chain of the found evidences.

After passing the subject and as learning results, students will be able to:
- Design strategies to distribute sensors in a network and analyze observed events to determine which are relevant in a particular case.
- Given a system under attack, identify the features of most of these attacks and point out the most probable sources.
- Given an attacked systems, find attack evidences and explain the required mechanisms to preserve the chain of custody of such evidences.
- Understand legal and technical aspects related to cybersecurity.

DESCRIPTION OF CONTENTS: PROGRAMME

Forensic analysis of information systems:
1. Introduction to forensic analysis
1.1. What is it?
1.2. Case examples

1.3. Key concepts

2. Forensic analysis lab
2.1. Lab description
2.2. Policies and procedures
2.3. Quality assurance
2.4. Tools
2.5. Evidences: gathering, analysis and custody
2.6. Forensic report

3. Forensics analysis tools
3.1. Forensic analysis of file systems
3.2. Forensic analysis of memory
3.3. Forensic analysis in computer networks
3.4. Forensic analysis related to Internet and e-mail
3.5. Forensic analysis of mobile devices
3.6. Anti-forensics tools and techniques

LEARNING ACTIVITIES AND METHODOLOGY

Learning activities:

Theoretical lectures
Practical lectures
Mixed theoretical and practical lectures
Laboratory practices
Tutoring sessions
Teamwork
Individual work by the student

In this subject, concepts will be applied live during the sessions. For this purpose, a set of exercises will be taken as a basis for each session. Students will have to develop several practical cases of forensic analysis. As part of their work, students may have to perform a critical analysis of other students' forensic reports.

Particularly, the methodology is based on:
- MD1. Lectures using computers in which key concepts are introduced and bibliography is pointed out.
- MD2. Critical analysis of readings (articles in press, reports, manuals, papers, etc.) suggested by teachers. This may be used for a further discussion or to consolidate concepts.
- MD3. Practical case and problems resolution, individually or in groups.
- MD4. Presentation or discussion of related topics and practical cases.
- MD5. Development of tasks and reports, individually or in groups.

ASSESSMENT SYSTEM

% end-of-term-examination/test:	10
% of continuous assessment (assigments, laboratory, practicals…):	90

Periodical assignment (90% of final mark) [SE2]

Periodical (e.g. weekly) assignment related to the topic addressed in each session. This task may also involve assessing the reports from peer students.

End of term examination (10% of final mark) [SE3]

It may contain theoretical or practical issues, as well as forensic cases.

In order to pass the subject it is necessary to fulfill the two following conditions:
- Pass the end of term examination (i.e. get at least 1.25 out of 2.5)
- Get at least 5.0 marks out of 10.0, considering both assignments and exam.

In the extraordinary sitting, unless otherwise specified at the beginning of the subject, students are not allowed to hand-in periodical assignments.

BASIC BIBLIOGRAPHY

- Aaron Phillip; David Cowen, Chris Davis Hacking Exposed: Computer Forensics (ISBN 0071626778), McGraw Hill Professional, 2009

- Andy Jones and Craig Valli Building a digital forensic laboratory, Syngress, 2011

- Casey, E. Handbook of Digital Forensics and Investigation (ISBN 0123742676), Academic Press. , 2009

- Casey, Eoghan Digital Evidence and Computer Crime, Third Edition, Elsevier, 2012

- John Sammons The basics of digital forensics, Syngress, 2012

- K S Rosenblatt High-Technology Crime: Investigating Cases Involving Computers, KSK Publications, 1995

- Kruse, W. & Heiser, J. Computer forensics: incident response essentials, Addison Wesley, 2002

- Marcella, A. & Greenfield Cyber forensics: A field manual for the collecting, examining, and preserving evidence of computer crimes, CRC Press, 2002

- Shinder, D Scene of the cybercrime: Computer forensics handbook, Syngress, 2002

- US Department of Justice Searching & seizing computers and obtaining electronic evidence in criminal investigations., Computer crime & intellectual property section US DoJ, 2001

ADDITIONAL BIBLIOGRAPHY

- Vrizlynn L.L. Thing, Kian-Yong Ng, Ee-Chien Chang Live memory forensics of mobile phones, doi:10.1016/j.diin.2010.05.010. ISSN 1742-2876, 2010

BASIC ELECTRONIC RESOURCES

- Safari Books Online . Proquest: //proquest.safaribooksonline.com

- n.a. . Forensic Wiki: //www.forensicswiki.org/wiki/Main_Page