Caracterização da Unidade Curricular / Characterization of the Curricular Unit

Designação da Unidade Curricular (UC) / Title of Curricular Unit (CU): Análise Forense Digital / Digital Forensic Analysis

Área científica da UC / CU Scientific Area: Ciências Informáticas / Computer Science

Semestre / Semester: 1º

Número de créditos ECTS / Number of ECTS credits: 6

Carga horária por tipologia de horas / Workload by type of hours: TP: 45; OT: 6; O: 9

Carga letiva semanal / Weekly letive charge: 3h

Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):

Os objetivos específicos pretendidos com a UC de Análise Forense Digital são:

- Conhecer, analisar e discutir criticamente, às normas da legislação vigente em torno das questões do cibercrime;
- Compreender às metodologias, tipos de análises e práticas utilizadas em computação forense;
- Compreender o processo da coleta forense e de composição da prova pericial;
- Realizar a implementação de procedimentos práticos, através da utilização de ferramentas e recursos computacionais para rastrear, recuperar, analisar e relatar dados e informações digitais.

Intended learning outcomes (knowledge, skills and competences to be developed by the students):

The specific objectives intended with the Digital Forensic Analysis UC are:

- Know, analyze and critically discuss the norms of the current legislation around cybercrime issues;
- Understand the methodologies, types of analysis, and practices used in computer forensics;
- Understand the process of forensic collection and composition of evidence;
- Carry out the implementation of practical procedures, through the use of computational tools and resources to track, retrieve, analyze, and report data and digital information.

Conteúdos programáticos:

1. Introdução aos fundamentos da análise e computação forense

1.1. Legislação acerca dos crimes cibernéticos

1.2. Direitos de propriedade intelectual e de autor

1.3. Normas técnicas sobre o tratamento de evidências e coleta forense (ISO 27037)

1.4. Investigação digital forense

1.5. Computação forense e prova pericial

2. Procedimentos computacionais técnicos fundamentais

2.1. Sistemas, dados computacionais e estruturas de ficheiros

2.2. Dispositivos de armazenamento de dados

2.3. Aquisição e recuperação de dados

2.4. Mapeamento de memórias e partições de discos rígidos

3. Procedimentos de investigação e análise forense digital

3.1. Esteganografia e análise de ficheiros

3.2. Cracking de palavras-passe

3.3. Análise de ficheiros de log de ambientes Windows e Linux

3.4. Análise de tráfego de rede, log de rede computacional

3.5. Monitorização de serviços e recursos em rede computacional

3.6. Rastreamento de e-mail

3.7. Investigação de ataques em redes wireless

3.8. Ataques cibernéticos na Web

3.9. Investigação e análise forense digital com Autopsy e FlareVM

4. Procedimentos e análise forense em dispositivos móveis (mobile)

4.1. Introdução aos conceitos de investigação forense mobile

4.2. Extração de dados de dispositivos mobile

4.3. Aplicações informáticas de investigação e análise forense em mobile

4.4. Extração de dados com a aplicação Magnet Acquire

4.5. Investigação e análise forense digital com a aplicação Santoku e Oxygen

Syllabus:

1. Introduction to the fundamentals of computer forensics and analysis

1.1. Legislation on cyber crimes

1.2. Intellectual property and copyright rights

1.3. Technical standards on evidence handling and forensic collection (ISO 27037)

1.4. Digital forensic investigation

1.5. Computer forensics and expert evidence

2. Fundamental technical computational procedures

2.1. Systems, computational data, and file structures

2.2. Data storage devices

2.3. Data acquisition and recovery

2.4. Mapping hard drive memories and partitions

3. Investigation procedures and digital forensic analysis

3.1. Steganography and file analysis

3.2. Password cracking

3.3. Analysis of log files for Windows and Linux environments

3.4. Network traffic analysis, computational network log

3.5. Monitoring of computer network services and resources

3.6. Email tracking

3.7. Investigation of attacks on wireless networks

3.8. Cyber attacks on the web

3.9. Digital forensic investigation and analysis with Autopsy and FlareVM

4. Procedures and forensic analysis on mobile devices (mobile)

4.1. Introduction to the concepts of mobile forensic investigation

4.2. Data extraction from mobile devices

4.3. Computer applications of investigation and forensic analysis on mobile

4.4. Data extraction with the Magnet Acquire application

4.5. Digital forensic investigation and analysis with the Santoku and Oxygen applications