CESPU
INSTITUTO UNIVERSITÁRIO
DE CIÊNCIAS DA SAÚDE

ANO LETIVO DE 2020-2021

CURSO DE LICENCIATURA EM CIÊNCIAS LABORATORIAIS FORENSES

Unidade curricular:

Cibercrime e Métodos Computacionais em Ciências Forenses

Curricular Unit:

Cybercrime and Computational Methods in Forensic Sciences

Docente responsável (preencher o nome completo):

Responsible teacher (fill in the fullname):

Rui Miguel Simões de Azevedo – TP: 26

Objetivos da unidade curricular e competências a desenvolver (1000 caracteres):

A proliferação de crime informático e de crimes comuns com recurso à informática, especialmente em redes como a Internet, obriga o futuro profissional a conhecer a legislação nesse domínio, e a reconhecer os diferentes vetores de ataque existentes e contramedidas, constituindo o primeiro objetivo da unidade curricular. Adicionalmente, a capacidade de tratamento automático de informação e a objetividade que é possível de atribuir a esse tratamento são as razões pelas quais a área de Computational Forensics tem emergido dentro das Ciências Forenses (CF).A unidade curricular (UC) tem por isso como segundo objetivo providenciar ao estudante a capacidade de utilizar uma linguagem de computação numérica, por forma a que possa implementar ferramentas que serão úteis em análise de dados de cibercrimes mas também em diferentes disciplinas das CF. Com esse conhecimento, o tratamento de dados de relevância forense será concretizado do ponto de vista prático. O estudante aprovado nesta unidade curricular deverá ser capaz de:
- conhecer legislação relevante no domínio do cibercrime, tipos de cibercrime e medidas de prevenção
- desenvolver programas em linguagens de computação numérica
- reconhecer algoritmos e criar formas de análise adequadas para dados de cibercrime e dados de outras especialidades forenses
- tratar computacionalmente dados em diversos formatos

Objectives of the curricular unit and competences to be developed

The proliferation of computer-related crimes and common crimes which are digitally supported, especially in networks such as the Internet, obliges the future professional to know the legislation in this field, and to recognize the different attack vectors and countermeasures, which constitutes the

first objective of the curricular unit. Additionally, the ability to process information automatically and the objectivity that is possible to attribute to that process are the reasons why the field of Computational Forensics has been emerging within Forensic Sciences (FS).The second objective of the course is to provide to the student skills in a numerical computing language such that he can implement tools which will be useful in cybercrime data analysis as well as across different disciplines in FS. With that knowledge, processing data relevant to forensics will be explored from the practical point of view. A student approved in this course should be able to:
- identify relevant legislation in the field of cybercrime, types of cybercrime and prevention measures
- develop programs in numerical computation languages
- recognize algorithms and create appropriate analysis methods for cybercrime and other forensic specialties data
- process data computationally in several formats

Conteúdos programáticos (1000 caracteres):

1 – Cibercrime
1.1. Legislação Nacional, Europeia e Mundial
1.2. Tipos de cibercrime
1.3. Princípios de segurança informática no contexto da Internet
2 – Ambientes de computação numérica (Octave)
2.1. Introdução ao Linux e ao Octave
2.2. Variáveis
2.3. Estruturas de controlo
2.4. Programas e funções
2.5. Input/Output
2.6. Representações gráficas
3 – Análise de dados em Cibercrime e outras especialidades forenses
3.1. Registos de servidores
3.2. Aplicações à esteganografia digital

Syllabus

1 – Cybercrime
1.1. National, European and World Legislation
1.2. Types of cybercrime
1.3. Principles of computer security in the context of the Internet
2 – Numeric computational environments (Octave)
2.1. Introduction to Linux and Octave
2.2. Variables
2.3. Control structures

2.4. Programs and functions

2.5. Input/Output

2.6. Graphical representations

3 – Data analysis in Cybercrime and other forensic specialties

3.1. Server logs

3.2. Applications to steganography

Referências bibliográficas (bibliography)

(máximo três títulos):

Os assuntos abordados na unidade curricular não são abordados na íntegra por um só livro em particular. As notas detalhadas do docente e os diferentes protocolos experimentais e folhas de exercícios fornecidas são suficientes para que um estudante complete com sucesso a unidade curricular. Algumas das notas são inspiradas em técnicas muito recentes. Contudo, o estudante beneficiará da leitura das seguintes referências principais:

- "Manual do GNU Octave" – disponível online gratuitamente
- "Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet", ISBN: 9780123742681

O regente: (data e nome completo):