

LABORATÓRIO DE ANÁLISE FORENSE

Pós-Graduação em Cibersegurança e Informática Forense

Código: 124008

Área Científica Predominante: Arquitetura de Computadores, Sistemas Distribuídos e Cibersegurança

Docente: Paulo Adriano Marques Sousa Teixeira

Idioma de Instrução: Português

Regime: S2

Carga Letiva: 20h Carga Trabalho: 60h

ECTS: 3,0

Objetivos

Pretende esta Unidade Curricular dotar os discentes do conhecimento necessário para a realização de análise forense, dando-lhes os ensinamentos basilares para a recolha, acondicionamento, análise de suportes digitais, interpretação de dados, tendo por base atingir um objectivo específico, e elaboração de relatório onde transpareça a sequenciação do processo e o resultado, perante os quesitos inicialmente determinados.

Resultados da Aprendizagem

- Definição de laboratório forense e regras a considerar;
- Identificação, manuseio e etiquetagem de suportes digitais, a utilizar em procedimentos forenses;
- Esterilização de suportes digitais;
- Processos de verificação de inviolabilidade de prova forense;
- Criação e gestão de dados forenses;
- Acções de um 'First Responder';
- Pesquisas forenses;
- Processos de análise de suportes digitais e dados;
- Sistema de ficheiros 'Fat32';
- Recuperação de dados em sistemas de ficheiros;
- Medidas antiforenses;
- Análise forense a equipamentos móveis;
- Relatório forense;

Conteúdos Programáticos

1. Polícia Judiciária e o cibercrime;

2. Laboratório de análise forense;
3. Análise forense (perspectiva de um perito);
4. Esterilização de dispositivos;
5. Cálculo de Hashing;
6. Criação e cópia de imagens forenses;
7. Gestão de imagens e extracção de informação;
8. Informação de sistema;
9. Pesquisas;
10. Memória RAM;
11. Registry;
12. Data Carving;
13. Recuperação de ficheiros
14. Medidas Anti-forenses;
15. Mobile forensics;
16. Relatório Forense;
17. Trabalho Final.

Bibliografia Recomendada

<https://www.ics.ulisboa.pt/projeto/policia-urbana-em-portugal-historia-da-policia-e-historias-de-policias-1860-1960>;

<https://www.psp.pt/Pages/sobre-nos/quem-somos/historia.aspx>;

<https://www.policiajudiciaria.pt/historial/>;

<https://www.itinsight.pt/news/seguranca/europol-aponta-as-tendencias-do-cibercrime>;

Métodos de Ensino e de Aprendizagem

Os conteúdos programáticos, concretamente a exposição dos temas, complementados com a realização de pequenos procedimentos práticos, possibilitarão a percepção das técnicas utilizadas nas práticas forenses, sendo testados os conhecimentos adquiridos quer pela resposta a perguntas com quesitos forenses digitais, quer através da apresentação do relatório onde são expostos os resultados obtidos.

Métodos de Avaliação

Elaboração de um trabalho prático final, com necessidade de resposta a algumas questões fundamentais, e elaboração de subseqüente relatório demonstrativo dos procedimentos e técnicas utilizadas e da informação obtida.