Co-funded by the
Erasmus+ Programme
of the European Union

Programa do Módulo 5: Fundamentos de forense digital

Carga de trabalho e ECTS

Aulas de vídeo: 8 horas

Trabalho autónomo: 67 horas

ECTS: 3

Resultados de Aprendizagem (Conhecimentos, Aptidões e Competências)

O módulo Comprehensive Digital Forensics Fundamentals fornece a utilização teórica e prática destes conhecimentos na recolha, análise e preservação de provas, resultando na sua constituição como prova em tribunal. Os conteúdos presentes no programa deste módulo, permitem consolidar o objectivo deste módulo. As competências a serem desenvolvidas são as seguintes:

1. O aluno conhece os modelos de análise forense digital;

2. O aluno conhece a relação entre pistas, evidências e crime;

3. O aluno realiza relatórios forenses;

4. O aluno no local, identifica, recolhe, adquire e conserva pistas digitais, utilizando diferentes técnicas, protegendo a integridade das provas;

5. O aluno utiliza as melhores práticas e procedimentos na aquisição e manipulação de provas digitais;

6. O aluno está familiarizado com várias técnicas forenses informáticas na recolha e análise de vários tipos de provas digitais, utilizando técnicas e ferramentas específicas.

Conteúdos

1. Conceitos, definições e modelos

2. Preservação e recolha de provas digitais no local do crime

3. Procedimentos de aquisição de provas digitais

3.1. Procedimentos de Esterilização

3.2. Técnicas de aquisição

4. Aquisição e análise de informação volátil

5. Identificação e análise de pontos de interesse de informação em Sistemas Operativos

6. Utilização de ferramentas de análise OpenSource

7. Estudos de casos forenses digitais

7.1 Estudo de Caso 1: Hacking com janelas Ferramentas SO

Demonstração da coerência do conteúdo com os resultados de aprendizagem da Unidade Curricular

Os objectivos deste módulo são o conhecimento teórico de conceitos forenses informáticos, e a utilização deste conhecimento na recolha, análise e preservação de provas, resultando na sua constituição como prova em tribunal. Os conteúdos presentes no programa deste módulo, permitem consolidar este objectivo do módulo.

Metodologias de Ensino

Vídeos teóricos e práticos, que incluem a apresentação de temas apoiados por demonstrações de professores, seguidos de questionários para avaliar a evolução dos alunos e a análise de casos de estudo do mundo real. De acordo com o desempenho dos alunos nos questionários, devem ser fornecidos diferentes vídeos aos alunos para reforçar as disciplinas em que a avaliação não atinge o nível mínimo declarado para a disciplina seguinte. Assim, cada aluno poderia ter o seu próprio percurso nos vídeos preparados para o módulo, de acordo com o seu desempenho.

Demonstração das Metodologias de Ensino Coerência com os Resultados de Aprendizagem da Unidade Curricular

As competências a atingir neste módulo estão divididas em duas áreas: o domínio teórico dos procedimentos de recolha, análise e preservação de provas. A metodologia de ensino adoptada divide-se em dois tipos de vídeos: vídeos de conferências teóricas e práticas centradas na consecução do objectivo relacionado com os conhecimentos teóricos das técnicas forenses informáticas e aulas laboratoriais orientadas para a aprendizagem do uso de ferramentas; vídeos de demonstração centrados na consecução do objectivo do uso eficiente de ferramentas de análise de pistas forenses digitais.

Métodos de avaliação

A avaliação baseia-se num conjunto de questionários, que se concentram em aspectos importantes de cada um dos conteúdos. Cada aluno deve atingir uma percentagem pré-configurada de respostas correctas para prosseguir para o próximo tópico sobre os conteúdos.

O apoio da Comissão Europeia à produção desta publicação não constitui uma aprovação do seu conteúdo, que reflecte apenas a opinião dos autores, e a Comissão não pode ser responsabilizada por qualquer utilização que possa ser feita das informações nela contidas.

Bibliografia principal

[1] BUNTING, Steve, The Official EnCE: EnCase Certified Examiner Study Guide, 2012.

[2] GRUNDY, Barry J., The Law Enforcement and Forensic Examiner's Introduction to Linux (http://www.linuxleo.com/Docs/linuxintro-LEFE-4.31.pdf), 2017.

[3] CASEY, Eoghan, Digital Evidence and Computer Crime, Academic press, 2011.

[4] BROWN, Christopher L. T., Computer Evidence: Recolha e Preservação, 2ª Edição, 2009.

[5] CARVEY, Harlan, Investigating Windows Systems, 1ª Edição, 2018.

[6] HALE LIGH, Michael, The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, e Mac Memory, 1ª Edição, 2014.

[7] ENISA, Identification and handling of electronic evidence Toolset, Setembro de 2013.

[8] ENISA, Identification and handling of electronic evidence Handbook, Setembro de 2013.

[9] NIST, Computer Security Incident Handling Guide, Publicação Especial 800-61r2.