Informação Geral:

Unidade Orgânica	Escola Superior de Tecnologia e Gestão	**Ano Letivo**	2017/2018
Curso	Mestrado em Engenharia Informática - Computação Móvel (D) [M238]	**Grau**	Mestrado
Ano Curricular	1	**Período**	S2
UC/Módulo	Análise Forense em Dispositivos Móveis a)	**ECTS**	6
Área Científica	Engenharia Informática	**Carácter**	Opcional

Horas Totais	161.6	**T**	0	**TP**	22.5	**PL**	30	**TC**	0	**S**	0	**E**	0	**OT**	0

T - Ensino Teórico; TP - Teórico Prático; PL - Prático e Laboratorial; TC - Trabalho de Campo; S - Seminário; E - Estágio; OT - Orientação Tutorial

Docente responsável:

Miguel Monteiro de Sousa Frade

Docentes que lecionam a unidade curricular:

Miguel Monteiro de Sousa Frade (52,50 horas semanais de contacto: TP: 22,50; PL: 30,00;)

Pré-requisitos:

Não há unidades curriculares pré-requeridas.
No entanto, recomendam-se conhecimentos de arquitectura de computadores, redes de dados e criptografia.

Idioma:

Português e Inglês

Enquadramento:

Quanto mais dependemos de aparelhos digitais nos mais variados aspectos das nossas vidas, mais este tipo de dispositivos estão envolvidos em investigações legais de todos os tipos. A análise forense digital é uma ciência dedicada à recolha, identificação, preservação, documentação, análise e apresentação de evidências digitais a partir de computadores, redes e outros dispositivos eletrónicos. A investigação forense é agora uma parte importante de muitas investigações criminais e civis; os seus instrumentos são frequentemente utilizados para a investigação, recuperação de dados e diagnósticos por agentes da lei e laboratórios privados. A área forense digital pode ser dividida em: computação forense, análise forense de redes de dados e análise forense de dispositivos móveis. Este curso tem como objetivo abordar os conceitos transversais a todas as áreas da ciência forense digital, tais como o método científico de investigação em forense digital e os diferentes tipos de evidências forenses digitais. Posteriormente, o curso foca-se na análise forense em dispositivos móveis. Os alunos irão aplicar os conhecimentos adquiridos através de vários trabalhos laboratoriais e realização de relatórios forenses.

Objetivos de aprendizagem:

Após a conclusão desta Unidade Curricular, o estudante deverá ser capaz de:

C01- Conhecer o código de conduta ético dos investigadores forenses digitais

C02- Identificar as diferentes fontes provas digitais forenses

C03- Recolher dados em suportes de armazenamento, redes de dados e dispositivos móveis

C04- Compreender e aplicar o método científico e a necessidade da sua utilização

C05- Utilizar ferramentas e técnicas de investigação forense digital

C06- Criar mapas de geolocalização

C07- Criar e usar hashsets

C08- Conhecer as limitações das técnicas atuais de investigação forense digital

C09- Conhecer o funcionamento dos principais sistemas operativos móveis

C10- Comunicar e reportar resultados de análise forense digital

Programa:

Conteúdos Programáticos:

1. Introdução à investigação forense digital

Privacidade e ética

Método científico

Conceitos técnicos básicos

2. Obtenção de provas

Procedimentos de 1ª intervenção

Fontes de provas

2.1 Suportes de armazenamento

Bloqueadores de escrita e cópias forenses

Partições MBR e GTP, volumes RAID

Sistemas de ficheiros FAT, NTFS, EXT4 e HPFS+

Integridade de cópia assinaturas digitais

3. Análise de imagens forenses com Autopsy

Espaço desalocado e slack

Ficheiros apagados

Metadados

Padrões de pesquisa

Incongruência do tipo de ficheiro e sua extensão

Limitações da análise forense digital

Navegação web

Clientes de email

Artefactos dos SO Windows, Linux e Mac OS X

4. Análise de redes de dados

Estudo da rede e recolha de tráfego

Geolocalização de IPs

Segmentação, cifra, temporalidade e localização

Anonimização de tráfego

5. SO móveis

Sistemas de ficheiros e estruturas de dados

Modelos de segurança

Geolocalização

Artefactos do Android, iOS e Windows Phone

Ferramenta XRY

6. Casos de estudo

Fundamentação da coerência dos conteúdos programáticos com os objetivos/competências da unidade curricular:

O tópico 1 visa dotar os estudantes das competências relacionadas com a aplicação do método científico e a ética dos investigadores forenses (C01, C04). O tópicos 2 visa dotar os estudantes das competências relacionadas com a identificação dos diversos meios para recolha de provas e conhecimento aprofundado dos suportes de armazenamentos de dados (C02, C03, C05). Os tópicos 3 e 4 permitirão dotar os estudantes com competências relacionadas com o uso de ferramentas para análise de provas digitais em suportes de armazenamento e redes de dados, bem como desenvolver as competências relacionadas com as insuficiências das técnicas de investigação forense digital (C05, C06, C07, C08). O tópico 5 aborda as estruturas e modelos de segurança dos principais sistemas operativos móveis (C05, C06, C08, C09). Por fim, no tópico 6 surge como a componente agregadora de competências que visa solidificar os objectivos de aprendizagem C04 e C10.

Metodologia de Ensino / Aprendizagem:

Presencial:

A metodologia a adotar para a generalidade das aulas Teóricas será o método expositivo. Nas aulas Práticas será aplicado o método ativo onde os alunos desenvolverão trabalhos laboratoriais que correspondem à aplicação dos conhecimentos teóricos e resolução autónoma de problemas.

Autónoma:

Consolidação dos conhecimentos teóricos.
Preparação das aulas laboratoriais e realização de exercícios.

Recursos Específicos:

Laboratório Informático: Computadores com >4GB RAM para usar máquinas virtuais
Internet
Plataforma de gestão e distribuição de conteúdos;
Software específico: VMware ou Virtual Box, Windows VM and Linux (kubuntu) VM e XRY Office
Recursos de apoio fornecidos pelo docente.

Avaliação:

Descrição:

Os resultados de aprendizagem são avaliados através de uma prova escrita individual (componente teórica) e de um projeto, em grupo, realizado ao longo do semestre (componente prática).

Avaliação periódica

Nota Final = 35% prova escrita individual + 65% projeto

mínimos: nenhum

Avaliação por exame final

Nota final = 35% prova escrita individual + 65% projeto

mínimos: nenhum

Notas:

- caso o estudante não se submeta a avaliação numa das componentes (teórica, ou prática), para o cálculo da nota final será usada a nota obtida na última época em que foi avaliado nessa componente no mesmo ano letivo;

- os alunos já aprovados, mas que desejam melhorar a sua nota, em exame têm obrigatoriamente de realizar as provas de ambas as componentes: teórica e prática;

Número de elementos de avaliação final:	2
Número de elementos de avaliação contínua/periódica:	2

Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular:

As metodologias de ensino estão em coerência com os objetivos da unidade curricular dado que:

1) Os métodos de ensino utilizados, ajustam-se à natureza dos conteúdos programáticos e dos objetivos a atingir em cada sessão. A realização de exposições sobre as diferentes matérias (demonstração e discussão), quer por parte do docente, quer dos estudantes, conjuga-se com a metodologia de avaliação estabelecida, permitindo assim atingir os objetivos definidos;

2) Competências complementares como sejam o trabalho de equipa, comunicação escrita e verbal serão também exploradas no âmbito da UC;

O regime de avaliação foi concebido para avaliar a extensão e o nível de aquisição das competências a desenvolver.

Bibliografia:

Recomendada:

[1] Sammons, J. (2012). The basics of digital forensics: the primer for getting started in digital forensics. Elsevier.

[2] Carrier, B. (2005). File system forensic analysis. Addison-Wesley Professional.

[3] Altheide, C., & Carvey, H. (2011). Digital forensics with open source tools. Elsevier.

[4] Tamma, R., & Tindall, D. (2015). Learning android forensics. Packt Publishing Ltd.

[5] Epifani, M., & Stirparo, P. (2015). Learning iOS Forensics. Packt Publishing Ltd.

Complementar:

[1] Shavers, B. (2013). Placing the suspect behind the keyboard: using digital forensics and investigative techniques to identify cybercrime suspects. Newnes.

[2] Carvey, H. (2009). Windows Forensic Analysis Toolkit, Fourth Edition: Advanced Analysis Techniques for Windows 8, 4th edition. Syngress.

[3] Carvey, H. (2011). Windows Registry forensics: advanced digital forensic analysis of the Windows Registry. Elsevier.