Trabalho Prático 7

CET 8493 | UFCD 9196 - Cibersegurança Ativa | Formador: Paulo Vaz

Formando: João Rodrigo Mota da Costa

1. O que é análise forense digital e como é utilizada em investigações criminais?

A análise forense digital é o processo de recolha, preservação, análise e apresentação de evidências digitais em investigações criminais ou civis. É usada para interpretar informações digitais, como arquivos, emails, registos de navegação na web e logs de rede, a fim de descobrir a origem, a autoria e a extensão de um crime.

2. Quais são as principais etapas de um processo de análise forense digital?

As principais etapas de um processo de análise forense digital incluem a identificação e preservação das evidências digitais, a extração de dados relevantes, a análise e interpretação das informações recolhidas e a apresentação dos resultados em um relatório forense.

3. Quais são as ferramentas e técnicas mais comuns utilizadas em análise forense digital?

As ferramentas e técnicas mais comuns utilizadas em análise forense digital incluem programas de recuperação de dados, ferramentas de imagem forense, técnicas de criptografia e análise de registos de eventos.

4. Como é que os peritos podem coletar e preservar evidências digitais sem comprometê-las?

Os peritos podem recolher e preservar evidências digitais seguindo as melhores práticas da indústria, como fazer uma cópia *bit-for-bit* do dispositivo de origem para um dispositivo de destino, armazenar as evidências num local seguro e seguir uma cadeia de custódia documentada para garantir que as evidências sejam autênticas e admissíveis em tribunal.

5. Como é feita a análise de dispositivos de armazenamento, como discos rígidos e pendrives, durante uma investigação?

A análise de dispositivos de armazenamento, como discos rígidos e *pens*, envolve a cópia do conteúdo do dispositivo para uma imagem forense e a análise dos arquivos e dados presentes na imagem. Isso pode incluir a análise de arquivos de sistema, logs de eventos, arquivos de *media* e documentos.

6. Como é que os peritos podem recuperar ficheiros apagados ou corrompidos durante uma investigação?

Os peritos podem recuperar ficheiros apagados ou corrompidos usando programas de recuperação de dados, que fazem *scan* ao dispositivo à procura de dados fragmentados ou apagados e recuperá-los para análise forense.

7. Quais são os desafios e limitações da análise forense digital?

Os desafios e limitações da análise forense digital incluem a complexidade dos sistemas e tecnologias envolvidos, a rapidez com que a tecnologia muda, a necessidade de recursos especializados e a possibilidade de falsificação ou adulteração de evidências digitais.

8. Como a análise forense digital é utilizada em casos de crimes cibernéticos, como roubo de identidade e phishing?

A análise forense digital é usada em casos de crimes cibernéticos para recolher evidências digitais, como registros de navegação na web, e-mails e mensagens eletrônicas, para identificar e rastrear os autores do crime.

9. Quais são as implicações éticas e legais da análise forense digital?

As implicações éticas e legais da análise forense digital incluem a proteção da privacidade e dos direitos dos indivíduos, a necessidade de seguir as melhores práticas da indústria para coleta e preservação de evidências digitais, e a garantia de que as evidências coletadas são autênticas e admissíveis em tribunal.

10. Como a análise forense digital pode ser utilizada para prevenir e detetar crimes?

A análise forense digital pode ser utilizada para prevenir e detetar crimes através da monitorização de atividades suspeitas, como acesso não autorizado a sistemas ou transferência de arquivos não autorizada, e pela criação de políticas de segurança da informação que ajudem a evitar violações de dados e a proteger informações confidenciais.