Computação Forense – Exercícios

CCA UFES – Departamento de Computação
Prof. Msc. Jacson Rodrigues

Questões

1. Descreva a estrutura (organização dos diretórios e dos arquivos) dos seguintes sistemas de arquivos: FAT, NTFS, MFS, iNode, HFS, EXT, Raiser.
2. Como recuperar arquivos nos sistemas de arquivos citados no exercício 1?
3. O que são cópias bit-stream?
4. O que são cópias raw?
5. Liste 2 aplicativos que podem ser utilizados no Windows e 2 no Linux para duplicar discos de evidências.
6. Descreva todos os passos de uma perícia.
7. Quais informações podem ser obtidas dentro de um programa?
8. Quais as informações que podem ser obtidas do programa PE Explorer?
9. Existem formas de alterar a execução de um programa sem a necessidade de compilá-lo novamente? Dê um exemplo.
10. O que é *slack space* e por que o mesmo pode ser utilizado em uma perícia?
11. O que é a assinatura de arquivos MZ? Onde pode ser encontrada? Como efetuar a perícia em arquivos com essa assinatura?
12. Como ocorre a troca de pacotes entre duas máquinas (utilize como exemplo um browser para acessar um servidor Web)? Qual a segurança existente sobre o protocolo HTTP e a troca de dados? E sobre o protocolo HTTPS?
13. O que é o protocolo *socks* e como utilizá-lo?
14. Como criar um DNS privado?
15. O que são proxies e qual sua finalidade?
16. O que são malwares?
17. Defina esteganografia.
18. Onde a esteganografia pode ser utilizada?
19. Como obter os dados de um arquivo esteganofrado?
20. Como implementar métodos/aplicativos de esteganografia?