

Exercícios – Computação Forense – CCA UFES – Prof. Msc Jacson Rodrigues

1. Qual a diferença entre a recuperação de arquivos e a perícia forense?
2. Onde as informações para a perícia digital podem ser obtidas? Dê exemplos.
3. O que é uma evidência digital? E uma evidência física?
4. Como realizar a coleta de evidências digitais?
5. O que é um litígio? Dê um exemplo.
6. Para você, o que é computação forense?
7. Quais assuntos se destacaram na história da computação forense?
8. Detalhe cada uma das etapas do processo de investigação digital.
9. Em qual momento um dado volátil deve ser coletado? Por quê? Dê exemplo de uma situação onde isso seja necessário.
10. Qual a função de *hashes* na cópia digital? Dê exemplos.
11. Qual a diferença quanto a tempo e tamanho dos *hashes* md5sum e shasum?
12. Como examinar os dados?
13. Como buscar por arquivos de formatos específicos em um sistema de arquivos?
14. Como deve ser realizada a análise de informações e a obtenção de resultados?
15. O que um Laudo? Como deve ser redigido? Quais informações deve abrigar?
16. Qual a importância de um Laudo bem escrito?
17. Qual o conhecimento necessário para criar ferramentas forenses?
18. O que é e como utilizar uma Cadeia de Custódia? Dê um exemplo.
19. O que é esterilização de uma mídia? Qual sua necessidade?
20. O que é um MAC time? Como pode ser utilizado (dê um exemplo)? Como implementá-lo?
21. O que é o princípio da troca de Lacard?
22. Quais as etapas necessárias para atuar com evidências? Explique a necessidade de cada uma.
23. Como agir no local da perícia?
24. O que é uma Jurisdição? E uma Jurisprudência? Quando deve ser utilizada?
25. O que é Código Penal e Código de Processo Penal?
26. Crie um texto descrevendo o que a lei brasileira estabelece sobre o perito e sobre uma perícia realizada.
27. Qual a importância de ser imparcial em uma perícia?
28. O que pode ocorrer a um perito intimado que não compareça a perícia?
29. Como uma invasão de computadores pode ser protegida pela lei brasileira?
30. O que é um mandado de intimação?
31. O que é um laboratório forense? Quais suas características e quais os itens básicos necessários?
32. O que é refrescamento? Quando deve ser realizado em uma mídia?
33. Como analisar os dados de uma mídia de forma segura?
34. Explique todas as etapas de uma perícia na empresa ARRÉ para buscar documentos roubados da empresa LARRÉ.