Computação Forense – Exercícios – Lista 07

Questões

1. Quais as dificuldades encontradas por um perito ao encontrar uma técnica anti-forense na cena do crime? Descreva dando exemplos para wipe, esteganografia, slack space e criptografia.
2. Busque na Internet e descreva pelo menos um sofware para cada item abaixo:
   a) realizar o wipe de uma mídia;
   b) realizar esteganografia;
   c) pesquisar por slack spaces;
   d) escrever em slack spaces;
   e) fazer criptografia;
   f) buscar esteganografia;
   g) quebrar criptografia.
3. Descreva como realizar a perícia ao encontrar um dado criptografado no computador da pessoa (Ex.: arquivo.zip).
4. Baixe a versão free do aplicativo WinHex[1] e descreva como realizar a busca por slack spaces utilizando-o.
5. Como os timestamps podem ser modificados?
6. O que são rootkits e como são utilizados?
7. Como detectar rootkits?

1 <https://www.x-ways.net/winhex/forensics.html>