Computação Forense – Exercícios – Lista 01

Questões

1. Defina computação forense com suas palavras.
2. O que são evidências? Cite três exemplos.
3. Suponha que uma empresa tenha seus dados roubados do servidor por um funcionário interno. Descreva como seria sua busca pelas provas necessárias e como seria construído seu laudo final.
4. Suponha que uma empresa suspeite que seu funcionário enviou e-mails com informações confidenciais de seus dados bancários. Porém, o funcionário afirma que não foi ele e que ele não tem nada a ver com o caso.
   a) Como eles devem agir para resolver o problema?
   b) Qual o trabalho do perito nessa situação?
5. Instale o Kali Linux ou outra distribuição Linux que permita fazer análise forense em uma Máquina Virtual (Virtual Box, por exemplo). Se quiser instalar no seu computador também ou em um pendrive, é uma boa opção. Após isso, faça:
   a) Faça uma ficha com a descrição de todos os comandos utilizados nesse exercício. Use o "`man`" e também a Internet para entender o que está sendo feito em cada um deles.
   b) Insira um pendrive.
   c) Verifique onde ele está disponível no sistema:
      (a referência para *pendrives* e *HDs* iniciam com "`sd`" e cartões com "`mmcblk`")
      - `dmesg | tail          #ou`
      - `cat /proc/partitions  #ou`
      - `cat /proc/diskstats   #ou`
      - `ls /dev/sd*`
   d) Com o `LOCAL` encontrado, monte sua partição para verificar os arquivos que ele possui:
      - `mkdir part`
      - `sudo mount -o ro /dev/LOCAL part`
      - `cd part`
      - `find -type d`
      - `find -type f`
      - `find -type f -exec md5sum {} \; > ../arquivos_md5.txt`
      - `cd ..`
      - `cp -r part copia`
      - `sudo umount part`
   e) Abra o arquivo `arquivos_md5.txt` e discuta seu conteúdo.
   f) Repita o processo da letra *d*. Porém, faça o `sha1sum` de todos os arquivos.
   g) Pesquise os arquivos apagados:
      - `sudo fls /dev/LOCAL | grep '*' #fls é um programa do sleuthkit`
   h) Salve a lista de arquivos apagados em um arquivo.
   i) Utilize o programa `testdisk` para ver e restaurar alguns dos arquivos apagados.
   j) Recupere todos os arquivos apagados:
      - `sudo foremost -T -o recup /dev/LOCAL`
      - `sudo chown -R $USER recup*`
   k) Verifique os arquivos apagados.
   l) Busque por outros programas de recuperação de arquivos e os aplique sobre sua mídia já pesquisada. Há diferença entre o resultado desses programas?