Computação Forense – Exercícios – Lista 02

Questões

1. Para cada uma das etapas do processo de investigação digital:
   a) Qual é o nome?
   b) O que deve ser analisado?
   c) Quais são as tarefas que devem ser feitas?
2. Crie um exemplo que demonstre todas as etapas descritas na questão 1.
3. Baseando-se na prioridade da coleta de dados, responda como seria o processo de coleta do seguinte caso:
   - Um homem foi indiciado por pedofilia. Sendo também integrante de um grupo que trocava fotos e vídeos referentes na Internet. Ao fazer a busca em sua casa, esse homem estava utilizando seu computador pessoal e seu laptop estava desligado na cama.
4. Execute e descreva os comandos abaixo (utilize o *man* para lhe ajudar):
   - `gpg --gen-key`
     (responda assim:
     `0 – 2048 – 0 – "s" ou "y"`
     `Nome completo:` *`coloque seu nome`*
     `Endereço de correio eletrônico:` *`coloque seu e-mail`*
     `Comentário:` *`deixe em branco`*
     `Chave secreta:` *`deixe em branco`*)
   - `gpg --list-secret-keys #chave secreta criada`
   - `gpg --list-public-keys #chave pública criada`
   - `mkdir exercicio4`
   - `cd exercicio4`
   - `wget -O - -q https://goo.gl/ipuy2N | tar xvf -`
   - `ls *.jpg`
   - `(md5sum *.jpg;sha1sum *.jpg;) > hash.txt`
   - `gpg --sign hash.txt`
   - `ls hash*`
   - `gpg --armour --sign hash.txt`
   - `ls hash*`
   - `rm -fv hash.txt`
   - `gpg hash.txt.gpg`
   - `ls hash*`
   - `cat hash.txt`
   - `rm hash.txt`
   - `gpg hash.txt.asc`
   - `ls hash*`
   - `md5sum --check --ignore-missing hash.txt`
   - `sha1sum --check --ignore-missing hash.txt`
5. Execute e descreva os comandos abaixo:
   - `wget https://goo.gl/gcVviN -O texto.txt`
   - `grep --color mas texto.txt`
   - `grep --color -i mas texto.txt`
   - `grep --color -i -m1 mas texto.txt`
   - `grep --color -i -o 'Mas.*?' texto.txt`
   - `grep --color -o -e '[A-Z][A-Z][A-Z]' texto.txt`
6. Execute e descreva os comandos abaixo:
   - `wget -q -O - https://goo.gl/dqSMPk | tar xvf -`
   - `strings arq.exe > strings-01.txt`
   - `strings -n 5 arq.exe > strings-02.txt`

- `hexdump -C arq.exe > hexdump.txt`
- `objdump -D arq.exe > objdump.txt`
- `objdump -p arq.exe`
- `grep -i '\.dll' strings-01.txt`
- `grep -i '\.dll' strings-02.txt`
- `grep -i '\.dll' hexdump.txt`

7. O que são assinaturas de arquivos? Dê um exemplo.
8. O que é *Live Forensics* e *Post Motern Forensics*?
9. Execute e descreva os comandos abaixo:
    - `ps faux`
    - `pstree`
    - `lscpu`
    - `lsblk`
    - `lspci`
    - `lsusb`
    - `lslogins`
    - `lshw`
    - `lsmod`
    - `xterm &`
    - `pidof xterm`
    - `xprop #clique em um programa agora`
10. Acesse o site da Microsoft <https://docs.microsoft.com/en-us/sysinternals/> e:
    a) Faça um catálogo com as ferramentas da Microsoft..
    b) Descreva como utilizar os *sysinternals* sem efetuar sua instalação no computador.
    c) Explique quais ferramentas e como as utilizaria para fazer a perícia da questão 3.
11. Siga os passos abaixo para fazer um *dump* em uma mídia de armazenamento. Logo após, descreva o que é feito em cada um dos comandos realizados.
    - `Insira um pendrive ou um cartão de memória no computador.`
    - `Descubra onde foi criado seu link para acesso em /dev (LOCAL)`
    - `Faça o dump (cópia raw / cópia bit a bit):`
        - `dd if=/dev/LOCAL of=copia1.img bs=1024`
        - `dfcldd if=/dev/LOCAL of=copia2.img hash=md5 md5log=copia2.md5`
    - `verifique a integridade das cópias:`
        - `md5sum /dev/LOCAL copia1.img copia2.img`
    - `Instale o VirtualBox e execute os LiveCDs abaixo nele:`
        - `Kati`
        - `Caine`
        - `Deft-Z`
        - `Parrot`
    - `Para cada um dos LiveCDs, utilize seus aplicativos para vasculhar a cópia da mídia de armazenamento e encontrar arquivos e informações apagadas.`
12. Qual é a diferença do *dd* e do *dcfldd* ?
13. Estude, utilize e explique sobre a seguinte ferramenta: <http://www.forensicswiki.org/wiki/Ddrescue>
14. Execute e explique os seguintes comandos:
    - `man ascii`
    - `python -c 'print 0x41'`
    - `python -c 'print chr(0x41)'`
    - `python -c 'for i in "Nome": print "%#x" % ord(i)'`
    - `python -c 'print u"\u3126"' #Google: unicode`
15. Crie um aplicativo capaz de encontrar um *File Signature* dentro de um arquivo qualquer.
16. Utilize o aplicativo da questão 15 para procurar arquivos na cópia do exercício 11.