Exercícios Respondidos – by Jeiks

1. Defina Unix Epoch.
A Era UNIX ou Posix Time ou Unix epoch ou Unix Timestamp teve início no dia a 1 de janeiro de 19701 . O nome se deve ao fato de esta data, dia 1 de janeiro de 1970 às 00:00:00 do Tempo Universal Coordenado (UTC) no calendário gregoriano proléptico, ser o marco zero do sistema de calendário usado pelo sistema operacional UNIX. Também pode ser chamada de era POSIX.
O horário Unix, definido como o número de segundos passados desde o epoch, não considerando segundos bissextos, é largamente utilizado em sistema operacionais do tipo Unix bem como em outros sistemas. Ele não é uma representação linear nem uma representação verdadeira do tempo UTC, por não considerar os segundos bissextos (e.g. 31-12-1998-12 23:59:60).

2. Confira o hash MD5 da imagem comprimida. Sempre faça isso. Depois, calcule os hashes SHA1, SHA224, SHA256, SHA384 e SHA512 da imagem descomprimida, colocando os resultados dentro de um arquivo.

md5sum...
d025dd88553fb71e2c1ba2849a59114d *caso_00.dd*
a093f2e85a7674ae873b555f31f6def5 *caso_00.dd.bz2*

sha1sum...
eba92bb2702912b88b1de9795bf9b9d4198e1548 *caso_00.dd*
95fe8b9580c133e7d334cb62350227e65e508d61 *caso_00.dd.bz2*

sha224sum...
39f39b1c18f68f8bf770ea22f6cef08d3b540d54e9aa7dfed89ec347 *caso_00.dd*
2789734fe32f087f62a63f8c0c54e8ef0487a95729dc5ff62233d959 *caso_00.dd.bz2*

sha256sum...
73f5a44fadf8731261cb70352ed68599aef082a8d89572487394ab20a5e68641 *caso_00.dd*
d8e937a3beaea8576c2cc5bf1cc6c6eaf9679a9f2363e117623079efecc5f0be *caso_00.dd.bz2*

sha384sum...
00a285e5ce9a6a148768bf24337fc4faf58ebd3d357c7b8ded4ff86ed057f8cbf364a87d7c645355a47f4b1e3ff2444f *caso_00.dd*
7b96636332825067eda4783f75b528416396b058f5936a40bad863f59c7c1c0ab9a3866c5ac588aadd16319305ba7172 *caso_00.dd.bz2*

sha512sum...
3af18bf5bc0093506faea435c1d0352e8e5cea5c7f998c67edc2a95c95a404f8299db5c3a75bb3af26718c9b461e9c545228de61b65ad54b866ed8d6cd490d03 *caso_00.dd*
1e79978b8140e9809d859426fced56d597a388de93dea7901b7382d4eba563a3bf4e7f7b146d0ac2a90d174b40934e62cd0520ea6eb830c8c94997a85d896398 *caso_00.dd.bz2*

3. Qual filesystem foi utilizado no pendrive? (file / hexedit / fsstat)
$ file caso_00.dd
caso_00.dd: x86 boot sector, code offset 0x58, OEM-ID "MSDOS5.0", sectors/cluster 4, reserved sectors 382, Media descriptor 0xf8, heads 255, sectors 2007040 (volumes > 32 MB) , FAT (32 bit), sectors/FAT 3905, reserved3 0x1800000, reserved 0x1, serial number 0xf423afb0, unlabeled

$ fsstat caso_00.dd
FILE SYSTEM INFORMATION

File System Type: FAT32

OEM Name: MSDOS5.0

$ hexedit caso_00.dd
MSDOS5.0 FAT32

4. Quantos setores possui o pendrive? (file / fsstat / fdisk -lu)
$ fsstat caso_00.dd
File System Layout (in sectors)
Total Range: 0 – 2007039

$ file caso_00.dd
sectors 2007040

$ /sbin/fdisk -lu caso_00.dd
Disk caso_00.dd: 1027 MB, 1027604480 bytes
255 heads, 63 sectors/track, 124 cylinders, total 2007040 sectors

5. Quantos arquivos estão acessíveis para usuários? (fls -ruF + grep -v + wc -l / find + wc -l no ponto de montagem)
```
$ fls -ruF caso_00.dd | grep -v 'SOUZA\|v/v' | wc -l
```
10
```
$ find -type f | wc -l
```
10

6. Quais tipos de arquivos estão acessíveis para usuários? (sorter -d / find -type f + egrep -o + sort -u)
```
$ mkdir sorter_index
$ sorter -d sorter_index caso_00.dd
$ cd sorter_index
$ for i in *;do
      echo -n "${i%.*} = "
      grep Image:.*Inode: $i | wc -l
done
```
documents = 6
images = 4
mismatch = 2
sorter = 0
text = 3
unknown = 12

ou

*$ egrep -o Image: * | uniq -c*
```
     6 documents.txt:Image:
     4 images.txt:Image:
     2 mismatch.txt:Image:
     3 text.txt:Image:
    12 unknown.txt:Image:
```

7. Qual é o inode do arquivo "Literary Review.doc" dentro da imagem original? (fls -rF)
$ fls -ruF caso_00.dd
…
r/r 18: Literary Review.doc
…

8. Qual é o inode do arquivo "Literary Review.doc" no ponto de montagem, dentro do filesystem do seu HD? (ls -li / stat)
$ ls -li Literary\ Review.doc
113 -rwxr-xr-x 1 root root 130048 Set 23 2009 Literary Review.doc

$ stat Literary\ Review.doc
File: "Literary Review.doc"
Size: 130048 Blocks: 256 IO Block: 2048 arquivo comum
Device: 700h/1792d Inode: 113 Links: 1

9. Explique porque há uma diferença no número dos inodes encontrados nos dois itens anteriores e cite qual deles é o correto para referenciar o arquivo em questão.
O problema ocorre porque o sistema de arquivos FAT não possui Inodes. Assim, o driver responsável por montar o sistema de arquivos sobre o VFS (Virtual File System – Camada de abstração criada sobre um sistema de arquivos para fornecer acesso superior igualitário as ferramentas do usuário) criará um novo número de inode cada vez que o sistema for montado, pois o catálogo e as referências aos arquivos e inodes são criadas dinamicamente.
O correto de referenciar é o inode da imagem, pois o mesmo sempre será calculado pela sua posição (onde está gravado) no sistema de arquivos.

10. Qual é a data da criação ou última modificação do arquivo "Literary Review.doc" no filesystem? (fls -rF ou find + grep para encontrar o arquivo) (ls -l / stat / fls + istat para ver a data)

$ fls -rF caso_00.dd | grep Literary\ Review.doc
r/r * 15: Literary Review.doc (REMOVIDO)
r/r 18: Literary Review.doc
r/r * 23: .~lock.Literary Review.doc# (REMOVIDO)

Do arquivo que não foi removido:
$ istat caso_00.dd 18
...
Written: Wed Sep 23 21:12:00 2009
Created: Fri Aug 13 16:23:58 201

Do arquivo removido:
$ istat caso_00.dd 15
...
Written: Fri Aug 13 14:30:50 2010
Created: Fri Aug 13 14:30:49 2010

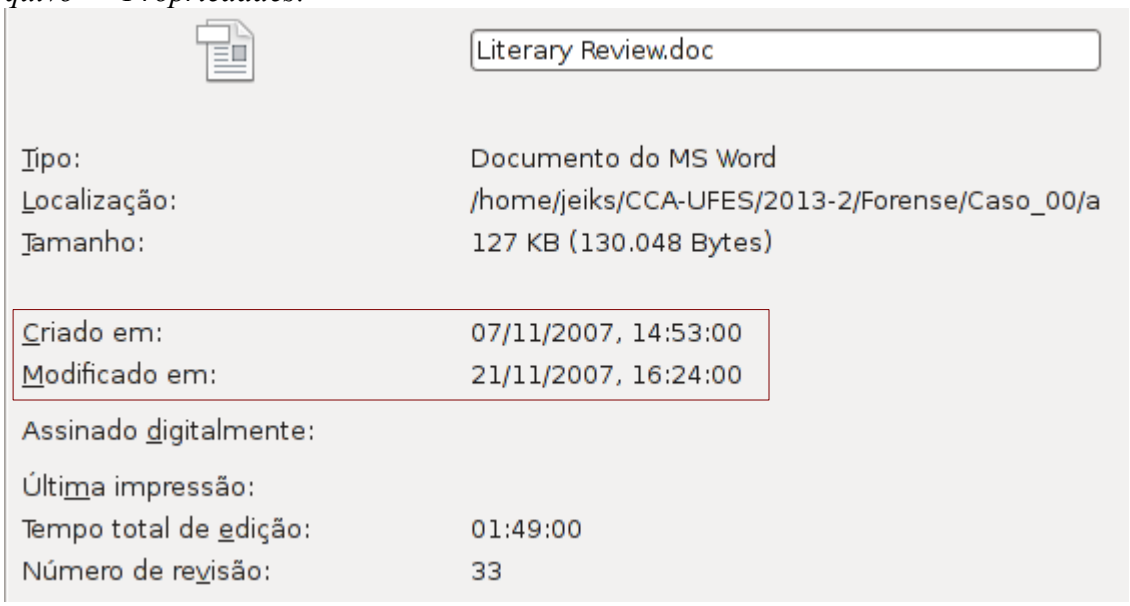
Do arquivo de trava:
$ istat caso_00.dd 23
...
Written: Fri Aug 13 11:48:28 2010
Created: Fri Aug 13 11:48:26 2010

11. Qual é a data do último acesso ao arquivo "Literary Review.doc" no filesystem? (fls ou find para encontrar o arquivo) (ls / stat / fls + istat)
Do arquivo que não foi removido:
$ istat caso_00.dd 18
...
Accessed: Sat Nov 21 00:00:00 2009
...

Do arquivo removido:
$ istat caso_00.dd 15
...
Accessed: Fri Aug 13 00:00:00 2010
…
Do arquivo de trava:
$ istat caso_00.dd 23
...
Accessed: Fri Aug 13 00:00:00 2010
...

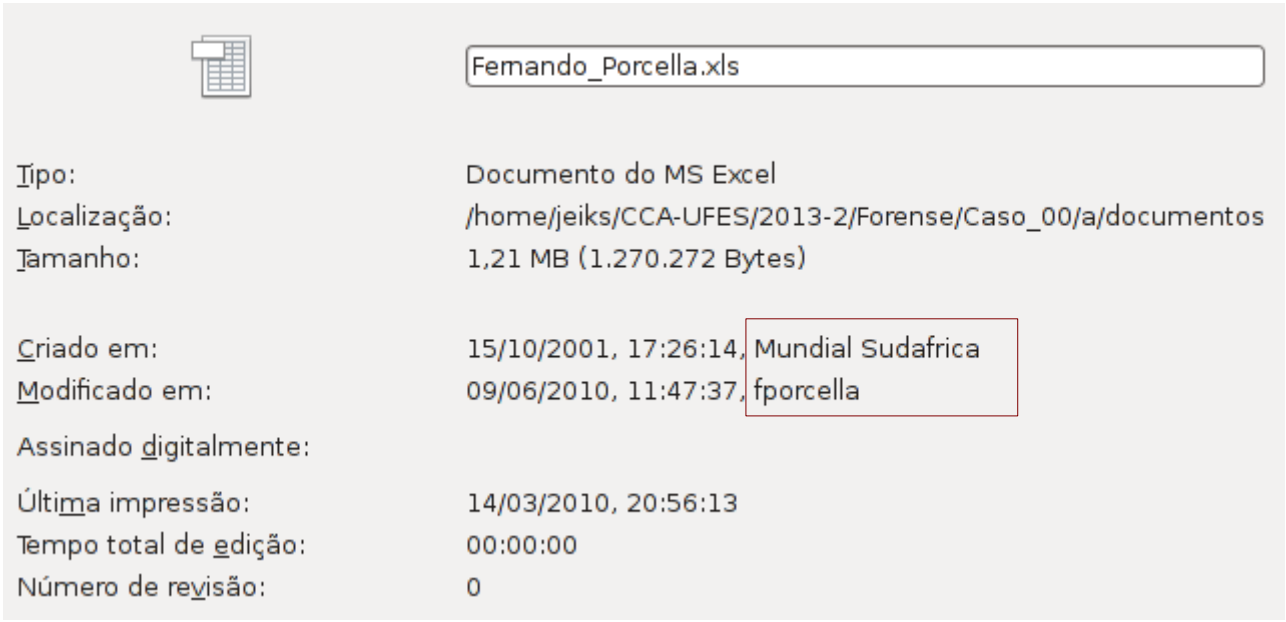
12. Quais são as datas de criação e última modificação do conteúdo arquivo "Literary Review.doc"? (dados no próprio arquivo) (ooffice / libreoffice)*

Em Arquivo → Propriedades:



13. Quem é o criador do conteúdo do arquivo "Fernando_Porcella.xls"? (dados no próprio arquivo) (ooffice / libreoffice / file)
*$ find -iname '*fernando*xls'*
./documentos/diversos/Fernando_Porcella.xl

Nas propriedades do documento (dentro do libreoffice):



$ file -Lks Fernando_Porcella.xls
Fernando_Porcella.xls: Composite Document File V2 Document, Little Endian, Os: Windows, Version 5.1, Code page: 1252, Title: Mundial Sudafrica 2010, Subject: World Cup SouthAfrica 2010, *Author: Mundial Sudafrica*, Keywords: Calendario Sudafrica 2010; Sudafrica 2010, Mundial de futbol, Mundial 2010, Comments: webmaster@mundialsudafrica.com, *Last Saved By: fporcella*, Name of Creating Application: Microsoft Excel, *Last Printed: Sun Mar 14 22:56:13 2010*, Create Time/Date: Mon Oct 15 20:26:14 2001, *Last Saved Time/Date: Wed Jun 9 13:47:37 2010*, Security: 0

14. Quem foi a última pessoa que modificou conteúdo do arquivo "Fernando_Porcella.xls"? (dados no próprio arquivo) (ooffice / libreoffice / file)
Resposta na questão 13:
Last Saved By: fporcella

15. Quando se deu a última impressão do conteúdo do arquivo "Fernando_Porcella.xls"? (dados no próprio arquivo) (ooffice / libreoffice)*
Resposta na questão 13:
Last Printed: Sun Mar 14 22:56:13 2010

16. Qual foi a data da última modificação do conteúdo da foto "paola-carvalho.jpg"? (dados no próprio arquivo) (strings + grep / hexedit)
Resposta na questão 13:
Last Saved Time/Date: Wed Jun 9 13:47:37 2010

17. Qual foi o software utilizado para fazer a modificação do conteúdo da foto "paola-carvalho.jpg"? (dados no próprio arquivo) (strings + grep / hexedit)
$ strings paola-carvalho.jpg | head
JFIF
Exif
Adobe Photoshop CS Windows
2008:12:19 18:22:12
JFIF
Adobe_CM
Adobe

18. Qual foi o software utilizado para produzir o documento "sec-us-

networkbasedfirewallservice.pdf"? (evince / okular / strings / strings + grep / hexedit)
Propriedes do arquivo obtidas do evince:

Produtor:	Adobe PDF Library 8.0
Criador:	Adobe InDesign CS3 (5.0.4)
Criado:	Ter 17 Nov 2009 10:21:10 BRST
Modificado:	Ter 17 Nov 2009 10:21:13 BRST
Formato:	PDF-1.4

$ strings sec-us-networkbasedfirewallservice.pdf | grep 'Producer\|Creator'
<pdf:Producer>Adobe PDF Library 8.0</pdf:Producer>
<</CreationDate(D:20091117102110-06'00')/Creator(Adobe InDesign CS3 \
(5.0.4\))/Producer(Adobe PDF Library 8.0)/ModDate(D:20091117102113-06'00')/Trapped/False>>

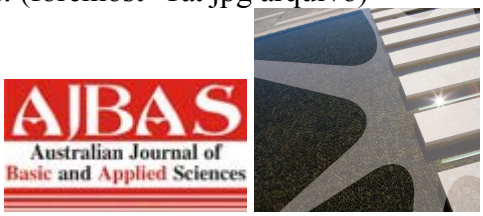
19. Qual foi a data de modificação do conteúdo do documento "1632-1640.pdf"? (dados no próprio arquivo) (evince / okular / strings + grep / hexedit)

Título:	Corel Office Document
Autor:	majid
Criador:	PScript5.dll Version 5.2.2
Produtor:	Acrobat Distiller 9.0.0 (Windows)
Páginas:	9
Criado:	ter 20 jul 2010 12:02:14
Modificado:	ter 20 jul 2010 12:02:14

20. Quem criou o conteúdo do documento "1632-1640.pdf"? (dados no próprio arquivo) (evince / okular / strings + grep / hexedit)
Resposta na questão 19

21. Pode-se afirmar que todas as datas levantadas nas perguntas anteriores são verídicas? Por quê?
Não, pois o binário pode ter sido alterado manualmente através de acesso direto. Isso permitiria que os valores apresentados nas propriedades dos arquivos fossem modificadas.
O relógio do computador e/ou o timezone também poderiam estar errados durante criação do arquivo.
Também troca-se a data do arquivo ao clicar no botão "Redefinir", dentro da caixa propriedades.

22. Dentro dos arquivos "sec-us-networkbasedfirewallservice.pdf" e "1632-1640.pdf" existem figuras JPG. Extraia as mesmas. (foremost -Tat jpg arquivo)



23. O que representa o número que o comando foremost utiliza como nome de cada arquivo encontrado?
É referente ao número do bloco onde se encontra o arquivo resgatado. Na imagem do arquivo 1632-1640.pdf, por exemplo: 00000019.jpg = 19º bloco, sendo por padrão blocos de 512bits
*Ao verificar o arquivo com o 'hexedit', encontra-se o jpg na posição 0x2760, que está dentro do 19º bloco. Este se inicia na posição 0x2600 (19*512) e termina na posição 0x27FF (19*512-1)*
*Isso é comprovado ao utilizar o foremost com a opção "-b 1024", opçãp responsável por utilizar blocos de 1024 bits. Com essa opção, a imagem resgatada passa a apresentar o número 9, pois o bloco 9 inicia em 0x2400 (9*1024) e termina em 0x27FF (10*1024-1)*