

## SI: LABORATORIO 6 ANALISIS FORENSE

Por Mònica Benet Cosculluela

Después de ejecutar Autopsy y crear un caso con la imagen.zip que simboliza el floppy disk a analizar, usando la terminal de comandos he buscado los espacios sin asignar de la imagen usando la herramienta blkls.

```
alumni@alumni-virtual-machine: ~
* python-q-text-as-data
* python3-q-text-as-data
Intente: apt install <paquete seleccionado>
oot@alumni-virtual-machine:/var/lib/autopsy/Jacobs/host1/output# strings -t d image.blkls.str |
ess
oot@alumni-virtual-machine:/var/lib/autopsy/Jacobs/host1/output# strings -t d image.blkls > imag
.blkls.str
oot@alumni-virtual-machine:/var/lib/autopsy/Jacobs/host1/output# cat image.blkls.str
548 bjbj
2560 Jimmy Jungle
2573 626 Jungle Ave Apt 2
2594 Jungle, NY 11111
2612 Jimmy:
2620 Dude, your pot must be the best
2653 It made the cover of High Times Magazine! Thanks for sending me the Cover Page. What do
ou put in your soil when you plant the marijuana seeds? At least I know your growing it and not
ome guy in Columbia.
2863 These kids, they tell me marijuana isn
2902 t addictive, but they don
2928 t stop buying from me. Man, I
2958 m sure glad you told me about targeting the high school students. You must have some expe
tence. It
3058 s like a guaranteed paycheck. Their parents give them money for lunch and they spend it o
my stuff. I
3161 m an entrepreneur. Am I only one you sell to? Maybe I can become distributor of the year!
3252 I emailed you the schedule that I am using. I think it helps me cover myself and not be p
edictive. Tell me what you think. To open it, use the same password that you sent me before wit
that file. Talk to you later.
3471 Thanks,
3480 Joe
6762 urn:schemas-microsoft-com:office:smarts
6806 Street
6824 urn:schemas-microsoft-com:office:smarts
6868 address
6887 urn:schemas-microsoft-com:office:smarts
6931 City
6947 urn:schemas-microsoft-com:office:smarts
6991 place
7008 urn:schemas-microsoft-com:office:smarts
7052 State
7069 urn:schemas-microsoft-com:office:smarts
7113 PostalCode
7738 ^{d&
9936 Jimmy Jungle
9972 0000
10012 Normal
10028 0000tl
10056 Microsoft Word 10.0
13992 0000
14076 Jimmy Jungle
14105 Title
```

> blkls images/image > output/image.blkls

Luego he utilizado el comando strings para extraer todos los strings ASCII del archivo de data sin asignar. Utilizo -td flags para imprimir el byte offset que se encontró el string.

> strings -t d output/image.blkls > output/image.blkls.str

> cat output/image.blkls.str

Con esta información ya podemos extraer el nombre del dealer, donde vive, el mail que le manda Joe y que lo incrimina directamente y podemos saber también que hay otros archivos adjuntados como quizás un microsoft word.

Dentro del Autopsy vemos distintas informaciones:

Con la opción File System he visto que hay tres ficheros: un jpgc, un .exe y un .doc. Se sabe que el .doc ha sido eliminado.

Esta información también la he encontrado via terminal.

Ejecutando el comando:

> fls -r images/image

```
0042 Word.Document.8
t@alumni-virtual-machine:/var/lib/autopsy/Jacobs/host1# fls -r images/image
* 5: Jimmy Jungle.doc
8: cover page.jpgc
11: Scheduled Visits.exe
45779: $MBR
45780: $FAT1
45781: $FAT2
45782: $OrphanFiles
t@alumni-virtual-machine:/var/lib/autopsy/Jacobs/host1#
```

Luego vemos el `coverpage.jpgc` y el `.exe` que ya he especificado anteriormente.

También he ejecutado `> istat images/image 5` para obtener información del inodo.

```
root@kali-virtual-machine: /var/lib/autopsy/Jacobs/host1# lsattr Images/image_5
Directory Entry: 5
Not Allocated
File Attributes: File, Archive
Size: 20480
Name: _IMYJ-1.DOC

Directory Entry Times:
Written:      2002-04-15 14:42:30 (CEST)
Accessed:    2002-09-11 00:00:00 (CEST)
Created:     2002-09-11 08:49:49 (CEST)

Sectors:
33 34 35 36 37 38 39 40
41 42 43 44 45 46 47 48
49 50 51 52 53 54 55 56
57 58 59 60 61 62 63 64
65 66 67 68 69 70 71 72

root@kali-virtual-machine: /var/lib/autopsy/Jacobs/host1#
```

Al ejecutar `> ffind -a images/image 5` me ha devuelto efectivamente `* /Jimmy Jungle.doc` que demuestra que fue eliminado.

```
root@alunne-virtual-machine: /var/lib/autopsy/Jacobs/host1# ls
host.aut images logs mnt output reports
root@alunne-virtual-machine: /var/lib/autopsy/Jacobs/host1# cd output/sorter-vol1/
root@alunne-virtual-machine: /var/lib/autopsy/Jacobs/host1/output/sorter-vol1# ls
archive archive.html documents documents.html images index.html mismatch.html unknown.html
root@alunne-virtual-machine: /var/lib/autopsy/Jacobs/host1/output/sorter-vol1# cat mismatch.html
<HTML><HEAD>
<TITLE>Extension Mismatches</TITLE><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"></HEAD>
<BODY>
<CENTER><H2>Extension Mismatch</H2></CENTER>
C:\Scheduled Visits.exe <BR>
&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&Zip archive data, at least v2.0 to extract (Ext: exe )<BR>
&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&Image: /var/lib/autopsy/Jacobs/host1/images/image Inode: 11<BR>
&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&Saved to: <A HREF=".archive/image-11.exe">".archive/image-11.exe</A><BR>
<BR>
root@alunne-virtual-machine: /var/lib/autopsy/Jacobs/host1/output/sorter-vol1# cat unknown.html
<HTML><HEAD>
<TITLE>Unknown Category</TITLE><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"></HEAD>
<BODY>
<CENTER><H2>Unknown Category</H2></CENTER>
C:\cover.jpg <BR>
&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&PC formatted floppy with no filesystem<BR>
&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&Image: /var/lib/autopsy/Jacobs/host1/images/image Inode: 8<BR>
<BR>
```

1. el .exe es probablemente un .zip
2. el coverage.jpgc es el fichero unknown “formatted floppy with no filesystem.

```
> dd if=images/image of=output/imageTotal bs=512
> strings -t d output/imageTotal > output/imageFF.str
> cat output/imageFF.str
```

he localizado el supuesto password. *pw=goodtimes* y un *ScheduledVisits.xls* que corresponde al .exe que he supuesto que es el recorrido que Jimmy toma para pasar la marihuana. Este password también lo he localizado de forma gráfica usando Autopsy.

```
Virtual Machine Help
alumni-virtual-machine: /var/lib/autopsy/Jacobs/host1
alumni@alumni-virtual-machine: ~
45316 NrH'
45361 pu0 k
45415 go}b
45579 /9'
45671 Tw l
45817 c\[M0
45899 T[9j
46445 k}Bx`VE
46564 sS6s,
46724 zz7q
46779 K;dlj
46828 )UfRcvm
46876 8- 'H$
46933 FFFy
47000 NrH'
47290 [7g%
47398 9' p+
47504 R*]I
47537 oqk4
47574 I+^L
53024 pw=goodtimes
53278 Scheduled Visits.xls
53394 skum
53474 gvnq[A
53575 N[!
53703 sC6g(
53709 yGU-
53728 nRuf
53707 .+bN
53813 \05'sjU7
53875 +bg^
54016 0hHZ
54035 1C/+N
54091 X%#$
54280 4N' L"
54293 Q- bY
54388 Y/*9
54461 b,W0$
54519 ot3;
54527 NBY4
54655 }aR$H
54696 N[iy
54826 w&M
54923 U- P
54999 1T('
55128 P(lsr=
55176 -V<f
55263 7*ou
55455 g#6U
55506 H00 +U
55626 Scheduled Visits.xlsPK
root@alumni-virtual-machine: /var/lib/autopsy/
```

He detectado que *ScheduledVisits.xls* aparece dos veces, por lo que he cogido el 53278 y el 55626 (donde aparece las dos veces) y los he dividido por el tamaño de un sector. Por un lado he obtenido el valor 104 y por el otro el 108. Lo que me da una pista de que el documento empieza en el sector 104 y termina en el 108.

He ejecutado lo mismo que anteriormente:

```
> blkcalc -u 104 images/image
```

lo que me ha devuelto 173 (que corresponde al fragmento al que está alojado)

```
> ifind -f fat -d 104 images/image
```

```
11 → inodo
```

y he hecho lo mismo para el 55626

Aquí como puedes comprobar me he liado un poco...

Después he accedido a Image Details en FAT Contents.

CONTENT INFORMATION	
Sector Size:	512
Cluster Size:	512
Total Cluster Range:	2 - 2848
FAT CONTENTS (in sectors)	
73-103 (31)	→ EOF
104-108 (5)	→ EOF

Donde nos indica los sectores que ocupa el *ScheduleVisits.xls* (sectores 104-108 ocupando 5 sectores) lo que ha corroborado la información que he encontrado antes por terminal. Por lo tanto he ejecutado el comando:

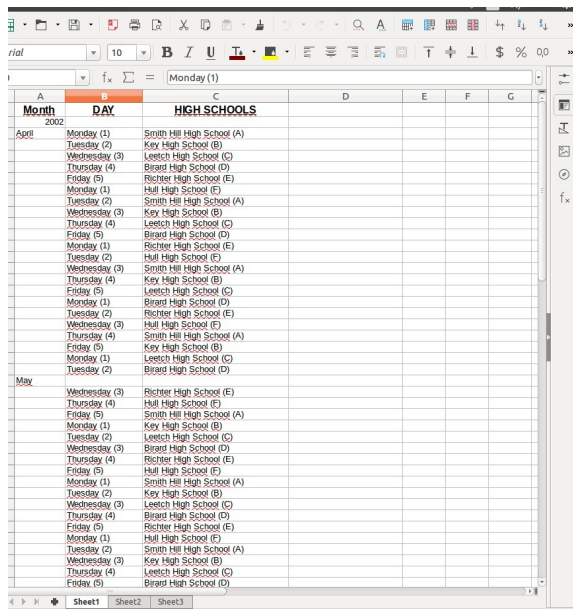
```
> dd if=images/image of=~/.Escritorio/recovered.exe bs=512 count=5 skip=104
```

Dentro del Escritorio abro el .exe generado, ingreso la password goodtimes y obtengo satisfactoriamente el excel con las escuelas a las que va Jimmy.

Y también el jpg que ocupa 31 sectores comenzando por el 73. He hecho lo mismo para el otro fichero:

```
> dd if=images/image of=~/.Escritorio/coverpage.jpg bs=512 count=31 skip=73
```

Y lo mismo. Dentro de escritorio he obtenido la imagen que faltaba.



Month	Day	HIGH SCHOOLS
April	Monday (1)	Smith Hill High School (A)
	Tuesday (2)	Knox High School (B)
	Wednesday (3)	Leitch High School (C)
	Thursday (4)	Braed High School (D)
	Friday (5)	Richter High School (E)
	Monday (1)	Hull High School (F)
	Tuesday (2)	Smith Hill High School (A)
	Wednesday (3)	Knox High School (B)
	Thursday (4)	Leitch High School (C)
	Friday (5)	Braed High School (D)
	Monday (1)	Richter High School (E)
	Tuesday (2)	Hull High School (F)
	Wednesday (3)	Smith Hill High School (A)
	Thursday (4)	Knox High School (B)
	Friday (5)	Leitch High School (C)
	Monday (1)	Braed High School (D)
	Tuesday (2)	Richter High School (E)
	Wednesday (3)	Hull High School (F)
	Thursday (4)	Smith Hill High School (A)
	Friday (5)	Knox High School (B)
	Monday (1)	Leitch High School (C)
	Tuesday (2)	Braed High School (D)
May	Wednesday (3)	Richter High School (E)
	Thursday (4)	Hull High School (F)
	Friday (5)	Smith Hill High School (A)
	Monday (1)	Knox High School (B)
	Tuesday (2)	Leitch High School (C)
	Wednesday (3)	Braed High School (D)
	Thursday (4)	Richter High School (E)
	Friday (5)	Hull High School (F)
	Monday (1)	Smith Hill High School (A)
	Tuesday (2)	Knox High School (B)
	Wednesday (3)	Leitch High School (C)
	Thursday (4)	Braed High School (D)
	Friday (5)	Richter High School (E)
	Monday (1)	Hull High School (F)
	Tuesday (2)	Smith Hill High School (A)
	Wednesday (3)	Knox High School (B)
	Thursday (4)	Leitch High School (C)
	Friday (5)	Braed High School (D)



Como conclusión aclarar que aunque me he liado un poco al principio para entender y asimilar la herramienta utilizada, finalmente he comprendido correctamente su funcionamiento para poder extraer la información necesaria.