

Práctica 7

Análisis Forense

Tabla de contenido

1. Objetivos	2
2. Adquisición de una imagen forense de un dispositivo Android	3
Rooteado del dispositivo Android	3
Adquisición Física	4
Adquisición Lógica	6
3. Análisis de datos	8
Descripción del caso de investigación	8
Preguntas a Resolver	8
Material policial proporcionado para el trabajo	9
Herramientas utilizadas	9
Actividades realizadas para dar respuesta a las preguntas	9
Examinar cada uno de los archivos.	17
Archivo Cover page.jpgc	17
Análisis Archivo Jimmy Jungle.doc	21
4. Ejercicio opcional	24
Análisis Archivo Schedueld Visits.exe	24

1. Objetivos

El análisis forense realizado en sistemas informáticos conlleva dos tareas bien diferenciadas, la recopilación de pruebas (evidencias) y el análisis de las mismas.

Esta práctica quiere abordar ambas tareas, por lo que se dividirá la misma en dos partes bien diferenciadas.

En la primera, se realizará una imagen de un dispositivo móvil. Concretamente la copia de la máquina virtual Android que tenemos instalada en VirtualBox. Sin embargo, esta máquina virtual carece de información a analizar, ya que carece de contactos, emails, imágenes, documentos y demás información que podríamos encontrar en cualquiera de nuestros smartphones. Por ello, para realizar la segunda parte de la práctica dedicada al análisis forense, utilizaremos una imagen distinta a la obtenida en la primera parte.

La imagen que será utilizada contendrá los ficheros necesarios para resolver un caso de investigación policial.

2. Adquisición de una imagen forense de un dispositivo Android

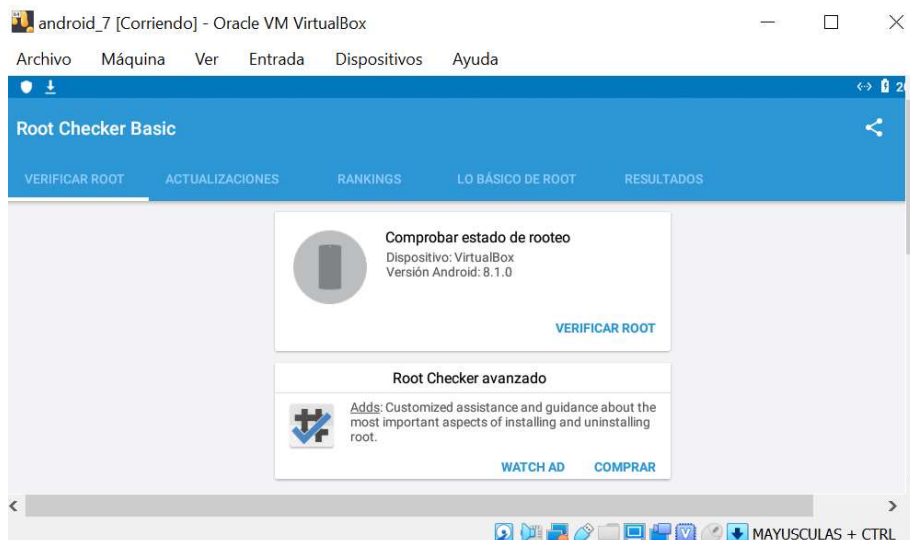
Rooteado del dispositivo Android

Para la realización de la imagen forense es necesario que el dispositivo Android esté *rooteado*.

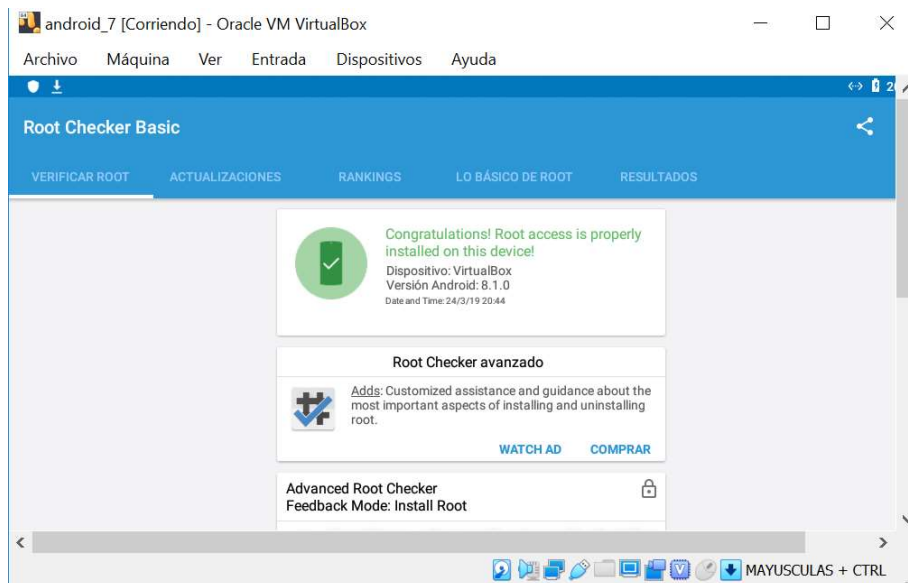
En nuestro ya lo está, si ejecutamos la app terminal e introduciendo la orden `su` y seguidamente pulsando intro, pondremos el terminal en modo root.

```
x86:/> su
x86:/#
```

Si no lo hubiera estado, habríamos tenido que *rootearlo* utilizando alguna de las aplicaciones disponibles en Google Play, capaces de hacerlo como *Root Checker*. En ella tenemos la opción de verificar inicialmente estado de nuestro móvil, seleccionando la opción *Verificar Root*



Podemos ver el estado del mismo, que en el caso de la imagen del laboratorio es *rooteado*.



Nota: Para recuperar la máquina Android tras un periodo de inactividad (pantalla en negro) se deberá pulsar Ctrl+ botón derecho del ratón.

Adquisición Física

La adquisición se llevará a cabo desde la máquina virtual Santoku, por lo que una vez iniciada, abrimos una *terminal* en el dispositivo y cambiamos al usuario *root*: Dado que el dispositivo Android no está conectado mediante USB a Santoku, deberemos acceder a él mediante la red. Para ello, debemos averiguar la IP del dispositivo Android, ejecutando en la orden *ifconfig* en un terminal que abriremos en Android. En el ejemplo de las imágenes contenidas en la práctica la IP del dispositivo Android obtenida es 192.168.0.6.

Con esta información, estableceremos una conexión a Android desde Santoku con la instrucción:

```
santoku@santoku-VirtualBox:~$ adb connect 192.168.0.6
connected to 192.168.0.6:5555
```

Permitiendo esto el poder abrir un terminal en Android desde Santoku:

```
santoku@santoku-VirtualBox:~$ adb -s 192.168.0.6:5555 shell
x86_64:/ $
```

Ya en Android deberemos averiguar donde se encuentra y el tamaño de la partición *data*, dado que es la única partición que puede modificar el usuario.

```
x86_64:/ $ df -a
Filesystem      1K-blocks    Used Available Use% Mounted on
tmpfs           1020248      3372    1016876   1% /
/dev/loop0      2189112 2073840    98888    96% /system
/dev/block/sda1 12250332 3380372   8853576  28% /data
tmpfs           1020248       456    1019792   1% /dev
devpts          0            0          0   0% /dev/pts
proc            0            0          0   0% /proc
sysfs           0            0          0   0% /sys
selinuxfs       0            0          0   0% /sys/fs/selinux
none            0            0          0   0% /acct
none            0            0          0   0% /dev/memcg
/sys/kernel/debug 0            0          0   0% /sys/kernel/debug
none            0            0          0   0% /dev/stune
tmpfs           1020248       0    1020248   0% /mnt
none            0            0          0   0% /config
none            0            0          0   0% /dev/cpuctl
none            0            0          0   0% /dev/cpuset
pstore          0            0          0   0% /sys/fs/pstore
none            1020248       0    1020248   0% /cache
tmpfs           1020248       0    1020248   0% /storage
tracefs         0            0          0   0% /sys/kernel/debug/tracing
/data/media     12250332 3380372   8853576  28% /storage/emulated
x86_64:/ $
```

Asumimos que hemos insertado en el dispositivo Android una tarjeta SD vacía para copiar en ella la imagen de la partición /data.

Para ello ejecutamos la orden dd con los parámetros correspondientes para crear la imagen, a la que nombraremos data.img en la tarjeta sdcard (/mnt/sdcard). Este proceso tarda un poco.

```
X86:/ # dd if=/dev/block/sda1 of=/mnt/sdcard/data.img
```

Una vez se haya realizado la imagen desde la consola de la máquina de análisis (Santoku), escribiendo la orden obtenemos la imagen de la partición de datos:

```
X86:/ #exit
```

```
santoku@santoku-VirtualBox:> adb -s 192.168.0.6:5555 pull /mnt/sdcard/data.img
```

Obteniendo la imagen de la partición del usuario.

Si no fuera posible insertar la tarjeta SD vacía podríamos haber hecho la transferencia directamente a la Santoku del siguiente modo:'

- Ejecutamos:

```
santoku@santoku-VirtualBox:> adb forward tcp:8888 tcp:8888
```

De esta manera nos aseguramos de que todo lo que le llega a adb por el puerto

8888 es transmitido a la máquina de análisis por el mismo puerto.

- En Android ejecutamos:

```
X86:/ # dd if=/dev/block/sda1 | busybox nc -l -p 8888
```

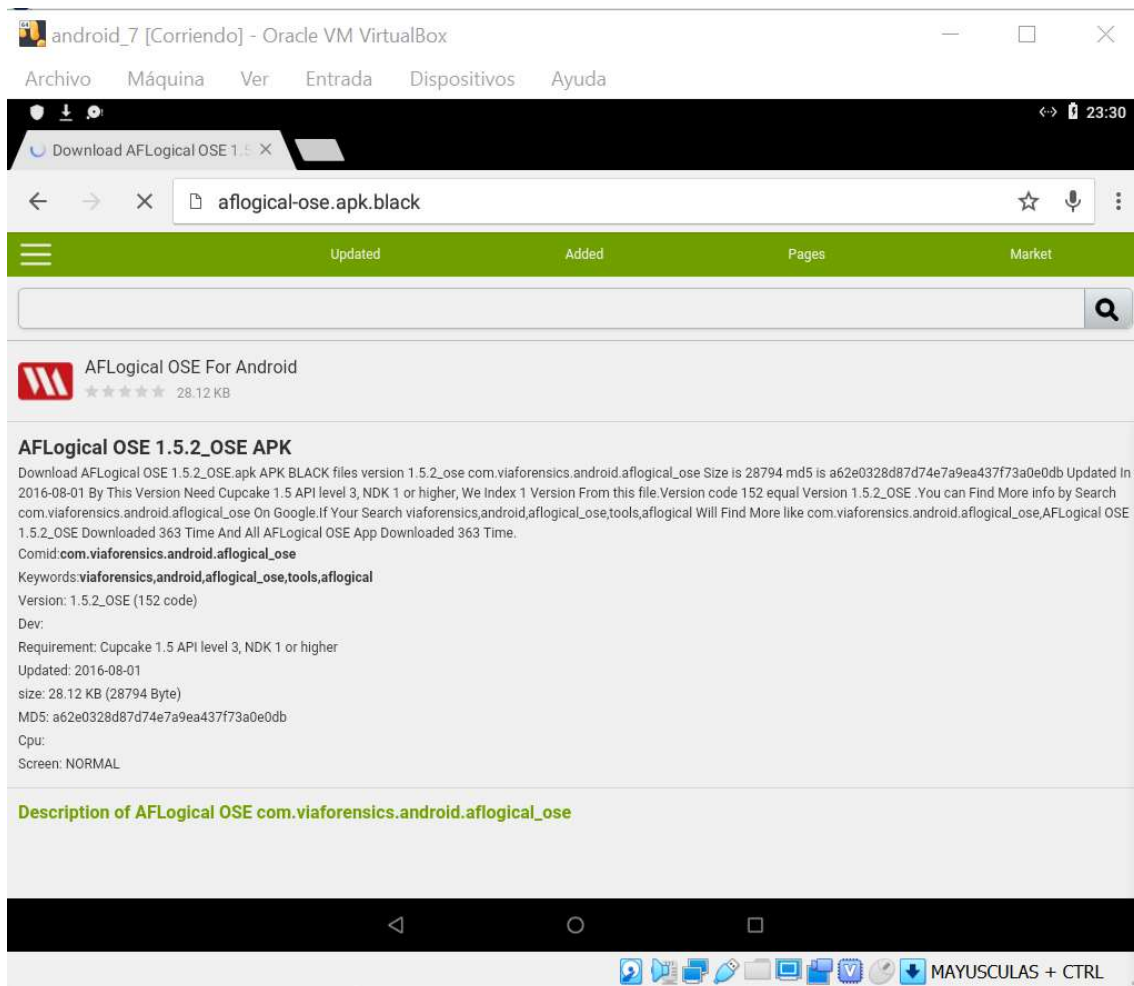
- En Santoku para recibir la imagen sólo deberemos ejecutar:

```
santoku@santoku-VirtualBox:> nc 192.168.0.6 8888 > data.img
```

Adquisición Lógica

La adquisición lógica también puede realizarse con ordenes adb, sin embargo para aprender el uso de otra herramienta, en este apartado lo realizaremos con la app AFLogical.

Lo primero que debemos hacer es instalarla en la máquina virtual Android, desde <http://aflogical-ose.apk.black>



Nota:

- Puede suceder que la descarga de AFLogical no se complete por falta de espacio en el dispositivo Android: Esto puede deberse a que tenemos almacenada la imagen física de la partición /data en el dispositivo. Como no vamos a necesitar

el fichero data.img en los ejercicios siguientes, procederemos a su eliminación, para poder descargar la aplicación AFLogical.

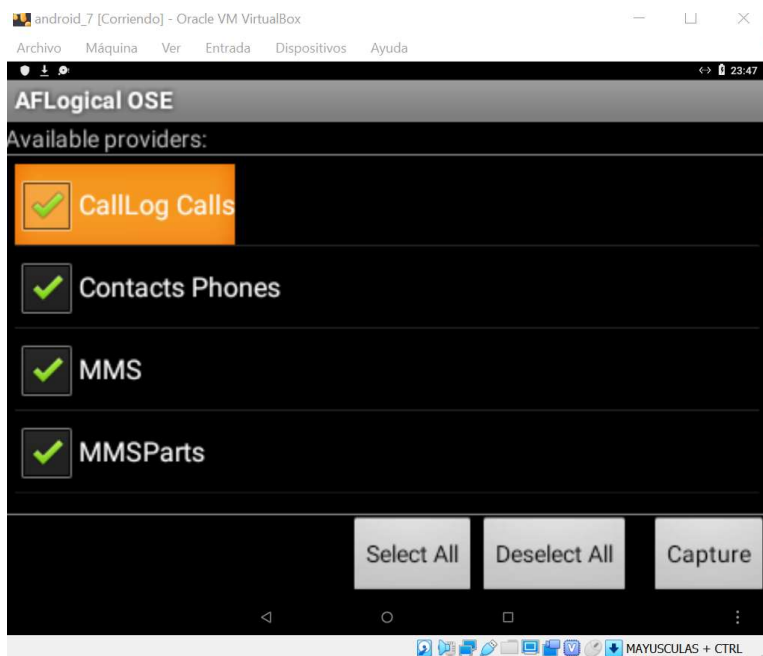
- Puede suceder que no tengamos acceso a Internet desde el dispositivo Android, debido a la configuración de red que tengamos en la máquina virtual Android_7. Para solucionar este problema realizaremos la configuración de red que llevamos a cabo en la práctica 5.

AFLogical es una aplicación de Android que contiene los permisos necesarios para extraer toda la información accesible mediante permisos de un sistema Android:

- Historial de llamadas.
- Contactos.
- Mensajes SMS, MMS y sus adjuntos.

y dado que se ejecuta a través de una aplicación normal, no requiere disponer de un teléfono *rootado*.

Una vez descargado, dado que es un .apk podemos proceder a su ejecución.

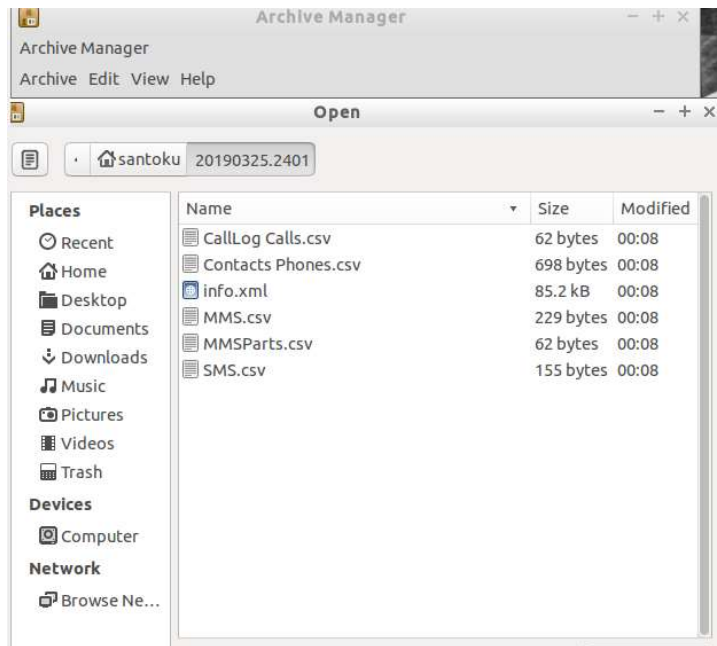


Los ficheros generados se guardarán en una carpeta identificada por la fecha de la captura en /mnt/sdcard/forensic.

Para exportarlos a Santoku para su posterior análisis ejecutaremos la orden:



Los resultados pueden ser inspeccionados utilizando el navegador de archivos de Santoku Linux.



Al terminar esta parte, cerraremos las máquinas virtuales Android y Santoku, y iniciaremos la máquina virtual Kali, en la que llevaremos a cabo el análisis de los datos.

3. Análisis de datos

Dado que la imagen de máquina virtual Android del laboratorio tiene un contenido mínimo, sin información personal (emails, contactos, fotos, ...) de forma que resulte interesante para un análisis forense más allá de la mera visualización de la estructura de ficheros de la misma, vamos a realizar nuestro análisis forense sobre otra imagen. A continuación, se describe el caso de la investigación de dicha imagen.

Descripción del caso de investigación

Joe Jacobs, de 28 años, fue arrestado ayer en el aparcamiento del instituto Smith Hill, por cargos de venta de drogas ilegales a estudiantes de secundaria. Jacobs niega la venta de drogas en cualquier otro instituto además de Smith Hill, y se niega a proporcionar a la policía el nombre de su proveedor de drogas. En el registro a su domicilio, el policía únicamente incautó un disquete, del que nos han proporcionado una copia para su análisis en busca de pruebas que puedan identificar al proveedor de drogas de Jacobs.

Preguntas a Resolver

1. ¿Quién es el proveedor de marihuana de Joe Jacobs y cuál es su dirección?
2. ¿Qué proceso realizaste tu como investigador para examinar con éxito el contenido completo de cada archivo?

Material policial proporcionado para el trabajo

1. Informa policial
Puede obtenerse en

```
wget https://raw.githubusercontent.com/SVelizDonoso/forense-autopsy/master/report.txt
```

2. Imagen física (obtenida mediante dd) del disquete incautado
Puede obtenerse en

```
wget https://github.com/SVelizDonoso/forense-autopsy/raw/master/image.zip  
MD5 de la imagen= b676147f63923e1f428131d59b1d6a72
```

Herramientas utilizadas

En el desarrollo práctico de este ejercicio serán utilizadas las siguientes herramientas:

- Autopsy
- VM VirtualBox 6.0
- Kali Linux ver 2.0
- Md5sum
- Unzip (Descompresión)

Actividades realizadas para dar respuesta a las preguntas

Una vez descargada la imagen se debe de calcular su MD5, para poder verificar su integridad posteriormente si fuera necesario.

```
root@kali:~/P6Forensic/JoeJacobs# md5sum image.zip  
b676147f63923e1f428131d59b1d6a72 image.zip  
root@kali:~/P6Forensic/JoeJacobs#
```

Ahora creamos una copia del archivo para trabajar con ella copy no contaminar la evidencia principal.

```
root@kali:~/P6Forensic/JoeJacobs# cp image.zip copiaimage.zip
```

Calculamos el md5 del archivo copiaimage.zip para verificar que estamos trabajando con una copia original de la evidencia.

```
root@kali:~/P6Forensic/JoeJacobs# md5sum copiaimage.zip  
b676147f63923e1f428131d59b1d6a72 copiaimage.zip
```

Descomprimos copiaimagen.zip

```
root@kali:~/P6Forensic/JoeJacobs# unzip copiaimage.zip  
Archive: copiaimage.zip  
inflating: image  
root@kali:~/P6Forensic/JoeJacobs#
```

Calculamos su MD5

```
root@kali:~/P6Forensic/JoeJacobs# md5sum image  
ac3f7b85816165957cd4867e62cf452b image  
root@kali:~/P6Forensic/JoeJacobs#
```

Ahora vamos a trabajar esta imagen con una herramienta especializada en análisis forense, autopsy. Para su ejecución escribimos el comando autopsy.

```
root@kali:~/P6Forensic/JoeJacobs# autopsy

=====

Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24

=====

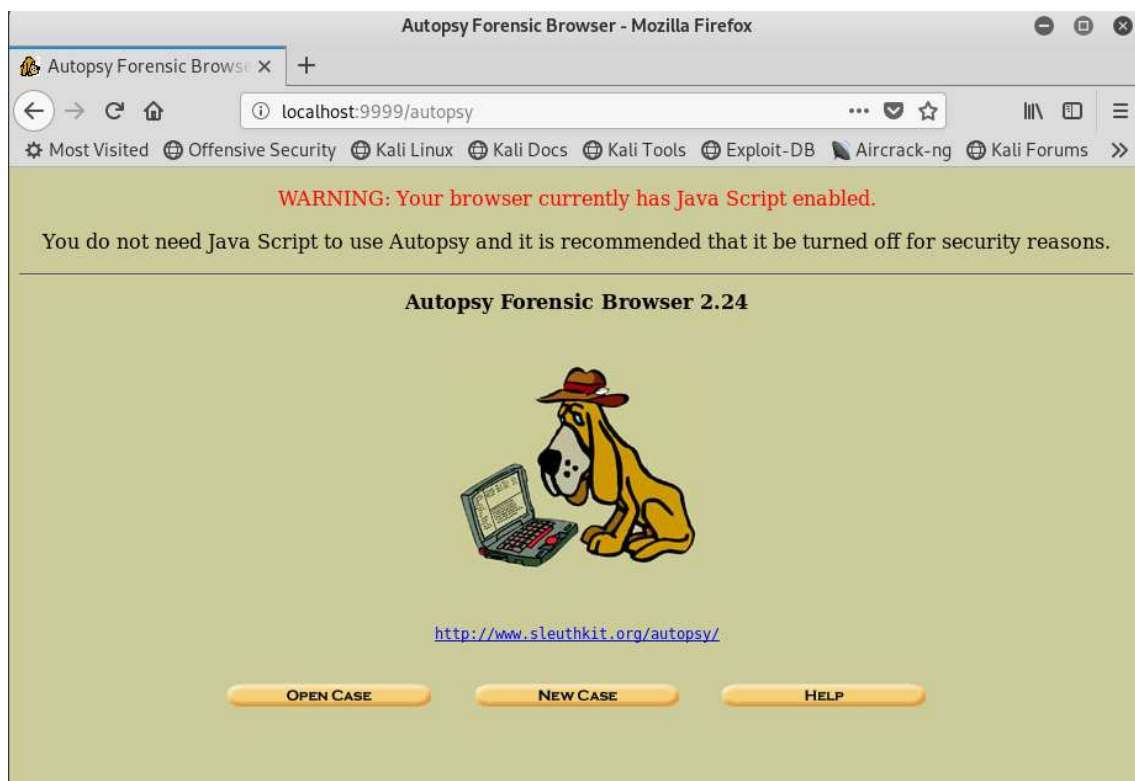
Evidence Locker: /var/lib/autopsy
Start Time: Mon Mar 25 14:21:17 2019
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

    http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
```

Copiamos la URL que nos indican el programa en el navegador para utilizar el programa.



Para iniciar un caso con autopsy damos Click sobre el botón que dice Open Case.



Una vez realizada esta tarea, nos aparecerá la siguiente pantalla



Ahora damos Click sobre el botón New Case



Y procedemos a llenar los datos del formulario.

CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

2. **Description:** An optional, one line description of this case.

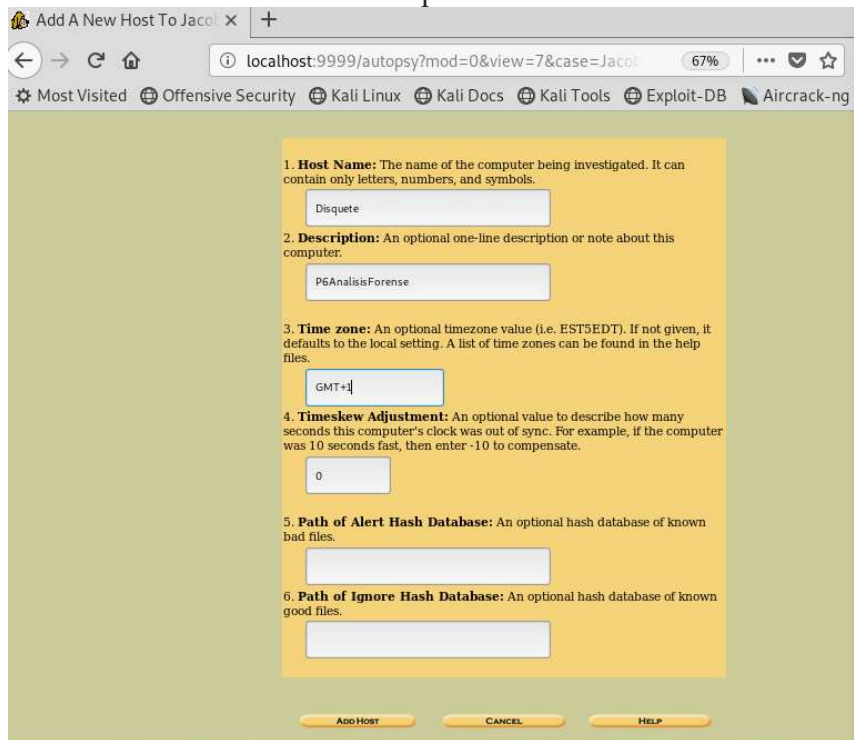
3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a. <input type="text" value="T.N."/>	b. <input type="text"/>
c. <input type="text"/>	d. <input type="text"/>
e. <input type="text"/>	f. <input type="text"/>
g. <input type="text"/>	h. <input type="text"/>
i. <input type="text"/>	j. <input type="text"/>

Damos Click en New Case nuevamente y nos aparecerà la siguiente pantalla



Rellenamos los campos del formulario y aceptamos.



1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.

Disquete

2. **Description:** An optional one-line description or note about this computer.

P6AnalysisForense

3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

GMT+1

4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

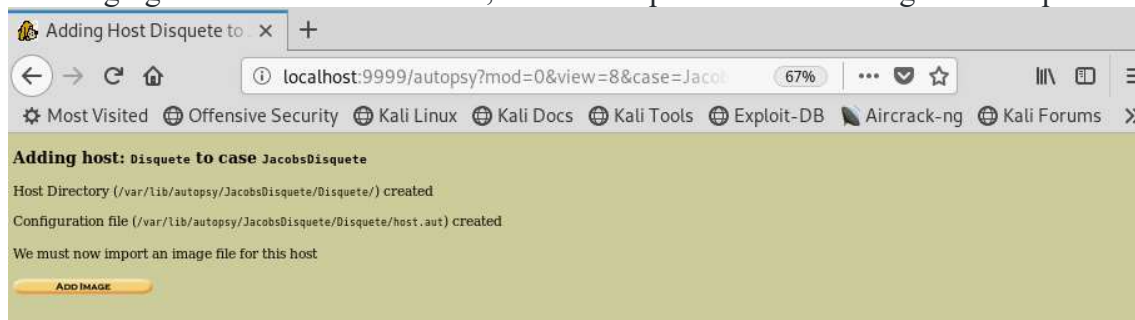
0

5. **Path of Alert Hash Database:** An optional hash database of known bad files.

6. **Path of Ignore Hash Database:** An optional hash database of known good files.

Add Host Cancel Help

Al agregar el nuevo host, nos aparecerá la siguiente pantalla



Adding Host Disquete to Jacobs

Host Directory (/var/lib/autopsy/JacobsDisquete/Disquete/) created

Configuration file (/var/lib/autopsy/JacobsDisquete/Disquete/host.aut) created

We must now import an image file for this host

ADD IMAGE

Ahora nos queda agregar la evidencia a revisar.

Add Image To JacobsDisque x

localhost:9999/autopsy?mod=0&view=13&host=Disque 67%

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums

Case: JacobsDisquette
Host: Disquette

ADD A NEW IMAGE

1. Location
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

/root/P6Forensic/joeJacobs/image

2. Type
Please select if this image file is for a disk or a single partition.

☒ Disk ☐ Partition

3. Import Method
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

☒ Symlink ☐ Copy ☐ Move

NEXT

CANCEL HELP

Ahora damos Click en Next.



seleccionamos Volume System Type Dos

Warning: Autopsy could not determine the volume system type for the disk image (i.e. the type of partition table). Please select the type from the list below or reclassify the image as a volume image instead of as a disk image.

Disk Image ☐ Volume Image ☒

Volume System Type (disk image only): dos

OK

Damos Ok.

Ahora procedemos a completar el formulario.

Collecting details on new x +

localhost:9999/autopsy?mod=0&view=14&spl_conf= 67%

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums >>

Image File Details

Local Name: images/image

Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

☐ Ignore the hash value for this image.
☒ Calculate the hash value for this image.
☐ Add the following MD5 hash value for this image:

☒ Verify hash after importing?

File System Details

Analysis of the image file shows the following partitions:

Partition 1 (Type: fat12)

Mount Point: File System Type:

ADD CANCEL HELP

Seleccionamos calcular Hash y comprobamos la integridad de nuestra evidencia.

Add a new image to an AI x +

localhost:9999/autopsy?mod=0&view=15&img_path= 67%

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums >>

Calculating MD5 (this could take a while)
 Current MD5: AC3F7B85816165957C04867E62CF4528
 Testing partitions
 Linking image(s) into evidence locker
 Image file added with ID img1
 Volume image (0 to 0 - fat12 - C:) added with ID vol1

OK ADD IMAGE

Damos Ok y comienza el inicio del análisis ya que tenemos la evidencia cargada en nuestro sistema con los procedimientos forenses adecuados.

Esta es la pantalla del inicio de análisis.

Open Image In JacobsDis x +

localhost:9999/autopsy?mod=0&view=16&case=JacobsDisquete 67%

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums >>

Case: JacobsDisquete
 Host: Disquete

Select a volume to analyze or add a new image file.

mount	name	fs type	
<input checked="" type="radio"/> C:/	image-0-0	fat12	details

ANALYZE ADD IMAGE FILE CLOSE HOST

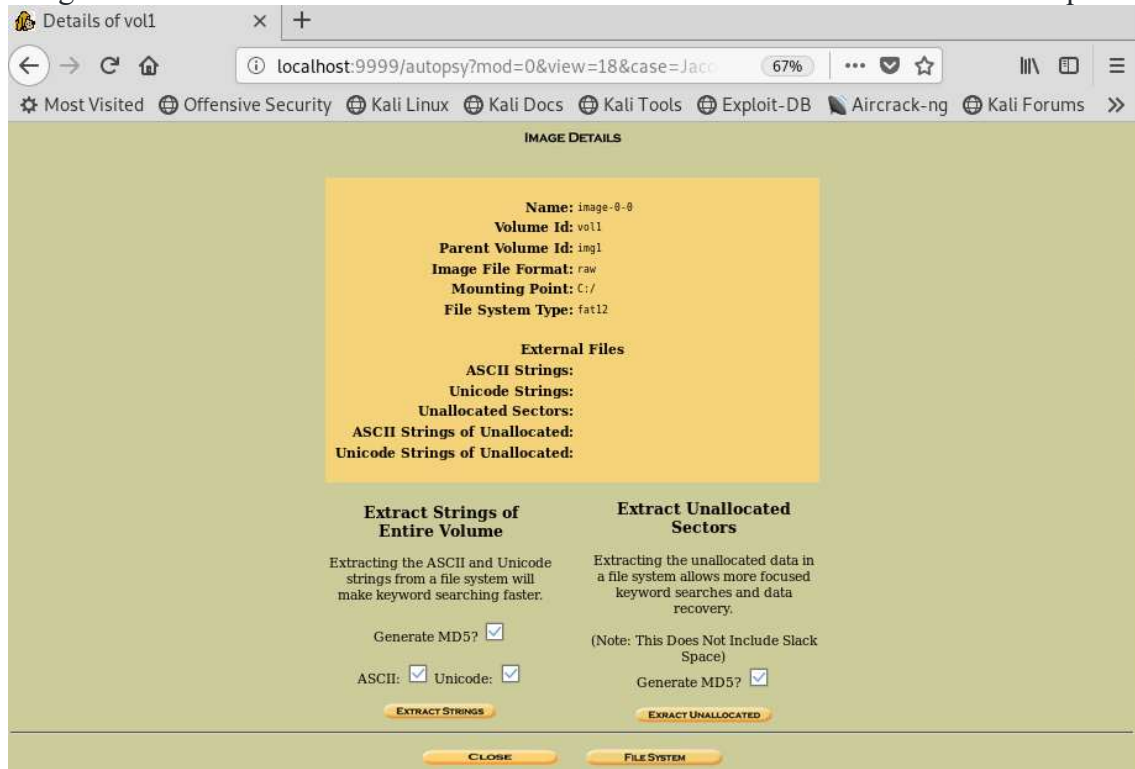
HELP

FILE ACTIVITY TIME LINES IMAGE INTEGRITY HASH DATABASES

VIEW NOTES EVENT SEQUENCER

Para comenzar damos Click en el link Details y procedemos a crear los índices de búsqueda.

Imagen antes de los índices de búsqueda:

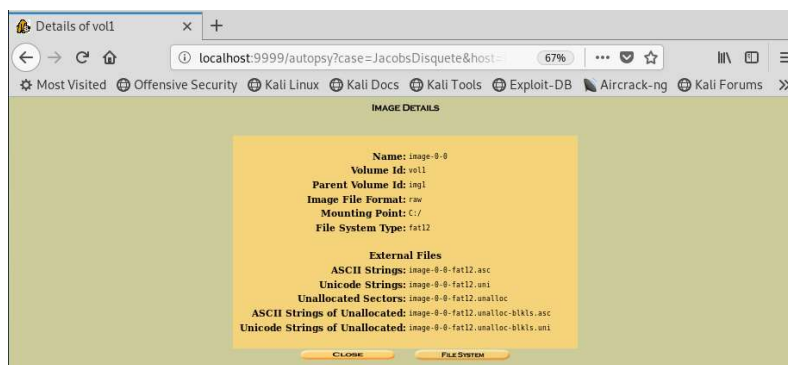


Para trabajar con la imagen damos Click sobre los botones Extract String



Volvemos a los detalles de la imagen haciendo click en Image Details y repetimos el proceso con Extract Unallocated.

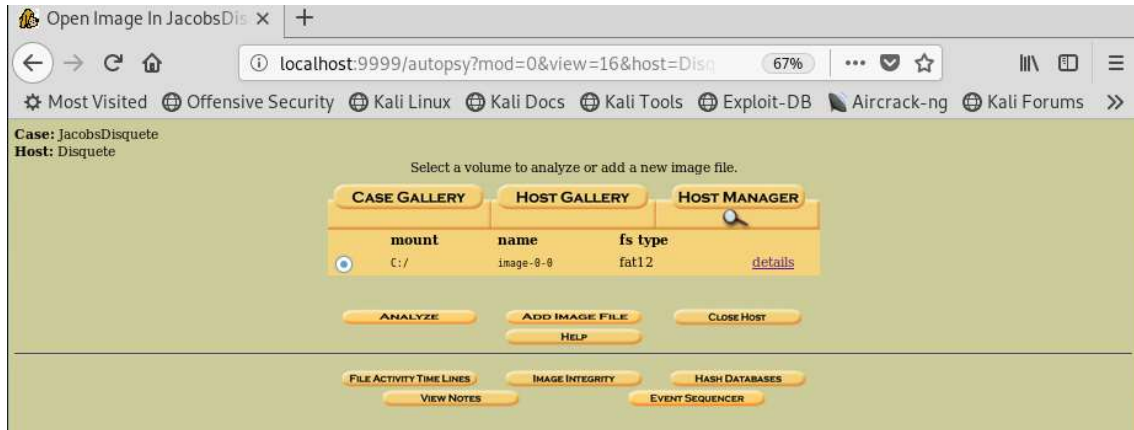
Obteniendo



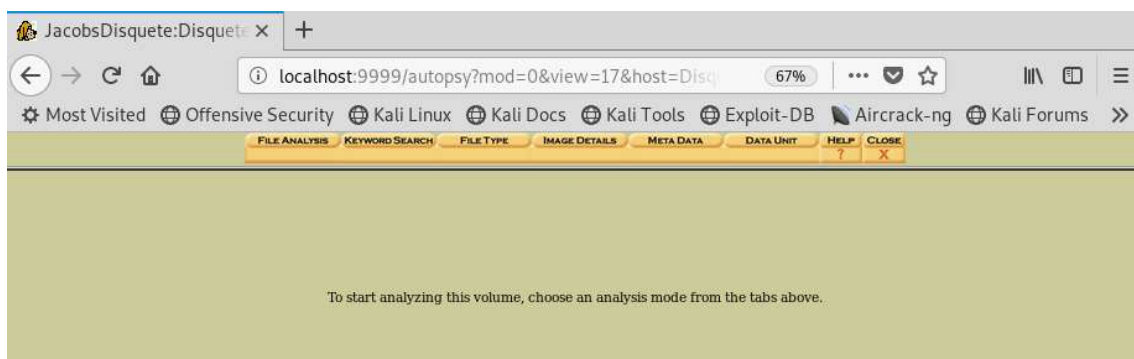
Después de este proceso de verificación damos Click sobre el botón Close que se encuentra al final del formulario y nos salimos de esta pantalla.



Si el paso anterior lo seguimos bien deberíamos estar en la siguiente pantalla nuevamente.

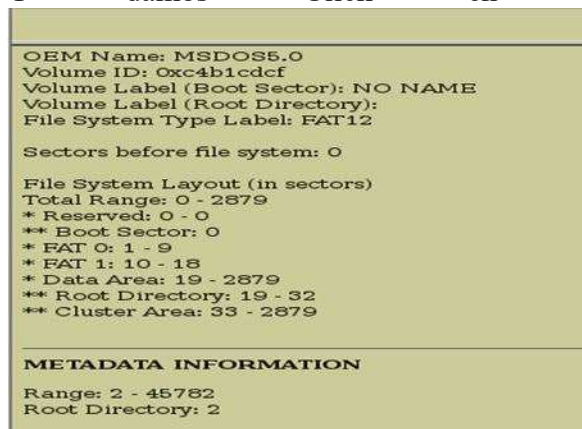


Ahora Damos Click sobre el botón Analyze



Y damos Click en el botón Image Details

Y damos Click en el botón Image Details



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

Con esto verificamos el tamaño del cluster, direcciones de memoria, metadatos y informacion volumen, FAT contents nos indica los sectores que contienen datos del disquete.

Ahora damos click en el boton que dice File Analyze y nos deberia llegar a la siguiente Pantalla



The screenshot shows the File Analyze interface with a directory listing. The current directory is `/`. The table below shows the files and directories found:

Del.	Type	NAME	WRITTEN	ACCESSED	CREATED	Size	UID	GID	META
v/v	dir	FAT1	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	4608	0	0	45780
v/v	dir	FAT2	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	4608	0	0	45781
v/v	dir	FAT3	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512	0	0	45779
d/d	dir	KirstenFiles/	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	45782
r/r	file	cover_page.jpg	2002-09-11 08:30:52 (American)	2002-09-11 00:00:00 (American)	2002-09-11 08:50:27 (American)	15585	0	0	8
r/r	file	Jimmy Turcole.doc	2002-04-15 14:42:30 (American)	2002-09-11 00:00:00 (American)	2002-09-11 08:49:49 (American)	20480	0	0	5
r/r	file	Scheduled Visits.xls	2002-05-24 08:20:32 (American)	2002-09-11 00:00:00 (American)	2002-09-11 08:50:38 (American)	1000	0	0	11

The interface also includes a 'Directory Seek' section on the left and a 'File Name Search' section at the bottom. The 'File Browsing Mode' section at the bottom states: 'In this mode, you can view file and directory contents.'

Examinar cada uno de los archivos.

Archivo

Cover

page.jpgc

r/r [cover_page.jpgc](#) 2002-09-11 08:30:52 (American) 2002-09-11 00:00:00 (American) 2002-09-11 08:50:27 (American) 15585 0 0 [8](#)

Damos click en HEX DISPLAY y verificamos que este archivo no es reconocido como un .jpeg , ya que si fuese de esta forma tendría los valores en HEX FF D8.

Current Directory: [X:/](#)

[ADD NOTE](#) [GENERATE MD5 LIST OF FILES](#)

DEL	Type	NAME	WRITTEN	ACCESSED	CREATED
	dir / in				
v / v	FEAT1		0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)
v / v	FEAT2		0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)
v / v	PMR		0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)
d / d	StorhamFiles/		0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)
r / r	cover page.jpg		2002-09-11 08:30:52 (American)	2002-09-11 00:00:00 (American)	2002-09-11 08:50:27 (American)
✓ r / r	Jimmy Juvela.doc		2002-04-15 14:42:30 (American)	2002-09-11 00:00:00 (American)	2002-09-11 08:49:49 (American)
r / r	Scheduled Visits.exe		2002-05-24 08:20:32 (American)	2002-09-11 00:00:00 (American)	2002-09-11 08:50:38 (American)

ASCII ([display](#) · [report](#)) * Hex ([display](#) · [report](#)) * ASCII Strings ([display](#) · [report](#)) * [Export](#)

File Type: PC formatted floppy with no filesystem

Hex Contents Of File: X:/cover page.jpg:

```

00000000: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000010: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000020: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000030: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000040: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000050: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000060: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000070: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000080: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000090: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000000A0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000000B0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000000C0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000000D0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

```

Ahora Vamos a visualizar los metadatos de esta imagen dando click en Meta

META
45780
45781
45779
45782
8
5
11

Tendremos la siguiente información en pantalla.

Search for File Name
<p>PREVIOUS</p> <p>REPORT VIEW CONTENTS</p> <p>File Type: PC formatted floppy with no filesystem</p> <p>MD5 of content: f49ed788acc2753e5a1736808dcdd138 -</p> <p>SHA-1 of content: dc13088a8389d974bc544ac32d6f7c4c904fba -</p> <p>Details:</p> <p>Directory Entry: 8 Allocated File Attributes: File, Archive Size: 15585 Name: COVERP-1.JPG</p> <p>Directory Entry Times: Written: 2002-09-11 08:30:52 (American) Accessed: 2002-09-11 00:00:00 (American) Created: 2002-09-11 08:50:27 (American)</p> <p>Sectors: 451</p>

La evidencia nos señala la siguiente inconsistencia:

El archivo posee un tamaño de 15585 bytes, sin embargo sólo se tiene un sector de 451 bytes asignado sobre 512 bytes correspondiente al tamaño de los sectores en FAT 12.

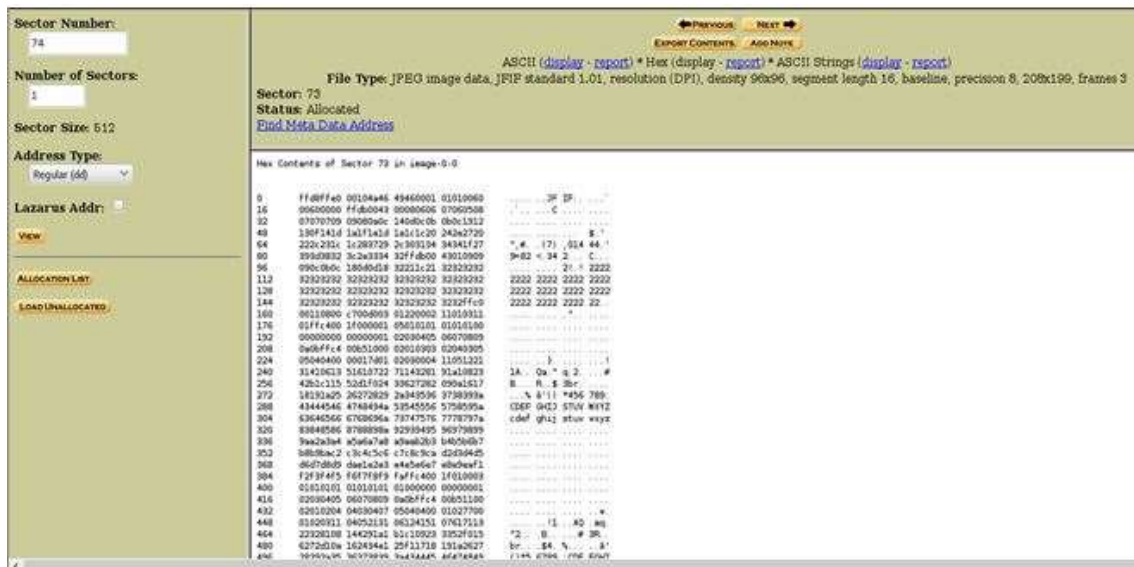
Procedemos entonces al cálculo del archivo:

- Tamaño archivo 15585 bytes
- Tamaño FAT 12 512 bytes
- Sectores a Ocupar = (Tamaño archivo + Tamaño FAT -1) / Tamaño FAT

Es decir: $(15585 + 511) / 512 = 31$

Por lo tanto, debemos ocupar 31 sectores para reconstruir la imagen.

Ahora procedemos a buscar una firma JPEG JFIF desde el sector 451 en sentido inverso, es decir, primero revisar el sector 451, después 450, después 449 hasta llegar al sector 73 donde encontramos una coincidencia con el contenido JI IF.

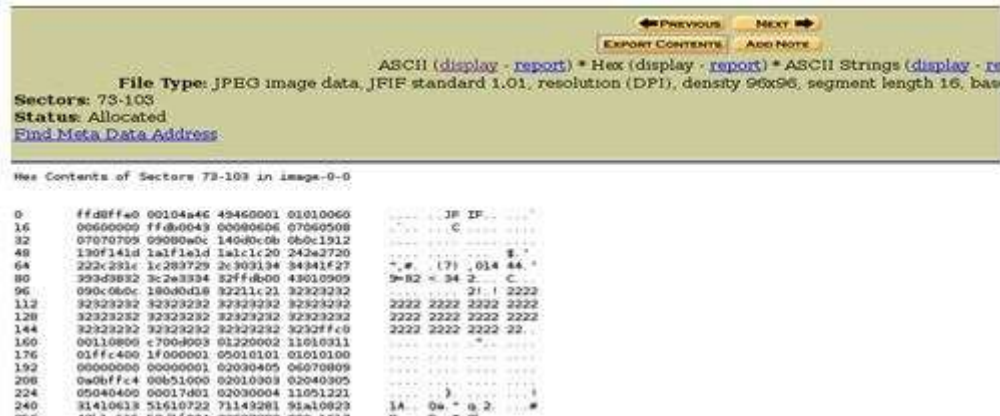


Como en el análisis FAT CONTENTS encontramos 31 sectores, significa que desde el inicio de la imagen debemos comenzar de sector 72 + 31 esto nos 103, es decir, del sector 73 al 103.

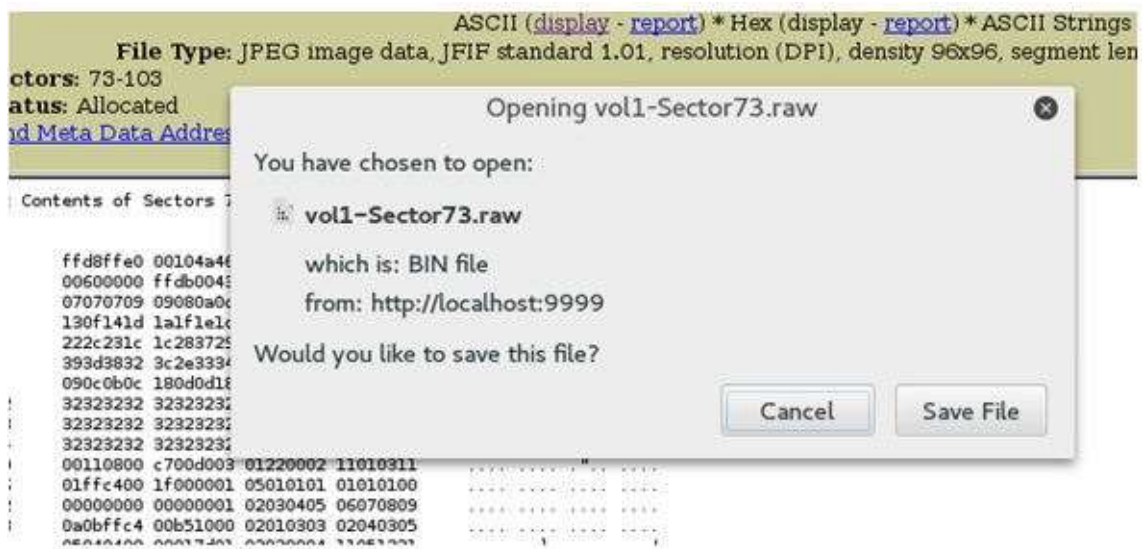


Damos click en View e inmediatamente el sistema reconoce el conjunto de byte donde se encuentra grabada la imagen en el disco que pertenecen a el archivo JPEG. Ahora

procedemos a extraer la imagen dando Click en Export Content



Nos aparecerá la siguiente Imagen.



Damos Click en Save File y Cambiamos la imagen de .raw a .jpeg

Sabemos que se trata de un fichero jpeg porque dicha información figura en los datos mostrados por Autopsy. Sin no fuera así, también podríamos ejecutar en un terminal en la máquina donde estamos realizando el análisis(en nuestro caso Kali), la orden:

```
# file nombre_fichero
```

para obtener el tipo de datos del mismo.



Guardamos el archivo y Damos Click sobre la imagen y visualizamos el contenido.

Análisis Archivo Jimmy Jungle.doc

En la primera visualización Autopsy, reconoce este archivo como eliminado y de extensión .doc

DEL	Type	NAME	WRITTEN	ACCESSED	CREATED
	dir / in				
	v / v	\$FAT1	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)
	v / v	\$FAT2	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)
	v / v	\$MBR	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)
	d / d	\$OrphanFiles/	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)
	r / r	cover_page.jpg	2002-09-11 08:30:52 (American)	2002-09-11 00:00:00 (American)	2002-09-11 08:50:27 (American)
✓	r / r	Jimmy Jungle.doc	2002-04-15 14:42:30 (American)	2002-09-11 00:00:00 (American)	2002-09-11 08:49:49 (American)
	r / r	Scheduled Visits.exe	2002-05-24 08:20:32 (American)	2002-09-11 00:00:00 (American)	2002-09-11 08:50:38 (American)

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * Add...

File Type: Composite Document File V2 Document, Little Endian, Os: Windows, Version 5.1, Code page: 1252, Title: Jimmy Jungle, Author: 0000t, Revision Number: 9, Name of Creating Application: Microsoft Word 10.0, Total Editing Time: 18:00, Create Time/Date: Mon Apr 15 21:42:00 2002, Number of Pages: 1, Number of Words: 138, Number of Characters: 787, Size: 4608 bytes

Deleted File Recovery Mode

Hex Contents Of File: X:/Jimmy Jungle.doc

```

00000000: 00CF 11E0 A1B1 1AE1 0000 0000 0000 0000  .....>.....
00000010: 0000 0000 0000 0000 3E00 0300 FEFF 0900  .....>.....
00000020: 0600 0000 0000 0000 0000 0000 0100 0000  .....>.....
00000030: 2300 0000 0000 0000 0010 0000 2500 0000  .....>.....
00000040: 0100 0000 FEFF FFFF 0000 0000 2200 0000  .....>.....

```

Ahora procedemos a verificar los metadatos del archivo dando Click sobre el link Meta.

SIZE	UID	GID	META
4608	0	0	45780
4608	0	0	45781
512	0	0	45779
0	0	0	45782
1) 15585	0	0	8
1) 20480	0	0	5
1) 1000	0	0	11

Verificamos sus datos para proceder al cálculo del número de bloques necesarios para extraer el archivo



Navigation: ◀ PREVIOUS NEXT ▶

Buttons: REPORT VIEW CONTENTS EXPORT CONTENTS ADD NOTE

[Search for File Name](#)

File Type:
Composite Document File V2 Document, Little Endian, Os: Windows, Version 5.1, Code page: 1252, Title: Jimmy Jungle, Author: 0000, Template: Normal, Last Save By: 0000t, Revision Number: 9, Name of Creating Application: Microsoft Word 10.0, Total Editing Time: 18:00, Create Time/Date: Mon Apr 15 20:30:00 2002, Last Saved Time/Date: Mon Apr 15 21:42:00 2002, Number of Pages: 1, Number of Words: 138, Number of Characters: 787, Security: 0

MD5 of content:
b775eb6a4ccc319759d9aaae1e349acc -

SHA-1 of content:
8bb25919c1c5762f05f528fc9c5c0edf74f96a39 -

Details:

Directory Entry: 5
Not Allocated
File Attributes: File, Archive
Size: 20480
Name: _JIMMYJ~1.DOC

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

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](#)

Entonces procedemos al Cálculo del archivo:
Números de sectores del archivo

- Desde sector 32
- Hasta Sector 72

Numero de sectores $72 - 32 = 40$

Con los datos obtenidos vamos al bloque 33, completamos el formulario y damos Click a View



Sector Number:

Number of Sectors:

Sector Size: 512

Address Type:

Lazarus Addr: ☐

VIEW

La operaci3n anterior debera haber mostrado la siguiente pantalla.

Sector Number:
33
Number of Sectors:
40
Sector Size: 512
Address Type:
Regular (dd)
Lazarus Addr:
View
Allocation List:
Load Unallocated

PREVIOUS
NEXT
EXPORT CONTENTS
ADD NOTE

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report)
File Type: Composite Document File V2 Document, Can't read SAT

Sectors: 33-72
Status: Not Allocated
Find Meta Data Address

Hex Contents of Sectors 33-72 in image-0-0

0	d0cf11e0	alb1lae1	00000000	00000000
16	00000000	00000000	3e000900	ffff0900
32	00000000	00000000	00000000	01000000
48	23000000	00000000	00100000	25000000
64	01000000	ffffffffff	00000000	22000000
80	ffffff	ffffff	ffffff	ffffff
96	ffffff	ffffff	ffffff	ffffff
112	ffffff	ffffff	ffffff	ffffff
128	ffffff	ffffff	ffffff	ffffff
144	ffffff	ffffff	ffffff	ffffff
160	ffffff	ffffff	ffffff	ffffff
176	ffffff	ffffff	ffffff	ffffff
192	ffffff	ffffff	ffffff	ffffff
208	ffffff	ffffff	ffffff	ffffff
224	ffffff	ffffff	ffffff	ffffff
240	ffffff	ffffff	ffffff	ffffff
256	ffffff	ffffff	ffffff	ffffff
272	ffffff	ffffff	ffffff	ffffff
288	ffffff	ffffff	ffffff	ffffff
304	ffffff	ffffff	ffffff	ffffff
320	ffffff	ffffff	ffffff	ffffff
336	ffffff	ffffff	ffffff	ffffff
352	ffffff	ffffff	ffffff	ffffff
368	ffffff	ffffff	ffffff	ffffff
384	ffffff	ffffff	ffffff	ffffff
400	ffffff	ffffff	ffffff	ffffff
416	ffffff	ffffff	ffffff	ffffff
432	ffffff	ffffff	ffffff	ffffff
448	ffffff	ffffff	ffffff	ffffff

Damos Click en Export Contents

PREVIOUS
NEXT
EXPORT CONTENTS
ADD NOTE

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report)
File Type: Composite Document File V2 Document, Can't read SAT

Sectors: 33-72
Status: Not Allocated
Find Meta Data Address

Contents of Sectors 33-72 in image-0-0

d0cf11e0 alb1lae1 00000000 00000000

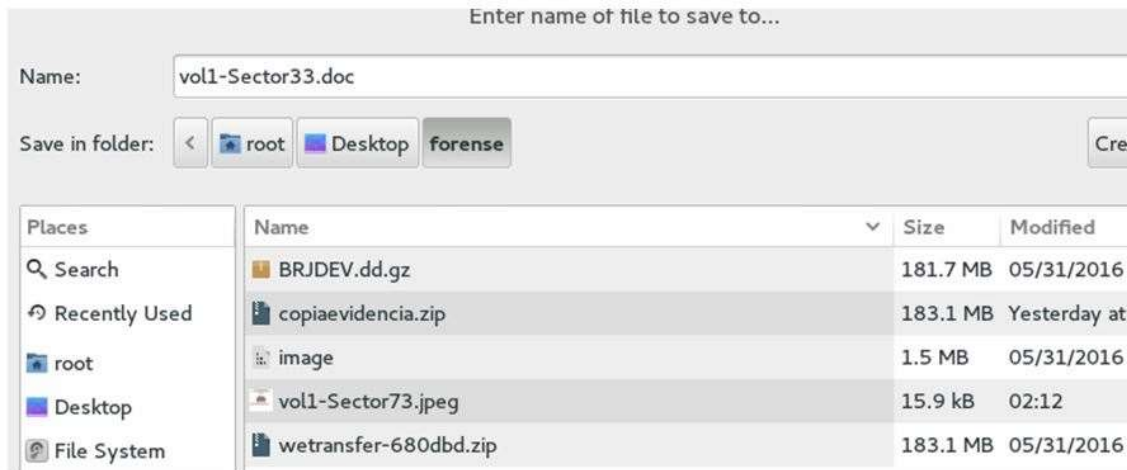
Damos Click en Guardar archivo

Opening vol1-Sector33.raw

You have chosen to open:
vol1-Sector33.raw
which is: BIN file
from: http://localhost:9999
Would you like to save this file?

Cancel
Save File

Cambiamos de extensión raw a Doc y guardamos



Y damos Click sobre el para verificar el contenido.

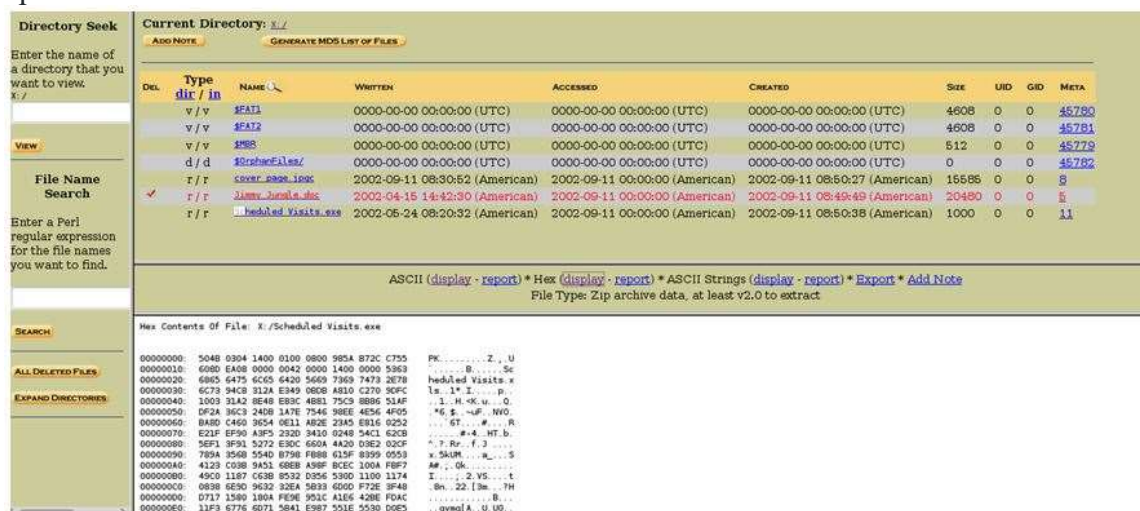
Respuestas al Caso

1. ¿Quién es el proveedor de marihuana de Joe Jacobs y cuál es su dirección?
2. ¿Qué proceso has realizado tu como investigador para examinar con éxito el contenido completo de cada archivo?

4. Ejercicio opcional

Análisis Archivo Scheduel Visits.exe

Damos Click sobre el archivo y verificamos los resultados entregados por la aplicación.



Ingresamos a Verificar sus metadatos.

	SIZE	UID	GID	META
	4608	0	0	45780
	4608	0	0	45781
	512	0	0	45779
	0	0	0	45782
n)	15585	0	0	8
n)	20480	0	0	5
n)	1000	0	0	11

Resultados de la pantalla metadatos

Dir Entry Number:

[VIEW](#)

[ALLOCATION LIST](#)

[PREVIOUS](#)
[REPORT](#) [VIEW CONTENTS](#)

[Search for File Name](#)
File Type:
Zip archive data, at least v2.0 to extract
MD5 of content:
082a5cc64dea22a3a580ffbb5a6fa66 -
SHA-1 of content:
c8e7f25380d63c9034d9f27faab29de1f09240b5 -
Details:
Directory Entry: 11
Allocated
File Attributes: File, Archive
Size: 1000
Name: SCHEDU~1.EXE
Directory Entry Times:
Written: 2002-05-24 08:20:32 (American)
Accessed: 2002-09-11 00:00:00 (American)
Created: 2002-09-11 08:50:38 (American)
Sectors:
[104](#) [105](#)

En la pantalla nos indica que el tamaño del archivo es de 1000 y que utiliza dos sectores 104 y 105.

Entonces procedemos al Cálculo del número de sectores del archivo. Con los datos obtenidos vamos al bloque 2, completamos el formulario y damos Click a View.

Procedemos a calcular el archivo

Sector Number:

Number of Sectors:

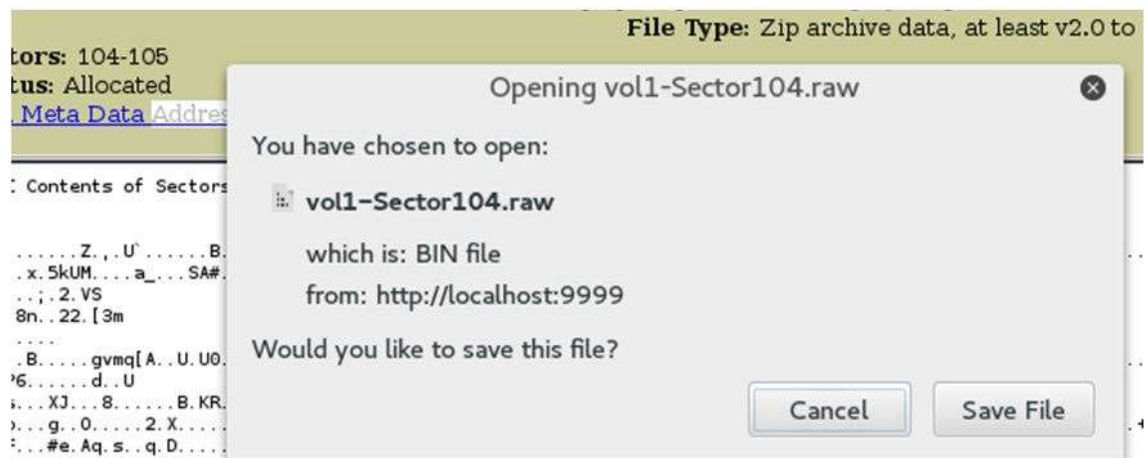
Sector Size: 512

Address Type:

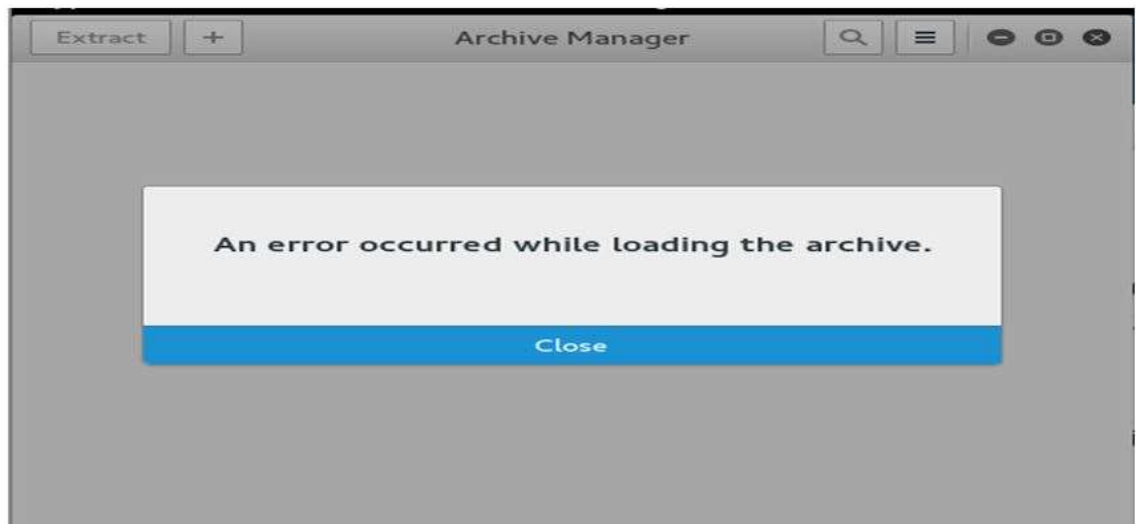
Lazarus Addr: ☐

VIEW

Ahora damos Click a Export Contents



Guardamos el archivo con extensión .zip y procedemos a extraer contenidos.



La siguiente imagen nos demuestra que el archivo está corrupto por lo que nos hacen falta más bloques para lograr crear el contenido. Así que probaremos a añadir un sector y haremos Export Content, tras cambiar la extensión a zip, procederemos a extraer el contenido. Si no tenemos éxito, repetiremos el mismo procedimiento añadiendo un sector más, hasta que consigamos abrir el fichero.

3. ¿Qué sectores conforman el fichero **Scheduld Visits.exe**?

Una vez hayáis conseguido el fichero .zip completo, procedemos a extraer el contenido.

4. ¿Cuál es el nombre del fichero contenido en el fichero .zip?

Al intentar descomprimir el fichero, vemos que es necesario introducir una clave. Al no disponer de ninguna clave explícitamente proporcionada, deberemos verificar las evidencias obtenidas en busca de ella, concretamente deberemos revisar el archivo jpeg y el doc para ver si pasamos por alto algún dato relevante que nos pueda indicar si la contraseña se encuentra dentro del diskette.

5. ¿Cuál es la contraseña? ¿Dónde la has localizado?

6. ¿Qué otros institutos (si los hay) adicionales a Smith Hill, frecuenta Joe Jacobs?

Escribe tu respuesta a las preguntas 1y 2 (ejercicios básicos) o 1,2,3,4,5,6 (con ejercicio opcional) en un fichero con tu nombre (o el de los componentes del grupo si trabajáis en grupo) y súbelo a tu espacio compartido de PoliformaT.



UNIVERSITAT
POLITÈCNICA
DE VALÈNCIA

