

SEGURIDAD EN SISTEMAS OPERATIVOS (2017-2018)  
GRADO EN INGENIERÍA INFORMÁTICA  
UNIVERSIDAD DE GRANADA

---

## Práctica 3 Sesión 1

---



**UNIVERSIDAD  
DE GRANADA**

Iván Rodríguez Millán  
ivanrodmil@gmail.com

## Índice

1	Vamos a crear en nuestro pendrive un archivo con un supuesto texto de una amenaza y luego vamos a borrarlo. Aplicando las herramientas anteriores vamos a intentar recuperar lo que quede del archivo borrado haciendo una copia del pendrive sobre la que trabajar, no directamente sobre el pendrive.	3
2	Realizar una imagen forense del pendrive con la herramienta guymager.	5
3	Como en el ejercicio 1 y partiendo de la imagen forense del 2, buscar con la herramienta Autopsy las evidencias de la amenaza realizada.	8

## Índice de figuras

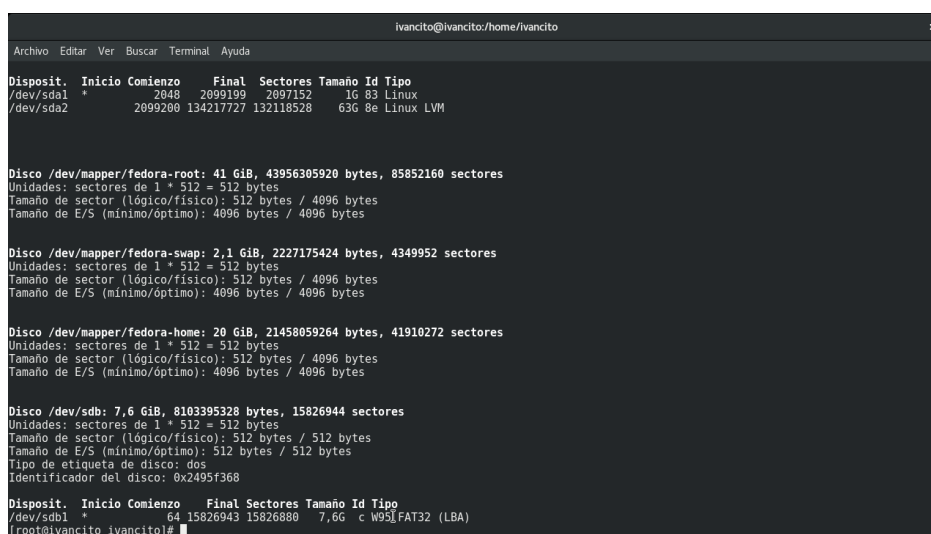
1.1.	Listado de particiones en Fedora. . . . .	3
1.2.	Montado de usb en Fedora. . . . .	3
1.3.	Creado y eliminado el fichero en el usb. . . . .	4
1.4.	Copiado del disco usb en nuestro portátil. . . . .	4
1.5.	Montando imagen restaurada. . . . .	4
1.6.	Listando la imagen montada. . . . .	5
1.7.	Fichero con palabras posibles a buscar. . . . .	5
1.8.	Mostrando datos borrados anteriormente. . . . .	5
2.1.	Corriendo Guymager. . . . .	6
2.2.	Adquiriendo imagen con Guymager. . . . .	6
2.3.	Modo running. . . . .	7
2.4.	Finalizado copia de imagen. . . . .	7
2.5.	Comprobación de la creación de la imagen. . . . .	8
3.1.	Inicialización de Autopsy. . . . .	9
3.2.	Creando nuevo caso con Autopsy. . . . .	9
3.3.	Creado nuevo caso con Autopsy. . . . .	10
3.4.	Añadiendo imagen a nuevo caso de Autopsy. . . . .	10
3.5.	Añadida imagen a nuevo caso de Autopsy. . . . .	11
3.6.	Buscando cadena en la imagen. . . . .	11
3.7.	Resultados de la búsqueda por cadenas. . . . .	12
3.8.	Nuevo caso de estudio. . . . .	12
3.9.	Buscando el fichero eliminado. . . . .	13

## Índice de tablas

1. Vamos a crear en nuestro pendrive un archivo con un supuesto texto de una amenaza y luego vamos a borrarlo. Aplicando las herramientas anteriores vamos a intentar recuperar lo que quede del archivo borrado haciendo una copia del pendrive sobre la que trabajar, no directamente sobre el pendrive.

En primer lugar listamos la tabla de particiones con todos los dispositivos de almacenamiento para mostrar que hemos introducido un pendrive:

Esto se realiza con el comando: **fdisk -l**. [2]



```
ivancito@ivancito:/home/ivancito
Archivo Editar Ver Buscar Terminal Ayuda

Disposit.  Inicio Comienzo    Final Sectores Tamaño Id Tipo
/dev/sda1  *          2048    2099199    2097152      1G 83 Linux
/dev/sda2          2099200 134217727 132118528     63G 8e Linux LVM

Disco /dev/mapper/fedora-root: 41 GiB, 43956305920 bytes, 85852160 sectores
Unidades: sectores de 1 * 512 = 512 bytes
Tamaño de sector (lógico/físico): 512 bytes / 4096 bytes
Tamaño de E/S (mínimo/óptimo): 4096 bytes / 4096 bytes

Disco /dev/mapper/fedora-swap: 2,1 GiB, 2227175424 bytes, 4349952 sectores
Unidades: sectores de 1 * 512 = 512 bytes
Tamaño de sector (lógico/físico): 512 bytes / 4096 bytes
Tamaño de E/S (mínimo/óptimo): 4096 bytes / 4096 bytes

Disco /dev/mapper/fedora-home: 20 GiB, 21458059264 bytes, 41910272 sectores
Unidades: sectores de 1 * 512 = 512 bytes
Tamaño de sector (lógico/físico): 512 bytes / 4096 bytes
Tamaño de E/S (mínimo/óptimo): 4096 bytes / 4096 bytes

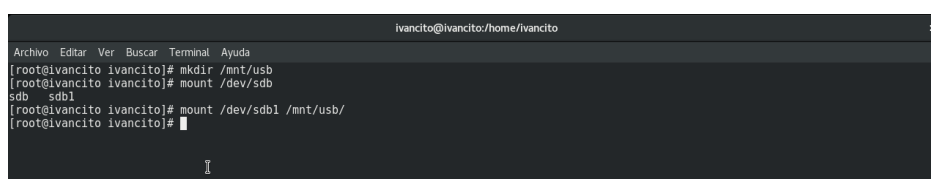
Disco /dev/sdb: 7,6 GiB, 8103395328 bytes, 15826944 sectores
Unidades: sectores de 1 * 512 = 512 bytes
Tamaño de sector (lógico/físico): 512 bytes / 512 bytes
Tamaño de E/S (mínimo/óptimo): 512 bytes / 512 bytes
Tipo de etiqueta de disco: dos
Identificador del disco: 0x2495f368

Disposit.  Inicio Comienzo    Final Sectores Tamaño Id Tipo
/dev/sdb1  *          64    15826943 15826880     7,6G c W95 FAT32 (LBA)

[root@ivancito ivancito]#
```

Figura 1.1: Listado de particiones en Fedora.

Después de listar los discos, montamos el dispositivo usb:



```
ivancito@ivancito:/home/ivancito
Archivo Editar Ver Buscar Terminal Ayuda

[root@ivancito ivancito]# mkdir /mnt/usb
[root@ivancito ivancito]# mount /dev/sdb
sdb sdb1
[root@ivancito ivancito]# mount /dev/sdb1 /mnt/usb/
[root@ivancito ivancito]#
```

Figura 1.2: Montado de usb en Fedora.

Seguidamente creamos un fichero de prueba, y lo eliminamos.

```

[root@ivancito usb]# nano ficheroPrueba.txt
[root@ivancito usb]# ls
15519720X.pdf  desktop.ini  ficheroPrueba.txt  'System Volume Information'
[root@ivancito usb]# cat ficheroPrueba.txt
Fichero de prueba para la practica 3 de SS0.
[root@ivancito usb]# rm ficheroPrueba.txt
rm: ¿borrar el fichero regular 'ficheroPrueba.txt'? (s/n) s
[root@ivancito usb]# ls
15519720X.pdf  desktop.ini  'System Volume Information'
[root@ivancito usb]#

```

Figura 1.3: Creado y eliminado el fichero en el usb.

Una vez realizamos el anterior paso, lo siguiente será crear una imagen del disco en estudio para asegurarnos de no afectar al disco original y darle los permisos necesarios por cuestiones de seguridad. Esto se realiza de la siguiente manera:

```

ivancito@ivancito:/mnt/usb
Archivo Editar Ver Buscar Terminal Ayuda
[root@ivancito usb]# dd if=/dev/sdb1 of=/home/ivancito/imagen.discol bs=512
15826880+0 registros leídos
15826880+0 registros escritos
8103362560 bytes (8,1 GB, 7,5 GiB) copied, 373,771 s, 21,7 MB/s
[root@ivancito usb]# chmod 444 /home/ivancito/imagen.discol
[root@ivancito usb]#

```

Figura 1.4: Copiado del disco usb en nuestro portátil.

Para seguir con el proceso montamos la imagen restaurada del pendrive:

```

ivancito@ivancito:/home/ivancito
Archivo Editar Ver Buscar Terminal Ayuda
[root@ivancito ivancito]# umount /mnt/usb
[root@ivancito ivancito]# mkdir /mnt/analisis
[root@ivancito ivancito]# mount
mount                                mount.lowmfs-3g  mount.nfs4      mount.ntfs-3g  mountpoint      mount.zfs
mount.cifs                          mount.glusterfs  mount.nfs       mount.ntfs     mount.ntfs-fuse  mountstats
[root@ivancito ivancito]# mount imagen.discol /mnt/analisis/

```

Figura 1.5: Montando imagen restaurada.

En el siguiente paso podemos ver el contenido de la imagen montada:

```
ivancito@ivancito:/mnt/analysis
Archivo Editar Ver Buscar Terminal Ayuda
[root@ivancito ivancito]# cd /mnt/analysis/
[root@ivancito analisis]# ls
15519720X.pdf  desktop.ini  'System Volume Information'  TicketCiudadanoCompletoAE15519720X.pdf
[root@ivancito analisis]# find . -type f -print > /home/ivancito/evidencias.archivos.2
[root@ivancito analisis]# cat /home/ivancito/evidencias.archivos.2
./15519720X.pdf
./desktop.ini
./Spotlight-V100/Store-V2/8BF71446-FB1A-4268-89F3-93583D1DD99E/psid.db
./Spotlight-V100/Store-V2/8BF71446-FB1A-4268-89F3-93583D1DD99E/tmp.SnowLeopard
./Spotlight-V100/Store-V2/8BF71446-FB1A-4268-89F3-93583D1DD99E/tmp.Lion
./Spotlight-V100/Store-V2/8BF71446-FB1A-4268-89F3-93583D1DD99E/Lion.created
./Spotlight-V100/Store-V2/8BF71446-FB1A-4268-89F3-93583D1DD99E/tmp.Cab
./Spotlight-V100/Store-V2/8BF71446-FB1A-4268-89F3-93583D1DD99E/Cab.created
./Spotlight-V100/Store-V2/8BF71446-FB1A-4268-89F3-93583D1DD99E/indexState
./Spotlight-V100/Store-V2/8BF71446-FB1A-4268-89F3-93583D1DD99E/0.indexHead
./Spotlight-V100/Store-V2/8BF71446-FB1A-4268-89F3-93583D1DD99E/0.indexIds
./Spotlight-V100/Store-V2/8BF71446-FB1A-4268-89F3-93583D1DD99E/0.indexGroups
./Spotlight-V100/Store-V2/8BF71446-FB1A-4268-89F3-93583D1DD99E/0.indexPostings
./Spotlight-V100/Store-V2/8BF71446-FB1A-4268-89F3-93583D1DD99E/0.indexTermIds
./Spotlight-V100/Store-V2/8BF71446-FB1A-4268-89F3-93583D1DD99E/0.indexPositions
./Spotlight-V100/Store-V2/8BF71446-FB1A-4268-89F3-93583D1DD99E/0.indexPositionTable
./Spotlight-V100/Store-V2/8BF71446-FB1A-4268-89F3-93583D1DD99E/0.indexDirectory
./Spotlight-V100/Store-V2/8BF71446-FB1A-4268-89F3-93583D1DD99E/0.indexCompactDirectory
./Spotlight-V100/Store-V2/8BF71446-FB1A-4268-89F3-93583D1DD99E/0.indexArrays
./Spotlight-V100/Store-V2/8BF71446-FB1A-4268-89F3-93583D1DD99E/0.indexUpdates
./Spotlight-V100/Store-V2/8BF71446-FB1A-4268-89F3-93583D1DD99E/0.directoryStoreFile
./Spotlight-V100/Store-V2/8BF71446-FB1A-4268-89F3-93583D1DD99E/live.0.indexHead
./Spotlight-V100/Store-V2/8BF71446-FB1A-4268-89F3-93583D1DD99E/live.0.indexIds
./Spotlight-V100/Store-V2/8BF71446-FB1A-4268-89F3-93583D1DD99E/live.0.indexGroups
./Spotlight-V100/Store-V2/8BF71446-FB1A-4268-89F3-93583D1DD99E/live.0.indexPostings
./Spotlight-V100/Store-V2/8BF71446-FB1A-4268-89F3-93583D1DD99E/live.0.indexTermIds
./Spotlight-V100/Store-V2/8BF71446-FB1A-4268-89F3-93583D1DD99E/live.0.indexPositions
./Spotlight-V100/Store-V2/8BF71446-FB1A-4268-89F3-93583D1DD99E/live.0.indexPositionTable
./Spotlight-V100/Store-V2/8BF71446-FB1A-4268-89F3-93583D1DD99E/live.0.indexDirectory
./Spotlight-V100/Store-V2/8BF71446-FB1A-4268-89F3-93583D1DD99E/live.0.indexCompactDirectory
./Spotlight-V100/Store-V2/8BF71446-FB1A-4268-89F3-93583D1DD99E/live.0.indexArrays
```

Figura 1.6: Listando la imagen montada.

Para ver si queda rastro del fichero eliminado nos vamos a crear un fichero con algunas de las palabras que aparecían en el fichero eliminado anteriormente:

```
ivancito@ivancito:/mnt/analysis
Archivo Editar Ver Buscar Terminal Ayuda
[root@ivancito analisis]# nano /home/ivancito/ficheroPalabras.txt
[root@ivancito analisis]# cat /home/ivancito/ficheroPalabras.txt
prueba
SS0
fichero
```

Figura 1.7: Fichero con palabras posibles a buscar.

Por último podemos mostrar los datos que se habían borrado, de tal forma que haciendo uso de del comando grep se vuelca el contenido común con la lista creada en la figura anterior, y después se observa que esté en tal archivo la frase que habíamos almacenado.

```
ivancito@ivancito:/home/ivancito
Archivo Editar Ver Buscar Terminal Ayuda
[root@ivancito ivancito]# grep -aibf ficheroPalabras.txt imagen.discol > aciertos.txt
[root@ivancito ivancito]# grep "Fichero de prueba para la practica 3 de SS0" aciertos.txt
Coincidencia en el fichero V2/Binary aciertos.txt
[root@ivancito ivancito]#
```

Figura 1.8: Mostrando datos borrados anteriormente.

## 2. Realizar una imagen forense del pendrive con la herramienta guymager.

Una vez instalado el programa procedemos a ejecutarlo. [1]

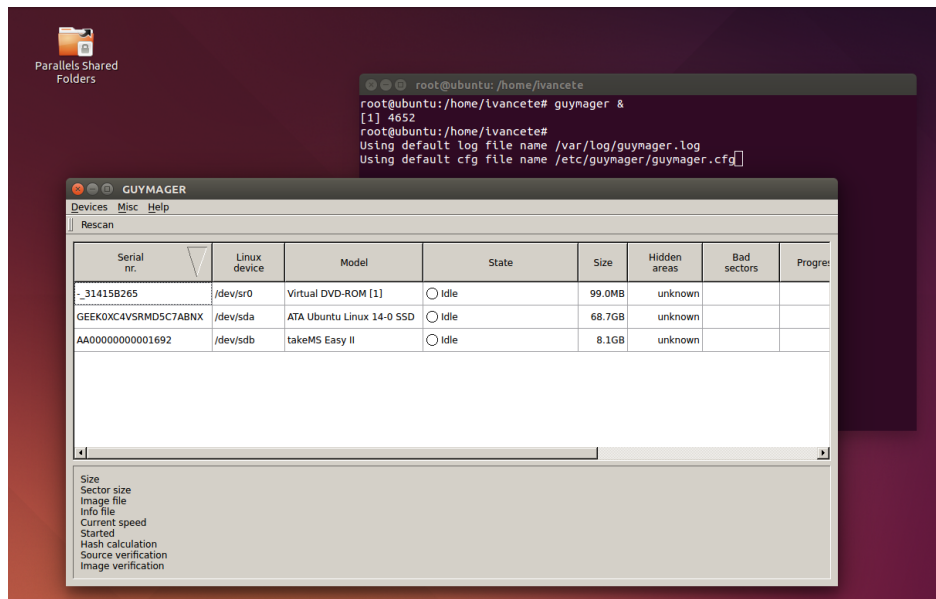


Figura 2.1: Corriendo Guymager.

Vemos como se nos muestran los distintos dispositivos montados, el último de ellos sería el pendrive. En el siguiente paso procedemos con botón derecho sobre el dispositivo y pulsamos sobre `acquireimage`:

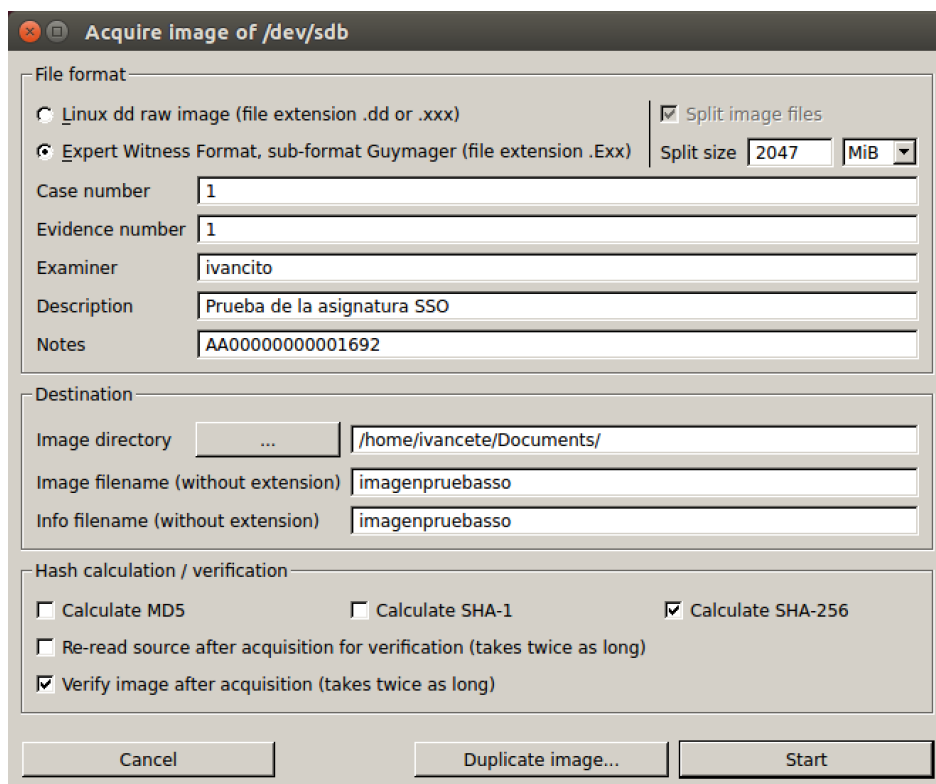


Figura 2.2: Adquiriendo imagen con Guymager.

Tras configurar todos los campos que nos pide procedemos a pulsar start, después nos saldrá algo parecido a lo siguiente en donde nos informará de que está en modo running:

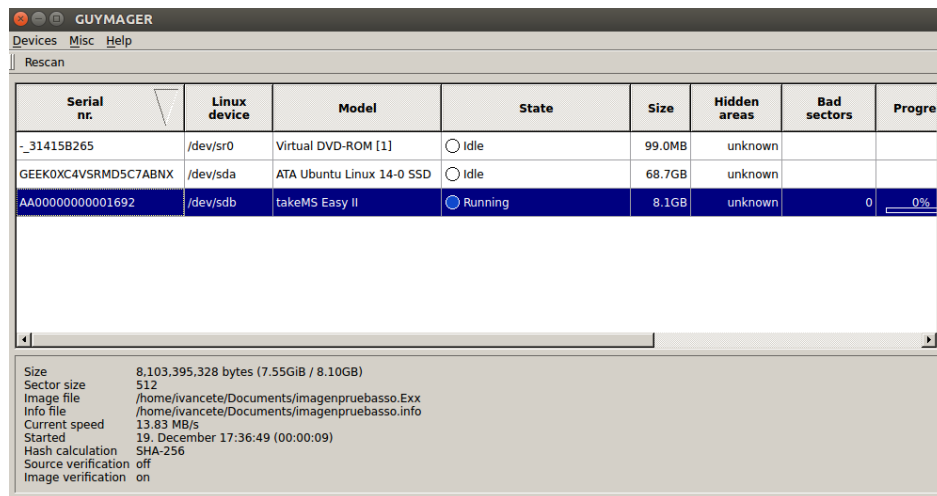


Figura 2.3: Modo running.

Después de todo este proceso deberá finalizar como sigue aquí:

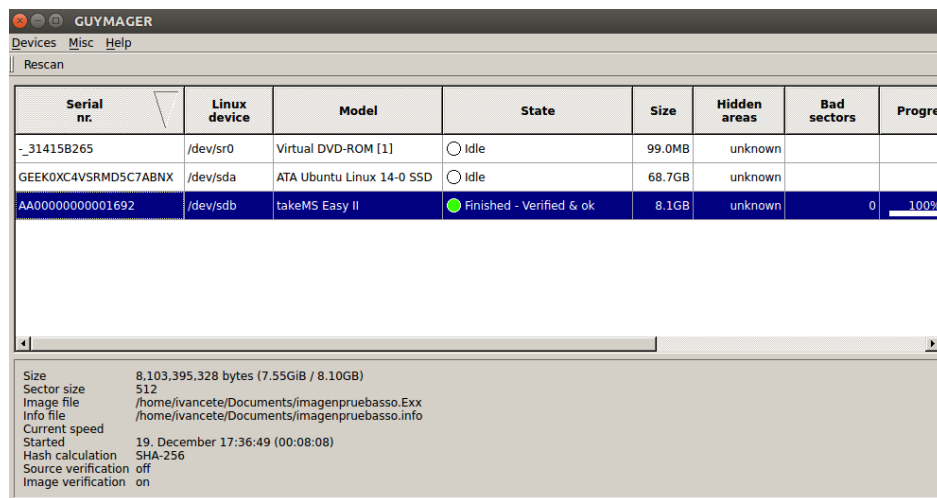


Figura 2.4: Finalizado copia de imagen.

Para finalizar comprobamos que ha realizado correctamente la creación de la imagen:

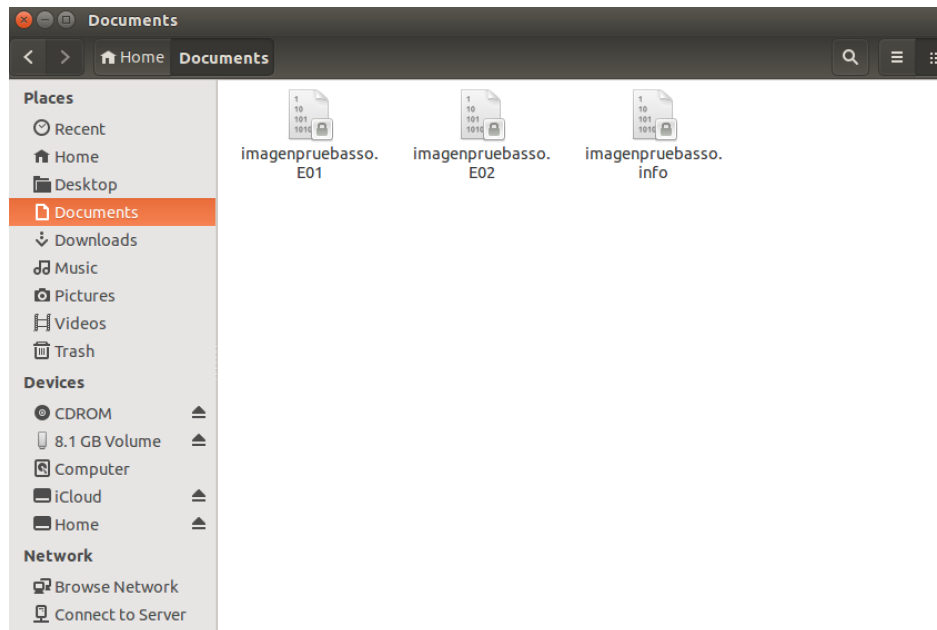


Figura 2.5: Comprobación de la creación de la imagen.

Como vemos no se ha creado la imagen, esto es debido a la versión instalada, pero es que para la versión de Ubuntu 14 no hay una versión de Guymager más moderna, se lamentan los problemas ocasionados.

### 3. Como en el ejercicio 1 y partiendo de la imagen forense del 2, buscar con la herramienta Autopsy las evidencias de la amenaza realizada.

Tras instalar tanto TSK como Autopsy, lo iniciamos, mostrándose lo siguiente: [4]



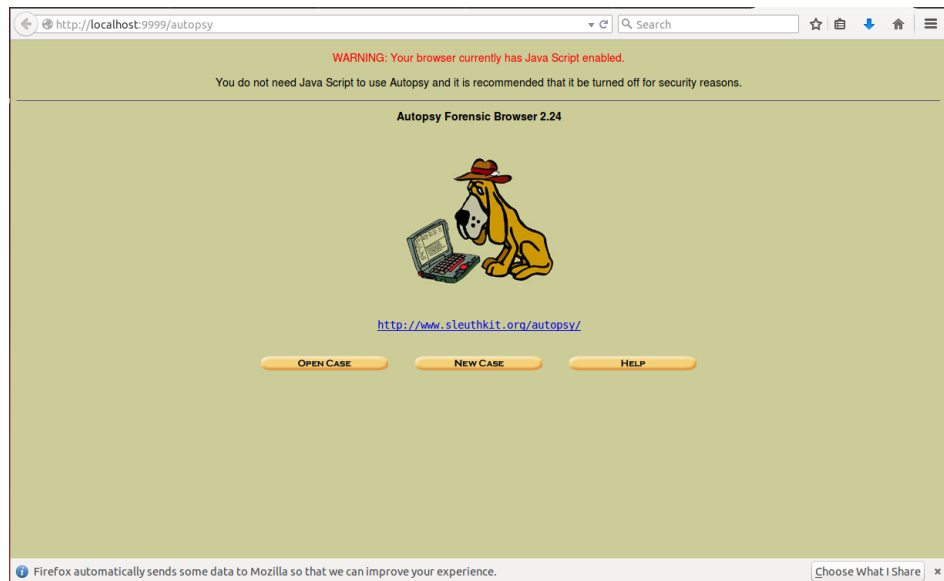


Figura 3.1: Inicialización de Autopsy.

Creamos un nuevo caso introduciendo los valores en los campos correspondientes.

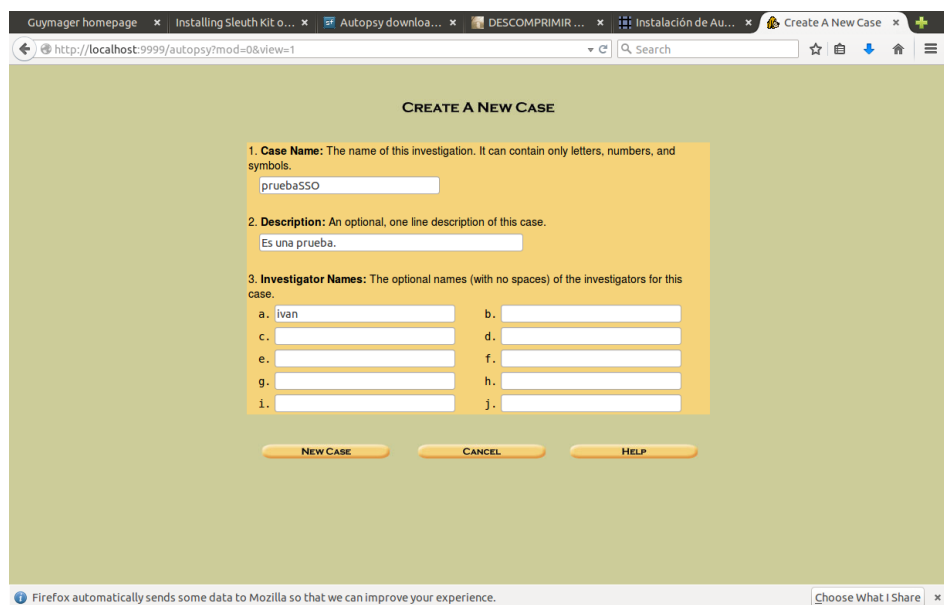


Figura 3.2: Creando nuevo caso con Autopsy.

Después nos saldrá la siguiente imagen, y deberemos añadir una imagen:

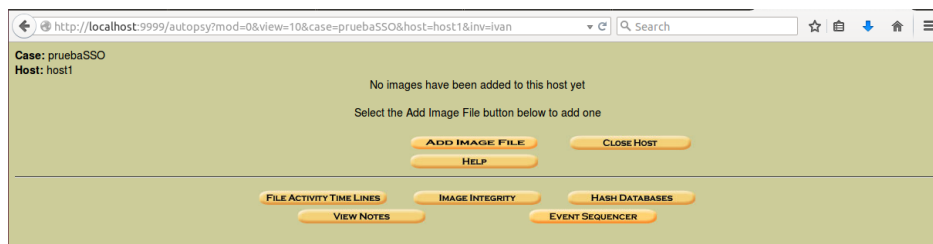


Figura 3.3: Creado nuevo caso con Autopsy.

Añadimos la imagen correspondiente realizada en el paso 1, ya que la del paso 2 no puede ser como se explicó anteriormente por un error de Guymager:

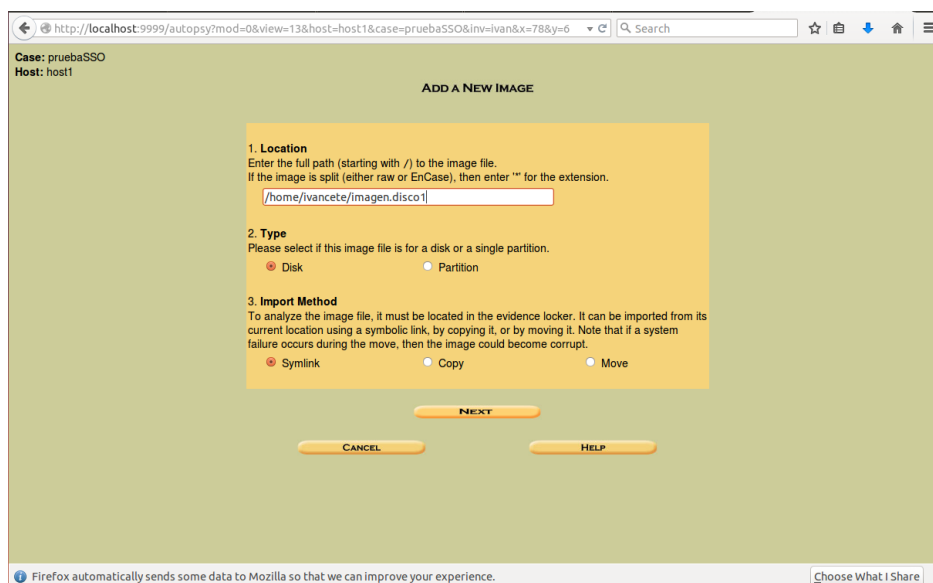


Figura 3.4: Añadiendo imagen a nuevo caso de Autopsy.

Una vez añadida la imagen nos saldrá algo como la siguiente imagen, y ahora podremos analizarla:

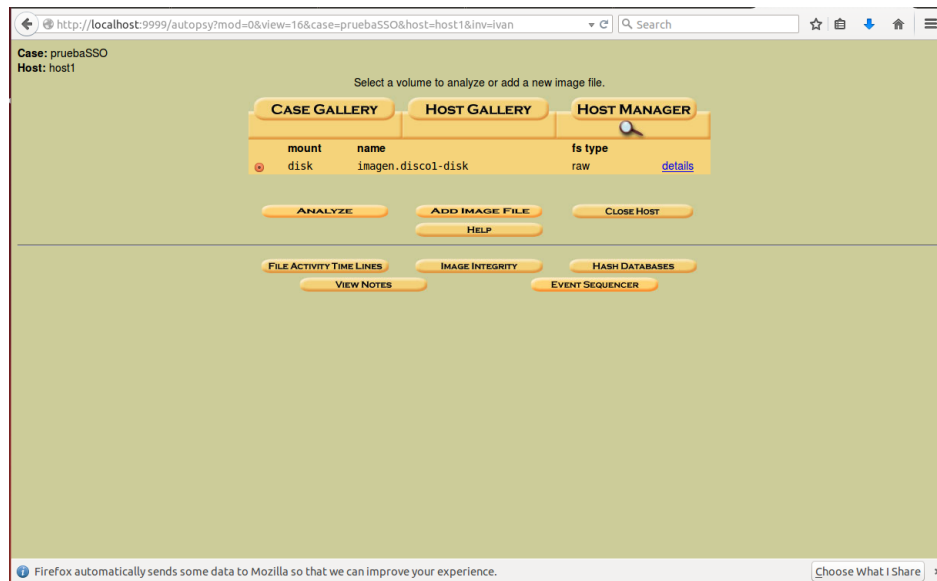


Figura 3.5: Añadida imagen a nuevo caso de Autopsy.

Por último nos queda buscar la cadena como hicimos en el ejercicio 1:

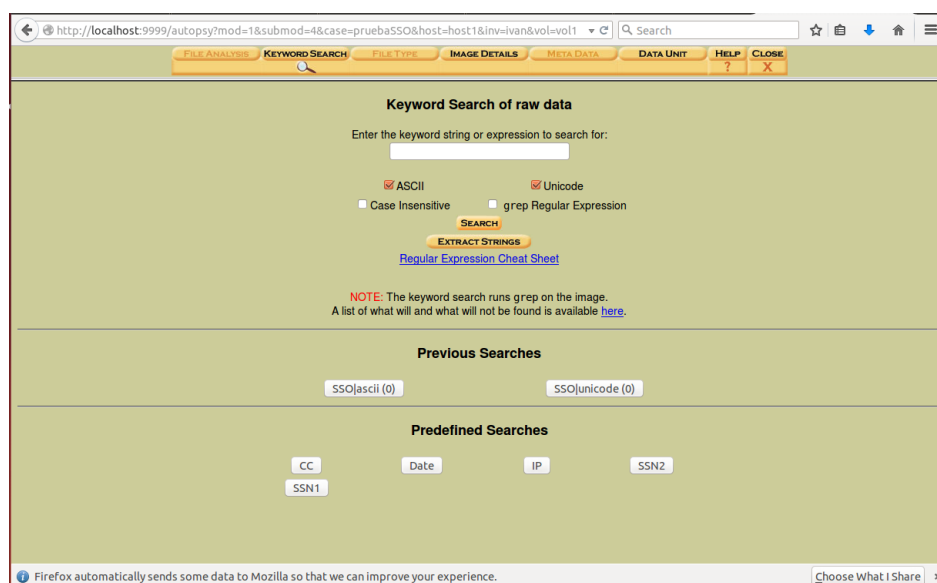


Figura 3.6: Buscando cadena en la imagen.

Comentar que se intentó buscar por varias cadenas tal y como hicimos en el ejercicio 1 y no se encontró ninguna coincidencia, esto puede ser debido al programa Autopsy ya que anteriormente en el ejercicio 1 no hubo ningún problema. [3]

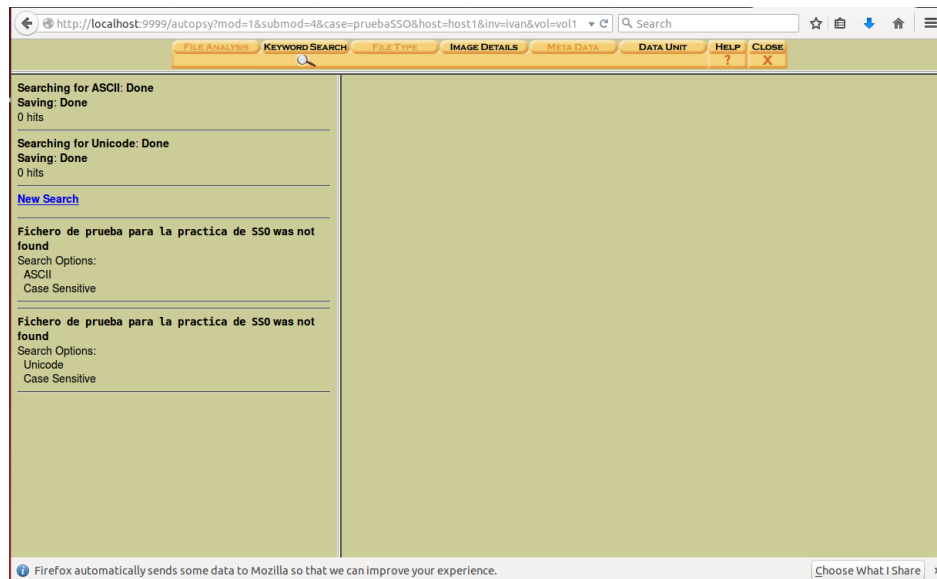


Figura 3.7: Resultados de la búsqueda por cadenas.

Sin embargo si volvemos a realizar otro caso de uso indicando que es una partición, se nos mostrará la siguiente imagen en donde ya si detecta el sistema de archivos de la partición:

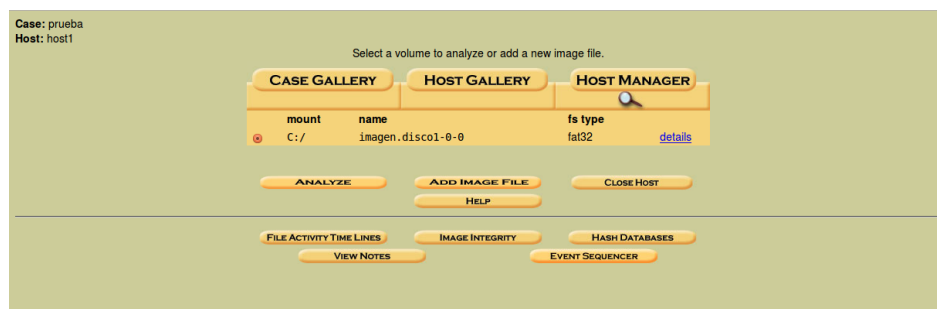


Figura 3.8: Nuevo caso de estudio.

Y si realizamos la búsqueda de ficheros, y nos vamos a File Analysis -> All Deleted File nos mostrará todos los ficheros eliminados anteriormente:

FILE ANALYSIS

KEYWORD SEARCH

FILE TYPE

IMAGE DETAILS

META DATA

DATA UNIT

HELP

CLOSE

Directory Seek

Enter the name of a directory that you want to view.  
C:/

VIEW

File Name Search

Enter a Perl regular expression for the file names you want to find.  
fichero

SEARCH

ALL DELETED FILES

EXPAND DIRECTORIES

All files with 'fichero' in the name

SHOW ALL FILES

Error Parsing File (invalid characters?)  
: V/V 252712070: \$OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0 0 0

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
✓	r / r	C:/ficheroPrueba.txt	2017-12-19 15:35:46 (CET)	2017-12-19 00:00:00 (CET)	2017-12-19 15:35:46 (CET)	45	0	0	39

ASCII (display - report) \* Hex (display - report) \* ASCII Strings (display - report) \* Export \* Add Note

File Type: ASCII text

Deleted File Recovery Mode

Contents Of File: C:/ficheroPrueba.txt

Fichero de prueba para la practica 3 de S50.

Figura 3.9: Buscando el fichero eliminado.

## Referencias

- [1] <http://guymager.sourceforge.net/>, consultado el 19 de Diciembre de 2017.
- [2] <http://manpages.ubuntu.com/manpages/trusty/es/man8/fdisk.8.html>, consultado el 19 de Diciembre de 2017.
- [3] <http://sleuthkit.org/autopsy/docs/user-docs/4.3/>, consultado el 19 de Diciembre de 2017.
- [4] <https://www.sleuthkit.org/autopsy/>, consultado el 19 de Diciembre de 2017.