

SEGURIDAD EN SISTEMAS OPERATIVOS

4º Grado en Informática – Complementos de Ing. del Software
Curso 2018-19

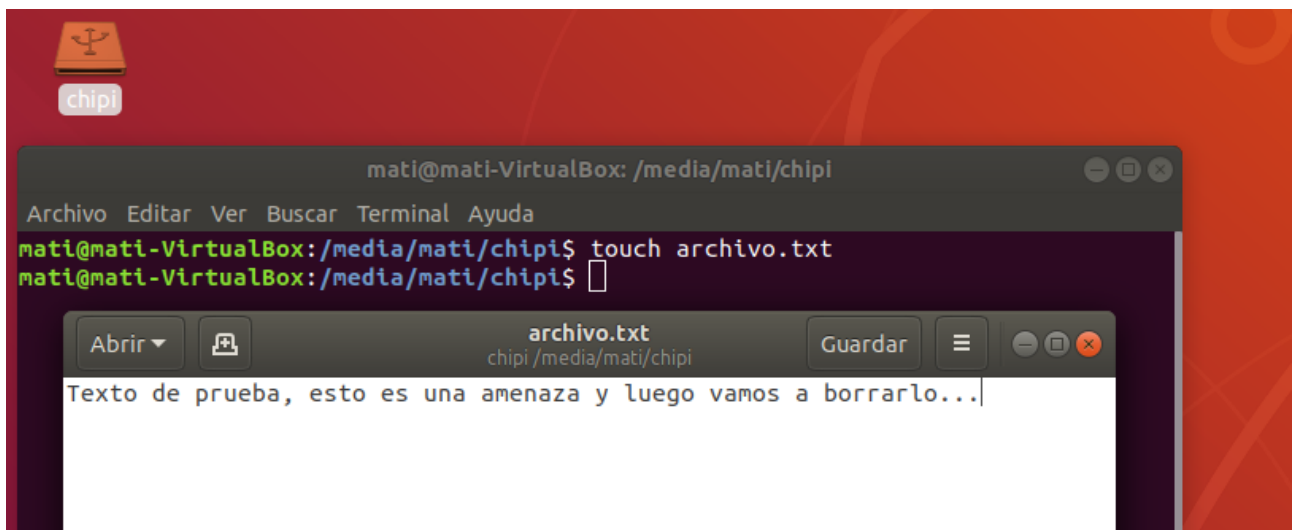
Práctica [3]. Auditoría informática e Informática forense

Sesión [1]. Análisis forense en Linux

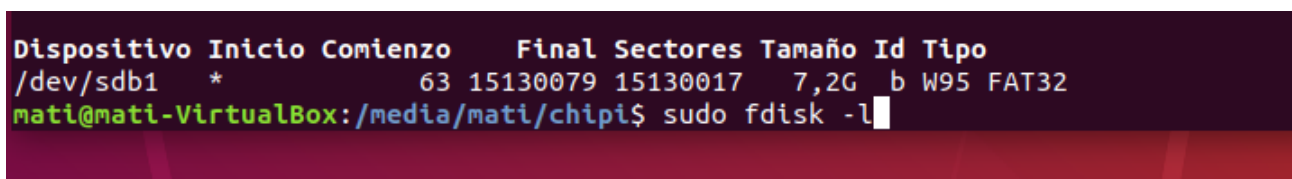
Autor¹: Matilde Cabrera González

Ejercicio 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*.



Borramos el archivo.txt y dejamos el pendrive vacío. Buscamos el dispositivo:



¹ Como autor declaro que los contenidos del presente documento son originales y elaborados por mi. De no cumplir con este compromiso, soy consciente de que, de acuerdo con la “Normativa de evaluación y de calificaciones de los estudiantes de la Universidad de Granada” esto “conllevará la calificación numérica de cero ... independientemente del resto de calificaciones que el estudiante hubiera obtenido ...”

Hacemos la copia a nuestra maquina:

```
mati@mati-VirtualBox:~$ dd if=/dev/sdb of=copiapen.disk1 bs=512
dd: No se puede abrir '/dev/sdb': Permiso denegado
mati@mati-VirtualBox:~$ sudo dd if=/dev/sdb of=copiapen.disk1 bs=512
15131636+0 registros leídos
15131636+0 registros escritos
7747397632 bytes (7,7 GB, 7,2 GiB) copied, 2266,29 s, 3,4 MB/s
mati@mati-VirtualBox:~$
```

Le damos permiso de solo lectura:

```
mati@mati-VirtualBox:~$ ls
copiapen.disk1  Documentos  Imágenes  Plantillas  Vídeos
Descargas      Escritorio  Música    Público
mati@mati-VirtualBox:~$ sudo chmod 444 copiapen.disk1
[sudo] contraseña para mati:
mati@mati-VirtualBox:~$
```

Buscamos el archivo borrado. Para ello primero creamos un duplicado exacto del dispositivo.

```
mati@mati-VirtualBox:~$ sudo dd if=copiapen.disk1 of=/dev/fd0 bs=512
dd: error al escribir en '/dev/fd0': No queda espacio en el dispositivo
4221881+0 registros leídos
4221880+0 registros escritos
2161602560 bytes (2,2 GB, 2,0 GiB) copied, 38,1462 s, 56,7 MB/s
mati@mati-VirtualBox:~$
```

Después montamos con: “sudo mount -t vfat -ro,noexec /dev/fd0 /home/mati/sso”

Generamos un archivo llamado aux.txt que dentro tiene la palabra amenaza.

Y por ultimo buscamos el archivo con: “grep -aibf aux.txt copiapen.disk1 > archivo.txt”

Esto nos devuelve el fichero con nuestro mensaje original.

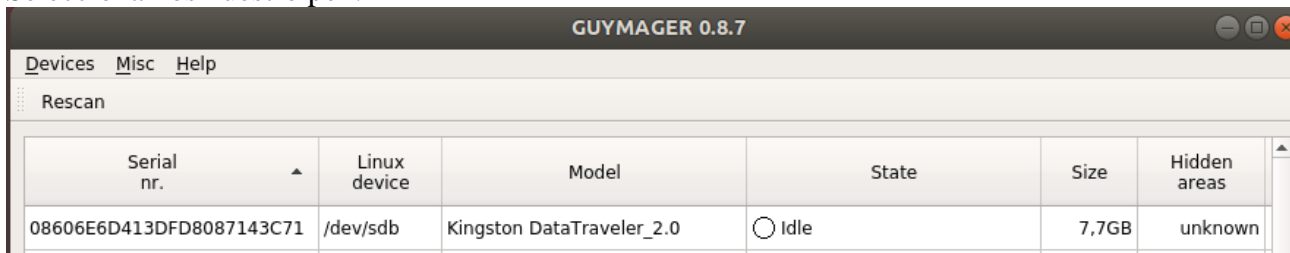
Ejercicio 2.

Realizar una imagen forense del *pendrive* con la herramienta guymager.

Instalamos la herramienta:

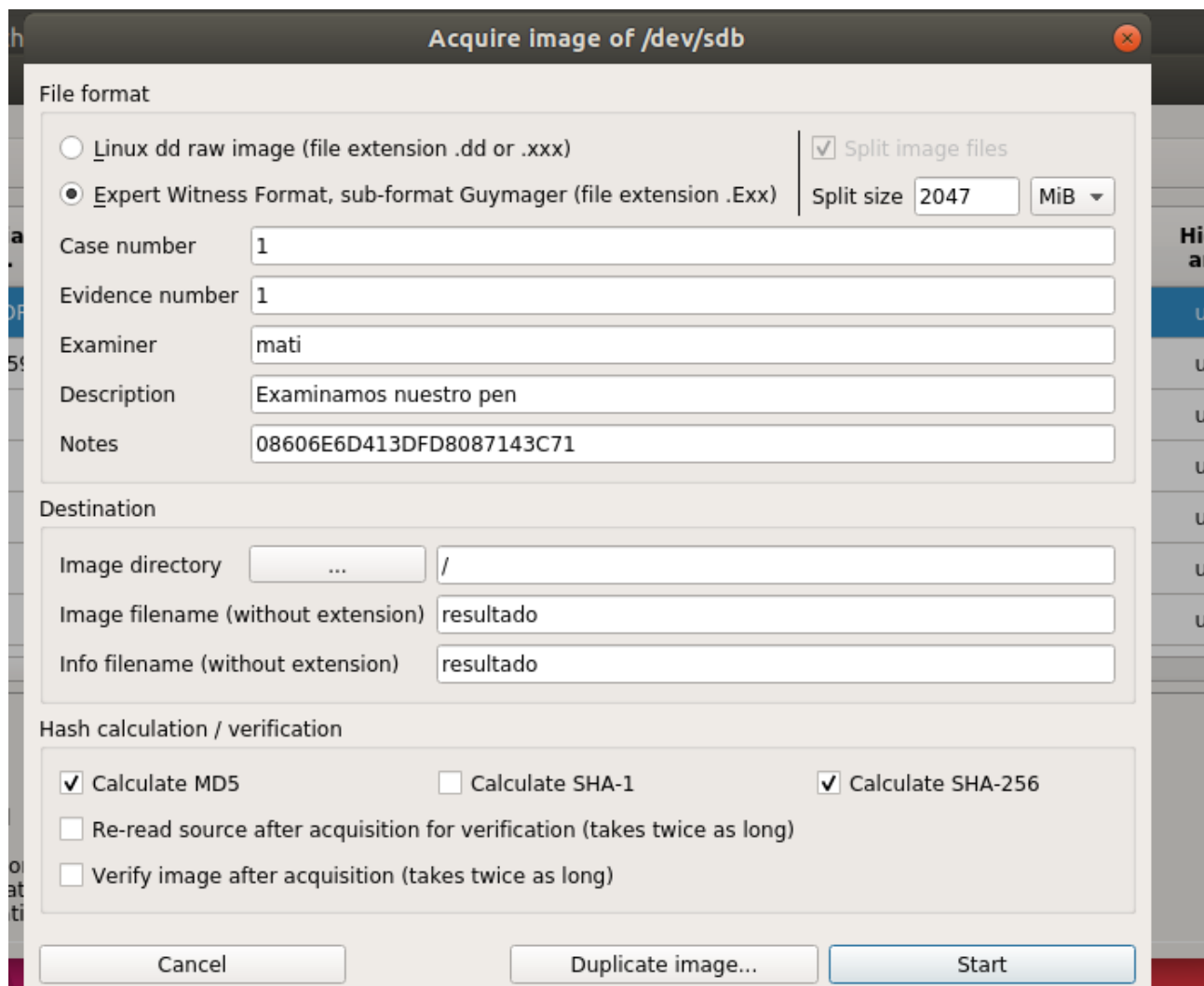
```
mati@mati-VirtualBox:~$ sudo apt-get install guymager
[sudo] contraseña para mati:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
guile-2.0-libs libbfio1 libdouble-conversion1 libewf2 libgsasl7 libguytools2
libkyotocabinet16v5 libmailutils5 libmysqlclient20 libntlm0 libqt5core5a
libqt5dbus5 libqt5gui5 libqt5network5 libqt5svg5 libqt5widgets5
libxcb-xinerama0 mailutils mailutils-common mysql-common postfix
qt5-gtk-platformtheme qttranslations5-l10n smartmontools
Paquetes sugeridos:
```

Seleccionamos nuestro pen:



Serial nr.	Linux device	Model	State	Size	Hidden areas
08606E6D413DFD8087143C71	/dev/sdb	Kingston DataTraveler_2.0	<input type="radio"/> Idle	7,7GB	unknown

Configuramos la creación de la imagen, le damos a start y a esperar...



Acquire image of /dev/sdb

File format

☐ Linux dd raw image (file extension .dd or .xxx) | ☒ Split image files

☒ Expert Witness Format, sub-format Guymager (file extension .Exx) | Split size: 2047 MiB

Case number: 1

Evidence number: 1

Examiner: mati

Description: Examinamos nuestro pen

Notes: 08606E6D413DFD8087143C71

Destination

Image directory: /

Image filename (without extension): resultado

Info filename (without extension): resultado

Hash calculation / verification

☒ Calculate MD5 | ☐ Calculate SHA-1 | ☒ Calculate SHA-256

☐ Re-read source after acquisition for verification (takes twice as long)

☐ Verify image after acquisition (takes twice as long)

Buttons: Cancel, Duplicate image..., Start

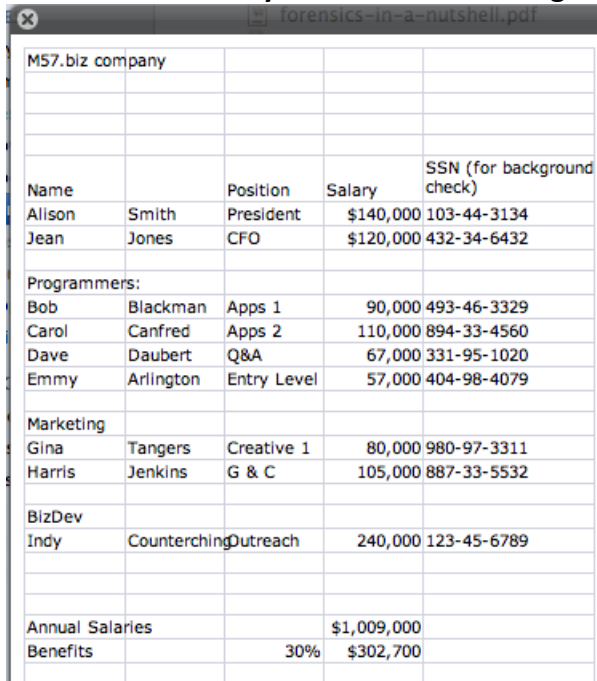
Tarda tanto en el análisis, que no esperamos los 8G que tiene el pen.

Ejercicio 3.

- Como en el ejercicio 1 y partiendo de la imagen forense del 2, buscar con la herramienta Atopsy las evidencias de la amenaza realizada.
- Una vez visto cómo funciona la herramienta, veamos un ejercicio más realista. Supongamos un caso donde una empresa denominada M57.biz tiene como personal actual a Alison Smith (presidente), Jean (CFO), Bob, Carole, David y Emmy (programadores), Gina, Harris (marketing) y Indy (BizDev). Los programadores trabajan normalmente en casa, tienen una sesión de chat diaria y semanalmente una reunión presencial en la oficina. Los de marketing y BizDev trabajan

normalmente fuera (suelen estar de viaje) y tienen una reunión presencial una vez cada dos semanas. La mayoría de los documentos se intercambiar vía correo electrónico.

El caso que nos afecta hace referencia a una exfiltración de datos. Una hoja de cálculo conteniendo información confidencial se ha remitido como adjunto en un foro de “soporte técnico” del sitio web de la competencia. Dicha hoja, cuyo nombre es m57plan.xlsx, proviene del computador del CFO Jean y su contenido es el siguiente:



Name		Position	Salary	SSN (for background check)
Allison	Smith	President	\$140,000	103-44-3134
Jean	Jones	CFO	\$120,000	432-34-6432
Programmers:				
Bob	Blackman	Apps 1	90,000	493-46-3329
Carol	Canfred	Apps 2	110,000	894-33-4560
Dave	Daubert	Q&A	67,000	331-95-1020
Emmy	Arlington	Entry Level	57,000	404-98-4079
Marketing				
Gina	Tangers	Creative 1	80,000	980-97-3311
Harris	Jenkins	G & C	105,000	887-33-5532
BizDev				
Indy	Counterch	Outreach	240,000	123-45-6789
Annual Salaries			\$1,009,000	
Benefits			30%	\$302,700

De las entrevistas con el personal de la empresa se extrajo el siguiente resumen de las declaraciones:

- **Alison (presidente):**

- No sabe de que esta hablando Jean.
- Nunca preguntó a Jean por la hoja de cálculo.
- Nunca recibió la hoja de cálculo por correo electrónico.

- **Jean (CFO):**

- Alison me pidió que preparara la hoja de cálculo como parte de la nueva ronda de financiación.
- Alison me pidió que le enviase la hoja de cálculo a su e-mail.
- Esto es todo lo que se.

Las identidades electrónicas del personal anterior son:

- **Alison (President):** alison@m57.biz ; password: "ab=8989
- **Jean (CFO):** jean@m57.biz ; password: gick*1212

Se pide responder a las cuestiones:

- a) ¿Cuándo se creo la hoja de cálculo?
- b) ¿Cómo llegó de su computador al sitio web de la competencia?
- c) ¿Quién más de la compañía esta involucrado?

Accede a las direcciones downloads.digitalcorpora.org/corpora/drives/nps-2008-m57-jean/nps-2008-jean.E01 y downloads.digitalcorpora.org/corpora/drives/nps-2008-m57-jean/nps-2008-jean.E02 y descarga los correspondientes archivos (nota: no están en Prado por su tamaño) que componen la imagen forense a analizar. Debes copiar esos dos archivos en la misma carpeta, y suministrar a Autopsy el nombre cuya extensión es .E01.

Instalamos autopsy:

```
mati@mati-VirtualBox:~$ sudo apt-get install autopsy
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  libafflib0v5 libcurl4 libdate-manip-perl libtsk13 sleuthkit
Paquetes sugeridos:
  mac-robber
Se instalarán los siguientes paquetes NUEVOS:
  autopsy libafflib0v5 libcurl4 libdate-manip-perl libtsk13 sleuthkit
0 actualizados, 6 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 2.199 kB de archivos.
Se utilizarán 15,6 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] S
Des:1 http://es.archive.ubuntu.com/ubuntu bionic/main amd64 libdate-manip-perl a
11.6-60.1 [5002 kB]
```

```
mati@mati-VirtualBox:~$ sudo apt-get install sleuthkit
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
sleuthkit ya está en su versión más reciente (4.4.2-3).
fijado sleuthkit como instalado manualmente.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
```

```
mati@mati-VirtualBox:~$ sudo autopsy

=====

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

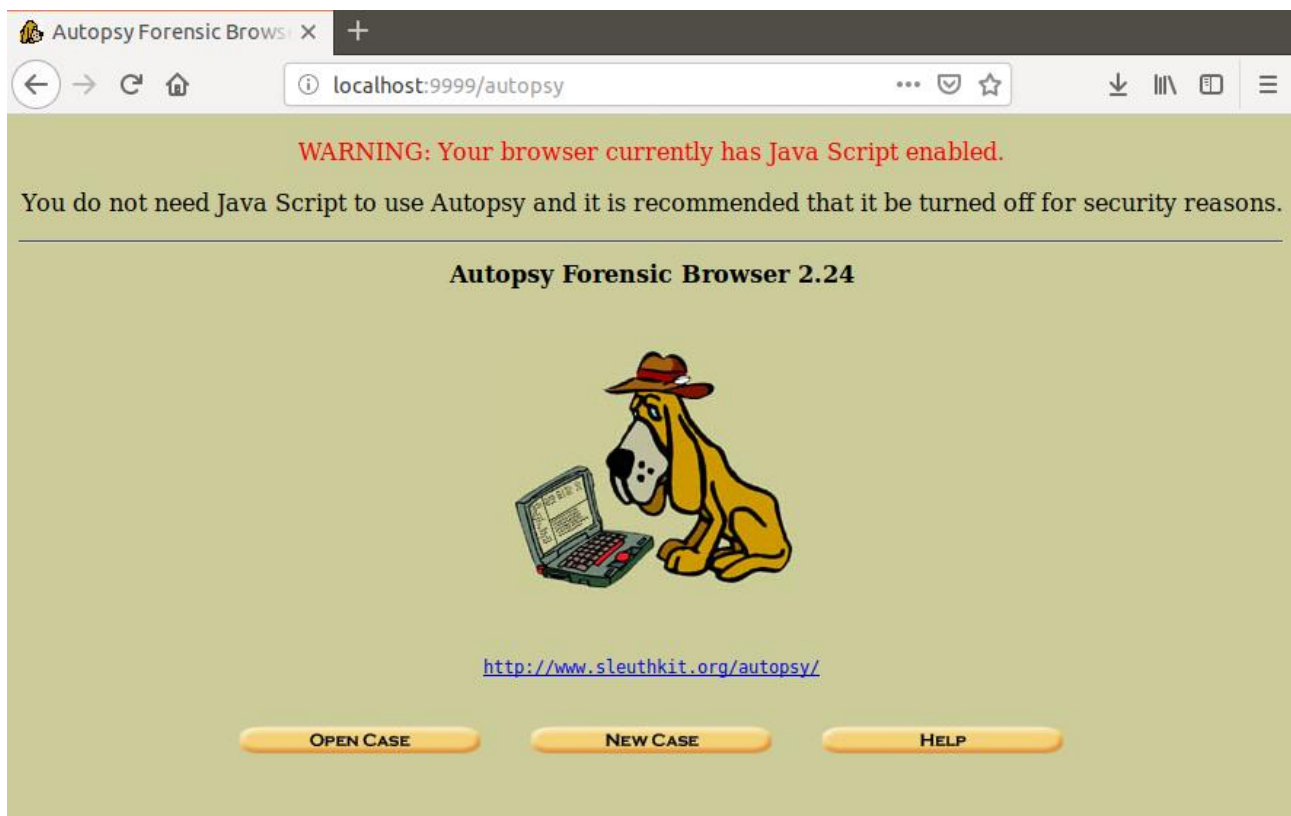
=====

Evidence Locker: /var/lib/autopsy
Start Time: Sun Dec 9 13:40:14 2018
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
```



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="Mati "/>	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"/>

NEW CASE CANCEL HELP

Descargamos los archivos indicados.
Luego añadimos un host. Y las imágenes.

Case: C1
Host: host1

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.

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

← → ↺ 🏠 ⓘ localhost:9999/autopsy?mod=0&view=16&case=C1& ⋮ 🔒 ☆ ⬇

Case: C1
Host: host1

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

CASE GALLERY		HOST GALLERY		HOST MANAGER 🔍	
mount	name	fs type			
<input checked="" type="radio"/> disk	nps-2008-jean.E02-disk	raw			details
<input type="radio"/> disk	nps-2008-jean.E01-disk	raw			details

ANALYZE **ADD IMAGE FILE** **CLOSE HOST**
HELP

FILE ACTIVITY TIME LINES **IMAGE INTEGRITY** **HASH DATABASES**
VIEW NOTES **EVENT SEQUENCER**

Realizamos un análisis de las imágenes. Solo nos deja buscar por keyboard y no logramos encontrar ninguna información.