SEGURIDAD EN SISTEMAS OPERATIVOS

4º Grado en Informática – Complementos de Ing. del Software

Curso 2017-18

Práctica [3]. Auditoría informática e Informática forense

Sesión [1]. Análisis forense en Linux (i)

Autor[1]: Rubén Calvo Villazán

Ejercicio 1.

Mostramos el dispositivo con fdisk -l

```
Device     Boot Start      End  Sectors  Size Id Type
/dev/sdb1  *     2048 15976447 15974400  7.6G  c W95 FAT32 (LBA)
```

Creamos la copia y le damos permisos de solo lectura:

```
root@valkyrie:~# dd if=/dev/sdb of=imagen.disco1 bs=512
15976448+0 records in
15976448+0 records out
8179941376 bytes (8.2 GB, 7.6 GiB) copied, 579.923 s, 14.1 MB/s
```

```
root@valkyrie:~# chmod 444 imagen.disco1
```

Montamos el disco:

```
root@valkyrie:~# mount -t vfat  -o,noexec,loop imagen.disco1 /mnt/analisis
```

Hacemos un sha512sum del archivo, usamos 512 ya que es más seguro.

Previamente teníamos un fichero de texto con el contenido:

“Esto es una amenaza si no nos paga 5000€ lanzaremos un virus, no avise a la policia”

Borramos el fichero.

Buscamos por ejemplo la palabra “virus” sobre el disco, ejecutamos la orden

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 ...”

cat imagen.disco1 | grep virus

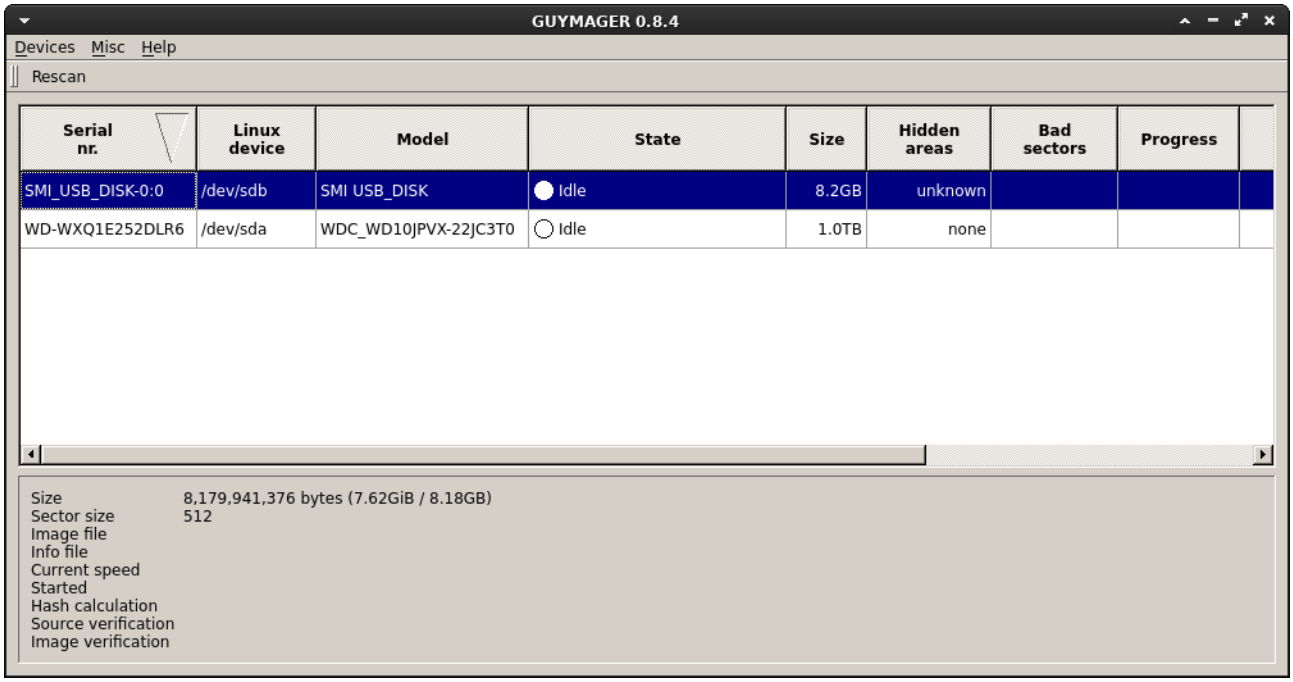
y nos aparece:

~�u�o�sk�Etsin�s��oEUam�ns�a#WPvirusEsto

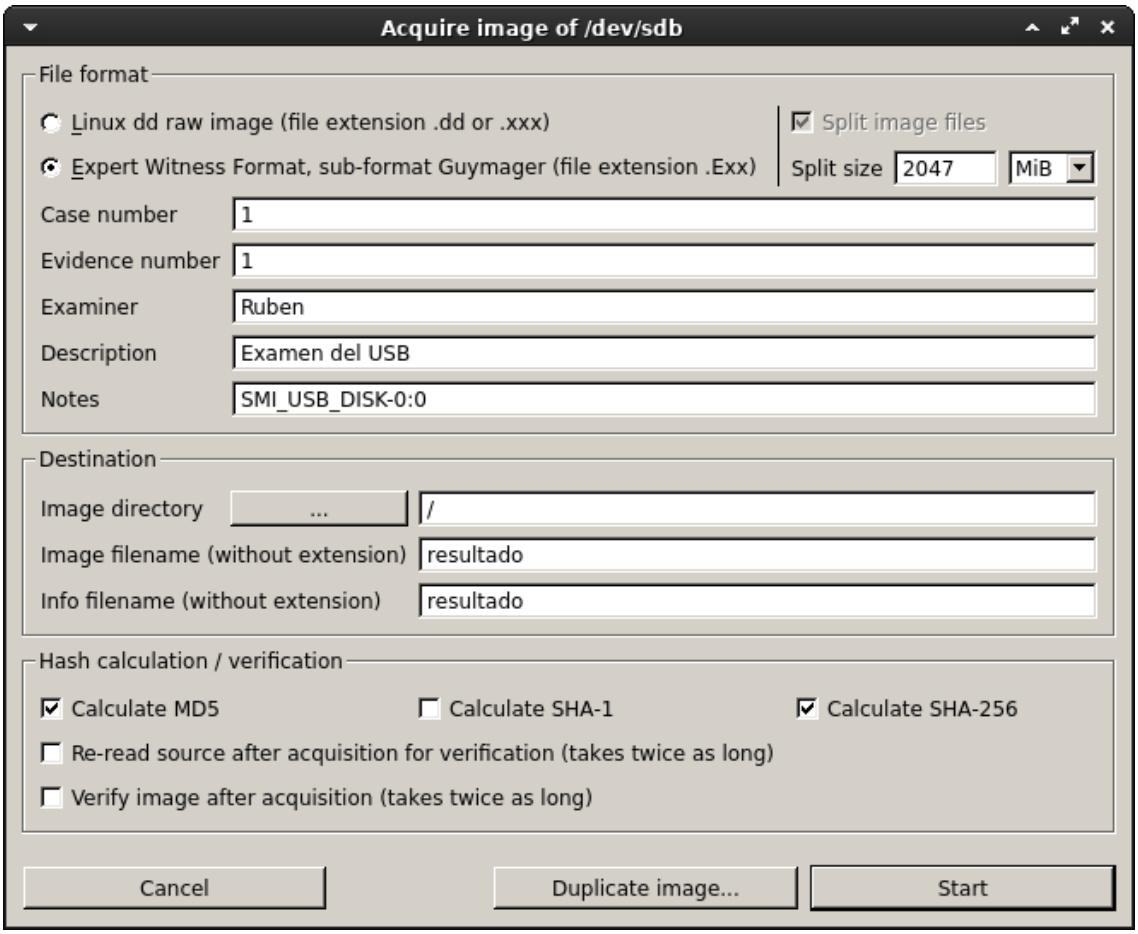
es una amenaza si no nos paga 5000€ lanzaremos un virus,"u�

Ejercicio 2.

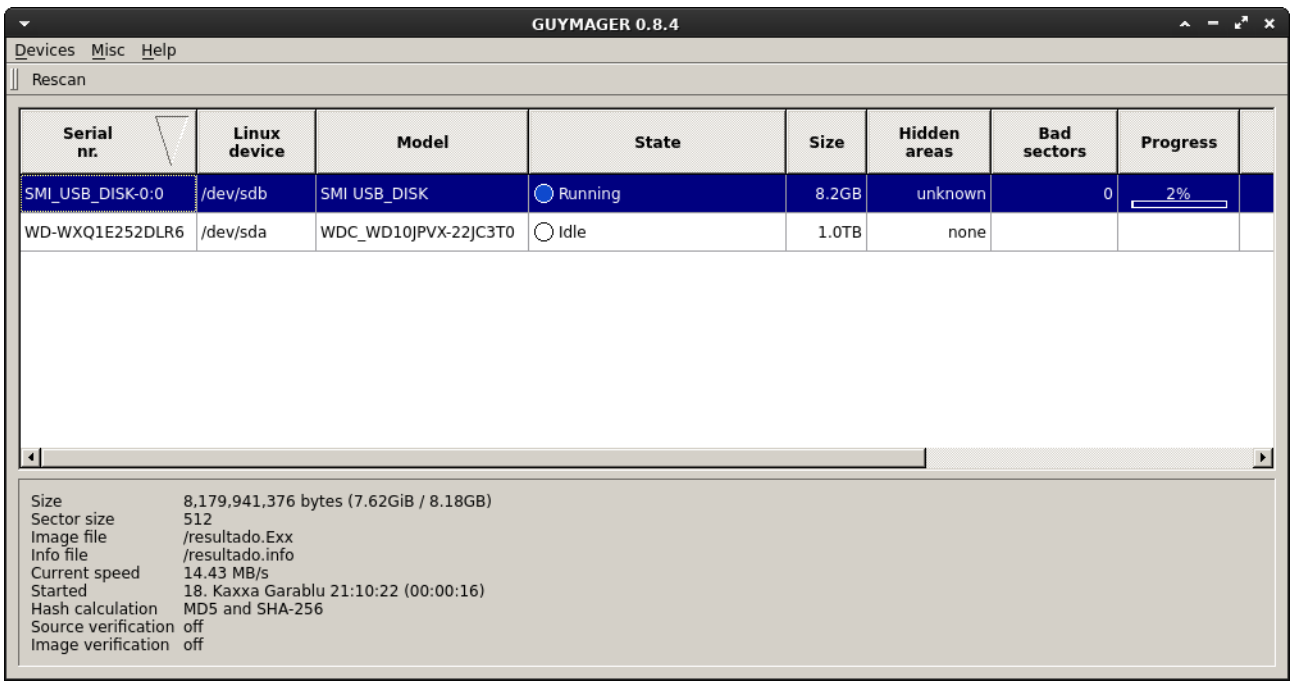
Ejecutamos Guymager:



Seleccionamos el USB y configuramos la creación de su imagen:

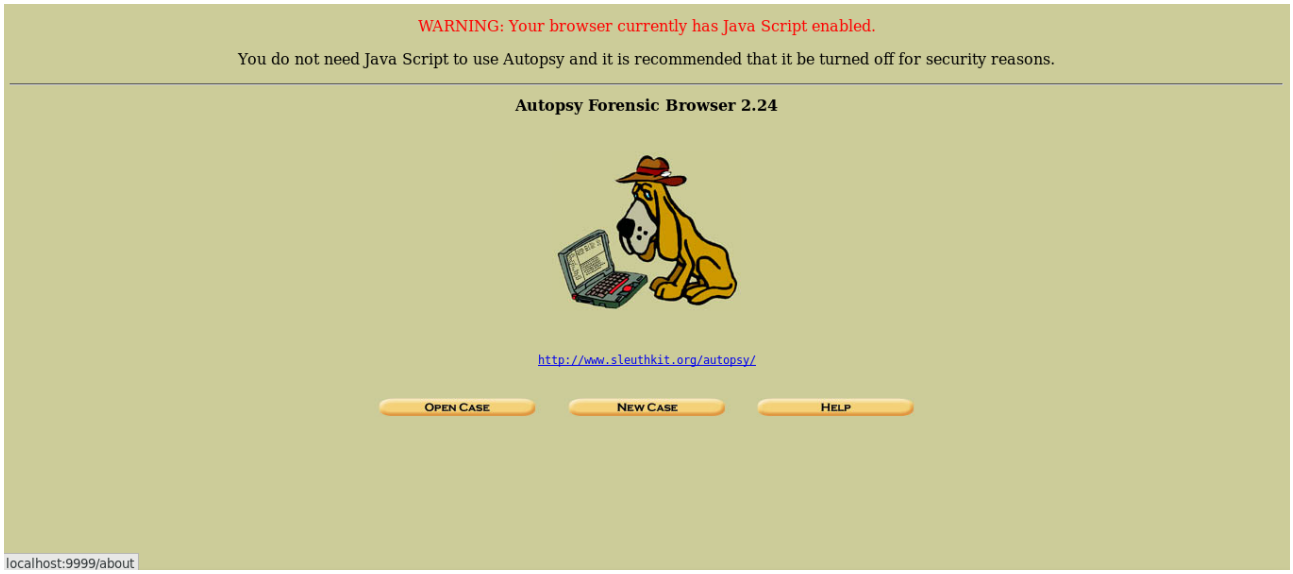


Finalmente le damos a Start y vemos que la creación de la imagen está en proceso, basta esperar a que termine.

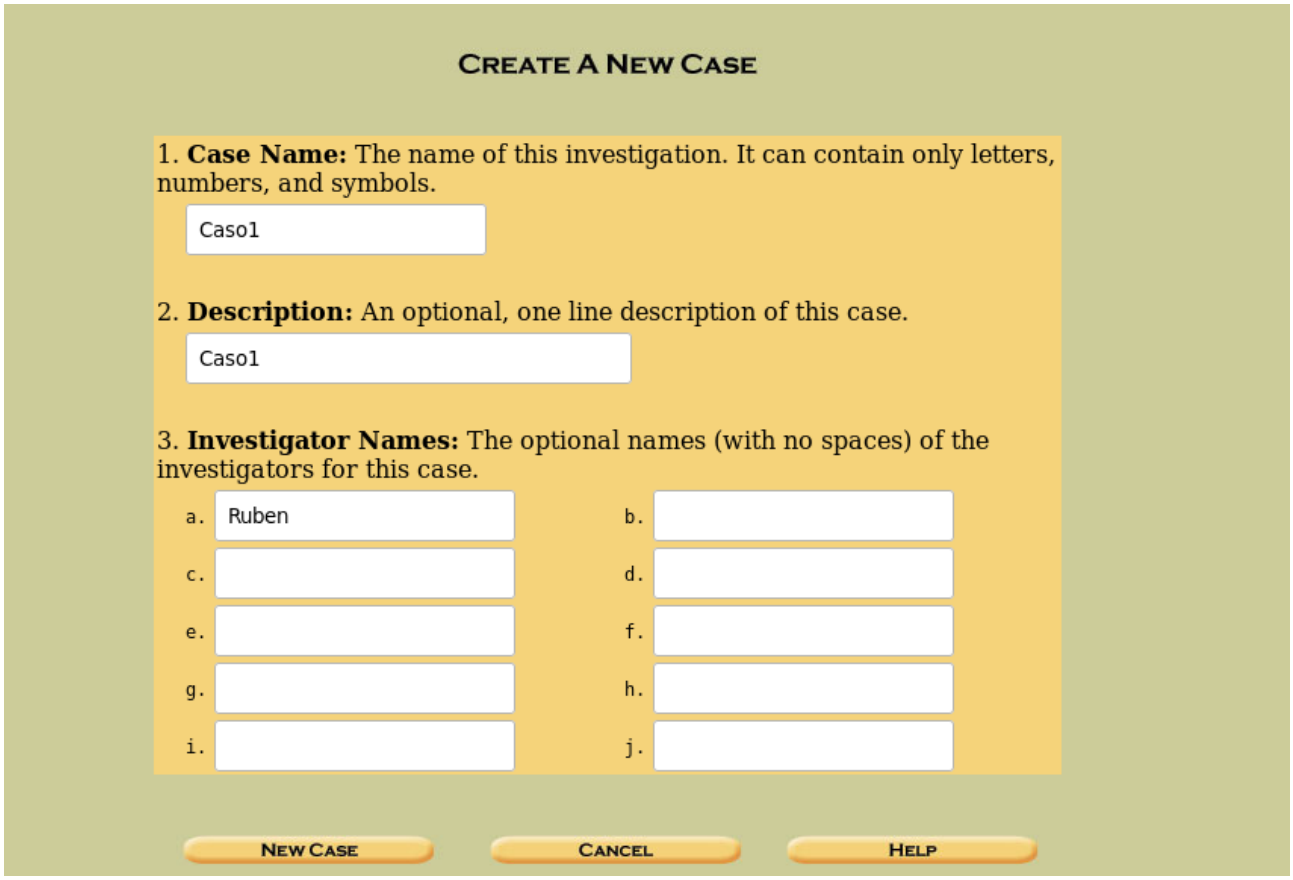


Ejercicio 3.

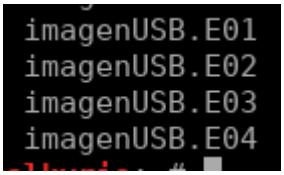
Ejecutamos Autopsy y nos dirigimos a la url indicada: http://localhost:9999/autopsy



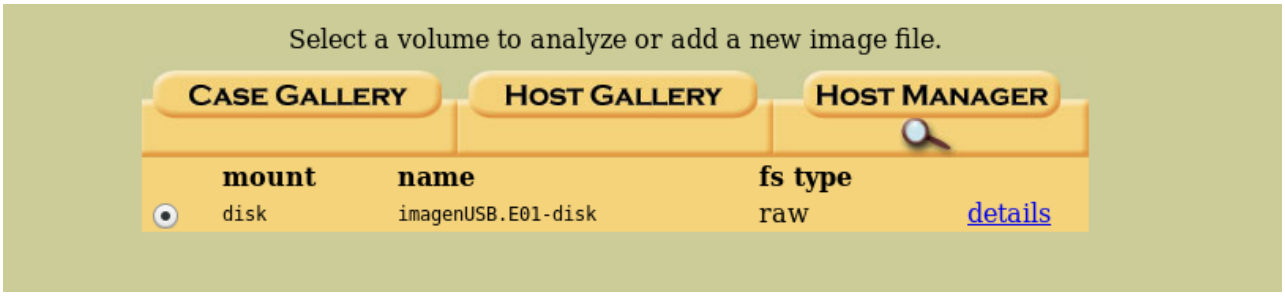
Creamos el caso:



Usamos la imagen creada previamente con Guymager del USB:



La añadimos:



Ejecutamos un análisis de la imagen, el análisis puede ser un 'keyword searh', busca la palabra especificada realizando un grep sobre la imagen.