

# 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<sup>1</sup>: 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:~#
```

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

Montamos el disco:

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

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

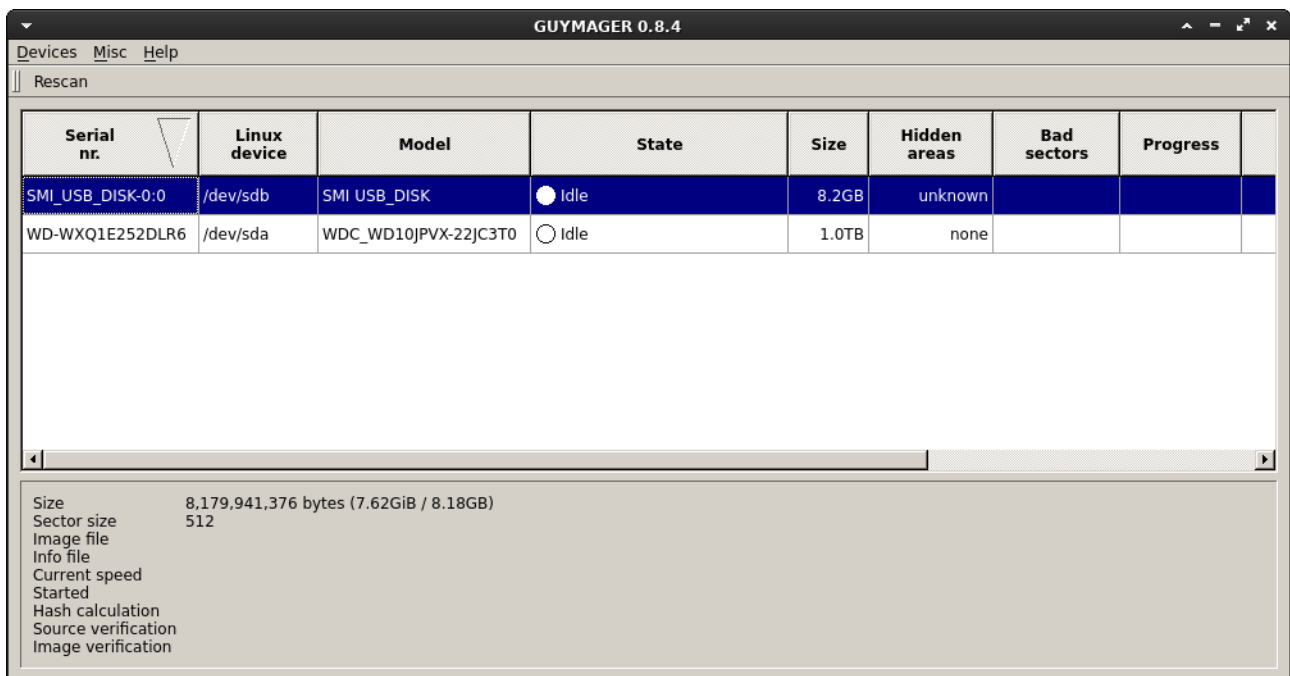
y nos aparece:

~?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:

**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  MiB

Case number   
 Evidence number   
 Examiner   
 Description   
 Notes

---

**Destination**

Image directory    
 Image filename (without extension)   
 Info filename (without extension)

---

**Hash calculation / verification**

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

☐ Re-read source after acquisition (takes twice as long)  
☐ Verify image after acquisition (takes twice as long)

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

**GUYMAGER 0.8.4**

Devices Misc Help

Rescan

Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors	Progress
SMI_USB_DISK-0:0	/dev/sdb	SMI USB_DISK	Running	8.2GB	unknown	0	2%
WD-WXQ1E252DLR6	/dev/sda	WDC_WD10JPVX-22JC3T0	Idle	1.0TB	none		

Size 8,179,941,376 bytes (7.62GiB / 8.18GB)

Sector size 512

Image file /resultado.Exx

Info file /resultado.info

Current speed 14.43 MB/s

Started 18. Kaxxa Garablu 21:10:22 (00:00:16)

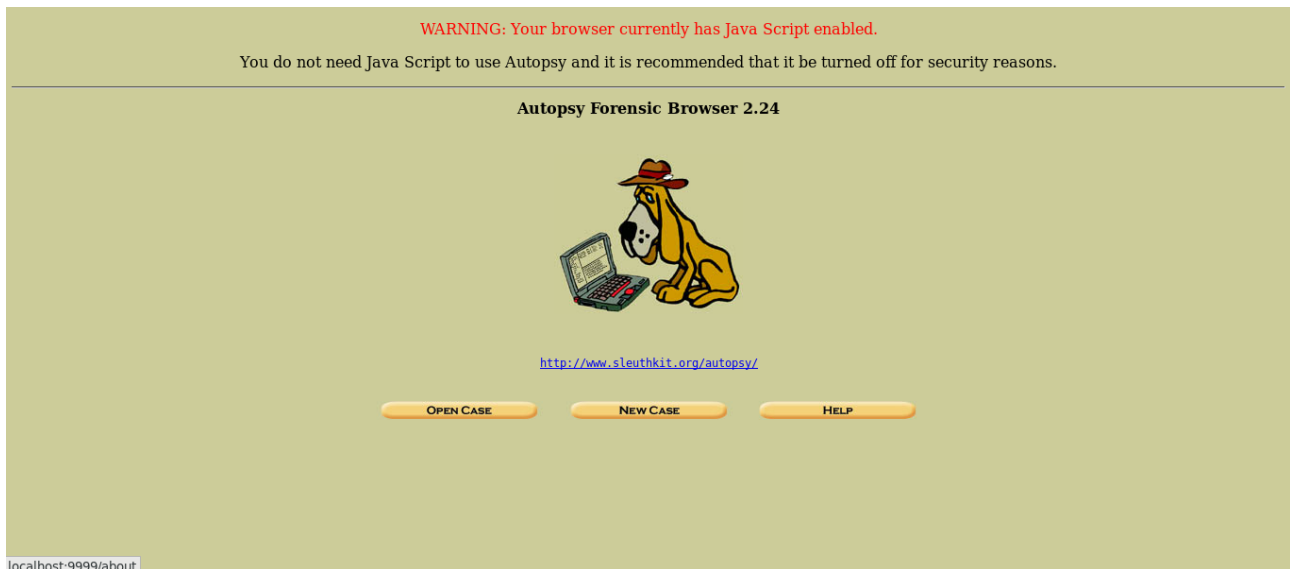
Hash calculation MD5 and SHA-256

Source verification off

Image verification off

### Ejercicio 3.

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



Creamos el caso:

### 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.

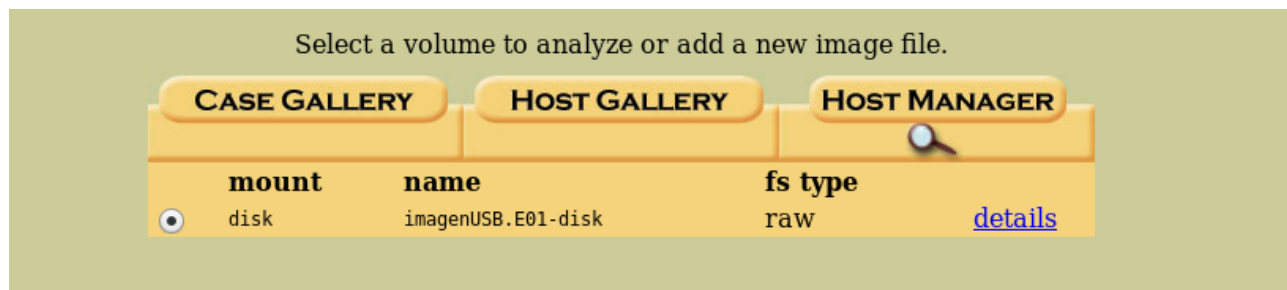
a.	<input type="text" value="Ruben"/>	b.	<input type="text"/>
c.	<input type="text"/>	d.	<input type="text"/>
e.	<input type="text"/>	f.	<input type="text"/>
g.	<input type="text"/>	h.	<input type="text"/>
i.	<input type="text"/>	j.	<input type="text"/>

At the bottom of the form are three yellow buttons: "NEW CASE", "CANCEL", and "HELP".

Usamos la imagen creada previamente con Guymager del USB:

```
imagenUSB.E01
imagenUSB.E02
imagenUSB.E03
imagenUSB.E04
```

La añadimos:



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

### Keyword Search of raw data

Enter the keyword string or expression to search for:

☒ ASCII ☒ Unicode

☐ Case Insensitive ☐ grep Regular Expression

[Regular Expression Cheat Sheet](#)