

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: Víctor García Carrera

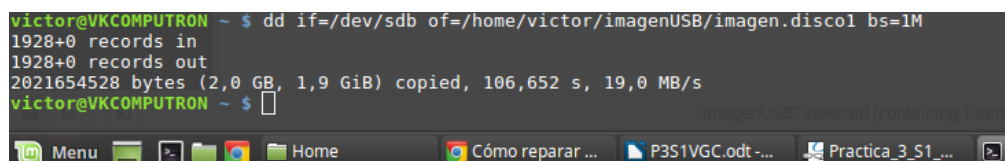
Ejercicio 1.

En este primer ejercicio vamos a simular el caso de un análisis forense sobre un USB en busca de un fichero borrado que simula ser una posible amenaza borrada para evitar que se detectara. Comprobaremos que, mediante diversas técnicas, es posible recuperar el contenido del mismo mediante la búsqueda de texto en espacio disperso o no asignado, pues aunque el estafador “borrara” el archivo, aun puede estar presente en la memoria del USB en bloques de disco no en uso. Creamos en el pendrive el archivo virus.txt que contiene la cadena mostrada a continuación y borramos el archivo.



Primero comenzamos creando una imagen forense del USB. A fin de no modificar ni influir en ningún aspecto sobre el USB original, para realizar en análisis forense creamos una imagen del USB ubicado en `/dev/sdb` mediante el comando:

`dd if=/dev/sdb of=/home/victor/imagenUSB/imagen.disco1 bs=1M`



Por cuestiones de seguridad y prácticas, cambiamos los permisos del mismo para impedir que se ejecute cualquier archivo con el comando `chmod 444 imagen.disco1`

Una vez que disponemos de la imagen del disco, queremos montarla en el directorio creado `/mnt/analisis` para poder ver su contenido. A continuación se muestra este proceso y cómo se encuentra, efectivamente, en la ruta `/mnt/analisis` la imagen del disco que copiamos. Cabe destacar que el montaje de esta imagen supuso algunos

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 ...”

```

victor@VKCOMPUTRON / $ fdisk -l /home/victor/imagenUSB/imagen.discol
Disk /home/victor/imagenUSB/imagen.discol: 1,9 GiB, 2021654528 bytes, 3948544 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xd348c306

Device            Boot Start      End Sectors  Size Id Type
/home/victor/imagenUSB/imagen.discolp1  2048 3948543 3946496   1,9G  c W95 FAT
victor@VKCOMPUTRON / $ sudo mount -t vfat -o,noexec,loop,offset=1048576 /home/victor/imagenUSB/imagen.discol /mnt/analisis
victor@VKCOMPUTRON / $ cd /mnt/analisis/
victor@VKCOMPUTRON /mnt/analisis $ ls
STUFF

```

```
grep -aibf listaBusqueda.txt /home/victor/imagenUSB/imagen.disco1 > aciertos.txt
```

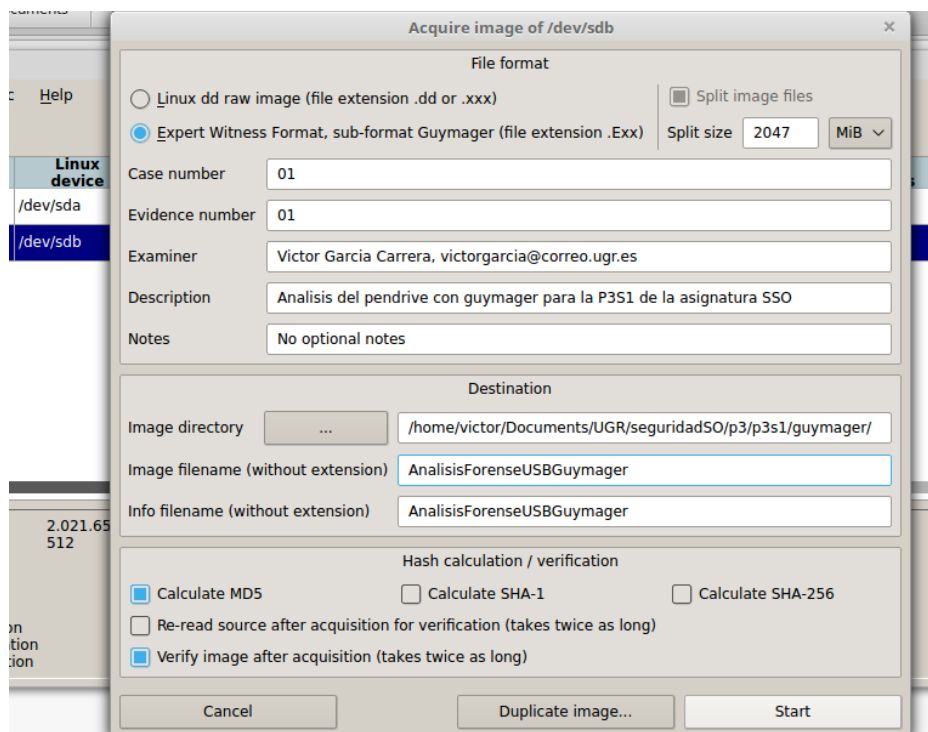
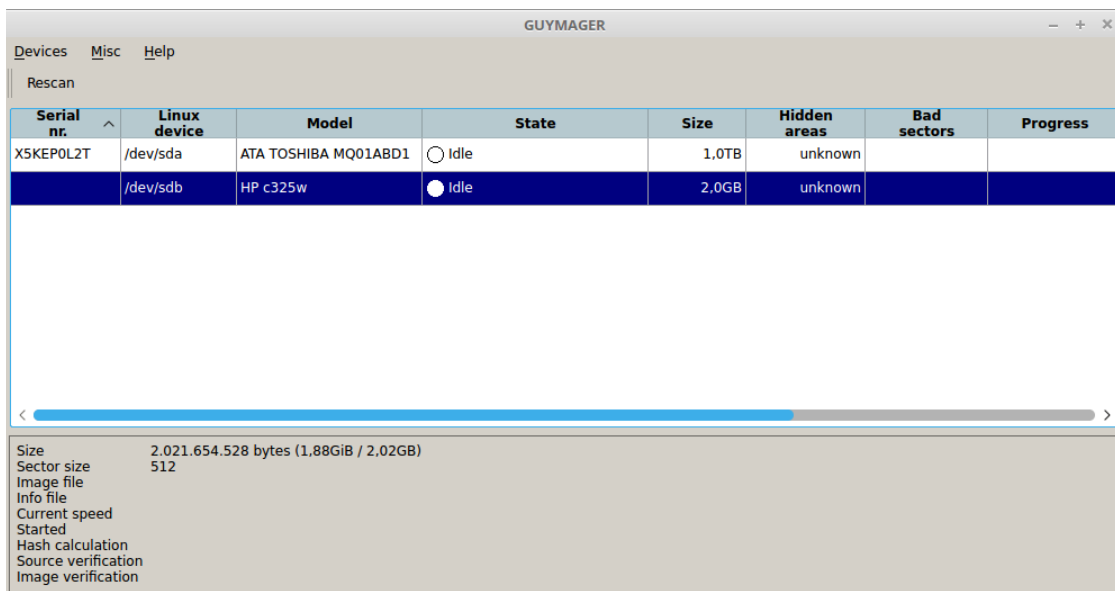
victor@VKCOMPUTRON ~/evidencias

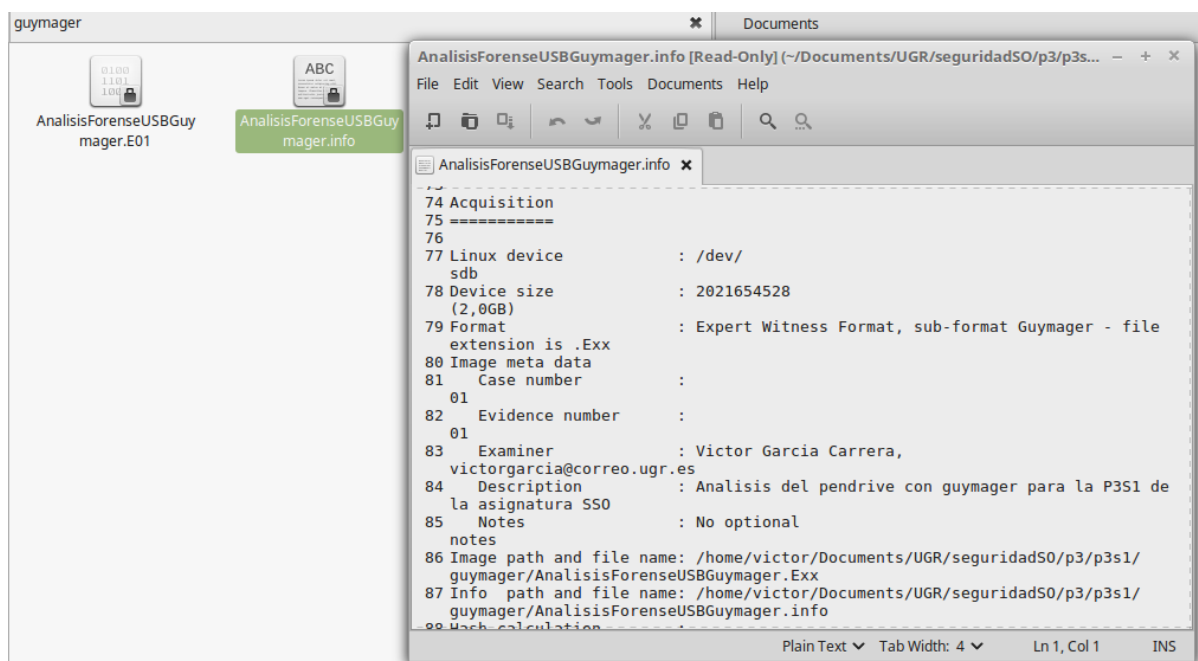
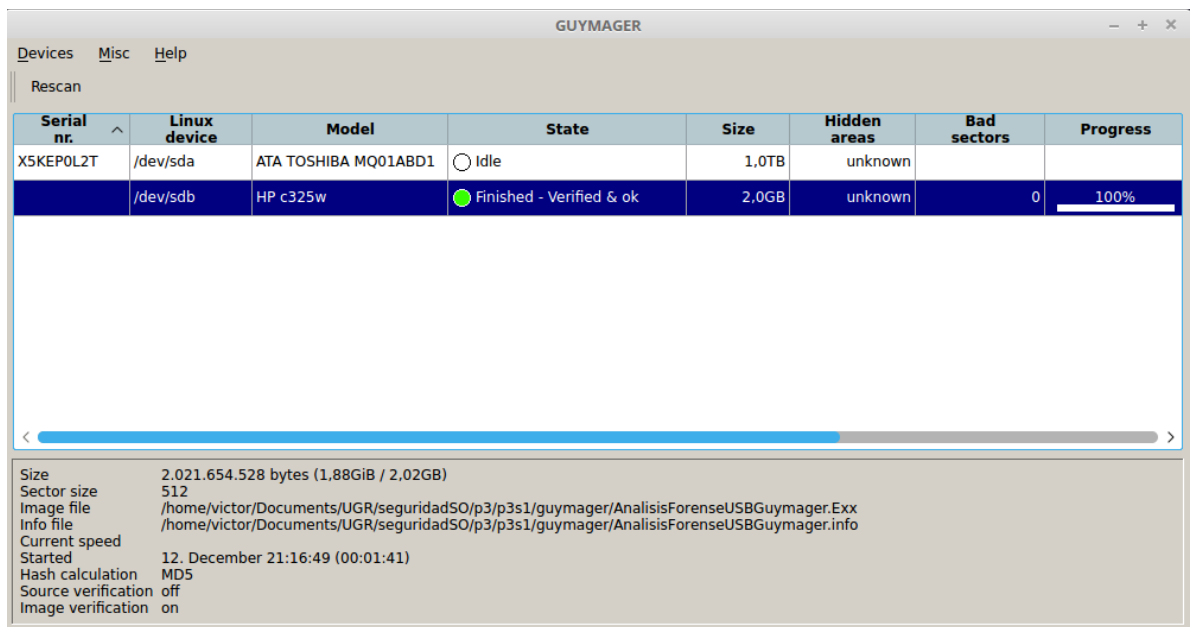
File Edit View Search Terminal Help

```
victor@VKCOMPUTRON ~/evidencias $ grep -aibf listaBusqueda.txt /home/victor/imagenUSB/imagen.disco1 > aciertos.txt
victor@VKCOMPUTRON ~/evidencias $ cat aciertos.txt
0x00000000:4[0]sm0tY0cg0:*000;010n0*[HJ]000F00K00000A0 [0]e[0]00000000! [0]란 01f00pr000000X05-0[0][0]ev[0]07gB00[0][0]00-[0]_0[0]
7E 0n00o [0][0]
0/[0]0HA00H`0Se trata de una amenaza que nunca será descubierta al borrar este archivo, o quizás...
victor@VKCOMPUTRON ~/evidencias $
```

Ejercicio 2.

En este ejercicio utilizamos la herramienta *guymager*, disponible mediante el comando `sudo apt install guymager`, para crear una imagen forense del pendrive utilizado en el ejercicio anterior. A continuación se muestra el proceso seguido.





Ejercicio 3.

En este último ejercicio vamos a trabajar con la herramienta Autopsy. Siguiendo los pasos indicados en el documento de la práctica descargamos la herramienta y nos da la dirección que introducir en el. Una vez dentro, creamos un nuevo caso con la imagen forense del anterior ejercicio y buscamos evidencias por la palabra clave *amenaza* con el fin de encontrar con Autopsy la misma.

Add A New Host To PENDRIVE - Mozilla Firefox

localhost:9999/autopsy?mod=0&view=7&case=PENDRIVE&inv=victor&x=137&y=13

Case: PENDRIVE

ADD A NEW HOST

- Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.
- Description:** An optional one-line description or note about this computer.
- 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.
- 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.
- Path of Alert Hash Database:** An optional hash database of known bad files.
- Path of Ignore Hash Database:** An optional hash database of known good files.

Add Image To PENDRIVE:host1 - Mozilla Firefox

localhost:9999/autopsy?mod=0&view=13&host=host1&case=PENDRIVE&inv=victor&x=91&y=9

Case: PENDRIVE
Host: host1

ADD A NEW IMAGE

- 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.
- Type**
Please select if this image file is for a disk or a single partition.
☒ Disk ☐ Partition
- 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

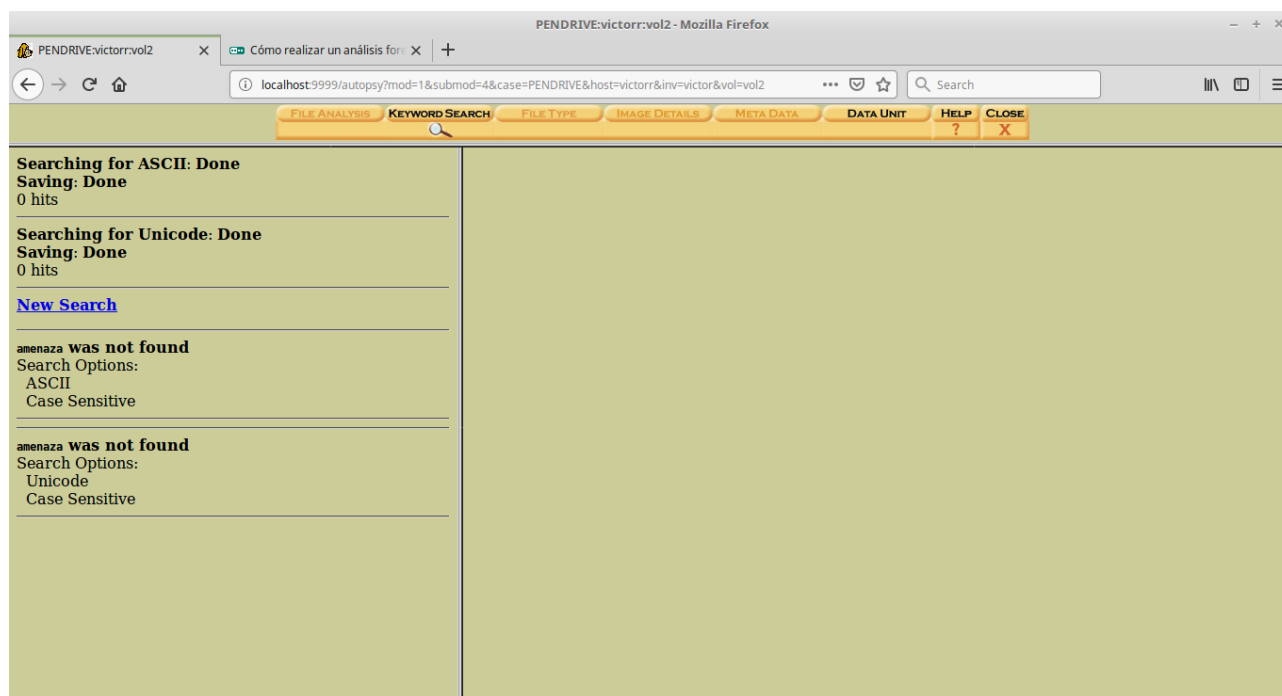
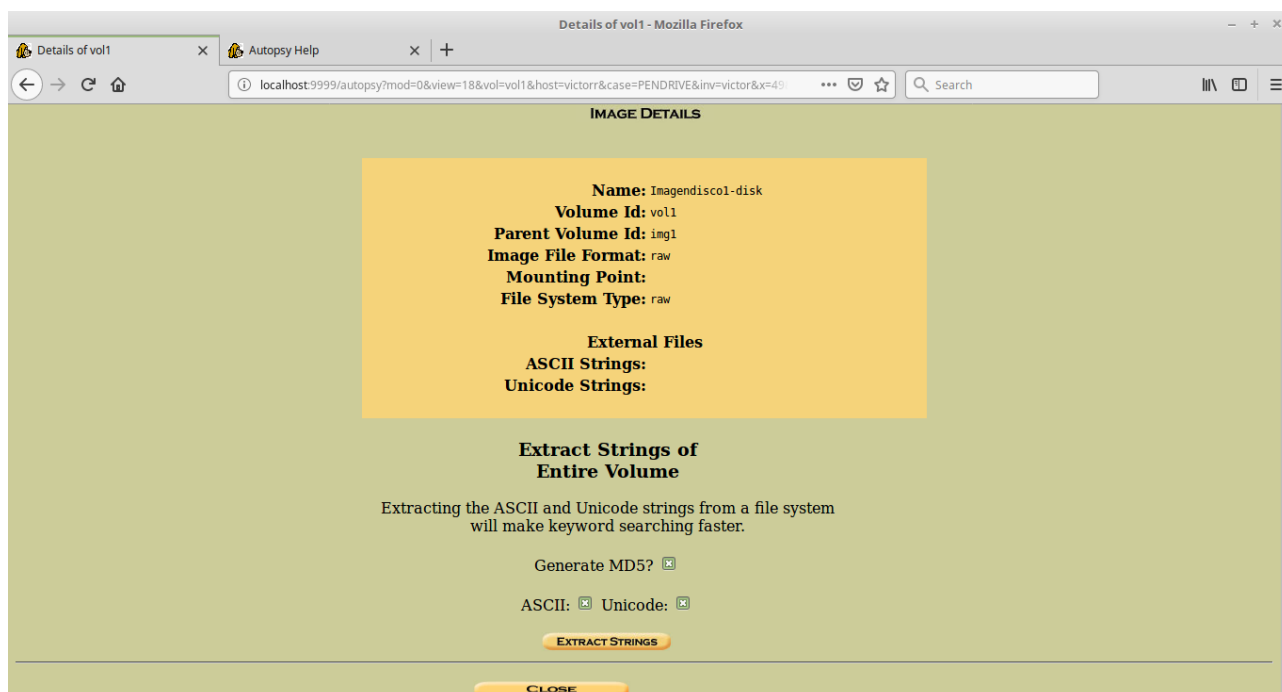
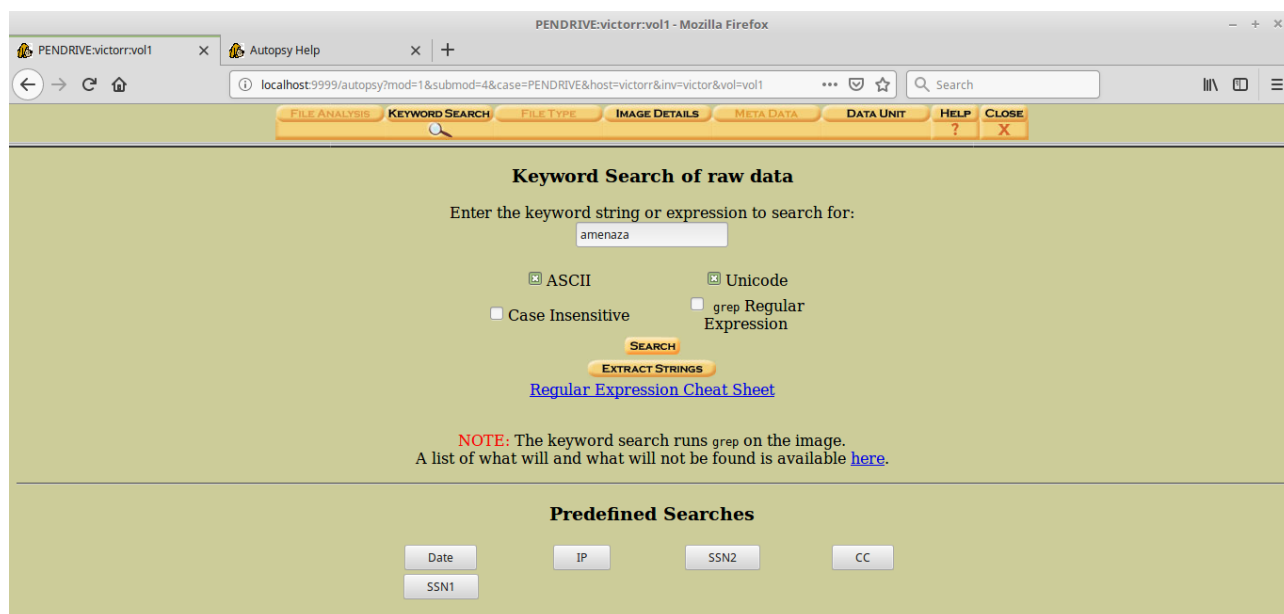
Add a new image to an Autopsy Case - Mozilla Firefox

localhost:9999/autopsy?mod=0&view=15&img_path=%2Fhome%2Fvictor%2FimagenUSB%2Fimagen

Testing partitions
Linking image(s) into evidence locker
Image file added with ID img1
Disk image (type dos) added with ID vol1
Volume image (2048 to 3948543 - raw - /1/) added with ID vol2

OK ADD IMAGE

Desgraciadamete, no obtenemos resultados.



Para simular un caso más realista, utilizamos dos imágenes forenses descargadas de un caso real en el que se produjo una filtración de documentos corporativos desde un ordenador de un alto ejecutivo de la empresa M57 y se publicaron en un foro del sitio web de la competencia. Utilizando Autopsy, debemos obtener información a partir de su análisis.