SEGURIDAD EN SISTEMAS OPERATIVOS

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

Curso 2019-20

Práctica [3]. Auditoría informática e informática forense.

Sesión [1]. Análisis forense en Linux.

Autor[1]: Nazaret Román Guerrero

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*.

Para comenzar, suponemos (de hecho, lo he hecho manualmente) que el *pendrive* ha sido formateado y está vacío y limpio, con la única partición que tiene llena de 0. Este paso lo he llevado a cabo con la herramienta gráfica de "`Disk`".

Tras esto, creamos un archivo dentro del *pendrive* con una amenaza, que estará en `archivo.txt`.

```
nazaret@nazaret-GE63-7RD:/media/nazaret/usb$ echo "Paga 1000 euros si no quieres
 que un virus te infecte el sistema" > archivo.txt
```

Comprobamos que en efecto el archivo se ha creado y procedemos a borrarlo.

```
nazaret@nazaret-GE63-7RD:/media/nazaret/usb$ ls
archivo.txt
nazaret@nazaret-GE63-7RD:/media/nazaret/usb$ rm archivo.txt
nazaret@nazaret-GE63-7RD:/media/nazaret/usb$ ls
nazaret@nazaret-GE63-7RD:/media/nazaret/usb$
```

Vamos a comenzar creando la imagen forense. Primero, guardamos la información mostrada por `fdisk -l` sobre el *pendrive*, por si nos es necesaria posteriormente.

---

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 ..."

```
Disco /dev/sdc: 961 MiB, 1007681536 bytes, 1968128 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: 0x6236d543

Dispositivo Inicio Comienzo   Final Sectores Tamaño Id Tipo
/dev/sdc1              2048 1968127  1966080   960M  c W95 FAT32 (LBA)
nazaret@nazaret-GE63-7RD:~$
```

Ahora, creamos una imagen del *pendrive* con la herramienta `dd`. Tras esto, para asegurarnos de que no escribimos nada, cambiamos los permisos a solo lectura.

```
nazaret@nazaret-GE63-7RD:~$ sudo dd if=/dev/sdc of=Escritorio/ETSIIT_comp/4º/Cuatri\ 1/SSO/Practic
as/P3/Sesión\ 1/imagen.usb bs=512
1968128+0 registros leídos
1968128+0 registros escritos
1007681536 bytes (1,0 GB, 961 MiB) copied, 10,8988 s, 92,5 MB/s
nazaret@nazaret-GE63-7RD:~$ sudo chmod 444 Escritorio/ETSIIT_comp/4º/Cuatri\ 1/SSO/Practicas/P3/Se
sión\ 1/imagen.usb
nazaret@nazaret-GE63-7RD:~$
```

Antes de seguir avanzando y montar el sistema para comprobar lo que contenía, vamos a hacer una copia de seguridad que guardaremos en otro *pendrive*:

```
nazaret@nazaret-GE63-7RD:~$ sudo dd if=Escritorio/ETSIIT_comp/4º/Cuatri\ 1/SSO/Practicas/P3/Sesión
\ 1/imagen.usb of=/dev/sdd1
1968128+0 registros leídos
1968128+0 registros escritos
1007681536 bytes (1,0 GB, 961 MiB) copied, 3,049 s, 330 MB/s
nazaret@nazaret-GE63-7RD:~$
```

Ahora sí, es el momento de montar la imagen restaurada. Para ello, vamos a crear un directorio, que llamaremos analisis, donde se montará la imagen.

```
root@nazaret-GE63-7RD:/home/nazaret# mkdir Escritorio/ETSIIT_comp/4º/Cuatri\ 1/SSO/Practicas/P3/Se
sión\ 1/analisis/
root@nazaret-GE63-7RD:/home/nazaret# mount -t vfat -ro,noexec /dev/sdc1 Escritorio/ETSIIT_comp/4º/
Cuatri\ 1/SSO/Practicas/P3/Sesión\ 1/analisis
root@nazaret-GE63-7RD:/home/nazaret#
```

Creamos los `HASH` para el disco y los archivos, tal y como se muestra en la imagen:

```
root@nazaret-GE63-7RD:/home/nazaret/Escritorio/ETSIIT_comp/4º/Cuatri 1/SSO/Practicas/P3/Sesión 1/anal
is# mkdir ../evidencias
root@nazaret-GE63-7RD:/home/nazaret/Escritorio/ETSIIT_comp/4º/Cuatri 1/SSO/Practicas/P3/Sesión 1/anal
is# find . -type f -exec sha1sum {} \; > ../evidencias/SHA.listaArchivos
root@nazaret-GE63-7RD:/home/nazaret/Escritorio/ETSIIT_comp/4º/Cuatri 1/SSO/Practicas/P3/Sesión 1/anal
is#
```

Guardamos la lista de los archivos presentes en el *pendrive* como método de asegurarnos de que todo lo que hay no es escrito por nosotros.

```
root@nazaret-GE63-7RD:/home/nazaret/Escritorio/ETSIIT_comp/4º/Cuatri 1/SSO/Practicas/P3/Sesión 1/anal
is# ls -laiRtu > ../evidencias/lista.archivos
root@nazaret-GE63-7RD:/home/nazaret/Escritorio/ETSIIT_comp/4º/Cuatri 1/SSO/Practicas/P3/Sesión 1/anal
is# cat ../evidencias/lista.archivos
.:
total 8
19662136 drwxr-xr-x 4 nazaret nazaret 4096 dic  4 22:59 ..
       1 drwxr-xr-x 2 root    root    4096 ene  1  1970 .
root@nazaret-GE63-7RD:/home/nazaret/Escritorio/ETSIIT_comp/4º/Cuatri 1/SSO/Practicas/P3/Sesión 1/anal
is#
```

No obstante, como podemos comprobar, no hay ningún archivo. Así que debemos buscar en los bloques del disco no asignados, ya que estamos buscando un archivo eliminado. Así que lo primero es crear una lista de palabras a buscar:

```
root@nazaret-GE63-7RD:/home/nazaret/Escritorio/ETSIIT_comp/4º/Cuatri 1/SSO/Practicas/P3/Sesión 1/anal
is# cat ../evidencias/lista_busqueda.txt
virus
infecte
root@nazaret-GE63-7RD:/home/nazaret/Escritorio/ETSIIT_comp/4º/Cuatri 1/SSO/Practicas/P3/Sesión 1/anal
is#
```

En nuestro caso, vamos a buscar dos palabras: virus e infecte. Cada palabra debe estar en una línea. Una vez hecho esto, buscamos el archivo que ha sido borrado. Como podemos comprobar, en el archivo de `aciertos.txt` ha introducido las líneas que contienen las palabras que buscábamos:

```
root@nazaret-GE63-7RD:/home/nazaret/Escritorio/ETSIIT_comp/4º/Cuatri 1/SSO/Practicas/P3/Sesión 1/anal
is# grep -aibf ../evidencias/lista_busqueda.txt ../imagen.usb > ../evidencias/aciertos.txt
root@nazaret-GE63-7RD:/home/nazaret/Escritorio/ETSIIT_comp/4º/Cuatri 1/SSO/Practicas/P3/Sesión 1/anal
is# cat ../evidencias/aciertos.txt
3291:U◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆archi◆vo.txt◆◆◆RCHIVO TXT '[illegible]O◆O[illegible]O[illegible]Paga 1000 euros si no quieres que un v
irus te infecte el sistema
root@nazaret-GE63-7RD:/home/nazaret/Escritorio/ETSIIT_comp/4º/Cuatri 1/SSO/Practicas/P3/Sesión 1/anal
is#
```

Por tanto, había un archivo eliminado que hemos conseguido encontrar para recuperar la información sobre la amenaza.

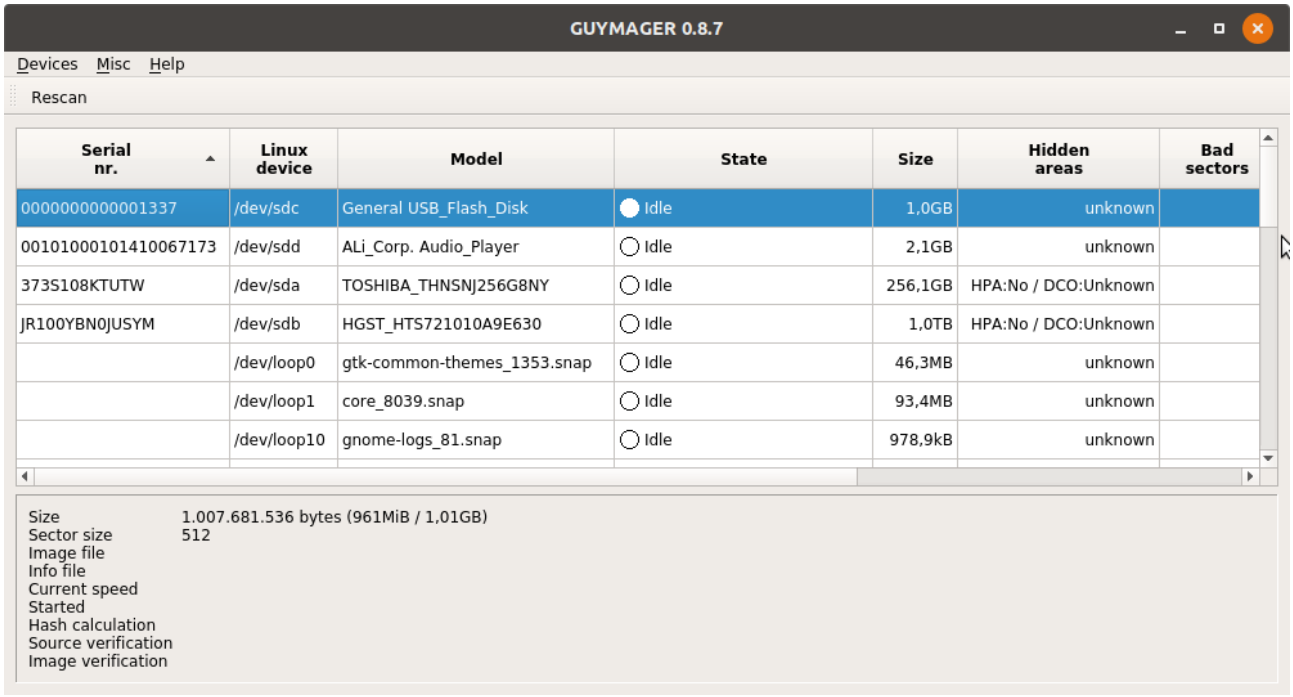
Ejercicio 2.

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

Lo primero es instalar la herramienta. Una vez instalada, la abrimos.

Aparecerá una lista con todos los dispositivos que hay montados en el sistema, así que tendremos que buscar el *pendrive*.

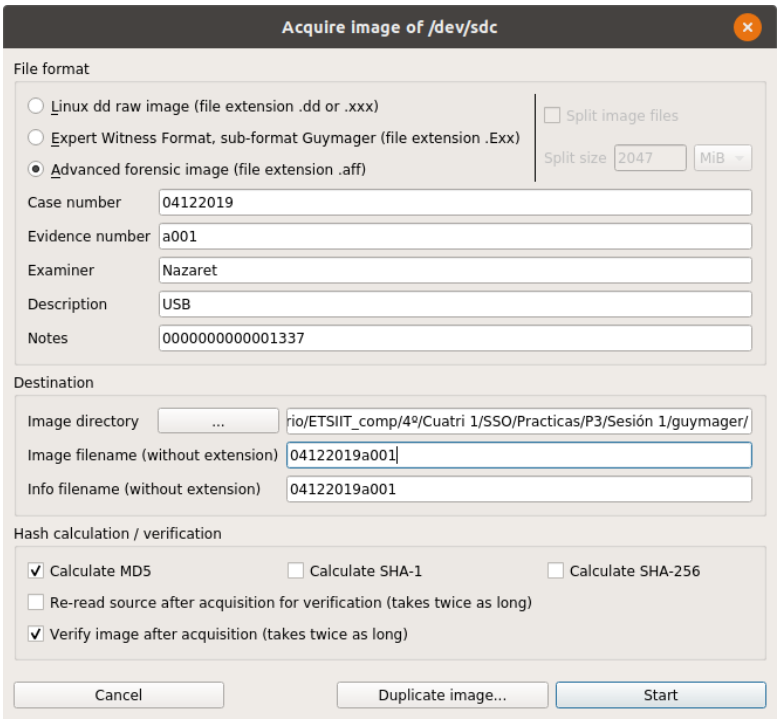
Para crear una imagen del *pendrive*, seleccionamos el dispositivo, en nuestro caso `/dev/sdc`, que se corresponde con el primer dispositivo montado de la lista.



Tras esto, pulsando click derecho sobre él, seleccionamos la opción de `acquire image`, y nos saldrá una ventana que tendremos que rellenar. Previamente, si queremos crear una imagen en formato `AFF`, será necesario modificar el archivo `/etc/guymager/guymager.cfg` y habilitar la opción `AffEnabled`:

```
EwfFormat                = Guymager
EwfCompression           = FAST
EwfCompressionThreshold  = 0.999
EwfNaming                = FTK
AffEnabled               = true
AffCompression           = 1
AffMarkBadSectors        = TRUE
```

Si ya lo tenemos a true, creamos una imagen tal y como se muestra en la imagen:



Mientras se hace la copia, podemos ver que en la ventana principal de la herramienta se muestra la palabra `running`:

Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors
0000000000001337	/dev/sdc	General USB_Flash_Disk	Running	1,0GB	unknown	
0010100010141006717 3	/dev/sdd	ALi Corp. Audio Player	Idle	2,1GB	unknown	

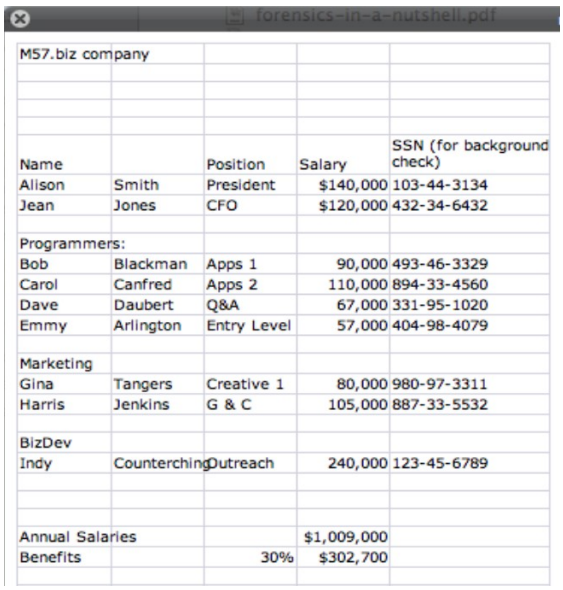
Cuando ha finalizado, se verifica automáticamente:

Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors
0000000000001337	/dev/sdc	General USB_Flash_Disk	Finished - Verified & ok	1,0GB	unknown	
0010100010141006717 3	/dev/sdd	ALi Corp. Audio Player	Idle	2,1GB	unknown	

Ejercicio 3.

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

b) Una vez visto como 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 intercambian 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 sito web de la competencia. Dicha hoja, cuyo nombre es `m57plan.xlsx`, proviene del computador del CFO Jean y su contenido es el siguiente:



forensics-in-a-nutshell.pdf

M57.biz company				
Name		Position	Salary	SSN (for background check)
Alison	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	Counterching	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 qué está 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 sé.

Las identidades electrónicas del personal anterior son:

- Alison (presidente): 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?

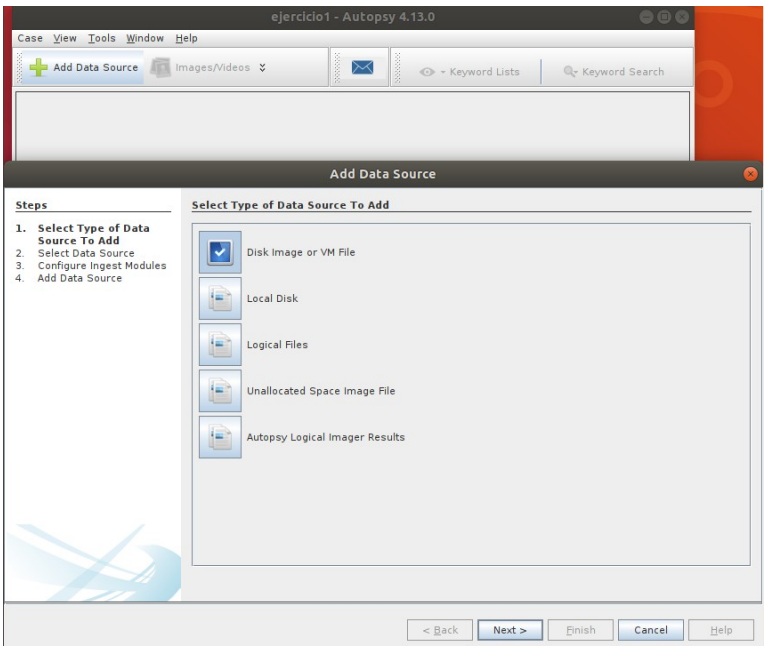
c) ¿Quién más de la compañía esta involucrado?

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`.

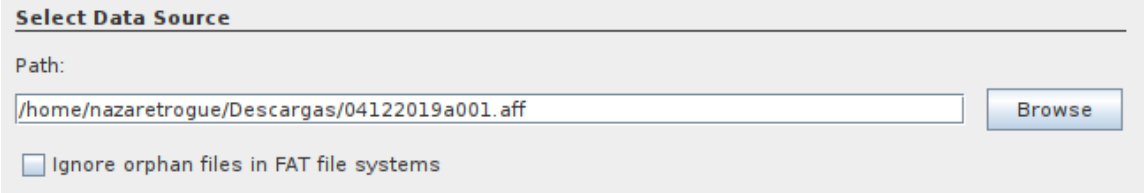
a) Vamos a instalar primero `sleuthkit` y `Autopsy`. Tras descargar los ficheros necesarios, empezamos por `sleuthkit`. Para ello, descomprimimos el `zip`, configuramos la herramienta usando `./configure` y lo compilamos con `make` y `make install`.

Ahora instalamos `Autopsy`. De nuevo, descomprimimos el `zip`, configuramos con `./configure` e iniciamos la herramienta con `./bin/autopsy`.

Una vez la iniciamos, creamos un nuevo caso, que nos pedirá el nombre del caso, el directorio donde almacenarlo y el nombre de la persona que va a llevar a cabo el análisis. Seleccionamos la imagen del disco que vamos a analizar.



En nuestro caso, buscamos la imagen creada con `guymager`:

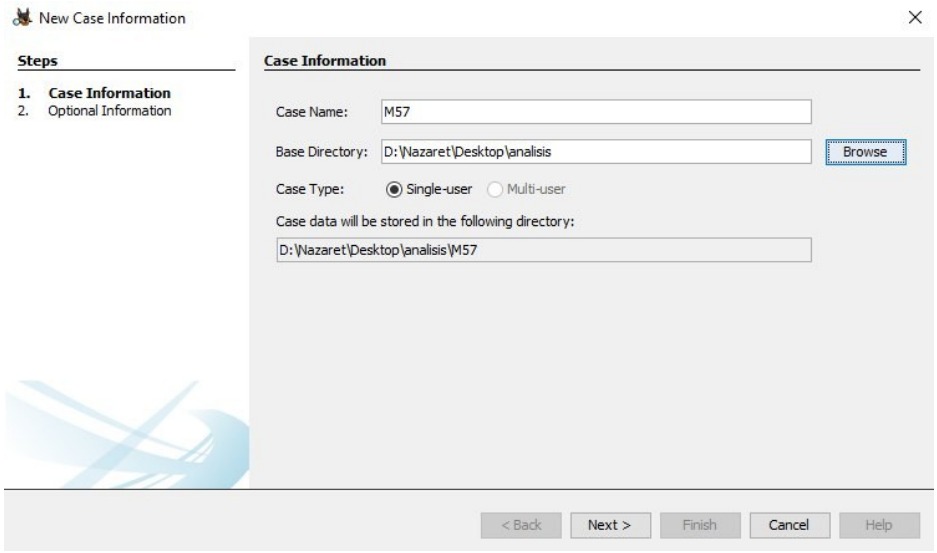


A partir de este momento, he sido incapaz de continuar el ejercicio, puesto que no ha habido manera de que `Autopsy` leyera correctamente la imagen. No aceptaba los formatos en los que estaba la imagen, a pesar de que he probado a crear la imagen 3 veces desde `guymager` con 3 formatos distintos: `.000`, `.ewf` y `.aff`. No sé si la imagen estaba mal, pero en el ejercicio anterior pude encontrar el archivo borrado, así que he supuesto que el fallo era del propio `Autopsy`, puesto que tampoco funcionaba este disco en `Windows`.

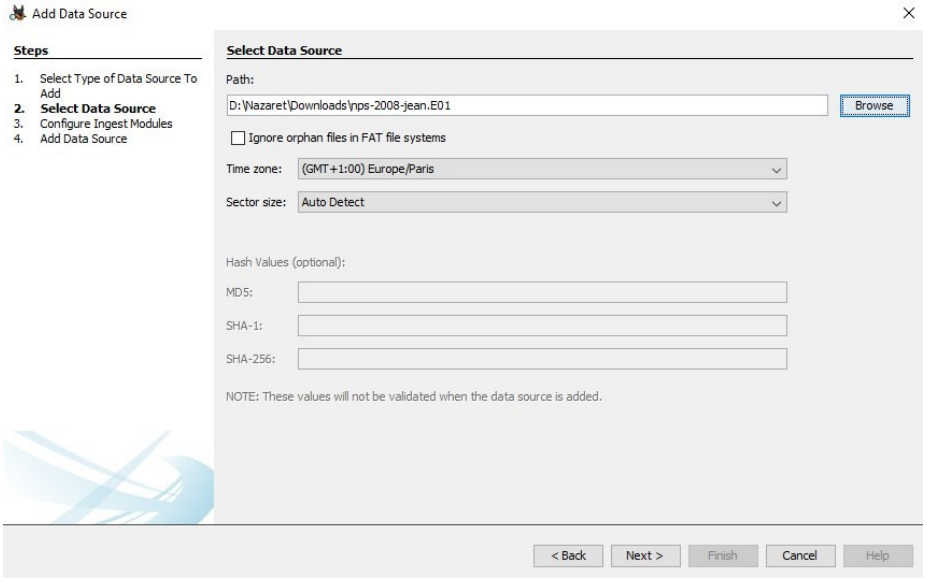
Así que he decidido dejar este apartado a medias, aunque lo he intentado, no ha funcionado.

b) En este ejercicio vamos a utilizar mi host con `Windows` en lugar de con `Ubuntu`, que es el que he utilizado en los dos ejercicios anteriores. Lo primero es descargase los discos de Jean de 1.5GB y 1.4GB respectivamente.

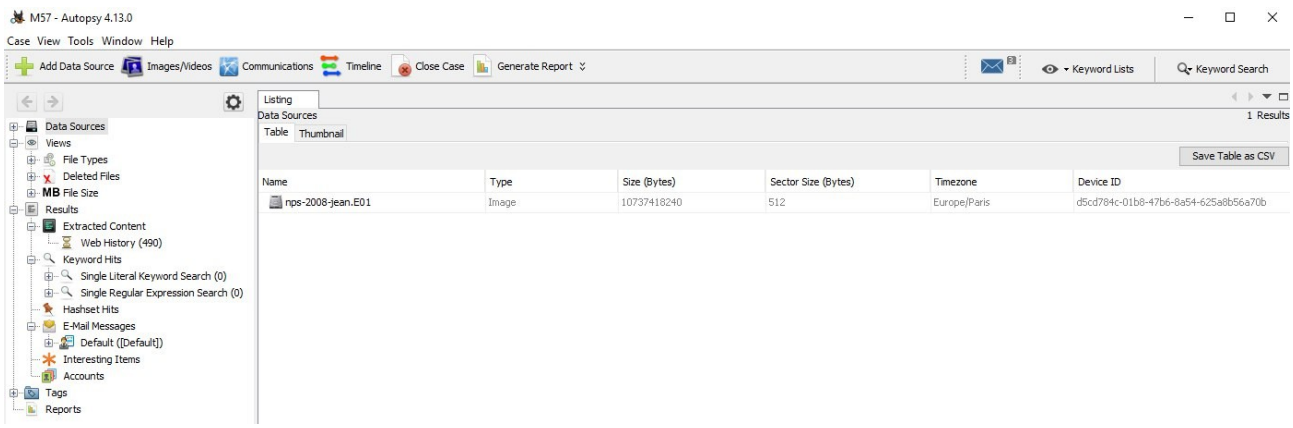
Una vez que los tenemos, abrimos `Autopsy` y creamos un nuevo caso.



Una vez creado el caso, seleccionamos el disco que queremos analizar:



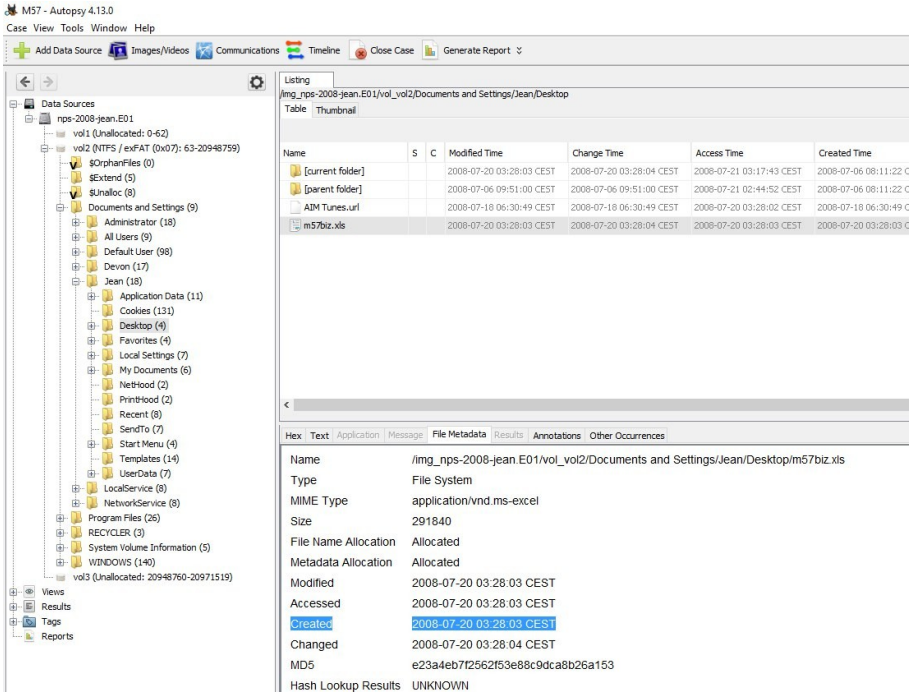
Tras añadir dicho disco al caso, se mostrará en pantalla el dispositivo y un árbol con las distintas carpetas y archivos para navegar a través de ellas:



Vamos a buscar el archivo. Para ello, entramos en el dispositivo marcado y navegamos para

encontrar los archivos de Jean. Encontramos el archivo de excel que buscábamos `m57biz.xls` en `vol2\Documents and Settings\Jean\Desktop`.

Pulsando sobre el archivo, podemos ver los metadatos y saber que fue creado el 20 de julio de 2008 a las 03:28:03 de la madrugada.



El archivo fue filtrado por correo electrónico según nos indica Jean, que dice que envió dicho archivo a Alison a través de un e-mail. Como podemos ver hay varios e-mails entre Alison y Jean cercanos a la fecha en la que se creo el archivo, es decir, que se intercambiaron varios correos entre ambos y posteriormente se creo el archivo, el cual, según Jean, envió por e-mail a Alison.

Hay una conducta un poco sospechosa en los e-mails de Alison, pues primero una gran cantidad de spam a Jean y posteriormente dice que su e-mail estaba desconfigurado y que por eso su correo hasta ese momento había sido alex@mz57.biz.

From: alex: alison@m57.biz
To: Jean User
CC:
Subject: RE: which email address are you using?

Headers | Text | HTML | RTF | Attachments (0)

Yes, I got this email.

-----Original Message-----
From: Jean User [mailto:jean@m57.biz]
Sent: Sunday, July 20, 2008 12:46 AM
To: alex
Subject: RE: which email address are you using?

So are you going to get this email?

-----Original Message-----
From: alex [mailto:alison@m57.biz]
Sent: Sunday, July 20, 2008 12:44 AM
To: Jean User
Subject: RE: which email address are you using?

Whoops. It looks like my email was misconfigured.

My email is alison@m57.biz, not alex. Sorry about that.

-----Original Message-----
From: alex [mailto:alex@m57.biz]
Sent: Sunday, July 20, 2008 12:33 AM
To: Jean User; alison@m57.biz
Subject: RE: which email address are you using?

This one, obviously.

-----Original Message-----
From: Jean User [mailto:jean@m57.biz]
Sent: Sunday, July 20, 2008 12:32 AM
To: alison@m57.biz
Subject: which email address are you using?

Are you going to use alex@m57.biz or alison@m57.biz?

Es decir, es muy posible que Jean enviara la hoja de cálculo al que creía que era el correo de Alison pero ésta última parece que no era quien de verdad decía ser, o sea, parece que su correo estaba hackeado, puesto que en el spam enviado hay enlaces sospechosos y Alison podría haber sido víctima de phising.

No hay emails que demuestren explícitamente que ha sido Alison quien ha filtrado la hoja de cálculo, pero hay evidencias con las que inculparla. ¿Tengo pruebas? No. ¿Pero tengo dudas? Pues tampoco.