

Auditoría y Legislación Informáticas

Análisis forense de discos

Índice

| | |
|--|----|
| 1. Introducción..... | 1 |
| 2. Objetivos..... | 1 |
| 3. Herramientas software y material..... | 2 |
| 3.1. Clonado de discos | 2 |
| 3.2. Comprobación de extensiones de archivos | 2 |
| 3.3. Recuperación de archivos borrados..... | 3 |
| 4. Metodología | 3 |
| 4.1. Obtención de imagen clonada de un disco duro | 3 |
| 4.1.1. Preparación de archivos | 3 |
| 4.1.2. Preparación de memoria USB | 5 |
| 4.1.3. Creando el Live Flash USB..... | 6 |
| 4.1.4. Clonado de la memoria USB | 8 |
| 4.1.5. Montando la imagen | 13 |
| 4.2. Recuperación de archivos borrados..... | 15 |
| 4.3. Preprocesado para asegurar formatos de archivos | 18 |
| 5. Resultados | 20 |
| 6. Recuperación de la memoria USB utilizada tras usar OSFClone | 20 |
| 7. Bibliografía y referencias | 20 |
| 8. Sesiones prácticas y entregas | 21 |
| 8.1. Sesión 1 | 21 |
| 8.2. Sesión 2 | 21 |
| 8.3. Sesión 3 | 22 |
| 8.4. Práctica 1..... | 22 |

1. Introducción

Se sospecha que un equipo informático puede contener archivos con información muy valiosa para aclarar ciertas circunstancias en un proceso judicial. Se requiere, por tanto, de un análisis forense para obtener estos archivos. En principio, parece que se dispone únicamente de un disco duro, extraído del equipo confiscado, y que es sobre el que deben realizarse las pruebas periciales pertinentes. Junto con el mismo, se dispone de un escrito judicial en el que el juez encargado de la investigación solicita recuperar los archivos sensibles a la investigación.

2. Objetivos

Para la realización del informe pericial solicitado, es preciso identificar una serie de objetivos parciales, que deben ir alcanzándose por orden hasta la finalización del análisis forense en cuestión. Se resumen en la siguiente lista:

FASE 1: Preservación de pruebas

1. Clonado del disco duro, siguiendo las técnicas clásicas de análisis forense, para evitar la alteración de la prueba original. De este modo, todas las pruebas que se realicen serán llevadas a cabo en una copia clonada exacta a la original, manteniendo inalterado el disco duro la original.

FASE 2: Localización de archivos con contenido sensible a la investigación

2. Recuperación de posibles archivos borrados.
3. Búsqueda exhaustiva de todos los archivos que tengan un formato determinado concordante con la información que se desea buscar. Habrá que tener especial atención a que el propietario del equipo no haya renombrado las extensiones de los archivos en cuestión, con el objetivo de ocultar su existencia, disimularla o confundir a cualquier otro usuario del equipo.

3. Herramientas software y material

Básicamente, se dispone de un disco duro original que es preciso clonar para preservarlo. Adicionalmente, se presenta en este apartado el software utilizado durante las tareas de análisis forense, indicando (en la sección de referencias) de dónde puede obtenerse.

3.1. Clonado de discos

Como material se dispone de un disco duro original, que es preciso preservar. Por ello, se debe obtener una imagen clonada del disco original, sobre la que se realizarán todas las pruebas. Existen muchas herramientas para realizar el clonado de discos. Una de ellas podría ser la que se ofrece desde OSForensics:

- **OSFClone**, en conjunción con **ImageUSB** y **OSFMount** [1]

Tal y como se comentará posteriormente, también se hace uso de la herramienta **Eraser** para realizar borrados seguros de archivos. Esta herramienta puede encontrarse en [2].

3.2. Comprobación de extensiones de archivos

En la web pueden encontrarse multitud de aplicaciones para determinar la extensión más probable de un archivo, en el caso de que ésta se desconozca o se desconfíe de la que muestra. Dado que es posible que los archivos con contenidos ilegales hayan sido renombrados a otras extensiones para evitar su identificación, resulta muy adecuado el uso de este tipo de herramientas. Esta opción se encuentra en los objetivos 2 y 3, anteriormente enumerados. De entre todas las posibilidades existentes, se seleccionan dos herramientas libres muy simples, para tratar de asegurar, de este modo, que los formatos propuestos concuerden adecuadamente:

- A. **TrID** [3]
- B. **HexBrowser.NET** [4]

3.3. Recuperación de archivos borrados

Para la consecución del objetivo 3, en lo relativo a la recuperación de archivos borrados, también existen varias posibilidades. De entre todas ellas, en este estudio se propone el uso de:

- **Recuva** [5]
- **MiniTool** [6]

4. Metodología

Siguiendo en orden cronológico los objetivos marcados, será necesario realizar las siguientes tareas, en el orden indicado.

- Obtención de una imagen clonada del disco duro original.
- Recuperación de archivos borrados.
- Preprocesado para comprobar los formatos de archivos.

4.1. Obtención de imagen clonada de un disco duro

En análisis forense de discos, lo habitual es realizar un clonado de unidades arrancando desde un Live CD o desde una unidad flash USB. Clonar un disco duro puede llevar bastante tiempo, dependiendo del tamaño del mismo, del equipo con el que se trabaja, de las herramientas utilizadas...

Para ilustrar todo el proceso de forma sencilla, en lugar de clonar un disco duro (**pongamos en clonar 1 TB**) se procederá a preparar una memoria USB del menor tamaño posible (512 MB en nuestro caso), con una serie de ficheros. Será más rápido clonar 512 MB que clonar 1 TB, además de que necesitaremos para almacenar la imagen clonada otra memoria USB, en lugar de otro disco duro de 1 TB.

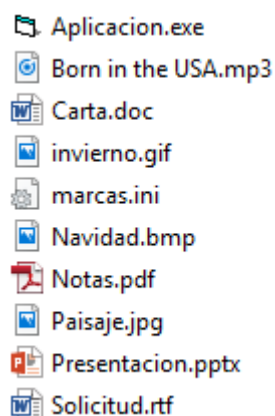
4.1.1. Preparación de archivos

Para la simulación, se descargarán de internet 10 archivos con **extensiones diferentes**, y **con tamaños pequeños**. Las extensiones pueden ser algunas de las siguientes: MID, MP3, AVI, WMV, RTF, DOC, DOCX, XLS, XLSX, PPT, PPTX, PDF, JPG, BMP, GIF, PNG, INI, TIF, EXE, TXT ...

Para buscar archivos con una extensión determinada en Google, bastará con incluir la cláusula **filetype:EXT**, donde EXT será la extensión del archivo que se está buscando. Por ejemplo:

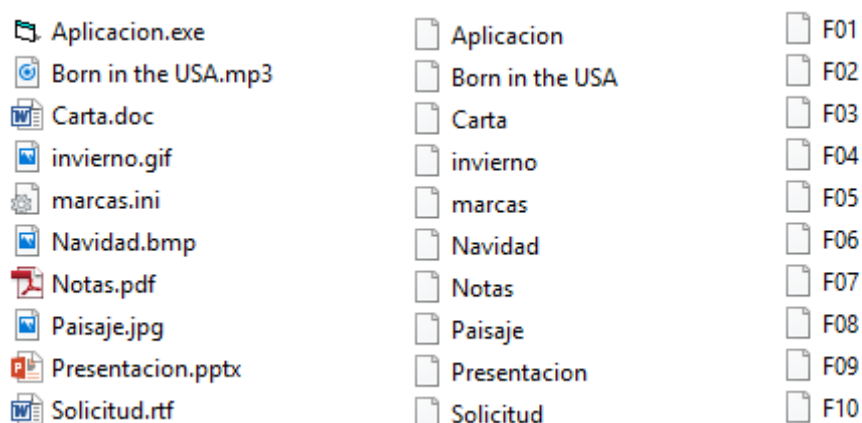
notas filetype:pdf

La relación de archivos que se usa en este ejemplo se muestra a continuación:



Cambiamos la extensión de estos ficheros con el objetivo de simular que el usuario del equipo ha modificado la extensión para dificultar el seguimiento de los archivos. Básicamente, se propone que se elimine directamente su extensión, en lugar de cambiarla a otra distinta.

Además, para no dar pistas sobre su contenido por el propio nombre del archivo, aunque éste no tenga extensión, sería conveniente renombrarlos con un nombre genérico. Por ejemplo (F01, F02, ... F10 para los 10 archivos considerados). De este modo, se tiene lo siguiente:



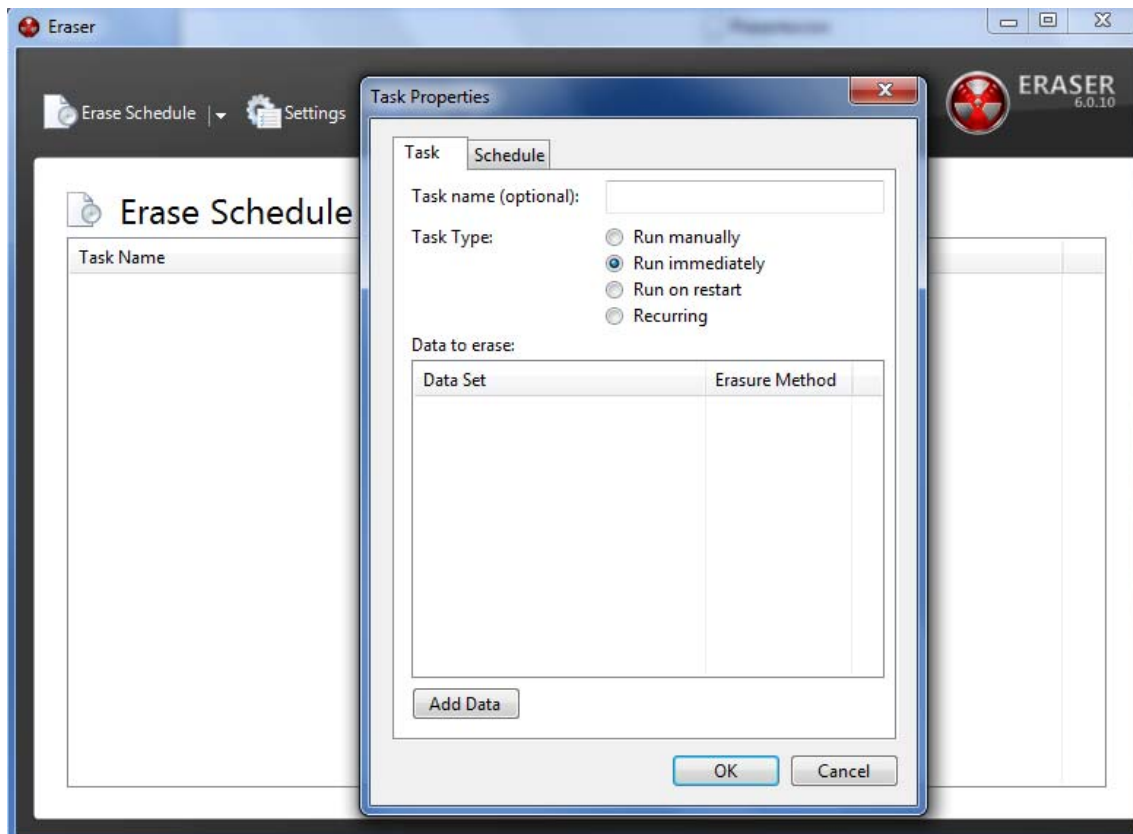
Resumiendo, en modo de tabla, se muestran los formatos de los diferentes archivos considerados:

| Archivo | Extensión | Nombre clave |
|---------------------|-----------|--------------|
| Aplicacion.exe | EXE | F01 |
| Born in the USA.mp3 | MP3 | F02 |
| Carta.doc | DOC | F03 |
| invierno.gif | GIF | F04 |
| marcas.ini | INI | F05 |
| Navidad.bmp | BMP | F06 |
| Notas.pdf | PDF | F07 |
| Paisaje.jpg | JPG | F08 |
| Presentacion.pptx | PPTX | F09 |
| Solicitud.rft | RTF | F10 |

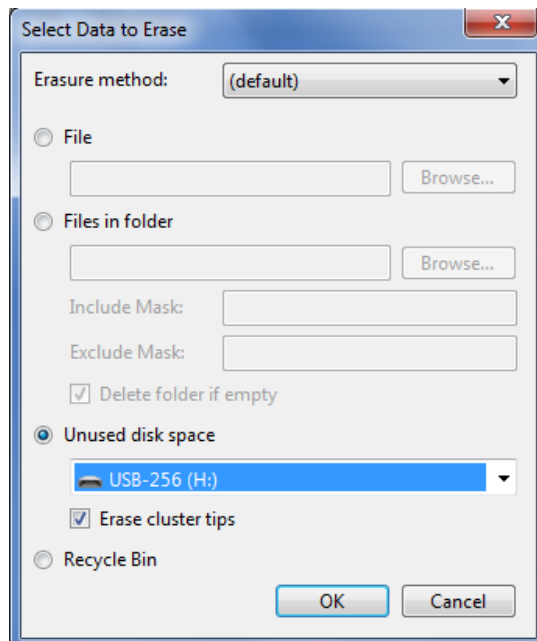
4.1.2. Preparación de memoria USB

Para continuar con la simulación, se debe preparar una memoria USB (preferiblemente de pequeño tamaño), donde se copiarán los archivos anteriores (sin extensión). Para evitar recuperar archivos no deseados en el proceso de recuperación de archivos que se realizará con posterioridad, se debe proceder a un borrado seguro de esta memoria USB, mediante herramientas como **Eraser** [2]. Proceso que se ilustra a continuación.

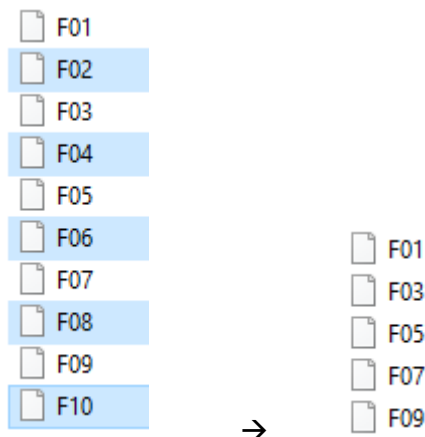
- Debe ejecutarse **Eraser**, en modo Administrador (“Ejecutar como Administrador”).
- Con el botón derecho del ratón, se selecciona una nueva tarea:



- Se elige “Run immediately” y se pulsa sobre “Add Data”. Se deben borrar los ficheros, así como el espacio libre que queda en la memoria USB y que puede contener archivos borrados hace tiempo.



- Una vez borrada la memoria USB, se procede a copiar los 10 archivos sin extensión sobre la misma (en el directorio raíz). Tras ello, se borrarán 5 archivos, arrastrándolos a la papelera de reciclaje o utilizando la tecla SUPR (es decir, se hará un borrado *no seguro* de los mismos). En el ejemplo siguiente, se observa cómo se eliminan los archivos que ocupan un orden par:



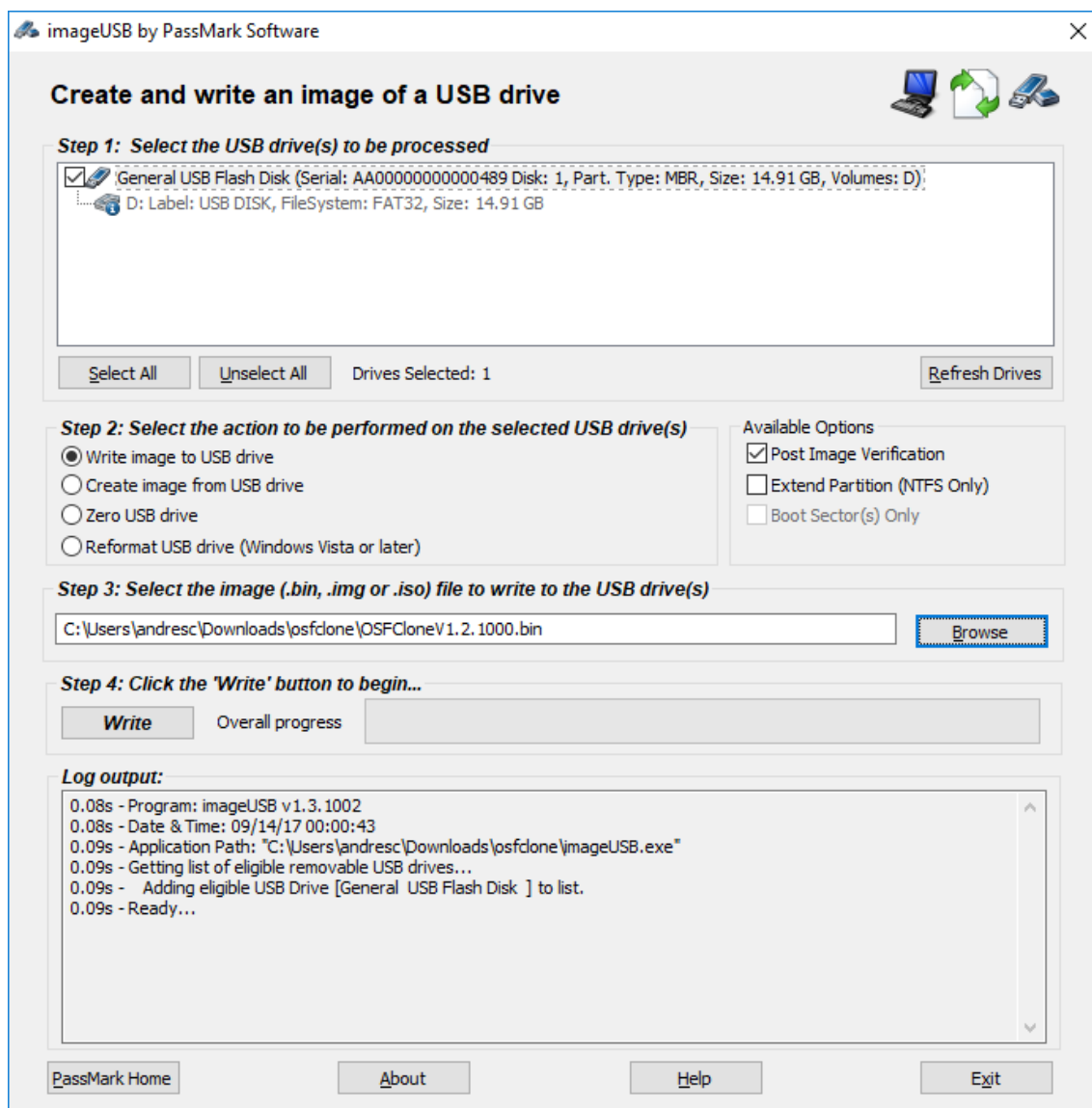
4.1.3. Creando el Live Flash USB

El siguiente paso consiste en realizar el clonado de la memoria USB, que contiene 5 archivos en el directorio raíz, y otros 5 archivos borrados, también en el directorio raíz.

Generalmente, para evitar la alteración / modificación de las pruebas (discos duros, por ejemplo), en informática forense suelen utilizarse **Live CDs** para arrancar el sistema y proceder a la fase de adquisición de pruebas. Existen varias distribuciones de Live CDs de análisis forense en la web, que permite multitud de opciones. En nuestro ejemplo en particular, básicamente se precisa realizar un clonado de un disco duro (memoria USB en nuestra simulación). Para ello, bastará con disponer de una herramienta de clonado ([OSFClone](#) [1]), que será montada en una unidad de arranque USB, en lugar de tener que generar un CD de arranque, algo más tedioso que la solución que se propone a continuación.

De este modo, para clonar esta memoria USB (con la herramienta **OSFClone**) se usa la aplicación **ImageUSB** [1], que permite realizar una unidad flash de arranque a partir del fichero descargado.

Tras descomprimir el archivo **OSFClone.zip**, se tiene el fichero **OSFClone.bin**. Se debe disponer de un Pendrive de al menos 2 GB, dado que no solo se copiará el fichero **OSFClone.bin**, sino también un **Core Linux** de arranque. Como es de esperar, se borrarán todos los datos que contenga. Al ejecutar **ImageUSB.exe**, se abre la siguiente pantalla:



Step 1. Debe seleccionarse la unidad USB que quiere convertirse en unidad de arranque (en este caso, la unidad D:).

Step 2. Se selecciona la opción **“Write image to UFD drive”**, que viene marcada por defecto.

Step 3. Se Selecciona el archivo OSFClone.bin.

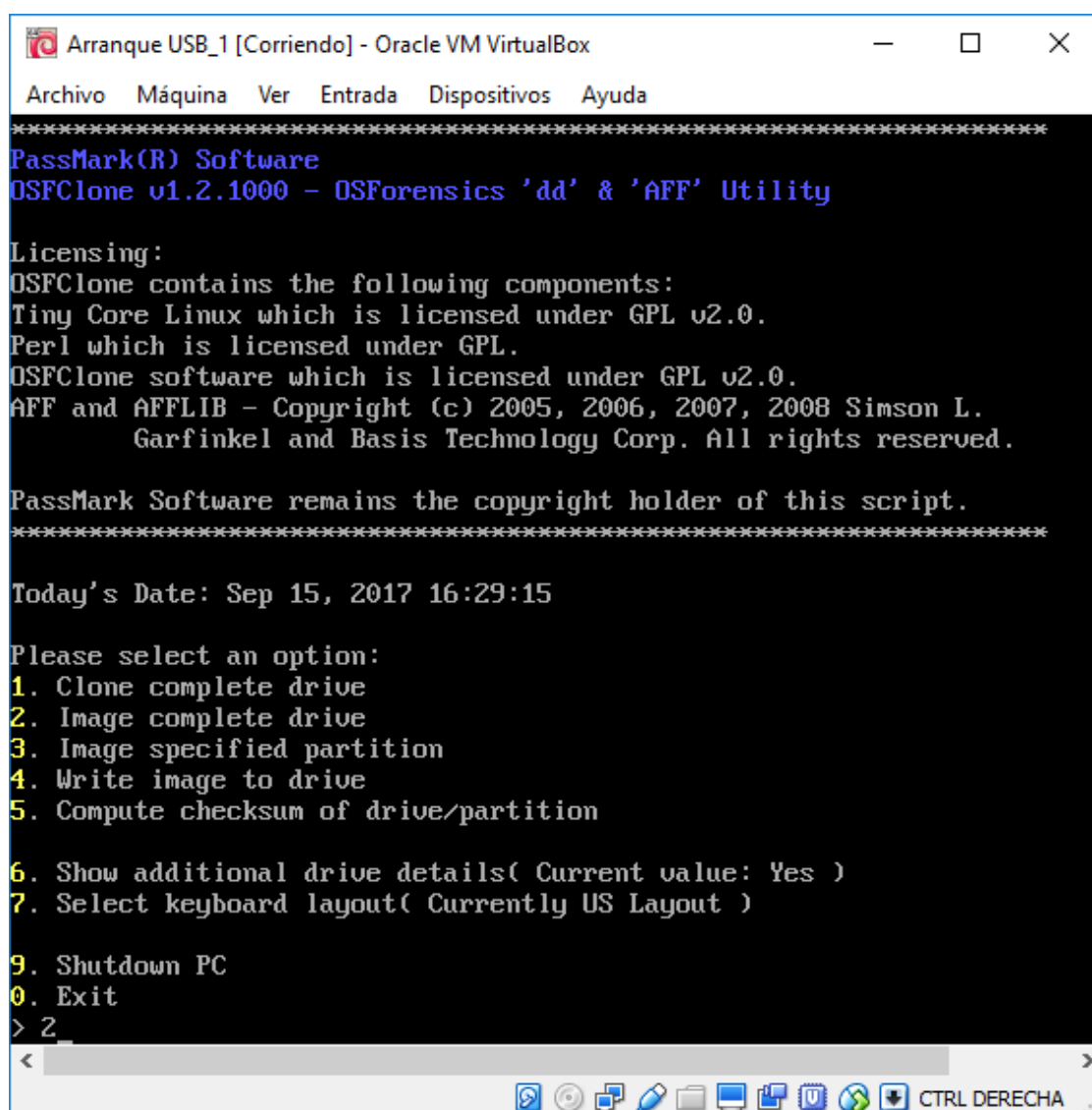
Step 4. Finalmente se graba el USB pulsando el botón **“Write”**.

4.1.4. Clonado de la memoria USB

Tras haber creado el Live FLASH según se ha explicado previamente, se introduce en el puerto USB y se arranca el equipo desde él (para ello seleccionar la opción necesaria de la BIOS en el arranque). Se arrancará un Tiny Core Linux, donde se pueden seleccionar las opciones mostradas en la imagen de más abajo (en nuestro caso, las capturas de pantalla se han realizado arrancando el live USB en una máquina virtual en Virtual Box).

Es importante indicar que, para clonar la memoria USB, debemos tener pinchada (además del live USB desde donde arranca el sistema), la memoria USB que contiene los 10 archivos con nombres genéricos y sin extensión (5 de ellos borrados). De este modo, se tienen 3 unidades:

- El disco duro del ordenador, donde se copiará la imagen clonada (será la ubicación destino del fichero de la imagen).
- La memoria USB desde donde arranca el sistema, con el Tiny Core Linux (una memoria de al menos 2 GB).
- La memoria que usamos para simular que es un disco duro, con la partición de 512 MB y los 10 archivos sin extensión (será la ubicación origen para realizar la clonación).



```
Arranque USB_1 [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
*****
PassMark(R) Software
OSFClone v1.2.1000 - OSForensics 'dd' & 'AFF' Utility

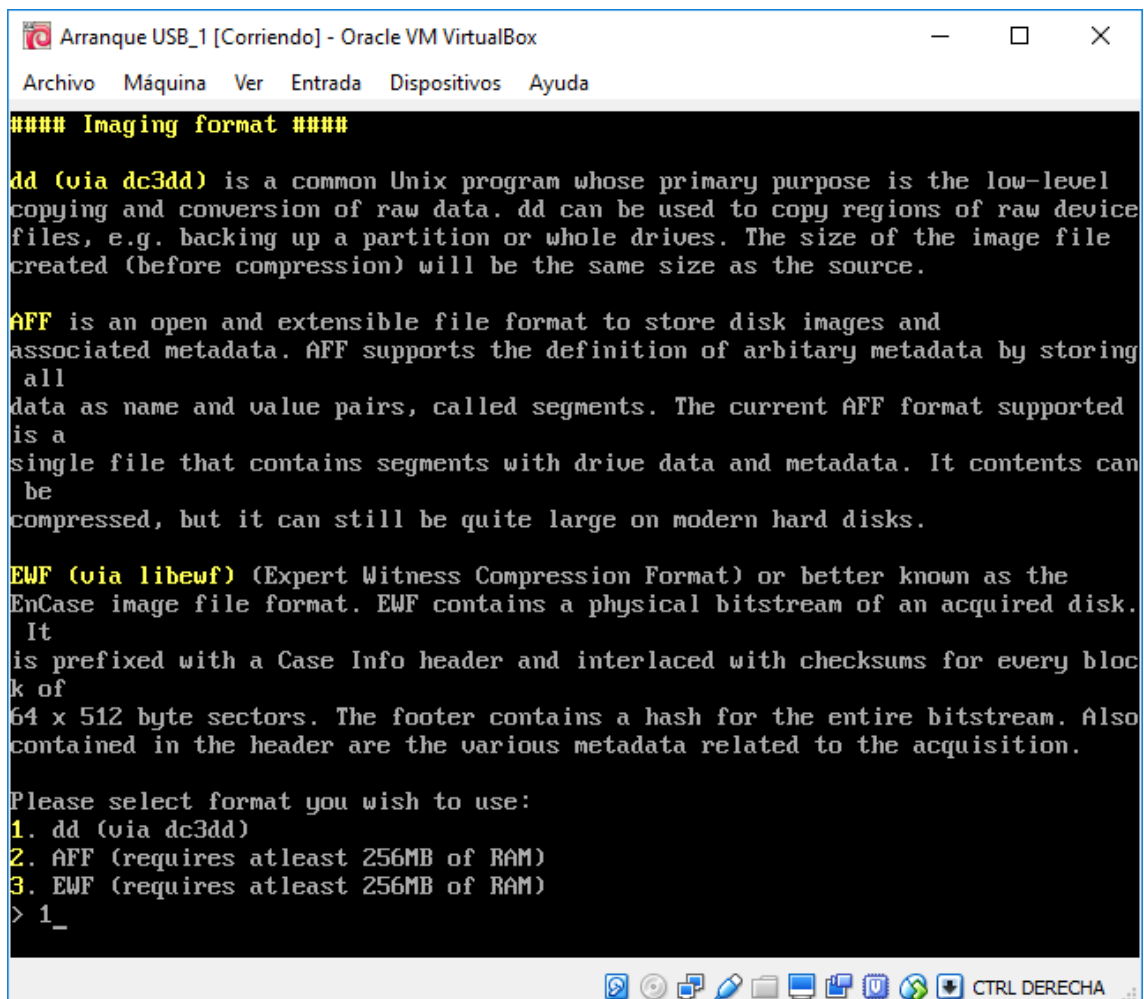
Licensing:
OSFClone contains the following components:
Tiny Core Linux which is licensed under GPL v2.0.
Perl which is licensed under GPL.
OSFClone software which is licensed under GPL v2.0.
AFF and AFFLIB - Copyright (c) 2005, 2006, 2007, 2008 Simson L.
Garfinkel and Basis Technology Corp. All rights reserved.

PassMark Software remains the copyright holder of this script.
*****

Today's Date: Sep 15, 2017 16:29:15

Please select an option:
1. Clone complete drive
2. Image complete drive
3. Image specified partition
4. Write image to drive
5. Compute checksum of drive/partition
6. Show additional drive details( Current value: Yes )
7. Select keyboard layout( Currently US Layout )
9. Shutdown PC
0. Exit
> 2
<
```


Se selecciona la opción “2. **Image complete drive**”. Al seleccionarla, se muestra una ventana para seleccionar el formato de copia a usar, como se observa en la siguiente imagen:



Se selecciona la opción “1. **Dd (via dc3dd)**”. Tras ello, se muestra un menú que debe completarse por partes:

```
Arranque USB_1 [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
#### Image Complete Drive using 'dd' ####
Destination drive size must be greater than source.

Number of Physical Storage Drives found: 3
Drives found:
ID:      Drive:      Size:
[0]      /dev/sda      16.0GB (Model: ATA VBOX HARDDISK Serial No: VBe15954eb-d
ba29202)
[1]      /dev/sdb      529MB (Model: USB 2.0 Flash Disk Serial No: Unknown)
[2]      /dev/sdc      4027MB (Model: Generic Flash Disk Serial No: Unknown)

Number of valid destination partitions on all drives: 3
Partitions found:
*      Options:
*          + checksum method = md5
*          + post 'dd' verify dst = no
*          + compression method = none
*          + split large files = no
*          + block size bs = 1M
*****

Menu choices:
1. Select source
2. Select destination
3. Change options
4. Change image filename
9. Execute 'dd'
0. Return to main menu
>
```

Se observa, en el rectángulo rojo, que hay 3 unidades conectadas al equipo.

Se selecciona opción **"1. Select Source"**, el disco duro fuente, esto es, la unidad que se quiere clonar. Tras ello, se selecciona el disco duro/partición de destino, con la opción **"2. Select Destination"**. A continuación, se seleccionan las opciones de copia, opción **"3. Change options"**:

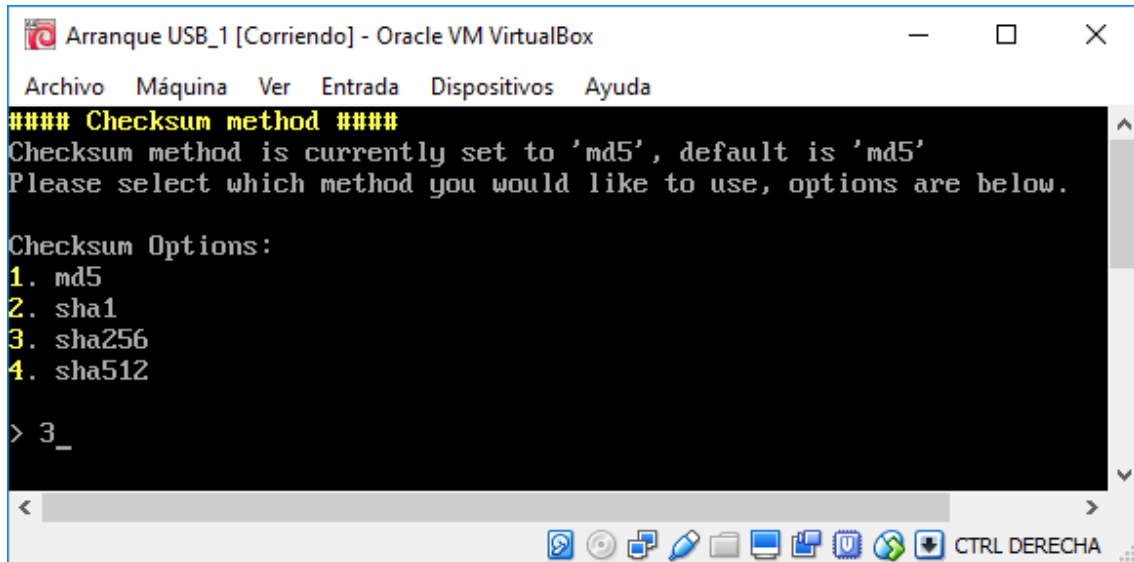
```
Arranque USB_1 [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
#### OPTIONS ####

Please select an option to change:
#      Option                Default Current
[1]    Checksum Method        md5      md5
[2]    Post 'dd' dst verify    Yes      no
[3]    Split image file        No       no
[4]    Split file size         2G       2G
[5]    Compress image          none     none
[6]    Compress level          6        6
[7]    BlockSize               1M       1M

[0]    Return to previous menu
>
```

Como puede verse, por defecto aparece **md5** como método de Checksum. Por seguridad, dado que en los últimos años han quedado patente las colisiones producidas por **md5**, se procede a cambiar el algoritmo por **SHA256**:

Se cambia el método de chequeo (opción 1) pasando de utilizar MD5 a usar SHA256

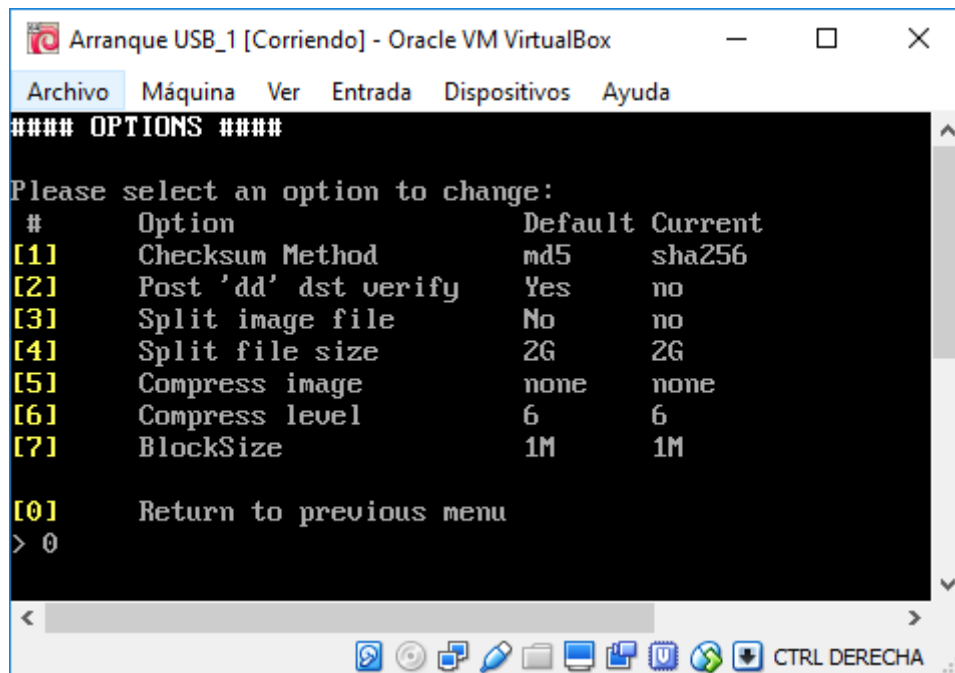


```
##### Checksum method #####
Checksum method is currently set to 'md5', default is 'md5'
Please select which method you would like to use, options are below.

Checksum Options:
1. md5
2. sha1
3. sha256
4. sha512

> 3_
```

Se seleccionará la opción “3. sha256”.



```
##### OPTIONS #####
Please select an option to change:

#      Option                Default Current
[1]    Checksum Method        md5      sha256
[2]    Post 'dd' dst verify   Yes      no
[3]    Split image file       No       no
[4]    Split file size        2G       2G
[5]    Compress image         none     none
[6]    Compress level         6        6
[7]    BlockSize              1M       1M
[0]    Return to previous menu

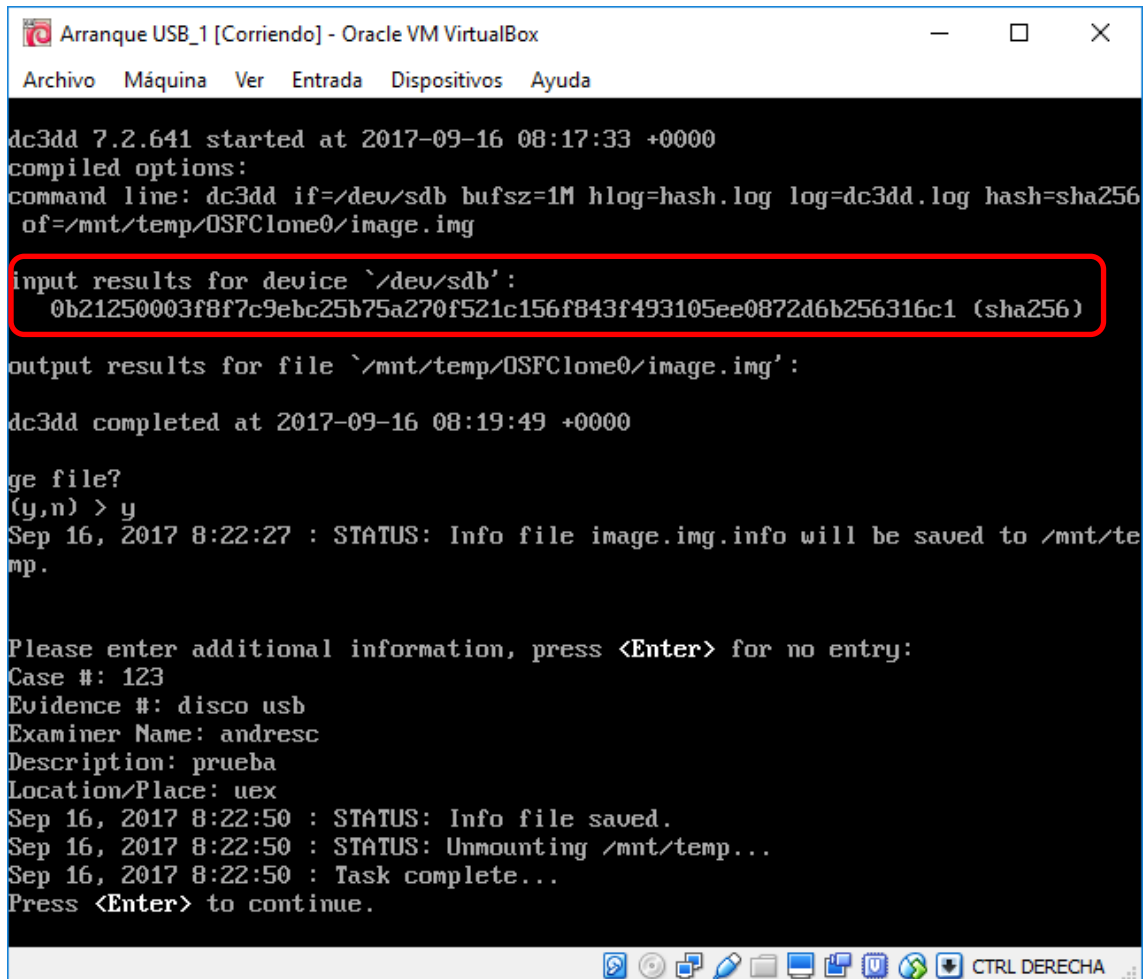
> 0
```

Tras este cambio, seleccionando 0 volvemos al menú de opciones.

Finalmente, en el menú principal, se selecciona la opción “9. Execute dd”. Se pedirá confirmación y comenzará la copia. Con esto se tendrá, después de un cierto tiempo (que variará en función del hardware y del tamaño de la clonación), una imagen llamada **image.img** en la partición de destino indicada.

En pantalla se muestra el hash sha256 correspondiente a la imagen que se ha creado, que servirá para validar la integridad del fichero y certificar que no ha sido modificado con posterioridad, asegurando así la “cadena de custodia” de las evidencias obtenidas.

Cuando finalice el proceso de clonación de la imagen, se pregunta al usuario si desea salvar un fichero de información en la misma ubicación del fichero de imagen:



```
Arranque USB_1 [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

dc3dd 7.2.641 started at 2017-09-16 08:17:33 +0000
compiled options:
command line: dc3dd if=/dev/sdb bufsz=1M hlog=hash.log log=dc3dd.log hash=sha256
of=/mnt/temp/OSFClone0/image.img

input results for device `/dev/sdb':
0b21250003f8f7c9ebc25b75a270f521c156f843f493105ee0872d6b256316c1 (sha256)

output results for file `/mnt/temp/OSFClone0/image.img':

dc3dd completed at 2017-09-16 08:19:49 +0000

ge file?
(y,n) > y
Sep 16, 2017 8:22:27 : STATUS: Info file image.img.info will be saved to /mnt/temp.

Please enter additional information, press <Enter> for no entry:
Case #: 123
Evidence #: disco usb
Examiner Name: andresc
Description: prueba
Location/Place: uex
Sep 16, 2017 8:22:50 : STATUS: Info file saved.
Sep 16, 2017 8:22:50 : STATUS: Unmounting /mnt/temp...
Sep 16, 2017 8:22:50 : Task complete...
Press <Enter> to continue.
```

En este caso, se pedirá el número de caso (Case #), el número de evidencia (Evidence #), el nombre del analista (Examiner Name), una descripción (Description) y localización/lugar (Location/Place).

```
Image created using OSFClone v1.2.1000
Image created on Sep 16, 2017 08:19:49
```

```
BASIC INFO:
Image source: /dev/sdb1
```

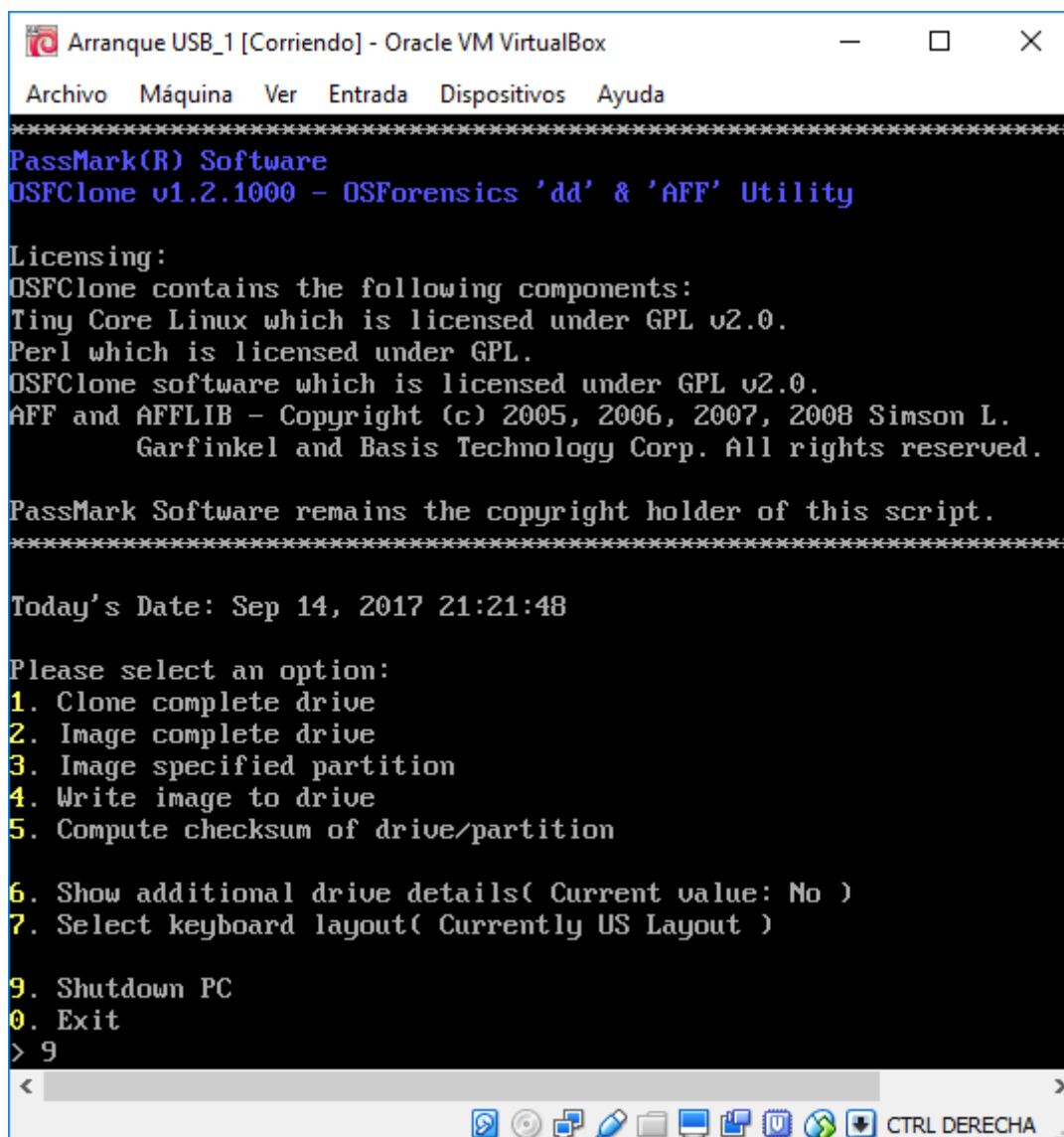
```
IMAGE FILE(S):
image.img

Image filesize: bytes
```

```
CHECKSUM:
```

```
Case #: 123
Evidence #: disco usb
Examiner Name: andresc
Description: prueba
Location/Place: uex
```

Para finalizar, se selecciona la opción 9, que apaga el equipo.



```
Arranque USB_1 [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
*****
PassMark(R) Software
OSFClone v1.2.1000 - OSForensics 'dd' & 'AFF' Utility

Licensing:
OSFClone contains the following components:
Tiny Core Linux which is licensed under GPL v2.0.
Perl which is licensed under GPL.
OSFClone software which is licensed under GPL v2.0.
AFF and AFFLIB - Copyright (c) 2005, 2006, 2007, 2008 Simson L.
Garfinkel and Basis Technology Corp. All rights reserved.

PassMark Software remains the copyright holder of this script.
*****

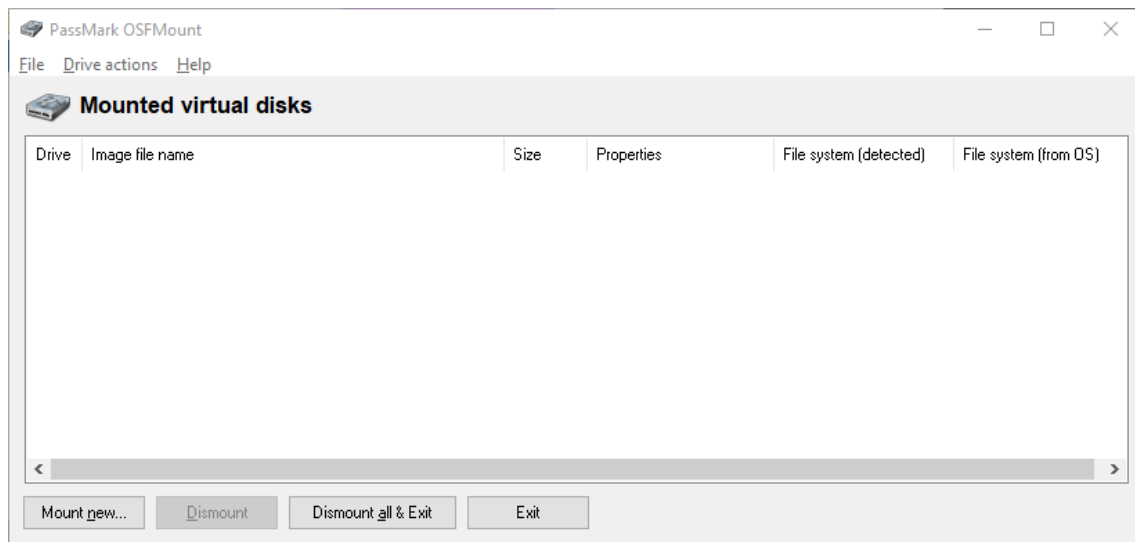
Today's Date: Sep 14, 2017 21:21:48

Please select an option:
1. Clone complete drive
2. Image complete drive
3. Image specified partition
4. Write image to drive
5. Compute checksum of drive/partition
6. Show additional drive details( Current value: No )
7. Select keyboard layout( Currently US Layout )
9. Shutdown PC
0. Exit
> 9
```

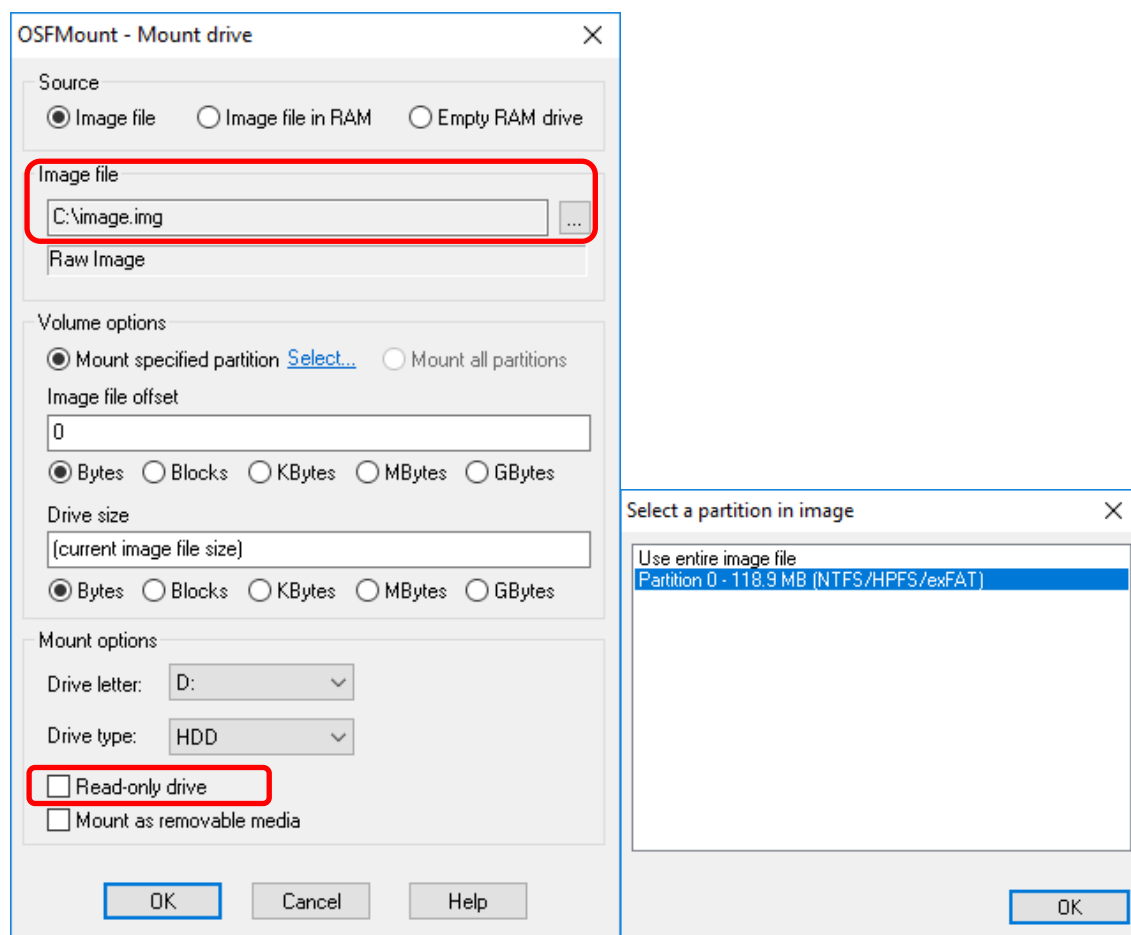
Una vez que se disponga de esta imagen clonada, por precaución, se procederá a almacenar una segunda copia de esta imagen en otra ubicación, para evitar tener que proceder a realizar nuevas clonaciones en el caso de que, por causas del análisis forense a realizar, la copia clonada se volviese inestable. Este proceso se repetirá cuantas veces sea necesario, en caso de que se destruya la copia clonada donde se esté realizando el análisis forense antes de la finalización de todas las tareas necesarias.

4.1.5. Montando la imagen

Así, se habrá creado una imagen clonada de la memoria USB, usando el formato de clonación dd. Para poder montar una imagen de este formato en Windows, se precisa la aplicación [OSFMount](#) [1].



Tras seleccionar el botón “Mount new...” aparece la siguiente pantalla, donde hay que seleccionar el archivo imagen. También se ha deshabilitado la opción de montar como sólo lectura, para permitir recuperar los archivos borrados sobre la propia unidad:

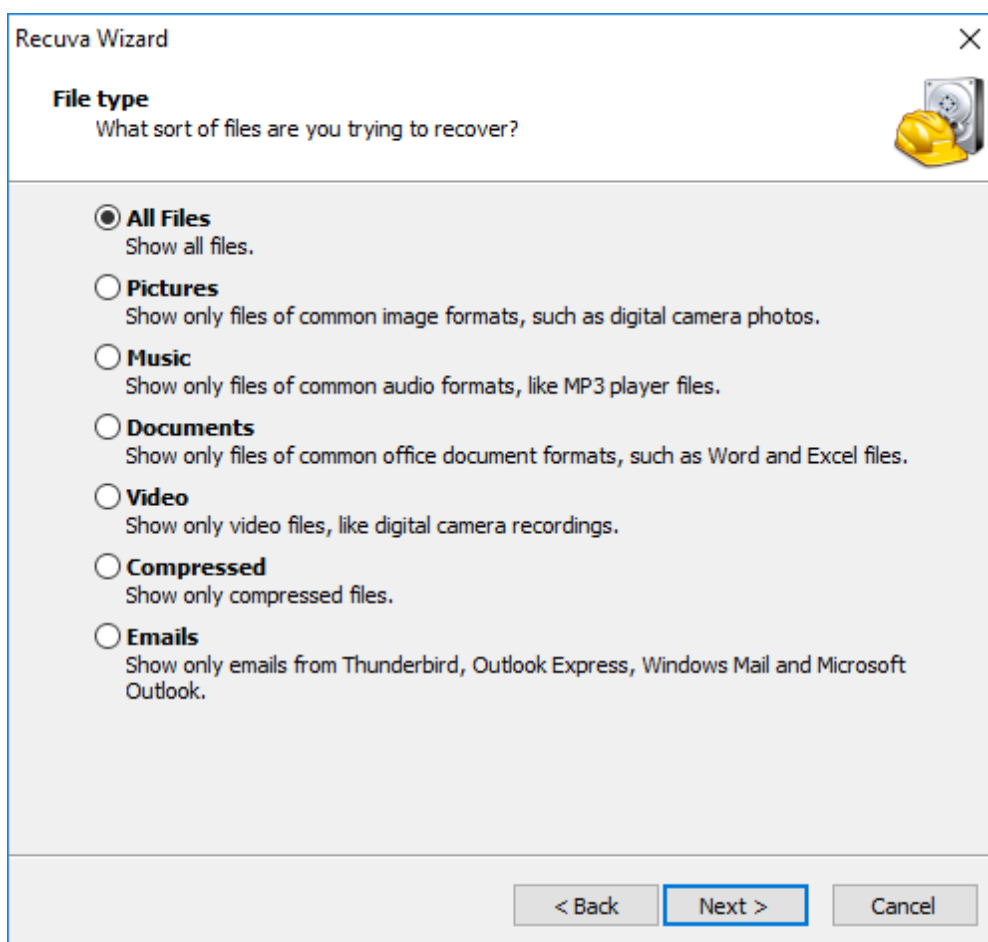


4.2. Recuperación de archivos borrados

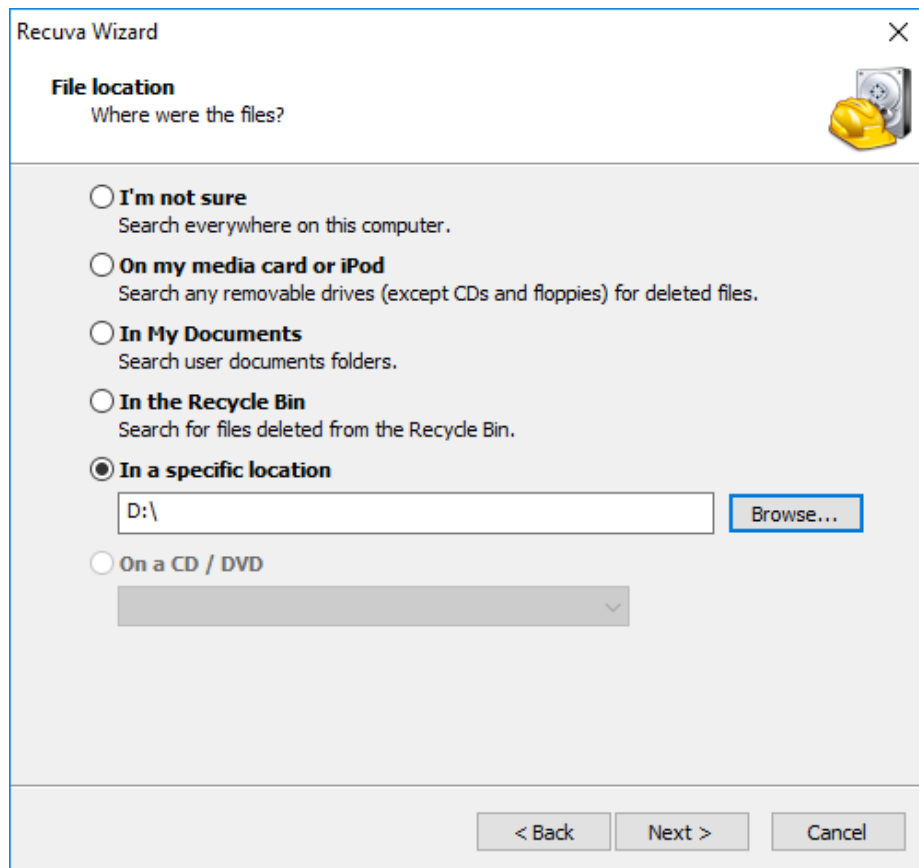
Es posible que el propietario del equipo haya borrado, previa a la intervención policial, determinados archivos. Para la consecución de este objetivo, existen varias posibilidades. [EaseUS Data Recovery Wizard Professional](#) [7] y [Stellar Phoenix Windows Data Recovery](#) [8] son dos aplicaciones comerciales muy interesantes. Como alternativa al software de pago, en [9] se muestra una relación de 15 aplicaciones gratis para recuperar archivos borrados. Para este análisis forense este tipo de aplicaciones libres es más que suficiente. De entre todas ellas, en este estudio se propone el uso:

- C. [Recuva](#) [5]
- D. [MiniTool](#) [6]

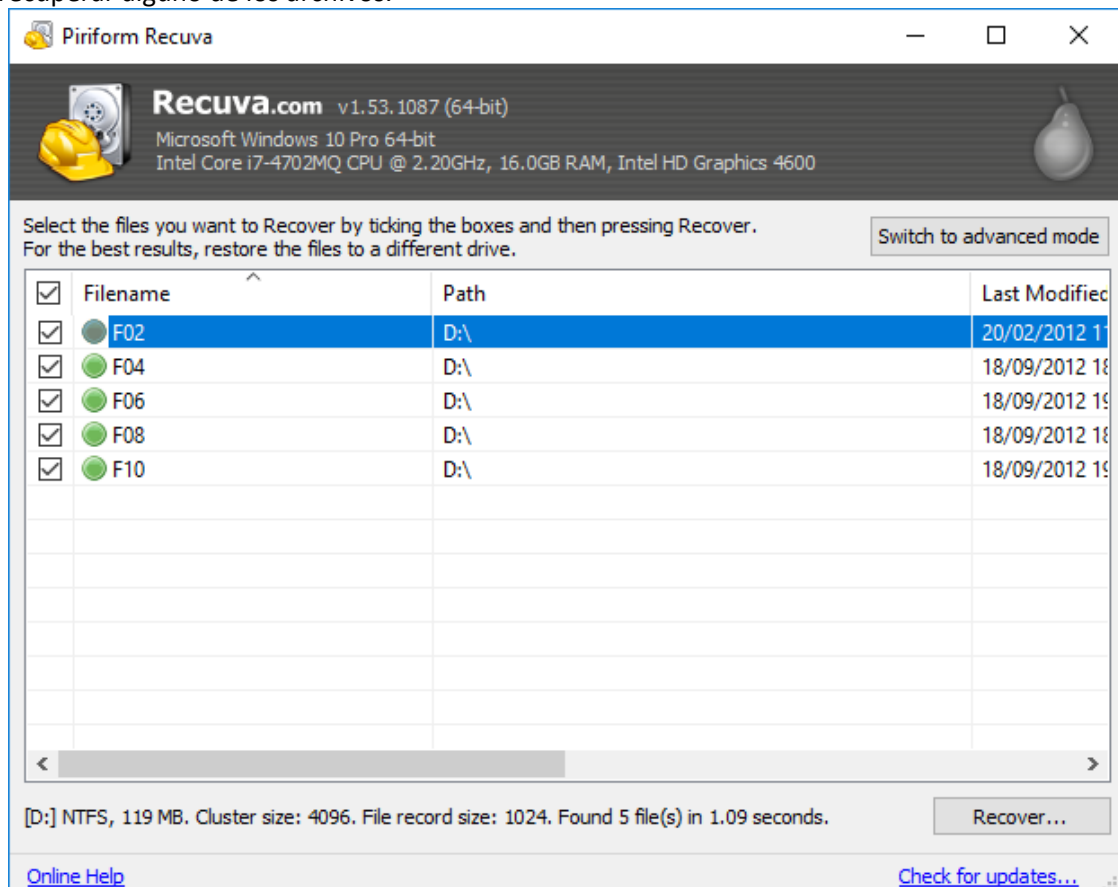
Una vez instalado [Recuva](#), inicialmente pregunta por el tipo de archivos que se está intentando recuperar.



A continuación, debe especificarse dónde se encuentran los ficheros que se desean recuperar. En nuestro caso, en la unidad virtual D: que acaba de montarse desde la imagen clonada.

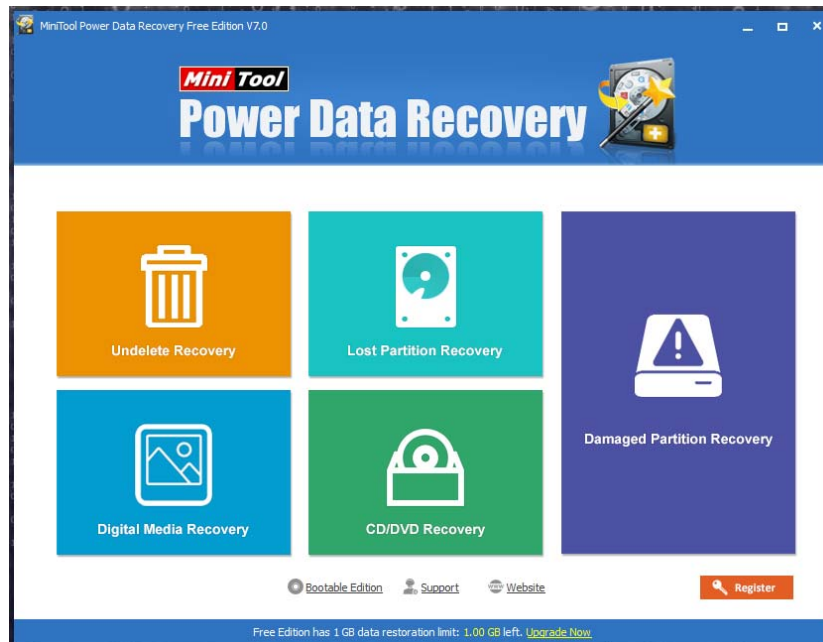


La aplicación localiza los archivos borrados. Cabe la posibilidad de que no sea posible recuperar alguno de los archivos.

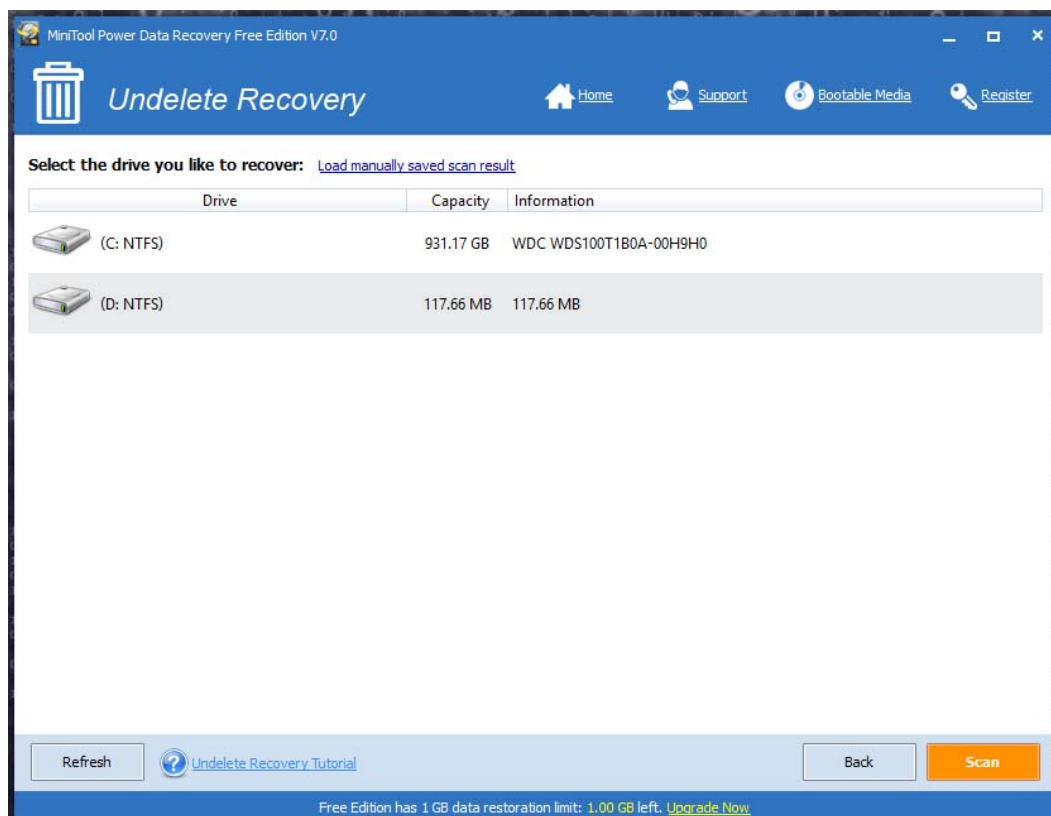


Al pulsar en el botón “Recover...” la aplicación nos pide la ubicación donde se recuperarán estos archivos (que puede ser una carpeta de nuestro disco duro), recuperando así los archivos.

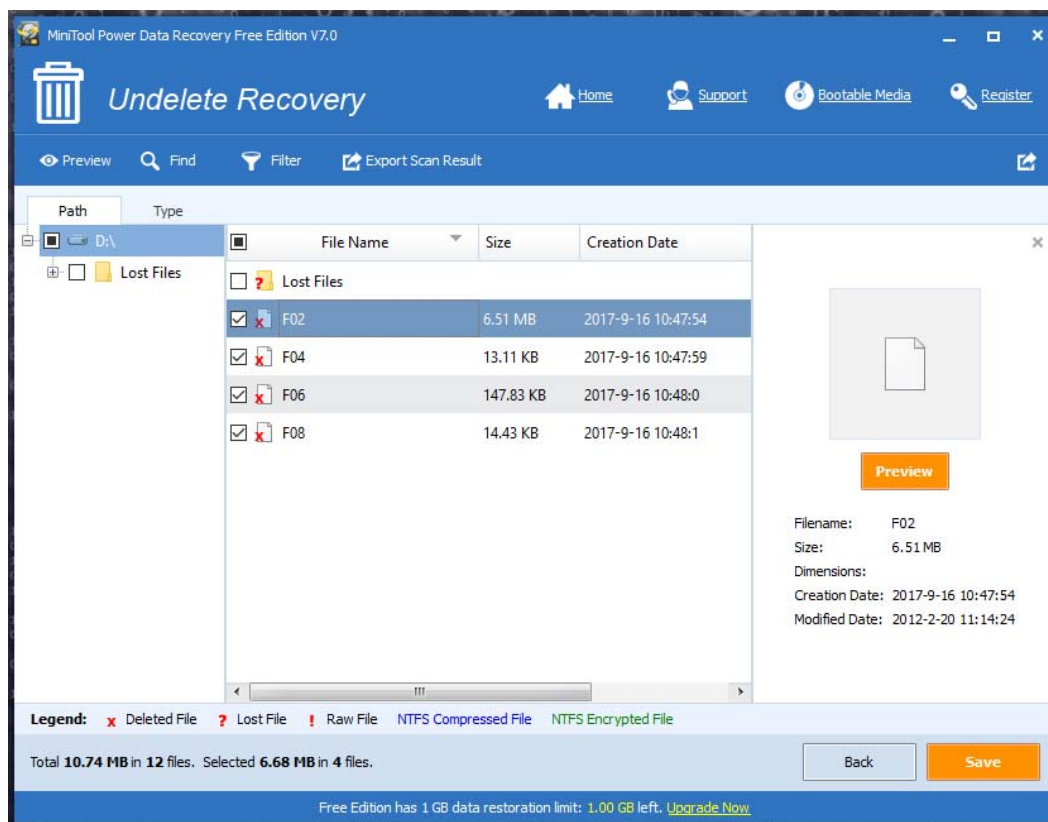
Con respecto a la aplicación **MiniTool**, una vez instalada, sobre la pantalla principal bastará con indicar que se desean recuperar los archivos borrados (opción “Undelete Recovery”):



En la siguiente pantalla, se debe indicar sobre qué unidad se desea realizar la recuperación de archivos:



Tras seleccionar la unidad en cuestión (**D:** en este caso), haciendo click en el botón “Scan” aparecen los archivos que han sido borrados.



Una vez que se seleccione el botón “Save”, habrá que indicar dónde se desean salvar los archivos marcados para recuperar. Es recomendable (¡y lógico!) salvar los archivos recuperados en otra unidad, ya que, en caso contrario, los datos borrados podrían sobrescribirse.

Al ser una versión gratuita, puede apreciarse que la cantidad de datos recuperados se limita a 1 GB, suficiente, al menos, para el ejemplo presentado en este documento.

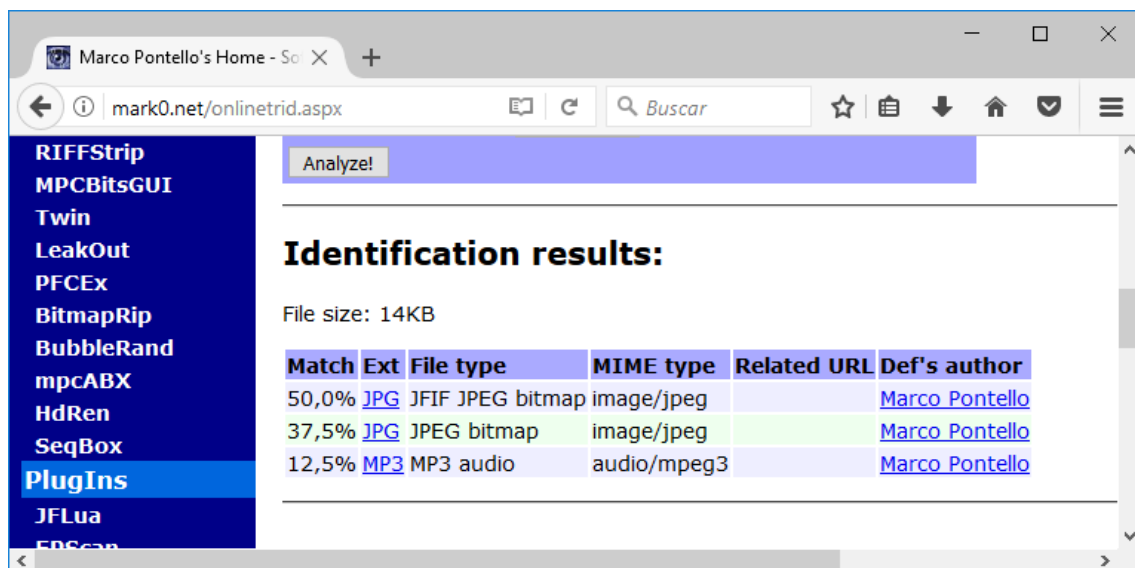
4.3. Preprocesado para asegurar formatos de archivos

En este momento se procederá a realizar la comprobación de extensiones de los archivos, por si el propietario del equipo hubiera renombrado las extensiones de los archivos, tal y como se ha comentado anteriormente. Para asegurar el correcto formato de los archivos (esto es, la extensión de los mismos) se dispone de varias posibilidades, que se presentan a continuación.

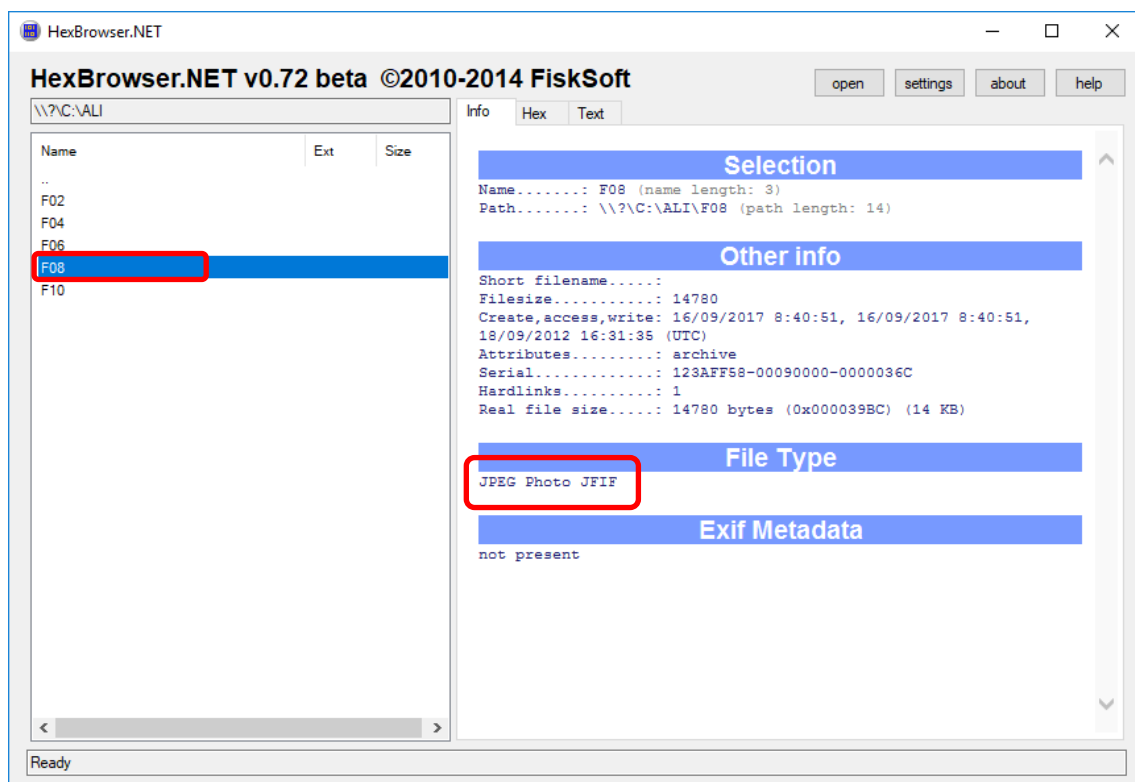
Una primera opción, para no iniciados consistiría en subir el archivo en cuestión a alguna web que permitiese identificar el tipo de archivo que es, por ejemplo, en la web de la aplicación TrID se puede hacer este tipo de comprobaciones de forma online:

<http://mark0.net/onetrid.aspx>

Por ejemplo, para el archivo F08, la web nos indica que se trata de un fichero JPG (JFIF JPEG) con una probabilidad del 50%, JPG (JPEG) con una probabilidad del 37,5% y un MP3 con una probabilidad del 12,5%. Bastará con cambiar la extensión y probar.













Otra posibilidad consiste en obtener en nuestro propio equipo algún programa que permita identificar extensiones de archivos desconocidos, o sin extensión, o, como en nuestro caso, con la extensión modificada. En [10] pueden encontrarse algunas aplicaciones muy sencillas de instalar y manejar. Una de ellas es **HexBrowser.NET**. Una vez descargada e instalada, puede comprobarse que identifica el archivo en cuestión como un archivo de JPG:



5. Resultados

De los trabajos presentados en el análisis forense realizado, se han recuperado los siguientes archivos:

| | | |
|----------|---|---|
| F01.exe | → |  Aplicacion.exe |
| F02.mp3 | → |  Born in the USA.mp3 |
| F03.doc | → |  Carta.doc |
| F04.gif | → |  invierno.gif |
| F05.txt | → |  marcas.ini |
| F06.bmp | → |  Navidad.bmp |
| F07.pdf | → |  Notas.pdf |
| F08.jpg | → |  Paisaje.jpg |
| F09.pptx | → |  Presentacion.pptx |
| F10.rtf | → |  Solicitud.rtf |

Para cada uno de los archivos recuperados, tras un chequeo de los mismos, se ha podido constatar que, efectivamente, la extensión se corresponde con el tipo de archivo adecuado.

6. Recuperación de la memoria USB utilizada tras usar OSFClone

Cuando se utiliza OSFClone con una memoria USB de más de 2 GB, ésta quedará con un tamaño de 2 GB, de modo que para recuperar el tamaño original y recuperar así toda la capacidad de almacenamiento hay que volver a formatearla. Si se realiza con Windows, el espacio no se recupera totalmente con un simple formateo, sino que habría que seguir los siguientes pasos:

- a) Abrir la consola de comandos y seguir los siguientes pasos.
- b) DISKPART
- 2) LIST DISK (aparecerá una lista de todos los discos del equipo)
- 3) select disk 1 (¡ojo! Hay que seleccionar el disco que se quiera formatear, en este caso el DISCO 1. **Cuidado con las equivocaciones**).
- 4) clean
- 5) create partition primary
- 6) format fs=NTFS
- 7) exit

7. Bibliografía y referencias

[1] OSFClone / ImageUSB / OSFMount
<http://www.osforensics.com/products.html>

[2] Eraser
<http://eraser.heidi.ie>

[3] TrID
<http://mark0.net/onlinetrid.aspx>

[4] HexBrowser.NET

<http://www.hexbrowser.com>

[5] Recuva

<https://www.piriform.com/recuva>

[6] MiniTool

<http://www.minitool.ca>

[7] EaseUS Data Recovery Wizard Professional:

<http://www.easeus.com/datarecoverywizardpro>

[8] Stellar Phoenix Windows Data Recovery:

<http://www.stellarinfo.com/es/recuperaciondeinformacion.htm>

[9] 15 aplicaciones gratis para recuperar archivos borrados

<http://www.emezeta.com/articulos/15-aplicaciones-gratis-para-recuperar-archivos-borrados>

[10] Como identificar archivos desconocidos o sin extensión en Windows

<https://norfipc.com/trucos/como-identificar-archivos-desconocidos-o-sin-extension-windows.php>

8. Sesiones prácticas y entregas

8.1. Sesión 1

- Explicación de la práctica.
- Planificación y recolección de ficheros para incluir en la memoria USB.
- Se comenzará a generar una imagen de una memoria USB de tamaño pequeño, que haya sido borrada de forma segura para eliminar todos los archivos previos. Sobre ella, copiar 10 archivos de extensiones diferentes, los cuales habrán sido renombrados como F01, ... F10, y a los que se les habrá eliminado también su extensión. Tras copiar en la memoria estos 10 archivos (con nombres genéricos y sin extensión), eliminar 5 de ellos para tratar de recuperarlos con posterioridad. Este trabajo continuará en casa y deberá quedar finalizado para la sesión 2, en que se procederá a la entrega de la imagen clonada de esa memoria USB.

ENTREGA: -

8.2. Sesión 2

- Durante la sesión se entregará la imagen clonada de la memoria USB que empezó a prepararse en la sesión 1. **Preferiblemente, debe traerse ya terminada de casa**, para evitar imprevistos que impidan su entrega durante esta sesión.
- Sobre esta imagen, comenzar a realizar en clase un estudio forense para tratar estudiar los archivos existentes, asegurando sus extensiones y buscando los posibles archivos borrados que en ella existan. Este proceso servirá para asegurar la validez de la imagen clonada en el punto anterior.

ENTREGA: (1) El fichero de la imagen clonada de la memoria USB.

8.3. Sesión 3

- En esta tercera sesión de prácticas, el profesor entregará a cada estudiante una imagen clonada de una memoria USB. El contenido de la misma es desconocido, aunque se sabe que tendrá el formato del ejemplo de las sesiones anteriores, esto es, habrá diez archivos con nombres genéricos, sin extensión, cinco de los cuales habrán sido borrados. Siguiendo la metodología ya conocida, la idea de esta sesión práctica es tratar de realizar un análisis forense sobre esta memoria USB que entrega el profesor.

ENTREGA: -

8.4. Práctica 1

La práctica 1 de la asignatura consistirá en el entregable que se detalla a continuación.

- En la sesión 2 de prácticas, debe entregarse:
 - (1) El **fichero de la imagen clonada** de la memoria propia (sesión 2).
 - (2) Un **informe** con el nombre y apellidos del autor del mismo, que incluya la tabla con los nombres de los archivos originales (con sus extensiones iniciales) y con el nombre genérico que se les ha asignado.
- El día programado en la agenda del estudiante como fecha de entrega de la práctica 1, en la tarea programada en el aula virtual de la asignatura, debe entregarse:

(3) Un **informe pericial** siguiendo el esquema habitual:

- Declaración de veracidad y presentación del perito
- Objeto del peritaje
- Alcance
- Antecedentes
- Fuentes de información y datos de partida
- Estándares y normas
- Limitaciones
- Resolución
- Conclusiones
- Anexos

El informe pericial debe ser simulado, indicando motivos inventados, currículum del perito inventado y siguiendo una línea argumental inventada y acorde a la situación que cada uno desee. Ha de indicarse que el perito ha realizado la fase de adquisición de pruebas de un disco duro (clonación, montaje, análisis...) y también de otro segundo disco duro que le ha facilitado otro perito (guardia civil/policía/perito, no debe indicarse que ha sido un compañero de clase, para mantener el hilo argumental del informe pericial profesional).

En el apartado de "Resolución" habrá que comentar todo lo realizado, parte por parte:

- Clonado de un disco duro
- Montaje del disco + recuperación de archivos + confirmación de extensiones

- Montaje del 2º disco + recuperación de archivos + confirmación de extensiones

Por último, como no se han usado discos duros, sino memorias USB preparadas para la "simulación", hay que añadir un anexo para el profesor, indicando cómo ha sido el proceso de creación de ese disco duro simulado: borrado seguro de memoria USB pequeña, búsqueda de archivos, eliminación de extensiones y nombres, copiado a la memoria USB y borrado de 5 archivos. Esta parte está claro que no habría que ponerla en un informe pericial real, es una parte académica que es preciso evaluar, y por eso se incluye como un anexo final al informe.