

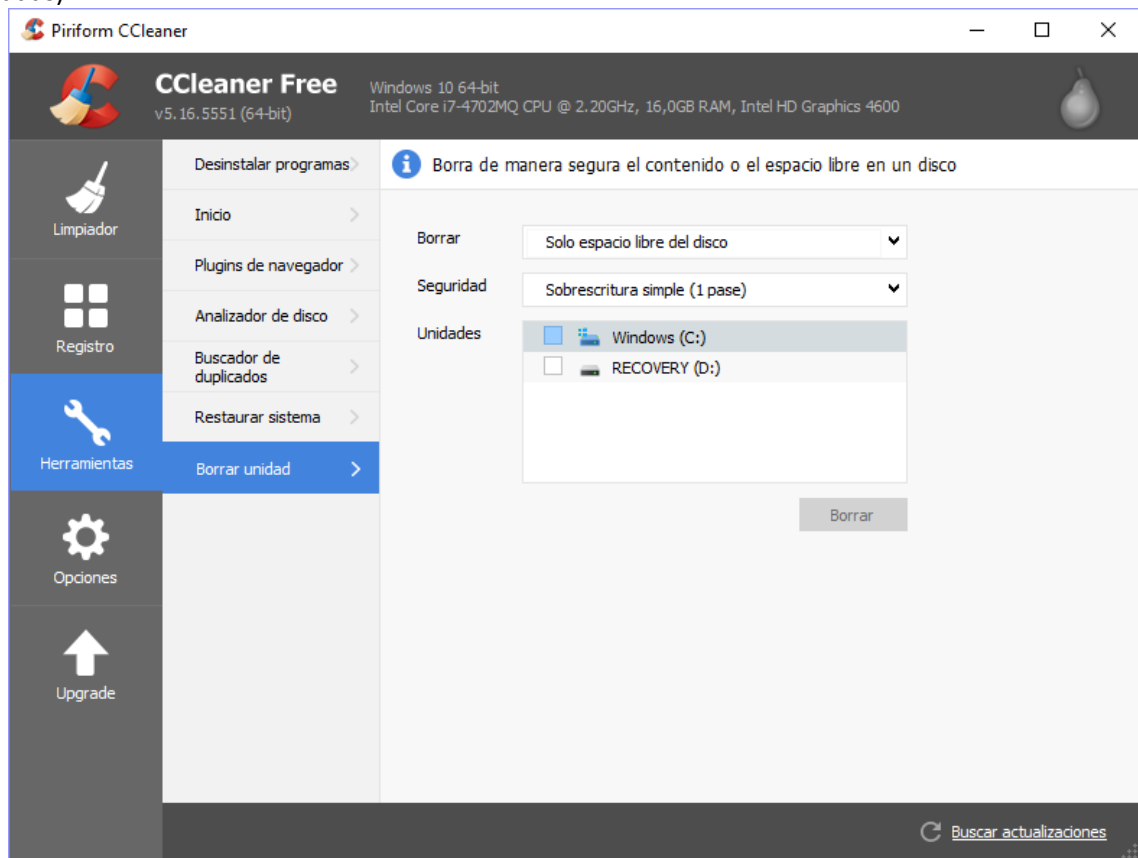
Borrado seguro

Hoy en día existe un gran número de aplicaciones que implementan el algoritmo de Gutmann para el borrado seguro de datos. Por ejemplo, para Windows son famosos CCleaner, Recuva o Darik's Boot and Nuke (este último para discos completos, únicamente). Los comandos shred, srm y wipe de Linux. Y para Mac OS X Disk Utility (discos enteros o espacio libre). Algunos de ellos disponen de versiones para múltiples plataformas.

CCLEANER (WINDOWS)

CCleaner es una herramienta orientada a optimizar el rendimiento de equipos Windows, eliminando archivos innecesarios y entradas no válidas en el registro de Windows. Además, permite realizar borrados de forma segura de un dispositivo completo.

En la siguiente imagen se observa esta posibilidad, donde se permite seleccionar si se desea realizar un borrado seguro del espacio libre del disco (recuérdese que el espacio libre contiene datos, ya que el borrado que se realiza es lógico y no físico sobre estas ubicaciones), o si se desea borrar toda la unidad (todos los archivos serían borrados). También permite configurar el nivel de seguridad con el que se realizará el borrado, permitiendo realizar una escritura simple (1 pase), avanzada (3 pasadas), compleja (7 pasadas) o muy compleja (35 pasadas).

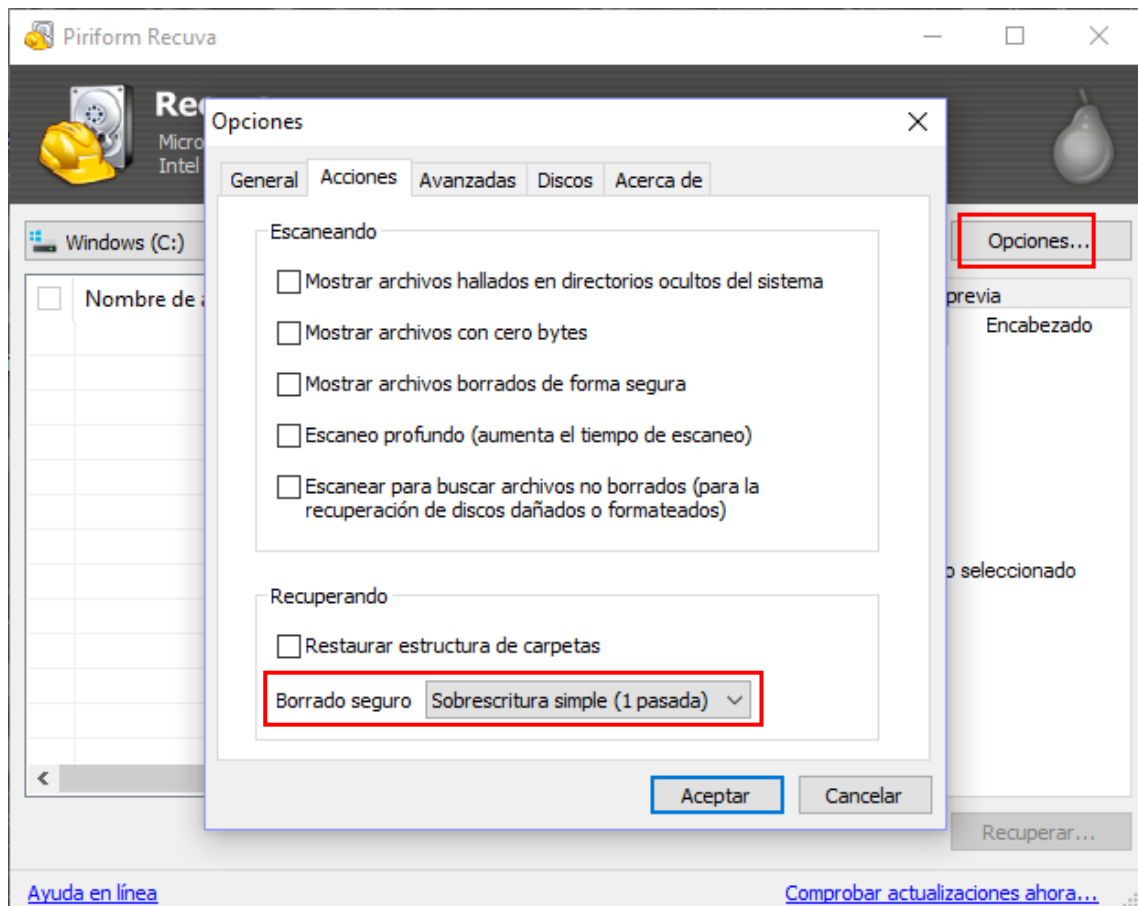


RECUVA (WINDOWS)

Recuva es un programa de recuperación de datos para Windows, que permite restaurar archivos que han sido borrados (marcados por el Sistema Operativo como espacio libre). Una opción interesante que tiene es que, en lugar de restaurar los archivos tras un borrado lógico, lo que puede interesar es realizar un borrado seguro de ese o esos archivos. Eso es posible seleccionando los archivos en cuestión y especificando (en el botón "Opciones")

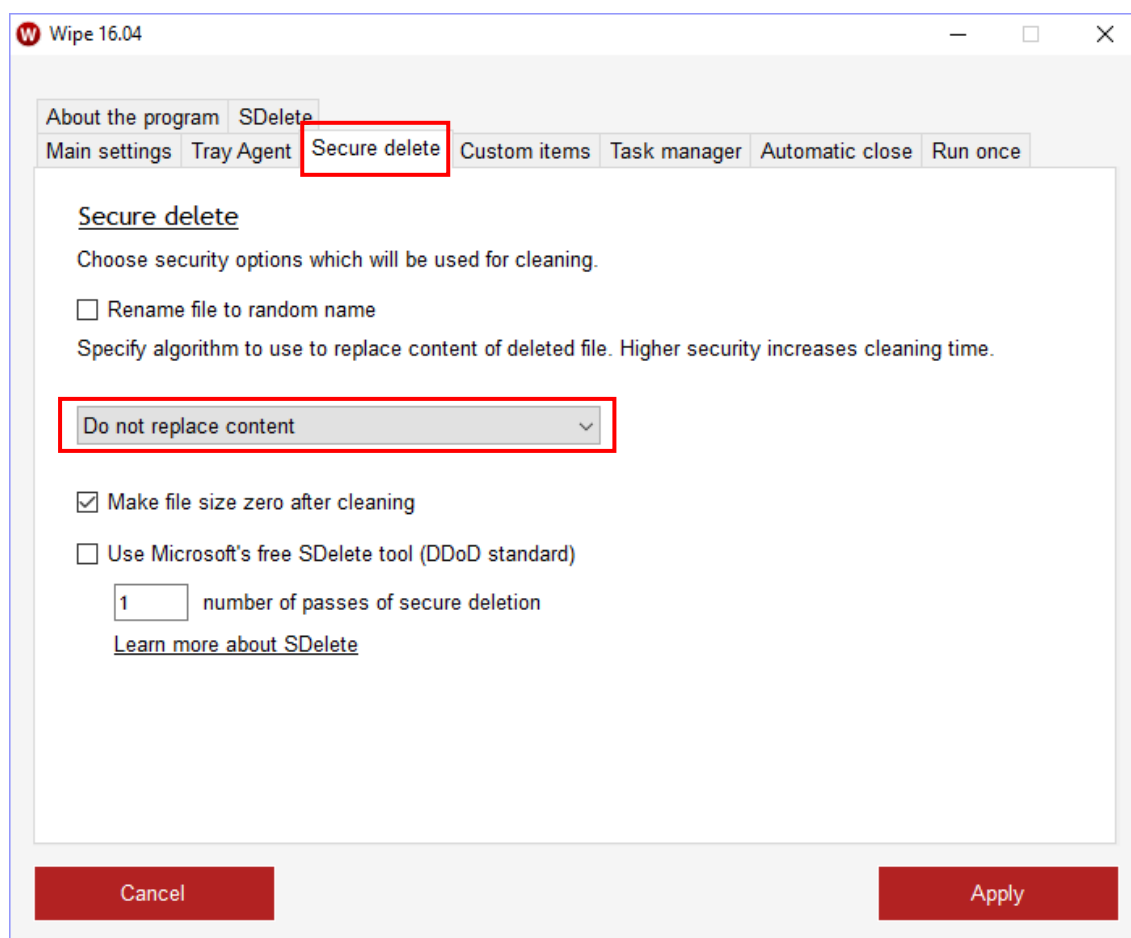
que se desea realizar un borrado seguro, que permite realizar mediante diferentes algoritmos de borrado seguro:

- Sobrescritura simple (1 pasada)
- DOD 5220.22-M (3 pasadas)
- NSA (7 pasadas)
- Gutmann (35 pasadas)



WIPE (WINDOWS)

Wipe es una aplicación que permite borrar el historial del navegador, la memoria cache, archivos index.dat, cookies, archivos temporales... Para la opción de borrado seguro es preciso seleccionar el botón "Settings" (Configuración) en la pantalla principal, mostrándose la siguiente pantalla:



En la pestaña “Secure delete” (borrado seguro) se puede seleccionar el algoritmo utilizado para sobrescribir los archivos borrados, que puede ser:

- No reemplazar el contenido
- 1 pasada (el mismo bloque aleatorio)
- 1 pasadas (cada vez un nuevo bloque aleatorio)
- 3 pasadas (el mismo bloque aleatorio)
- 3 pasadas (cada vez un nuevo bloque aleatorio)
- 7 pasadas (el mismo bloque aleatorio)
- 7 pasadas (cada vez un nuevo bloque aleatorio)
- Método de Peter Gutmann
- DDoD US Standard
- Russian GOST

Por desgracia, la mayoría de estas opciones sólo están disponibles en la versión PRO.

DARIK'S BOOT AND NUKE (SISTEMA DE ARRANQUE)

La aplicación **Darik's Boot and Nuke** se descarga como una ISO, y consiste en una mini-distribución Linux que se puede copiar en una memoria USB. Arrancando el ordenador desde esa memoria USB se lanza la aplicación.

Darik's Boot and Nuke

Warning: This software irrecoverably destroys data.

This software is provided without any warranty; without even the implied warranty of merchantability or fitness for a particular purpose. In no event shall the software authors or contributors be liable for any damages arising from the use of this software. This software is provided "as is".

<http://www.dban.org/>

- * Press the F2 key to learn about DBAN.
- * Press the F3 key for a list of quick commands.
- * Press the F4 key to read the RAID disclaimer.
- * Press the **ENTER** key to start DBAN in interactive mode.
- * Enter autonuke at this prompt to start DBAN in automatic mode.

boot: _

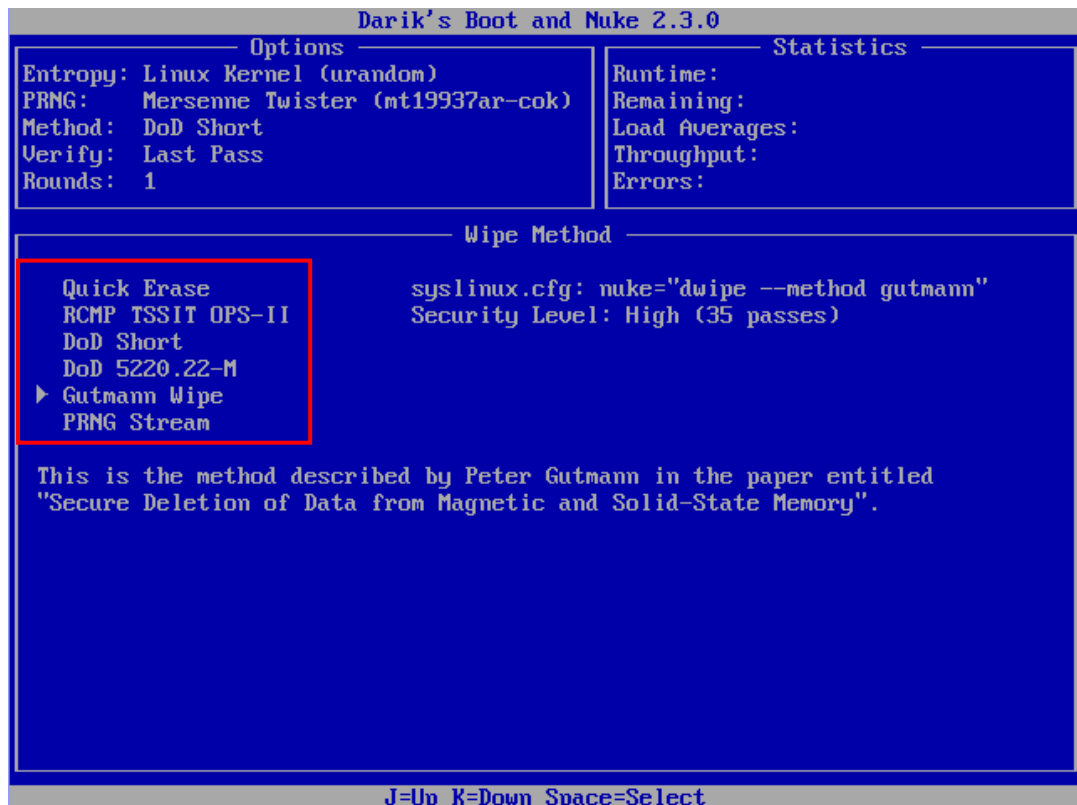
Pulsando ENTER para iniciar DBAN, se pasa a la siguiente pantalla:

Darik's Boot and Nuke 2.3.0	
Options	Statistics
Entropy: Linux Kernel (urandom)	Runtime:
PRNG: Mersenne Twister (mt19937ar-cok)	Remaining:
Method: DoD Short	Load Averages:
Verify: Last Pass	Throughput:
Rounds: 1	Errors:

Disks and Partitions	
▶ [wipen] ATA Disk VBOX HARDDISK 1.0 8GiB (8589MB) VB42db169f-1f1f4378	

P=PRNG M=Method U=Verify R=Rounds, J=Up K=Down Space=Select, F10=Start	
---	--

Tras seleccionar la unidad de disco a borrar, se elige el método de borrado (M).



Como puede apreciarse, es posible seleccionar alguno de los siguientes métodos de borrado seguro:

- Quick Erase (1 pasada, seguridad baja)
- RCMP TSSIT OPS-II (8 pasadas, seguridad media)
- DoD Short (3 pasadas, seguridad media)
- DoD 5220.22-M (7 pasadas, seguridad media)
- Gutmann Wipe (35 pasadas, seguridad alta)
- PRNG Stream

COMANDO SHRED (LINUX)

El comando **shred** de linux sobrescribe varias veces el archivo o archivos indicados (25 veces, por defecto). Utiliza varios patrones de texto, transformando el archivo original en otro totalmente distinto y con información sin sentido. El ejemplo más sencillo sería:

```
root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~# nano borrame.txt
root@kali:~# cat borrame.txt
archivo a borrar para DTIF
root@kali:~# shred borrame.txt
root@kali:~# ls borrame.txt
borrame.txt
root@kali:~# cat borrame.txt
!P0,NU00/K00Y038Y3"iU000b00*000[HH]0[0]0e0e0s0[HH]'00[0]
00F00H'0P000[0]00 10[0]000U30b0o00<0J040090%0X$!0{0[0]000F:0[0]0 0.zJ0a00%[0]u?00q0E0000
[0]00C!0Y[0]0:000ww

00}0
0#0tSM02t0#hh0!0I0?B0|KG0:y.000%x0[0]0;0ntw00
0e0Kt00/ZX0000 0Mv0lhT0]c0000w-00[0];0[0]00kF000?{m0h0m00BJ0[HH]G"000[0]00E-00000B-io0[0]G
00bI02010[0]0/U0000{09*[0]0[0]0[0]0t{00ST 0000 P[00[0]
90@0[000H}
000S70b0i[0]0[0]0,0[0]0<000+000-0"0H0ãe00000SE0[HH]040=000d0[0]0/A[0]0[0]0I0:000>00[0]0000y0;
[0]00Y09h[0]0o000X'00U0mDU^_k0S0z[0]0#00t0590'h
1c[0]0000pm000>0b200000Z??[0]0000r0Se000=[0]0000"04A[0]0[0]0[0]0[0]0SAK0^00Cq0000[(t[0]0[0]0?0D00
)0P[0]0[0]I0/0[0]0[0]0[0]0?0[0]#a0=000
0<000"003l000M0y0[0]0Se0i700T[0]0[0].{00V0^0[0]0,0b0@0)00YD0 0U0[0]0[0]0P0400G>t0U 0yb[0]
0000000[0]0[0]00D<Δπ0 00K[0]0[0]2ss[0]08'0*80@0000[0]0[0]0c0900'Z0g00)a~0I
/0[0]6RngJz0Q0060(
=000040Tw00000N/'0000)z@000-Z0#00*0[0]00*G[0]0[0]~κ00bItC)o{90A001z
```

Como se aprecia en la imagen anterior, se ha creado un archivo llamado **borrame.txt** (con el comando **nano**), que contiene el texto “archivo a borrar para DTIF”. Posteriormente, se especifica que se desea borrar de forma segura al archivo **borrame.txt** mediante el comando:

```
root@kali:~# shred borrame.txt
```

En realidad, el archivo no se elimina, sino que se transforma después de las múltiples pasadas, como puede observarse al visualizar su contenido con el comando **cat**.

Para eliminar el archivo, debe usarse la opción **-u**:

```
root@kali:~# shred -u borrame.txt
root@kali:~# ls borrame.txt
ls: no se puede acceder a borrame.txt: No existe el fichero o el directorio
root@kali:~#
```

Este comando puede eliminar directorios y unidades por completo.

COMANDO SRM (LINUX)

Otra posibilidad más avanzada para realizar un borrado seguro en Linux consiste en el comando **srm**, cuya instalación se realiza así:

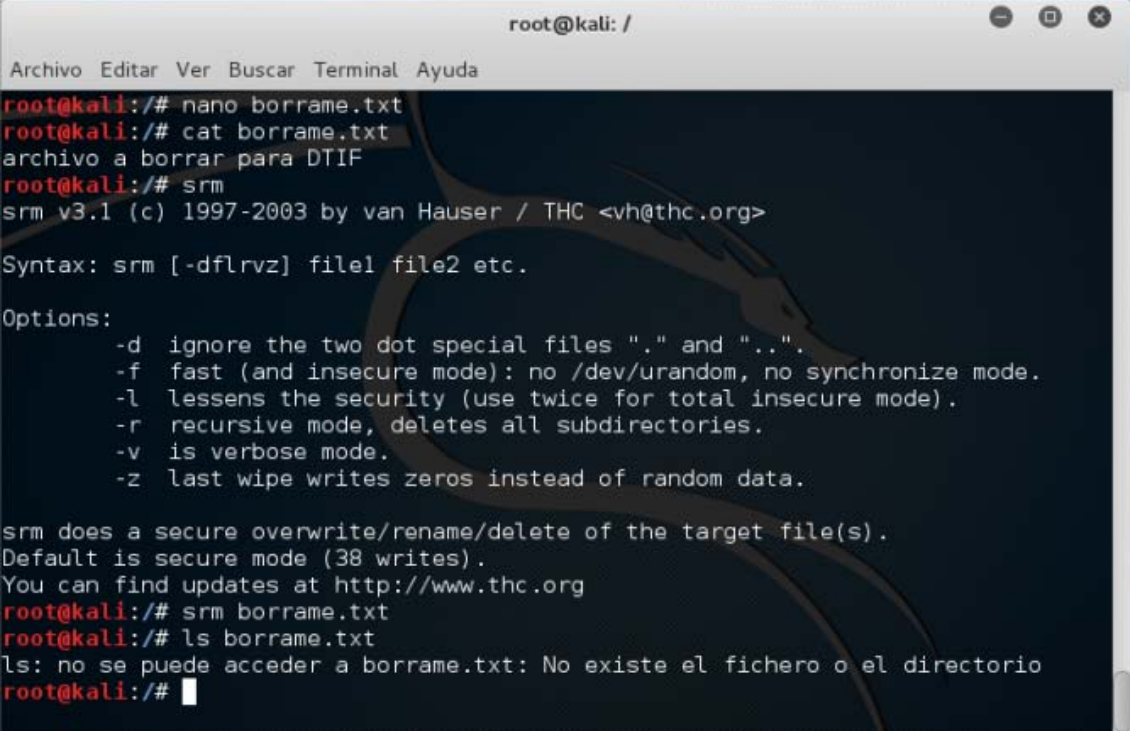
```
root@kali:~# apt-get install secure-delete
```

A diferencia del comando **shred**, en vez de sobrescribir los archivos con datos aleatorios, utiliza valores obtenidos mediante el algoritmo de Gutmann para sobrescribir los archivos.

El proceso de borrado seguro de datos con **shred** es el siguiente:

- 1 pasada con 0xff
- 5 pasadas aleatorias
- 27 pasadas con valores especiales definidas por el algoritmo de Gutmann
- 5 pasadas aleatorias
- Se cambia el nombre del archivo a un valor aleatorio
- Se trunca (fragmenta) el archivo

Realizando las mismas acciones que antes (se crea un archivo llamado **borrame.txt** y se muestra su contenido), a continuación se invoca al comando **srm** para ver sus opciones y, finalmente se elimina de forma segura el archivo **borrame.txt**.

A screenshot of a terminal window titled 'root@kali: /'. The terminal shows the following commands and output:

```
root@kali:~# nano borrame.txt
root@kali:~# cat borrame.txt
archivo a borrar para DTIF
root@kali:~# srm
srm v3.1 (c) 1997-2003 by van Hauser / THC <vh@thc.org>

Syntax: srm [-dflrvz] file1 file2 etc.

Options:
  -d ignore the two dot special files "." and "..".
  -f fast (and insecure mode): no /dev/urandom, no synchronize mode.
  -l lessens the security (use twice for total insecure mode).
  -r recursive mode, deletes all subdirectories.
  -v is verbose mode.
  -z last wipe writes zeros instead of random data.

srm does a secure overwrite/rename/delete of the target file(s).
Default is secure mode (38 writes).
You can find updates at http://www.thc.org
root@kali:~# srm borrame.txt
root@kali:~# ls borrame.txt
ls: no se puede acceder a borrame.txt: No existe el fichero o el directorio
root@kali:~#
```

COMANDO WIPE (LINUX)

Otra posibilidad para el borrado seguro en Linux es mediante el comando **wipe**, el cual tiene un funcionamiento muy rápido. Para su instalación, basta con teclear:

```
root@kali:~# apt-get install wipe
```

En la línea de los ejemplos anteriores, creando el archivo **borrame.txt** la siguiente imagen muestra cómo eliminar este archivo con **wipe**.

```
root@kali: /
Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~# nano borrame.txt
root@kali:~# cat borrame.txt
archivo a borrar para DTIF
root@kali:~# wipe -f borrame.txt
Operation finished.
1 file wiped and 0 special files ignored in 0 directories, 0 symlinks removed but not followed, 0 errors occurred.
root@kali:~# ls borrame.txt
ls: no se puede acceder a borrame.txt: No existe el fichero o el directorio
root@kali:~#
```

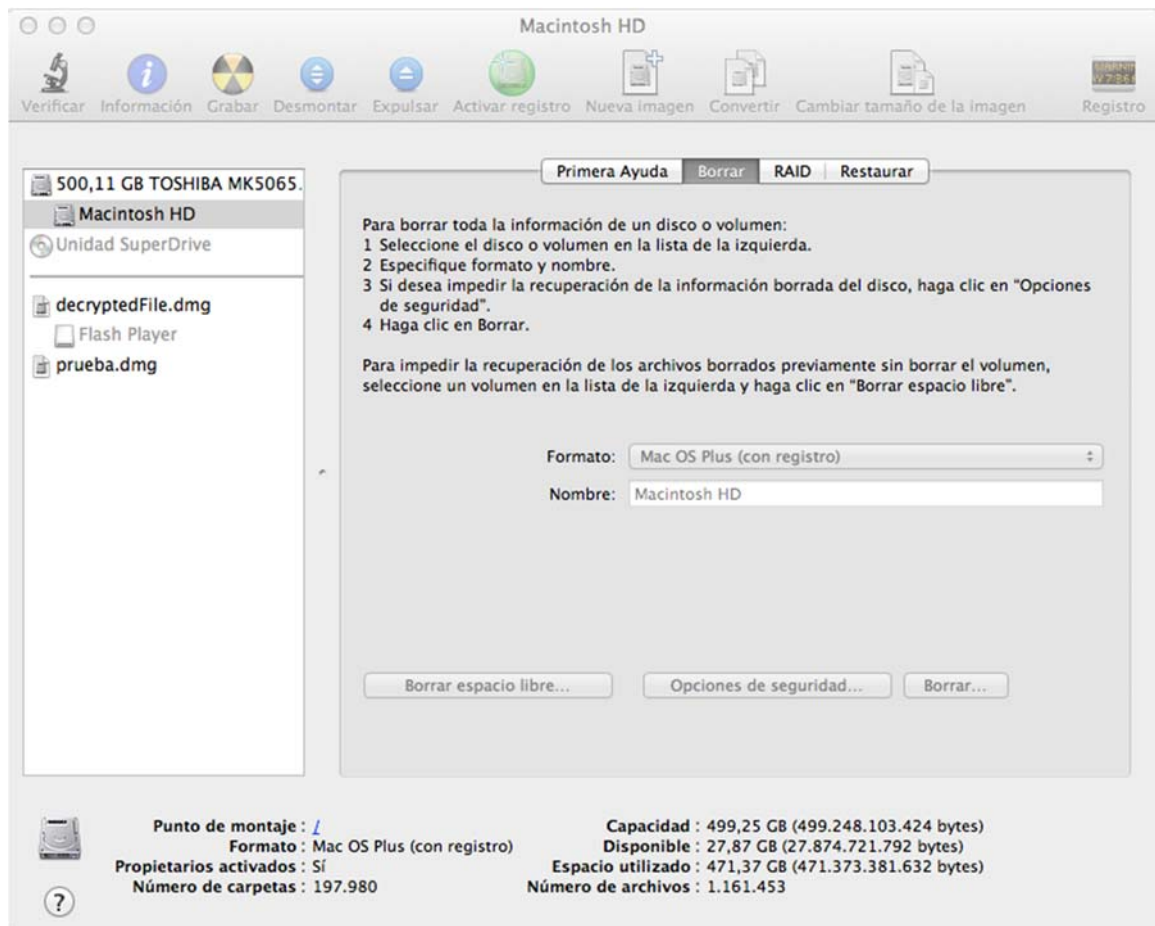
Indicar que, por defecto, se utiliza el algoritmo de Gutmann (35 pasadas). El parámetro `-f` indica que no es necesario pedir confirmación de borrado (no solicita que tecleemos Yes/No para proceder al borrado del archivo, lo cual es más cómodo para el usuario).

DISK UTILITY (Mac OS X)

Desde la versión OS X 10.4 (Tiger) hasta la OS X 10.10 (Yosemite) se podía eliminar información de forma segura, simplemente moviéndola a la papelera y seleccionando la opción “Vaciar la papelera de forma segura” en el Finder. En la última versión OS X 10.11 (El Capitán), Apple la eliminó del sistema operativo porque dicha opción no funciona con los discos SSD que actualmente están cada vez más implantados en los equipos. Pero de todas maneras, para prevenir la recuperación forense de la información borrada, se debe utilizar la aplicación UTILIDADES DE DISCO (DISK UTILITY).



Esta aplicación permite eliminar la información de forma segura, tanto de discos o particiones, como del espacio libre.



A la hora de **borrar la información de discos**, se tienen 4 niveles de seguridad:

- Más rápido, borra los archivos pero es posible que alguna aplicación de recuperación de discos pueda volver a recuperarlos.
- El siguiente nivel escribe ceros en todo el disco en un único paso y se sobrescriben los datos una vez.
- Borrado seguro en 3 pasos. Se borra la información y se sobrescriben los datos 3 veces.
- Por último y el más seguro, sigue el estándar 5220-22 M del Departamento de Defensa de EEUU. Los datos son eliminados y sobrescritos 7 veces.

Si se quisiera borrar el contenido de un Mac de forma segura, habría que iniciar el equipo desde una unidad externa o diferente al disco de arranque. También se pueden borrar de forma segura los archivos eliminados y a los que no se quiera que se pueda acceder.

Para hacer un **borrado del espacio libre**, se tienen 3 niveles de seguridad:

- Opción más rápida, se escriben ceros sobre el espacio no utilizado del disco una sola vez.
- Borrado seguro en 3 pasos. Se sobrescribe 3 veces el espacio no utilizado del disco. Este nivel cumple el estándar del Departamento de Energía de los Estados Unidos.
- Por último y el más seguro, sigue el estándar 5220-22 M del Departamento de Defensa de EEUU. Se sobrescribe 7 veces el espacio no utilizado del disco.

7 pass overwrite data (DoD 5220.22-M specification)		
Pass	Data written	
	Binary notation	Hexadecimal notation
1	11110110	0xF6
2	00000000	0x00
3	11111111	0xFF
4	Random	Random
5	00000000	0x00
6	11111111	0xFF
7	Random	Random

Esta opción es la más segura que se puede seleccionar mediante el interfaz gráfico de esta aplicación (7 pasadas). Sin embargo, si se arranca desde el modo comandos, aún se puede borrar el espacio libre con el algoritmo de Gutmann. El comando sería `diskutil secureErase` seleccionando el nivel de seguridad deseado.

```
$ diskutil secureErase
Usage: diskutil secureErase [freespace] level MountPoint|DiskIdentifier|DeviceNode
Securely erases either a whole disk or a volume's freespace.
Level should be one of the following:
    0 - Single-pass zeros.
    1 - Single-pass random numbers.
    2 - US DoD 7-pass secure erase.
    3 - Gutmann algorithm 35-pass secure erase.
    4 - US DoE 3-pass secure erase.
Ownership of the affected disk is required.
Note: Level 2, 3, or 4 secure erases can take an extremely long time.
```