

[Inicio](#) » Borrado seguro de información

Borrado seguro de información

15/06/2017

Introducción

Con base en la [circular DGTIC/003/2017](#) se presenta esta guía para el borrado seguro de información almacenada en medios digitales que vayan a ser dados de baja o eliminados por parte de alguna dependencia UNAM. El proceso de borrado seguro consiste en sobrescribir al menos una vez con un valor definido, por ejemplo 0, la información almacenada en el medio¹. De manera alternativa, el uso de otros valores o más pases puede ser utilizado.

En esta guía se muestra el proceso de eliminación de datos de forma segura en los sistemas operativos:

- [Windows](#)
 - [SDelete](#) (versión 2.04)
 - [Hddguru \(Wipe My Disks\)](#) (versión 1.10)
- [MacOS](#)
 - [Permanent eraser](#) (versión Mac OS X 10.6+)
 - [Disk Utility](#) (versión Mac OS X 10.13+)
- [GNU/Linux](#)
 - [srm](#)
 - [Ubuntu 21.10](#) (versión 3.1-7)
 - [Ubuntu 20.04](#) (versión 3.1-6ubuntu2)
 - [Debian 11](#) (versión 3.1-6)
 - [Debian 10](#) (versión 3.1-6)
 - [CentOS 8](#) (versión 1.2.15-12.el8)

- CentOS 7 (versión 1.2.15-1.el7)
- Fedora 37 (versión 1.2.15-16.fc36)
- Fedora 36 (versión 1.2.15-16.fc36)
- Fedora 35 (versión 1.2.15-15.fc35)
- SUSE (versión 1.2.15-bp154.1.5)
- [wipe](#)

- Ubuntu 21.10 (versión 0.24-7)
- Ubuntu 20.04 (versión 0.24-6)
- Debian 11 (versión 0.24-7)
- Debian 10 (versión 0.24-4)
- CentOS 8 (versión 0.30-1.el8)
- CentOS 7 (versión 0.24-2.el7)
- Fedora 37 (versión 0.21-25.fc36)
- Fedora 36 (versión 0.21-25.fc36)
- Fedora 35 (versión 0.21-24.fc35)
- SUSE (versión 2.3.1-bp154.1.5)

Formato

El formato de [Responsiva de borrado de información en equipo de cómputo dado de baja por obsolescencia](#) se encuentra en el sitio web de la [Dirección General del Patrimonio Universitario](#) en el menú Normativos sección [descargas](#).

Windows

En sistemas operativos Windows, se tienen las siguientes herramientas para el eliminado seguro de información:

- SDelete
- Hddguru (Wipe My Disks)

SDelete

Es una herramienta de borrado seguro que forma parte de la Suite de Sysinternals e implementa el estándar DOD5220.22-M de sanitizado y eliminación del Departamento de Defensa de Estados Unidos.

Esta herramienta está disponible tanto para sistemas de 32 y 64 bits, y solo puede ser ejecutada mediante línea de comandos.

Para ejecutar la herramienta SDelete, se tiene que [descargar](#), descomprimir, abrir la aplicación cmd.exe y ejecutar la aplicación pasando como parámetro el directorio que se quiere eliminar de forma segura.

Como se puede apreciar en el siguiente ejemplo:

```
Administrator: Command Prompt

C:\Users\unamcert\Downloads\SDelete>sdelete64.exe datos.txt

SDelete v2.04 - Secure file delete
Copyright (C) 1999-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

SDelete is set for 1 pass.
C:\Users\unamcert\Downloads\SDelete\datos.txt...deleted.

Files deleted: 1

C:\Users\unamcert\Downloads\SDelete>
```

De forma predeterminada el programa sobrescribe una sola vez el archivo, esta opción puede ser modificada utilizando el parámetro `-p <número>`, entre más veces se sobrescriba el archivo más tiempo tardará el proceso de borrado seguro.

```
Administrator: Command Prompt

C:\Users\unamcert\Downloads\SDelete>sdelete64.exe -p 30 datos.txt

SDelete v2.04 - Secure file delete
Copyright (C) 1999-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

SDelete is set for 30 passes.
No files/folders found that match datos.txt.

C:\Users\unamcert\Downloads\SDelete>
```

También se pueden eliminar de forma recursiva directorios que contengan archivos utilizando el parámetro `-s`, como se muestra en el siguiente ejemplo:

```
Administrator: Command Prompt

C:\Users\unamcert\Downloads\SDelete>sdelete64.exe -p 10 -s .\otrosArchivos

SDelete v2.04 - Secure file delete
Copyright (C) 1999-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

SDelete is set for 10 passes.
.\otrosArchivos\nuevosArchivos\AdministracionDHCP.ps1...deleted.
.\otrosArchivos\nuevosArchivos\Aplicacion.exe...deleted.
.\otrosArchivos\nuevosArchivos\Aplicacion2.exe...deleted.
.\otrosArchivos\nuevosArchivos\datos.txt...deleted.
.\otrosArchivos\AdministracionDHCP.ps1...deleted.
.\otrosArchivos\Aplicacion.exe...deleted.
.\otrosArchivos\Aplicacion2.exe...deleted.
.\otrosArchivos\datos.txt...deleted.

Files deleted: 8
Directories deleted: 2

C:\Users\unamcert\Downloads\SDelete>
```

Hddguru (Wipe My Disks)

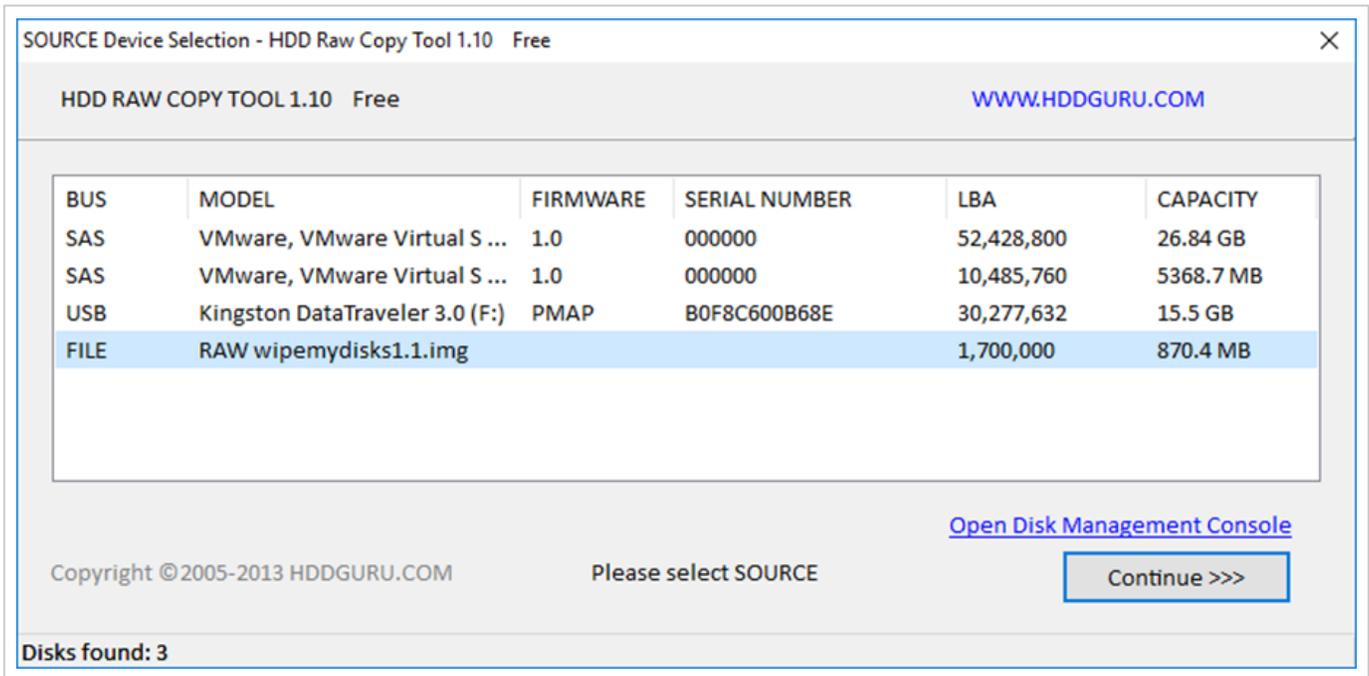
Esta herramienta permite el borrado total (formato a bajo nivel) de un disco o partición. La herramienta eliminará todas las particiones y sistemas de archivos sin importar el sistema operativo instalado en el sistema.

La herramienta es proporcionada como un archivo de imagen y se necesita copiar en una memoria flash para poder ejecutar la aplicación en la secuencia de arranque, como se realiza la instalación de un sistema operativo tradicionalmente.

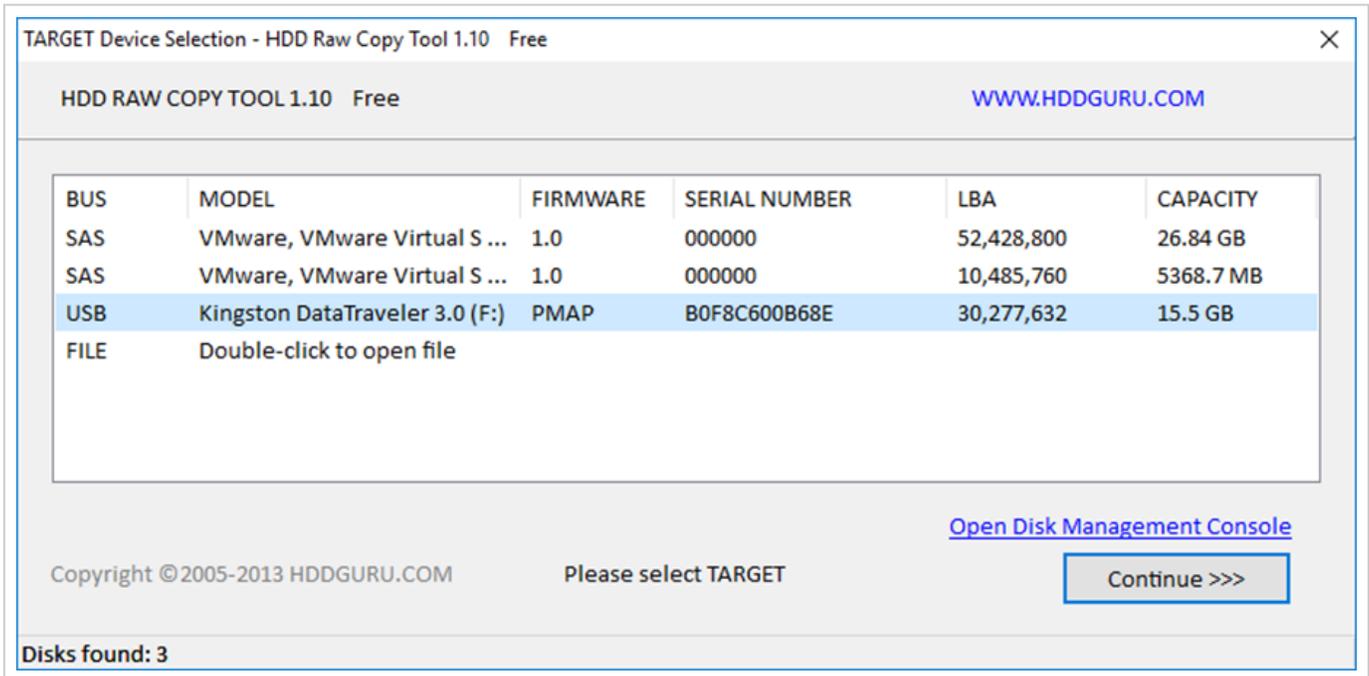
Para poder utilizar la aplicación se necesita copiar la imagen en una memoria flash, se puede utilizar la utilidad dd en GNU/Linux con la imagen raw o utilizando la aplicación HDD Raw Copy Tool, como se muestra a continuación:

Se tiene que descargar la [imagen en formato RAW](#) y [HDD Raw Copy Tool](#), descomprimir la imagen "wipemydisks1.1.img.zip" e insertar la memoria flash que servirá como medio para ejecutar la aplicación en la secuencia de arranque del equipo de dónde se eliminará la información en la unidad de almacenamiento.

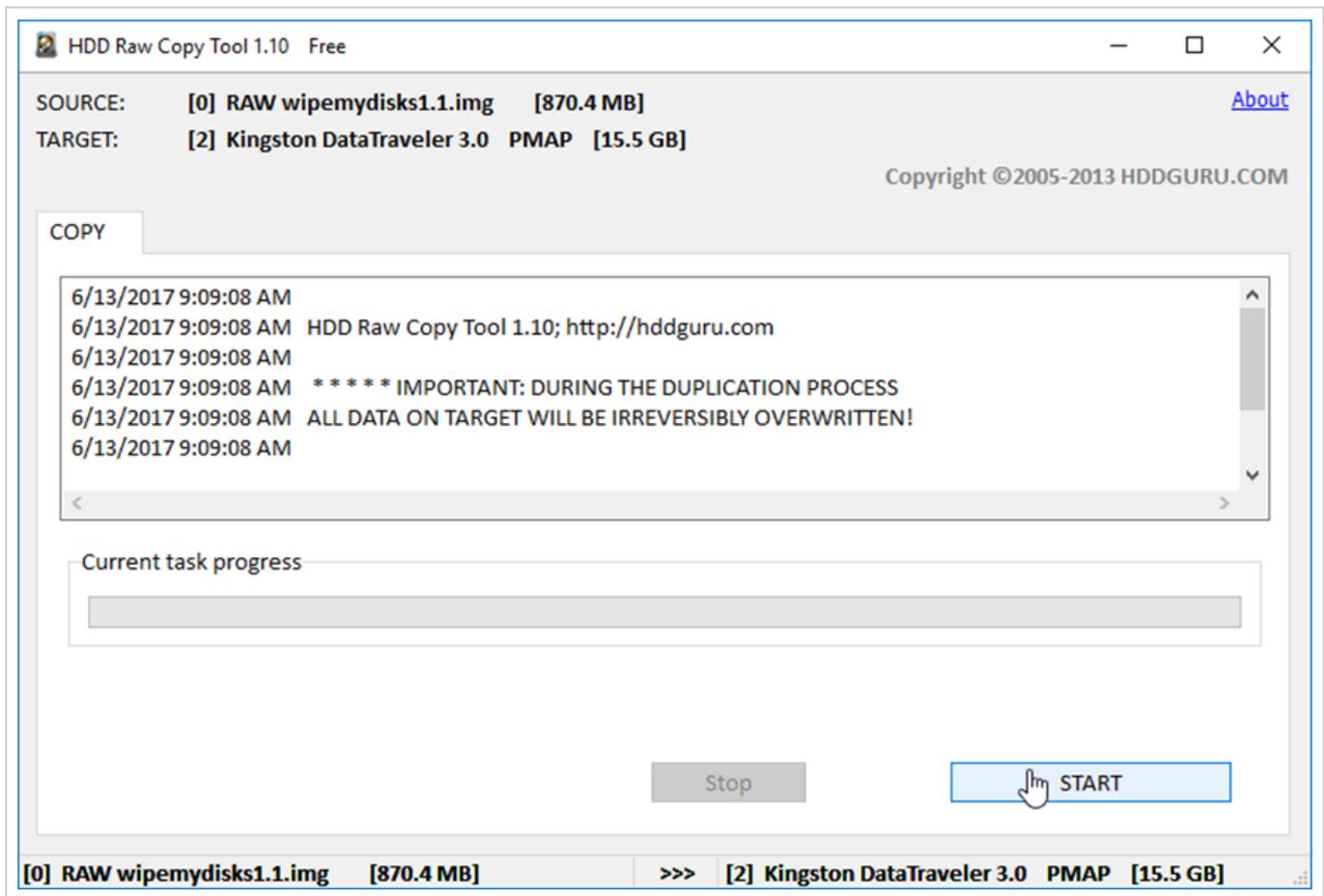
Una vez que ya se tiene descomprimido el archivo de la imagen, se deberá ejecutar la herramienta HDDRawCopy1.10Portable.exe con permisos de administrador, se mostrará una ventana que solicita el archivo origen, se deberá dar doble clic en la opción "Double-click to open file" y seleccionar el archivo que fue descomprimido.



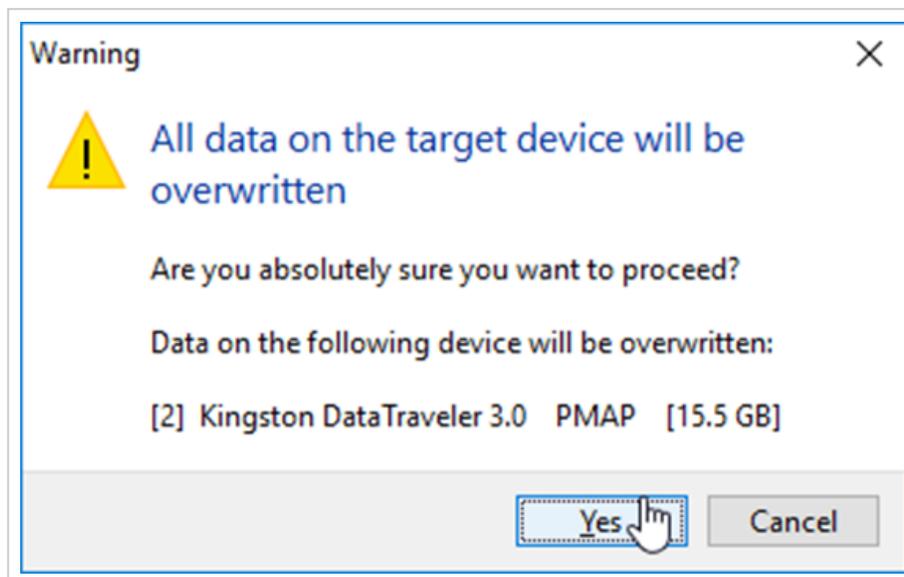
En la siguiente etapa se debe de seleccionar el dispositivo destino dónde serán copiados todos los archivos de la imagen previamente seleccionada y se deberá seleccionar la memoria flash.



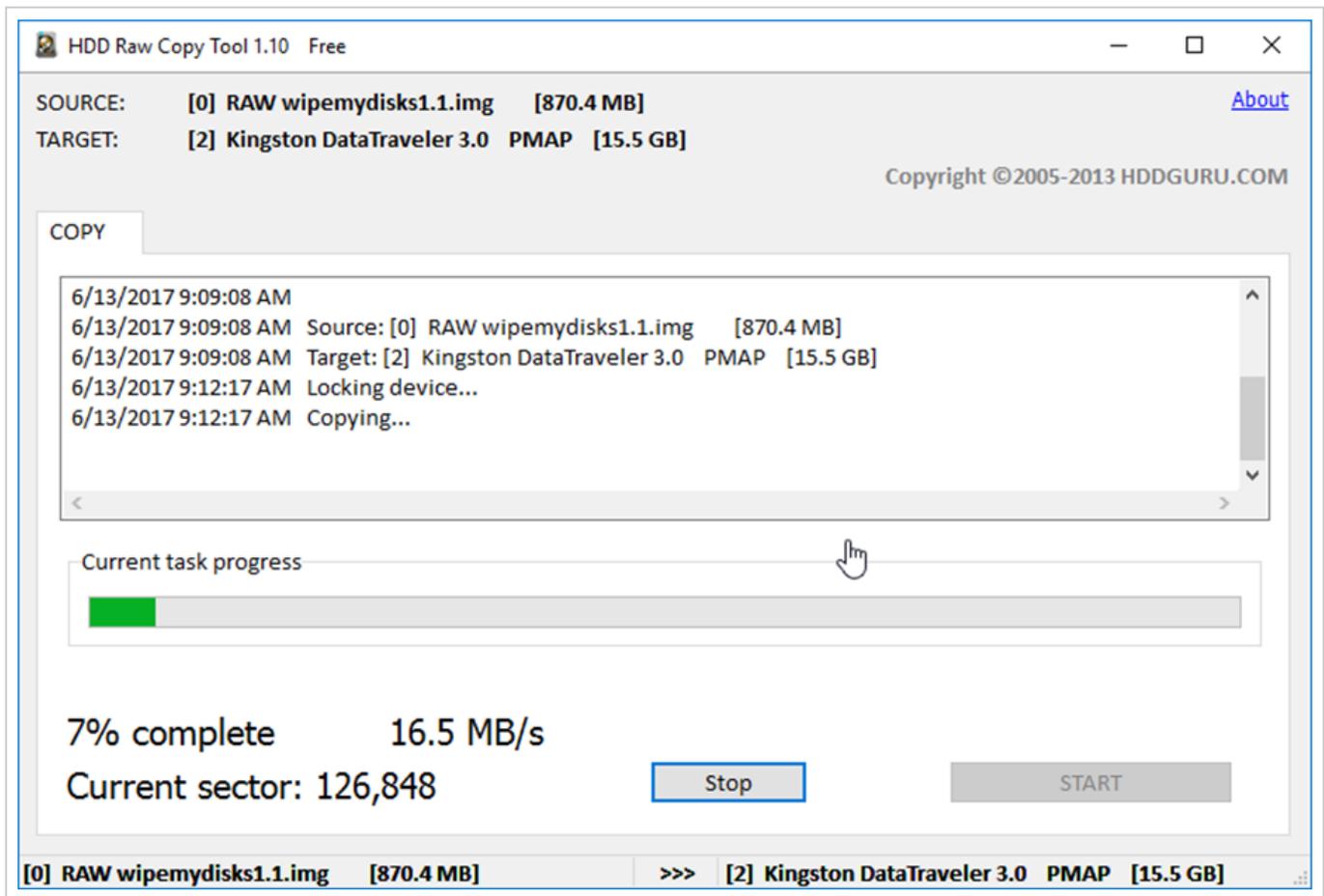
A continuación, se debe de dar clic en el botón "Start".



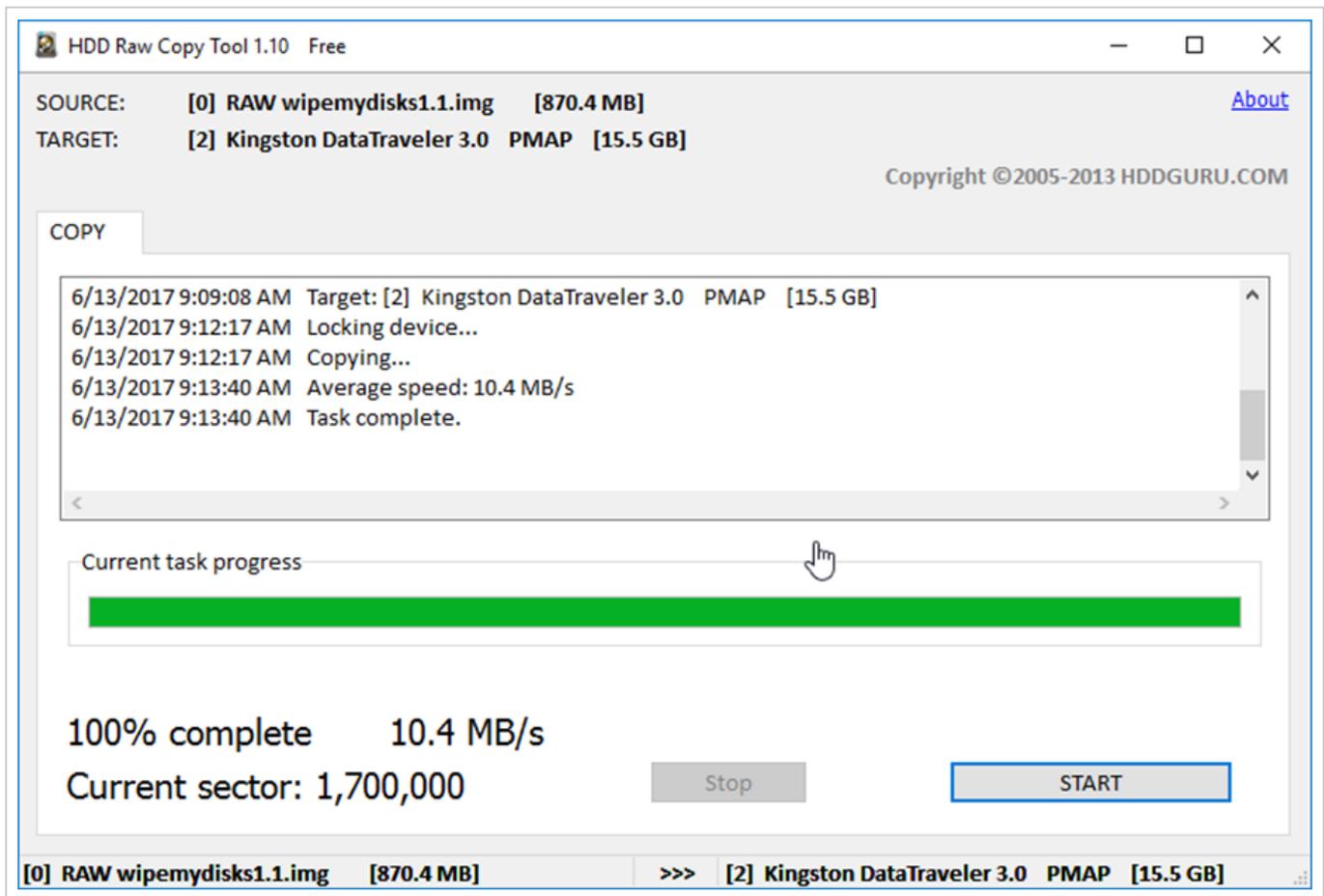
La aplicación solicita una confirmación de que se sobrescribirán todos los datos en el dispositivo destino. Se deberá de dar clic en el botón “Yes”.



A continuación, iniciará el proceso de copiado de archivos en la memoria flash.

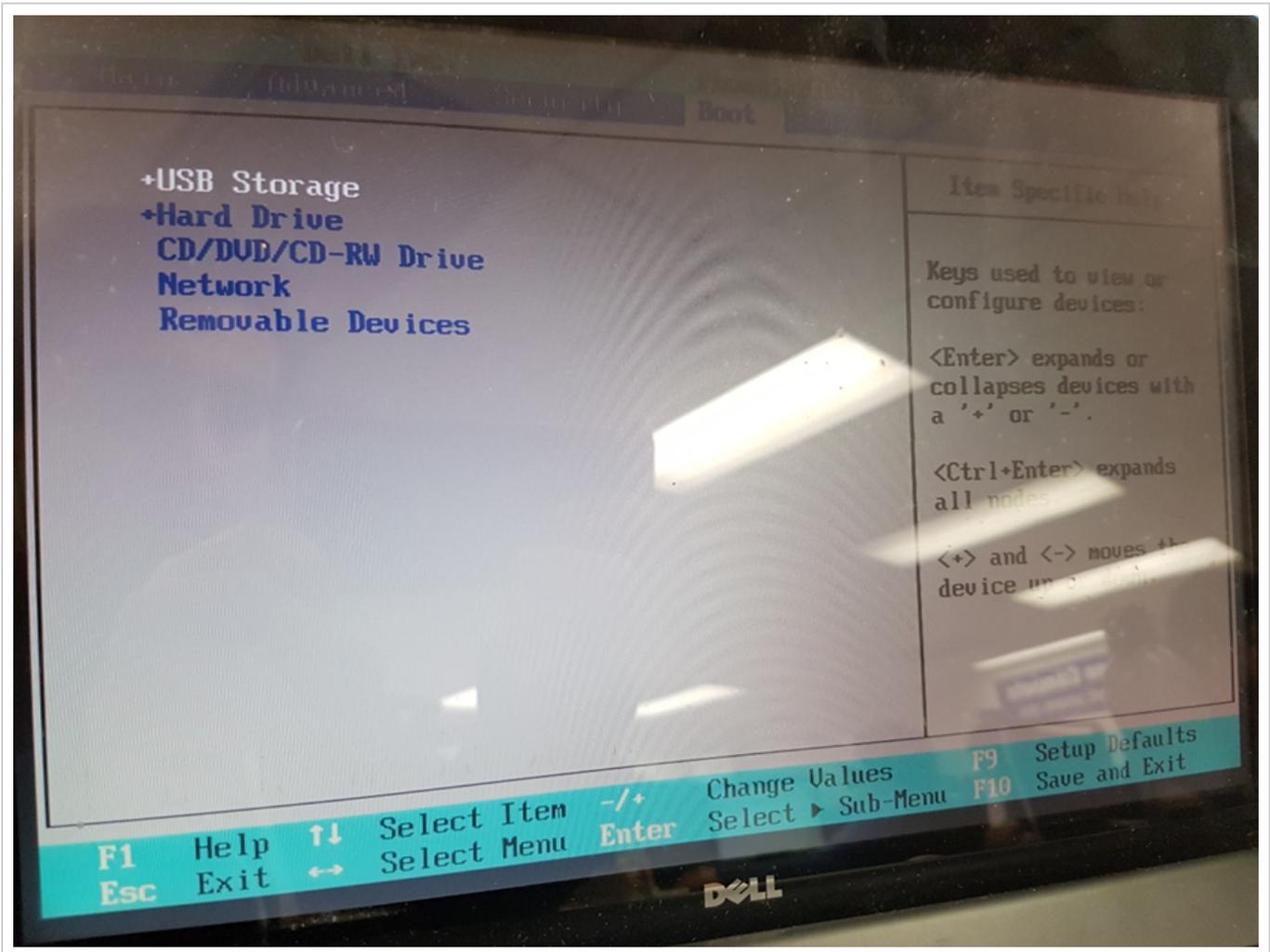


Al finalizar deberá aparecer una ventana como la siguiente:



Ahora se deberá de desconectar la memoria flash e insertar en el equipo que contiene la unidad de almacenamiento que se quiere borrar de forma segura.

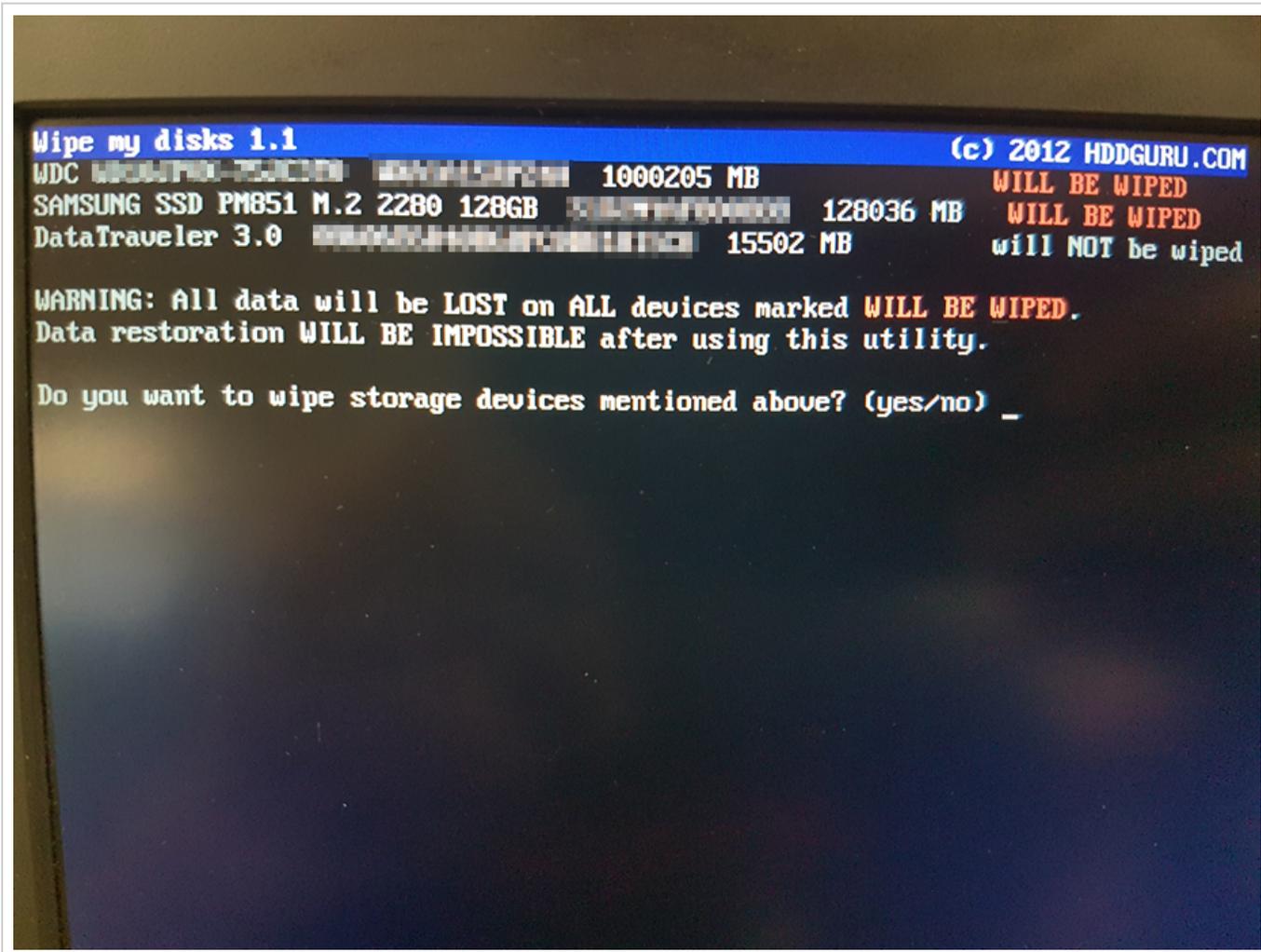
Una vez insertada la memoria en el equipo se deberá cambiar la secuencia de arranque, indicando en primer lugar la memoria flash.



Los archivos que contiene la memoria serán inicializados en la memoria RAM del equipo para poder utilizar la aplicación de eliminación segura de datos. La aplicación detectará automáticamente las unidades de almacenamiento conectadas al equipo.

NOTA: Se deberá conectar al equipo solo las unidades de almacenamiento que serán eliminadas por la aplicación de Wipe My Disks

Se deberá escribir la palabra "Yes" para confirmar que la información de los dispositivos conectados será eliminada.



MAC OS

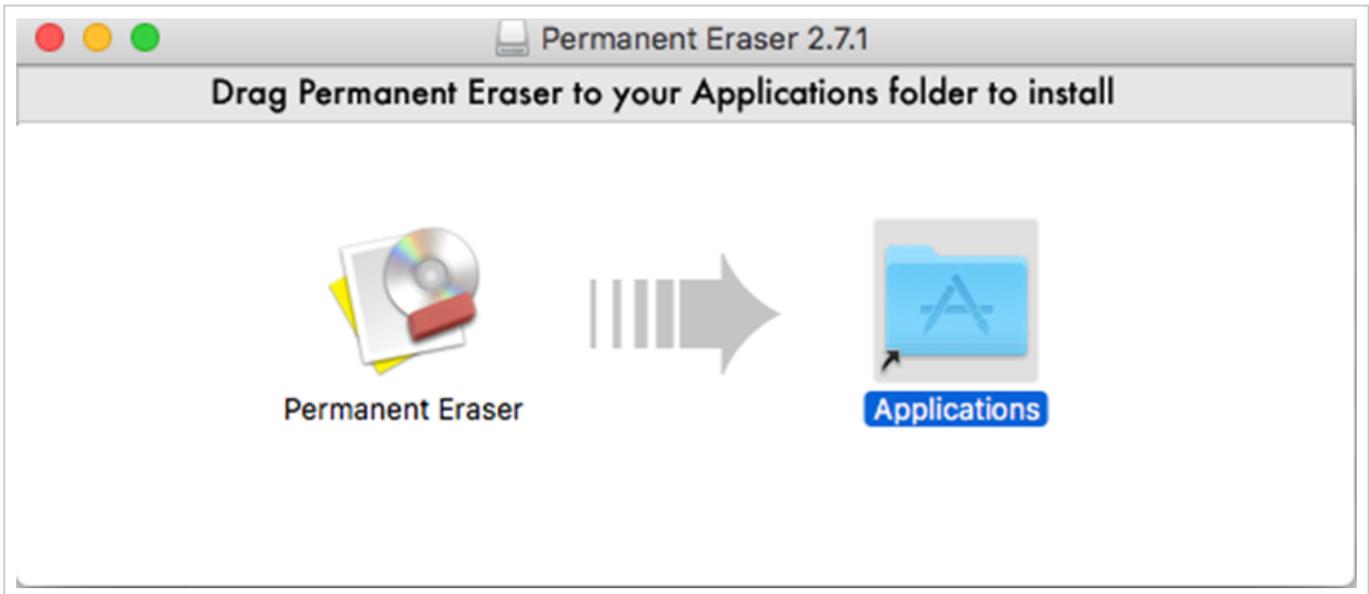
En sistemas operativos MAC OS, se tienen las siguientes herramientas para el eliminado seguro de información:

- Permanent eraser
- Disk Utility

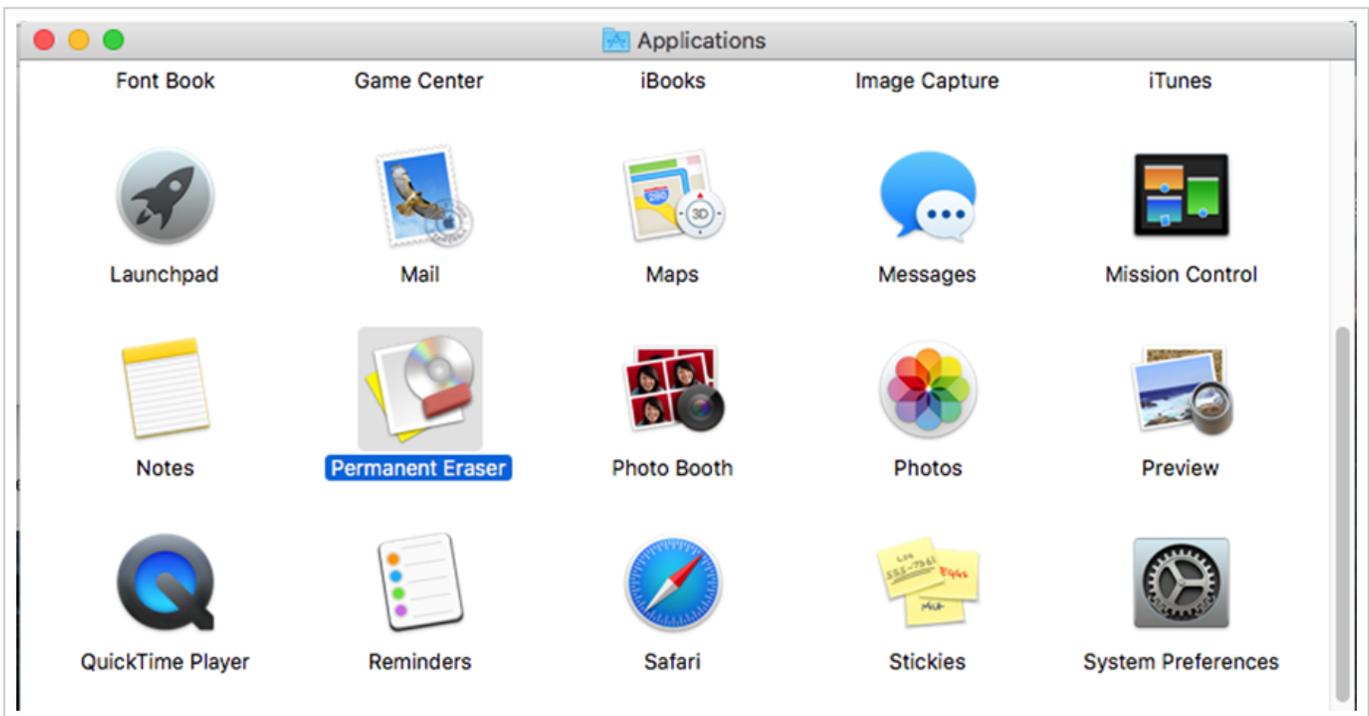
Permanent eraser

Esta herramienta permite hacer un borrado seguro de los archivos en la papelera de reciclaje o los archivos que se le pasen a la aplicación.

Descargar la herramienta desde el sitio oficial². Dar doble clic en el icono y mostrará la ventana de instalación de aplicaciones, arrastrar el ícono de “Permanent Eraser” al ícono del directorio “Applications” para instalar la aplicación.



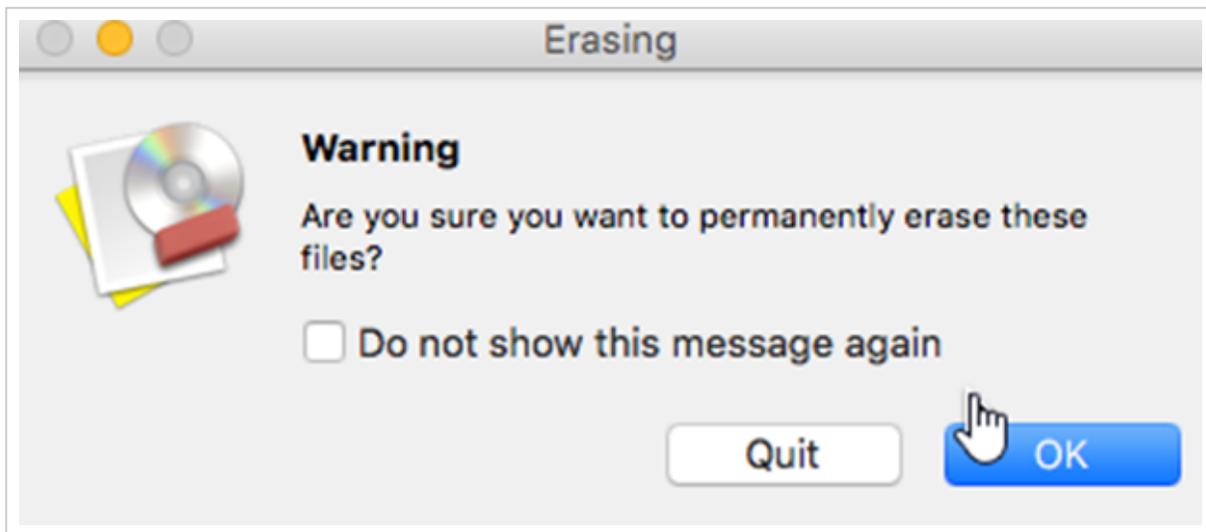
Dar doble clic en el icono "Applications" y se abrirá la ventana de aplicaciones disponibles en el sistema operativo. Buscar la aplicación "Permanent Eraser" y dar doble clic para ejecutarla.



De manera predeterminada la aplicación preguntará si se quiere eliminar el contenido de la papelera y se da clic en el botón "Ok" para eliminar su contenido.



También se pueden eliminar archivos que no se encuentren en la papelera, esto se logra arrastrando el archivo deseado a borrar al icono de la aplicación "Permanent Eraser", la aplicación mostrará la siguiente ventana.



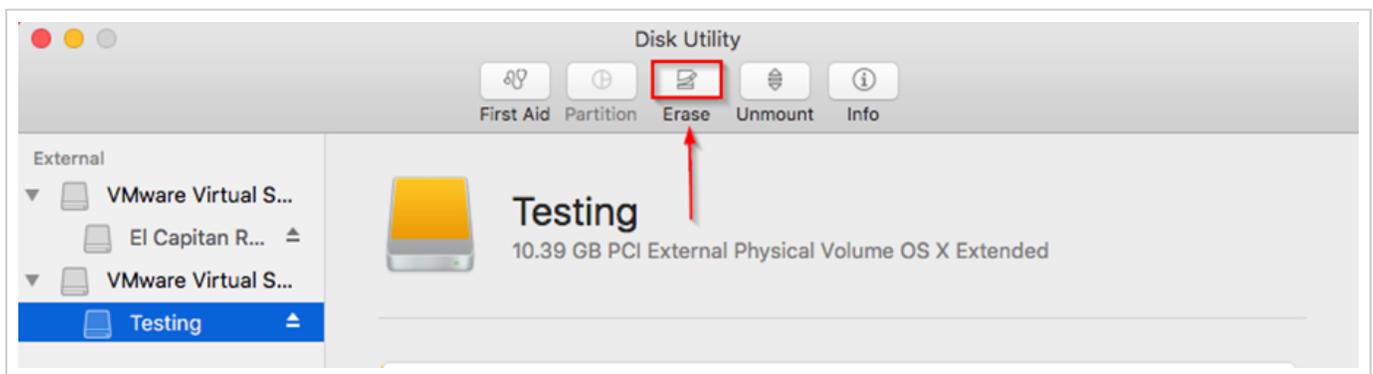
Dar clic en "Ok" para eliminar el archivo.

Disk Utility

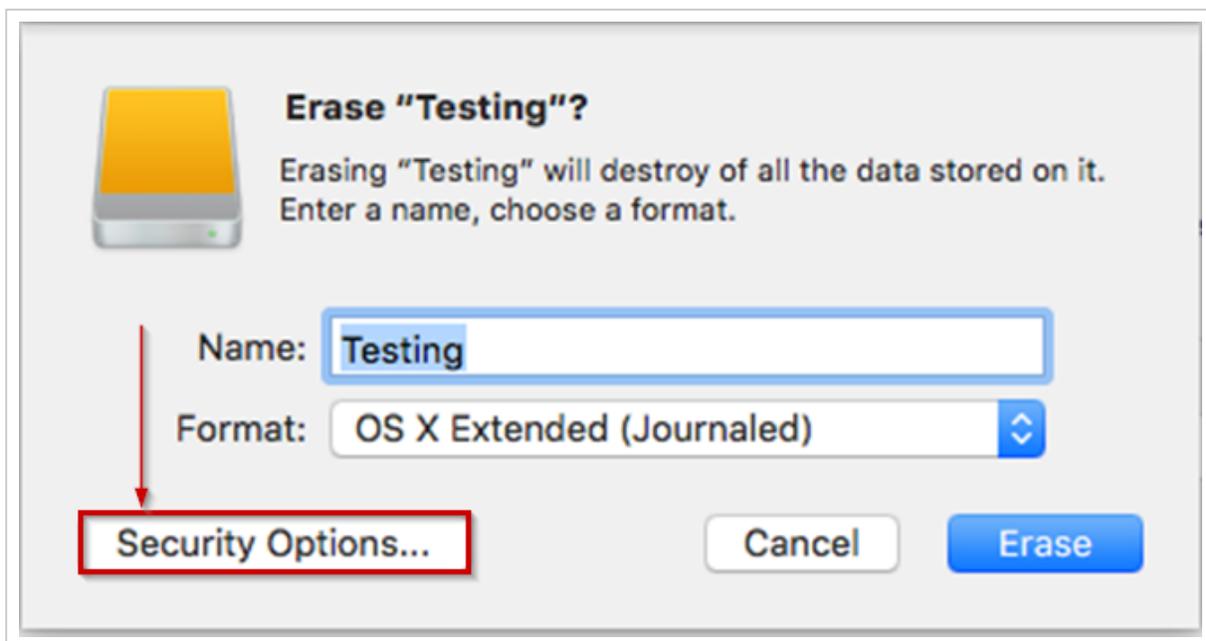
La herramienta Disk Utility forma parte de las aplicaciones nativas del sistema operativo MAC OS X, para ejecutar la aplicación se deberá de ingresar la palabra "Disk" en el LaunchPad y aparecerá el siguiente ícono.



La siguiente imagen muestra la interfaz de la aplicación, se debe seleccionar la opción "Erase" para borrar de forma segura la unidad de almacenamiento.

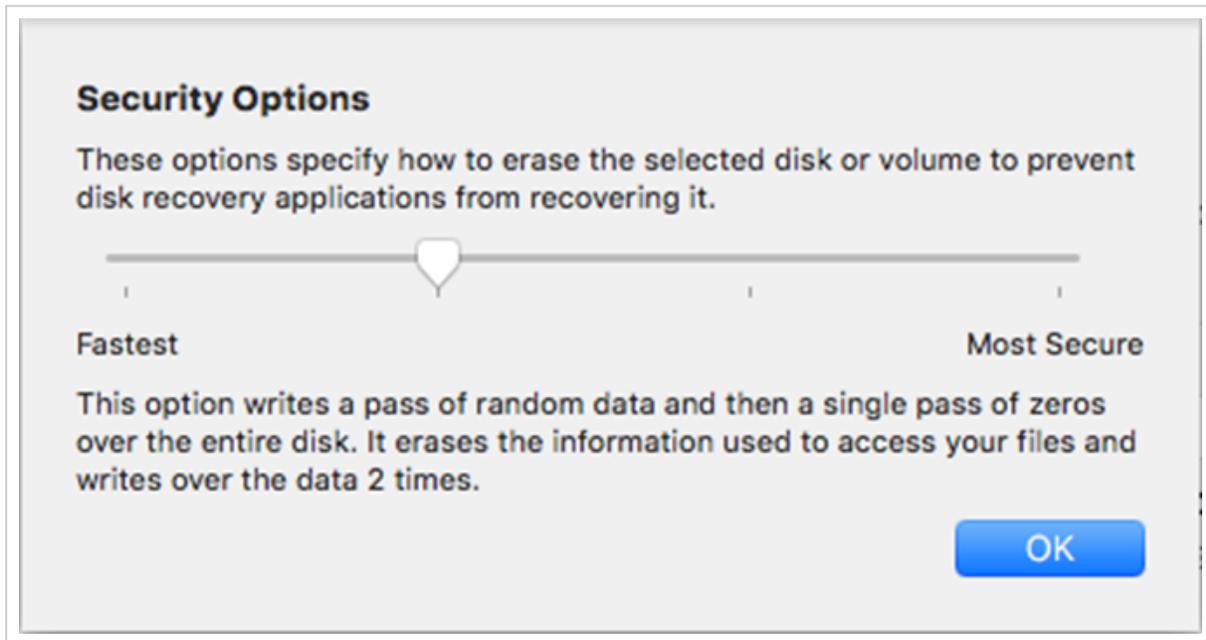


Se abrirá una ventana como la siguiente en dónde se puede especificar el nombre, el tipo de sistema de archivos y definir el tipo de borrado que se le aplicará a la unidad almacenamiento.

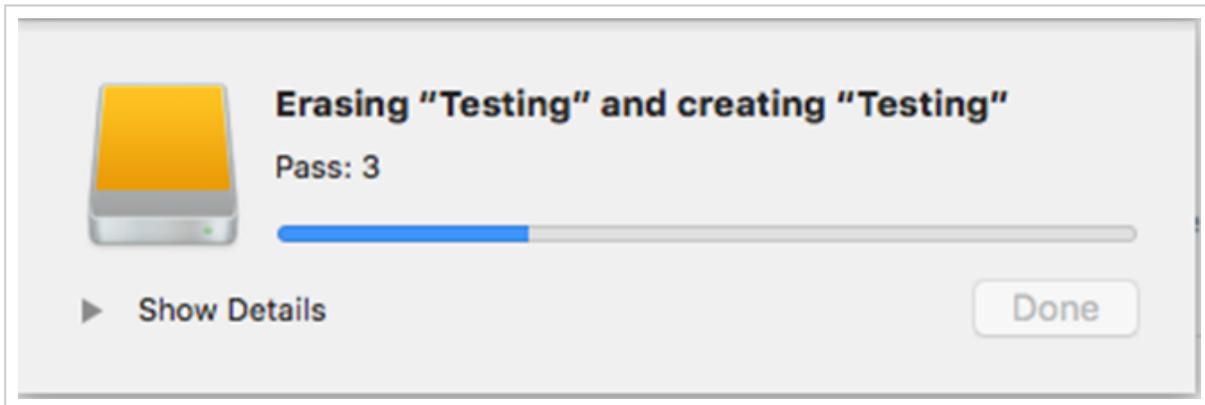
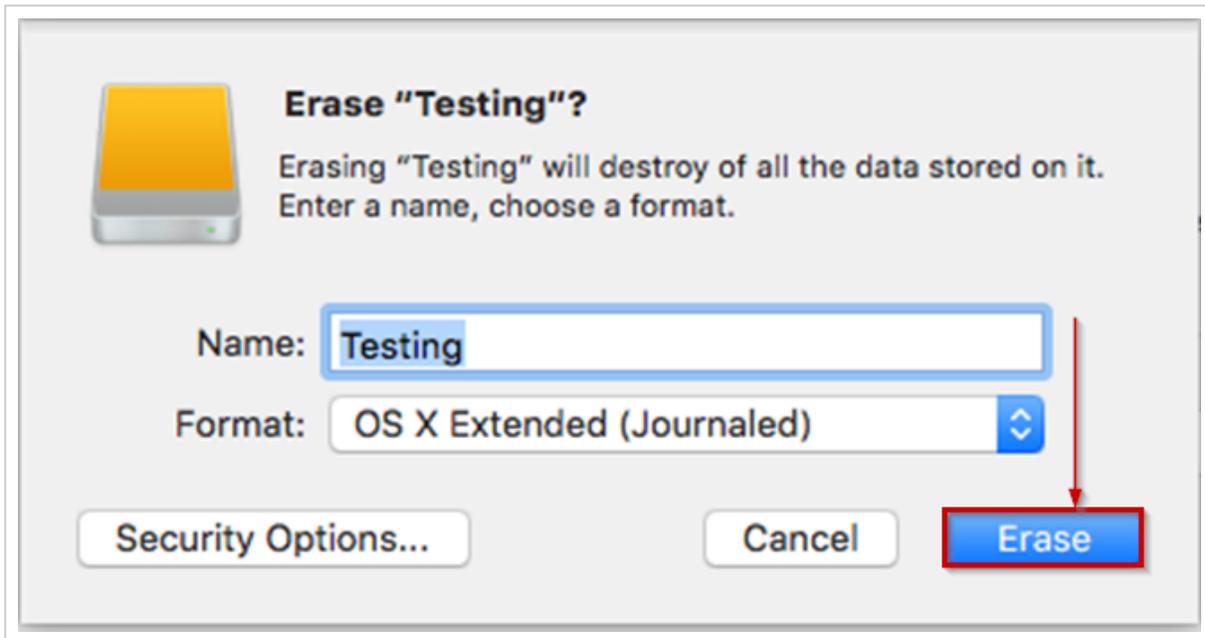


Para borrar de forma segura el contenido de una unidad de almacenamiento dar clic en el botón “Opciones de Seguridad...” y seleccionar una de las siguientes opciones:

- 1. La más rápida: No realiza borrado seguro.
- 2. Dos pases: Sobrescribe una ronda de datos aleatorios en el disco y después escribe ceros en todo el medio.
- 3. Cumplimiento con DOE: Sobrescribe el disco dos veces con valores aleatorios y escribe un valor definido en todo el disco, realizando tres pases.
- 4. Estándar DOD5220-22M: Realiza siete pases escribiendo datos en el disco.



Se recomienda utilizar la opción 2 o posteriores. Al seleccionar la opción de borrado seguro, se tiene que dar clic en el botón “Ok” y regresará a la ventana anterior, en esta se tiene que dar clic en el botón “Erase” e iniciará el proceso de borrado seguro de archivos.



Al final se mostrará una ventana de que el proceso ha finalizado satisfactoriamente.



GNU/Linux

En sistemas operativos GNU/Linux, se tienen las siguientes herramientas para el eliminado seguro de información:

- srm
- wipe

Utilería srm

Se necesita instalar el paquete secure-delete con el gestor de paquetes apt

```
# apt install secure-delete
```

Se tiene la siguiente estructura de directorios que contienen archivos:

```
root@unamcert:/home/luis/Documents# tree archivos/  
archivos/  
├── english_18.0.pdf  
├── linuxfun.pdf  
├── nuevosArchivos  
│   ├── english_18.0.pdf  
│   ├── linuxfun.pdf  
│   └── TheLinuxCommandLine.pdf  
└── TheLinuxCommandLine.pdf  
  
1 directory, 6 files  
root@unamcert:/home/luis/Documents# █
```

Para borrar un solo archivo se puede ejecutar el siguiente comando:

```
root@unamcert:/home/luis/Documents# srm archivos/linuxfun.pdf
```

En caso de que se requiera eliminar de forma recursiva todos los archivos, se necesita especificar el parámetro -r, como se muestra en la siguiente imagen:

```
root@unamcert:/home/luis/Documents# srm -r archivos/
```

Utileria wipe

Esta herramienta permite realizar un borrado seguro de archivos a bajo nivel. Al igual que la utilidad srm, también se necesita instalar el paquete wipe utilizando el administrador de paquetes apt utilizando el siguiente comando:

```
# apt install wipe
```

Se puede eliminar un archivo de forma segura utilizando el comando wipe pasando como parámetro la ruta del archivo a eliminar, una vez que se ejecuta el comando, la herramienta solicita al usuario aceptar que se quiere eliminar el archivo y para continuar con la operación se necesita ingresar la palabra "Yes", como se muestra a continuación:

```
root@unamcert:/home/luis/Documents# wipe archivos/linuxfun.pdf
Okay to WIPE 1 regular file ? (Yes/No) Yes
```

Se puede eliminar de forma recursiva un directorio utilizando la opción -r, adicionalmente se puede definir el número de pases que se aplicará con la opción -P como se muestra en la siguiente imagen:

```
root@unamcert:/home/luis/Documents# wipe -P 10 -r archivos/
Okay to WIPE 1 directory ? (Yes/No) Yes
```

Una vez finalizado el proceso de borrado seguro de información se mostrará lo siguiente:

```
root@unamcert:/home/luis/Documents# wipe -P 10 -r archivos/
Okay to WIPE 1 directory ? (Yes/No) Yes
Operation finished.
6 files wiped and 0 special files ignored in 2 directories, 0 symlinks removed but not followed, 0 errors occurred.
root@unamcert:/home/luis/Documents#
```

Para eliminar de forma segura una unidad de almacenamiento, se debe de montar la unidad en un cierto directorio del sistema de archivos en GNU/Linux y realizar un borrado recursivo de archivos. También es posible borrar toda la información en la unidad utilizando el siguiente comando:

```
root@unamcert:/home/luis/Documents# wipe -r -P 10 /dev/sdc
Okay to WIPE 1 special file ? (Yes/No) Yes
Operation finished.                /dev/.0i ->                /dev/qglSyncing...
0 files wiped and 1 special file ignored in 0 directories, 0 symlinks removed but not followed, 0 errors occurred.
```

Referencias

1.- NIST. (2014). NIST 800-88 Guía para sanitización de medios. 22-febrero-2022, de National Institute of Standards and Technology Sitio web: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>

2.- Edenwaith. (2022). Permanent Eraser 2.7.1 :: Securely erase your files. 22-febrero-2022, de Edenwaith Sitio web: <http://www.edenwaith.com/products/permanent%20eraser/>

3.- Microsoft. (2022). SDelete v2.04. 22-febrero-2022, de Microsoft Sitio web: <https://technet.microsoft.com/en-us/sysinternals/sdelete.aspx>

4.- HDDGURU.COM. (2022). Wipe My Disks. 22-febrero-2022, de HDDGURU Sitio web: <http://hddguru.com/software/Wipe-My-Disks/>

5.- Apple Inc. (2022). Disk Utility for Mac: Erase a volume using Disk Utility. 22-febrero-2022, de Apple Sitio web: <https://support.apple.com/es-es/guide/disk-utility/dskutl14079/mac>

6.- Sin autor. (Sin año de publicación). wipe(1) - Linux man page. 22-febrero-2022, de die.net Sitio web: <https://linux.die.net/man/1/wipe>

7.- Canonical Ltd. (2019). srm. 22-febrero-2022, de Ubuntu manuals Sitio web: <https://manpages.ubuntu.com/manpages/impish/en/man1/srm.1.html>

8.- Canonical Ltd. (2019). wipe. 22-febrero-2022, de Ubuntu manuals Sitio web: <https://manpages.ubuntu.com/manpages/impish/en/man1/wipe.1.html>

La Coordinación de Seguridad de la Información/UNAM-CERT agradece el apoyo en la elaboración y revisión de este documento a:

Luis Daniel Sánchez Vélez
Ing. Demian García
Sergio Anduin Tovar Balderas

Para mayor información acerca de este documento contactar a:

UNAM-CERT: Equipo de Respuesta a Incidentes UNAM
Coordinación de Seguridad de la Información
Dirección General de Cómputo y Tecnologías de Información y Comunicación
Universidad Nacional Autónoma de México
<http://www.cert.unam.mx>

Tel: 55 56 22 81 69

Liberación original: Miércoles, 15 Junio 2017

Actualización: Martes, 22 Febrero 2022