Tutorial para el Borrado Seguro de la Información por Software

en los discos de los usuarios

Que algo desaparezca de la vista no significa que haya dejado de existir. Esto es particularmente cierto en el área de informática, donde lo que se ve es solo una fracción de lo que ocurre dentro del ordenador.

Existen dos niveles de borrados: a nivel software y a nivel hardware. A su vez, a nivel software existen dos maneras de borrar información, se puede hacer tanto lógicamente como físicamente.

Los beneficios de estos procedimientos se centran en la preservación de la privacidad de quienes deciden realizar una destrucción de la información de sus dispositivos, ya sea mediante un borrado por software o por hardware. La recuperación de la información que descuidadamente haya quedado en estos dispositivos puede perjudicar al usuario particular.

El borrado a nivel hardware es específicamente la destrucción física del dispositivo de almacenamiento. Existen diferentes equipos de hardware para realizar este proceso, pero todos con el mismo resultado: la destrucción de los datos del dispositivo y su inutilización. La destrucción física es realizada a través de la trituración, desintegración, pulverización, fusión e incineración del dispositivo, también se puede realizar por medio de desmagnetización. Estos métodos inutilizan a los dispositivos de almacenamiento, por ende el acceso a los mismos no es posible, siendo así un procedimiento difícil de certificar en algunos casos. Puede llegar a ser un proceso costoso de acuerdo al tipo de destrucción y certificación.

El borrado a nivel software consiste en diferentes herramientas de software que contienen una lista de varios algoritmos que sobre-escriben los sectores del disco duro con diferentes patrones. Cada algoritmo posee una forma distinta de sobre-escritura. Este procedimiento imposibilita la recuperación de los datos, dejando al disco duro en un perfecto estado para su reutilización como también para su correcta certificación que los antiguos datos no se encuentran en el dispositivo de almacenamiento y que los mismos no se pueden recuperar. Es un proceso más económico. Cabe destacar que este tipo de borrado es irreversible, definitivo.

El proyecto de extensión de la Facultad de Informática de la Universidad Nacional de La Plata, desarrollado por el laboratorio LINTI, denominado **E-Basura** recibe diferente equipamiento informático, dentro de los cuales se encuentran los ordenadores. Los mismos son restaurados y donados a instituciones sin fines de lucro para reducir la brecha digital-social en los sectores vulnerables de la comunidad. Para que los ordenadores puedan ser donados, deben pasar por un proceso de higienización, el cual consiste en destruir la información del usuario anterior pero a su vez preservar el disco duro, por lo que se realiza un borrado a nivel de software, con lo cual se protegen a los usuarios.

Se aconseja a todo usuario o empresa que se deshaga de un ordenador realizar una copia de los datos y luego ejecutar un procedimiento de borrado seguro para protección de datos personales como se menciona a continuación.

¿Cómo realizar un borrado a nivel software?

Cuando un usuario decide llevar a cabo el borrado de la información de su dispositivo a través de una destrucción ***a nivel software***, lo que requiere es la utilización de un software (propietario o libre) de borrado seguro.

Los pasos básicos que se aconsejan seguir serían los siguientes:

1. Seleccionar una herramienta de software a utilizar para la higienización.
2. Seleccionar el algoritmo de borrado seguro a utilizar.
3. Ejecutar la herramienta con el algoritmo seleccionado (borrado).
4. Seleccionar una herramienta de recuperación de información.
5. Ejecutar sobre el dispositivo de almacenamiento la herramienta seleccionada para la recuperación.

Los últimos dos pasos (4 y 5) son opcionales. Su fin es asegurar y demostrar al usuario que su información ya no se encuentra en el dispositivo.

Respecto a los pasos 1 y 2, mostraremos un ejemplo de cómo se aconseja a los usuarios realizarlos utilizando la herramienta de software libre ***DBAN (Darik's Boot and Nuke).***

Darik's Boot and Nuke (DBAN).

DBAN es una herramienta gratuita que no necesita de un Sistema Operativo ya que se utiliza un CD/DVD o un memoria USB booteable.

DBAN proporciona a los usuarios una prueba de eliminación, a través de un informe, también llamado log o registró, de borrado listo para auditorías.

Al arrancar el ordenador desde el DVD/CD o memoria USB, iniciara el programa comenzando con cinco (5) opciones:

1. Presionar la tecla F2 para aprender sobre DBAN.
2. Presionar la tecla F3 para listar comandos rápidos.
3. Presionar la tecla F4 para solución de problemas.
4. Presionar la tecla ENTER para comenzar DBAN en el modo interactivo.
5. Introducir “autonuke” en la línea de comandos para iniciar DBAN en modo automático.

El comando “autonuke” correrá el algoritmo de higienización sobre ***todos*** los discos que estén conectados al ordenador.

Para comenzar la higienización de los datos debemos presionar la tecla ENTER. Una vez presionada, se listarán todos los discos conectados al ordenador.

A continuación se listarán los comandos a utilizar para la selección y configuración de los discos, más adelante se dará un ejemplo de cómo usarlos:

- ✓ Para seleccionar los discos para su borrado, se debe posicionar en cada uno de ellos y presionar la tecla SPACE. Se indicara con un "*" (asterisco) que el disco esta seleccionado.
- ✓ Para la selección del algoritmo a utilizar se debe presionar la letra "M".
- ✓ Para seleccionar el porcentaje de verificación, se debe presionar la letra "V".
- ✓ Para seleccionar el número de rondas, se debe presionar la letra "R".
- ✓ Para cambiar el orden de ejecución de los discos se utiliza:
  - "J" para subir (up - arriba).
  - "K" para bajar (down - abajo).
- ✓ Para comenzar el borrado se debe presionar la tecla F10.

DBAN cuenta con seis (6) algoritmos de higienización, los cuales son:

1. Quick Erase: One pass zeros (1 pass)
2. Canadian RCMP TSSIT OSP-II (7 passes, verify)
3. DoD Short: US DoD 5220.22-M (3 passes, verify)
4. US DoS 5220.22-M (ECE) (7 passes, verify)
5. Peter Gutmann (35 passes, verify)
6. PRNG Stream: método random. Su nivel de seguridad dependerá de la cantidad de rondas que se le asigno. Equivale al "One pass random", y la cantidad de pasadas es igual a la cantidad de rondas.

Si se inicia el modo automático de DBAN el algoritmo a utilizar es el DoD Short.

Ejemplo de utilización.

Se debe iniciar el ordenador desde una memoria USB o CD. Una vez inicializado el programa, se mostrará una pantalla azul, como se muestra en la ***figura 01***, en la cual se debe presionar la tecla ENTER.

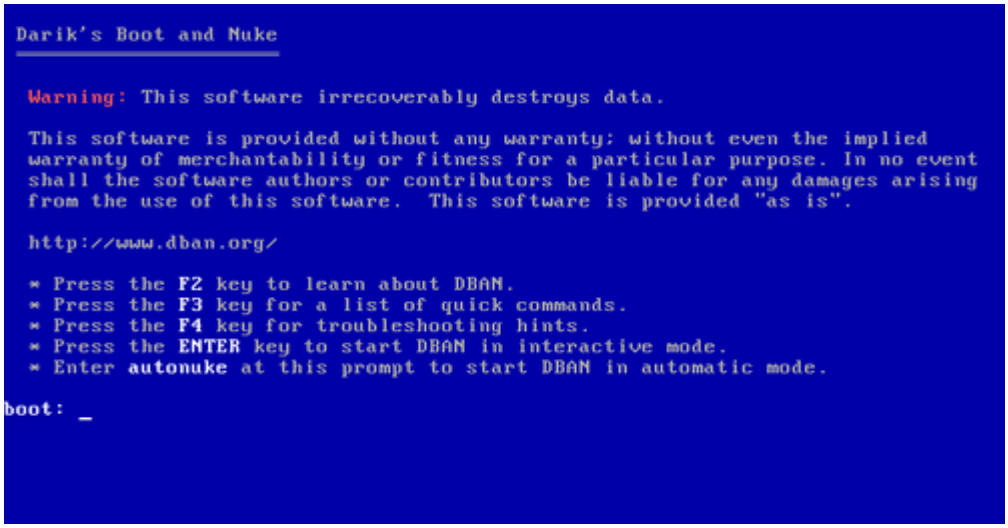

Figura 01.

Una vez que termina el arranque, luego de un momento, aparecerá la siguiente pantalla, como se muestra en la ***figura 02.***

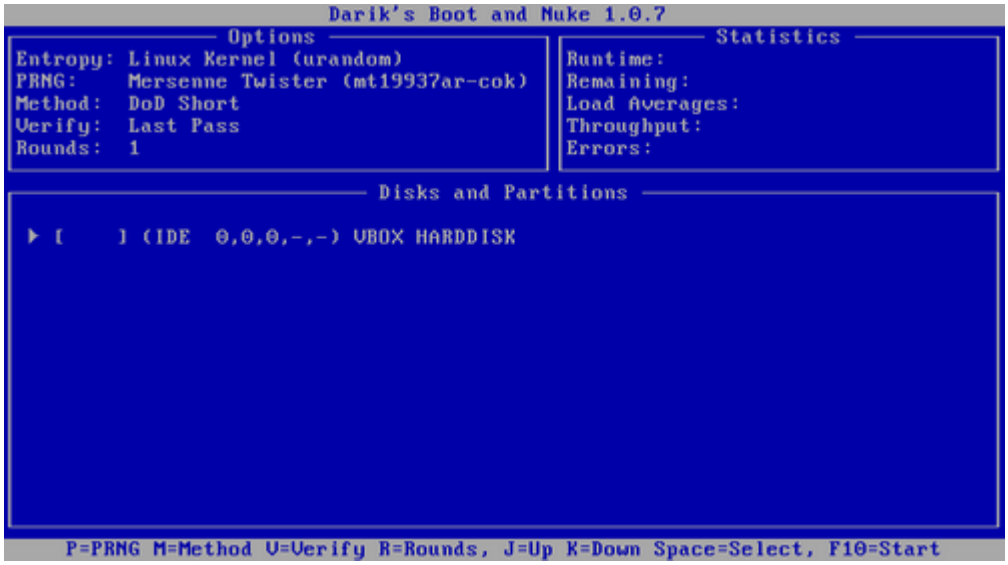

Figura 02.

Cuando aparece esta pantalla, ya se puede retirar el USB/CD.

Al presionar la tecla "M", se abre el menú en el cual se podrá seleccionar el método a utilizar, como se muestra en la ***figura 03***. En este caso se selecciona el método "PRNG Stream" (con las flechas arriba/abajo y ENTER) que nos permite elegir la cantidad de pasadas aleatorias que se realizará.

Figura 03.

Al presiona la tecla "R", se podrá ingresar la opción del número de pasadas que se desea realizar, como se muestra en la ***figura 04***, luego se debe presiona la tecla ENTER.

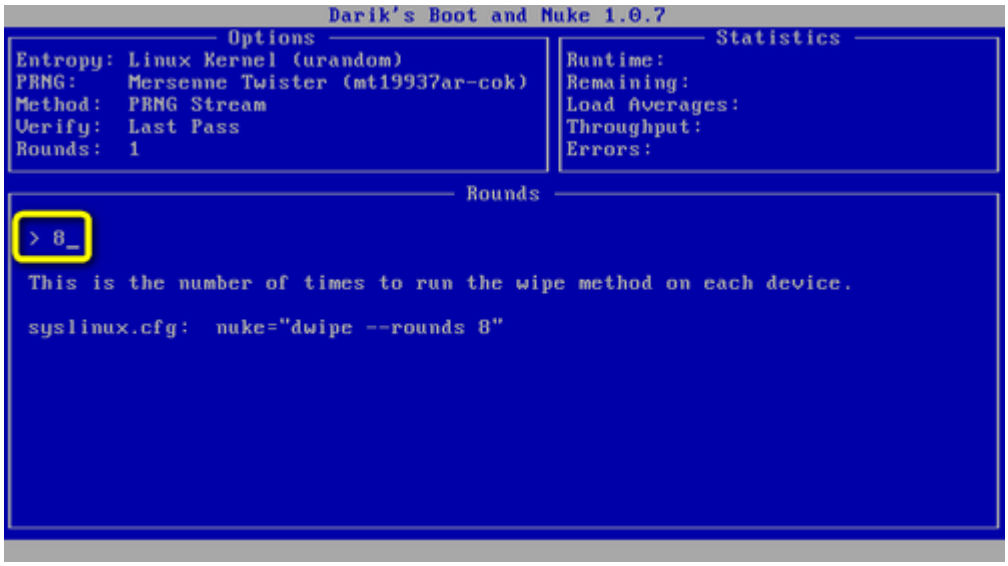

Figura 04.

Una vez configurado el algoritmo a utilizar, y en este caso la cantidad de pasadas, se debe presionar la tecla ESPACE y se volverá al primer menú donde seleccionamos el disco duro a borrar, como se muestra en la ***figura 05***:

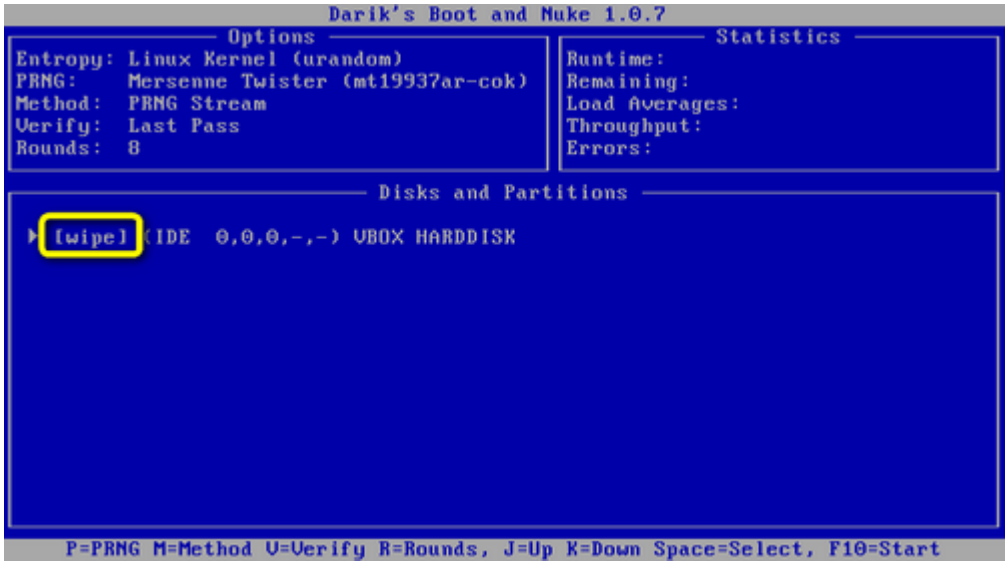

Figura 05.

A continuación se presiona F10 para iniciar el borrado de datos y espera que termine la operación, como se muestra en la ***figura 06***.

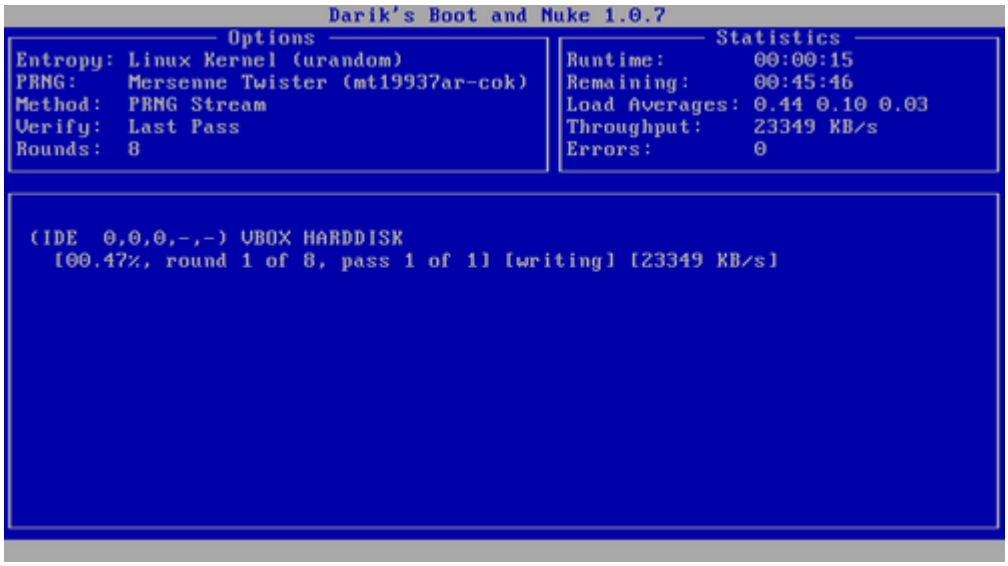

Figura 06.

Cuando finalice la operación el log será guardado y se deberá apagar el equipo para retirar el dispositivo.

Agradecimiento

A la alumna Guillermina Belli por su contribución y su tesis de Higienización de Discos

Viviana Ambrosi

Proyecto E-Basura