UNIVERSIDAD NACIONAL DE LA PLATA

FACULTAD DE INFORMÁTICA

TESINA DE LICENCIATURA

Título: Higienización de dispositivos de almacenamiento para la preservación de la privacidad.
Autores: Guillermina Belli (9155/2).
Director: Lic. Paula Venosa.
Director: Mg. Lia Molinari.
Asesor profesional: CC. Viviana M. Ambrosi.
Carrera: Licenciatura en Sistemas – Plan 2007.

Resumen

La evolución tecnológica exige la renovación y la compra de nuevos equipamientos. Los diferentes usuarios van acumulando gran cantidad de equipamiento de descarte que pasan a formar parte de la llamada: basura electrónica. Si bien hay proyectos que disponen y re-utilizan estos rezagos cuando es posible, quienes lo llevan a cabo se han tenido que enfrentar con la situación donde el equipamiento supuestamente descartado cuenta aún con información registrada. La presente tesina desarrolla la investigación de cómo debería tratarse esta situación, presentando y comparando diferentes procedimientos para la correcta destrucción de la información a través de diferentes herramientas y algoritmos de higienización de los datos. También se presentan distintas herramientas de recuperación de la información para certificar la eficiencia de dicha destrucción.

Palabras Claves

- *Higienización.*
- *Borrado lógico.*
- *Borrado físico.*
- *RAEE (Residuos de Aparatos Eléctricos y Electrónicos).*
- *Privacidad.*
- *Recuperación.*
- *Discos duros.*

Trabajos Realizados

- *Desarrollo e investigación sobre los RAEE.*
- *Investigación sobre el dispositivo de almacenamiento sobre el cual se realizaran las pruebas.*
- *Presentación y ejecución de las herramientas y algoritmos de higienización a nivel lógico.*
- *Comparación de las herramientas de higienización.*
- *Presentación y ejecución de las herramientas de recuperación de la información.*
- *Resultados y estadísticas de recuperación de la información.*

Conclusiones

Se deben estar informado y a su vez tener en cuenta todas las medidas de seguridad para preservar la información de los diferentes tipos de usuarios, incluso a la hora de donar o reutilizar equipamiento. Asegurar la protección de los datos de los usuarios, evita que su información sea manipulada; esto a su vez permite el aumento de donaciones completas a proyectos de reacondicionamiento lo que implica el cuidado y la protección del medio ambiente a través del reciclaje y la reutilización de los AEE.

Trabajos Futuros

- *Investigación y ejecución de las diferentes herramientas de higienización a nivel hardware.*
- *Comprobación de la eficiencia de la higienización a nivel hardware.*
- *Investigación y ejecución de las herramientas de destrucción y recuperación física.*
- *Comprobación de la eficiencia de la destrucción y recuperación de la información a través de métodos físicos.*

Fecha de la presentación: Diciembre 2013

Universidad Nacional de La Plata

Facultad de Informática

Higienización de dispositivos de almacenamiento para la preservación de la privacidad.

Tesina de Licenciatura en Sistemas

Alumna: Belli, Guillermina.

Directoras: Lic. Paula Venosa – Mg. Lia Molinari.

Asesora profesional: CC. Viviana M. Ambrosi.

Agradecimientos

Quiero agradecer especialmente a mis directoras Paula Venosa y Lia Molinari, como también a mi asesora profesional Viviana Ambrosi por guiarme y ayudarme a crecer en este último trayecto de mi formación tanto académica como profesional.

Gracias al proyecto E-Basura, dirigido por Viviana Ambrosi, por recibirme en sus instalaciones. Especialmente a Edgar Vega por estar siempre incondicionalmente ayudándome en el desarrollo de mi investigación.

También quiero agradecer a mi familia, que sin su apoyo permanente no podría haber llegado a esta etapa de mi vida.

Por último, quiero gradecer a la Universidad Nacional de La Plata por las amplias herramientas que brindan gratuitamente para la formación de nuevos profesionales a través de diferentes carreras universitarias.

Índice.

Motivación

En la actualidad existe mucha basura de la llamada “basura electrónica”, que se refiere a todos aquellos dispositivos eléctricos o electrónicos que han llegado al final de su vida útil y, por lo tanto, son desechados. En su gran mayoría son equipos informáticos.

El principal problema con la basura electrónica es que muchas veces es vertida a cielo abierto, lo cual resulta altamente contaminante. Los metales y demás elementos que poseen estos Residuos de Aparatos Eléctricos y Electrónicos (conocidos como RAEE) son tóxicos para la salud y contaminan el medio ambiente, perjudicando el aire que respiramos, la tierra y el agua que bebemos.

El proyecto E-Basura [1], desarrollado por el laboratorio LINTI de la Faculta de Informática de la Universidad Nacional de La Plata, recibe “equipos de informática y telecomunicaciones”, que se encuentran dentro de los tipos IT de RAEE, para su restauración, y así darles una nueva vida útil, para luego donarlos a instituciones sociales sin fines de lucro para reducir la brecha digital y social.

En la provincia de Buenos Aires el 50% de los RAEE corresponde a equipamiento que proviene de la línea de informática. De este porcentaje un 50% permanece acumulado en los hogares, en las oficinas o en las industrias; un 40% son enterrados o van a algún tipo de relleno sanitario; y solo un 10% es reciclado actualmente. [2]

El proyecto busca la concientización sobre la problemática de los RAEE. Y además fomenta y recibe donaciones de equipos con el fin de analizarlos y clasificarlos y posteriormente donarlos.

Todas las donaciones pasan por un sector llamado “testing” para clasificar las partes que se encuentran en correcto funcionamiento, como también las que no. Las partes no funcionales son descartadas y enviadas a empresas para su reciclaje; las demás son reparadas, si así lo necesitan, y reutilizadas.

En el caso del armado de nuevos ordenadores, los discos de almacenamiento de las mismas pasan por un proceso de higienización, o también llamado “borrado seguro”, para eliminar todo tipo de información, con dos fines principales:

1. Preservar la privacidad de los donantes.
2. Evitar la destrucción de los discos de almacenamiento.

Al finalizar el armado de las PC dentro del taller, las mismas son dirigidas al sector de “formateo” para la instalación del Sistema Operativo “LIHUEN” [3], el cual es desarrollado en el Laboratorio de Investigación en Nuevas Tecnologías Informáticas, LINTI, de la Universidad Nacional de La Plata.

Por último, el equipo completo debe pasar a una etapa de testeo, “test de stress”, para asegurarse de su correcto funcionamiento. Una vez pasado con éxito la última etapa, son donadas.

El proceso de higienización, dentro del armado de ordenadores, es una etapa importante del ciclo de recuperación y reutilización. Asegurar la protección de los datos de los

donantes es primordial para que los mismos realicen una completa donación, sin tener que considerar que su información será manipulada.

En el caso específico que los discos se encuentren dañados, no podrán pasar por la etapa de higienización. Por lo tanto, se opta por otra forma de destrucción permanente de los datos, la destrucción física. Así siempre se asegura la privacidad de los miembros donantes.

La obtención y no destrucción de los discos de almacenamiento para su correcta reutilización, es una parte muy importante del proyecto, ya que la probabilidad de conseguir discos viejos o modelos que ya no son fabricados es casi nula. Por lo tanto los porcentajes de donaciones se reducirían por falta de discos duros necesarios para que vuelvan a funcionar los equipos a donar.

Objetivo

El objetivo de la presente tesis radica principalmente en la selección de la herramienta más adecuada para realizar el procedimiento de higienización de datos a nivel lógico en los dispositivos recuperados/reciclados por el proyecto E-Basura y la elaboración de la documentación formal correspondiente, tanto para el procedimiento como su ejecución, con el fin de avalar la destrucción y no permanencia de la información dentro de los discos de almacenamientos donados permitiendo que diferentes entidades realicen donaciones de equipos completos y evitar que le quiten componentes.

Este procedimiento cuenta con diferentes algoritmos que se pueden ejecutar para cumplir con el mismo fin. Por lo tanto, se realizará un estudio de su funcionamiento y una comprobación de su efectividad.

También, se realizará una evaluación de las diferentes herramientas de Higienización por software utilizando aquellas que cumplan con criterios pre-establecidos, y seleccionado aquella que haya resultado más eficiente para la obtención de un certificado que avale la higienización de los discos de almacenamiento.

Introducción

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 diferentes maneras de borrar archivos en un Sistema Operativo, se pueden hacer tanto lógicamente como físicamente. Por ejemplo, en el caso del borrado de un archivo cuando se arrastra el mismo hasta la papelera de reciclaje y luego se la vacía, los datos no han sido eliminados, solo se han borrado lógicamente pero físicamente en el disco aun existen.

¿Por qué el Sistema Operativo realiza borrados lógicos?

Ante la posibilidad de arrepentimiento de la acción de borrado, el borrado lógico posibilita volver atrás dicho proceso, pues la información sigue existiendo en el medio. Por esta misma razón, el borrado lógico puede constituir una potencial vulnerabilidad ante la posibilidad de revelar información privada que se mal asume como borrada definitivamente

Para acabar verdaderamente con un archivo, impidiendo cualquier forma de recuperó o reconstrucción, se necesitan programas especiales.

El borrado de archivos corresponde a la acción que ejerce sobre una unidad de disco duro al marcar un grupo de sectores ocupados del mismo como sectores libres. El borrado lógico se ejecuta cuando sobre el disco duro no se realiza la tarea de borrado completo, sino que marca al “espacio en uso” como “espacio libre”, dejando así espacio disponible para su utilización por otros archivos que se quieran crear en el futuro. El borrado seguro (higienización de los datos) se ejecuta cuando al borrar un archivo, algún software con un algoritmo determinado de borrado graba ceros (0), unos (1) o una combinación de ambos sobre el archivo, no permitiendo que éste se pueda recuperar posteriormente.

Los Sistemas Operativos ordenan la información en archivos, dentro del dispositivo de almacenamiento. Para encontrar estos archivos, por ejemplo en un disco duro, hay que acudir a la “lista de archivos”, donde se indica tanto el nombre del archivo como su ubicación dentro del espacio de almacenamiento.

Cuando se utilizan métodos de borrado dispuestos por el propio Sistema Operativo como el comando “suprimir”, se realiza el borrado exclusivamente en la “lista de archivos” sin que se elimine realmente el contenido del archivo que permanece en la zona de almacenamiento hasta que se reutilice este espacio con un nuevo archivo.

Por lo tanto, toda aquella acción que no conlleve la eliminación, tanto de la información de la “lista de archivos” como del contenido del mismo, no consigue destruir eficazmente dicha información. De forma específica:

- Los comandos de borrado del Sistema Operativo, acceden a la “lista de archivos” y marcan el archivo como suprimido, pero su contenido permanece intacto. Por lo tanto, no son un método de destrucción segura.

- Al formatear un dispositivo normalmente se sobre-escribe el área destinada a la “lista de archivos” sin que el área de datos donde se encuentra el contenido de los archivos sea alterada. Por lo tanto tampoco es un método de destrucción segura.

¿Por qué el Sistema Operativo no hace un borrado seguro?

La higienización de los datos es un proceso lento y costoso. Si por cada archivo borrado el Sistema Operativo tuviese que sobrescribir los datos a fondo, liberar espacio y ocuparlo, tomaría muchas horas cada día. El Sistema Operativo deja que sean los programas quienes se encarguen de esto. Por lo tanto, sólo quita la entrada en el directorio del sistema de archivos, debido a que esto requiere menos trabajo y a su vez es más rápido. Los contenidos del archivo permanecen en el medio de almacenamiento, aunque el espacio queda marcado como disponible, libre para hacer reasignado y quedarán ahí hasta que el Sistema Operativo escriba nuevos datos en el espacio asignado a los datos anteriores.

¿Cuándo hay que realizar una higienización de los datos?

El borrado lógico es muy conveniente, puesto que en muy pocas ocasiones hace falta borrar los datos tan a fondo e impedir, así, su recuperación. Al “marcar como libre” el espacio antes ocupado por un archivo, el tiempo necesario para "borrar" se reduce mucho.

Pero hay situaciones en las que el borrado debe ser irreversible, definitivo. Las agencias gubernamentales, los bancos y empresas de servicios que manejen información sensible deben recurrir a la destrucción de datos para preservar la confidencialidad de sus operaciones y de su personal. El borrado seguro de archivos informáticos equivale, en este sentido, a la trituración de papel.

En el caso de los usuarios domésticos, la necesidad de destruir datos se relaciona, sobre todo, con el mantenimiento de la privacidad, especialmente en entornos con ordenadores compartidos (cibercafés, aulas, lugar de trabajo, etc.). Al tramitar informáticamente cada vez más asuntos, el ciudadano debe preocuparse por su correcta eliminación. Los usuarios domésticos son los menos conscientes en términos de eliminación y recuperación de datos, por lo tanto no están correctamente informados sobre las facilidades de la recuperación de datos sensibles o de importancia para ellos, y por ende tampoco están informados de la correcta manera de eliminación definitiva.

Por consecuente, cuando se desecha un ordenador se debe dar importancia a la higienización de todos los datos del mismo. El borrado lógico es una opción simple y útil para un usuario particular que no posee información sensible o de importancia, pero es realmente crítico para las agencias gubernamentales, los bancos, las empresas, entre otros. Por lo tanto hay que asegurarse de haber borrado bien los datos para impedir que datos confidenciales sean recuperados por otros.

¿Cómo se borra un archivo para siempre?

Los archivos son muy difíciles de eliminar. Borrarlos, sobrescribirlos con otros datos o incluso formatear el disco no basta; las herramientas de informática forense son capaces de

dar con rastros de la información antigua, sobre todo si quien las usa sabe qué buscar, cómo y dónde buscarlo.

Es por ello que quien desee borrar un archivo de una vez por todas tiene que informarse y armarse de programas que apliquen métodos de higienización de datos, siendo conscientes que este tipo de borrado llevará un tiempo considerado.

¿Un formateo de los discos duros no es suficiente?

Podemos afirmar que con un formateo el disco duro vuelve a cero, pero realmente no es así. En informática, cuando hablamos de unos (1) y ceros (0) haciendo referencia a la escritura de datos en un determinado disco duro, implica que el sector contiene o no información respectivamente.

Suponiendo el caso de un disco en el que se han escrito, por ejemplo: 0101 como se muestra en la ***Figura 1***.

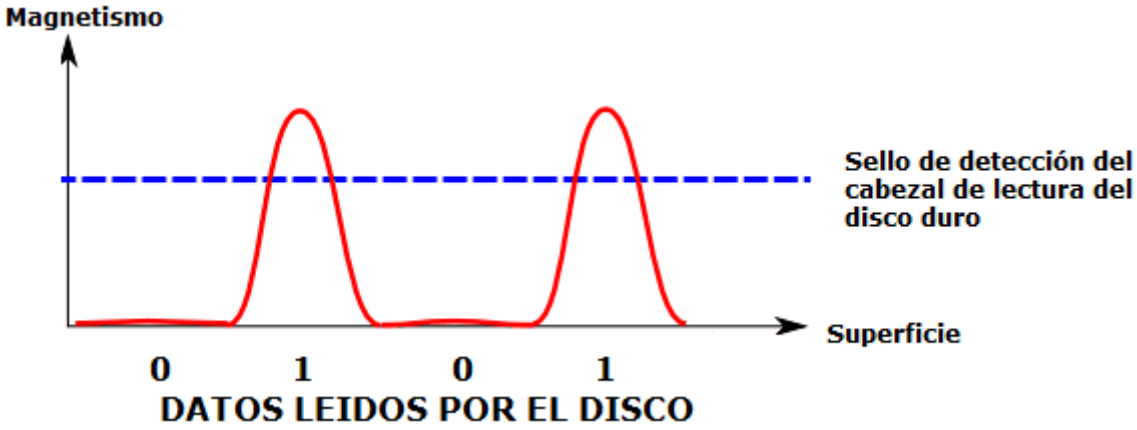


Figura 1. Ejemplo de magnetismo producido en la escritura de datos en un disco magnético.

Al realizar un formateo todos los sectores del disco vuelven a 0, por lo tanto, se llevaría toda la secuencia, en este caso 0101, a 0, por ende en el disco duro quedaría solo ceros, y la secuencia quedaría 0000, como se muestra en la ***Figura 2***. Pero también se puede observar que donde antes habían unos (1), los ceros (0) aún tienen un magnetismo residual. Este magnetismo puede ser leído con equipos de hardware especializados. En la actualidad existen empresas especializadas en este tipo de recuperación de datos.

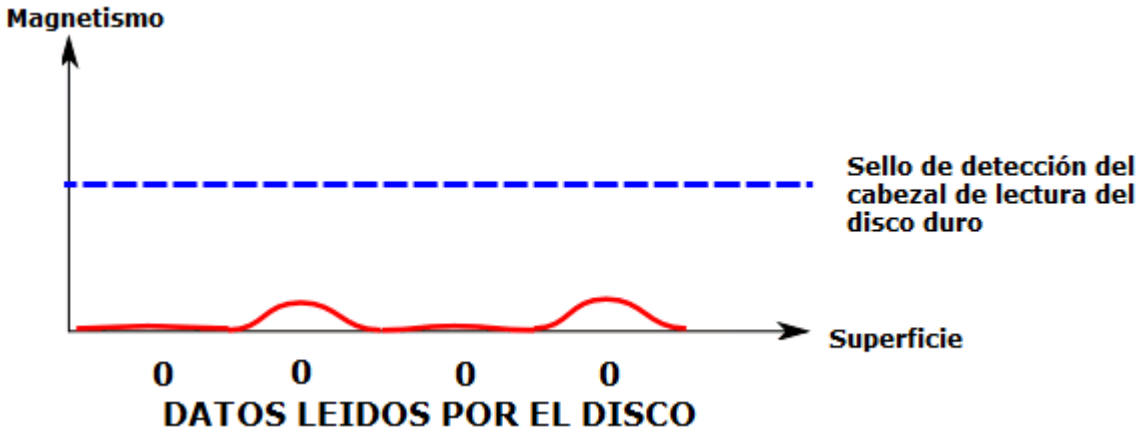


Figura 2. Ejemplo de magnetismo producido en la escritura de datos en un disco magnético.

Por lo tanto al realizar estudios sobre el disco se puede deducir que antes de borrar el disco/formatearlo se encontraban los datos 0101. Con este indicio, se pueden recuperar datos aunque se haya escrito encima. Por ejemplo, en caso del disco en el que se escribió 0101 anteriormente, ahora escribimos 0011, como se muestra en la ***Figura 3***.

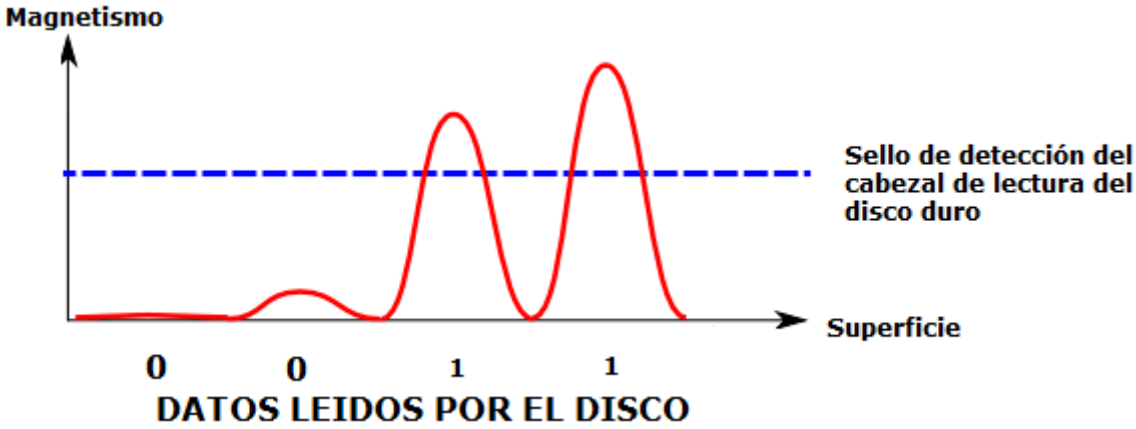


Figura 3. Ejemplo de magnetismo producido en la escritura de datos en un disco magnético.

Los dos unos (1) no tienen el mismo magnetismo, uno es más fuerte que el otro. Por lo que podemos deducir lo que había antes. Lo mismo para los dos ceros (0).

Podemos deducir el magnetismo precedente (0101) a pesar que hemos escrito ceros (0000) y luego otros datos (0011). Este es el trabajo de las herramientas de software de recuperación de datos, y es el foco en el que se centra las herramientas de higienización de datos.

Entonces, es posible en ciertos casos recuperar antiguos datos de un disco duro, a pesar de haberlo formateado y de haber escrito encima nuevos datos.

Por lo tanto es importante encontrar métodos eficaces para borrar completamente el disco duro. Como no todos los métodos de higienización garantizan el borrado completo de los datos, ya que hay maneras de recuperar los mismos a nivel hardware, muchas empresas, etc. optan por la destrucción física de los mismos. Por ejemplo, la Armada Americana funde sus discos duros para asegurarse que nadie pueda recuperar los datos contenidos en él, otros utilizan aparatos que generan un potente campo magnético, pero esto provoca la destrucción del disco duro. En todos estos casos, es imposible su reutilización.

La destrucción de los discos duros se realiza una vez llegado el fin de su vida útil, convirtiendo así al resto del ordenador en "basura electrónica". Mucha de esta basura es desechada, reciclada o donada. En el específico caso de las donaciones, que va de la mano con el reciclaje, permite que los ordenadores no se convierta en basura electrónica y pueda ser reparado y reutilizado. Por ende, es importante la obtención y no destrucción de los discos de almacenamiento para su correcta reutilización, ya que la probabilidad de conseguir discos duros viejos o modelos que ya no son fabricados es casi nula, y por lo tanto no se podrá reciclar el equipo para su funcionamiento, convirtiéndolo en basura electrónica.

La concientización sobre el reciclaje, la reutilización y la recuperación de los residuos electrónicos es muy importante hoy en día. Por lo tanto, los diferentes usuarios deben estar informados de las distintas opciones de destrucción de los datos que existen para que estos se sientan seguros de que su información sensible o confidencial no será recuperada, y así realicen donaciones completas de sus ordenadores.

¿Qué tipos de borrados existen?

Existen dos tipos de borrados: a nivel software y a nivel hardware.

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. Todos estos procedimientos se explicaran más adelante.

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 de ceros (0) y unos (1). 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 de que los antiguos datos no se encuentran en el dispositivo de almacenamiento y que los mismos no se pueden recuperar.

Residuos de Aparatos Eléctricos y Electrónicos

(RAEE).

Figura 4. Símbolo RAEE.

El término “Residuos de Aparatos Eléctricos y Electrónicos” (RAEE) se refiere a aparatos dañados, descartados u obsoletos que consumen electricidad. Incluye una amplia gama de aparatos como ordenadores, equipos electrónicos de consumo, celulares y electrodomésticos que ya no son utilizados o deseados por sus usuarios [4].

Debido a los grandes avances en tecnología, los Aparatos Eléctricos y Electrónicos (AEE) quedan obsoletos en poco tiempo y son rápidamente sustituidos por equipos nuevos, convirtiéndolos así en RAEE. Por lo tanto, una adecuada gestión de estos residuos permitiría la promoción del reciclaje, la reutilización y la recuperación de los residuos eléctricos y electrónicos para reducir la contaminación que los mismos producen.

Se estima que en los países de América Latina se están generando aproximadamente 120.000 toneladas de RAEE al año, una cantidad que se triplicará hacia el 2015 [5].

Específicamente en Argentina, según la Cámara Argentina de Máquinas de Oficina, Comerciales y Afines (CAMOCA) [6], en el año 2012 se descartaron más de 120.0000 toneladas [7] de RAEE sólo considerando ordenadores, impresoras, monitores, fotocopiadoras y afines: más de 3 kilogramos de basura electrónica por habitante por año.

Solo en la provincia de Buenos Aires el 50% de los RAEE corresponde a equipamiento que proviene de la línea de informática, de este porcentaje un 50% permanece acumulado en los hogares, en las oficinas o en las industrias; un 40% son enterrados o van a algún tipo de relleno sanitario; y solo un 10% es reciclado actualmente [2][8].

Regla de las tres “R”.

Esta regla permite cuidar el medio ambiente, y está muy relacionada con el fin del proyecto de ley RAEE [9]. Es muy importante que se realice en el siguiente orden: reducir, reutilizar y reciclar.

Reducir: Esto puede realizarse en dos niveles “Reducción de consumo de bienes” y “Reducción de consumo de energía”, su principal objetivo es reducir o minimizar la generación

de residuos. Se centra en disminuir el consumo, o consumir los productos menos contaminantes.

Reutilizar: Como su nombre indica, más productos se vuelven a re-usar, significa menos gastos de dinero. Al reutilizar un producto, se está prolongando su vida útil esperada en el momento de su compra. La mayoría de los bienes pueden incrementar su vida útil, sea reparándolos o utilizando la imaginación para darles otro uso. Reutilizar también incluye la compra de productos de segunda mano, ya que esto alarga la vida útil del producto y a la vez implica una reducción de consumo de productos nuevos.

Reciclar: Hace referencia a la transformación de materiales que ya han sido utilizados, en materia prima para luego generar nuevos productos destinados al consumo. Se centra en someter materiales usados o desperdicios a un proceso de transformación o aprovechamiento para que puedan ser nuevamente utilizables.

Clasificación de los aparatos eléctricos y electrónicos.

La clasificación de estos aparatos se divide en "líneas". Los diferentes tipos de líneas que existen en la actualidad son:

- ✓ Línea IT (Tecnología Informática): rezagos de informática y telecomunicaciones, como ordenadores, notebooks, monitores, impresoras, faxes, telefonía fija, telefonía celular, centrales, etc.
- ✓ Línea Blanca: incluye todos los electrodomésticos de la línea blanca como heladeras, lavarropas, microondas, electrónica de cocina, etc.
- ✓ Línea Marrón: equipos de televisión.
- ✓ Línea Gris: todos los equipos de audio y video [10].

¿Qué materias primas se recuperan al reciclar los RAEES?

La recuperación de las diferentes materias primas, llamados en algunos centros académicos como "minería urbana", buscan sacar provecho de los metales, fundamentalmente cobre, aluminio, aceros, estaño, cinc y los metales preciosos, y sus aleaciones[1] presentes en los rezagos. Esto se debe a que los mismos comienzan a tener un valor significativo en el mercado y se produce una demanda local e internacional.

Con la reducción del uso de compuestos bromados en los plásticos, o metales pesados tales como mercurio o plomo en dispositivos LED, soldaduras y demás, resulta una buena promesa la denominada "minería urbana" que consisten en la obtención de metales base (cobre, estaño) y metales preciosos (oro, paladio, iridio y plata) a partir de la valorización y refinamiento de los RAEE.

En la mayoría de los países latinoamericanos operan gran cantidad de empresas dedicadas a la compra/venta de chatarras ferrosas y no ferrosas. Más del 70 % del acero y del

[1] Combinación, de propiedades metálicas, que está compuesta de dos o más elementos, de los cuales, al menos uno es un metal.

60 % de cobre y el aluminio que se usa a diario en la región proviene del recuperó de chatarras, que son mezclados con materiales virgen [10].

Disposición final de los RAEE.

En la disposición final, intervienen desde empresas de recolección de residuos municipales, que retiran gran parte de los rezagos que son desechados en la actualidad para enviarlos a rellenos sanitarios o basurales municipales, mezclados con residuos domésticos, hasta empresas operadores de residuos peligrosos que procesan, reciclan y/o recuperan partes como insumos de nuevos procesos, especialmente chatarras metálicas o plásticos.

Si bien el re-uso o re-manufactura resulta la mejor opción económica y ambiental, los AEE tienen una vida útil definida. Por lo tanto, estos aparatos cumplen un ciclo y deben ir, en un esquema ideal y sustentable, a:

- Disposición final (incineración, relleno sanitario municipal, etc.).
- Recuperó o reciclado de materias primas.

En la actualidad, Sudamérica se cuenta con una deficiente gestión de disposición final de residuos domésticos o de generación universal. Por lo tanto, cada vez será más relevante la recolección de los RAEE pos-consumo y su procesamiento para recuperar y reciclar las materias primas que los constituyen [10].

En la Argentina, la Ley Nacional N° 24.051 de Residuos Peligrosos, incorporó los lineamientos de la Convención de Basilea, y expresa, en el Artículo Nº 2; - *"Será considerado peligroso, a los efectos de esta ley, todo residuo que pueda causar daño, directa o indirectamente, a seres vivos o contaminar el suelo, el agua, la atmósfera o el ambiente en general"* [11].

La Convención de Basilea involucra los siguientes tipos de residuos:

- ✓ Los llamados "desechos peligrosos"
- ✓ Los llamados "otros desechos" que son residuos domiciliarios o las cenizas de los mismos luego de su incineración.

En países desarrollados, el fabricante está obligado a asumir los costos al final de ciclo de vida del producto. Por lo tanto, él mismo se obliga a replantearse la etapa de diseño con el fin de adaptar al producto a los requisitos de gestión de residuos y de este modo reducir los costos posteriores. En esta etapa inicial, interviene una directiva complementaria, la RoHS (Restricción de ciertas Sustancias Peligrosas en AEE) y en la etapa final, la RAEE.

El objetivo de la RoHS es la reducción de las sustancias peligrosas usadas en la fabricación, lo cual disminuyen con su aplicación los riesgos del tratamiento de los residuos, con lo que se requieren menos precauciones de manipulación. Actualmente, en Sudamérica no existe una directiva RoHS.

El proyecto E-Basura.

Figura 5. Logo proyecto E-Basura.

E-Basura [1] es un Proyecto de Extensión de la Facultad de Informática [12] de la Universidad Nacional de La Plata [13], desarrollado por el laboratorio LINTI [14]. El mismo recibe la línea IT dentro de los RAEE. Los ordenadores recuperados son donadas posteriormente a instituciones sin fines de lucro (escuelas, comedores populares, bibliotecas, ONG´s) para reducir la brecha digital-social en los sectores vulnerables de la comunidad.

Desde el año 2009 el proyecto fue creciendo a partir de la visibilidad que fue adquiriendo en los medios de comunicación a través de notas y filmaciones realizadas, así como también convenios con distintas entidades y donaciones a instituciones sin fines de lucro.

El proyecto se centra en la concientización sobre la problemática de los RAEE, ya que en la actualidad la basura electrónica es vertida a cielo abierto, lo cual resulta altamente contaminante, y no todos los usuarios saben de las alternativas que poseen al momento de deshacerse de este tipo de basura. Los metales y demás elementos que poseen los RAEE son tóxicos y contaminan el medio ambiente, perjudicando el aire, la tierra y el agua.

La contaminación ambiental afecta, por ende, la salud de todos los seres humanos. Profesionales de la salud detallan los problemas que causan para el organismo material como:

- El plomo: perturbaciones en la biosíntesis de la hemoglobina y anemia, incremento de la presión sanguínea, daño a los riñones, abortos, perturbaciones del sistema nervioso y disminución de la fertilidad del hombre.
- El arsénico: veneno letal.
- El selenio: desde sarpullido e inflamación de la piel hasta dolores agudos.
- El cadmio: diarrea, dolor de estómago y vómito severo, fractura de huesos, daños al sistema nervioso, e incluso puede provocar cáncer.
- El cromo: erupciones cutáneas, malestar de estómago, úlcera, daños en riñones e hígado y cáncer de pulmón.
- El níquel: afecta los pulmones, provoca abortos espontáneos.

Todas las donaciones pasan por pruebas de análisis y clasificación. En primer lugar, ingresan a un sector llamado “testing” para clasificar las partes que se encuentran en correcto funcionamiento, como también las que no. Las partes no funcionales son descartadas y enviadas a empresas para su reciclaje; las demás son reparadas, si así lo necesitan, y reutilizadas.

En el caso del armado de nuevos ordenadores, los discos de almacenamiento de las mismas pasan por un proceso de “higienización”, o también llamado “borrado seguro”, para eliminar todo tipo de información, con dos fines principales:

1. Preservar la privacidad de los donantes.
2. Evitar la destrucción de los discos de almacenamiento.

El proceso de higienización es una etapa importante del ciclo de recuperación y reutilización. Asegurar la protección de los datos de los donantes es primordial para que los mismos realicen una completa donación, sin tener que considerar que su información será manipulada. Por lo tanto, el proyecto busca informar a los usuarios y certificar el proceso de higienización con el fin de la obtención y no destrucción de los discos de almacenamiento para su correcta reutilización, ya que la probabilidad de conseguir discos viejos o modelos que ya no son fabricados es baja.

Como consecuencia de la falta de información o certificación sobre la higienización de los datos de los discos de almacenamiento, los porcentajes de donaciones se reducen ya que una parte de los donantes no incluyen los discos duros, por lo tanto un porcentaje de los quipos obtenidos no están completos.

El fin de mi tesina de grado es la investigación y la comprobación sobre la eficiencia de los diferentes algoritmos de borrado seguro, a través de diferentes herramientas.

En el caso específico que los discos se encuentren dañados, no podrán pasar por la etapa de higienización. Por lo tanto, se consideran no reutilizables por lo que se opta por otra forma de destrucción permanente de los datos, la destrucción física; y así siempre se asegura la privacidad de los miembros donantes.

El material que no puede ser reutilizado es enviado a empresas con certificación ambiental para su disposición final y segura. En la Argentina, ya operan varias empresas en el Mercado de Gestión de los Rezagos Electrónicos, centrándose en telefonía, informática y circuitos impresos de diverso origen. Entre éstas empresas se encuentran Scrap y Rezagos SRL [15], Silkers SA [16], Scrapex SRL [17], Botrade SRL [18] y Dalafer SRL [19].

El proyecto E-Basura [1] trabaja con un convenio con Scrap y Rezagos SRL [15]**,** Silkers S.A. [16] y Dalafer [19].

Dispositivos de almacenamiento.

En el presente capítulo, se profundizará sobre el dispositivo de almacenamiento en estudio, discos duros, como también el Sistema Operativo en el cual será montado y el formato que se le otorgará.

Ejemplos dispositivos de almacenamiento.

En la actualidad la diversidad de dispositivos de almacenamiento es muy amplia. Los tipos de dispositivos de almacenamiento destacados son:

Discos duros.

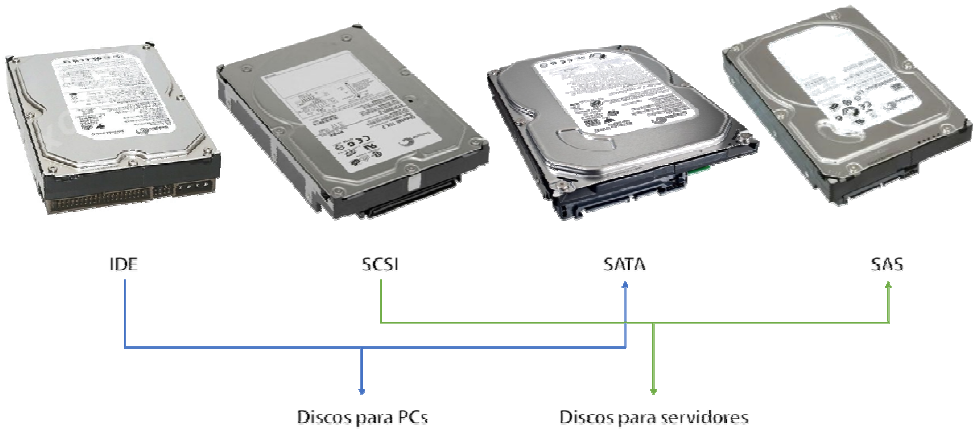


Figura 6. Ejemplos discos duros.

Dispositivos de Estado Sólido (SSD - Solid-State Drive).

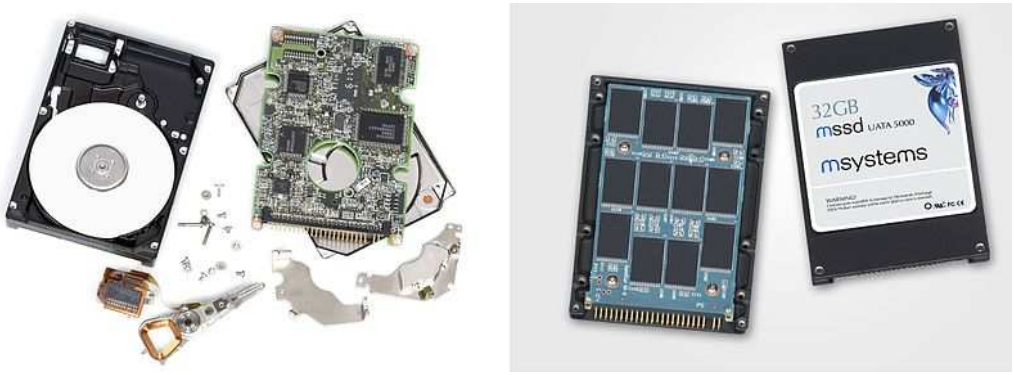


Figura 7. Disco Duro vs SSD, composición interna.

Cintas magnéticas DAT/DDS/ LTO.

Figura 8. Ejemplos Cintas magnéticas DAT/DDS (Digital Audio Tape/Digital Data Storage).

Figura 9. Ejemplo LTO (Linear Tape-Open).

CD/ DVD/BD.

Figura 10. Ejemplo CD (Compact Disc)/DVD (Digital Versatile Disc)/BD (Blu-ray Disc).

Sistemas de almacenamiento en red o NAS (Network Attached Storage).

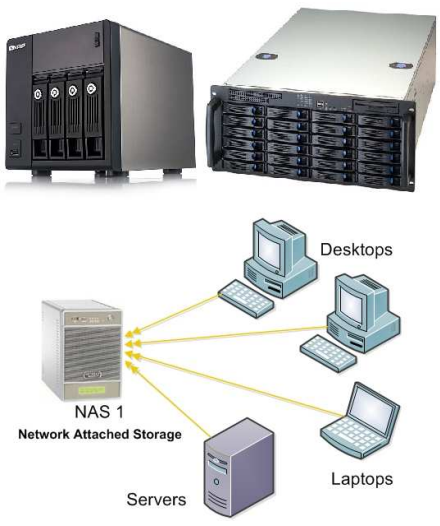


Figura 11. Ejemplo de almacenamiento en red.

Memoria USB (pendrive).

Figura 12. Ejemplo memorias USB.

Sistemas de archivos.

Cada dispositivo de almacenamiento puede emplear uno o varios sistemas de archivos, dependiendo su utilidad. Los sistemas empleados en los discos duros, organizan la información contenida en el mismo. Existen dispositivos que emplean sistemas de archivos idénticos o similares a los de los discos duros, como son las memorias USB. Por lo tanto, la información proporcionada en este capítulo también será válida para este tipo de dispositivos.

El conocimiento interno de los sistemas de archivos permitirá comprender y llevar a cabo de forma más eficiente la destrucción definitiva de la información, como también la comprobación de que no se puede recuperar dicha información de los discos duros.

En este capítulo, a nivel de ejemplo, se presentan los sistemas de archivos en disco más empleados en el mundo de los ordenadores, descartando otros tipos de sistemas de archivos, como los empleados en red, CD/DVD/BD, etc.

Todo disco duro, particionado o no, para que posea un sistema de archivos se le debe dar formato. Por ejemplo, Windows utiliza la utilidad *format* para ello, mientras que Unix utiliza la utilidad *mkfs*. Durante el formateo se suele llevar a cabo una comprobación de la superficie del disco para desechar sectores defectuosos[2]. Desde el punto de vista del Sistema Operativo cada sistema de archivos es visto como un volumen. El Sistema Operativo asocia a cada volumen un identificador único. Por ejemplo, Windows típicamente asocia una letra a cada volumen (C:, D:, etc.), mientras que Unix asocia un nombre de dispositivo a cada volumen (/dev/hda1, /dev/hda2, etc).

Un sistema de archivos no es más que una gran estructura de datos que ocupa la totalidad del volumen, en la cual se almacenan datos y programas, así como información de estado y localización de éstos.

Los sistemas de archivos de disco duro típicos en el mundo de los ordenadores dependen del Sistema Operativo que esté instalado en el mismo. En la siguiente tabla se

[2] En el caso de Windows es la opción por defecto, mientras que en Linux debe especificarse con la opción –c de la utilidad mkfs.

detallan los diferentes sistemas de archivos que existen y en qué Sistema Operativo son admitidos:

Sistema Operativo	Tipos de sistema de archivos admitidos
DOS	FAT16
Windows 95	FAT16
Windows 95 OSR2	FAT16, FAT32
Windows 98	FAT16, FAT32
Windows NT4	FAT, NTFS
Windows 2000/XP	FAT, FAT16, FAT32, NTFS
Windows Vista/7/8	FAT, FAT32, NTFS
Linux	Ext2, Ext3, ReiserFS, Linux Swap (FAT16, FAT32, NTFS)
MacOS	HFS (Sistema de Archivos Jerárquico), MFS (Sistemas de Archivos Macintosh)
OS/2	HPFS (Sistema de Archivos de Alto Rendimiento)
SGI IRIX	XSF
FreeBSD, OpenBSD	UFS (Sistema de Archivos Unix)
Sun Solaris	UFS (Sistema de Archivos Unix)
IBM AIX	JFS (Sistema Diario de Archivos)

Durante el proceso de formateo, la gran estructura de datos que constituye el sistema de ficheros se inicializa. Una vez que una partición ha sido formateada, ésta es accesible para la lectura y escritura de datos.

Características de los sistemas de archivos.

Aunque todos los sistemas de archivos persiguen el mismo propósito, no todos incorporan la misma funcionalidad ni son igual de eficientes. A continuación, se resumen las principales características de los sistemas de archivos, las cuales servirán como base para comparar unos con otros:

- **Rendimiento**. La velocidad de las operaciones de lectura y escritura en el disco no sólo dependen de aspectos de hardware del sistema como la velocidad del disco, sino también del sistema de archivos empleado. A la hora de evaluar las mejoras de rendimiento, debe tenerse en cuenta que estas dependen mucho del tamaño de los archivos involucrados. Por lo general, los sistemas de archivos más modernos suelen incorporar mejoras de rendimiento.
- **Fiabilidad.** Algunos sistemas de archivos son más tolerantes a fallos que otros. Por ejemplo, hay sistemas de archivos que incluyen copias de seguridad de las estructuras de datos clave del sistema de archivos, detectan sectores defectuosos que son re-mapeados a sectores libres y llevan a cabo un registro de transacciones (journaling). La inclusión de registro de transacciones tiene un impacto negativo sobre el rendimiento, pues la escritura en el archivo de registro tiene un coste temporal.
- **Limitaciones de tamaño.** Todos los sistemas de archivos tienen limitaciones en cuanto al tamaño máximo del sistema de archivos soportado, máximo tamaño de archivos, máximo número de caracteres en el nombre de archivos, etc.

- **Encriptación.** La información se guarda en el disco de forma encriptada, lo que dificulta la obtención de información del disco duro. La encriptación se lleva a cabo por software, por lo que afecta negativamente al rendimiento del sistema. La clave de encriptación suele guardarse en el sistema de archivos encriptada mediante una clave del usuario.
- **Compresión**. Algunos sistemas de archivos permiten la compresión de archivos de forma transparente al usuario. De nuevo, esto afecta negativamente al rendimiento del sistema.
- **Metadatos que incorpora.** Los sistemas de archivos no sólo almacenan archivos (datos), sino información acerca de los archivos (metadatos). Ejemplo de metadatos son las fechas de creación y acceso, y las listas de control de acceso.
- **Cuotas**. Permiten establecer límites sobre la capacidad de disco usada por usuarios o grupos de usuarios.

El sistema de archivos NTFS.

En el estudio y pruebas realizadas se le da principal importancia al sistema de archivos NTFS, ya que las pruebas de recuperación se realizan sobre máquinas con el Sistema Operativo Windows 7. Para que este Sistema Operativo pueda montar el disco y así acceder al mismo, se le debe dar formato, y el otorgado en este caso es el NTFS. Una vez dado formato al disco duro, se crean archivos natos del mismo. Por lo tanto antes de sacar conclusiones sobre la destrucción y recuperación de datos debo introducir sobre el sistema de archivos utilizado.

Microsoft introdujo un nuevo sistema de archivos denominado NTFS, con la introducción del Sistema Operativo Windows NT, precursor de las versiones actuales de Windows. Pocos años después se convirtió en el sistema de archivos para discos duros estándar en todas las versiones de Windows.

La idea clave del sistema de archivos NTFS es que los metadatos se almacenan también en archivos. Por lo tanto, las estructuras de control del sistema de archivos no están almacenadas en lugares prefijados, sino que al ser archivos, pueden ubicarse en cualquier lugar del disco, como cualquier otro archivo. La única excepción es el archivo **$Boot**, ubicado al principio del volumen.

La estructura de datos clave del sistema de archivos NTFS es el MFT (Master File Table - Tabla maestra de archivos). Se trata de un archivo de nombre **$MFT** que contiene al menos una entrada por cada archivo y directorio del sistema. La ubicación del archivo MFT está definida en el archivo **$Boot**. Todos los datos almacenados en un volumen están contenidos en archivos, incluyendo las estructuras de datos utilizadas para localizar y recuperarlos, los datos de rutina de carga, y el mapa de bits que registra el estado de asignación de todo el volumen (los metadatos NTFS). El almacenamiento de “todo en archivos” permite poder localizar y mantener fácilmente los datos para el sistema de archivos, como también para que cada archivo separado pueda estar protegido por un descriptor de seguridad. Además, si un sector concreto del disco no funciona correctamente, NTFS puede reubicar los archivos de metadatos

para evitar que el disco se convierta en inaccesible. El archivo MFT es el corazón de la estructura del volumen NTFS.

El archivo MFT contiene un registro para cada archivo en el volumen. Además, cada volumen NTFS incluye un conjunto de archivos de metadatos que contienen la información que se utiliza para implementar la estructura del sistema de archivos. Cada uno de los archivos de metadatos NTFS tiene un nombre que comienza con un signo de dólar ($), aunque los signos están ocultos. Por ejemplo, el nombre de archivo del MFT es de **$MFT**. El resto de los archivos en un volumen NTFS son archivos de usuario y directorios normales.

El volumen NTFS está dividido en tres diferentes zonas, mostradas en la ***figura 13.***

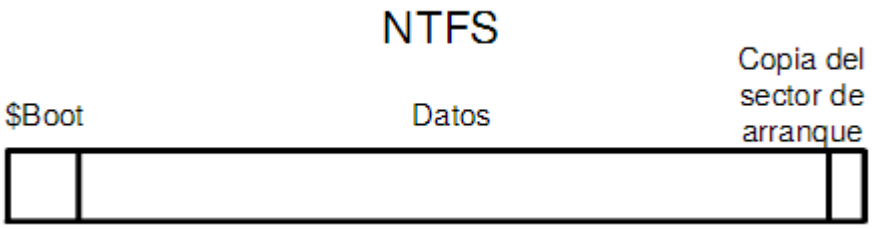


Figura 13. Zonas del volumen NTFS.

La zona de datos incluye todos los archivos NTFS excepto el archivo **$Boot**.

Al final del volumen NTFS se deja una copia del primer sector del volumen, para que en caso de pérdida, el volumen no sea inaccesible.

El archivo **$Boot** es el único archivo NTFS ubicado en una posición fija dentro del volumen. Está formado por los 16 primeros sectores del volumen. El primero de sus sectores es el sector de arranque del volumen NTFS, el cual coincide con el primer sector, el sector 0. Por lo tanto, el archivo **$Boot** comienza en el sector 0.

Durante el arranque desde la partición NTFS, el sector de arranque anterior es cargado en memoria y se lleva a cabo un salto a la primera posición en memoria del sector. En la primera posición se encuentra una instrucción de salto que produce el salto a la posición la primera instrucción del Initial Program Loader (IPL). El IPL es el fragmento de código que comienza en la posición 0054h y termina en la posición 01FDh del sector de arranque, como se muestra en el ejemplo de la ***figura 14***. Su misión es cargar el archivo *ntldr* que arranca el Sistema Operativo. Esto requiere la lectura previa del MTF, para localizar el directorio raíz del sistema de archivos NTFS y así poder localizar el archivo *ntldr* y cargarlo en memoria. Debido a la complejidad de acceso al sistema de archivos NTFS, el IPL carga en memoria los 15 sectores siguientes, los cuales constituyen la extensión del IPL, y prosigue la ejecución. En un momento dado de su ejecución, el IPL carga en memoria el archivo *ntldr* y le transfiere el control. Al final del sector de arranque se encuentra la firma 55AAh, como se puede observar en el ejemplo de la ***figura 14***.

Figura 14. Ejemplo de sector de arranque de un volumen con formato NTFS.

En la ***figura 14*** se pueden observar que desde la posición 0003h a la 000Ah, se define una etiqueta de texto que identifica el sistema de archivos o fabricante, en este caso NTFS. Esta etiqueta resulta muy útil para buscar una partición NTFS que ha sido eliminada y así poder recuperarla. También se puede observar que desde la posición 0183h a la 01FDh se incluye un mensaje de error del IPL. En las posiciones 1FEh y 1FFh contienen la firma 55AAh. Las posiciones 000Bh a 0053h contienen el BIOS Parameter Block (BPB), el cual describe la geometría de la partición y características básicas del sistema de archivos NTFS, como es la ubicación del archivo **$MFT**.

El archivo de sistema **$MTF** es la pieza clave del sistema de archivos NTFS, pues indica donde se pueden encontrar los archivos y los directorios. Cada archivo o directorio tiene al menos una entrada en el MFT. El tamaño de estas entradas se especifica en el sector de arranque del volumen.

Toda la información administrativa del sistema de archivos se almacena en unos archivos denominados archivos de metadata. Las primeras entradas del MFT están reservadas para estos archivos.

A continuación se listarán los archivos de metadata ordenados a partir de su índice en el MTF, comenzando por el índice 0:

Índice 0 **$MFT**

Índice 1 **$MFTMirr**

Índice 2 **$LogFile**

Índice 3 **$Volume**

Índice 4 **$AttrDef**

Índice 5 **/** (Directorio raíz)

Índice 6 **$Bitmap**

Índice 7 **$Boot**

Índice 8 **$BadClus**

Índice 9 **$Secure**

Índice 10 **$Upcase**

Índice 11 **$Extend**

Como se puede observar, el archivo **$MFT** tiene la entrada 0 dentro del MFT (es decir, el MFT se describe a sí misma a través de dicha entrada). La entrada 5 se corresponde con el directorio raíz. La entrada 11, se corresponde al archivo **$Extend** que es un directorio empleado para poder añadir más archivos de metadata. En la práctica también se incluye los archivos de metadata **$Objid** y **$Quota**.

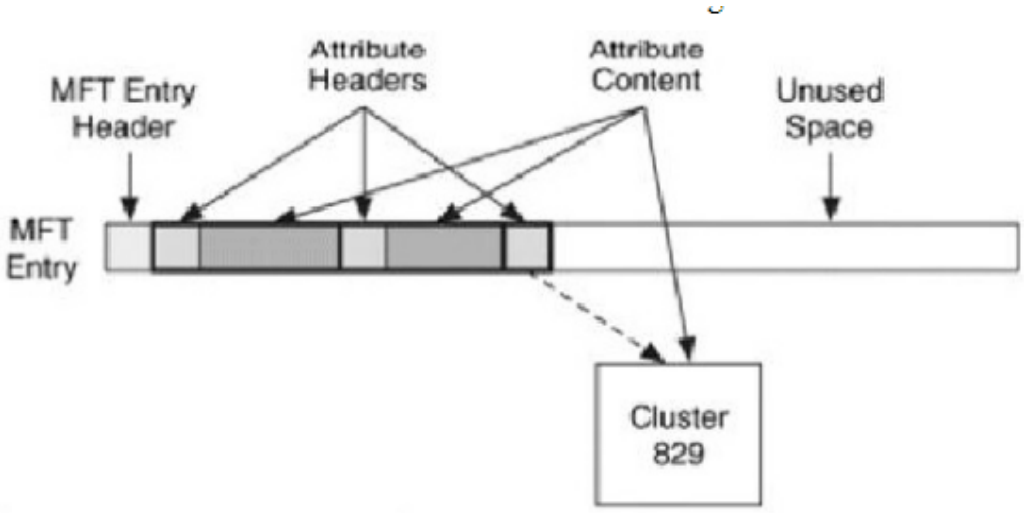


Figura 15. Estructura de una entrada MFT.

Como se puede observar en la ***figura 15***, cada entrada del MFT comienza con una cabecera (MFT Entry Header). A continuación de la cabecera vienen los atributos, los cuales son estructuras de datos que almacenan un tipo de datos específico. Prácticamente todo son atributos, desde el nombre de un archivo, fecha de creación e incluso su contenido. Cada

atributo tiene una cabecera que lo identifica (Attributes Headers) y un contenido (Attributes Content) justo después. Cuando todos los atributos no caben en la entrada del MFT, lo cual es habitual, la cabecera indica los sectores en los que se encuentra, como por ejemplo el Cluster 829, ilustrado en la ***figura 15***.

El archivo **$MFT** comienza con un tamaño inicial y crece progresivamente según se van creando nuevos archivos y directorios. Los sectores al lado de la MFT son los últimos en asignar, para evitar la fragmentación de la MFT cuando esta crece.

A continuación se detalla la información que contiene cada archivo de metadata:

- ✓ El archivo **$MFTMirror** contiene una copia de las primeras entradas de la MFT, las cuatro primeras entradas **($MFT**, **$MFTMirr**, **$LogFile** y **$Volume**) suelen ubicarse en el centro del volumen para poder ser accedido en caso de que el archivo MFT esté corrupto o inaccesible. Por lo tanto, la copia parcial del archivo MFT se utiliza para localizar los archivos de metadatos si una parte del archivo MFT no se puede leer por alguna razón.
- ✓ El archivo **$LogFile** contiene el registro de las transacciones llevadas a cabo en el disco. NTFS utiliza el archivo de registro para registrar todas las operaciones que afectan a la estructura del volumen NTFS, incluyendo la creación de archivos o los comandos, como copiar, que alteran la estructura de directorios. El archivo de registro se utiliza para recuperar un volumen NTFS después de un fallo del sistema.
- ✓ El **/** (directorio raíz) contiene un índice de los archivos y directorios almacenados en la raíz de la estructura de directorios NTFS. Cuando se pregunta a NTFS para abrir un archivo, comienza la búsqueda del mismo en el registro de archivos del directorio raíz. Luego de abrirlo, NTFS almacena una referencia del archivo MFT para que se pueda acceder directamente al registro MFT del archivo cuando se lee y escribir mas tarde.
- ✓ El archivo **$Volume** contiene información sobre el volumen, como el nombre del volumen, la versión de NTFS para el que se ha formateado el volumen, etc.
- ✓ El archivo **$AttrDef** contiene información sobre los atributos, tales como sus nombres, sus identificadores y sus tamaños. Define los tipos de atributos soportados sobre el volumen e indica si pueden ser indexados, se recuperó durante una operación de recuperación del sistema, y entre otros.
- ✓ El archivo **$Bitmap** contiene información sobre el estado de cada sector. Dispone de un bit para cada sector que indica si está asignado o no.
- ✓ El archivo **$Boot** almacena el código de arranque de Windows. Para que el sistema arranque, el código de arranque debe estar ubicado en una zona específica del disco. Durante el proceso de formateo, sin embargo, el comando *format* define esta zona como un archivo mediante la creación de un registro de archivo para ello. Crear el archivo de arranque NTFS permite que se adhiera a su estructura de almacenamiento de “hacer todo un archivo”. El archivo de arranque, como también archivos de metadatos NTFS, pueden estar protegidas individualmente por medio de los descriptores de seguridad que se aplican a todos los objetos de Windows. El uso del modelo "todo en el disco es

un archivo" también significa que el arranque puede ser modificado por el archivo de E/S normal, aunque el archivo de arranque está protegida contra ediciones.

- ✓ El archivo **$BadClus** contiene una lista con los sectores defectuosos.
- ✓ El archivo **$Secure** contiene información de seguridad y control de acceso a los archivos y directorios. Almacena la base de datos del descriptor de seguridad en todo el volumen. Los archivos NTFS y directorios individualmente tienen descriptores de seguridad ajustables, pero para ahorrar espacio, NTFS almacena los ajustes en un archivo común, lo que permite que los archivos y directorios que tienen la misma configuración de seguridad para hacer referencia a la misma descriptor de seguridad. En la mayoría de los entornos, los árboles de directorios completos tienen la misma configuración de seguridad, por lo que esta optimización proporciona un archivo importante del sistema guardado.
- ✓ El archivo **$Upcase** contiene la versión mayúscula de cada carácter Unicode. Incluye una tabla de conversión entre caracteres en mayúsculas y minúsculas.
- ✓ El archivo **$Objid** contiene una lista de atributos de un cierto tipo empleados en el volumen.
- ✓ El archivo **$Quota** lleva la contabilidad de las cuotas de disco.
- ✓ El archivo **$Extend** contiene varios archivos de metadatos con sus extensiones. El mismo incluye, el archivo de objeto identificador (**$ObjId**), el archivo de cuota (**$Quota**), el archivo de diario de cambios (**$UsnJrnl**), el archivo de punto de análisis (**$Reparese**) y el directorio de administración de recursos predeterminado (**$RmMetadata**). Estos archivos almacenan la información relacionada con las características opcionales de NTFS.
- ✓ El archivo **$RmMetadata** contiene directorios relacionados con el soporte transaccional de NTFS (TxF), que incluye el directorio de registro de transacciones (**$TxfLog**), el directorio de aislamiento de transacción (**$TxF**), y el directorio de reparación transacción (**$Repair**). El $TxfLog contiene el archivo de registro de base de TxF (**$TxfLog.blf**) y cualquier número de archivos contenedores de registro, dependiendo del tamaño del registro de transacciones, pero siempre contiene al menos dos:
    1. Administrador de Transacciones del Kernel (Kernel Transaction Manager KTM) secuencia de registro (**$TxfLogContainer00000000000000000001**).
    2. Secuencia de registro TxF (**$TxfLogContainer00000000000000000002**).

  Y además, el **$TxfLog** también contiene la secuencia de TxF página de edad (**$Tops**).

Higienización de los datos.

Cuando termina el ciclo de vida de la información, la misma debe ser destruida a través de métodos que aseguren la no recuperación de la misma, estos son llamados métodos de "borrado seguro" o de "higienización de los datos". Cuando el fin de la destrucción es la no recuperación, se debe optar por la correcta higienización de los datos a través de diferentes métodos, los cuales pueden ser físicos o lógicos.

Métodos de higienización de los datos.

Los medios eficaces, tanto físicos como lógicos, que evitan completamente la recuperación de los datos contenidos en los dispositivos de almacenamiento son:

Desmagnetización.

La desmagnetización es un método físico de destrucción de los datos, el cual consiste en la exposición de los soportes de almacenamiento a un potente campo magnético, proceso que elimina los datos almacenados en el dispositivo. Este método es válido para la destrucción de datos de los dispositivos magnéticos.

Cada dispositivo, según su tamaño, forma y tipo de soporte magnético, necesita de una potencia específica para asegurar la completa polarización de todas las partículas.

Los inconvenientes que presenta este método son:

- Los dispositivos deben trasladarse al lugar donde se encuentre el desmagnetizador, lo que implica un costo de transporte y el aseguramiento de la cadena de custodia.
- Tras el proceso, estos dispositivos dejan de funcionar correctamente y por lo tanto requieren de un reciclado que sea respetuoso con el medio ambiente.
- Para comprobar que todos los datos han sido borrados completamente es necesario acceder a los dispositivos. Al no funcionar correctamente, este acceso no es posible, lo que dificulta la certificación del proceso.
- Es recomendable analizar el campo aplicado para desmagnetizar cada dispositivo. En ocasiones se opta por aplicar la máxima potencia, desperdiciando energía de forma innecesaria.

Destrucción física.

Es un método físico de destrucción de los datos. El objetivo de la destrucción física es la inutilización del soporte que almacena la información en el dispositivo para evitar la recuperación posterior de los datos contenida en él.

Existen diferentes tipos de técnicas y procedimientos para la destrucción de medios de almacenamiento:

- ***Desintegración, pulverización, fusión e incineración:*** son métodos diseñados para destruir por completo los medios de almacenamiento. Estos métodos suelen llevarse a cabo en una destructora de metal o en una planta de incineración autorizada, con las capacidades específicas para realizar estas actividades de manera eficaz, segura y sin peligro.
- ***Trituración:*** las trituradoras de papel se pueden utilizar para destruir los medios de almacenamiento flexibles. El tamaño del fragmento de la basura debe ser lo suficientemente pequeño para que haya una seguridad razonable en proporción a la confidencialidad de los datos que no pueden ser reconstruidos. Los medios ópticos de almacenamiento (CD, DVD, magneto-ópticos), deben ser destruidos por pulverización, trituración de corte transversal o incineración. Cuando el material se desintegra o desmenuza, todos los residuos se reducen a cuadrados de cinco milímetros (5mm) de lado.

Como todo proceso de higienización de datos, su correcta realización implica la imposibilidad de recuperación posterior por ningún medio conocido. En el caso de los discos duros se deberá asegurar que los platos internos del disco han sido destruidos eficazmente.

Los métodos de destrucción física pueden llegar a ser seguros totalmente en cuanto a la destrucción real de los datos pero presenta algunos inconvenientes:

- Implican la utilización de métodos industriales de destrucción distintos para cada soporte.
- Obligan al transporte de los dispositivos a un centro de reciclaje adecuado, obligando a extremar las medidas de custodia para asegurar el control de los dispositivos.
- Los residuos generados deben ser tratados adecuadamente.
- No permite la reutilización de los dispositivos.
- La certificación de la operación de destrucción es compleja, ya que no es posible acceder a los dispositivos para confirmar que la información ha sido eliminada y se deben hacer comprobaciones manuales, como fotografías y anotación de número de serie que certifique que el dispositivo ha sido eliminado.

Figura 16. Ejemplos de discos destruidos con métodos de destrucción física.

Sobre-escritura.

Es un método lógico de destrucción de los datos. La sobre-escritura consiste en la escritura de un patrón de datos sobre los datos contenidos en los dispositivos de almacenamiento. Para asegurar la completa destrucción de los datos se debe escribir la totalidad de la superficie de almacenamiento.

El método de sobre-escritura se realiza accediendo al contenido del dispositivo y modificando los valores almacenados, por lo que no se puede utilizar en aquellos que están dañados ni en los que no son regrabables, como los CD's y DVD's.

Este método para la destrucción segura de la información es el que dispone del mayor número de ventajas entre las que se pueden destacar:

- Se puede utilizar para todos los dispositivos regrabables.
- Tras el proceso de borrado es posible acceder de nuevo al dispositivo para certificar que todos los datos que se encontraban almacenados previamente han sido sustituidos por el patrón de borrado.
- Es posible realizar la operación de borrado en cualquier ubicación, evitando la necesidad de guardar la cadena de custodia en el transporte a un centro de reciclaje autorizado.
- Permite la reutilización de los dispositivos.
- La certificación es sencilla ya que la sobre-escritura se realiza a través de programas de software dedicados a la destrucción de datos, que proveen un conjunto de algoritmos que poseen cada uno un patrón de escritura específico, la mayoría de éstos permite la generación de un log donde se certifica el éxito de la operación detallando la misma.

Siendo el único inconveniente que no es posible utilizarlo en aquellos dispositivos que no sean regrabables o en aquellos que tengan alguna avería física o posea sectores dañados.

En la siguiente tabla se realiza una comparación entre los diferentes métodos de higienización de los datos, citando sus ventajas (✓) y desventajas (**X**):

Destrucción Física	Desmagnetización	Sobre-Escritura
✓ Eliminación de forma segura de la información.	✓ Eliminación de forma segura de la información.	✓ Eliminación de forma segura de la información.
X Un sistema de destrucción para cada soporte.	**X** Una configuración del sistema para cada soporte.	✓ Una única solución para todos los dispositivos.
X Dificultad de certificación del proceso.	**X** Dificultad de certificación del proceso.	✓ Garantía documental de la operación.
X Necesidad de transportar los equipos a una ubicación externa.	**X** Necesidad de transportar los equipos a una ubicación externa.	✓ Posibilidad de eliminación en las propias oficinas.
X Medidas extraordinarias para garantizar la cadena de custodia.	**X** Medidas extraordinarias para garantizar la cadena de custodia.	✓ Garantía de la cadena de custodia.
✓ Destrucción de dispositivos, no Regrabables, ópticos.	**X** Sólo válido para dispositivos de almacenamiento magnético.	**X** No válido para dispositivos no regrabables ni ópticos.
X Destrucción definitiva y dificultad del reciclaje completo de los dispositivos.	**X** Tras el proceso el dispositivo deja de funcionar correctamente.	✓ Reutilización de los dispositivos con garantías de funcionamiento.

Según cuál sea el tipo de dispositivo de almacenamiento, se le puede aplicar uno o varios métodos de higienización de los datos. En la siguiente tabla se listan los diferentes soportes, junto a su respectivo tipo, y los correspondientes métodos de higienización que se les puede aplicar:

Soporte	Tipo	Destrucción Física	Desmagnetización	Sobre-escritura
Discos Duros	Magnético	✓	✓	✓
Discos Flexibles	Magnético	✓	✓	✓
Cintas de Backup	Magnético	✓	✓	✓
CD/DVD	Óptico	✓	**X**	**X**
CD/DVD regrabable	Óptico	✓	**X**	✓
BD (Blu-ray Disc)	Óptico	✓	**X**	**X**
Memoria USB	Electrónico	✓	**X**	✓[3]

[3] A pesar que actualmente la sobre-escritura es un método seguro de destrucción de datos para dispositivos basados en memorias de estado sólido Nand-Flash, diversos trabajos de investigación forense apuntan la posibilidad de recuperación posterior con técnicas de lectura directa de los chips de memoria. Uno de estos estudios es el de la Universidad de California http://nvsl.ucsd.edu/sanitize/.

Destrucción física: Dispositivos disponibles en el mercado.

Agencias de inteligencia de diferentes gobiernos (Reino Unido, China, Korea) tienen herramientas sofisticadas como Microscopios de fuerza magnética, Microscopios atómicos, Análisis de imágenes que estudian los residuos magnéticos producidos en la escritura de antiguos datos en los dispositivos los cuales permiten la detección de valores anteriores de bits en las áreas borradas; incluso una vez utilizados su propio método. Por lo tanto, existen procedimientos de seguridad de estas Agencias donde consideran que un disco sobre-escrito de manera segura sigue siendo un material aun sensible, por lo que optan por la destrucción física del dispositivo de almacenamiento ya que la misma deja inaccesible la información.

En el mercado existen diferentes dispositivos de destrucción física. A continuación como modo de ejemplo se citan algunos productos que realizan la destrucción física de, en este caso, los discos duros.

1. **Desmagnetizador – Ontrack® Eraser™ Degausser [20]**

Figura 17. Imagen del desmagnetizador Ontrack® Eraser™ Degausser.

2. **Destrucción de la información en unidades de disco duro - Desmagnetizador HDD [21]**

Tamaño máximo:	100
Tiempo de borrado el primer disco duro:	5-10 sec.
Campo magnético (Oe):	5.500 / 0,55 Tesla
Peso bruto (kg):	3 kg
Peso neto (kg):	2,3 kg
Profundidad (cm):	18 cm
Alto (cm):	7 cm
Ancho (cm):	14 cm

Figura 18. Imagen dispositivo intimus 5000 junto a su ficha técnica.

Descarga capacitiva:	X
Tamaño máximo:	149/109/38 mm
Consumo de energía en carga:	4,0
Consumo de energía en espera:	0,2
Consumo de energía al borrar:	0,5
Tiempo de borrado el primer disco duro:	60
Tiempo de ciclo repetitivo:	60
Campo magnético (Oe):	8.300 / 0,83 Tesla
Tensión nominal (voltios):	230 Voltios
Peso bruto (kg):	22 kg
Peso neto (kg):	19 kg
Profundidad (cm):	31 cm
Alto (cm):	19 cm
Ancho (cm):	45 cm

Figura 19. Imagen dispositivo intimus 8000 junto a su ficha técnica.

Descarga capacitiva:	X
Tamaño máximo:	149/109/38 mm
Consumo de energía en carga:	7,0
Consumo de energía en espera:	0,2
Consumo de energía al borrar:	0,5
Tiempo de borrado el primer disco duro:	12
Campo magnético (Oe):	9000 / 0,9 Tesla
Tensión nominal (voltios):	230 Voltios
Peso bruto (kg):	35 kg
Peso neto (kg):	25 kg
Profundidad (cm):	33 cm
Alto (cm):	48 cm
Ancho (cm):	31 cm
Dimension en posición básica - An cm:	31
Dimension en posición básica - Prof cm:	58
Dimension en posición básica - Al cm:	48

Figura 20. Imagen dispositivo intimus 9000 junto a su ficha técnica.

Descarga capacitiva:	Sí
Tamaño máximo:	149/109/38 mm
Tiempo de borrado el primer disco duro:	45 sec
Campo magnético (Oe):	20.000 Gauss, 2.0 Tesla
Tensión nominal (voltios):	230 Voltios
Peso neto (kg):	66 kg
Profundidad (cm):	44 cm
Alto (cm):	48 cm
Ancho (cm):	55 cm

Figura 21. Imagen dispositivo intimus 20000 junto a su ficha técnica.

Destrucción lógica: Algoritmos de Higienización de datos.

Cuando se realiza la sobre escritura de los discos regrabables se utilizan los llamados "algoritmos de borrado seguro" o "algoritmos de higienización de datos". Existen diferentes algoritmos, la principal diferencia entre ellos es el número de pasadas (desde 1 a 35) y la información que escriben (0, 1 o aleatoria).

A continuación se realiza un resumen de los algoritmos que existen junto al número de pasadas que realizan y la información que escriben en cada una de ellas [34]:

1. ***One pass zeros (1 pass) or One pass random (1 pass):*** Al utilizar cualquiera de estos dos métodos, el número de pasadas es fijo y no puede cambiarse. Cuando el cabezal de escritura pasa a través de un sector, se escribe sólo ceros o una serie de caracteres random.
2. ***User Defined (Definido por el usuario):*** Se indica el número de veces que el cabezal de escritura pasa por encima de cada sector. Cada paso de sobre-escritura se realiza con un buffer que contiene el patrón que ha especificado (cadena ASCII).
3. ***US DoD 5220.22-M (3 passes, verify):*** El cabezal de escritura pasa por encima de cada sector en tres ocasiones. La primera vez es con ceros (0x00), la segunda vez con 0xFF y la tercera vez con caracteres random. Hay un último pase para verificar caracteres aleatorios mediante la lectura.
4. ***US DoS 5220.22-m (ECE) (7 passes, verify):*** El cabezal de escritura pasa por encima de cada sector siete veces (0x00, 0xFF, Random, 0x96, 0x00, 0xFF, Random). Hay un último pase para verificar caracteres aleatorios mediante la lectura.
5. ***Canadian OSP-II (7 passes, verify):*** El cabezal de escritura pasa por encima de cada sector siete veces (0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF, Random). Hay un último pase para verificar caracteres aleatorios mediante la lectura.
6. ***Greman VSITR (7 passes, verify):*** El cabezal de escritura pasa por encima de cada sector en siete ocasiones (0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF, 0xAA). Hay un último pase para verificar caracteres aleatorios mediante la lectura.
7. ***Russian GOST p50739-95 (2 passes, verify):*** El cabezal de escritura pasa por encima de cada sector dos veces (0x00, Random). Hay un último pase para verificar caracteres aleatorios mediante la lectura.
8. ***US Army AR380-19 (3 passes, verify):*** El cabezal de escritura pasa por encima de cada sector en tres ocasiones. La primera vez con 0xFF, segundo tiempo con ceros (0x00) y la tercera vez con caracteres random. Hay un último pase para verificar caracteres aleatorios mediante la lectura.
9. ***Peter Gutmann (35 passes, verify):*** El cabezal de escritura pasa por encima de cada sector 35 veces. A continuación se listan la escritura en las 35 pasadas:

Número de pasada	Datos escritos
1	Random
2	Random
3	Random
4	Random
5	01010101 01010101 01010101 0x55

6	10101010 10101010 10101010 0xAA
7	10010010 01001001 00100100 0x92 0x49 0x24
8	01001001 00100100 10010010 0x49 0x24 0x92
9	00100100 10010010 01001001 0x24 0x92 0x49
10	00000000 00000000 00000000 0x00
11	00010001 00010001 00010001 0x11
12	00100010 00100010 00100010 0x22
13	00110011 00110011 00110011 0x33
14	01000100 01000100 01000100 0x44
15	01010101 01010101 01010101 0x55
16	01100110 01100110 01100110 0x66
17	01110111 01110111 01110111 0x77
18	10001000 10001000 10001000 0x88
19	10011001 10011001 10011001 0x99
20	10101010 10101010 10101010 0xAA
21	10111011 10111011 10111011 0xBB
22	11001100 11001100 11001100 0xCC
23	11011101 11011101 11011101 0xDD
24	11101110 11101110 11101110 0xEE
25	11111111 11111111 11111111 0xFF
26	10010010 01001001 00100100 0x92 0x49 0x24
27	01001001 00100100 10010010 0x49 0x24 0x92
28	00100100 10010010 01001001 0x24 0x92 0x49
29	01101101 10110110 11011011 0x6D 0xB6 0xDB
30	10110110 11011011 01101101 0xB6 0xDB 0x6D
31	11011011 01101101 10110110 0xDB 0x6D 0xB6
32	Random
33	Random
34	Random
35	Random

10. ***US Air Forece 5020 (3 passes, verify):*** El cabezal de escritura pasa por encima de cada sector en tres ocasiones. La primera vez con caracteres random, la segunda vez con ceros (0x00) y la tercera vez con 0xFF. Hay un último pase para verificar caracteres aleatorios mediante la lectura.
11. ***HMG IS5 BaseLine (1 pass, verify) (línea base):*** sobrescribe la superficie del disco con sólo ceros (0x00). Hay un último pase para verificar caracteres aleatorios mediante la lectura.
12. ***HMG IS5 Enhanced (3 passes, verify) (mejorado):*** el cabezal de escritura pasa por encima de cada sector en tres ocasiones. La primera vez con ceros (0x00), la segunda vez con 0xFF y la tercera vez con caracteres random. Hay un último pase para verificar caracteres aleatorios mediante la lectura.
13. ***Navso P-5329-26 (RL) (3 passes, verify):*** el cabezal de escritura pasa por cada sector tres veces (0x01, 0x27FFFFFF, Random). Hay un último pase para verificar caracteres aleatorios mediante la lectura
14. ***Navso P-5329-26 (MFM) (3 passes, verify):*** el cabezal de escritura pasa por encima de cada sector tres veces (0x01, 0x7FFFFFFF, Random). Hay un último pase para verificar caracteres aleatorios mediante la lectura.

15. ***NCSC-TG-025 (3 passes, verify):*** El cabezal de escritura pasa por encima de cada sector tres veces (0x00, 0xFF, Random). Hay un último pase para verificar caracteres aleatorios mediante la lectura.
16. ***NSA 130-2 (2 passes, verify):*** El cabezal de escritura pasa por encima de cada sector dos veces (random, random). Hay un último pase para verificar caracteres aleatorios mediante la lectura.
17. ***Bruce Schneier (7 passes, verify):*** El cabezal de escritura pasa por encima de cada sector siete veces (0xFF, 0x00, random, random, random, random, random). Hay un último pase para verificar caracteres aleatorios mediante la lectura.
18. ***DoE M 205.1-2 (U.S. Department of Energy) (3 passes, verify):*** El cabezal de escritura pasa por encima de cada sector tres veces (random, random, random). Hay un último pase para verificar caracteres aleatorios mediante la lectura.

En el estudio realizado, se aplicaron los algoritmos "Canadian RCMP TSSIT OSP-II", "US DoD 5220.22-M", "US DoS 5220.22-M (ECE)" y "Peter Gutman", ya que son los más utilizados y recomendados por los usuarios.

Las herramientas utilizadas poseen en común casi todos estos algoritmos, solo una de ellas no permite la utilización del algoritmo "Canadian RCMP TSSIT OSP-II", pero la misma no se descartará ya que se pueden estudiar los demás algoritmos.

Se descartan los algoritmos "One pass zeros" y "One pass random", a pesar que también los tengan en común todas las herramientas. Esto se justifica a continuación.

Herramientas de higienización de los datos.

Existen diferentes métodos y normas para borrar discos duros, pero dada la gran variedad de métodos de codificación de la información en soportes magnéticos, el único que nos garantiza la privacidad es el de sobre-escribir varias veces el disco duro con datos aleatorios. En un principio parece un método sencillo, pero generar datos realmente aleatorios con un ordenador no es fácil, ya que el ordenador es por naturaleza determinista. Es por esta razón que los algoritmos "One pass zeros" y "One pass random", son descartados en el estudio realizado ya que los mismos equivalen a un formateo.

Al utilizar un mal generador de números aleatorios, se puede adivinar los valores siguientes examinando las secuencias pasadas. Lo que quiere decir que el uso de un mal generador de números aleatorios (PRNG[4]) permitiría la recuperación de todos los datos.

Se debe tener en cuenta que el borrado seguro tarda bastante tiempo, aunque todo dependerá del tamaño del disco duro o los archivos en cuestión. No se producirá de forma instantánea como cuando se borra un archivo de la papelera, sino que el proceso de sobre-escritura tardará su tiempo dependiendo del tamaño del mismo y el algoritmo que se utilice. En el estudio realizado se pudo observar que el tiempo que tarda el algoritmo no dependía de

[4] Algoritmo que produce una sucesión de números que es una muy buena aproximación a un conjunto aleatorio de números. La sucesión no es exactamente aleatoria en el sentido de que queda completamente determinada por un conjunto relativamente pequeño de valores iniciales, llamados el estado del PRNG.

la herramienta utilizada, sino de la velocidad de RAM del ordenador en el que se corre la herramienta y la velocidad del disco duro en cuestión.

Para realizar un borrado seguro se pueden utilizar diferentes herramientas de software. En la presente tesina se presentarán cinco (5) diferentes herramientas encargadas de la higienización de datos, seleccionadas por su popularidad en la Internet. De las mismas se estudiará su funcionamiento y los recursos que ofrecen. Estas son:

Windows

- Eraser [22].
- BCWipe [23].
- Disk Wipe [24].
- KillDisk [25].

Consola:

- Darik's Boot and Nuke (DBAN) [26].

ERASER.

Figura 22. Logo herramienta Eraser.

Eraser [22] es una herramienta gratuita que se puede instalar en sistemas de escritorio (por ejemplo, Windows) como también en servidores. Es una aplicación interesante para utilizar sobre todo con dispositivos extraíbles que circulan dentro de una organización y/o clientes. A la vez también es recomendable su uso en dispositivos portátiles.

Las técnicas que se utilizan consisten en borrar archivos y sobre-escribirlos. Cuantas más veces se repita esta operación más seguro será el borrado, por lo que podemos hacerlo en este caso hasta 35 veces mediante el algoritmo Gutman.

Eraser [22] está programado para iniciar junto con el sistema, por lo tanto los archivos se pueden eliminar de diferentes maneras. Cuando se crea la tarea de eliminación se debe especificar el tipo de tarea, los cuales son:

1. **Ejecutar manualmente:** una vez creada la tarea de borrado, se deberá comenzar la tarea manualmente desde el programa.
2. **Ejecutar inmediatamente:** una vez creada la tarea de borrado, comienza a ejecutarse inmediatamente.
3. **Ejecutar al reiniciar:** una vez creada la tarea de borrado, comenzará a ejecutarse en el próximo reinicio del equipo.
4. **Periódico:** una vez creada la tarea de borrado, la misma se ejecutará periódicamente.

Los primeros dos casos son recomendables para unidades externas como discos duros o memorias USB; el tercer caso es quizás mejor para los archivos que tengamos en los discos duros de nuestros ordenadores; y el cuarto caso es recomendable hacerlo con archivos que se deben eliminar todos los días, como es el caso de la papelera de reciclaje.

También dispone de un menú contextual, como se ilustra en la ***figura 23***, por lo tanto cuando queramos enviar un archivo a Eraser [22] para su borrado seguro sólo tenemos que utilízalo con el botón derecho para que aparezcan las opciones de eliminación del archivo. Se pueden eliminar directamente o programar su borrado para el próximo reinicio del equipo.

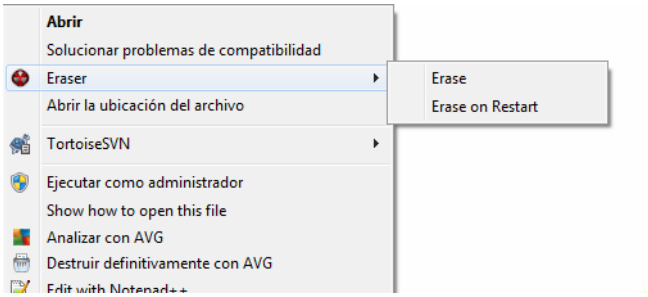


Figura 23. Imagen menú contextual Erase.

Cuando se crea una tarea se puede seleccionar el algoritmo que se desea utilizar, el cual se debe especificar en la sección de ajustes, esta configuración se detallará más adelante. En el caso del menú contextual se usa el algoritmo por defecto

Eraser [22] cuenta con trece (13) algoritmos de higienización, los cueles son:

1. Peter Gutmann (35 passes, verify)
2. US DoS 5220.22-m (ECE) (7 passes, verify)
3. Canadian RCPMP TSSIT OSP-II (7 passes, verify)
4. Bruce Schneier (7 passes, verify)
5. Greman VSITR (7 passes, verify)
6. US DoD 5220.22-M (3 passes, verify)
7. HMG IS5 Enhanced (3 passes, verify)
8. US Air Forece 5020 (3 passes, verify)
9. US Army AR380-19 (3 passes, verify)
10. Russian GOST p50739-95 (2 passes, verify)
11. HMG IS5 Baselune (1 pass, verify)
12. Pseudorandom: One pass random (1 pass)
13. First/last 16KB Erasure: One pass zeros (1 pass)

BCWipe.

Figura 24. Logo herramienta BCWipe.

BCWipe [23] es una herramienta comercial para el Sistema Operativo Windows. Permite el borrado seguro de ficheros utilizando métodos reconocidos para eliminar cualquier carpeta o archivo del disco duro. Es capaz de destruir tanto archivos individuales como carpetas, así como además liberar espacio del disco y el archivo Swap.

El administrador de tareas de BCWipe [23] te permite crear o planificar cualquier acción que necesites, incluso dejar programado un plan de borrado. También incluye soporte para carpetas del sistema como la caché del navegador, las cookies, los documentos recientes o las listas MRU (objetos más recientemente usados).

Los tipos de tareas que se pueden programar son:

- ✓ **Borrar y limpiar:** se realiza el borrado para ficheros o carpetas existente o una ruta dentro del sistema de archivos.
- ✓ **Limpiar espacio libre:** se realiza el borrado para el espacio libre de los discos seleccionados. Si el disco se encuentra sin información el mismo será borrado por completo.
- ✓ **Limpiar historial de Internet:** limpieza de cookies, favoritos, historial, caché, entre otros.
- ✓ **Limpiar historial local:** limpieza de archivos temporales, papelera de reciclaje, entre otros.
- ✓ **Limpieza en segundo plano**: te permite realizar la limpieza y a la vez seguir utilizando el ordenador para otras tareas.
- ✓ **Cifrado de archivo de Swap:** CryptoSwap es una eficaz utilidad que te permite encriptar el archivo Swap de Windows, utilizando para ello un algoritmo de encriptación de máxima potencia.

Las tareas se pueden planificar, indicando la frecuencia de la tarea y el horario de inicio. Dependiendo de la frecuencia con la que la tarea está planificada se deben configurar diferentes ajustes:

- ✓ **Una vez:** se debe configurar el horario del inicio de la tarea y el día a ejecutarse.
- ✓ **Diaria:** se debe configurar el horario del inicio de la tarea y cada cuanto día(s) se ejecutará.
- ✓ **Semanal:** se debe configurar el horario del inicio de la tarea, cada cuanta(s) semana(s) se ejecutará y se seleccionarán los días de la semana a ejecutarse.

- ✓ **Mensual:** se debe configurar el horario del inicio de la tarea, cada cuanto(s) día(s) o los días específicos de la semana, y que mes (meses) se ejecutará.
- ✓ **Al conectar el usuario (encendido); Al inicio; Al desconectar el usuario (apagado):** las opciones son,
  - Siempre.
  - Una vez al día.
  - Una vez a la semana.
  - Una vez al mes.

Dentro de las opciones de la limpieza se encuentra la selección del algoritmo a utilizar. BCWipe [23] cuenta con catorce (14) algoritmos de higienización, los cuales son:

1. US DoS 5220.22-m (ECE) (7 passes, verify)
2. US DoD 5220.22-M (3 passes, verify)
3. Greman VSITR (7 passes, verify)
4. DoE M 205.1-2 (U.S. Department of Energy)
5. Peter Gutmann (35 passes, verify)
6. Bruce Schneier (7 passes, verify)
7. Russian GOST p50739-95 (2 passes, verify)
8. HMG IS5 Baseline (1 pass, verify)
9. HMG IS5 Enhanced (3 passes, verify)
10. Navso P-5329-26 (MFM) (3 passes, verify)
11. Navso P-5329-26 (RL) (3 passes, verify)
12. Canadian OSP-II (7 passes, verify)
13. US Army AR380-19 (3 passes, verify)
14. One pass random (1 pass)

BCWipe [23] también da la opción de utilizar el fichero log, el cual guarda la información de la higienización. Para que el fichero se guarde, se debe crear un archivo ".log" o ".txt" donde se guardará la información, también de debe especificar la ruta donde se encuentra este fichero, además se puede decidir si se elimina el contenido anterior y solo queda el nuevo o se añade al contenido anterior, como también el tamaño máximo a añadir.

Los datos guardados en el log, como se muestra en la ***figura 25***, son:

- ✓ **Time:** fecha y hora del borrado.
- ✓ **Reporter:** código del proceso.
- ✓ **Status:** resultado de la tarea.
- ✓ **Action:** tipo de tarea seleccionada.
- ✓ **Scheme:** algoritmo seleccionado.
- ✓ **Path:** nombre completo del archivo o directorio.
- ✓ **Version:** versión del software.
- ✓ **Comment:** comentarios (formato de archivo, tamaño total, espacio libre, tamaño cluster).

```
Time: 2014/6/1 20:24:36:688     Reporter: 0470:0474     Status: Task is assigned
Action: Limpiar espacio libre (1)
Command line: "C:\Program Files (x86)\Jetico\BCWipe\BCWipeTM.exe" TaskProcessing
Module: 'BCWipeTM.exe' v.3.04.2 OS: pl 2, mj 6, mn 1, bn 1db1
Time: 20:24:42:415      Reporter: 0470:0474     Status: Task is queued
Action: Limpiar espacio libre (1)
Time: 20:24:42:471      Reporter: 0470:1C30     Status: START
Action: Limpiar espacio libre (1)
Time: 20:24:42:503      Reporter: 0470:1C30     Action: 'Limpiar espacio libre (1)'
Status: Started Scheme: 'One random pass', passes 1,
verification Off, type 19480117 Version: 3.04.2
Time: 2014/6/1 20:24:43:854     Reporter: 0BC8:1F0C     Action: Wipe Drive
Path: I:\       Status: Started Scheme: 'One random pass', passes 1,
verification Off, type 19480137 Comment: FAT, total size 3,6 GB, free space 3,6 GB,
cluster size 4 KB       Version: 6.05,OS pl 2, mj 6, mn 1, bn 1db1.
Command line: "C:\Program Files (x86)\Jetico\BCWipe\BCWipe.exe" FreeSpace -OF
"C:\Windows\TEMP\BCO52E15370.tmp" "@*C:\Windows\TEMP\BC52E152E0.tmp"
Module: 'BCWipe.exe' v.3.10.3   Instance: 'BCWipe.dll' v.6.05   OS: pl 2, mj 6, mn 1, bn 1db1
Time: 20:24:43:891      Reporter: 0BC8:1F0C     Action: Wipe Directory Entries
Path: I:\       Status: Started
Time: 20:24:43:892      Reporter: 0BC8:1F0C     Path: 'I:\'
Type: FAT32, rootDirStartCluster 2
Time: 20:24:47:239      Reporter: 0BC8:1F0C
Action: Wipe directory entries  Status: passed 123/0    Result: Success Path: I:\
Time: 20:24:47:239      Reporter: 0BC8:1F0C
Action: Wipe Directory Entries  Path: I:\       Status: Success
Time: 20:24:47:240      Reporter: 0BC8:1F0C
Action: Wipe free space Path: I:\       Status: Started
```

Figura 25. Ejemplo de un fragmento del log creado por el programa BCWipe al borrar un pendrive Kingston de 4GB.

Disk Wipe.

Figura 26. Logo herramienta Disk Wipe.

Disk Wipe [24] es una herramienta gratuita para el Sistema Operativo Windows, es un software portable que no requiere instalación. Ayuda a los usuarios asegurar la eliminación permanente de los datos de sus discos duros u otros dispositivos de almacenamiento de memoria, como memorias USB, tarjetas de memoria SD o cualquier otro dispositivo que la memoria puede servir como un dispositivo de almacenamiento. Mientras el dispositivo de memoria posea formato NTFS, FAT o FAT32 se puede limpiar del disco toda la información, sin hacerle un daño físico.

Disk Wipe limpia los diferentes dispositivos de almacenamiento con una variedad de algoritmos predefinidos, básicamente escribe sobre los datos ya existentes en el dispositivo con nuevos datos sin sentido, al azar, y lo hace varias veces.

La pantalla principal de Disk Wipe [24] lista lo dispositivos de almacenamiento que están conectados al ordenador, ya sea en las unidades de disco internas o dispositivos de memoria externos. Al hacer clic en un dispositivo de disco muestra información detallada sobre el mismo, como se muestra en la ***figura 27***.

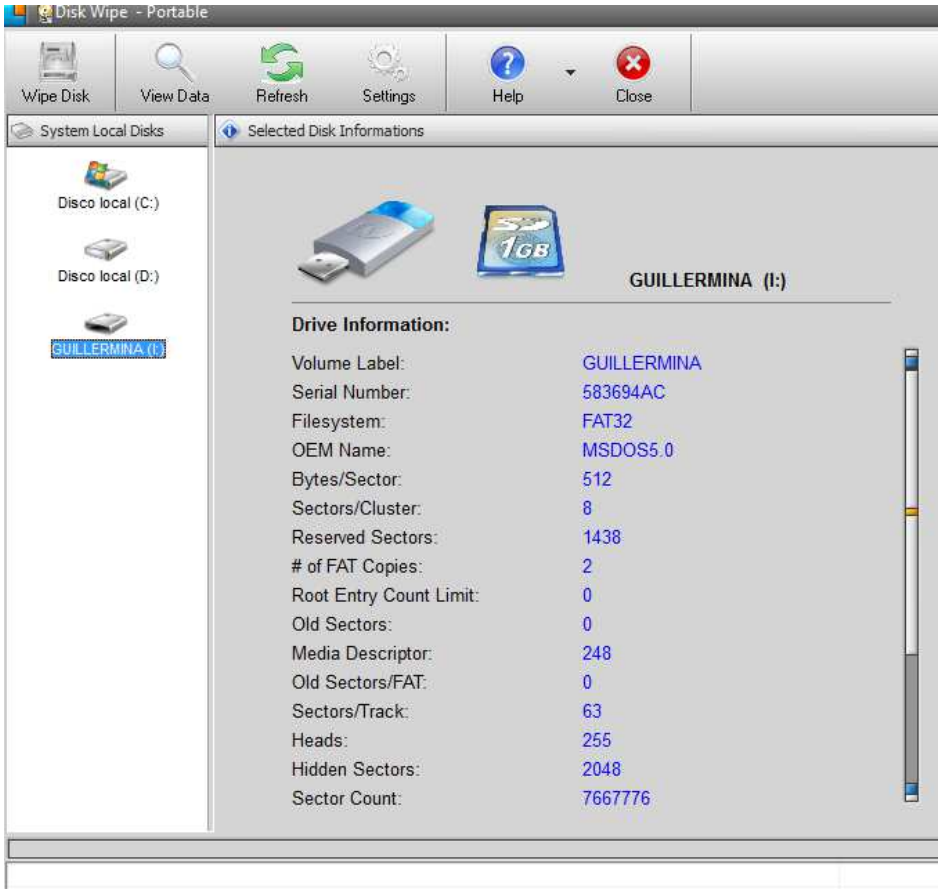


Figura 27. Imagen ejemplo funcionamiento programa Disk Wipe.

La información listada es la siguiente:

- ✓ **Tipo de disco:** disco local, tarjeta SD, memorias USB, etc.
- ✓ **Información del disco:**
  - Etiqueta del volumen.
  - Número del serial.
  - Sistema de Archivos.
  - Nombre OEM.
  - Bytes/Sector.
  - Sectores/Clusters.
  - Sectores reservados.
  - Descriptores de medios.
  - Sectores/Track.
  - Cabezales.
  - Sectores ocultos.
  - Recuento total de sectores.
  - Número serial del disco.
  - Bloque de arranque.
- ✓ **Información de la tabla maestra:**
  - Comienzo cluster.
  - Espejo de partida de cluster.

- Tamaño de archivo de registro (cluesters).
- Clusters/Índice del bloque.

Al hacer clic sobre el icono de "Data View" (vista de los datos) abrirá una nueva ventana que muestra el contenido del disco, los datos binarios sin formato. Los usuarios avanzados con conocimientos pueden encontrar esta opción útil.

El panel de configuración “Settings” (ajustes) le permite omitir opcionalmente la confirmación de los pasos antes de la limpieza del dispositivo, los cuales son:

- ✓ Sistema de archivos.
- ✓ Algoritmo de borrado.
- ✓ Confirmación.

También se puede colocar un nuevo nombre al disco, en el campo "Etiqueta de volumen". El nombre por defecto es "Disco Blanco".

Otra configuración que se puede realizar es el ajuste de la prioridad de la tarea, que fijará el nivel de energía del procesador. Si se establece en "Baja" o "Inferior" significa que otras aplicaciones en ejecución tomarán más o todo el poder del procesador, por lo que la limpieza del disco será más lenta si se tiene otras aplicaciones activas haciendo algún otro trabajo. Sin embargo, el establecimiento de Disk Wipe [24] al "Superior" o "Alto" podría fácilmente hacer que todo el sistema este lento, ya la potencia del procesador se da principalmente a Disk Wipe [24], por lo que sería prudente dejarlo en default (“Normal”).

Al hacer clic sobre el icono “Wipe Disk” (limpia el disco) se abrirá una nueva ventana en la cual se configurarán los pasos no omitidos antes de la limpieza.

Paso 1: se deberá seleccionar un sistema de archivos (NTFS, FAT o FAT32).

Paso 2: se deberá seleccionar el algoritmo a utilizar para el borrado.

Paso 3: se debe confirmar el comienzo del borrado ingresando “ERASE ALL”.

Disk Wipe [24] cuenta con siete (7) algoritmos de higienización, los cuales son:

1. One pass zeros (1 pass)
2. One pass random (1 pass)
3. Russian GOST p50739-95 (2 passes, verify)
4. HMG IS5 Enhanced (3 passes, verify)
5. US DoD 5220.22-M (3 passes, verify)
6. US DoS 5220.22-m (ECE) (7 passes, verify)
7. Peter Gutmann (35 passes, verify)

El borrado del disco consiste en:

1. Se prepara el disco para darle formato, listando el tipo de sistema de archivo a utilizar.
2. Se le da formato, creando la estructura del sistema de archivo.

3. Se indica la finalización del formateo, y se lista el espacio total del disco y el espacio disponible.
4. A continuación comienza la higienización del disco y se lista el algoritmo a utilizar.
5. Una vez finalizado el borrado, se lista el tiempo que llevo el mismo.

KillDisk.

Figura 28. Logo herramienta KillDisk.

KillDisk [25] es una herramienta comercial para el Sistema Operativo Windows. Cumple la función de limpiar los datos confidenciales de espacio no utilizado en el disco duro, borrar los datos de las particiones o desde un disco duro completo, y destruir datos permanentemente. También se pueden borrar memoria SD y unidad USB/disco extraíble.

Si se tiene varios discos duros físicos conectados a la máquina, KillDisk [25] puede borrarlos simultáneamente en el modo multi-threaded (multi-hilos), lo que le ahorra tiempo y costos.

Una vez finalizado el proceso de borrado o limpieza, KillDisk [25] ofrece las opciones de inicialización de discos borrados, apagar el ordenador, guardar un archivo de registro y el certificado (en los formatos txt o PDF para ser impreso), e incluso el envío de archivos de registro por e-mail a la casilla especificada. Los certificados se pueden crear, utilizando el logotipo y los atributos de cualquier empresa. Todas estas opciones se deben configurar en "Settings" (ajustes), en la parte superior derecha del programa, o en el proceso de borrado.

Independientemente del Sistema Operativo, los sistemas de archivos o el tipo de máquina, KillDisk [25] pueden destruir todos los datos de todos los dispositivos de almacenamiento.

KillDisk [25] cuenta con diecisiete (17) algoritmos de higienización, los cuales son:

1. One pass zeros (1 pass)
2. One pass random (1 pass)
3. US DoD 5220.22-M (3 passes, verify)
4. US Army AR380-19 (3 passes, verify)
5. Canadian OSP-II (7 passes, verify)
6. Greman VSITR (7 passes, verify)
7. Russian GOST p50739-95 (2 passes, verify)
8. Peter Gutmann (35 passes, verify)
9. US DoS 5220.22-m (ECE) (7 passes, verify)
10. US Air Forece 5020 (3 passes, verify)

11. HMG IS5 Baselune (1 pass, verify)
12. HMG IS5 Enhanced (3 passes, verify)
13. Navso P-5329-26 (RL) (3 passes, verify)
14. Navso P-5329-26 (MFM) (3 passes, verify)
15. NCSC-TG-025 (3 passes, verify)
16. NSA 130-2 (2 passes, verify)
17. Bruce Schneier (7 passes, verify)

Cuando se inicia KillDisk [25] todos los dispositivos físicos y particiones lógicas se muestran en una lista. Los dispositivos de disco duro se listan según el orden que se encuentra en la BIOS del sistema. Al seleccionar un dispositivo se puede leer la información detallada sobre el mismo en el panel derecho; además se puede seleccionar una partición lógica, su información también se listará en el panel.

KillDisk [25] ofrece una vista previa de los sectores del disco físico o lógico como también de los archivos del disco. Haciendo clic en "Hex Preview" (Vista previa) en la barra de herramientas, se obtendrá la vista previa de los sectores del disco. Para obtener una vista previa de los archivos del disco, se debe seleccionar el volumen y pulsar ENTER o hacer doble clic en él. KillDisk [25] escaneará los directorios de la partición. Los archivos y carpetas existentes están marcados con iconos amarillos y los archivos y carpetas eliminados están marcados con iconos grises. Si sólo se está limpiando los datos de las zonas no ocupadas, se eliminan los nombres de archivo de color gris después de completar el proceso de limpieza.

Una vez seleccionado el/los dispositivo/s a borrar, se debe presionar el botón "Kill" (matar) el cual abrirá una nueva ventana donde se seleccionara el algoritmo de higienización a utilizar. En la misma también se podrá establecer la configuración de "Settings" (ajustes) haciendo clic en el enlace de "more options" (más opciones) en la parte inferior. Una vez configurado el programa, se hace clic sobre el botón "Start" (comenzar) para iniciar con el borrado.

Si se produce algún error, por ejemplo debido a sectores dañados, se informará en la pantalla interactiva y en el registro. Si aparece este mensaje, se puede cancelar la operación (clic Abortar), o puede continuar borrando datos (haga clic en Ignorar o Ignorar todo).

Los datos guardados en el registro, también llamado log, como se muestra en la ***figura 29***, son:

- ✓ La información del disco borrado
  - Número de serial.
  - Tamaño del disco.
- ✓ La fecha y hora del inicio del borrado.
- ✓ El algoritmo seleccionado.
- ✓ El estado de cada pasada del algoritmo.
- ✓ Estado de la verificación del disco (si se encuentra dañado o no).
- ✓ La fecha y hora del fin del borrado.
- ✓ Tiempo total que llevo realizar el borrado.

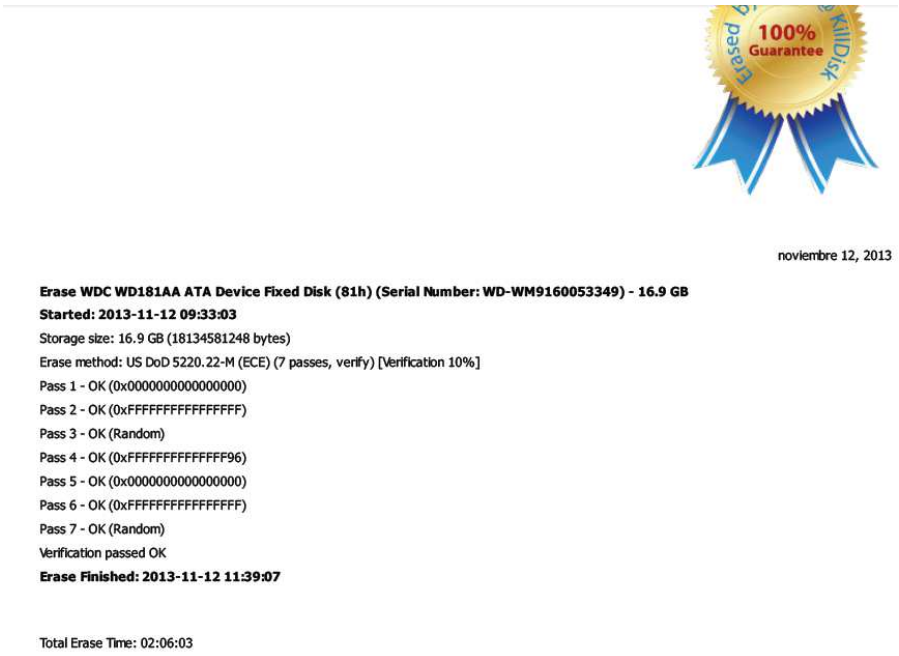


Figura 29. Ejemplo de log creado por el programa KillDisk.

Darik's Boot and Nuke (DBAN).

Figura 30. Logo herramienta DBAN.

DBAN [26] es una herramienta gratuita que no necesita de un Sistema Operativo ya que se utiliza un disquete, un CD/DVD o un memoria USB booteable. Es un disco de arranque independiente que elimina automáticamente el contenido de cualquier disco duro que puede detectar. Este método puede ayudar a prevenir el robo de información antes de reciclar un ordenador.

DBAN [26] evita todas las técnicas conocidas de análisis forense del disco duro. Además 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 diquete, DVD/CD o memoria USB, iniciara el programa comenzando con cinco (5) opciones:

1. Presionar la tecla F2 para aprender sobre DBAN [26].
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 [26] en el modo interactivo.

5. Introducir “autonuke” en la línea de comandos para iniciar DBAN [26] 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. Los comandos a utilizar para la selección y configuración de los discos para la correcta higienización son:

- ✓ 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 [26] 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 [26] el algoritmo a utilizar es el DoD Short.

Una vez completado el proceso de higienización, DBAN [26] ofrece guardar un log con la información del mismo. El log contiene toda la información del proceso. Se guarda una carpeta bajo el nombre “dbanXXX”, donde XXX es el número asignado, ejemplo “001”. La estructura de la carpeta está compuesta por:

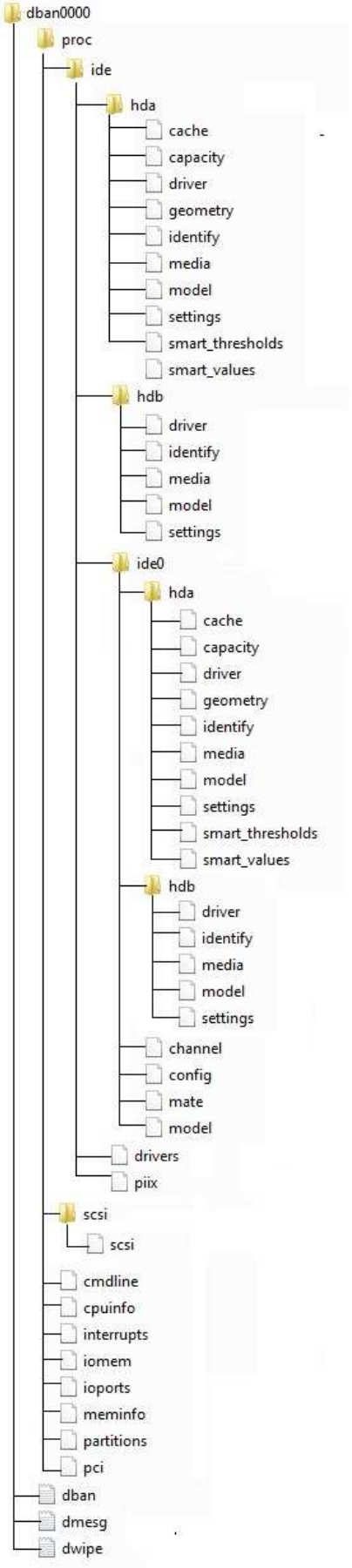


Figura 31. Contenido del log de DBAN.

El contenido más importante correspondiente al log de DBAN [26], mostrados en la ***figura 31***, son:

El archivo “dban.txt” contiene:

[Fecha Hora] dban: Version comienzo.

[Fecha Hora] dban: Found floppy drive /dev/floppy/0.

[Fecha Hora] dban: Found 0 seed files on the floppy disk.

[Fecha Hora] dban: Wipe started.

[Fecha Hora] dban: DBAN succeeded. All selected disks have been wiped.

El archivo “dmesg.txt” contiene la información del hardware de la máquina en la que está corriendo (RAM, CPU, etc.).

El archivo “dwipe.txt” contiene las especificaciones del algoritmo utilizado, la hora y fecha que comenzó a ejecutarse, como también la hora y fecha del fin de su ejecución.

La información propia del disco correspondiente se encuentra en la ruta dban000/proc/ide/hda, dándole importancia al archivo “model” ya que con el mismo se puede comprobar el modelo y número de serie del disco.

Criterios de comparación.

Las herramientas de higienización de datos deben cumplir ciertos requisitos para lograr los resultados esperados en la presente tesina.

Principalmente la herramienta debe certificar la máxima destrucción de la información sin posibilidad de recuperación de datos sensibles del usuario. Los algoritmos de borrado seguro no siempre son 100% efectivos, y nunca se puede afirmar esto, ya sea por una falla del software o hardware. Por lo tanto lo que se busca de la herramienta es que su destrucción se aproxime al 100%.

La combinación de las cualidades de eficiencia y rapidez deben estar presentes. Una herramienta efectiva pero con una alta tasa de tiempo de ejecución no siempre es una buena opción ya que la probabilidad de que se produzcan fallos de software es alta. Siempre se deben evaluar los costos y el tiempo. Como tampoco es una opción la selección de una herramienta que no sea efectiva.

La complejidad del uso de la herramienta no se debe tomar en cuenta a la hora de su selección. Si la complejidad de una herramienta es alta pero posee una tasa de destrucción elevada y a la vez combina las cualidades de eficiencia y rapidez, debe ser seleccionada y no descartada por su complejidad. A su vez, la herramienta debe ser configurable al gusto del usuario y, a pesar de que realice gran parte del proceso automáticamente, el usuario debe confirmar cada paso del mismo.

La certificación del borrado siempre es una buena opción, aunque no indispensable. En los mismos se especifica todo el proceso de higienización, como por ejemplo, el algoritmo

utilizado, la fecha y hora que se realiza el borrado, el tiempo total de ejecución, si finalizo o no con éxito el proceso (fallos), entre otros datos.

Para una certificación formal del proceso se debe contar tanto con una documentación otorgada por el software como también una escrita y firmada por un escribano que presencie el inicio y/o fin del proceso y sus resultados.

Cuando se trabaja con una gran cantidad de discos se debe tener en cuenta la ejecución en paralelo o la programación de varios borrados secuenciales. Es decir, la herramienta debe poder ejecutar el borrado de varios discos a la vez o debe permitir la destrucción de varios discos secuencialmente. Esto tiene como ventaja la reducción del espacio físico a utilizar para la ejecución de la higienización y la intervención humana a la hora de la destrucción, como por ejemplo cambio de discos, falta de personal al momento de la finalización de la destrucción, etc. Estas opciones no dan como ventaja la reducción del tiempo de ejecución de los algoritmos pero tampoco los aumenta.

La licencia de la herramienta como también en el Sistema Operativo en el que corre son criterios a evaluar.

Dependiendo el tipo de la licencia de software se pueden clasifican según:

1. Según los derechos que cada autor se reserva sobre su obra:
    - **Licencia de software de código abierto permisivas**: Se puede crear una obra derivada sin que ésta tenga obligación de protección alguna.
    - **Licencia de software de código abierto robustas**: Estas licencias aplican algunas restricciones a las obras derivadas, haciendo que según el grado de aplicación se puedan dividir a su vez en dos subcategorías:
        - **Fuertes**: Las licencias de software de código abierto robustas fuertes o con copyleft fuerte, contienen una cláusula que obliga a que las obras derivadas o modificaciones que se realicen al software original se deban licenciar bajo los mismos términos y condiciones de la licencia original. Este es el caso de la licencia GNU (General Public License) [27].
        - **Débiles**: Las licencias de software de código abierto robustas débiles, con copyleft débil/suave o híbridas, contienen una cláusula que obliga a que las modificaciones que se realicen al software original se deban licenciar bajo los mismos términos y condiciones de la licencia original, pero que las obras derivadas que se puedan realizar de él puedan ser licenciadas bajo otros términos y condiciones distintas.
    - **Licencia de software de código cerrado:** Estas licencias también se conocen con el nombre de software propietario o privativo. En ellas los propietarios establecen los derechos de uso, distribución, redistribución, copia, modificación, cesión y en general cualquier otra consideración que se estime necesaria.

Este tipo de licencias, por lo general, no permiten que el software sea modificado, desensamblado, copiado o distribuido de formas no especificadas en la propia licencia (piratería de software), regula el número de copias que pueden ser instaladas e incluso los fines concretos para los cuales puede ser utilizado. La mayoría de estas licencias limitan fuertemente la responsabilidad derivada de fallos en el programa.

- **Software de dominio público (sin licencia):** Se permite uso, copia, modificación o redistribución con o sin fines de lucro.

2. Según su destinatario:
   - **Licencia de Usuario Final (EULA o End User License Agreement)**: Es una licencia por la cual el uso de un producto sólo está permitido para un único usuario (el comprador). Este tipo de acuerdo expresa los usos qué se pueden dar y cuáles no al producto, ya que quien lo compra no es, legalmente, en ninguna forma dueño del producto, sino sólo de una licencia para su uso, considerándose esto último por algunas personas como una limitación a los derechos del consumidor. Este tipo de acuerdos son unilaterales pues el usuario no tiene más opción que aceptar o rechazar el contenido del mismo.
   - **Licencia de distribuidores:** En este tipo de contrato, se le asigna derechos restringidos a un comerciante de tipo comisionario para que venda el producto (software) dando una comisión al fabricante.

Por lo tanto, al seleccionar una herramienta de higienización de la información se debe tener en cuenta:

1. Nivel de destrucción.
2. Tiempo de ejecución vs Costos.
3. Capacidad de ejecución en paralelo o secuencial.
4. Opciones de certificación del proceso, certificación otorgada por la herramienta y/o certificación a través de un escribano.

Tabla de criterios de comparación de las herramientas.

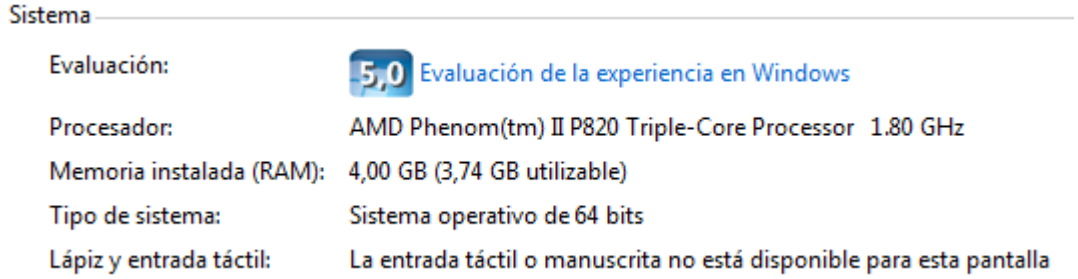
Criterios de comparación	Eraser	BCWipe	Disk Wipe	KillDisk	DBAN
Sistema Operativo	Windows XP (with Service Pack 3)/Server 2003 (with Service Pack 2)/Vista/Server 2008/Server 2008 R2/7.	Windows.	Windows con sistema de archivos NTFS, Fat, Fat32.	Windows XP/Vista/7/8 (x86/x64) Windows 2003 / 2008 Server. Linux.	Consola.

Licencia	Software gratuito. Su código fuente se distribuye bajo la licencia: *GNU General Public License*.	Software comercial. Se distribuye a través de la licencia EULA	Software gratuito para uso personal o comercial, sin ninguna restricción. Se distribuye a través de la licencia EULA	Posee dos versiones Gratuita y Comercial. Se distribuye a través de la licencia EULA	Software gratuito. Su código fuente se distribuye bajo la licencia: *GNU General Public License*.
Capacidad de ejecución en paralelo	✘	✔	✘	✘	✘
Capacidad de ejecución secuencial	✔	✔	✔	✔	✔
Certificación del proceso.	No genera ningún log de certificación. Solo confirma la correcta o no finalización de la tarea en la columna "status" (estado).	Genera un fichero .log con los detalles del proceso.	No genera ningún log de confirmación. Solo confirma la correcta o no finalización de la tarea, listando los pasos realizados.	Genera un log, dependiendo de la configuración puede ser un archivo .txt o .pdf, con los detalles del proceso.	Genera una carpeta DBAN que contiene los logs correspondientes al borrado.
Cantidad de algoritmos de higienización	13	14	7	17	6

Estudio comparativo de tiempos.

A continuación se comparan las herramientas y algoritmos en base al tiempo de ejecución del borrado completo del dispositivo. Se borró, con las diferentes herramientas, un mismo dispositivo sobre un mismo ordenador para comparar la eficiencia de los mismos en tiempos transcurridos para finalizar las tareas.

La máquina donde se realizó el borrado es una Notebook HP Pavilion dv6-3077la, con las siguientes especificaciones:



El dispositivo higienizar es un pendrive de marca Kingston de 4GB, como se muestra en la ***figura 32***.

Figura 32. Pendrive Kingston.

Eraser.

	Canadian RCMP TSSIT OSP-II	US DoD 5220.22-M	US DoS 5220.22-M (ECE)	Peter Gutman
Comienzo	18:05 pm	3:08 am	3:58 am	19:42 pm
Fin	19:42 pm	3:56 am	5:41 am	3:06 am
Tiempo transcurrido	1 hora 37 minutos.	48 minutos	1 hora 43 minutos	8 horas 24 minutos

Eraser [22] no comunica el horario de inicio y fin del borrado, y tampoco el tiempo total que llevo ejecutar la tarea.

BCWipe.

	Canadian RCMP TSSIT OSP-II	US DoD 5220.22-M	US DoS 5220.22-M (ECE)	Peter Gutman
Comienzo	1:23 am	15:34 pm	16:11 pm	18:16 pm
Fin	2:46 am	16:10 pm	17:33 pm	1:04 am
Tiempo transcurrido	1 hora 23 minutos	36 minutos	1 hora 22 minutos	7 horas 48 minutos

BCWipe [23] comunica el horario de inicio y fin del borrado, pero no el tiempo total que llevo ejecutar la tarea.

Disk Wipe.

	Canadian RCMP TSSIT OSP-II	US DoD 5220.22-M	US DoS 5220.22-M (ECE)	Peter Gutman
Comienzo	-	15:40 pm	14:31 pm	16:54 pm
Fin	-	16:41 pm	15: 27 pm	18:00 pm
Tiempo transcurrido	-	1 hora 1 minutos	56 minutos	1 hora 6 minutos

Disk Wipe [24] informa el tiempo que llevo ejecutar la tarea pero no especifica el horario de inicio y fin del borrado.

KillDisk.

	Canadian RCMP TSSIT OSP-II	US DoD 5220.22-M	US DoS 5220.22-M (ECE)	Peter Gutman
Comienzo	2:54 am	4:15 am	4:51 am	6:22 am
Fin	4:14 am	4:49 am	6:11 am	13:03 pm
Tiempo transcurrido	1 hora 20 minutos	34 minutos	1 hora 20 minutos	6 horas 40 minutos

KillDisk [25] comunica el horario de inicio y fin del borrado, como también el tiempo total que llevo ejecutar la tarea.

DBAN.

	Canadian RCMP TSSIT OSP-II	US DoD 5220.22-M	US DoS 5220.22-M (ECE)	Peter Gutman
Comienzo	21:42 pm	19:17 pm	16:08 pm	3:22 am
Fin	00:36 am	20:29 pm	18:53 pm	16:04 pm
Tiempo transcurrido	2 horas 54 minutos	1 horas 22 minutos	2 horas 45 minutos	12 horas 42 minutos

DBAN [26] comunica el horario de inicio y fin del borrado, pero no el tiempo total que llevo ejecutar la tarea.

Tabla comparativa de tiempos.

A continuación de resumirá, en la siguiente tabla, las comparaciones finales del tiempo necesario para la ejecución de los diferentes algoritmos en las diferentes herramientas.

Algoritmo	Canadian RCMP TSSIT OSP-II	US DoD 5220.22-M	US DoS 5220.22-M (ECE)	Peter Gutman
Pasadas	**7**	**3**	**7**	**34**
Eraser	1 hora 37 minutos.	48 minutos	1 hora 43 minutos	8 horas 24 minutos
BCWipe	1 hora 23 minutos	36 minutos	1 hora 22 minutos	7 horas 48 minutos
Disk Wipe	-	1 hora 1 minutos	56 minutos	1 hora 6 minutos
KillDisk	1 hora 20 minutos	34 minutos	1 hora 22 minutos	6 horas 40 minutos
DBAN	2 horas 54 minutos	1 horas 22 minutos		12 horas 42 minutos

Discos fallados ¿Cómo proceder?

Ante la presencia de discos duros que poseen sectores dañados y, por lo tanto, los diferentes software de higienización de datos no son capaces de realizar un procedimiento de sobre-escritura correcto, se proceder a realizar una destrucción física del dispositivo y luego son llevados a empresas de reciclaje. Con el fin de evitar el acceso a la información.

Los diferentes componentes de los AEE son materiales potencialmente reciclables, en general se pueden reciclan en un 80%, por ejemplo un televisor viejo se recicla en un 50%. En el caso particular de los ordenadores, los mismos son 95% reciclables, no se desperdician en nada. Pero no siempre lo más importante es el porcentaje del reciclaje, se debe destacar que los productos reciclados contienen materiales muy tóxicos, como el plomo, y al ser reciclados estos se neutralizan ya que son estos materiales los que producen el daño, por lo tanto su correcta manipulación es fundamental. Cuando se recicla un ordenador se neutralizan muchos materiales tóxicos ya que la misma está compuesta de un 2% de Zinc, un 6% de plomo, un 7% de cobre, un 14% de aluminio, un 21% de hierro, un 24% de plástico y un 26% de sílice. [28]

Con el fin de recuperar estos materiales, es indispensable el tratamiento de los RAEE y a su vez, es necesario que este tratamiento sea específico y cuidadoso, para evitar que se contaminen los materiales reciclables con aquellos que no lo son.

Dentro de los materiales que pueden ser reciclados se encuentran los metales como cobre, hierro y plásticos. Y dentro de los materiales contaminantes se pueden distinguir el plomo, mercurio, compuestos bromados (BFR), entre otros. El cristal de los monitores y televisores contiene el 20% en peso de plomo, los compuestos bromados se encuentran en carcasas de plástico, el plomo de los circuitos electrónicos, entre otros.

Los tipos de residuos reciclables generados por los ordenadores se pueden clasificar en:

- **Placas de circuitos:** aquellas tarjetas de circuitos que no pueden ser reusadas, son molidas y separadas la fibra de vidrio, el metal, y los metales preciosos. Las placas de circuitos pueden contener metales pesados como antimonio, plata, cromo, cobre, lata y plomo.
- **Carcasas de plástico:** actualmente estos plásticos tiene difícil mercado ya que contiene resinas mixtas que no pueden ser identificadas o separadas, así como algunos aditivos como BFR que hacen del reciclado un proceso más engorroso. Muchos de estos plásticos son usados como relleno de cama de pavimento. Sin embargo se está tratando de buscar una aplicación de mayor valor para estos plásticos en productos como pisos, computación y partes de automóviles.
- **Componentes de plástico pequeñas:** por lo general están hechas de polietileno de alta densidad (PEAD). Esto los hace fácil de remover, moler y procesar.
- **Tornillos, clips, partes de pequeños metales:** se separan magnéticamente entre aquellos ferrosos y no-ferrosos.

- **<u>Monitores:</u>** el tubo de rayo catódico (TRC) es un tubo de vidrio con plomo, con un marco de metal en su interior. En primer lugar se le deberá eliminar el revestimiento fluorescente. El tubo es luego destruido y el vidrio de plomo y el metal es separado. Los contaminantes del vidrio son retirados y gran parte del vidrio puede ser vendido a fabricantes de TRC. El metal es vendido. [29]

Más del 90% de los materiales de los RAEE pueden ser recuperados y reciclados, como se cito anteriormente en el caso de los ordenadores se puede reciclar en un 95%, desde el disco duro y la memoria hasta la tarjeta madre y los circuitos impresos de los cuales se puede recuperar oro y plata (excluyendo los monitores) [29]. Por cada tonelada de equipo se pueden extraer 100 gr de oro [35].

En el específico caso de los discos duros, las diferentes empresas con certificación ambiental reciben aquellos que no funcionan o son obsoletos, para obtener placas de circuitos como también tornillos, clips o partes de pequeños metales. Lo extraído principalmente de los discos duros son las denominadas "placas electrónicas" que se encuentran en la parte posterior de los discos, como se muestra en la ***figura 33***.

Figura 33. Discos Duros utilizados en el estudio.

Otro de los componentes de interés para su recuperación son los imanes, que se encuentran en el interior de la estructura del disco duro, como se muestra en la ***figura 34***.

Figura 34. Imanes pertenecientes al Disco Duro.

Jorge Daniel Santkovsky, director de la empresa Scrap y Rezagos SRL [15], informa, en una entrevista que le realice, que la empresa solo reciben los discos duros que no han pasado por métodos de destrucción física que destruyan los componentes deseados, como por ejemplo el método de trituración, pero si son aceptados los discos que no han sido destruidos físicamente aunque pasado por métodos de destrucción física como es el caso de la desmagnetización.

Al recibir disco duros, dependiendo el estado del mismo, es como se debe proceder, por ejemplo:

- Si el disco no es obsoleto y funciona se reutiliza directamente y se vende.
- Si el disco no es obsoleto y no funciona pero es reparable, se repara y se vende.
- Si el disco no es obsoleto, no funciona y no se puede reparar, se recicla.
- Si el disco es obsoleto, funcione o no, se recicla.

Por lo tanto, si un disco duro no permite la correcta destrucción de los datos el mismo debe ser destruido físicamente para conservar la privacidad del usuario. En este caso la mejor destrucción física que se le puede aplicar al mismo es la desmagnetización, ya que destruye la información dejando intacta la estructura del disco duro y así el mismo será aceptado para su correcto reciclaje.

Recuperación de la información.

El objetivo básico de un dispositivo de almacenamiento es guardar información para que la misma esté disponible posteriormente. Para ello todos los componentes físicos del dispositivo tienen que funcionar correctamente y el Sistema Operativo debe encontrar la información que ha sido almacenada de un modo ordenado.

Los Sistemas Operativos almacenan la información dentro del disco duro en archivos. Al guardar cada archivo, se anota también su ubicación en una "lista de archivos". Esta lista es el índice que utiliza el Sistema Operativo para encontrar el contenido de los archivos dentro del disco.

La información almacenada en el soporte se denomina datos, por lo que son equivalentes la pérdida de información y la pérdida de datos.

Hay tres (3) atributos clave que confirman que el modo en que se trata la información es seguro:

- **Confidencialidad:** es la propiedad por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados.
- **Integridad:** es la propiedad de salvaguardar la exactitud y completitud de los activos.
- **Disponibilidad:** es la propiedad de ser accesible y utilizable por una entidad autorizada.

Se dice que se produce una pérdida de información cuando se altera alguno de sus atributos y, específicamente en el proceso del almacenamiento, la disponibilidad es el atributo más crítico. Se dice que la información se pierde cuando no se consigue el acceso a la misma o esta ha desaparecido.

Si se ha perdido el acceso a una información almacenada, dicha pérdida puede no ser definitiva si existen medios para restaurar la disponibilidad de acceso, en cuyo caso se puede plantear la recuperación de la información.

El acceso a la información se puede perder por varios motivos, los cuales podrían ser:

- Porque el dispositivo tiene dañado algún componente físico necesario para su funcionamiento.
- Porque, aún funcionando correctamente, la "lista de archivos" se ha corrompido impidiendo conocer la ubicación de los archivos almacenados.
- Porque los datos almacenados han sido reemplazados por nuevos datos a través de la sobre-escritura.

En los dos primeros casos se puede intentar un proceso de recuperación a través de un software que ofrezca este servicio, en el tercer caso si la sobre-escritura fue realizada por el usuario puede haber posibilidades de la recuperación de los datos, pero en el caso de una sobre-escritura por medio de un algoritmo de higienización eficiente al realizar una

recuperación con un software de recuperación de información, los resultados pueden no ser efectivos ya que estos datos podrían no existir.

El fin de los algoritmos de higienización de datos es la destrucción completa de los datos. En muchos casos los programas de recuperación obtienen datos luego de la ejecución de un algoritmo de borrado seguro, pero estos tienden a no ser legibles o están corrompidos. Cuando se realiza una recuperación de la información sobre dispositivos de almacenamiento, por lo general lo que se recupera sigue un patrón de qué "tipo de datos" puede ser, es decir, codificaciones especificas escritas sobre la superficie del dispositivo; al momento de reconstruir el dato no se cuenta con todo lo necesarios para que el mismo sea legible, como también puede ser el caso de que el patrón seguido no sea el correspondiente a la información recolectada.

Causas de la pérdida de datos.

Las causas por las cuales se producen las pérdidas de acceso a la información son múltiples y en muchos casos imprevisibles. Entre estas, destacan las siguientes:

- **Fallos mecánicos en los dispositivos de almacenamiento:** causados bien por motivos externos (como cortes de suministro eléctrico o picos de tensión en la red eléctrica), o internos de los propios dispositivos (por ejemplo, por degradación de las piezas mecánicas al final de la vida útil de los mismos).
- **Errores humanos**: por borrado o formateo de las unidades de almacenamiento o por manipulación indebida de los dispositivos. A veces la mala preparación del personal y la toma de decisiones erróneas a la hora de intentar recuperar la información tras un incidente son las causas de estos errores.
- **Fallos en el software utilizado**: como fallos imprevistos en los sistemas operativos por reinicios inesperados o mal funcionamiento de las propias herramientas de diagnóstico.
- **Virus o software malicioso:** ya que en ocasiones los programas instalados en los ordenadores buscan causar un fallo en el sistema y/o robar información que envían a un equipo remoto.
- **Desastres naturales o estructurales:** como incendios e inundaciones que causan la destrucción de las instalaciones donde se encuentran los equipos.

Métodos de recuperación de la información.

Por métodos de recuperación de datos se entienden aquellos procesos llevados a cabo con el objetivo de restablecer el acceso a la información que sigue estando almacenada en los dispositivos, pero que no está disponible por alguna de las causas señaladas anteriormente.

Los métodos de recuperación de datos se agrupan principalmente en:

1. Métodos de recuperación lógica: éstos se utilizan cuando todos los componentes del dispositivo funcionan correctamente y por lo tanto se puede acceder a todos y cada uno de los sectores donde se almacena la información. Si se ha perdido acceso a los datos podrá ser debido a que:

- Alguna parte de la estructura del sistema de archivos se encuentra dañada.
- Algún archivo ha sido borrado con los comandos del sistema y por tanto no aparece en la “lista de archivos” que contiene el sistema.

La recuperación lógica de datos consiste en analizar la estructura de archivos que permanece, identificar el daño producido y acceder a los datos que aún están en el dispositivo. En algunos casos se pueden recuperar los datos identificativos del archivo, (nombre, extensión, tamaño, fecha de creación, etc.) y en otros sólo el contenido del mismo.

Algunas herramientas emplean el término análisis profundo o “en bruto” que consiste en analizar toda la superficie del disco buscando aquellas codificaciones específicas que permiten identificar a cada tipo de archivo.

2. Métodos de recuperación física: si algún componente físico del dispositivo se encuentra dañado, pero el soporte de almacenamiento sigue inalterado, se podrá abordar una recuperación física reparando o sustituyendo el componente dañado y accediendo nuevamente a la información guardada, y recuperando directamente el contenido de los mismos, sin tener en cuenta la información presente en la “lista de archivos”, por lo que se pierden el nombre y las fechas de los archivos recuperados.

Los métodos de recuperación física requieren un conocimiento profundo de cada uno de los componentes de los dispositivos.

En el caso de que el soporte de almacenamiento, por ejemplo los platos en los discos duros, se encuentre dañado hay posibilidades de que se produzca una recuperación de la información, pero el procedimiento y las herramientas utilizadas son diferentes y más costosas. Existen muchas empresas que se encargan de realizar este proceso denominado recuperación de información a nivel hardware.

En la investigación de esta tesina, se utilizaran únicamente los métodos de recuperación lógica a través de diferentes herramientas para la comprobación de la correcta destrucción de la información realizada a nivel software.

Herramientas de recuperación lógica.

Existen diferentes herramientas de recuperación de información lógica por medio de software que escanean el disco de diferentes formas. A continuación se describirán las cuatro (4) herramientas, seleccionadas por su popularidad, utilizada hoy en día.

Las cuatro (4) herramientas seleccionadas son:

1. Easy Recovery [30].
2. Recovery My Files [31].
3. Handy Recovery [32].
4. Recuva [33].

Easy Recovery.

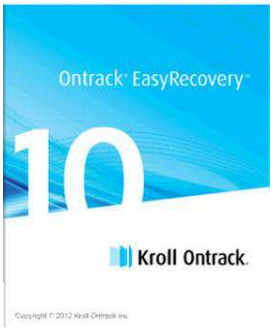


Figura 35. Logo herramienta Easy Recovery.

Compatible con Windows 95/98/NT/ME/2000/XP/Vista/2003/7/8, y todas las versiones de Windows Servers. Recupera archivos Windows de sistemas FAT12, FAT16, FAT32, NTFS, NTFS 5. También recupera los datos del sistema de archivos Mac HFS en dispositivos externos y los datos de sistemas de archivos Linux Ext2/Ext3.

Permite la recuperación de discos formateados, particiones y todo tipo de medios digitales, unidades de disco duro/SSD, dispositivos de memoria flash, dispositivos USB externos, y todos los otros tipos de medios extraíbles.

Es compatible con SATA/IDE/SCSI, y permite la recuperación de CD/DVD (ISO9660/UDF combinado con ISO9660) y archivos Linux (Ext2/3).

Es una herramienta comercial.

Recovery My Files.

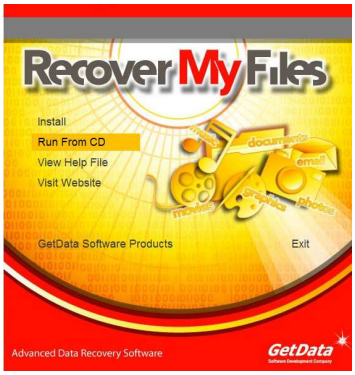


Figura 36. Logo herramienta Recovery My Files.

Recupera discos duros formateados, incluso si se ha reinstalado Windows, también recupera archivos después de un fallo físico del disco duro o después de un error al realizar una partición. Recupera documentos, fotos, vídeo, música y correos electrónicos; también datos de un disco duro, una tarjeta SD, un medio de almacenamiento USB, una unidad Zip, un disco flexible o cualquier otro medio.

Es una herramienta comercial, la versión de prueba permite realizar todo el análisis pero no la recuperación.

Handy Recovery.

Figura 37. Logo herramienta Handy Recovery.

Trabaja con los Sistemas Operativos Microsoft Windows 2000/XP/2003/Vista/Win7. El programa soporta todos los sistemas de ficheros de Windows para discos duros y disquetes incluso FAT12/16/32, NTFS/NTFS 5 y recuperación de imágenes de tarjetas CompactFlash, SmartMedia, MultiMedia y Secure Digital. Puede recuperar los ficheros borrados y cifrados en los discos NTFS.

Es una herramienta comercial.

Recuva.

Figura 38. Logo herramienta Recuva.

Trabaja con el Sistema Operativo Windows, es capaz de recuperar datos de la papelera de reciclaje, tarjetas de memoria o reproductores de MP3.

Es una herramienta gratuita.

Durante la etapa de recuperación de información sobre la muestra de discos duros seleccionados y descripta más adelante también, se utilizaron las herramientas Easy Recovery [30] y Recovery My Files [31]; las herramientas Handy Recovery [32] y Recuva [33] fueron descartadas ya que el proceso de recuperación de la información que realizan no permite un escaneo profundo sector por sector, por lo tanto los resultados no son tan específicos y eficientes como el de las herramientas seleccionadas.

Estudio realizado.

Durante el intervalo de octubre del 2013 a marzo del 2014 realice un estudio de higienización y recuperación de información sobre diferentes discos magnéticos donados al proyecto E-Basura [1], con el fin de comprobar la correcta eliminación y la no recuperación de datos sensibles de los diferentes donantes.

Es importante realizar la correcta higienización de la información contenida en los discos duros que son entregados al proyecto, ya que los mismos son donados de diferentes maneras, por ejemplo:

- Con el Sistema Operativo instalado y toda la información, es decir, sin ningún borrado realizado.
- Con el Sistema Operativo instalado, y solo borrada la información con el comando "suprimir".
- Con el Sistema Operativo instalado, el disco particionado, y la partición de datos formateada con la herramienta que ofrece el mismo Sistema Operativo.
- Formateados completos, sin Sistema Operativo.
- Donaciones después de abril del 2013, discos inundados. Sin borrados realizados.

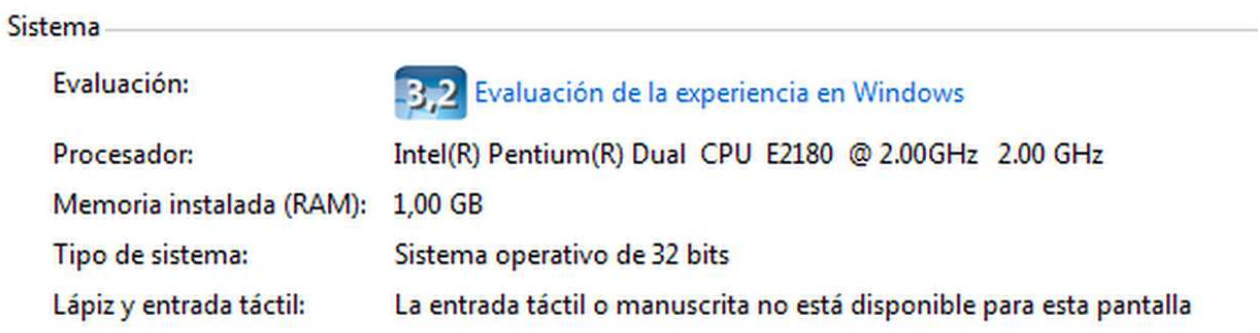
Por otro lado, actualmente muchas de las empresas que reciben o entregan este tipo de material no poseen un correcto protocolo de entrega de donaciones. Por lo tanto, mucha de la información sensible o importante es dejada. Como también existe el caso que los datos específicos del disco son suprimidos o no, por ejemplo los discos duros suelen ser entregados:

- Con etiquetas correspondientes a la empresa donante, por lo que se podría identificar a quien corresponde la información que los mismos contengan.
- Discos sin sus etiquetas de información correspondientes, es decir, le han sacado las etiquetas donde se encuentra la información del disco (número de serie, capacidad, etc.). Esto afecta en la correcta identificación univoca del disco.
- Información escrita sobre los discos, por ejemplo la dirección IP sobre la red que corría dentro de una empresa.
- Máquinas con nombre de usuarios y contraseñas, incluyendo los discos sin ningún borrado, permitiendo el acceso al mismo sin ninguna restricción.

En el estudio realizado se produjo una correcta higienización y recuperación de información de un total de veinticuatro (24) discos, de diferentes marcas y con capacidades distintas, sobre cuatro (4) máquinas diferentes.

Las especificaciones de las máquinas utilizadas son:

Máquina 1:



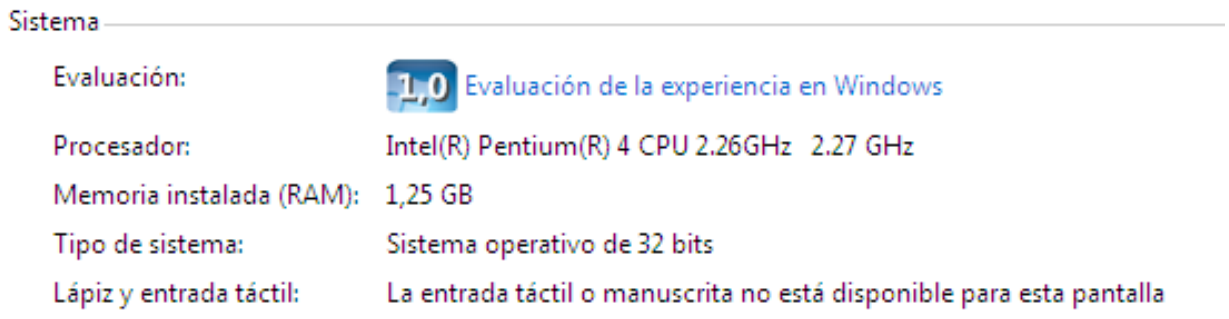
Máquina 2:

Procesador: Intel (R) Celeron (R) 2.66 GHz

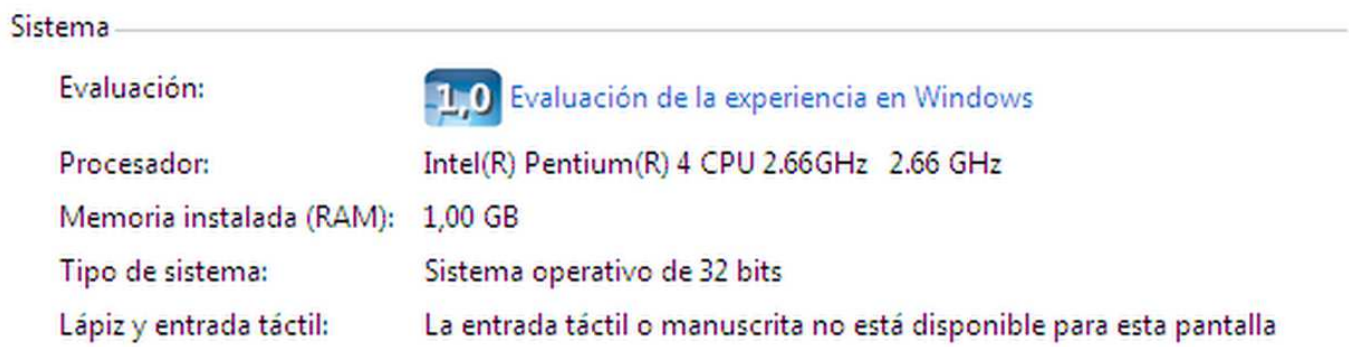
Memoria Instalada (RAM): 512 MB

Tipo de Sistema: ningún Sistema Operativo instalado. Utilización de CD de booteo.

Máquina 3:



Máquina 4:



Discos sobre los cuales se realizaron los estudios.

#Disco	Marca Disco Duro	Tamaño	Algoritmo aplicado	Herramienta utilizada
1	Deskstar HITACHI	82.3 GB	Canadian RCMP TSSIT OSP-II (7 pasadas)	DBN
2	Samnsung	3.2 GB	Canadian RCMP TSSIT OSP-II (7 pasadas)	Eraser
3	Western Digital	80 GB	Canadian RCMP TSSIT OSP-II (7 pasadas)	Eraser
4	Western Digital	40 GB	Canadian RCMP TSSIT OSP-II (7 pasadas)	KillDisk
5	QUANTUM	4 GB	Canadian RCMP TSSIT OSP-II (7 pasadas)	BCWipe
6	FUJITSU LIMITED	4 GB	DoD 5220.22-M (7 pasadas)	DBN
7	Samnsung	8.4 GB	DoD 5220.22-M (7 pasadas)	DBN
8	Western Digital	40 GB	DoD 5220.22-M (7 pasadas)	Disk Wipe
9	Samnsung	80 GB	DoD 5220.22-M (7 pasadas)	KillDisk
10	Samnsung	4.3 GB	DoD 5220.22-M (7 pasadas)	Eraser
11	Maxtor	160 GB	DoD 5220.22-M (7 pasadas)	KillDisk
12	Western Digital	17.7 GB	DoD 5220.22-M (7 pasadas)	BCWipe
13	Maxtor	2.5 GB	Peter Gutmann (35 pasadas)	Eraser
14	Samnsung	40 GB	Peter Gutmann (35 pasadas)	DBN
15	Western Digital	40 GB	Peter Gutmann (35 pasadas)	BCWipe
16	Western Digital	80 GB	Peter Gutmann (35 pasadas)	KillDisk
17	Seagate	80 GB	Peter Gutmann (35 pasadas)	Disk Wipe
18	Western Digital	20 GB	Peter Gutmann (35 pasadas)	KillDisk
19	Western Digital	80 GB	DoD 5220.22-M (3 pasadas)	Eraser
20	Western Digital	20 GB	DoD 5220.22-M (3 pasadas	KillDisk
21	Samnsung	40 GB	DoD 5220.22-M (3 pasadas)	BCWipe
22	Samnsung	4.3 GB	DoD 5220.22-M (3 pasadas)	Disk Wipe
23	Seagate	20 GB	DoD 5220.22-M (3 pasadas)	DBN
24	Seagate	4.2 GB	DoD 5220.22-M (3 pasadas)	DBN

Información del borrado de los discos.

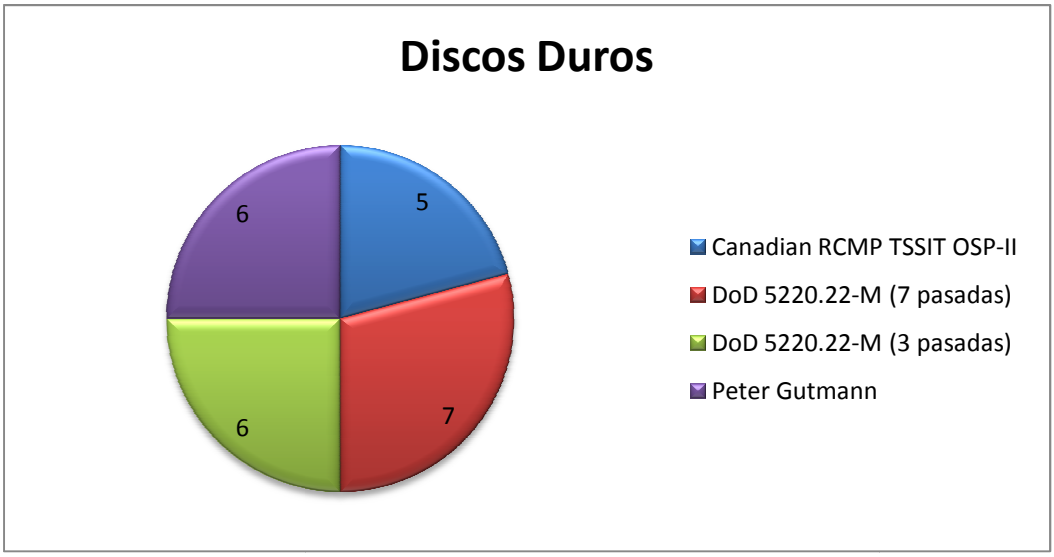


Gráfico 1. Algoritmos utilizados sobre los discos duros.

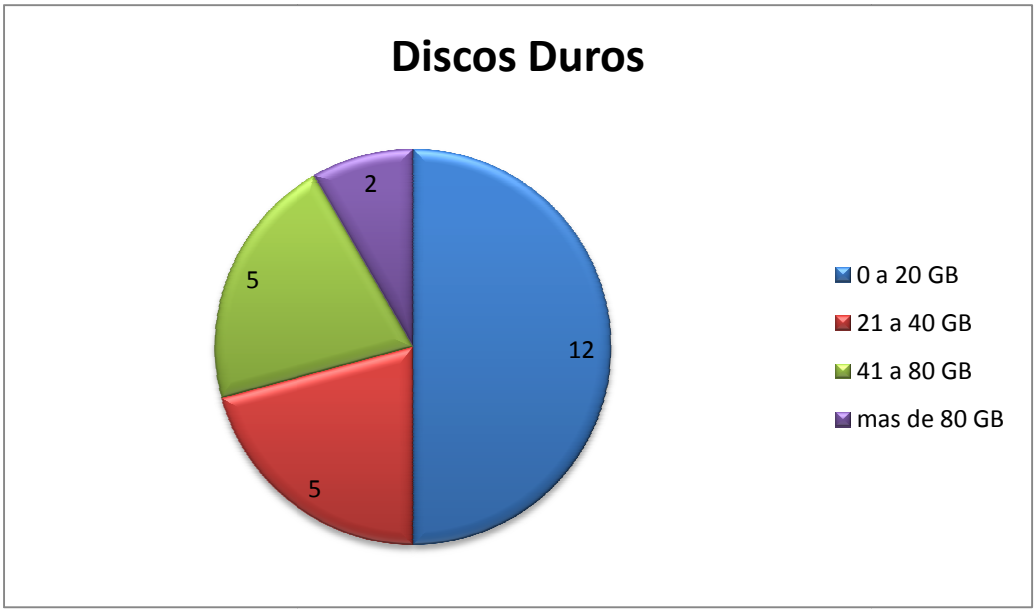


Gráfico 2. Tamaño de los discos duros.

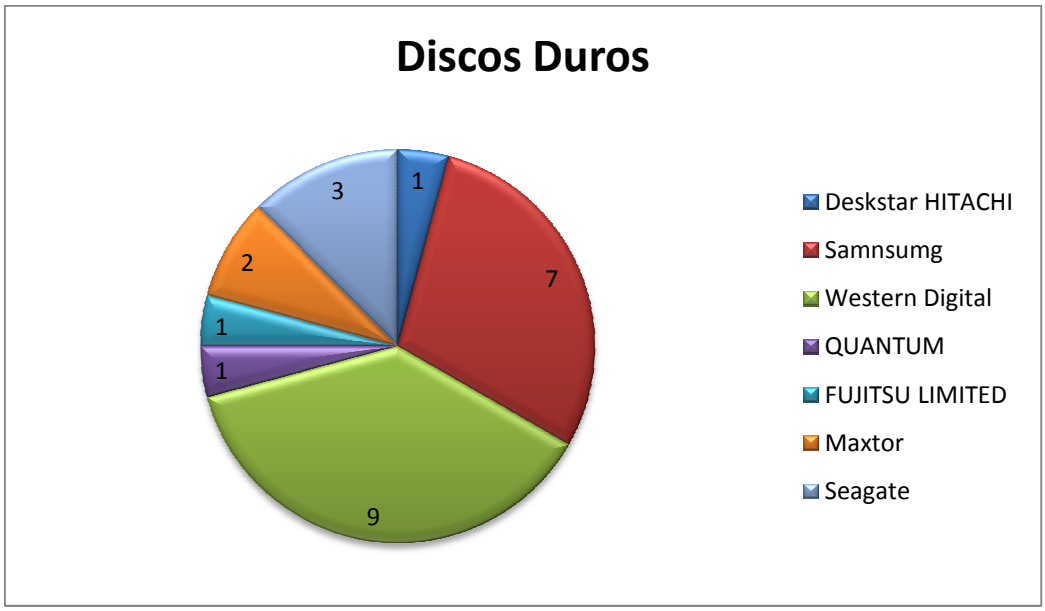


Gráfico 3. Marcas de los discos duros.

Proceso de recuperación sobre los discos higienizados.

Las herramientas seleccionadas para la recuperación de información luego del proceso de higienización son:

- ✓ Easy Recovery [30].
- ✓ Recovery My Files [31].

La selección de las herramientas se baso en la prueba y comparación de la información otorgada por las mismas.

A continuación se mostrará una tabla con un resume de los resultados obtenidos de los diferentes discos duros analizados, sobre las diferentes herramientas. La misma se divide en:

- Información de los discos duros analizados (número de disco, descripción).
- Herramienta ejecutada.
- Resultados del análisis con la herramienta. Éstos pueden ser:
  - **No se recuperó datos:** en el análisis realizado sobre el disco duro no se recuperaron ningún tipo de datos. Por ejemplo, en la tabla se pueden observar discos duros que tanto con la herramienta Recovery My Files [31] como con Easy Recovery [30] no se recuperaron datos, y esto se puede observar en las ***figuras 39 y 40/41*** respectivamente.
  - **Se recuperaron datos basura:** en el análisis realizado sobre el disco duro se recuperaron datos denominados "basura", ya que éstos a pesar de que el programa le asigno un tipo, los mismos no es legibles o están corrompidos por lo tanto no se puede acceder a la información contenida en ellos. Por ejemplo, en la tabla se pueden observar discos duros que tanto con la herramienta Recovery My Files [31] como con Easy Recovery [30] se recuperaron datos "basura", y esto se puede observar en las ***figuras 42 y 43*** respectivamente.
  - **Se recuperaron datos creados por dar formato (NTFS):** en el análisis realizado sobre el disco duro se recuperaron datos creados al momento de dar formato al disco, este es el caso del formato NTFS. Los datos recuperados se describe en el capítulo de "sistemas de archivos" específicamente en "sistemas de archivos NTFS". Por ejemplo, en la tabla se pueden observar discos duros que tanto con la herramienta Recovery My Files [31] como con Easy Recovery [30] se recuperaron archivos creados por dar formato, y esto se puede observar en las ***figuras 44 y 45*** respectivamente.
  - **Se recuperaron datos del usuario:** se espera que en el análisis realizado sobre el disco duro se recuperen datos legibles y no corrompidos creados por el usuario, pero al realizar el análisis correspondiente no se recuperaron datos legibles y no corrompidos.
  - **Disco dañado, no se recuperaron datos:** en el análisis realizado sobre el disco duro no se recuperaron datos ya que diferentes sectores del disco se encontraban dañados, esto fue justificado en el capítulo de "higienización de datos" específicamente en "discos fallados ¿Cómo proceder?". Por ejemplo, en la tabla se pueden observar discos duros que tanto con la herramienta Recovery My Files [31] como con Easy Recovery [30] se detecto que el disco se encontraba dañado, y esto se puede observar en las ***figuras 46/47 y 48/49*** respectivamente.

Figura 39. Ejemplo no se recuperó ningún dato con Recovery My Files.

Figura 40. Ejemplo no se recuperó ningún dato con Easy Recovery.

Figura 41. Ejemplo no se recuperó ningún dato con Easy Recovery.

Figura 42. Ejemplo se recuperaron datos basura con Recovery My Files.

Nota: se encontraron 3 archivos creados el 14-jul-2009 a las 6:18 AM.

Figura 43. Ejemplo se recuperaron datos basura con Easy Recovery.

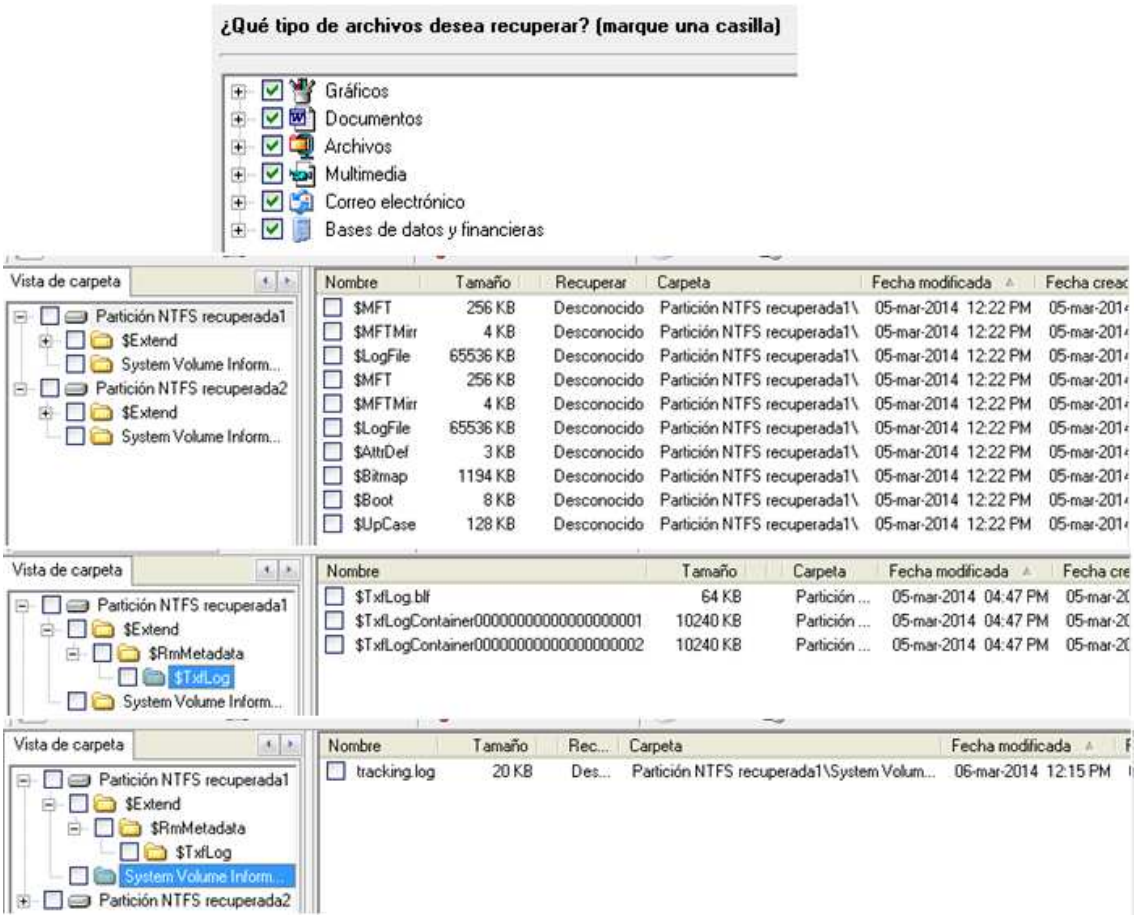


Figura 44. Ejemplo datos recuperados por dar formato con Recovery My Files.

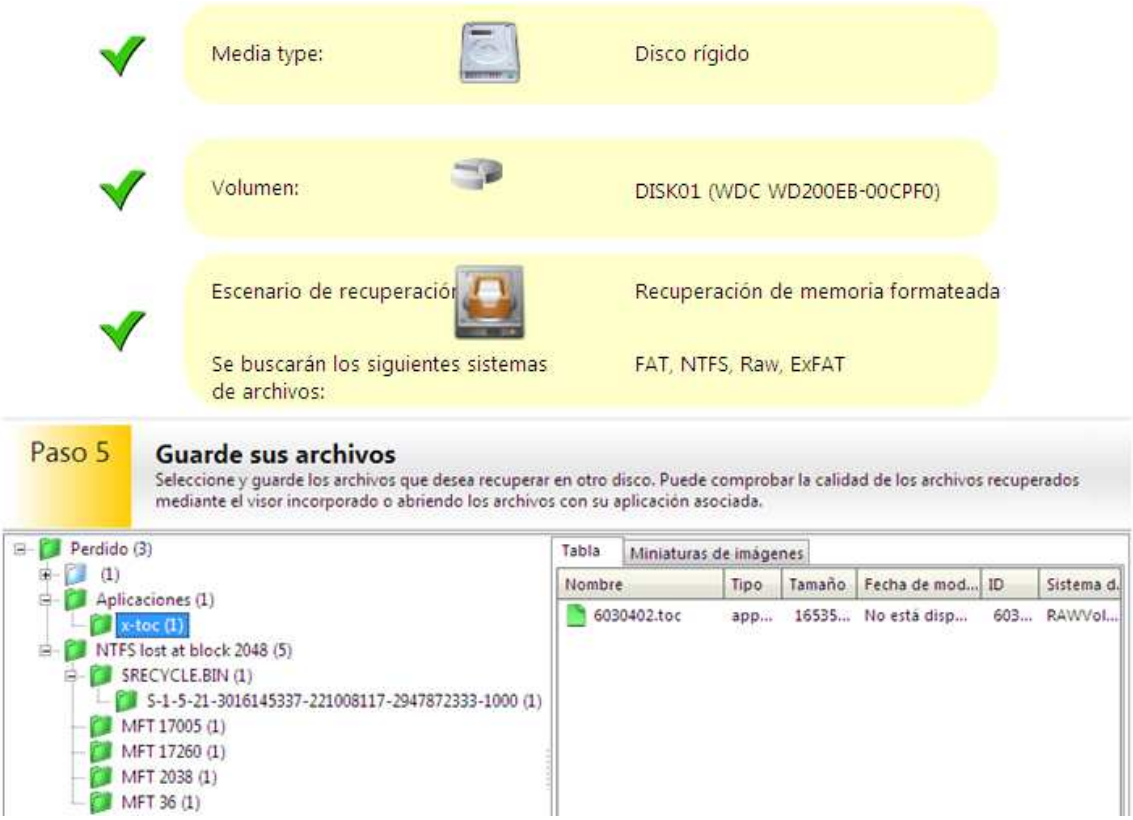


Figura 45. Ejemplo datos recuperados por dar formato con Easy Recovery.

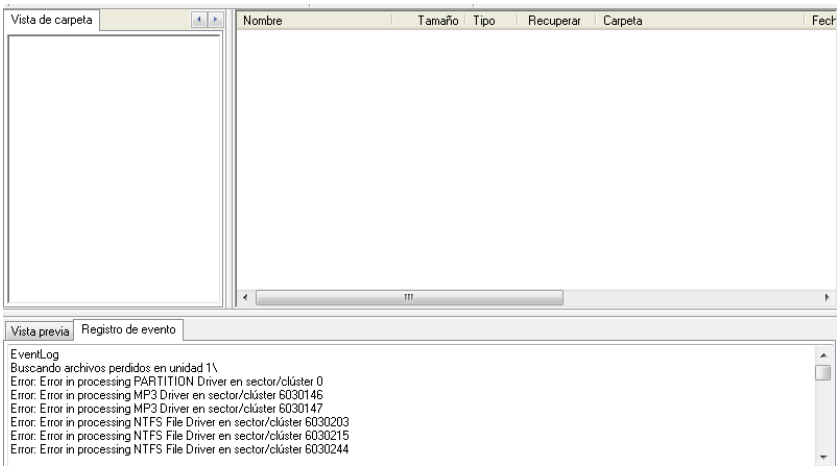


Figura 46. Ejemplo disco dañado con Recovery My Files.

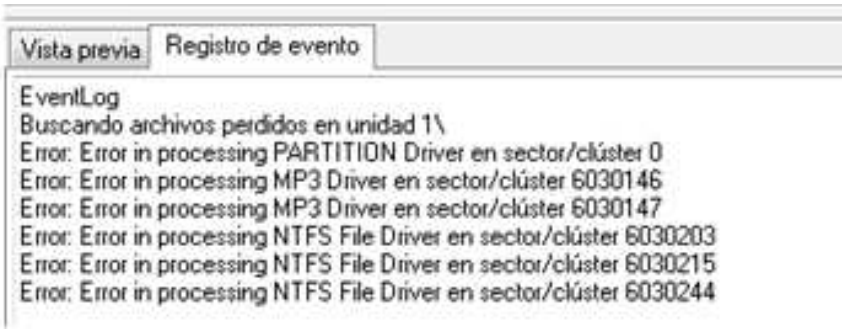


Figura 47. Ejemplo disco dañado con Recovery My Files.

Figura 48. Ejemplo disco dañado con Easy Recovery.

Figura 49. Ejemplo disco dañado con Easy Recovery.

Tabla de resultados obtenidos de las herramientas.

En la siguiente tabla se mostrará el resume de los resultados obtenidos de los diferentes discos duros analizados, sobre las diferentes herramientas.

#Disco	Descripción	Herramienta	No se recuperó datos.	Se recuperaron datos basura.	Se recuperaron datos creados por dar formato (NTFS)	Se recuperaron datos del usuario.	Disco dañado. No se recuperaron datos.
1	Deskstar HITACHI (82.3 GB) **Algoritmo:** Canadian RCMP TSSIT OSP-II (7 pasadas) **Herramienta:** DBAN	Recovery My Files	✘	✔	✔	✘	✘
		Easy Recovery	✘	✔	✔	✘	✘
2	Samnsung (3.2 GB) **Algoritmo:** Canadian RCMP TSSIT OSP-II (7 pasadas) **Herramienta:** Eraser	Recovery My Files	✘	✘	✔	✘	✘
		Easy Recovery	✔	✘	✘	✘	✘
3	Western Digital (80 GB) **Algoritmo:** Canadian RCMP TSSIT OSP-II (7 pasadas) **Herramienta:** Eraser	Recovery My Files	✘	✘	✔	✘	✘
		Easy Recovery	✔	✘	✘	✘	✘
4	Western Digital (40 GB) **Algoritmo:** Canadian RCMP TSSIT OSP-II (7 pasadas) **Herramienta:** KillDisk	Recovery My Files	✘	✘	✔	✘	✘
		Easy Recovery	✔	✘	✘	✘	✘
5	QUANTUM (4 GB) **Algoritmo:** Canadian RCMP TSSIT OSP-II (7 pasadas) **Herramienta:** BCWipe	Recovery My Files	✘	✘	✔	✘	✘
		Easy Recovery	✔	✘	✘	✘	✘
6	FUJITSU LIMITED (4 GB) **Algoritmo:** DoD 5220.22-M (7 pasadas) **Herramienta:** DBAN	Recovery My Files	✘	✘	✔	✘	✘
		Easy Recovery	✔	✘	✘	✘	✘

7	Samnsung (8.4 GB) **Algoritmo:** DoD 5220.22-M (7 pasadas) **Herramienta:** DBAN	Recovery My Files	✔	✘	✘	✘	✔
		Easy Recovery	✔	✘	✘	✘	✔
8	Western Digital (40 GB) **Algoritmo:** DoD 5220.22-M (7 pasadas) **Herramienta:** Disk Wipe	Recovery My Files	✘	✘	✔	✘	✘
		Easy Recovery	✔	✘	✘	✘	✔
9	Samnsung (80 GB) **Algoritmo:** DoD 5220.22-M (7 pasadas) **Herramienta:** KillDisk	Recovery My Files	✘	✔	✔	✘	✘
		Easy Recovery	✘	✔	✔	✘	✘
10	Samnsung (4.3 GB) **Algoritmo:** DoD 5220.22-M (7 pasadas) **Herramienta:** Eraser	Recovery My Files	✘	✘	✔	✘	✘
		Easy Recovery	✔	✘	✘	✘	✘
11	Maxtor (160 GB) **Algoritmo:** DoD 5220.22-M (7 pasadas) **Herramienta:** KillDisk	Recovery My Files	✘	✘	✔	✘	✘
		Easy Recovery	✔	✘	✘	✘	✘
12	Western Digital (17.7 GB) **Algoritmo:** DoD 5220.22-M (7 pasadas) **Herramienta:** BCWipe	Recovery My Files	✘	✘	✔	✘	✘
		Easy Recovery	✘	✔	✔	✘	✘
13	Maxtor (2.5 GB) **Algoritmo:** Peter Gutmann (35 pasadas) **Herramienta:** Eraser	Recovery My File	✔	✘	✘	✘	✘
		Easy Recovery	✔	✘	✘	✘	✘
14	Samnsung (40 GB) **Algoritmo:** Peter Gutmann (35 pasadas) **Herramienta:** DBAN	Recovery My Files	✘	✘	✔	✘	✘
		Easy Recovery	✘	✔	✘	✘	✘

15	Western Digital (40 GB) **Algoritmo:** Peter Gutmann (35 pasadas) **Herramienta:** BCWipe	Recovery My Files	✘	✘	✔	✘	✘
		Easy Recovery	✔	✘	✘	✘	✘
16	Western Digital (80 GB) **Algoritmo:** Peter Gutmann (35 pasadas) **Herramienta:** KillDisk	Recovery My Files	✘	✘	✔	✘	✘
		Easy Recovery	✔	✘	✘	✘	✘
17	Seagate (80 GB) **Algoritmo:** Peter Gutmann (35 pasadas) **Herramienta:** Disk Wipe	Recovery My Files	✘	✘	✔	✘	✘
		Easy Recovery	✘	✔	✘	✘	✘
18	Western Digital (20 GB) **Algoritmo:** Peter Gutmann (35 pasadas) **Herramienta:** KillDisk	Recovery My Files	✘	✘	✔	✘	✘
		Easy Recovery	✘	✘	✔	✘	✘
19	Western Digital (80 GB) **Algoritmo:** DoD 5220.22-M (3 pasadas) **Herramienta:** Eraser	Recovery My Files	✘	✔	✔	✘	✘
		Easy Recovery	✘	✔	✘	✘	✘
20	Western Digital (20 GB) **Algoritmo:** DoD 5220.22-M (3 pasadas **Herramienta:** KillDisk	Recovery My Files	✘	✘	✔	✘	✘
		Easy Recovery	✘	✘	✔	✘	✘
21	Samnsung (40 GB) **Algoritmo:** DoD 5220.22-M (3 pasadas) **Herramienta:** BCWipe	Recovery My Files	✘	✘	✔	✘	✘
		Easy Recovery	✔	✘	✘	✘	✘
22	Samnsung (4.3 GB) **Algoritmo:** DoD 5220.22-	Recovery My Files	✔	✘	✘	✘	✘

	M (3 pasadas) **Herramienta:** Disk Wipe	Easy Recovery	✔	✘	✘	✘	✘
23	Seagate (20 GB) **Algoritmo:** DoD 5220.22-M (3 pasadas) **Herramienta:** DBAN	Recovery My Files	✔	✘	✘	✘	✘
		Easy Recovery	✔	✘	✘	✘	✘
24	Seagate (4.2 GB) **Algoritmo:** DoD 5220.22-M (3 pasadas) **Herramienta:** DBN	Recovery My Files	✔	✘	✘	✘	✔
		Easy Recovery	✘	✔	✔	✘	✘

Estadísticas de recuperación sobre los discos.

En los siguientes gráficos se mostrará el resume de los resultados obtenidos de los diferentes discos duros analizados, sobre las diferentes herramientas.

En el primer y segundo gráfico se ilustrarán, en un gráfico de barras, las estadísticas de recuperación sobre los diferentes discos duros. El primer gráfico corresponde a la ejecución sobre la herramienta Easy Recovery, y el segundo a la ejecución sobre la herramienta Recovery My Files.

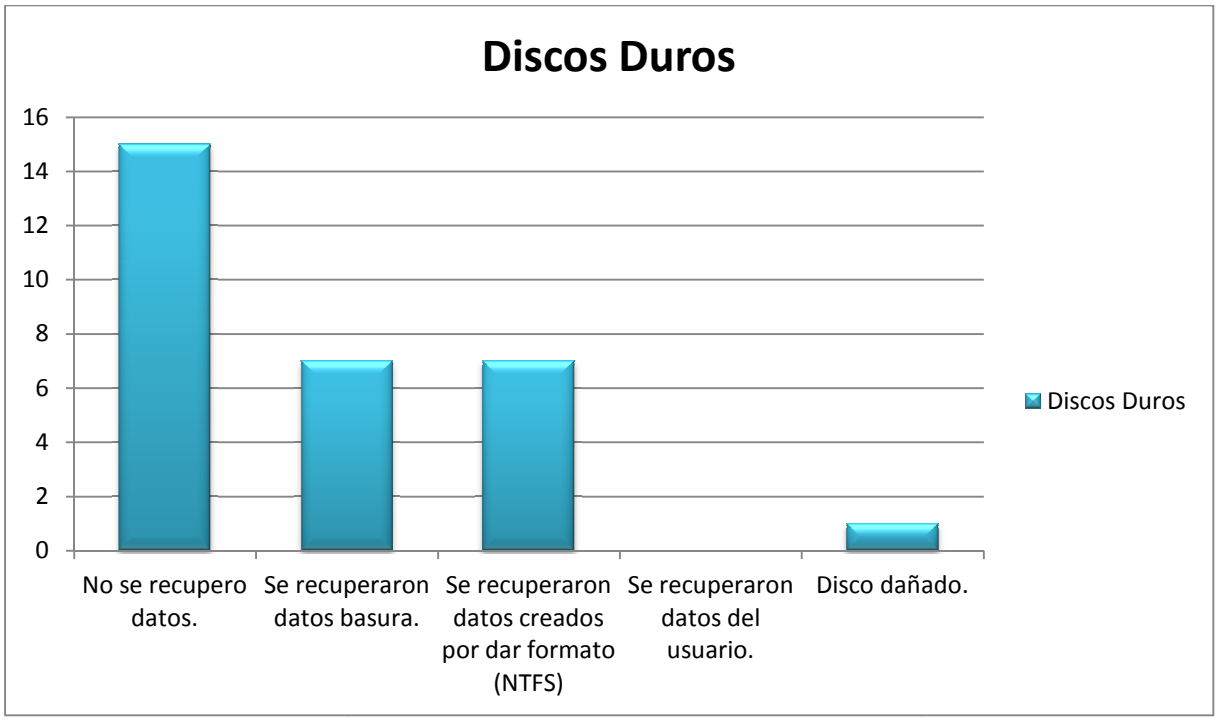


Gráfico 4. Estadísticas de recuperación – Easy Recovery.

Gráfico 5. Estadísticas de recuperación – Recovery My Files

Conclusión.

La destrucción y no permanencia de la información dentro de los discos de almacenamiento de los usuarios es algo no trivial. La correcta forma de realizar este procedimiento es a través de herramientas, que pueden ser a nivel software como hardware, certificadas y probadas.

Este trabajo expone un análisis de cómo destruir con diferentes herramientas de software y diferentes algoritmos de borrado seguro, pre-seleccionados, distintos discos duros con el fin de avalar la destrucción y no permanencia de la información dentro de este tipo de dispositivos de almacenamientos.

La comprobación de la eficiencia de las herramientas y de los algoritmos de borrado seguro posibilita la certificación de este procedimiento. La herramientas son detalladas junto a las diferentes opciones que las mismas ofrecen, permitiendo una comparación y selección de la más adecuada dependiendo de cada tipo de problema.

Una vez seleccionadas y aplicadas las herramientas y algoritmos de higienización sobre el tipo de dispositivo elegido, en este caso discos duros, los mismos son sometidos a herramientas de software de recuperación de la información, permitiendo así completar la evaluación de su eficiencia.

El análisis desarrollado y la aplicación del mismo permitieron la comprobación que las herramientas de higienización investigadas cumplen con sus objetivos y así se logra asegurar la protección de los datos de los usuarios, evitando que su información sea manipulada.

Se debe estar informado y a su vez tener en cuenta todas las medidas de seguridad para preservar la información de los usuarios, incluso a la hora de donar o reutilizar equipamiento dentro de una organización. Asegurar la protección de los datos, evita que su información sea manipulada; y a su vez permite el incremento de donaciones de equipos completos a proyectos de reacondicionamiento, lo que implica un beneficio social para la reducción de la brecha digital y el cuidado y la protección del medio ambiente a través del reciclaje y la reutilización de los RAEE.

Trabajos futuros.

Las pruebas y certificaciones de la destrucción de la información sobre los diferentes dispositivos de almacenamiento, en todas sus áreas, es un tema amplio y extenso para el desarrollo en todas sus partes en una única tesina de grado por lo que se deben plantear diferentes trabajos a futuro.

El desarrollo de la investigación de la presente tesina de grado abarca el área a nivel software. En la actualidad existen una gran cantidad de herramientas que permiten la correcta higienización y recuperación de la información dependiendo de las necesidades del usuario final.

También se presentan diferentes procedimientos para la destrucción y recuperación de la información. Estos se ramifican según las herramientas que se utilicen, por lo tanto se dividen en destrucción y recuperación a nivel software y hardware.

Una línea de trabajo futuro, que no fue desarrollada en la presente tesis, abarcaría el examen de todos los discos duros que fueron sometidos a los distintos algoritmos de higienización de la información por medio de las diferentes herramientas de hardware para la comprobación de la destrucción absoluta de la información. Este procedimiento certificaría en un 100% la eficacia y eficiencia de los algoritmos de higienización que existen.

Otra línea de trabajo futuro abarcaría la investigación sobre la rama de la destrucción física de dispositivos a través de herramientas de destrucción a nivel hardware, como por ejemplo un desmagnetizador. Este procedimiento se presenta como una alternativa en el caso puntual cuando un disco se encuentra dañado y el mismo no puede ser borrado a través de herramientas de software.

Anexo.

Discos duros sobre los cuales se trabajo.

Disco #1

Número de serie disco: HDS728080PLAT20

Fecha borrado: 11/11/13

Herramienta: Darik's Boot and Nuke (DBAN) (CONSOLA)

Algoritmo: Canadian OSP-II (7 passes, verify)

Disco #2

Número de serie disco: dW09211503308a

Fecha borrado: 11/11/13

Herramienta: Eraser (Windows)

Algoritmo: Canadian OSP-II (7 passes, verify)

Disco #3

Número de serie disco: WMAM9VJ50539

Fecha borrado: 11/11/13

Herramienta: Erase (Windows)

Algoritmo: Canadian OSP-II (7 passes, verify)

Disco #4

Número de serie disco: WCAATD797022

Fecha borrado: 05/11/13

Herramienta: KillDisk (WINDOWS)

Algoritmo: Canadian OSP-II (7 passes, verify)

Disco #5

Número de serie disco: 691000635590

Fecha borrado: 11/11/13

Herramienta: BCWipe (Windows)

Algoritmo: Canadian OSP-II (7 passes, verify)

Disco #6

Número de serie disco: MPB3043ATU

Fecha borrado: 12/11/13

Herramienta: Darik's Boot and Nuke (DBAN) (CONSOLA)

Algoritmo: US DoD 5220.22-m (ECE) (7 passes, verify)

Disco #7

Número de serie disco: SV0844A

Fecha borrado: 12/11/13

Herramienta: Darik's Boot and Nuke (DBAN) (CONSOLA)

Algoritmo: US DoD 5220.22-m (ECE) (7 passes, verify)

Disco #8

Número de serie disco: WCAAT7176396

Fecha borrado: 05/11/13

Herramienta: Disk Wipe (Windows)

Algoritmo: US DoS 5220.22-m (ECE) (7 passes, verify)

Disco #9

Marca: Samsung

Número de serie disco: S0DWJ1JL511656

Fecha borrado: 01/11/13

Herramienta: KillDisk (WINDOWS)

Algoritmo: US DoD 5220.22-m (ECE) (7 passes, verify)

Disco #10

Número de serie disco: 0093J1EK133724

Fecha borrado: 11/11/13

Hora fin borrado: 14:10 PM

Herramienta: Erase (Windows)

Algoritmo: US DoD 5220.22-m (ECE) (7 passes, verify)

Disco #11

Número de serie disco: L31ZT8AG

Fecha borrado: 11/11/13

Herramienta: KillDisk (Windows)

Algoritmo: US DoD 5220.22-m (ECE) (7 passes, verify)

Disco #12

Número de serie disco: WM9160053349

Fecha borrado: 12/11/13

Herramienta: BCWipe (Windows)

Algoritmo: US DoD 5220.22-m (ECE) (7 passes, verify)

Disco #13

Número de serie disco: L31TR0FA

Fecha borrado: 06/01/13

Herramienta: Erase (Windows)

Algoritmo: Peter Gutmann (35 passes, verify)

Disco #14

Número de serie disco: S01JJ50Y522692

Fecha borrado: 06/11/13

Herramienta: Darik's Boot and Nuke (DBAN) (CONSOLA)

Algoritmo: Peter Gutmann (35 passes, verify)

Disco #15

Número de serie disco: WMAMC3576977

Fecha borrado: 05/11/13

Herramienta: BCWipe (Windows)

Algoritmo: Peter Gutmann (35 passes, verify)

Disco #16

Número de serie disco: WMAM9VM23893

Fecha borrado: 06/11/13

Herramienta: KillDisk (Windows)

Algoritmo: Peter Gutmann (35 passes, verify)

Disco #17

Número de serie disco: 6QZ0L75B

Fecha borrado: 06/11/13

Herramienta: Disk Wipe (Windows)

Algoritmo: Peter Gutmann (35 passes, verify)

Disco #18

Marca: Western Digital

Número de serie disco: WMAAU5215433

Fecha borrado: 01/11/13

Herramienta: KillDisk (WINDOWS)

Algoritmo: Peter Gutmann (35 passes, verify)

Disco #19

Número de serie disco: WMAM9LN19272

Fecha borrado: 07/11/13

Herramienta: Erase (Windows)

Algoritmo: NCSC-TG-025 (3 passes, verify)

Disco #20

Número de serie disco: WMAATC314510

Fecha borrado: 05/11/13

Herramienta: KillDisk (WINDOWS)

Algoritmo: US DoD 5220.22-M (3 passes, verify)

Disco #21

Número de serie disco: S01JJ40XA82084

Fecha borrado: 06/11/13

Herramienta: BCWipe (Windows)

Algoritmo: US DoD 5220.22-M (3 passes, verify)

Disco #22

Número de serie disco: 0105J1FK417495

Fecha borrado: 02/12/13

Herramienta: Darik's Boot and Nuke (DBAN) (CONSOLA)

Algoritmo: US DoD 5220.22-M (3 passes, verify)

Disco #23

Número de serie disco: 7ED1BBHH

Fecha borrado: 02/12/13

Herramienta: Darik's Boot and Nuke (DBAN) (CONSOLA)

Algoritmo: US DoD 5220.22-M (3 passes, verify)

Disco #24

Número de serie disco: 5BF1TGP2

Fecha borrado: 02/12/13

Herramienta: Darik's Boot and Nuke (DBAN) (CONSOLA)

Algoritmo: US DoD 5220.22-M (3 passes, verify)

Herramientas de Higienización de los datos: ¿Cómo utilizarlas?

Eraser.

Una vez iniciado el programa, en la solapa “Erase Schedule” (Planificar Borrado), seleccionamos la opción “New Task” (nueva tarea) para realizar el borrado seguro, en este caso de una memoria USB, como se muestra en la ***figura 50***.

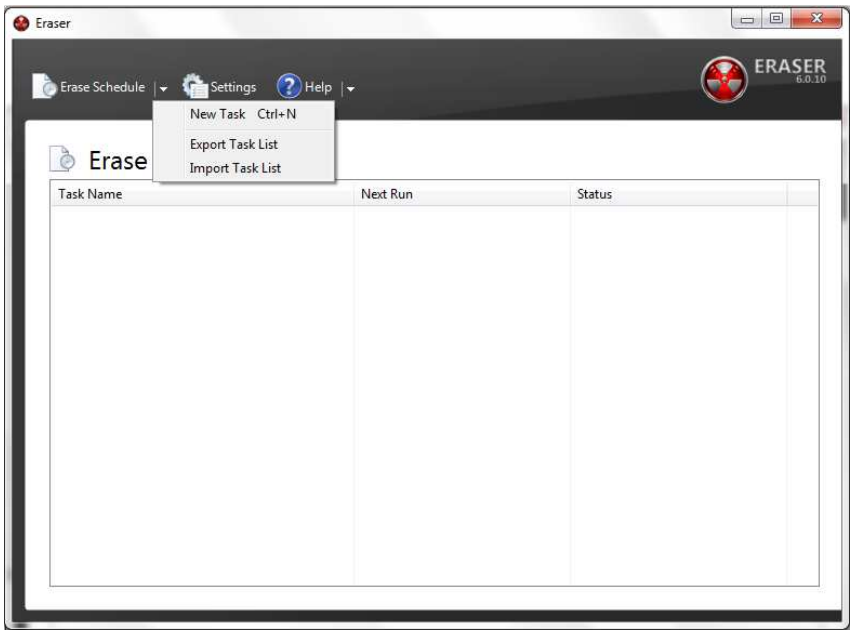


Figura 50. Imagen ejemplo funcionamiento programa Eraser.

Como se muestra en la ***figura 51***, se abrirá una nueva ventana en la cual se debe:

- Colocar un nombre a la tarea (opcional).
- Seleccionar el tipo de tarea:
  - ✓ Ejecutar manualmente.
  - ✓ Ejecutar inmediatamente.
  - ✓ Ejecutar al reiniciar.
  - ✓ Periódico.
- Agregar los datos/discos a borrar.

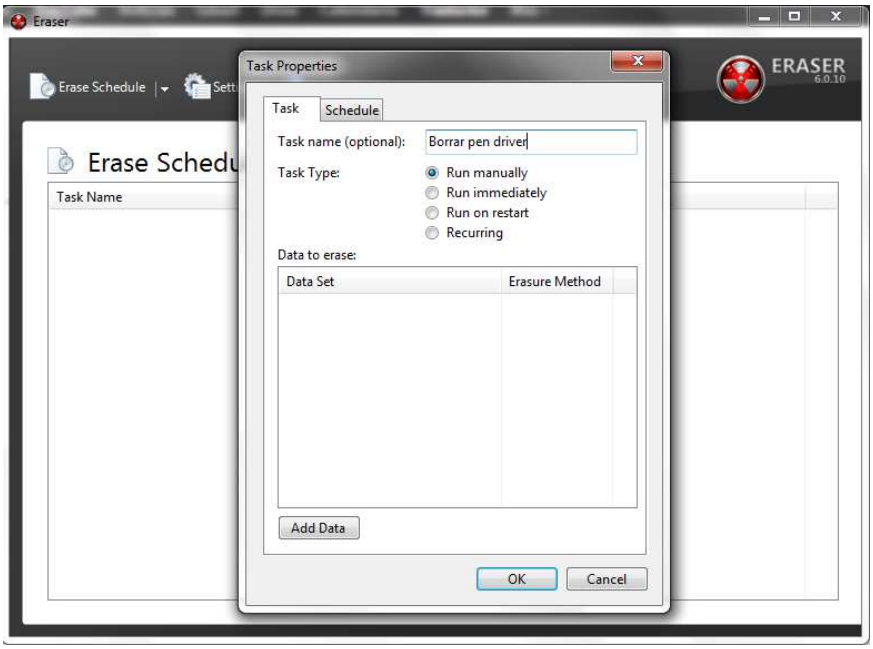


Figura 51. Imagen ejemplo funcionamiento programa Eraser.

En este caso le colocaremos el nombre de “Borrar pendriver” y seleccionaremos el tipo manual. Para agregar la memoria USB a borrar debemos apretar el botón “add data” (agregar datos). Por lo tanto se abrirá una nueva ventana, como se muestra en la ***figura 52***.

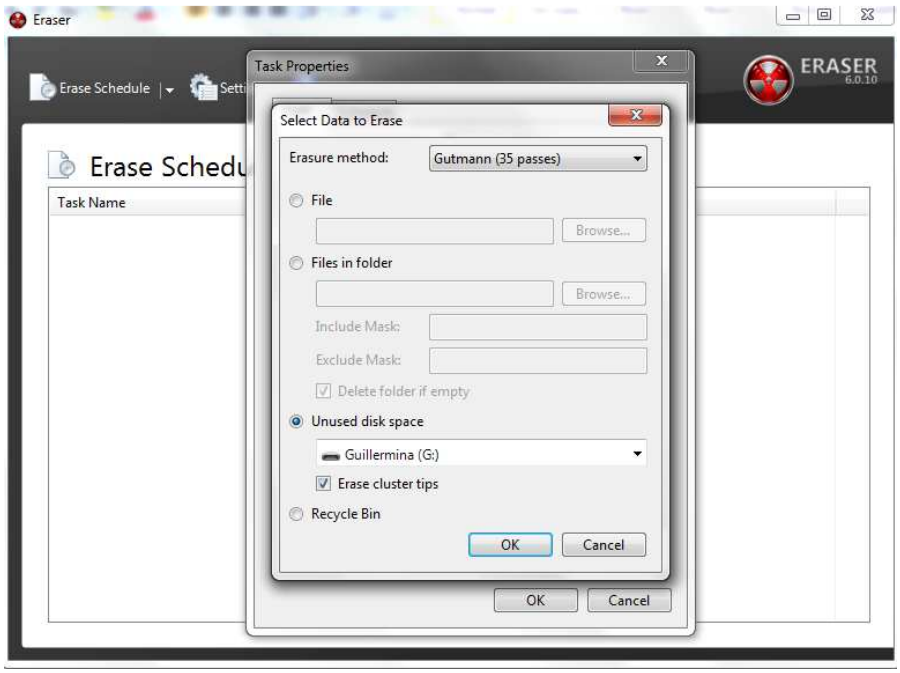


Figura 52. Imagen ejemplo funcionamiento programa Eraser.

Primero debemos definir el Algoritmo a utilizar en la opción “Erasure method” (método de borrado), en este caso optamos por el Algoritmo Gutmann. Luego

seleccionaremos la opción “unused disk space” (espacio de disco no utilizado) para especificar que vamos a borrar la memoria USB. Y por último, apretamos el botón “ok” (aceptar).

Ahora la memoria USB aparecerá en la lista de los datos a borrar, como se muestra en la ***figura 53***. Volvemos a apretar el botón “ok” (aceptar).

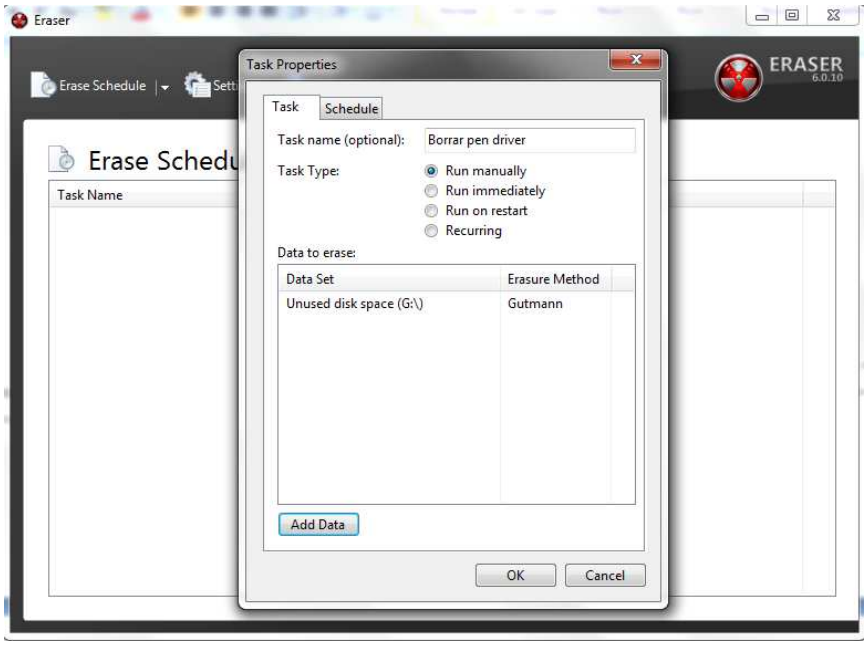


Figura 53. Imagen ejemplo funcionamiento programa Eraser.

Ahora la tarea aparecerá en la lista de borrados programados, como se muestra en la ***figura 54***.

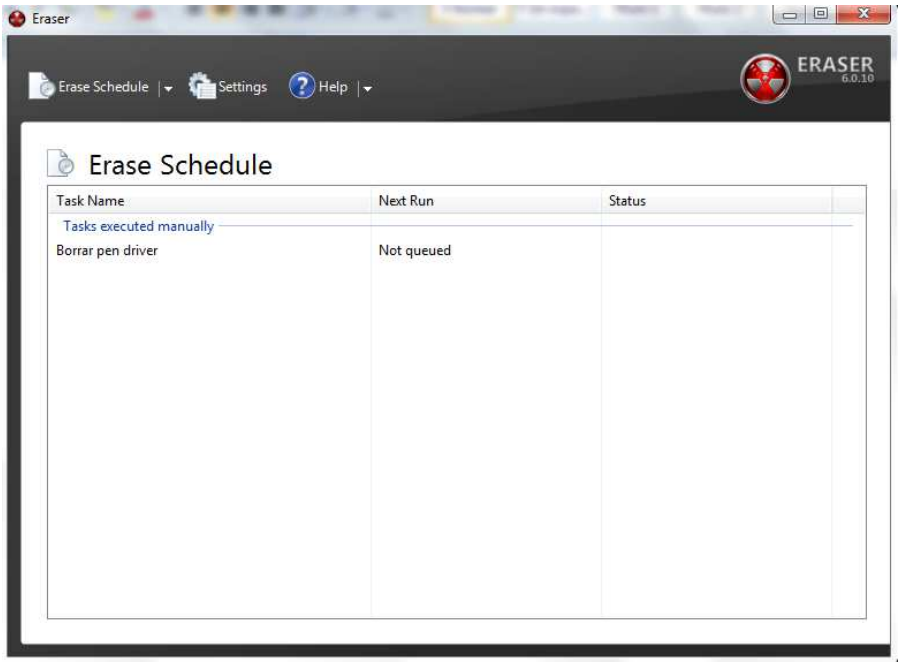


Figura 54. Imagen ejemplo funcionamiento programa Eraser.

Para iniciar la tarea debemos realizar un clic derecho sobre la tarea y seleccionar la opción “run task” (correr tarea), como se muestra en la ***figura 55***.

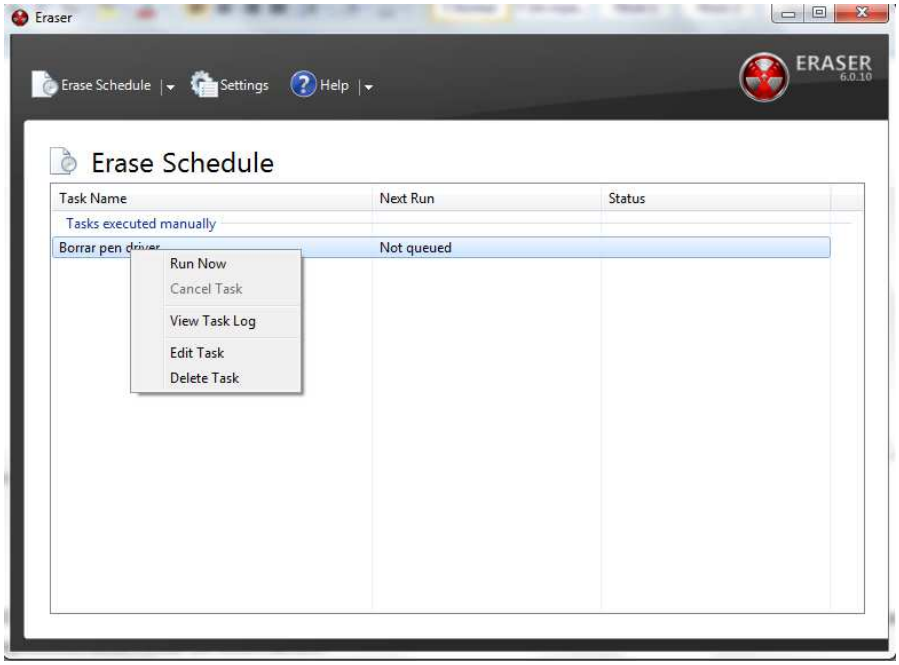


Figura 55. Imagen ejemplo funcionamiento programa Eraser.

Una vez seleccionada la opción de ejecutar la tarea comenzará el borrado, como se muestra en la ***figura 56***.

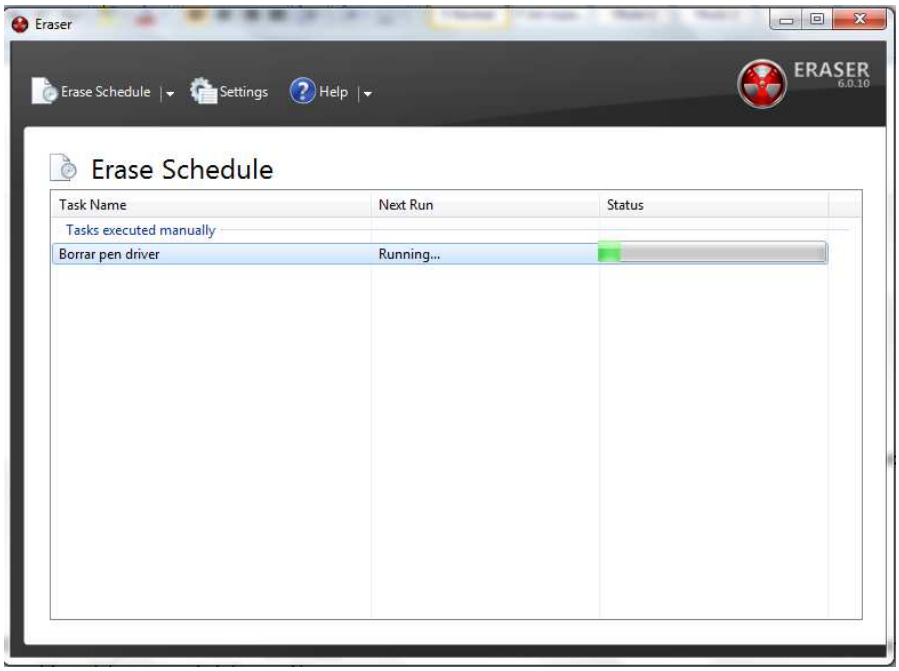


Figura 56. Imagen ejemplo funcionamiento programa Eraser.

Una vez finalizado el borrado (el tiempo depende del algoritmo seleccionado y del tamaño del dispositivo), el estado del mismo será “completed” (completado) como se muestra en la ***figura 57***.

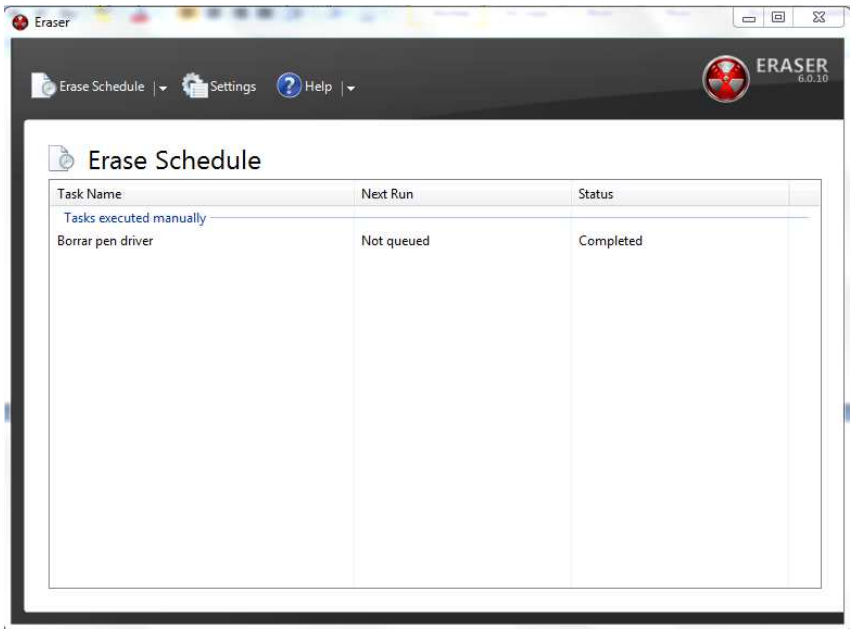


Figura 57. Imagen ejemplo funcionamiento programa Eraser.

Para poder ver el log, se hace clic derecho sobre la tarea, como se muestra en la ***figura 58***, y se selecciona la opción “view task log” (ver el log de la tarea).

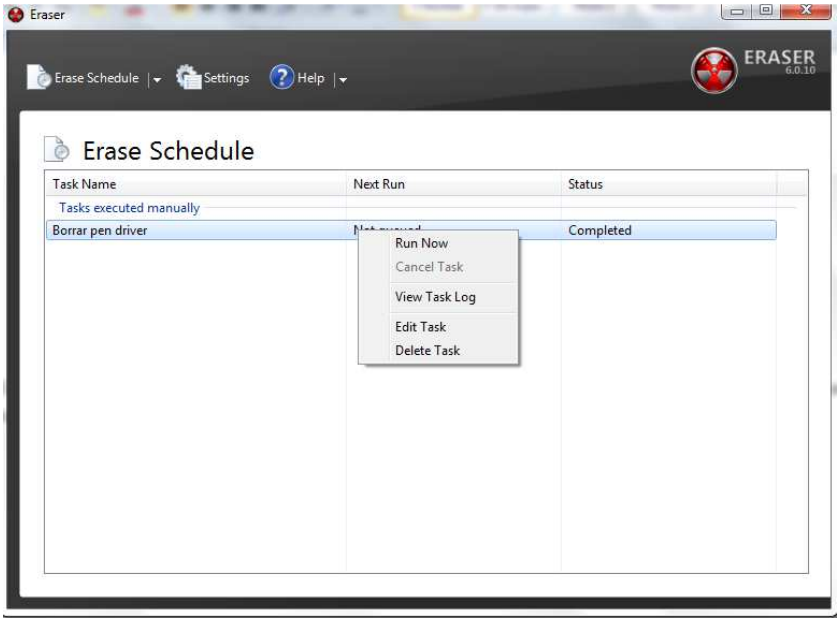


Figura 58. Imagen ejemplo funcionamiento programa Eraser.

BCWipe.

Una vez iniciado el programa, se abrirá una ventana de presentación donde se permitirá realizar dos tareas, como se muestra en la ***figura 59***:

- Ejecutar administrador de tareas:
- Activar limpieza en segundo plano:

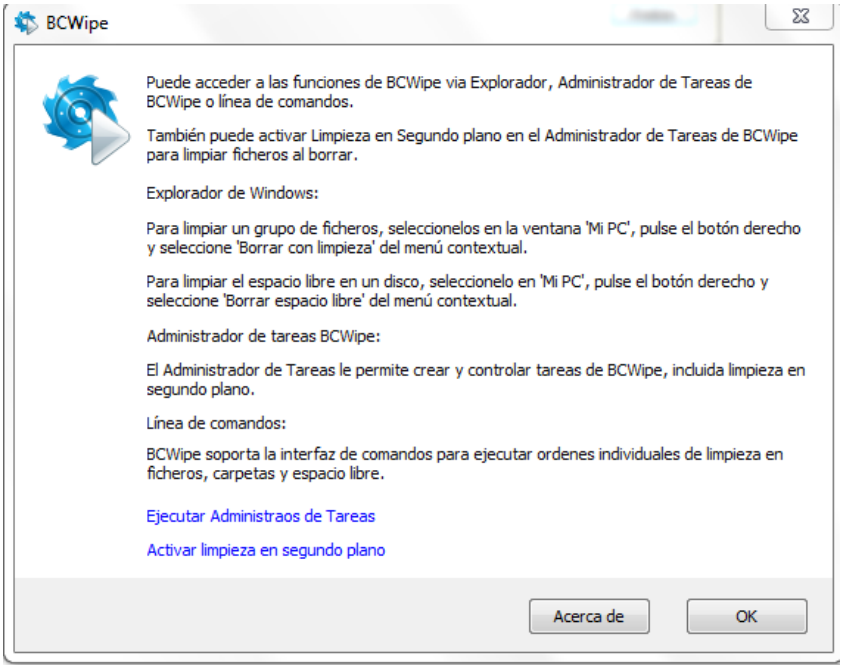


Figura 59. Imagen ejemplo funcionamiento programa BCWipe.

Para realizar una mejor limpieza seleccionamos la opción de Ejecutar Administrador de Tareas y se abrirá una nueva ventana, como se muestra en la ***figura 60***.

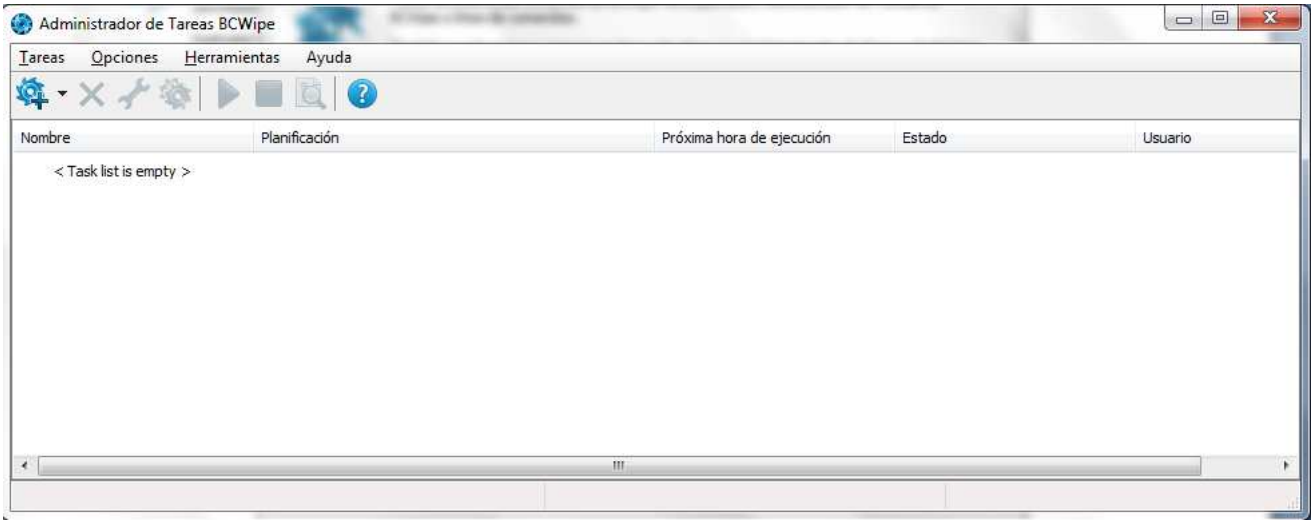


Figura 60. Imagen ejemplo funcionamiento programa BCWipe.

Para crear una nueva tarea, como se muestra en la ***figura 61***, se debe hacer clic en la solapa “Tareas”. Luego seleccionar “Crear una nueva tarea”, en la cual se despliega una lista de las diferentes tareas que se pueden realizar. Las cuales son:

- Borrar y limpiar.
- Limpiar espacio libre.
- Limpiar historial de internet.
- Limpiar historial local.
- Limpieza en segundo plano.
- Cifrado de archivos de Swap.

En nuestro caso, nos interesa seleccionar la opción de “Limpiar espacio libre”. Es necesario que se haya eliminado todo el contenido del dispositivo a borrar, ya que BVWipe no cuenta con la opción de borrar por completo el dispositivo en cuestión, solo borra los sectores libres.

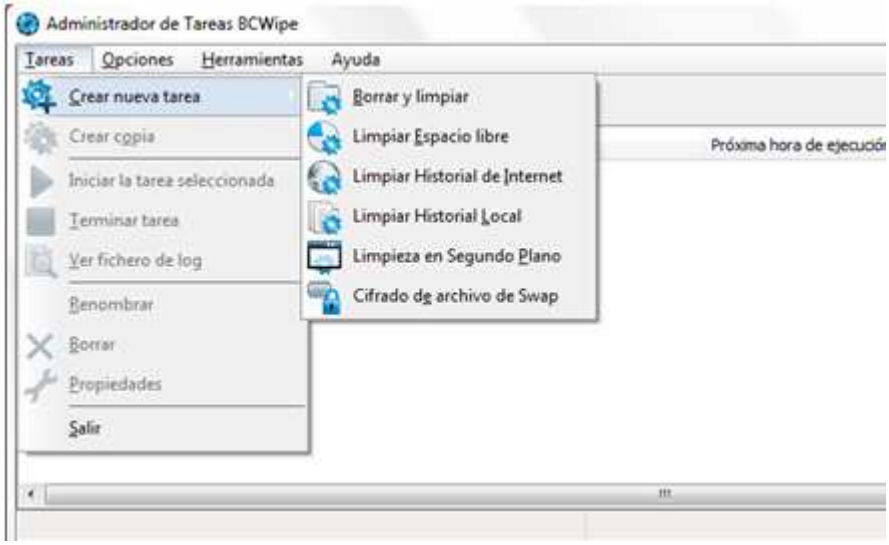


Figura 61. Imagen ejemplo funcionamiento programa BCWipe.

Una vez seleccionada la opción, se abrirá una nueva ventana, como se muestra en la ***figura 62***. En la misma, en la solapa limpiar espacio libre, seleccionaremos el dispositivo a borrar, en este ejemplo el dispositivo es un pendrive.

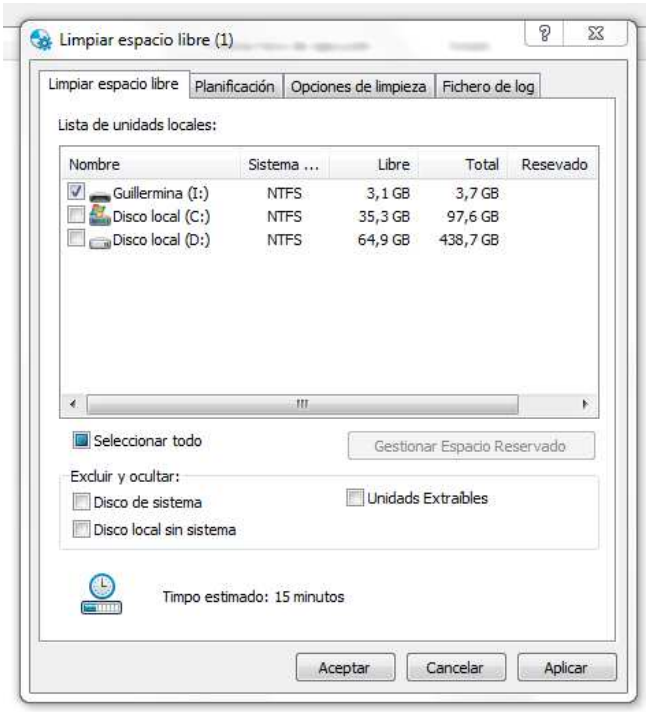


Figura 62. Imagen ejemplo funcionamiento programa BCWipe.

Como se muestra en la ***figura 63***, pasamos a la siguiente solapa denominada "planificación". En esta se puede planificar cuando y en que horario puede comenzar a ejecutarse la tarea. Como en este ejemplo la ejecutaremos en este momento no es necesario planificarla.

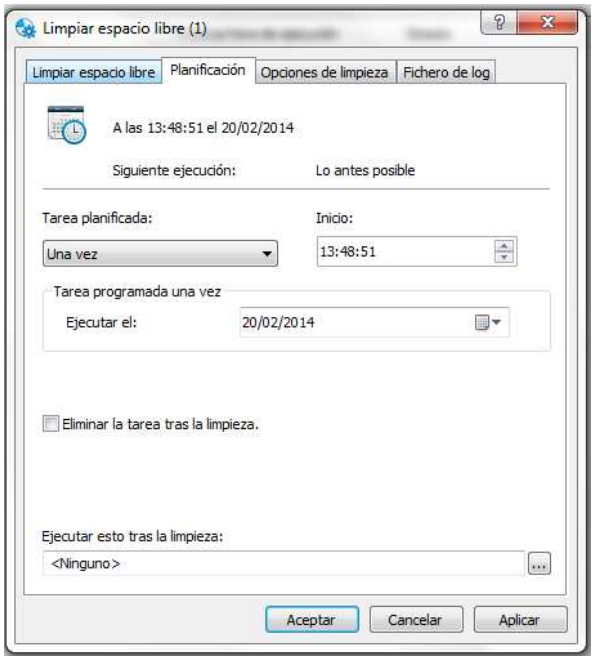


Figura 63. Imagen ejemplo funcionamiento programa BCWipe.

Como se muestra en la ***figura 64***, pasamos a la siguiente solapa denominada “opciones de limpieza”.

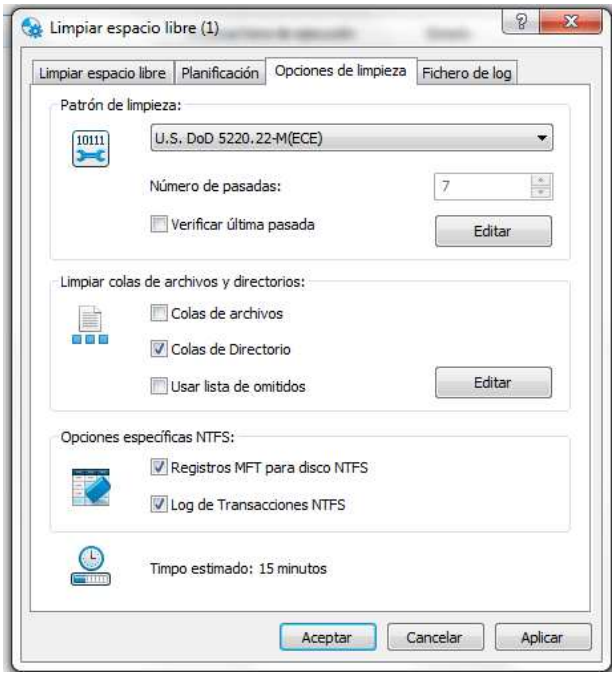


Figura 64. Imagen ejemplo funcionamiento programa BCWipe.

En esta solapa, principalmente se realiza la selección del algoritmo de limpieza a utilizar. En la ***figura 65*** se puede observar la lista de los algoritmos que BCWipe [23] ofrece, en este caso se selecciona el algoritmo “One random pass”.

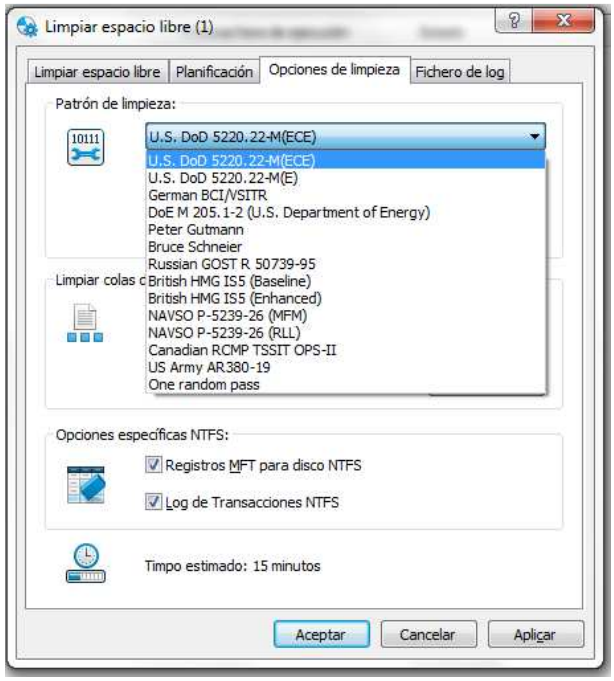


Figura 65. Imagen ejemplo funcionamiento programa BCWipe.

Una vez seleccionado el algoritmo, como se muestra en la ***figura 66***, se procede a pasar a la siguiente solapa la cual se denomina “fichero de log”.

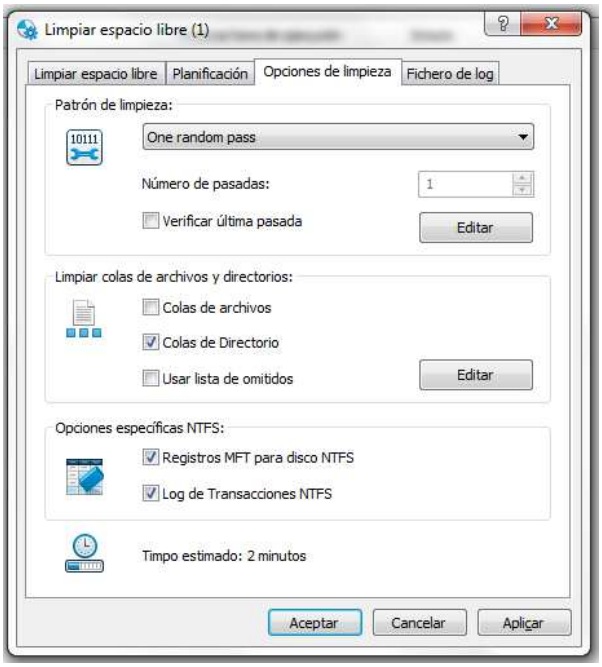


Figura 66. Imagen ejemplo funcionamiento programa BCWipe.

Esta solapa es opcional, en la misma se configura la opción de generación de un log, como se muestra en la ***figura 67***. El log es un archivo, en este caso un “.log”, donde se especifica lo que el programa realizo durante la higienización de los datos.

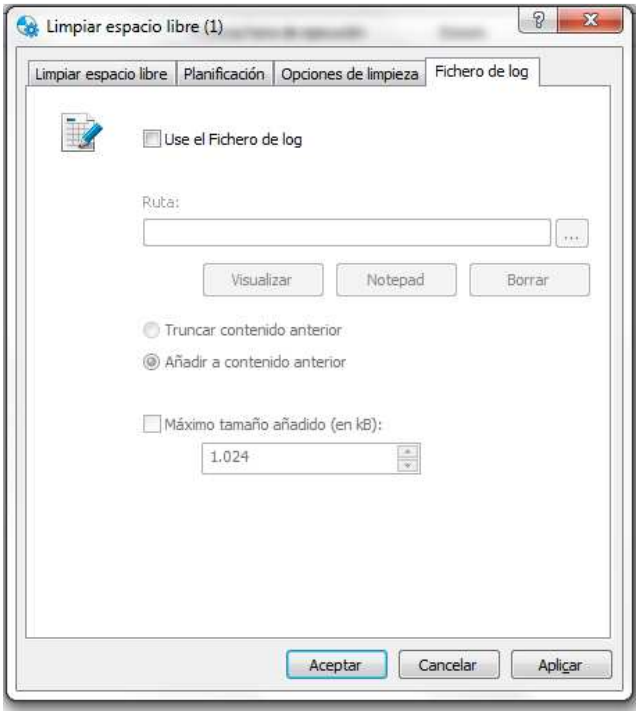


Figura 67. Imagen ejemplo funcionamiento programa BCWipe.

Al seleccionar el check box “Use el fichero de log”, se debe especificar la ruta en donde se encuentra el archivo “.log” en el cual se guardar la información, como se muestra en la ***figura 68***.

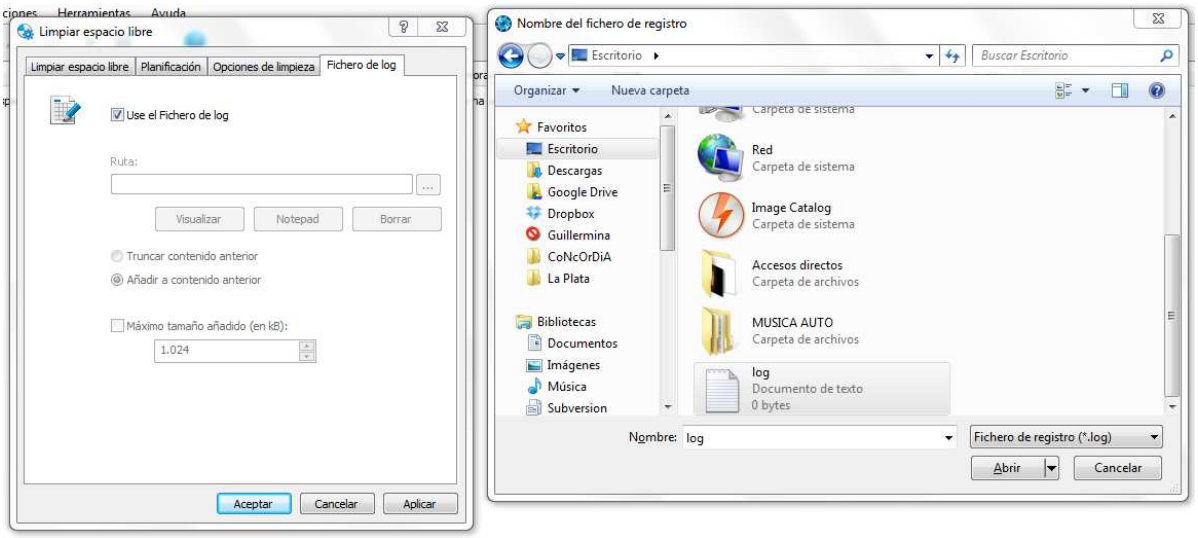


Figura 68. Imagen ejemplo funcionamiento programa BCWipe.

Una vez seleccionado el archivo y especificada la ruta se debe configurar si el nuevo contenido debe ser añadido a la información que ya existe en el mismo, en este caso se debe seleccionar la opción “Añadir a contenido anterior”, o el contenido anterior del archivo debe ser eliminado y reemplazado por el nuevo contenido, en este caso se debe seleccionar la opción “Truncar contenido anterior”. Como se muestra en la ***figura 69***, se selecciona la opción de añadir al contenido anterior.

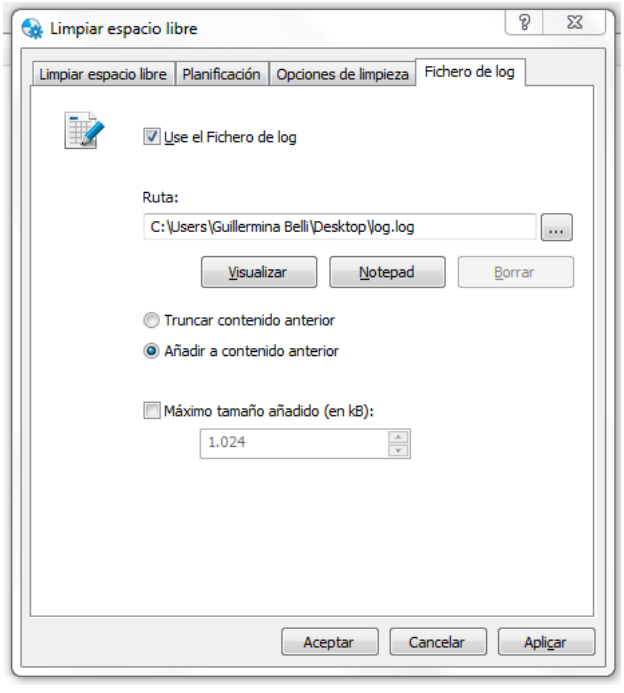


Figura 69. Imagen ejemplo funcionamiento programa BCWipe.

También se puede configurar el tamaño máximo, en KB, que se puede añadir al archivo ".log", en este caso no se lo especificada por lo tanto no tiene restricción alguna del tamaño que puede agregar al mismo.

Una vez configurado todo, se hace clic sobre el botón "aceptar" y se crea la tarea, como se muestra en la ***figura 70***.

Figura 70. Imagen ejemplo funcionamiento programa BCWipe.

Una vez creada la tarea se procede a iniciarla, ya que en este caso no la hemos programado para que comience en algún momento específico en la solapa de "Planificación" por lo que se debe iniciar manualmente. Como se muestra en la ***figura 71***, se realiza un clic derecho sobre la nueva tarea y se selecciona la opción "Iniciar la tarea seleccionada".

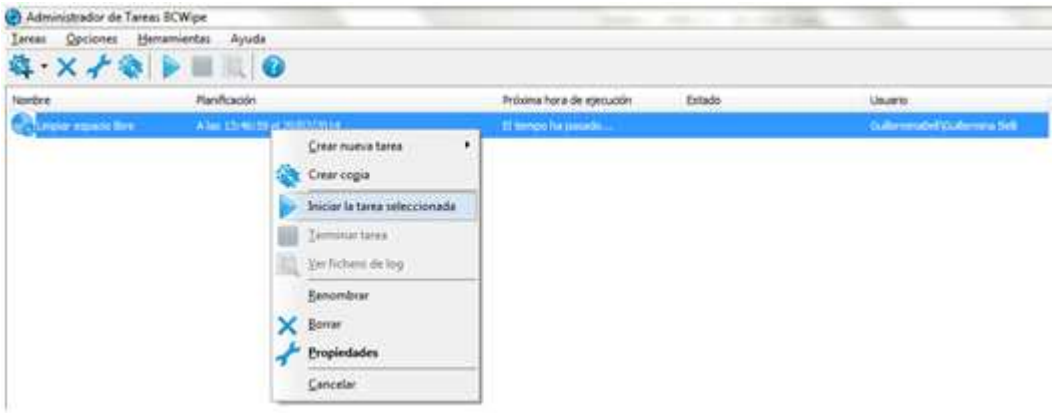


Figura 71. Imagen ejemplo funcionamiento programa BCWipe.

Una vez iniciada la tarea, como se muestra en la ***figura 72***, se puede observar que se mostrarán diferentes datos en las diferentes columnas, estos datos son:

- **Nombre de la tarea**, en este caso "Limpiar espacio libre".
- **Planificación**, como no se especifico ninguna en un principio se lista el horario y la fecha en la que fue creada y luego, una vez iniciada, se lista el horario y la fecha en la que fue iniciada.
- **Próxima hora de ejecución**, en la planificación de puede especificar que una tarea se ejecute varias veces y/o en diferentes días por lo tanto en esta columna se especificaría cual sería la próxima fecha y hora que se ejecutará la

tarea. Como en nuestro ejemplo no se configuró la planificación sólo especificará “El tiempo ha pasado…”.

- **Estado,** en esta columna se especifica, en porcentaje, el espacio borrado del total.
- **Usuario,** se especifica el usuario que creó la tarea.

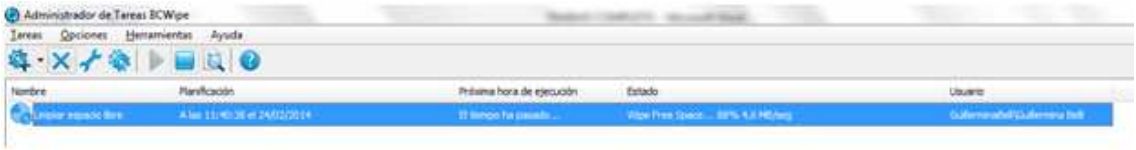
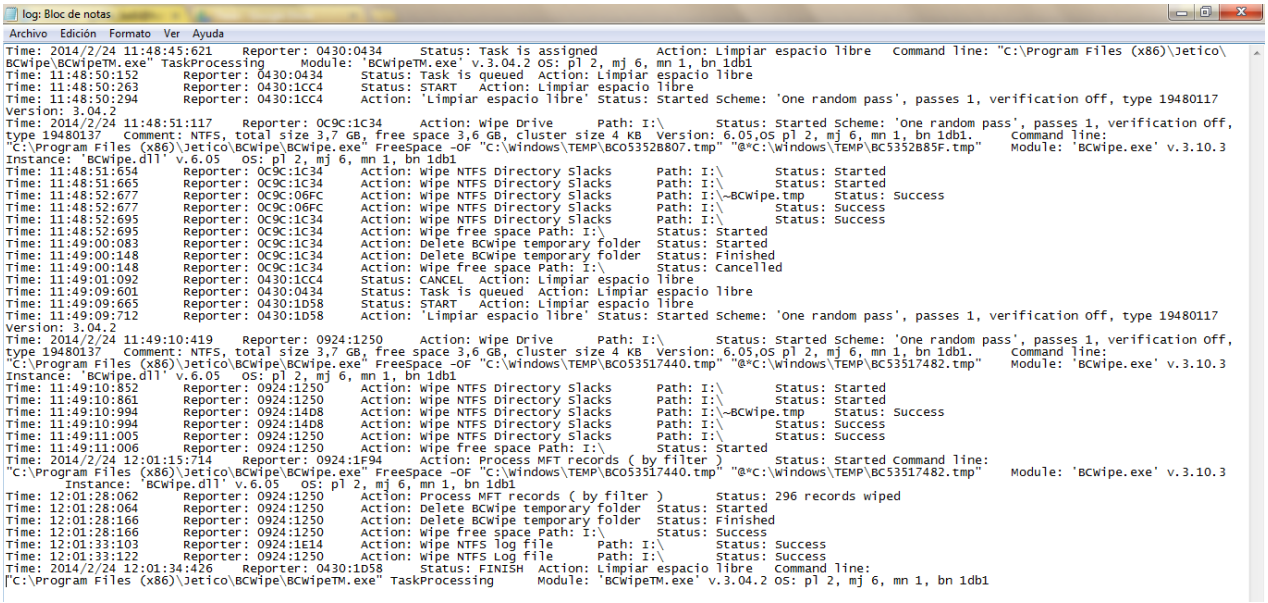


Figura 72. Imagen ejemplo funcionamiento programa BCWipe.

Al finalizar la tarea, como se muestra en la ***figura 73***, en la columna del estado se especificara el horario en el que la misma finalizo.

Figura 73. Imagen ejemplo funcionamiento programa BCWipe.

Como se muestra en la ***figura 74***, el archivo .log ha sido rellenado con la información correspondiente de la higienización.


log: Bloc de notas

Archivo Edición Formato Ver Ayuda

```
Time: 2014/2/24 11:48:45:621    Reporter: 0430:0434     Status: Task is assigned        Action: Limpiar espacio libre   Command line: "C:\Program Files (x86)\Jetico\
BCWipe\BCWipeTM.exe" TaskProcessing     Module: 'BCWipeTM.exe' v.3.04.2 OS: pl 2, mj 6, mn 1, bn 1db1
Time: 11:48:50:152      Reporter: 0430:0434     Status: Task is queued  Action: Limpiar espacio libre
Time: 11:48:50:263      Reporter: 0430:1CC4     Status: START   Action: Limpiar espacio libre
Time: 11:48:50:294      Reporter: 0430:1CC4     Action: 'Limpiar espacio libre' Status: Started Scheme: 'One random pass', passes 1, verification off, type 19480117
Version: 3.04.2
Time: 2014/2/24 11:48:51:117    Reporter: 0C9C:1C34     Action: Wipe Drive      Path: I:\       Status: Started Scheme: 'One random pass', passes 1, verification off,
type 19480137   Comment: NTFS, total size 3,7 GB, free space 3,6 GB, cluster size 4 KB  Version: 6.05,OS pl 2, mj 6, mn 1, bn 1db1.     Command line:
'C:\Program Files (x86)\Jetico\BCWipe\BCWipe.exe" FreeSpace -OF "C:\Windows\TEMP\BCO5352B807.tmp" "@*C:\Windows\TEMP\BC5352B85F.tmp"    Module: 'BCWipe.exe' v.3.10.3
Instance: 'BCWipe.dll' v.6.05   OS: pl 2, mj 6, mn 1, bn 1db1
Time: 11:48:51:654      Reporter: 0C9C:1C34     Action: Wipe NTFS Directory Slacks      Path: I:\       Status: Started
Time: 11:48:51:665      Reporter: 0C9C:1C34     Action: Wipe NTFS Directory Slacks      Path: I:\       Status: Started
Time: 11:48:52:677      Reporter: 0C9C:06FC     Action: Wipe NTFS Directory Slacks      Path: I:\~BCWipe.tmp    Status: Success
Time: 11:48:52:677      Reporter: 0C9C:06FC     Action: Wipe NTFS Directory Slacks      Path: I:\       Status: Success
Time: 11:48:52:695      Reporter: 0C9C:1C34     Action: Wipe NTFS Directory Slacks      Path: I:\       Status: Success
Time: 11:48:52:695      Reporter: 0C9C:1C34     Action: Wipe free space Path: I:\       Status: Started
Time: 11:49:00:083      Reporter: 0C9C:1C34     Action: Delete BCWipe temporary folder  Status: Started
Time: 11:49:00:148      Reporter: 0C9C:1C34     Action: Delete BCWipe temporary folder  Status: Finished
Time: 11:49:00:148      Reporter: 0C9C:1C34     Action: Wipe free space Path: I:\       Status: Cancelled
Time: 11:49:01:092      Reporter: 0430:1CC4     Status: CANCEL  Action: Limpiar espacio libre
Time: 11:49:09:601      Reporter: 0430:0434     Status: Task is queued  Action: Limpiar espacio libre
Time: 11:49:09:665      Reporter: 0430:1D58     Status: START   Action: Limpiar espacio libre
Time: 11:49:09:712      Reporter: 0430:1D58     Action: 'Limpiar espacio libre' Status: Started Scheme: 'One random pass', passes 1, verification off, type 19480117
Version: 3.04.2
Time: 2014/2/24 11:49:10:419    Reporter: 0924:1250     Action: Wipe Drive      Path: I:\       Status: Started Scheme: 'One random pass', passes 1, verification off,
type 19480137   Comment: NTFS, total size 3,7 GB, free space 3,6 GB, cluster size 4 KB  Version: 6.05,OS pl 2, mj 6, mn 1, bn 1db1.     Command line:
"C:\Program Files (x86)\Jetico\BCWipe\BCWipe.exe" FreeSpace -OF "C:\Windows\TEMP\BCO53517440.tmp" "@*C:\Windows\TEMP\BC53517482.tmp"    Module: 'BCWipe.exe' v.3.10.3
Instance: 'BCWipe.dll' v.6.05   OS: pl 2, mj 6, mn 1, bn 1db1
Time: 11:49:10:852      Reporter: 0924:1250     Action: Wipe NTFS Directory Slacks      Path: I:\       Status: Started
Time: 11:49:10:861      Reporter: 0924:1250     Action: Wipe NTFS Directory Slacks      Path: I:\       Status: Started
Time: 11:49:10:994      Reporter: 0924:14D8     Action: Wipe NTFS Directory Slacks      Path: I:\~BCWipe.tmp    Status: Success
Time: 11:49:10:994      Reporter: 0924:14D8     Action: Wipe NTFS Directory Slacks      Path: I:\       Status: Success
Time: 11:49:11:005      Reporter: 0924:1250     Action: Wipe NTFS Directory Slacks      Path: I:\       Status: Success
Time: 11:49:11:006      Reporter: 0924:1250     Action: Wipe free space Path: I:\       Status: Started
Time: 2014/2/24 12:01:15:714    Reporter: 0924:1F94     Action: Process MFT records ( by filter )       Status: Started Command line:
"C:\Program Files (x86)\Jetico\BCWipe\BCWipe.exe" FreeSpace -OF "C:\Windows\TEMP\BCO53517440.tmp" "@*C:\Windows\TEMP\BC53517482.tmp"    Module: 'BCWipe.exe' v.3.10.3
        Instance: 'BCWipe.dll' v.6.05   OS: pl 2, mj 6, mn 1, bn 1db1
Time: 12:01:28:062      Reporter: 0924:1250     Action: Process MFT records ( by filter )       Status: 296 records wiped
Time: 12:01:28:064      Reporter: 0924:1250     Action: Delete BCWipe temporary folder  Status: Started
Time: 12:01:28:166      Reporter: 0924:1250     Action: Delete BCWipe temporary folder  Status: Finished
Time: 12:01:28:166      Reporter: 0924:1250     Action: Wipe free space Path: I:\       Status: Success
Time: 12:01:33:103      Reporter: 0924:1E14     Action: Wipe NTFS log file      Path: I:\       Status: Success
Time: 12:01:33:122      Reporter: 0924:1250     Action: Wipe NTFS Log file      Path: I:\       Status: Success
Time: 2014/2/24 12:01:34:426    Reporter: 0430:1D58     Status: FINISH  Action: Limpiar espacio libre   Command line:
"C:\Program Files (x86)\Jetico\BCWipe\BCWipeTM.exe" TaskProcessing      Module: 'BCWipeTM.exe' v.3.04.2 OS: pl 2, mj 6, mn 1, bn 1db1
```

Figura 74. Imagen ejemplo del log completo creado por el programa BCWipe al borrar un pendrive Kingston de 4GB.

Disk Wipe.

Al iniciar el programa se selecciona el dispositivo a realizar la higienización. En este caso, como se muestra en la ***figura 75***, se selecciona una memoria USB:

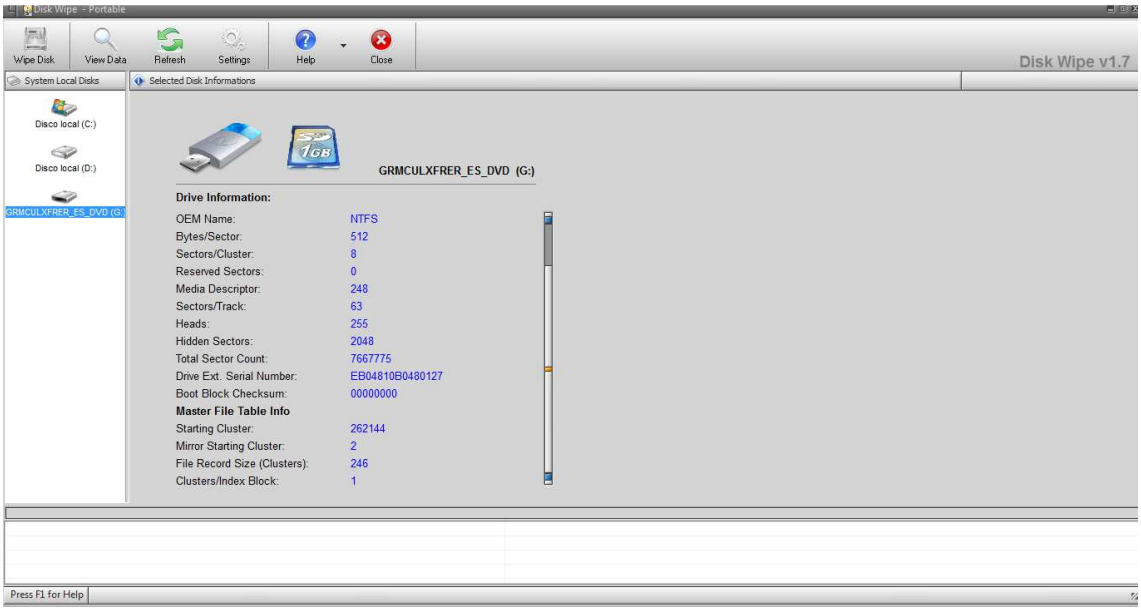


Figura 75. Imagen ejemplo funcionamiento programa Disk Wipe.

Luego, se oprime el botón “Wipe disk” (limpiar disco), el cual abre una nueva ventana donde se debe seleccionar el File System (Sistema de Archivos) y las opciones de formato, como se muestra en la ***figura 76***.

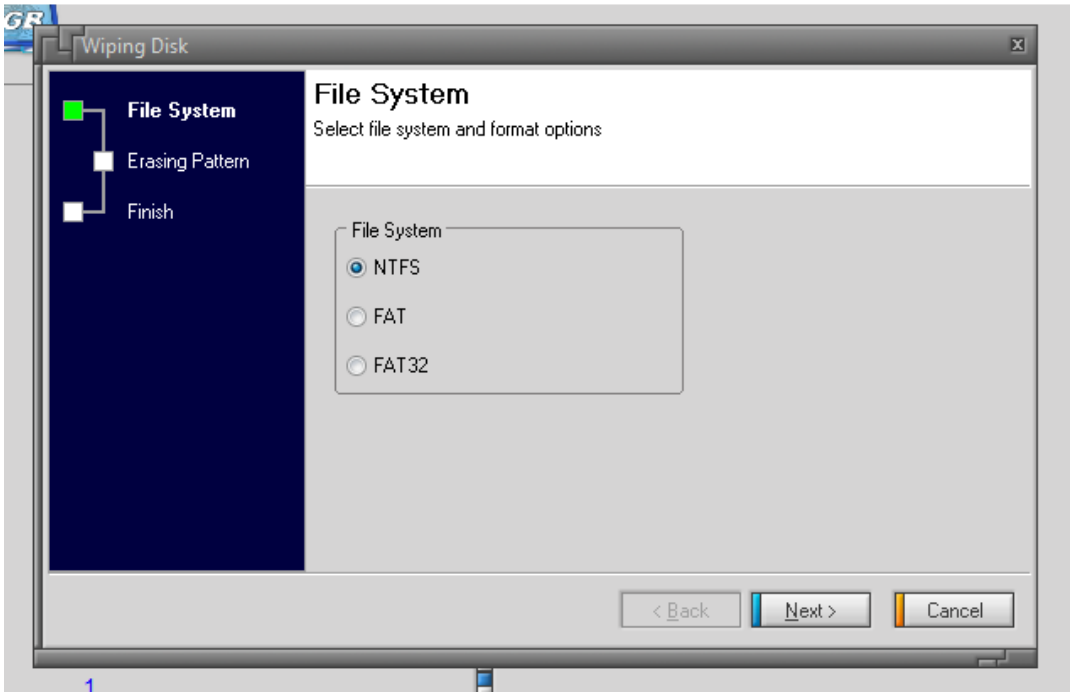


Figura 76. Imagen ejemplo funcionamiento programa Disk Wipe.

Una vez seleccionado se presiona el botón “Next” (siguiente). A continuación se pedirá seleccionar el algoritmo de higienización que se desea utilizar, como se muestra en la ***figura 77***.

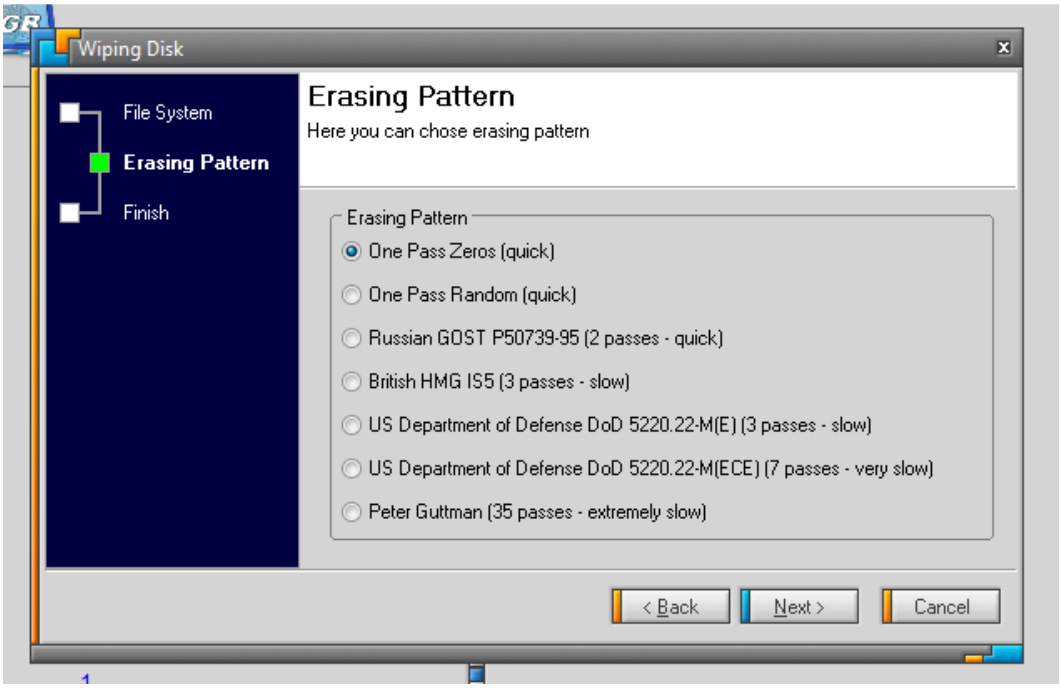


Figura 77. Imagen ejemplo funcionamiento programa Disk Wipe.

Una vez seleccionado se presiona el botón “Next” (siguiente). A continuación se debe confirmar la operación introduciendo un la palabra “ERASE ALL” (borrar todo) y presionar el botón “Next” (siguiente) como se muestra en la ***figura 78.***

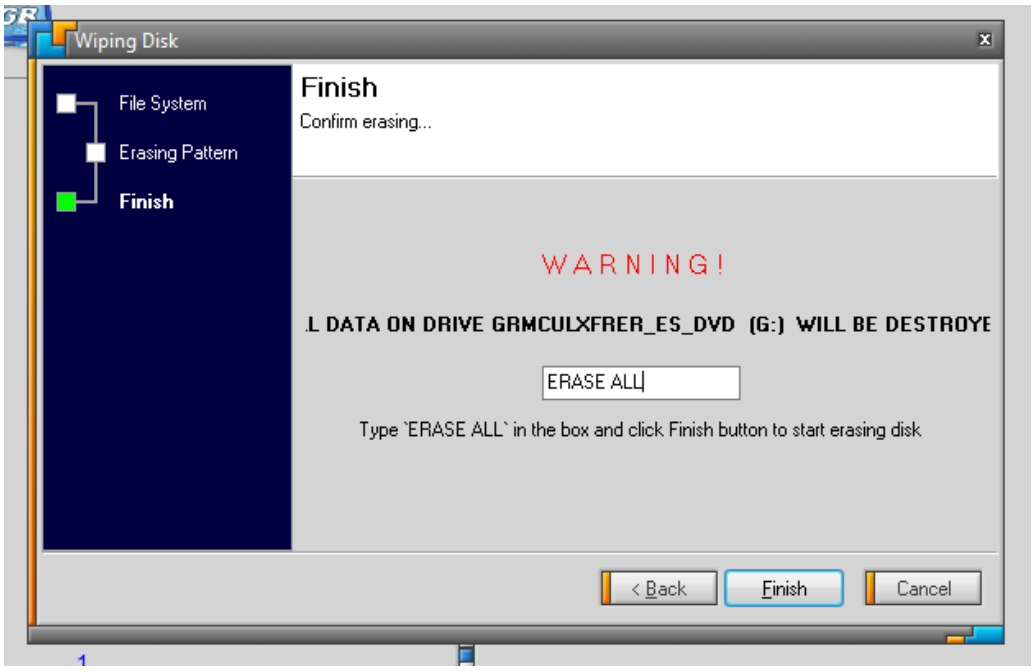


Figura 78. Imagen ejemplo funcionamiento programa Disk Wipe.

Se debe volver a confirmar la operación presionando el botón “Yes” (si) como se muestra en a ***figura 79***.

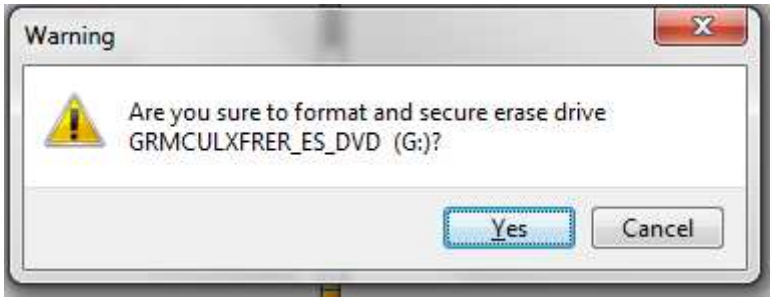


Figura 79. Imagen ejemplo funcionamiento programa Disk Wipe.

Una vez confirmado comenzará el proceso de borrado seguro, primero se prepara el formato que en este caso en NTFS como se muestra en la ***figura 80***.

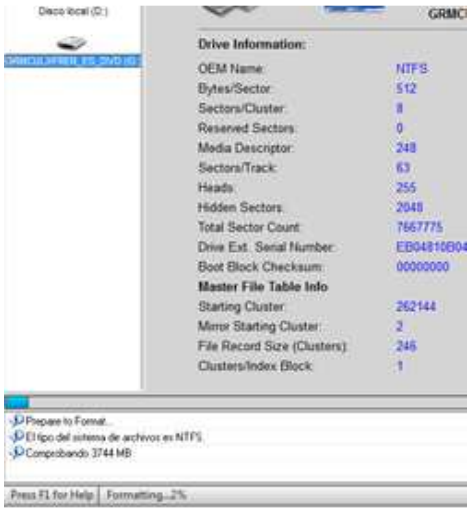


Figura 80. Imagen ejemplo funcionamiento programa Disk Wipe.

Una vez finalizado el proceso de dar formato a la memoria USB, comienza por último el proceso de borrado, como se muestra en la ***figura 81***.

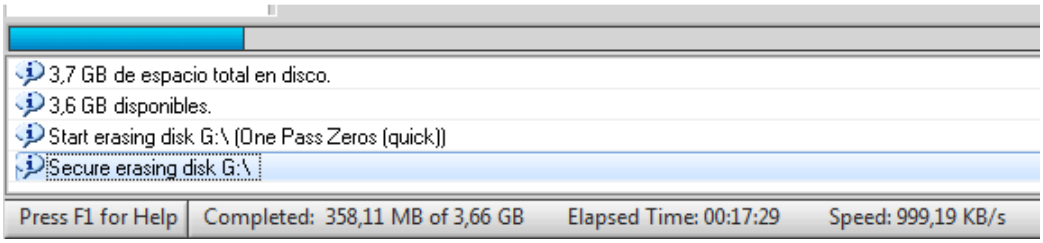


Figura 81. Imagen ejemplo funcionamiento programa Disk Wipe.

Una vez finalizado el proceso de higienización, como se muestra en la ***figura 82***, la memoria USB ha sido borrada por completo.

Figura 82. Imagen ejemplo funcionamiento programa Disk Wipe.

En la ***figura 83*** se muestra el proceso completo.

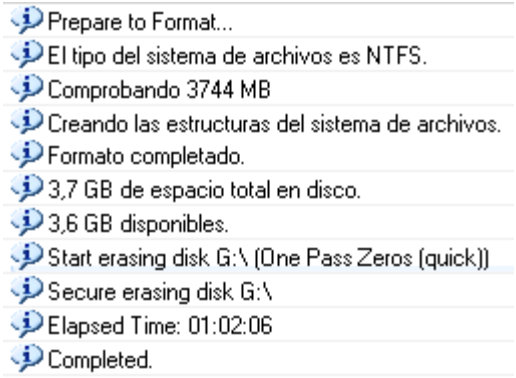


Figura 83. Imagen ejemplo funcionamiento programa Disk Wipe.

KillDisk.

Una vez iniciado el programa, si se tiene varios discos duros físicos conectados a la máquina, KillDisk [25] puede borrarlos simultáneamente. Los mismos se listan en la parte izquierda en "Local System Devices" (dispositivos del sistema local), como se muestra en la ***figura 84***.

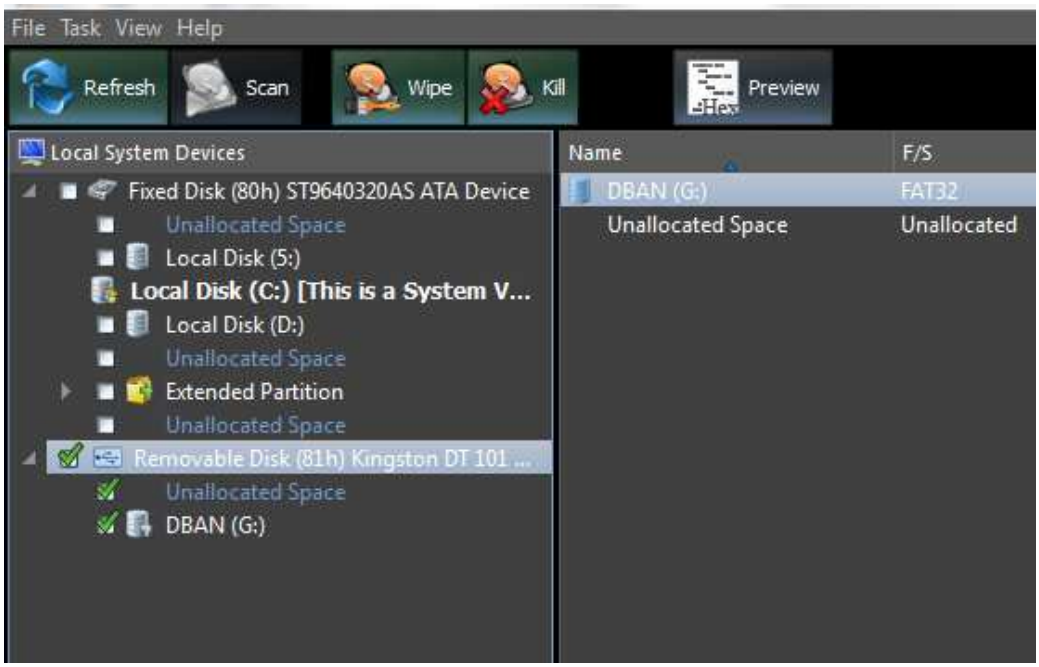


Figura 84. Imagen ejemplo funcionamiento programa KillDisk.

Al seleccionar un dispositivo, las propiedades correspondientes del mismo se listan en la parte derecha de la pantalla en “Properties” (propiedades), como se muestra en la ***figura 85***.

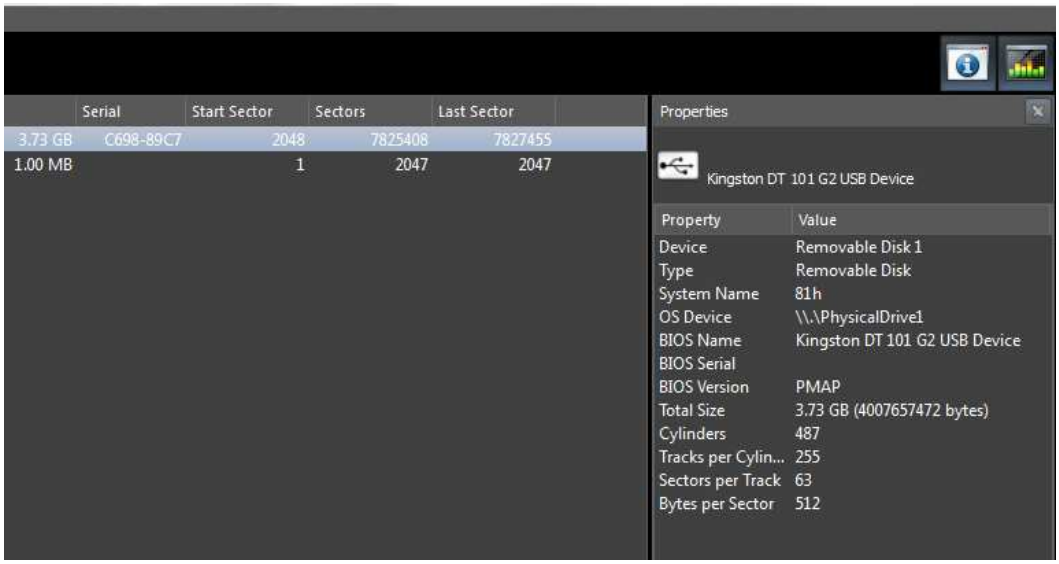


Figura 85. Imagen ejemplo funcionamiento programa KillDisk.

Una vez seleccionado el dispositivo a borrar, en este caso un pendrive Kingston como ya se mostro en la ***figura 85***, se debe presionar el botón “KILL” (matar) el cual abre una nueva ventana, como se muestra en la ***figura 86***, en la misma se debe seleccionar el algoritmo de borrado. También se pueden seleccionar diferentes opciones:

- ✓ Inicializar el disco después de borrar.
- ✓ Omitir la confirmación del borrador del disco.
- ✓ Guardar log y apagar la PC después de finalizar el borrado.

Figura 86. Imagen ejemplo funcionamiento programa KillDisk.

También se pueden configurar más opciones seleccionando “more options” (más opciones). Al presionar esta opción se abre una nueva ventana con 4 solapas en las que se puede configurar lo siguiente:

1. Solapa “General” (general), como se muestra en la ***figura 87***, se pueden configurar las siguientes opciones:
    - Inicializar el disco después de borrar.
    - Guardar log y apagar la PC después de finalizar el borrado.
    - Guardar log y apagar la PC después de finalizar el borrado.
    - Ignorar los errores de escritura de disco (sectores defectuosos).
    - Limpiar el archivo log antes del inicio.
    - Incluir logo/técnico dentro del certificado.
    - Enviar notificación por e-mail.
    - Leer/escribir los reintentos (se selecciona un número).
    - Estilo de la aplicación: oscuro o claro.
    - Registro de eventos: mínimo o detallado.

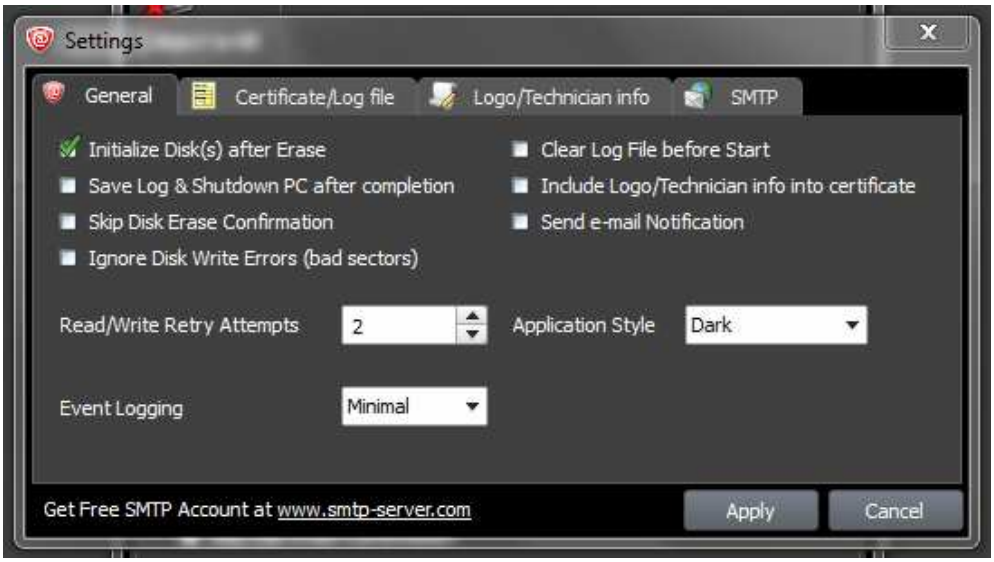


Figura 87. Imagen ejemplo funcionamiento programa KillDisk.

2. Solapa "Certificate/Log file" (Certificado/Archivo Log), como se muestra en la ***figura 88***, se pueden configurar las siguientes opciones:
    - Mostrar el certificado después de borrar/limpiar.
    - Guardar el certificado de borrado/limpieza en PDF.
    - Ruta donde se guardar el certificado.
    - Nombre del certificado.

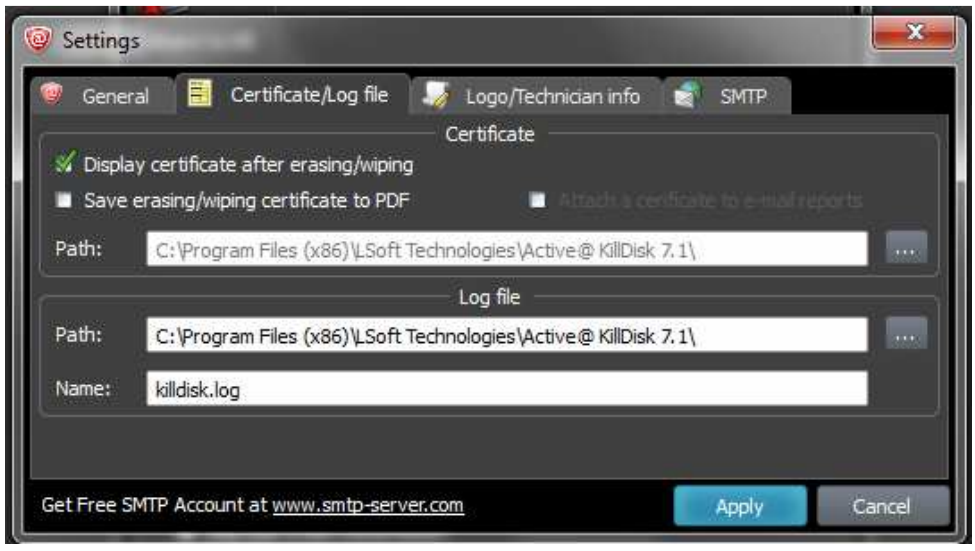


Figura 88. Imagen ejemplo funcionamiento programa KillDisk.

3. Solapa "Log/Technician info" (Información técnica del Log), como se muestra en la ***figura 89***, se pueden configurar las opciones que corresponden a la información de la compañía que realiza el borrado, el mismo será incluido en el certificado, estas son:
    - Foto de la compañía.
    - Nombre del Cliente.

- Nombre técnico.
- Nombre de la compañía.
- Dirección de la compañía.
- Teléfono de la compañía.
- Comentarios.

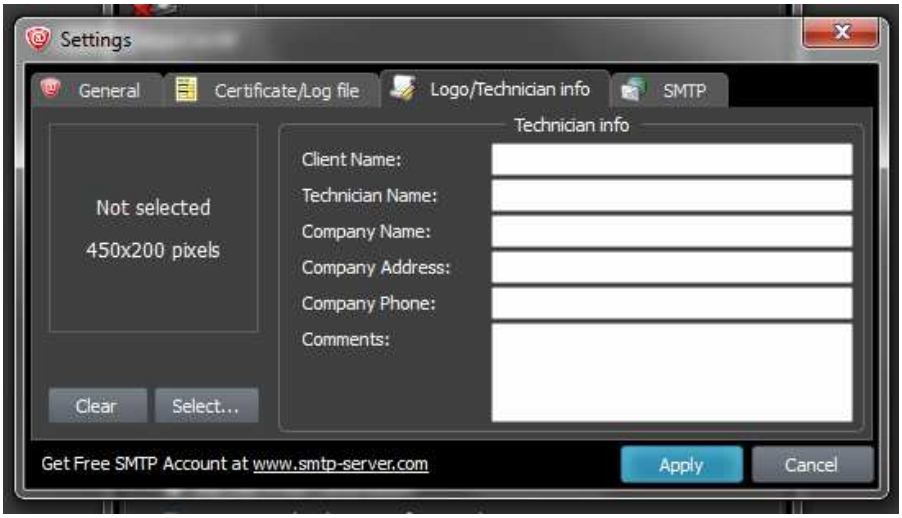


Figura 89. Imagen ejemplo funcionamiento programa KillDisk.

4. Solapa “SMTP” (Simple Mail Transfer Protocol - Protocolo para la transferencia simple de correo electrónico), como se muestra en la ***figura 90***, se pueden configurar las opciones para el envió de correo electrónico una vez finalizado el borrado, estas son:
    - Tipo de cuenta: cuenta gratuita o personalizada.
    - Para.
    - De.
    - Servidor SMTP.
    - Puerto SMTP.
    - Usuario y contraseña para el servidor SMTP, ya configurados.

Figura 90. Imagen ejemplo funcionamiento programa KillDisk.

Luego de configurar todo se hace clic sobre el botón “Apply” (aplicar) para guardar los cambios.

Para inicializar el borrado se debe presionar el botón “Start” (comenzar). Luego se debe confirmar el borrado ingresando “ERASE-ALL-DATA” (borrar todos los datos), como se muestra en la ***figura 91***.

Figura 91. Imagen ejemplo funcionamiento programa KillDisk.

A continuación comenzará la ejecución del algoritmo de borrado seleccionado previamente, como se muestra en la ***figura 92***.

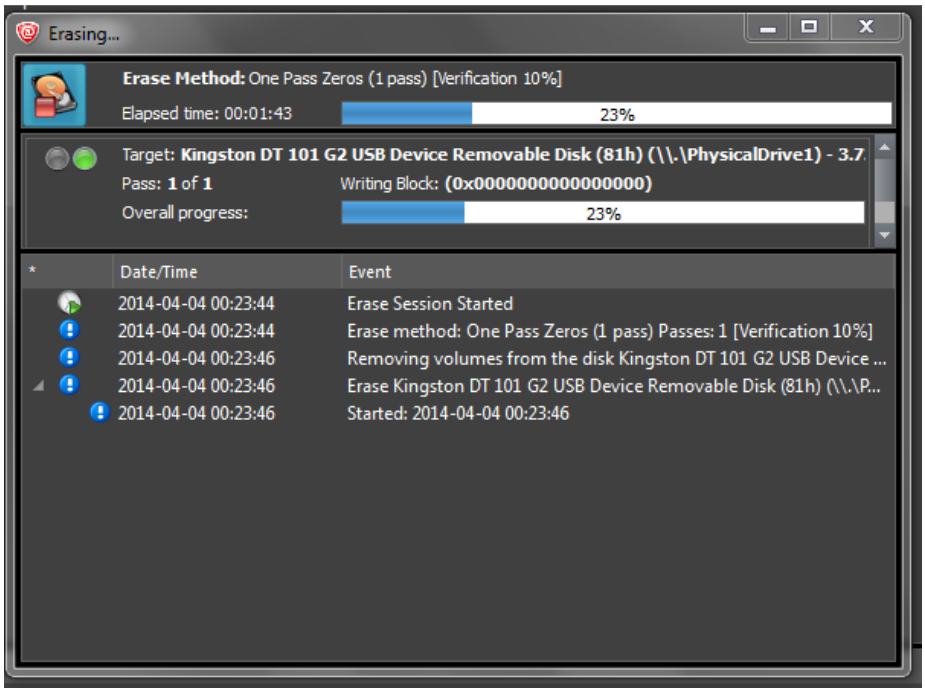


Figura 92. Imagen ejemplo funcionamiento programa KillDisk.

Una vez finalizado el proceso se abre el archivo log, en el formato configurado.

Darik's Boot and Nuke (DBAN).

Se debe iniciar el ordenador desde un disquete, una memoria USB o CD. Una vez inicializado el programa, se mostrará una pantalla azul, como se muestra en la ***figura 93***, en la cual se debe presionar la tecla ENTER.

Figura 93. Imagen ejemplo funcionamiento programa DBAN.

Una vez que termina el arranque, luego de un momento, aparecerá la siguiente pantalla, como se muestra en la ***figura 94***.

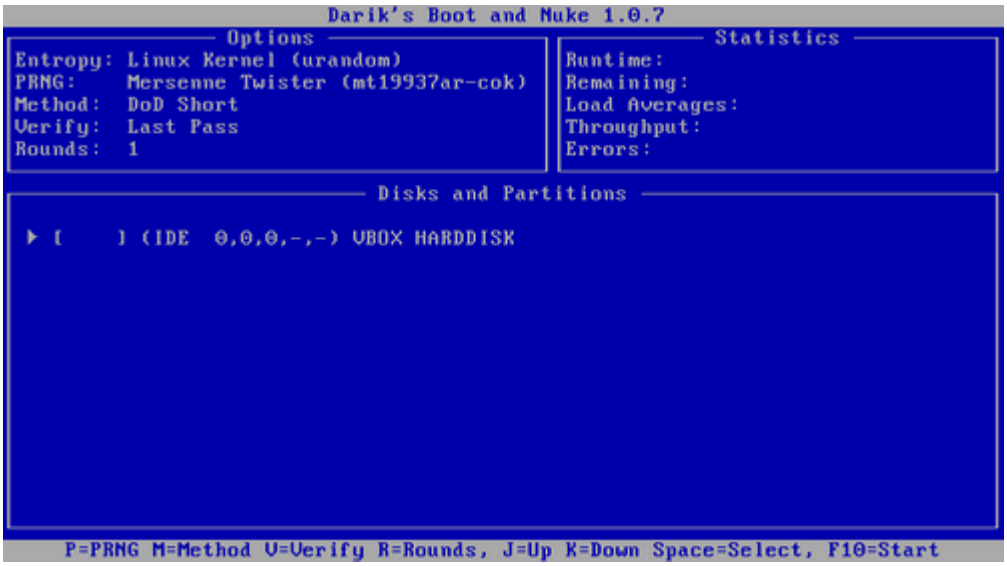


Figura 94. Imagen ejemplo funcionamiento programa DBAN.

Cuando aparece esta pantalla, ya se puede retirar el disquete/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 95***. 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 95. Imagen ejemplo funcionamiento programa DBAN.

Al presiona la tecla “R”, se pobra ingresar la opción del número de pasadas que se desea realizar, como se muestra en la ***figura 96***, luego se debe presiona la tecla ENTER.

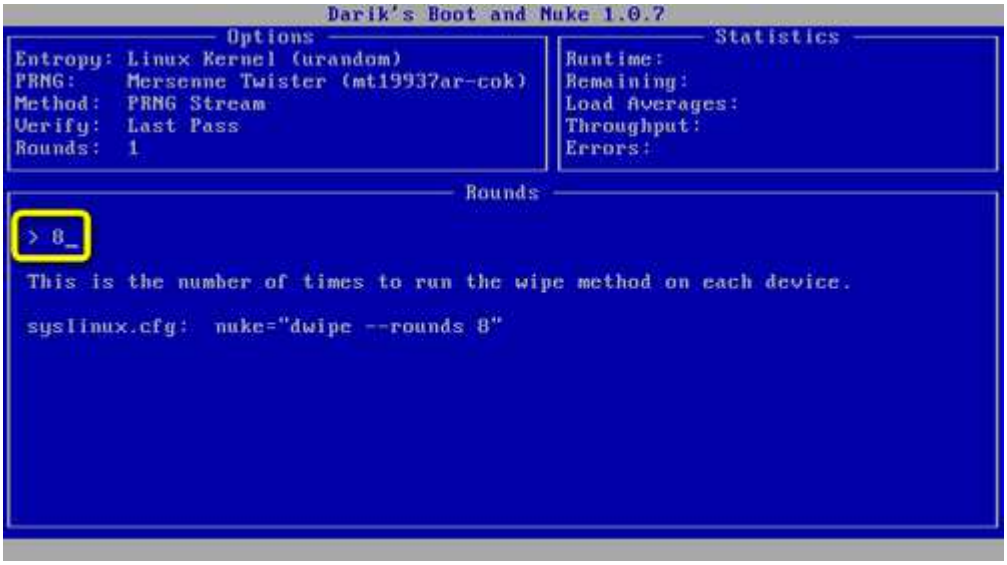


Figura 96. Imagen ejemplo funcionamiento programa DBAN.

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 97***:

Figura 97. Imagen ejemplo funcionamiento programa DBAN.

A continuación se presiona F10 para iniciar el borrado de datos y espera que termine la operación, como se muestra en la ***figura 98***.

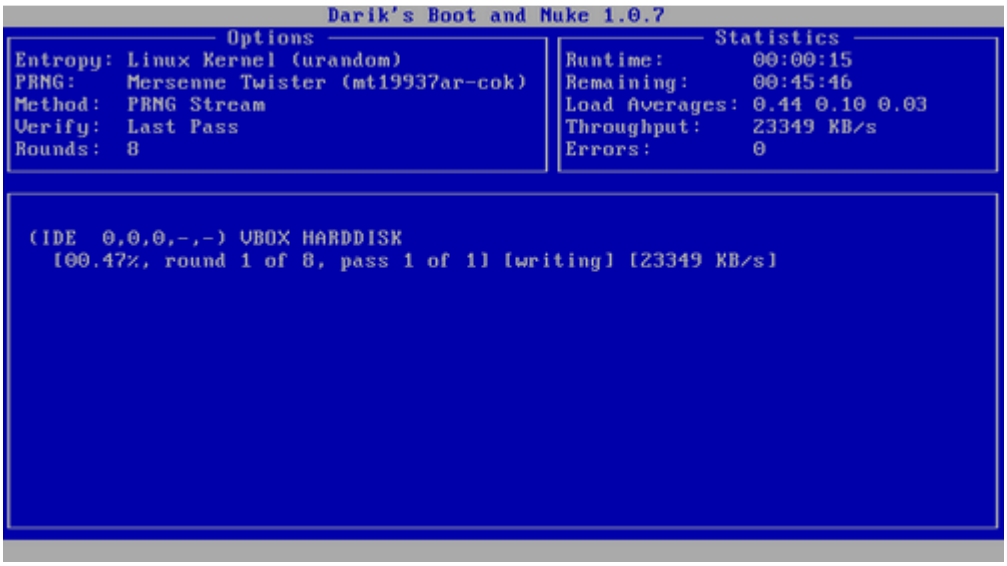


Figura 98. Imagen ejemplo funcionamiento programa DBAN.

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

Herramientas de Recuperación de los datos: ¿Cómo utilizarlas?

EasyRecovery.

El proceso de recuperación de la información de un disco específico consta de 5 pasos.

Al iniciar el programa correspondiente, se abrirá una ventana de presentación, como se muestra en la ***figura 99***.

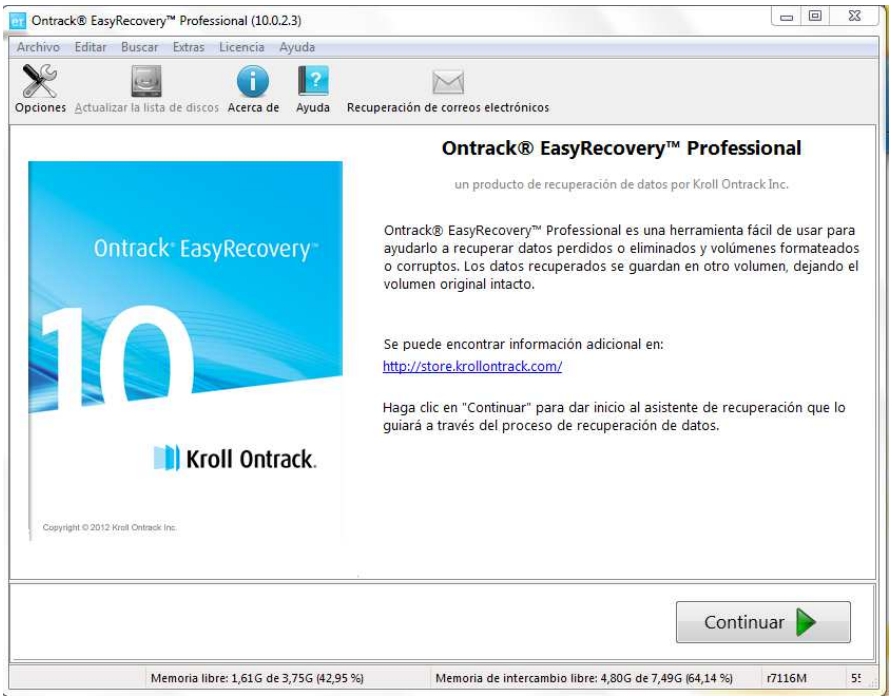


Figura 99. Imagen ejemplo funcionamiento programa EasyRecovery.

Al presionar el botón “Continuar”, se procederá a la configuración del primer paso.

El “paso 1”, como se muestra en la ***figura 100***, consiste en seleccionar el tipo de dispositivo de almacenamiento a analizar. Una vez seleccionado se oprime el botón “Continuar”.

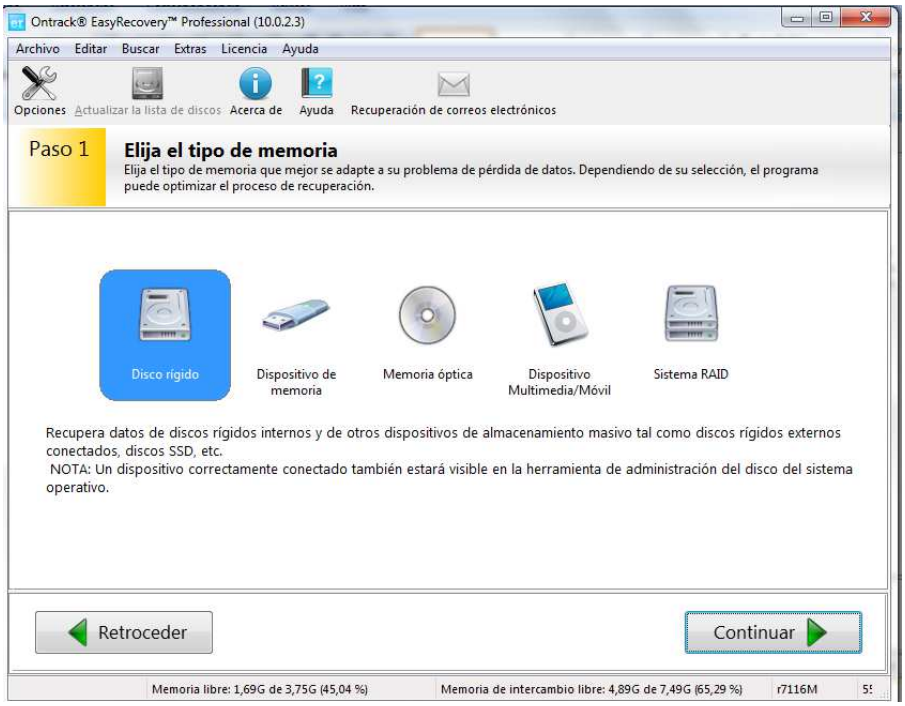


Figura 100. Imagen ejemplo funcionamiento programa EasyRecovery.

El "paso 2" consiste en seleccionar el volumen a analizar, como se muestra en la ***figura 101***. Una vez seleccionado el dispositivo correspondiente se debe presionar el botón "Continuar".

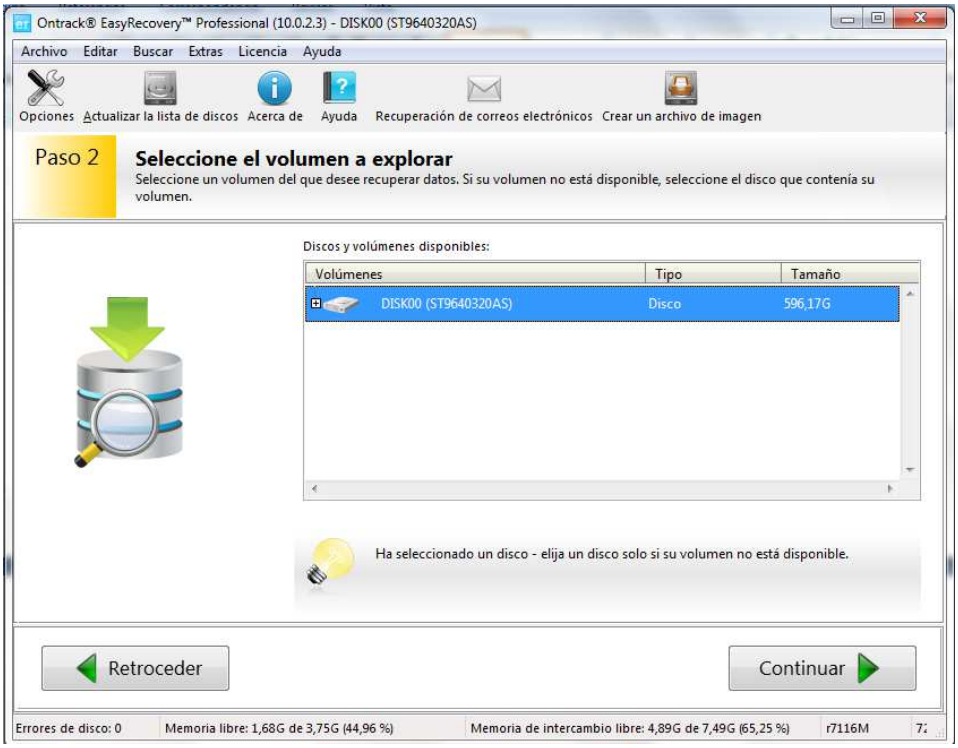


Figura 101. Imagen ejemplo funcionamiento programa EasyRecovery.

El “paso 3” consiste en seleccionar el tipo de recuperación que se desea realizar, como se muestra en las ***figuras 102 y 103***. Las opciones que ofrece la herramienta son:

- **Recuperación de un archivo (figura 102):** encontrar archivos eliminados de forma accidental o pérdida, por medio del contenido de los archivos. Asimismo, seleccione esta opción se elimino archivos de su papelera de reciclaje o si la recuperación formateada no puede encontrar sus archivos. De acuerdo a las opciones, se explorarán todos los bloques o solo los bloques no usados en un volumen.
- **Recuperación de memoria (figura 103)**: recupera datos de un volumen formateado. También se puede usar para recuperar archivos perdidos de un volumen no formateado. Esta opción toma más tiempo de exploración pero tiene mejores posibilidades de recuperación. Explora todos los bloques de un volumen para buscar estructuras de sistemas de archivos perdidos.
- **Buscar volúmenes**: explora un disco para buscar volúmenes perdidos o eliminados. Explora todos los bloques para buscar firmas de volúmenes perdidos. También puede encontrar volúmenes que no se montan.
- **Diagnóstico del disco**: muestra el disco/volumen como una imagen gráfica. Puede ejecutar un análisis de bloques para detectar bloques defectuosos, ver los distintos volúmenes de un disco u obtener los detalles sobre el uso de los bloques.
- **Herramientas del disco**: ofrece la posibilidad de generar y manipular imágenes del disco:
    - Creación y restauración de imágenes.
    - Copia, limpieza y vistas directas del disco.

Cabe destacar, que en el proceso de recuperación de datos que estudiamos, utilizamos solo dos tipos de procesos, los cuales son “Recuperación de un archivo” y “Recuperación de memoria”.

En cualquiera de las opciones se le puede especificar el tipo de sistema de archivos que contenía el disco para una mayor eficiencia, como se muestra en la ***figura 104***. En el caso de no conocer el sistema de archivos se pueden seleccionar todos. Se recomienda no tildar la “exploración rápida” ya que la busqueda no es tan eficiente aunque llevará menos tiempo.

Figura 102. Imagen ejemplo funcionamiento programa EasyRecovery.

Figura 103. Imagen ejemplo funcionamiento programa EasyRecovery.

Figura 104. Imagen ejemplo funcionamiento programa EasyRecovery.

Una vez seleccionado el tipo de recuperación correspondiente se debe presionar el botón “Continuar”.

El “paso 4” consiste en verificar que todas las opciones anteriormente seleccionadas sean las correctas, como se muestra en la ***figura 105***. Una vez verificadas todas las opciones se debe presionar el botón “Continuar”.

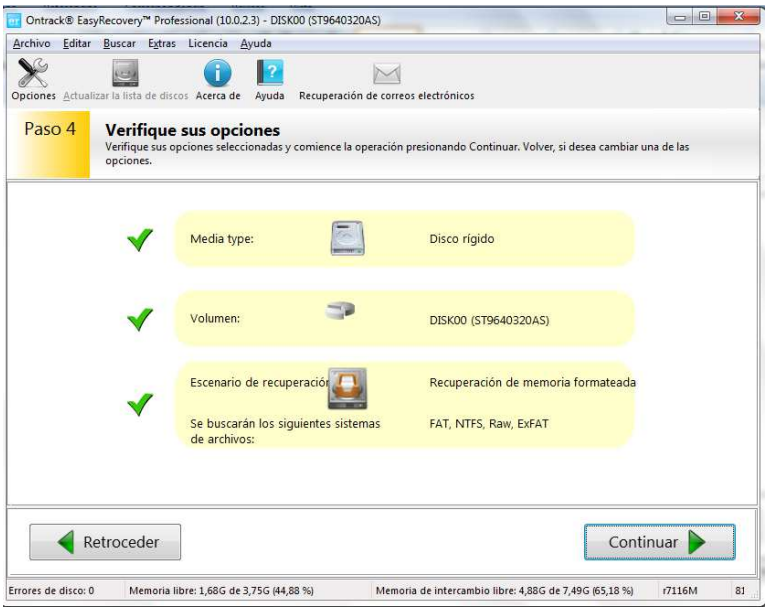


Figura 105. Imagen ejemplo funcionamiento programa EasyRecovery.

El “paso 5” consiste en la exploración y búsqueda de los archivos perdidos en el dispositivo, como se muestra en la ***figura 106***. Dependiendo del tipo de búsqueda seleccionada y el tamaño del dispositivo, es el tiempo que tarda en realizar la exploración.

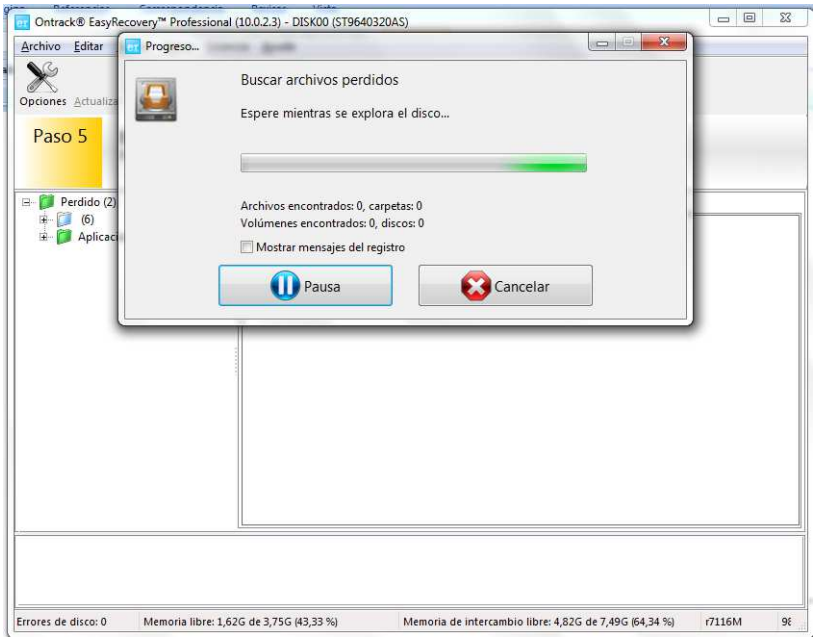


Figura 106. Imagen ejemplo funcionamiento programa EasyRecovery.

Una vez finalizada la exploración, se listarán:

- Los archivos encontrados, con sus correspondientes metadatos. Por ejemplo, como se muestra en la ***figura 107***.
- Una lista vacía, si no se ha encontrado ningún tipo de archivo. Por ejemplo, como se muestra en la ***figura 108***.

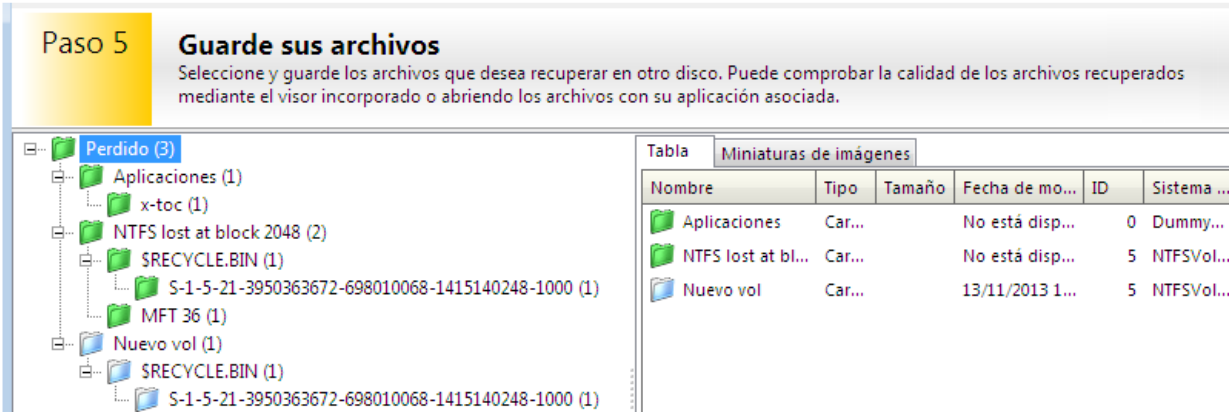


Figura 107. Imagen ejemplo funcionamiento programa EasyRecovery.

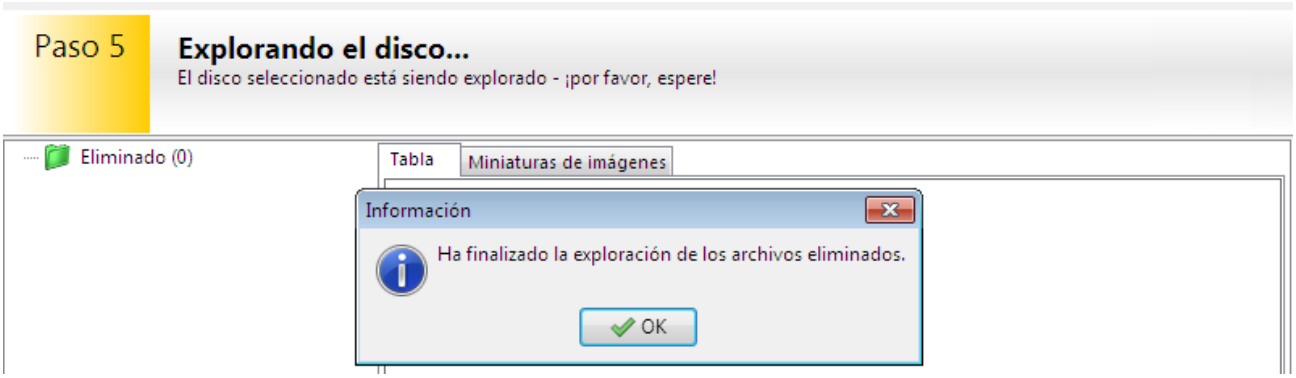


Figura 108. Imagen ejemplo funcionamiento programa EasyRecovery.

A continuación, se deben seleccionar los archivos que se desean recuperar y luego se debe presionar el botón “Guardar” donde se debe especificar la ruta en la que los archivos se almacenarán.

Recovery my files.

El proceso de recuperación de la información de un disco específico consta de 5 pasos.

Al iniciar el programa correspondiente, se abrirá una ventana de presentación, como se muestra en la ***figura 109***, donde se especifica el primer paso “¿Qué le gustaría hacer?”.

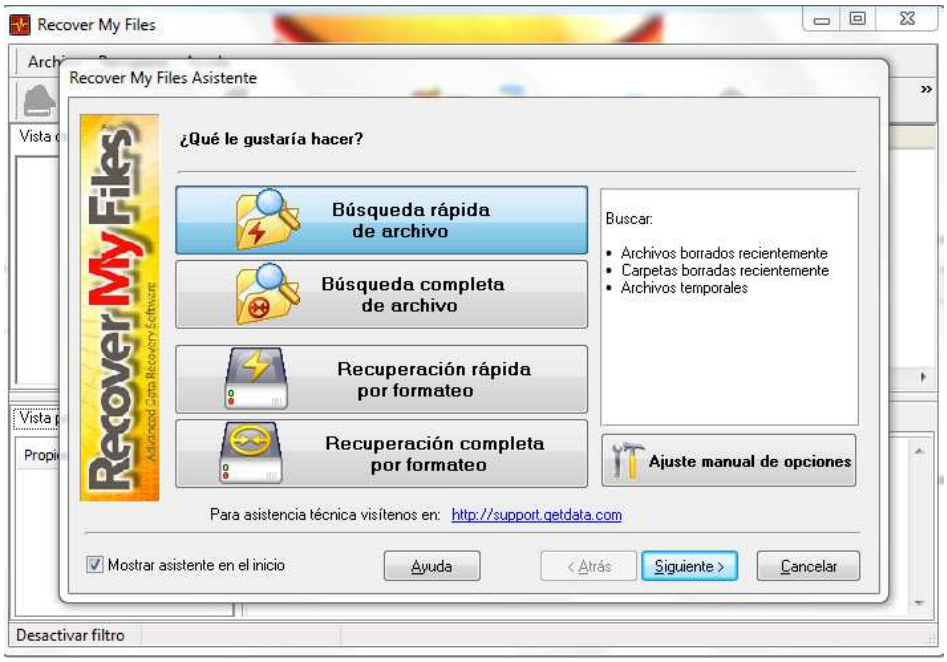


Figura 109. Imagen ejemplo funcionamiento programa Recovery My Files.

En este paso se debe seleccionar que tipo de recuperación se desea hacer. Las opciones que ofrece la herramienta son:

- **Búsqueda rápida de archivo**: en esta opción se buscan,
  - ✓ Archivos borrados recientemente.
  - ✓ Carpetas borradas recientemente.
  - ✓ Archivos temporales.
- **Búsqueda completa de archivo**: la búsqueda llevará más tiempo que una búsqueda rápida, pero sin embargo recuperara más archivos. En esta opción se buscan,
  - ✓ Archivos borrados recientemente.
  - ✓ Carpetas borradas recientemente.
  - ✓ Archivos temporales.
  - ✓ Búsqueda completa a nivel de cluster (sectores) de disco duro (archivos perdidos).
- **Recuperación rápida por formateo**: busca archivos en una partición que ha sido accidentalmente formateada. Realiza una búsqueda rápida de particiones existentes.
- **Recuperación completa por formateo**: busca archivos en una partición que ha sido accidentalmente formateada. Búsqueda en el disco duro a nivel de sector completo (archivos perdidos). Esta es una búsqueda larga, por lo tanto es la que conlleva más tiempo de ejecución.

Cabe destacar, que en el proceso de recuperación de datos que estudiamos, utilizamos solo dos tipos de procesos, los cuales son “Recuperación rápida por formateo” y “Recuperación completa por formateo”.

Una vez seleccionado el tipo de búsqueda a realizar, se presiona el botón “siguiente”.

En el siguiente paso se debe seleccionar las unidades y/o carpetas donde se realizara la búsqueda, como se muestra en la ***figura 110***. Una vez seleccionado el tipo de búsqueda a realizar, se presiona el botón “siguiente”.

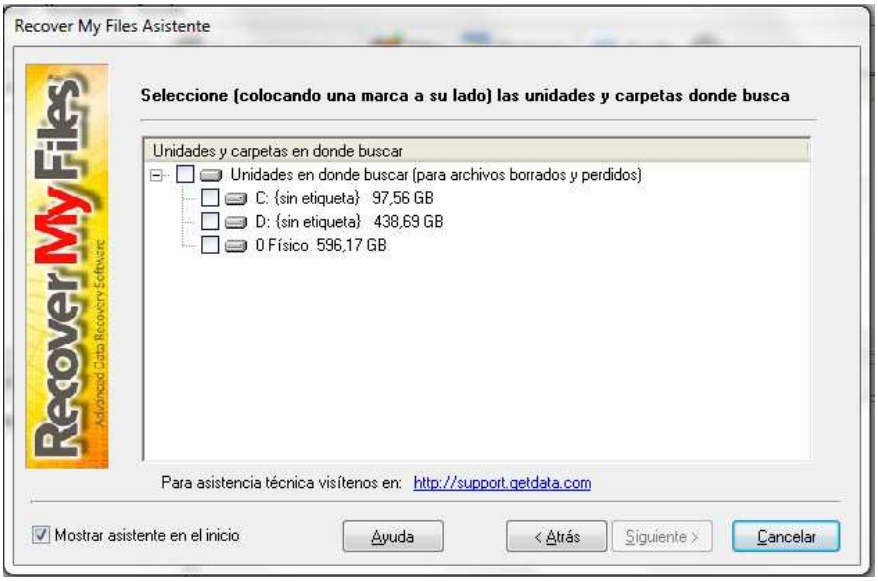


Figura 110. Imagen ejemplo funcionamiento programa Recovery My Files.

En el próximo paso “¿Qué tipo de archivo desea recuperar?”, como se muestra en la ***figura 111***, se debe seleccionar el/los tipo/os de archivos que se desean buscar.

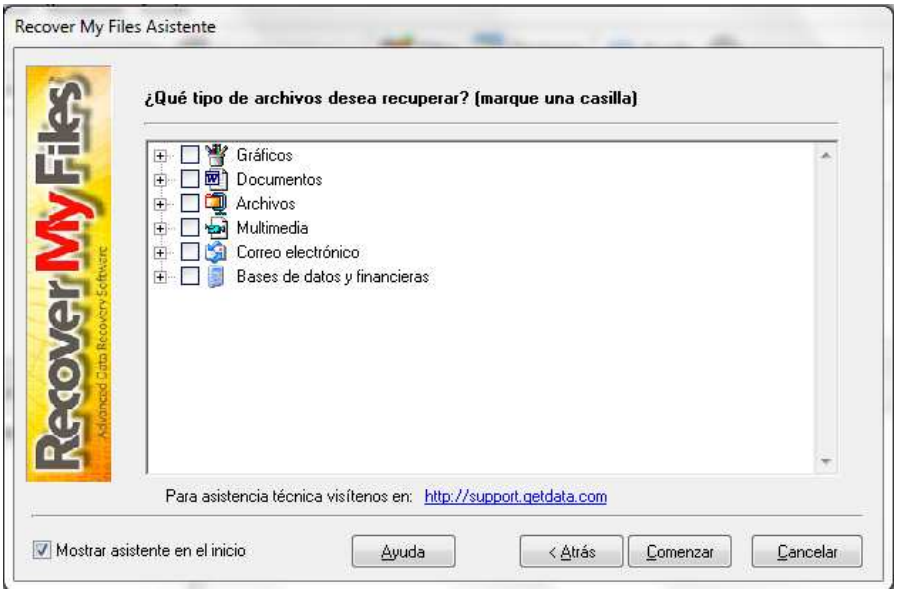


Figura 111. Imagen ejemplo funcionamiento programa Recovery My Files.

A continuación se listarán las capturas, ***figura 112, 113, 114, 115, 116 y 117***, con los detalles de las diferentes opciones que se pueden seleccionar:

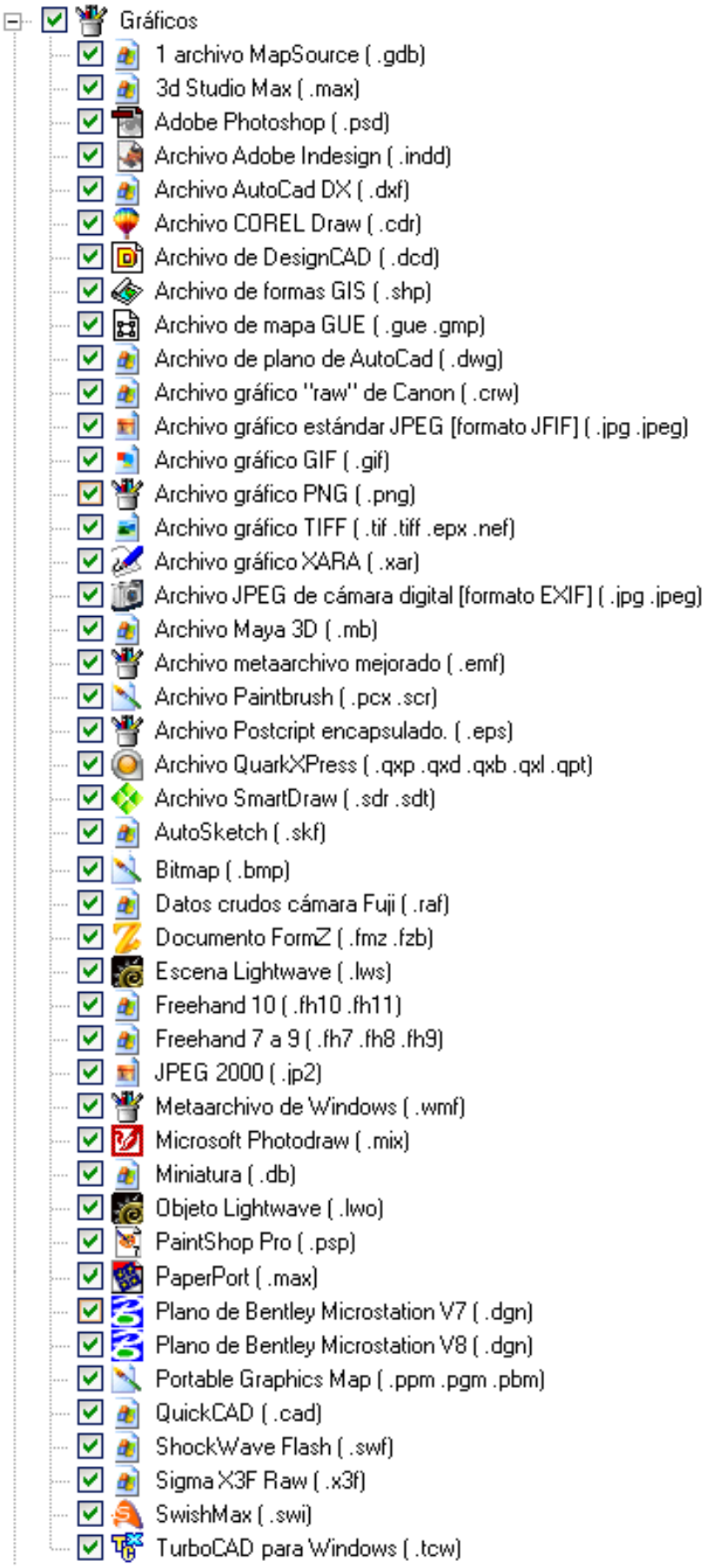


Figura 112. Imagen ejemplo funcionamiento programa Recovery My Files.

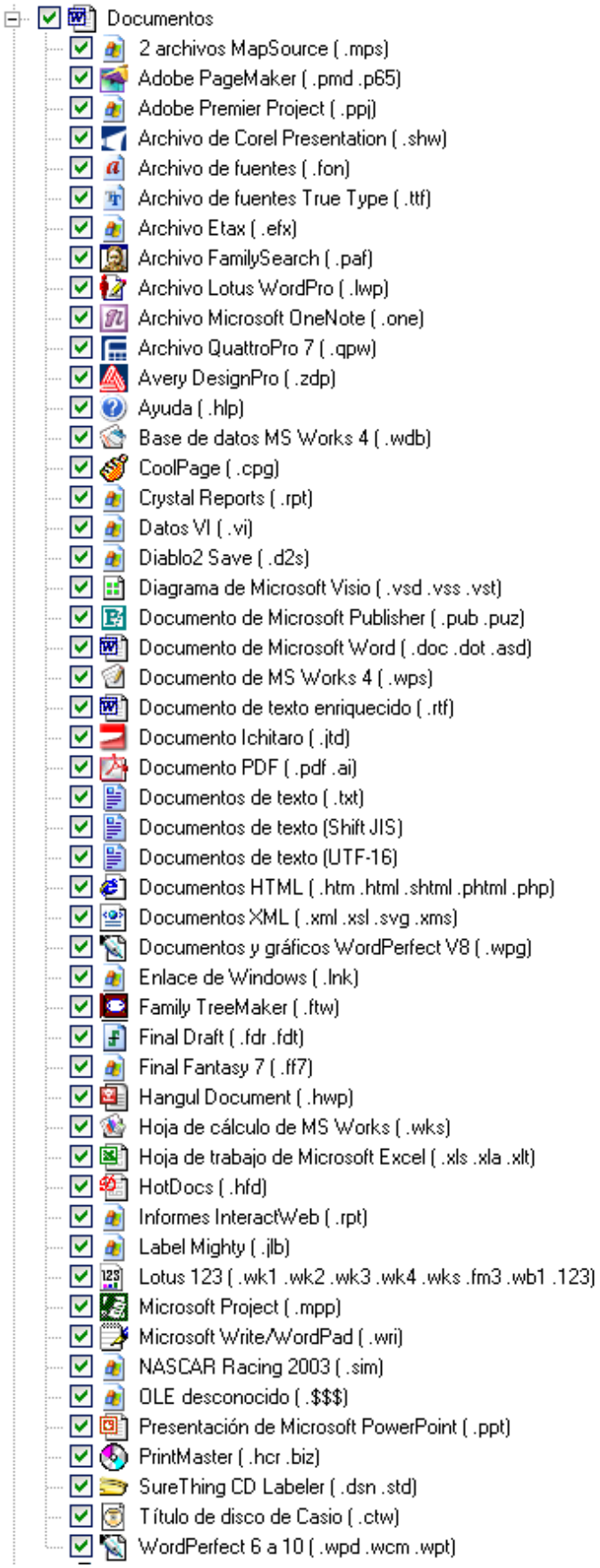


Figura 113. Imagen ejemplo funcionamiento programa Recovery My Files.

Figura 114. Imagen ejemplo funcionamiento programa Recovery My Files.

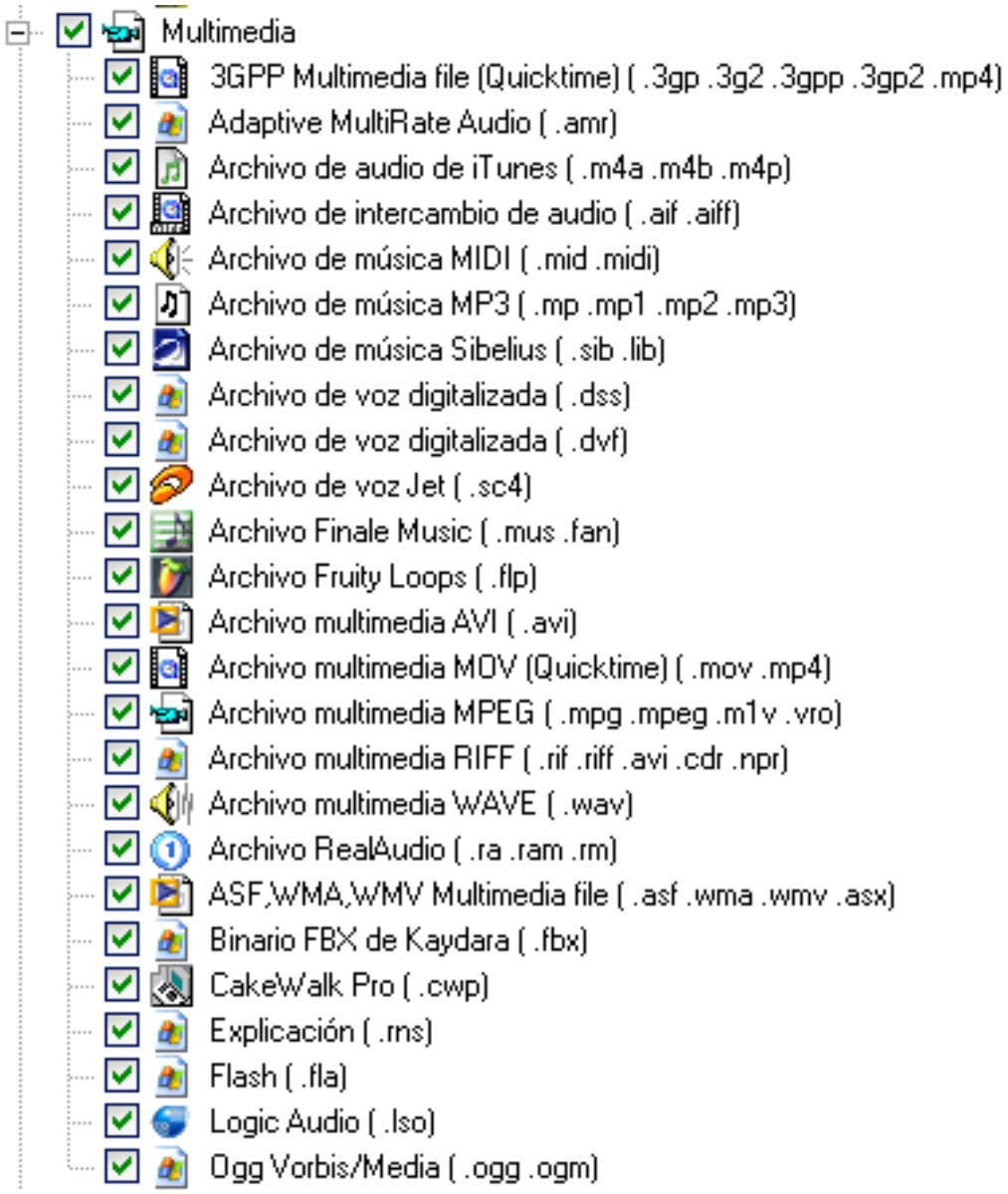


Figura 115. Imagen ejemplo funcionamiento programa Recovery My Files.

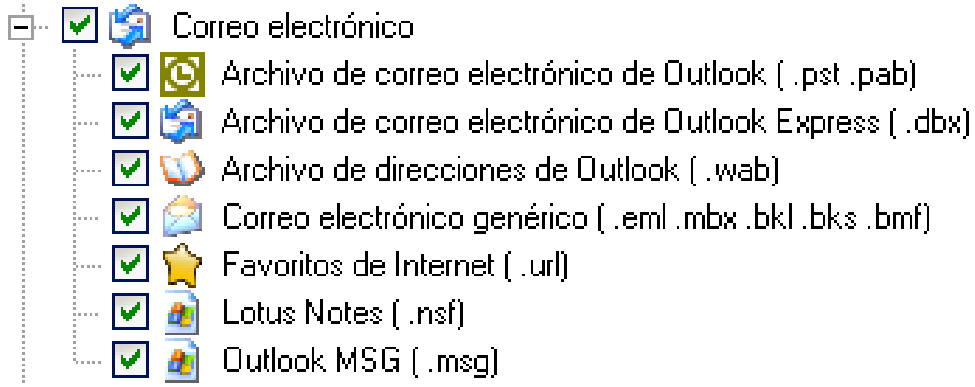


Figura 116. Imagen ejemplo funcionamiento programa Recovery My Files.

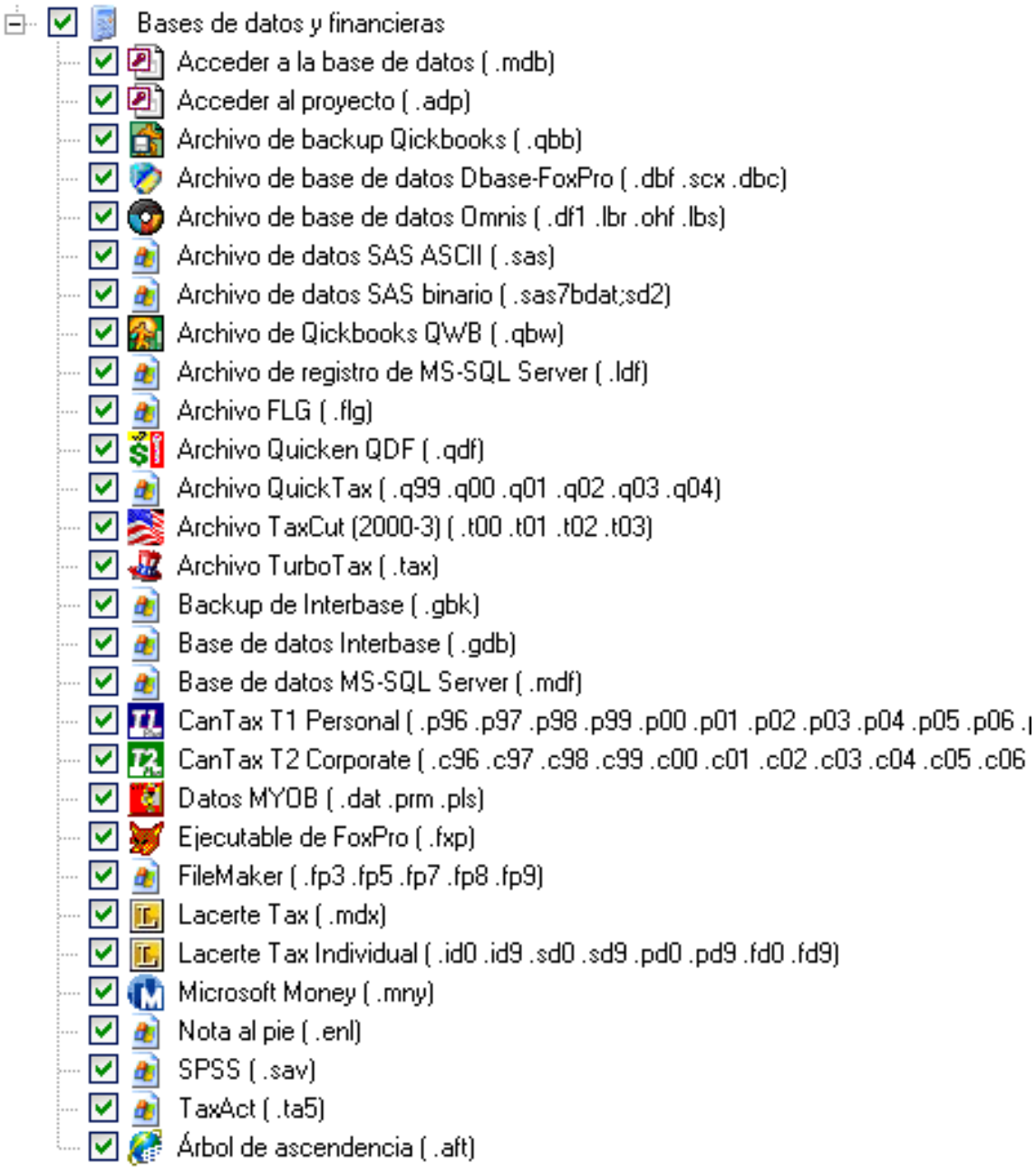
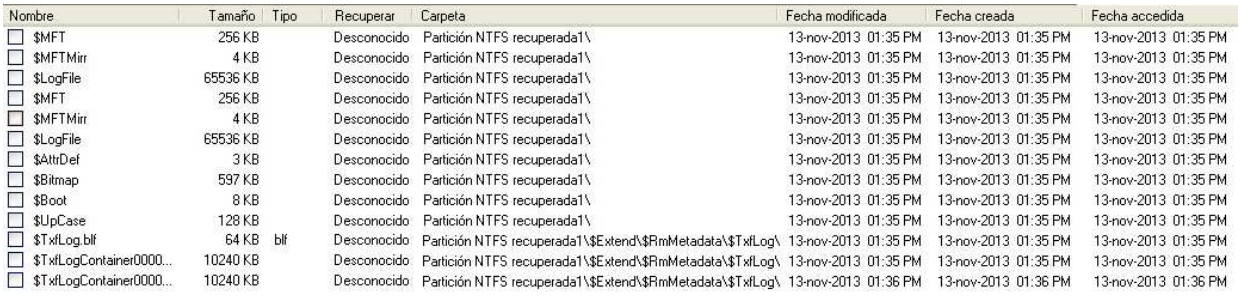


Figura 117. Imagen ejemplo funcionamiento programa Recovery My Files.

Una vez seleccionado el tipo de búsqueda a realizar, se presiona el botón “siguiente” y comenzará el proceso de búsqueda.

Cuando la búsqueda finalice, se listarán los archivos encontrados con sus correspondientes metadatos, como se muestra en la ***figura 118.***



Nombre	Tamaño	Tipo	Recuperar	Carpeta	Fecha modificada	Fecha creada	Fecha accedida
$MFT	256 KB		Desconocido	Partición NTFS recuperada1\	13-nov-2013 01:35 PM	13-nov-2013 01:35 PM	13-nov-2013 01:35 PM
$MFTMirr	4 KB		Desconocido	Partición NTFS recuperada1\	13-nov-2013 01:35 PM	13-nov-2013 01:35 PM	13-nov-2013 01:35 PM
$LogFile	65536 KB		Desconocido	Partición NTFS recuperada1\	13-nov-2013 01:35 PM	13-nov-2013 01:35 PM	13-nov-2013 01:35 PM
$MFT	256 KB		Desconocido	Partición NTFS recuperada1\	13-nov-2013 01:35 PM	13-nov-2013 01:35 PM	13-nov-2013 01:35 PM
$MFTMirr	4 KB		Desconocido	Partición NTFS recuperada1\	13-nov-2013 01:35 PM	13-nov-2013 01:35 PM	13-nov-2013 01:35 PM
$LogFile	65536 KB		Desconocido	Partición NTFS recuperada1\	13-nov-2013 01:35 PM	13-nov-2013 01:35 PM	13-nov-2013 01:35 PM
$AttrDef	3 KB		Desconocido	Partición NTFS recuperada1\	13-nov-2013 01:35 PM	13-nov-2013 01:35 PM	13-nov-2013 01:35 PM
$Bitmap	597 KB		Desconocido	Partición NTFS recuperada1\	13-nov-2013 01:35 PM	13-nov-2013 01:35 PM	13-nov-2013 01:35 PM
$Boot	8 KB		Desconocido	Partición NTFS recuperada1\	13-nov-2013 01:35 PM	13-nov-2013 01:35 PM	13-nov-2013 01:35 PM
$UpCase	128 KB		Desconocido	Partición NTFS recuperada1\	13-nov-2013 01:35 PM	13-nov-2013 01:35 PM	13-nov-2013 01:35 PM
$TxfLog.blf	64 KB	blf	Desconocido	Partición NTFS recuperada1\$Extend\$RmMetadata\$TxfLog\	13-nov-2013 01:35 PM	13-nov-2013 01:35 PM	13-nov-2013 01:35 PM
$TxfLogContainer0000...	10240 KB		Desconocido	Partición NTFS recuperada1\$Extend\$RmMetadata\$TxfLog\	13-nov-2013 01:35 PM	13-nov-2013 01:35 PM	13-nov-2013 01:35 PM
$TxfLogContainer0000...	10240 KB		Desconocido	Partición NTFS recuperada1\$Extend\$RmMetadata\$TxfLog\	13-nov-2013 01:36 PM	13-nov-2013 01:36 PM	13-nov-2013 01:36 PM

Figura 118. Imagen ejemplo funcionamiento programa Recovery My Files.

A continuación, se deben seleccionar los archivos que se desean recuperar y luego se debe presionar el botón “Guardar archivos” donde se debe especificar la ruta en la que los archivos se almacenarán.

Bibliografía.

- [1] Proyecto E-Basura http://e-basura.linti.unlp.edu.ar
- [2] Canal Encuentro - Basura Electrónica, Electrón Memories Joyería sustentable en Cambio Ambiental (http://www.youtube.com/watch?v=O2tYY1fU7hU)
- [3] www.lihuen.linti.unlp.edu.ar
- [4] Lineamientos Técnicos para el Manejo de Residuos de Aparatos Eléctricos y Electrónicos (AEE). Ministerio de Ambiente, Vivienda y Desarrollo Territorial República de Colombia.
- [5] H. Boeni, U. Silva, and D. Ott, E-Waste Recycling in Latin America: Overview, Challenges and Potential, in REWAS. 2008: Cancún.
- [6] Cámara Argentina de Máquinas de Oficina, Comerciales y Afines (CAMOCA). http://www.camoca.com.ar/
- [7] El Caso de Argentina. Reunión Internacional sobre RAEE en Latinoamérica "Hacia la Implementación de Políticas Regionales sobre RAEE en LAC 2013-2014", octubre de 2012. Alberto Santos CAPRA.
- [8] Minería y Basura Electrónica. El manejo irracional de los recursos, marzo 2012. GREENPEACE.
- [9] Proyecto de Ley RAEE - http://www.rezagos.com/descargas/Ley-RAEE-Filmus.pdf
- [10] Estudio sobre los circuitos formales e informales de gestión de Residuos de Aparatos Eléctricos y Electrónicos (RAEE) en Sudamérica. http://www.inti.gob.ar/basilea/pdf/Informe_raee_sudamerica.pdf
- [11] RESIDUOS PELIGROSOS Ley Nº 24.051 http://www.infoleg.gob.ar/infolegInternet/anexos/0-4999/450/texact.htm
- [12] Facultad de Informática http://info.unlp.edu.ar
- [13] Universidad Nacional de La Plata http://www.unlp.edu.ar
- [14] Laboratorio de Investigación en Nuevas Tecnologías Informáticas. http://linti.unlp.edu.ar
- **Empresas encargadas del reciclaje de los RAEE:**
  - ✓ [15] Scrap y Rezagos SRL (http://www.rezagos.com/)
  - ✓ [16] Silkers S.A. (http://www.silkers.com.ar/)
  - ✓ [17] Scrapex SRL (http://www.scrapex.com.ar/)
  - ✓ [18] Botrade SRL (http://www.botrade.es)
  - ✓ [19] Dalafer (http://www.dalafer.com.ar/).

- **Destrucción física, dispositivos disponibles en el mercado:**
  - ✓ [20] www.ontrackdatarecovery.es
  - ✓ [21] http://www.intimus.com
- **Herramientas de Higienización:**
  - ✓ [22] Eraser http://eraser.heidi.ie/
  - ✓ [23] BCWipe http://www.jetico.com/
  - ✓ [24] Disk Wipe http://www.diskwipe.org/
  - ✓ [25] KillDisk http://killdisk.com/
  - ✓ [26] Darik's Boot and Nuke (DBAN) http://www.dban.org/
- [27] GNU General Public License http://www.gnu.org/licenses/gpl.html
- [28] Revista Dconstrucción http://www.dconstruccion.cl/media/pdf/junio2012.pdf
- [29] CEMPRE (Compromiso EMpresarial Para el REciclaje) – Uruguay. http://cempre.org.uy/index.php?option=com_content&view=article&id=87&Itemid=105
- **Herramientas de recuperación:**
  - ✓ [30] Easy Recovery http://store.krollontrack.com/index.html?Langue=es_ES
  - ✓ [31] Recovery My Files http://www.recovermyfiles.com/es/
  - ✓ [32] Handy Recovery http://www.handyrecovery.es/
  - ✓ [33] Recuva http://www.piriform.com/recuva
- [34] Documentación sobre los parámetros y configuraciones de KillDisk. http://killdisk.com/notes.htm
- [35] Reciclaje y rehusó de computadoras como beneficio al medio ambiente. http://www.residuoselectronicos.net/archivos/panorama/pais/ve/docs/propuestadeproyecto.pdf
- The WEEE (RAEE) Man. http://www.weeeman.org/
- Eco RAEE. http://www.eco-raee.com/
- Gestor de Residuos. http://gerelux.com/
- Instituto Nacional de Tecnologías de la Comunicación. http://www.inteco.es/
- ***A Guide to Understanding Data Remanence in Automated Information System. National Computer Security Center.*** September 1991. Retrieved 2007-12-10. (***Rainbow Series*** "Forrest Green Book").

  "Una guía para entender la permanencia de datos en el Sistema Automatizado de Información. Centro Nacional de Seguridad Informática".
- ***Tutorial on Disk Drive Data Sanitization*** Gordon Gughes, UCSD Center for Magnetic Recording Research, Tom Coughlin, Coughlin Associates.

"Tutorial de higienización de datos en unidades de discos".

- ***Why Information Must Be Destroyed – Overview of paper-based destruction*** Ben Rothke, CISSP, British Telecom.

  "Porque la información debe ser destruida - Listado de destrucción en papel".

- ***Why Information Must Be Destroyed Part 2 – Overview of digita-based destruction*** Ben Rothke, CISSP, British Telecom.

  "Porque la información debe ser destruida Parte 2 - Listado de destrucción digital".

- UNIVERSIDAD NACIONAL DE LOMAS DE ZAMORA – FACULTAD DE INGENIERIA; 1998: ***"Curso de Gestión de Residuos Domiciliarios y Especiales"***, Argentina.
- ISWA – ARS; 1999: ***"Primera Jornada Internacional de Reciclado y Minimización de Residuos"***, Argentina.
- Greenpeace ***"Guide to Greener Electronics".*** December, 2006.
- ***"Secure Deletion of Data from Magnetic and Solid-State Memory"*** Peter Gutmann, Department of Computer Science University of Auckland. www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html
- ***"Los residuos electrónicos: Un desafío para la Sociedad del Conocimiento en América Latina y el Caribe, Unesco 2010"*** - Organización de las Naciones Unidas para la Educación, Ciencia y Cultura (UNESCO – United Nations Educational, Scientific and Cultural Organization). http://www.unesco.org/new/es/unesco/resources/publications/unesdoc-database/
- "Reutilización y sustitución de dispositivos de almacenamiento de datos y seguridad de la información", Observatorio de la Seguridad de la Información, INTECO. http://www.egov.ufsc.br/portal/sites/default/files/reutilizacion_y_sustitucion_de_dispositivos_de_almacenamiento_de_datos_y_seguridad_de_la_informacion.pdf