COMUNIDAD DE POLICÍAS DE AMÉRICA

AMERIPOL

Boletín Tecnológico

2

2012

Prólogo

Actualmente nuestros países se encuentran en un escenario de nuevas y variadas amenazas que afectan a los Estados y sus sociedades de forma diversa. Algunos de estos flagelos son de alcance global y multidimensional por lo que se requiere de una cooperación hemisférica para combatirlos. Entre las amenazas más destructivas se encuentran el crimen organizado y sus delitos conexos, entre otras que cada vez presentan rasgos más sofisticados, los cuales implican que la acción policial sea más especializada y con nuevos métodos tecnológicos.

La Comunidad de Policías de América (AMERIPOL) como mecanismo de cooperación orientado a prevenir, neutralizar y contrarrestar dichas amenazas pone a disposición de sus miembros y de la comunidad policial a nivel mundial herramientas operativas y de asistencia técnica como éste Boletín, como reconocimiento de que además de inteligencia, capacitación y voluntad política se requiere de colaboración e intercambio de tecnologías de punta existentes.

La creación de la División Científica dentro de la Policía Federal de México, como elemento clave de investigación, inteligencia y operación, es muestra de esa nueva visión y operación contra el crimen organizado a través de la adquisición de la tecnología más avanzada al servicio de los mexicanos y de la comunidad del hemisferio. Así como la selección y formación profesional de los integrantes de dicha División conformada por varias especialidades entre ingenierías, química, biología, informática, derecho entre otras. Cuenta con la tecnología necesaria para manejar evidencias electrónica, y atender los delitos que se efectúan con tecnologías informáticas.

Ejemplo de ello, es la creciente demanda de recuperación de datos e información contenida en discos duros con daños físicos, y los costos tan altos que esto representa. El presente Artículo tiene como finalidad presentar el procedimiento de la rehabilitación de un disco duro, en específico de la marca Western Digital, que presentaba daño físico y por tanto la información era inaccesible, mediante el uso de equipos informáticos y el detalle de la metodología de diagnóstico, rehabilitación y extracción de información.

Finalmente es importante resaltar que la Policía Federal de México con el objetivo de coadyuvar en el esfuerzo de todas las instituciones de seguridad pone a disposición de ellas y sus gobiernos las herramientas humanos y técnicas como apoyo al esfuerzo de la comunidad.

Maestra Maribel Cervantes Guerrero
Comisionada General de la Policía Federal de México y
Secretaria Ejecutiva de AMERIPOL

Rehabilitación de un disco duro,
Western digital que presenta daño electrónico

Data recovery,
Western digital hard disk drive with electronic damage

Reabilitação de um disco rígido,
Western digital que apresenta dano eletrônico

Investigación

Sumario

Autores del artículo

Fecha de recepción del artículo: 1º. de Junio 2012.

Gabriela Henríquez Campos

SSP Policía Federal, Maestra en Ingeniería (Computación), UNAM. ingghenriquez@gmail.com

Maricarmen Pérez García

SSP Policía Federal, Maestra en Ingeniería en Seguridad y Tecnologías de la Información, IPN. maricarmen.perez@ssp.gob.mx

Juan Carlos Hernández Rubio

SSP Policía Federal, Ingeniero en Comunicaciones y Electrónica, IPN. juan.hernandezr@ssp.gob.mx

Resumen y palabras claves (Español, Inglés y Portugués)

Resumen

En las instalaciones de la División Científica, en la Coordinación para la Prevención de Delitos Electrónicos y en particular en el área de la Dirección General de Laboratorios en Electrónica y Forense de la Policía Federal, se recibió un Disco Duro dañado, marca Western Digital, con la instrucción de recuperar la información contenida, la cual era crítica para el funcionamiento de otra área de la Policía Federal. Tras examinar el dispositivo, se determinó que el mal funcionamiento se debía a un daño en la tarjeta lógica debido a que varios de sus componentes se encontraban quemados, probablemente debido a un corto circuito. Para la rehabilitación del dispositivo se utilizó un Disco Duro donador, de características similares al disco dañado para poder así remplazar los componentes dañados de la tarjeta.

Palabras clave

Rehabilitación de Discos Duros, Recuperación de Información, Tarjeta Lógica Dañada, Remplazo de Componentes de Tarjeta Lógica, Disco Donador.

Abstract

At the Scientific Division Facilities, in the General Direction of Forensic and Electronic Laboratories Directorate, all within the Federal Police, a damaged Western Digital hard drive was received along with specific instructions to recover the information withheld which was considered critical for the operations of a different Federal Police area. After the device was examined, it was determined that its malfunction was due to damages in the logic board, some of its components were burned. In order to successfully repair the device, a "donor" hard drive with similar characteristics to the damaged hard drive was used in order to replace the logic boards damaged components.

Keywords

Data recovery, hard drive repair, damaged circuit board, damaged circuit board components exchange, donor hard drive.

Resumo

Nas instalações da Divisão Científica, na Coordenação para a Prevenção de Delitos Eletrônicos e em particular na área da Direção-Geral do Laboratórios em Eletrônica e Forense da Polícia Federal, foi recebido um Disco Rígido danificado, marca Western Digital, com a instrução de recuperar a informação nele contida, a qual era fundamental para o funcionamento de outra área da Polícia Federal. Após examinar o dispositivo, constatou-se que o mal funcionamento devia-se a um dano na placa lógica, já que vários de seus componentes estavam queimados, provavelmente devido a um curto-circuito. Para a reabilitação do dispositivo, foi utilizado um Disco Rígido doador, com características similares, para substituir os componentes danificados da placa.

Palavras chave

Reabilitação de Discos Rígidos, Recuperação de Informação, Placa Lógica Danificada, Substituição de Componentes de Placa Lógica, Disco Doador.

Introducción

En la actualidad, la información es uno de los bienes más valiosos con los que cuenta una institución, empresa o corporación, ya sea pública o privada. Debido al avance tecnológico de los últimos años la información es contenida en diversos dispositivos de almacenamiento digital. Datos sobre procesos de producción, clientes, transacciones comerciales, y en el caso de las Corporaciones Policiales, informes de los casos, avances de las investigaciones, relación de los hechos y personas involucradas, entre otros, están almacenados en discos duros, tanto internos como externos, memorias extraíbles y, en algunas ocasiones, "la nube".

Los dispositivos de almacenamiento digital generalmente tienen características que los hacen propensos a dañarse con cierta facilidad. Los Disco Duros en particular son equipos altamente sensibles debido a su arquitectura y el tamaño de sus componentes que, en algunos casos, miden nanómetros [1]. Una caída, un golpe, un movimiento brusco o una pequeña descarga de energía eléctrica, por mencionar algunos incidentes, pueden derivar en el mal funcionamiento de los dispositivos e incluso en la pérdida total de la información que contienen.

Esto es particularmente grave para las Corporaciones Policiales debido al tipo de información que se maneja. Por lo que la recuperación de la información es primordial en caso de que un dispositivo de almacenamiento digital falle.

En este artículo se presenta la metodología utilizada para diagnosticar y reparar el daño presentado en un Disco Duro tradicional (electromagnético), además del procedimiento empleado para rehabilitar un Disco Duro, marca Western Digital, con la tarjeta lógica dañada.

Metodología

Diagnóstico y rehabilitación de un disco duro

Al recibir un Disco Duro (DD), en las instalaciones de la Dirección General de Laboratorios en Investigación Electrónica y Forense, se procede con la siguiente metodología para emitir un diagnóstico y, si es necesario, rehabilitar el dispositivo para extraer la información contenida. El método consta de 4 etapas:

ETAPA 1 - Identificación del tipo de daño

a) Se identifica el DD;
   - ✓ Marca
   - ✓ Modelo
   - ✓ Número de modelo
   - ✓ Número de serie
   - ✓ Capacidad,
   - ✓ etcétera.

b) El DD es revisado físicamente en busca de golpes, abolladuras o lesiones visibles a las que se les pueda atribuir el mal funcionamiento del dispositivo.

c) Se energiza el DD, prestando particular atención a la presencia de ruidos atípicos o, en su caso a la ausencia de sonidos comunes relacionados con el arranque y funcionamiento adecuado del dispositivo.

d) El DD es conectado a un equipo de cómputo mediante un bloqueador físico de escritura, para comprobar si el BIOS de la computadora, el Sistema Operativo o alguna aplicación de diagnóstico lo reconoce y para prevenir la modificación accidental de la información en el Disco Duro.

En esta etapa existen tres variantes:

1. Que lo reconozca el sistema operativo sin ningún problema
2. Que no lo reconozca el BIOS
3. Si lo reconoce el BIOS, pero sistema operativo no.

En caso de que suceda el punto 1 se procede a extraer la información. Para los puntos 2 y 3, se asume que existe un daño que puede ser lógico o físico, ya sea por un fallo de la tarjeta lógica, de la mecánica interna del dispositivo o ambos; y se prosigue con la etapa de reparación física temporal.

ETAPA 2 – Reparación física temporal

a) Se identifican los elementos dañados, ya sea en la tarjeta lógica y/o, la mecánica interna del DD.

b) En caso de no contar con los elementos necesarios para la reparación del Disco Duro, se busca un "DD donador", el cual es un disco en buen estado y de características similares al dispositivo dañado, que se empleará para sustituir los componentes deteriorados por piezas funcionales. La compatibilidad entre el Disco Duro dañado y el donador, se define en base a la información publicada por el fabricante de los discos duros y por reconocidos expertos en recuperación de datos como Scott Moulton [2] y Stanislav Korb [3].

c) Se realiza la reparación física temporal del Disco Duro.

d) Se conecta a un equipo de cómputo, mediante un bloqueador físico de escritura. Si es reconocido correctamente, se pasa a la etapa de extracción de información. En caso contrario, se inicia nuevamente la revisión del disco en busca del problema, hasta lograr la reparación física, o hasta determinar que no es posible rehabilitar al Disco Duro.

Se realiza una reparación física temporal, ya que el Disco Duro después de ser rehabilitado no es confiable para ser puesto en operación nuevamente, y sólo se extrae la información.

ETAPA 3 – Extracción de la información

a) Se conecta el DD a un equipo de cómputo, mediante un bloqueador de escritura, o a un dispositivo para clonar discos duros.

b) Se genera una imagen forense (copia bit-a-bit) del DD.

Si durante la generación de la imagen se vuelve a presentar o se genera un nuevo daño, se vuelve a la etapa de Reparación física temporal.

c) Al finalizar la imagen forense, o al obtener una imagen parcial, se monta en un equipo de cómputo para verificar la información que se ha podido recuperar. En caso de detectar daño lógico en la imagen, se procede a la etapa de Recuperación lógica.

ETAPA 4 – Recuperación lógica

a) Se analiza la estructura del sistema de archivo para identificar el daño lógico y poder elegir el software de recuperación adecuado.

b) Se ejecuta el software de recuperación de información.

c) Se extrae la información recuperada.

Esta metodología está basada en las prácticas exitosamente aplicadas por empresas dedicadas a ofrecer el servicio de Recuperación de Datos, tales como: Forensic Strategy [4], Ontrack Data Recovery [5], y a la experiencia laboral de los autores.

Procedimiento de rehabilitación de disco duro marca western digital

Se recibió un Disco Duro externo, marca Western Digital, dañado. Las características del dispositivo se describen en la Tabla 01.

Número	Marca	Modelo	Número de Modelo	Número de Serie	Capacidad	Características Particulares
1	Western Digital	WD Caviar SE	WD5000AA JS-22TKA0	WCAPW386 7049	500 GB	Disco Duro, con daño físico visible Indica señales de daño en la tarjeta lógica.

Tabla 01. Características de Disco Duro marca Western Digital.

1. Se revisó físicamente la carcasa en donde se encontraba el Disco Duro (DD), la cual presentaba ligeras raspaduras y desgastes atribuibles al uso normal de un dispositivo de este tipo. Posteriormente se procedió a la remoción de la misma. Figura 01.

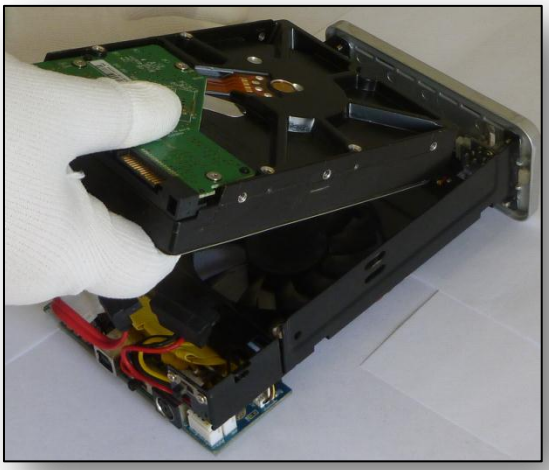

Foto 01. Remoción de la carcasa exterior del dispositivo.

2. Una vez fuera de la carcasa, se llevó a cabo la identificación y revisión física del DD. Los datos de origen: marca, modelo, número de serie y características particulares del dispositivo se muestran en la Tabla 01. Durante la revisión, se encontraron manchas y decoloraciones en la tarjeta lógica.

3. Se conectó el DD a un equipo de cómputo, marca DELL, modelo OPTIPLEX 980, como disco externo, usando un dispositivo bloqueador de escritura marca WEIBETECH, modelo Forensics UltraDock 4.

4. Al ser energizado el DD no presentaba ningún ruido, ni las vibraciones normales resultantes de la rotación del motor, tampoco se percibió el cambio de temperatura esperado en el dispositivo como parte de su funcionamiento normal.

5. El bloqueador de escritura no lo detectó, por lo que se procedió a conectarlo de forma interna a la computadora. Obteniendo un resultado negativo, tampoco fue reconocido.

6. Como resultado de los pasos anteriores, se decidió remover la tarjeta lógica para comprobar un fallo en la alimentación del dispositivo o algún daño visual.

7. Al retirar la tarjeta lógica, se pudo observar que algunos de los componentes electrónicos presentaban daños. Dos diodos, D3 y D4, dos resistencias R64 y R67, y un capacitor C81, mostraban quemaduras. Figura 02

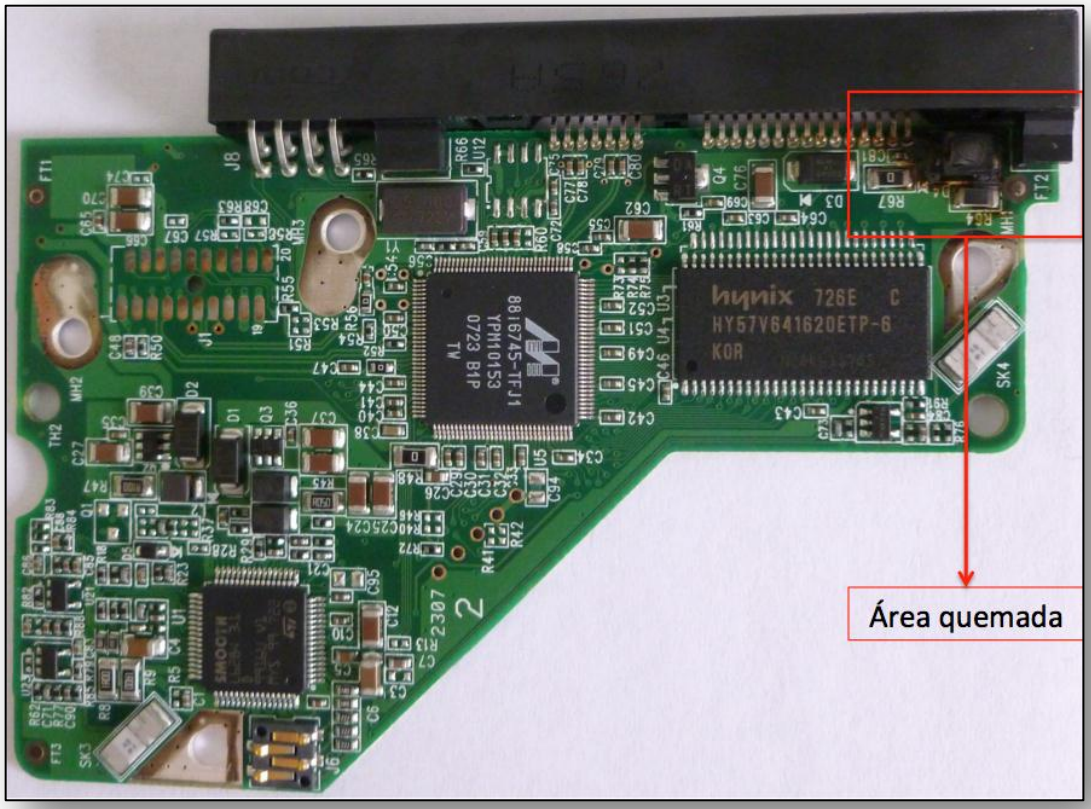

Foto 02. Área quemada de la tarjeta lógica.

8. Al tener identificado el problema y no contar con los elementos electrónicos necesarios para su reparación, se inició la búsqueda de un disco donador, de la misma marca y modelo que el DD externo, cuya tarjeta lógica fuera compatible con la tarjeta dañada para proceder al intercambio de piezas.

   Son varios factores los que determinan la compatibilidad de los discos, la misma marca y modelo son imprescindibles, adicionalmente, el lugar y la fecha de fabricación debe ser similares y en el caso de esta última, lo más cercana posible.

   En el caso de los discos Western Digital existe un código, el "DCM", que permite identificar los componentes compatibles. Esta información es provista por el fabricante y en diversos blogs y foros en Internet se explica, de forma sencilla, como interpretarlo [6-8].

9. Se realizó una exhaustiva búsqueda en los lugares donde se pueden adquirir discos duros y se verificó en distintos sitios en internet y se llamó a varias compañías que venden este producto en México.

10. Al ser un modelo relativamente "atrasado", del 2007, los proveedores locales no contaban con un disco similar compatible, derivado de ello, se opto por buscarlo en Internet en sitios extranjeros.

11. En la página de Internet de hddSupplier (www.hddsupplier.com), dedicada a la venta de equipos de cómputo de modelos no recientes, se ubicó un modelo compatible para el intercambio de piezas. La Foto 03 muestra la página de hddSuplier del Disco Duro seleccionado, el cual se logró obtener.

Foto 03. Página de hddSupplier

12. Una vez que el disco donador fue recibido en el laboratorio, se verificó que fuera el disco de la Foto 03. Los datos de origen del disco donador se encuentran en la Tabla 02.

Número	Marca	Modelo	Número de Modelo	Número de Serie	Capacidad	Características Particulares
1	Western Digital	WD Caviar SE	WD5000AAJS-22TKA0	WCAPW5470484	500 GB	Disco duro, que a primera vista y al revisarlo físicamente no presenta señales de daño en la tarjeta lógica

Tabla 02. Características de Disco Duro Donador marca Western Digital.

13. El Disco Duro donador se conectó a un equipo de cómputo del laboratorio, para comprobar que funcionara correctamente.

14. Se verificó la similitud entre las tarjetas lógicas de ambos discos. Figura 04

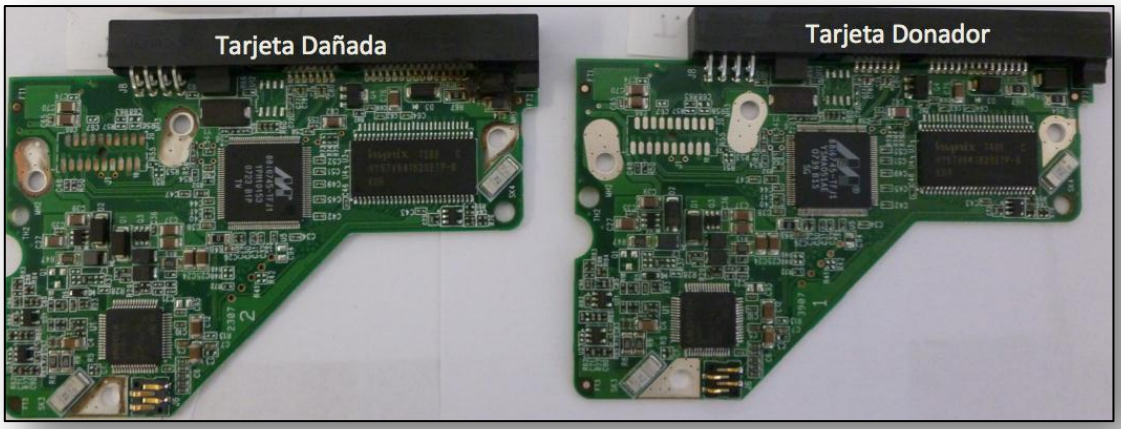

Foto 04. Verificación de la similitud de las tarjetas lógicas

15. Una vez probada la funcionalidad del disco donador y la compatibilidad de las tarjetas, se procedió al cambio de componentes electrónicos, utilizando técnicas de desoldado y soldado.

16. Después de reparar la tarjeta lógica, se ensambló con el Disco Duro dañado.

17. Se preparó un DD de 1TB para almacenar la imagen del DD ya reparado. Se sometió a un proceso de borrado seguro y se le generó una partición con un sistema de archivos NTFS.

18. El DD reparado se conectó a un Tableu Forensic Duplicador, y se utilizó el DD de 1TB, para guardar la imagen forense del disco.

19. Se verificó que la imagen se obtuvo al 100%, al igual que la información contenida en el DD reparado.

Conclusiones

Se logró recuperar el 100% de la información contenida en el Disco Duro externo, aún cuando el área solicitante pensaba que no sería posible, debido a la probable descarga de corriente eléctrica que recibió. Al final se entregó en un Disco Duro en buenas condiciones de 1TB.

En la reparación de un dispositivo de almacenamiento digital el objetivo primordial es recuperar la información que contienen. Los discos que han sido rehabilitados, sirven y pueden ser usados, pero su vida útil se acorta significativamente, y son más propensos a sufrir daños irreparables. Es por eso que se tiene que extraer la información, de preferencia, a uno nuevo e ir haciendo respaldos continuamente.

Por esta razón no es recomendable emplearlos para las mismas funciones previas al incidente, ya que se corre el riesgo de perder la información de forma definitiva.

Una sugerencia que se debe seguir, es revisar previamente todos los dispositivos que se empleen durante este tipo de procedimientos, los discos duros, clonadores, equipos de cómputo, e incluso los cables, para evitar agravar o no identificar de forma correcta el daño.

Bibliografía

[1] Chen, B., M., Lee, T., H., Peng, K. y Venkataramanan, V. (2006). Hard Disk Drive Servo System. Segunda Edición. Springer 2006.

[2] Moulton, S. (2007). Scott Moulton's Speech Research Material and Notes on Data Recovery . Junio 2007. Recuperado el 12 de noviembre 2010, de www.MyHardDriveDied.com.

[3] Korb, S. (2005). Copyright 2005-2011. Head Stack replacement: Questions and answers . Recuperado el 12 de enero 2011, de http://hddguru.com/articles/2006.02.17-Changingheadstack-Q-and-A/.

[4] Solomon, M., G., Barrett, D. y Broom, N. (2005). Computer Forensics JumpStart. Sybex © 2005.

[5] Ontrack Data Recovery, Inc. The Data Recovery Solution . Recuperado el 20 de enero 2011, de www.ontrack.com.

[6] Hard Drive Repair & Data Recovery Information, Hard Drive Parts. Recuperado el 01 de junio de 2012, de http://www.harddrive-repair.com/hard-drive-parts.html

[7] Hddguru Forums, Western Digital Head Stack swap and DCM. Recuperado el 01 de junio de 2012, de http://forum.hddguru.com/western-digital-head-stack-swap-and-dcm-t16441.html

[8] Data Recovery FAQ, Donor Drives. Recuperado el 01 de junio de 2012, de http://www.hddrecoveryfaq.org/donor.html


COMUNIDAD DE POLICÍAS DE AMÉRICA
AMERIPOL