INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA

SECCIÓN DE ESTUDIOS DE POSGRADO E INVESTIGACIÓN

UNIDAD CULHUACAN

"RECUPERACIÓN DE INFORMACIÓN EN DISCOS DUROS ELECTROMECÁNICOS A NIVEL FÍSICO Y LÓGICO PARA SU ANÁLISIS FORENSE INFORMÁTICO"

T E S I S

QUE PARA OBTENER EL GRADO DE

MAESTRO EN INGENIERÍA EN SEGURIDAD Y TECNOLOGÍAS DE LA INFORMACIÓN

PRESENTA

ING. MARICARMEN PÉREZ GARCÍA

ASESORES:

M. EN C. MARCOS ARTURO ROSALES GARCÍA
DR. GUALBERTO AGUILAR TORRES

MEXICO D.F. MAYO 2011

SIP-14-BIS

INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

ACTA DE REVISIÓN DE TESIS

En la Ciudad de México, D. F. siendo las 11:00 horas del día 27 del mes de mayo del 2011 se reunieron los miembros de la Comisión Revisora de la Tesis, designada por el Colegio de Profesores de Estudios de Posgrado e Investigación de SEPI-ESIME-CULHUACAN para examinar la tesis titulada:

"Recuperación de Información en Discos Duros Electromecánicos a Nivel Físico y Lógico para su Análisis Forense Informático"

Presentada por el alumno:

Pérez	**García**	**Maricarmen**
Apellido paterno	Apellido materno	Nombre(s)

Con registro:

A	0	9	0	4	6	8

aspirante de:

MAESTRÍA EN INGENIERÍA EN SEGURIDAD Y TECNOLOGÍAS DE LA INFORMACIÓN

Después de intercambiar opiniones los miembros de la Comisión manifestaron ***APROBAR LA TESIS***, en virtud de que satisface los requisitos señalados por las disposiciones reglamentarias vigentes.

LA COMISIÓN REVISORA

Directores de tesis

M. en C. Marcos Arturo Rosales García

Dr. Gualberto Aguilar Torres

Dr. Héctor Manuel Pérez Meana

Dr. Rubén Vázquez Medina

Dr. Gabriel Sánchez Pérez

INSTITUTO POLITECNICO NACIONAL
ESTADOS UNIDOS MEXICANOS
S.E.P.
SECCION DE ESTUDIOS DE POSGRADO E INVESTIGACION
ESIME CULHUACAN

PRESIDENTE DEL COLEGIO DE PROFESORES

Dr. Gonzalo Isaac Duchen Sánchez

INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

CARTA CESIÓN DE DERECHOS

En la Ciudad de México, D.F. el día 30 del mes mayo del año 2011, el (la) que suscribe C. Maricarmen Pérez García alumno (a) del Programa de Maestría en Ingeniería en Seguridad y Tecnologías de la Información con número de registro A090468, adscrito a SEPI-ESIME-CULHUACAN, manifiesta que es autor (a) intelectual del presente trabajo de Tesis bajo la dirección de M. en C. Marcos Arturo Rosales García y cede los derechos del trabajo intitulado Recuperación de Información en Discos Duros Electromecánicos a nivel Físico y Lógico para su Análisis Forense Informático, al Instituto Politécnico Nacional para su difusión, con fines académicos y de investigación.

Los usuarios de la información no deben reproducir el contenido textual, gráficas o datos del trabajo sin el permiso expreso del autor y/o director del trabajo. Este puede ser obtenido escribiendo a la siguiente dirección mperezg0808@ipn.mx. Si el permiso se otorga, el usuario deberá dar el agradecimiento correspondiente y citar la fuente del mismo.

Ing. Maricarmen Pérez García
Nombre y firma

Agradecimientos

Al Consejo Nacional de Ciencia y Tecnología (CONACyT) por el apoyo brindado para la realización de este trabajo.

Al Instituto Politécnico Nacional (IPN) por las facilidades otorgadas para el desarrollo de este trabajo de Tesis.

A mi esposo Miguel Angel, por todos sus consejos, revisiones y aportaciones en este trabajo. Por ser mi compañero profesional.

A mi madre por enseñarme a luchar y esforzarme para alcanzar las metas, a mis hermanos por todo el apoyo y confianza.

A Marcos por la oportunidad de desarrollar esta tesis, por su orientación y apoyo para realizar y llevar a buen término este trabajo.

A todos los profesores de la sección, por contribuir y enriquecer en gran medida en el desarrollo y enfoque del trabajo con sus consejos. Gracias Gualberto, Gabriel, Héctor Manuel, Gina, Moisés, Eleazar, Alejandro.

A todos mis amigos que han formado parte de cada uno de mis éxitos.

A todos mis amigos y compañeros de la sección, por todos los buenos momentos y por la colaboración con este proyecto.

Resumen

Al llevar a cabo una investigación de informática forense en un disco duro electromecánico se puede presentar el caso en el que el disco tenga un daño lógico ó físico, no permitiendo el análisis en busca de evidencia. Por tanto se requerirá realizar el proceso de recuperación de información.

La recuperación de información, así como la informática forense, debe tener su propia metodología, ya que en ambos casos se trabaja con la información, siendo ésta el objeto principal de estudio.

Debido a que no existe una metodología estándar para este proceso, únicamente "mejores prácticas", que ayuda a una adecuada y rápida recuperación, el propósito de esta tesis es proporcionar una metodología cuyo objetivo sea recuperar la mayor cantidad de información de forma íntegra.

Para establecer la metodología es necesario conocer las causas y consecuencias que originan los daños, estas consecuencias determinan cada etapa de la metodología a seguir utilizando la toma de decisión correspondiente, y de esta forma aplicar la solución apropiada.

Para conocer las causas que originan daños en los discos duros electromecánicos, es necesario conocer primero la estructura física y lógica, así como entender su funcionamiento.

En este trabajo se realizan pruebas de ataques a la estructura lógica para establecer la clasificación de los daños lógicos. Mientras que para establecer la clasificación de daños físicos y la metodología, se analizaron muestras de discos duros de 2.5" y 3.5" con diferentes características.

Los resultados obtenidos al aplicar la metodología en un grupo de discos duros electromecánicos se muestran mediante un modelo de análisis de regresión multivariada, donde se observa el impacto que causa la metodología sobre la tasa de recuperación de información.

Abstract

During an investigation of Computer Forensic in an electromechanical hard disk drive, it could happen that the hard disk has a physical or logical damage, turning the analysis for searching evidence becomes impossible, a Data Recovery process will be required.

The Data Recovery on damaged hard disk drive and the Computer Forensic must have its own methodology, since both cases the experts handle with information, which it is the target of the analysis.

Due the absence of a standard methodology for this process and because there are only “best practices”, which helps to an adequate and earlier recovery, the purpose of this research is to provide an applicable methodology which objective is to recover as much reliable data as possible.

In order to establish the methodology is necessary to know the causes and consequences that arises the damages, these effects determine each stage of the methodology using the correspondent decision taking, and then apply the suggested solution by this methodology.

Finding those causes that arise the damages in electromechanical hard disk drives, it is necessary to understand the logical and physical structure as their operation.

In order to establish the classification of logical damages, attacks on logical structure were tested. For physical classification and methodology, it was used groups of hard disk drives of 2.5” and 3.5” with different features.

The results of applying the methodology in a group of electromechanical hard disk drives are displayed using a model of multivariate regression analysis, which shows the impact that the methodology caused on the recovery data rate.

CONTENIDO

Índice de Figuras

Índice de Tablas

Objetivo general

Desarrollar una metodología basada en mejores prácticas para recuperar información en discos duros electromecánicos a nivel físico y lógico, para su posterior análisis forense informático.

Objetivos específicos

- Identificar las principales causas y consecuencias de los daños en los DDEs, para realizar una clasificación de los diferentes tipos de daños de índole física y lógica, y posteriormente proponer posibles soluciones.
- Aplicar “mejores prácticas” para el proceso de recuperación de información sobre una muestra de DDEs dañados para verificar su eficiencia.
- Diseña y establecer las etapas y fases de la metodología propuesta.
- Probar la metodología propuesta sobre una muestra de DDEs dañados que requieren el proceso de recuperación de información, para verificar su eficiencia.
- Analizar los resultados obtenidos de los procesos de recuperación de información, mediante un modelo de análisis de regresión multivariante para obtener la tasa de recuperación.

Alcance

La metodología y soluciones propuestas se aplican con la finalidad de recuperar información de discos duros electromecánicos IDE y SATA de 3.5” y 2.5” los cuales fueron donados para esta investigación, y son de las siguientes marcas: *WD, Fujitsu, Maxtor, Quantum, Seagate, IBM, Toshiba, Samsung* y *Hitachi.*

Introducción

La información es uno de los activos más importantes, no sólo para las empresas sino para las personas en general. La universidad de California en Berkeley en su estudio llamado *How much Information?,* 2003 [1], indica que el noventa y dos por ciento de la nueva información que se generaba se almacenaba en medios magnéticos, principalmente discos duros.

Un estudio realizado por una empresa dedicada a la investigación de mercados, *eTForecasts* [2] calcula que en el año 2008 tan sólo en México hubo 19.94 millones de computadoras en uso, las cuales contienen al menos un disco duro como dispositivo de almacenamiento.

Los discos duros electromecánicos por su propia naturaleza de funcionamiento electrónico y mecánico y factores como condiciones de uso o errores humanos, son susceptibles a presentar fallas. Dichas fallas pueden ir desde un borrado accidental de archivo, hasta un problema severo en las cabezas.

En los dos últimos años, setenta y cuatro por ciento de las empresas experimentan incidentes que involucran la pérdida de datos, según estudios realizados por *Kroll Ontrack* [3] (empresa dedicada a la Recuperación de Información). Otro estudio realizado por *DeepSpar Data Recovery Systems* [4] revela que el costo por un sólo incidente de pérdida de datos puede oscilar entre 350US a 1,500US dependiendo de la severidad del daño y de la necesidad de un servicio especializado; si se le añade el costo de producción que ocasiona el que la información no esté disponible, el costo varía entre 475US a 2,300US. Estas cifras son estimadas, aunque en realidad cada caso de pérdida de información varía en función del daño, de su magnitud, la capacidad del disco, entre otros factores.

El problema de pérdida de datos se agrava más cuando se está en un proceso de análisis forense informático, ya que el objetivo de estos procesos es búsqueda y obtención de evidencia de un ilícito, por lo cual la integridad de la información es de gran importancia. Dentro de las metodologías que existen para la informática forense no se considera cuando el disco duro a analizar presenta un daño principalmente físico.

En México existe poca investigación en dispositivos de almacenamiento y aún es más escasa en cuanto a recuperación de información en discos duros. La mayor investigación que se realiza, se hace en el sector privado y muchas veces dicha investigación es sin algún sustento

científico, realizando recuperaciones de información sin seguir una metodología adecuada. Estas investigaciones no son publicadas por miedo al robo de secreto industrial.

El proceso de recuperación de información debe realizarse siguiendo una metodología, ya que se trabaja con la información, la cual es donde se realizará el análisis forense informático. Para establecer la metodología es necesario conocer las causas y consecuencias que originan los daños, estas consecuencias determinan cada etapa de la metodología a seguir utilizando la toma de decisión correspondiente, y de esta forma aplicar la solución sugerida por la metodología.

Al contar con una metodología adecuada a los tipos de daños que se presentan en los discos duros y considerando la ausencia de una previamente establecida, el número de casos de éxito se incrementa permitiendo continuar con el proceso de análisis forense informático para encontrar la evidencia; y el tiempo de recuperación de información disminuye.

La importancia de este trabajo radica tanto en la aportación de la metodología, la clasificación y esquematización de soluciones acorde a los daños, como el antecedente para futuras investigaciones.

Estado del arte

Para la informática Forense desde su creación en 1984, se han desarrollado varias metodologías por organizaciones como:

1. National Institute of Standard and Technology**, NIST 800-86, "Guide to Integrating Forensic Techniques into Incident Response",** Agosto 2006.
   La metodología consta de las siguientes fases: Colección, examen, análisis y reporte.
2. Institute of Justice United States, **"Forensic Examination of Digital Evidence: A Guide for Law Enforcement"**, **NIJ Special Report** , Abril 2004.
   La metodología consta de los siguientes pasos: Evaluación, Adquisición, Examen y Documentación y reporte de informes.

Y algunas mejores prácticas como las de ENFSI (European Network of Forensic Science Institute) en el documento **"Guidelines for Best Practice in the Forensic Examination of Digital Technology"**, Abril 2009.

Dentro de las metodologías arriba mencionadas y mejores prácticas, no se considera cuando el dispositivo electrónico de almacenamiento objeto del análisis informático forense presenta algún tipo de daño, ya sea de índole física o lógica. Sin embargo el establecimiento de metodologías enfocadas al análisis forense informático es un precedente para el establecimiento de una metodología para la recuperación de datos en discos duros.

Charles H. Sobey, ChannelScience. Laslo Orto y Glenn Sakaguchi, ActionFront Data Recovery Labs, Inc. "Drive-Independent Data Recovery: The Current State-of-the-Art". IEEE TRANSACTIONS ON MAGNETICS, VOL. 42, NO. 2, FEBRUARY 2006.

En este artículo se da una definición de recuperación de datos: "Acceso lógico y/o físico a dispositivos de almacenamiento dañados, para los cuales no existe un respaldo funcional". Menciona que no existe mucha investigación conocida para la recuperación de datos, ya que las empresas las protegen como propiedad intelectual. Las técnicas más conocidas para la recuperación de datos en caso de daño físicos son el "reemplazo de partes", es decir sustituir el elemento por uno similar tomado de un disco donador. Aunque esta técnica está siendo cada vez más difícil de aplicar conforme avanza la tecnología. Se menciona la importancia de crear una imagen del disco duro dañado durante el proceso de recuperación de información.

La definición del término Recuperación de Datos proporcionada en el artículo de Sobey et al. es un poco limitada para encerrar lo que realmente implica por lo que dentro de este trabajo se propondrá una definición, asimismo tampoco proporciona alguna metodología que permita dirigir de una forma más eficiente este proceso. Sin embargo el crear una imagen, se tomará en consideración como una etapa dentro de la metodología, debido a la gran importancia que representa. Se enfoca a los daños físicos y posibles soluciones, estos servirán como punto de partida para el análisis que se realizará de los tipos de daños a nivel físico.

Ben M. Chen, Tong H. Lee, Kemao Peng y Venkatakrishnan Venkataramanan. "Hard Disk Drive Servo System". Second Edition, Springer 2006.

Abdullah Al Mamun, GuoXiao Guo y Chao Bi. "Hard Disk Drive Mechatronics and Control". CRC Press 2007.

Los dos libros arriba mencionados, indican la estructura de los discos duros electromecánicos, elemento por elemento así como el funcionamiento en conjunto de estos. Este estudio permite conocer las condiciones de funcionamiento a las que están sujetos cada elemento y por tanto obtener una explicación de los posibles daños que puedan sufrir, con ello se podrá pensar en una posible solución.

Chengdu Yiwo. Data Recovery E-Book V1.5. Tech Development Co., 2006.

www.easeus.com (acceso Mayo 11, 2010).

En este libro electrónico se describe la estructura lógica de los discos duros, así como la forma de recuperar la información en estos a nivel lógico, dentro de estos problemas se presenta cuando se borran archivos, se dañan los archivos o la estructura del archivo de sistema o en caso de formato al disco duro. Abarca los sistemas de archivo NTFS y FAT.

La información proporciona en este libro, sobre la estructura y los daños a nivel lógico se tomarán como punto de partida para este trabajo con respecto a los daños a nivel lógico.

Scott Moulton. Manuscript: "Scott Moulton's speech research material and notes on Data Recovery". Forensic Strategy Services, LLC. 2007.

Este manuscrito presenta 4 fases para la recuperación de datos en discos duros:

1. Reparación del disco duro: Usualmente requiere hardware o equipo especial.
2. Imagen, copiar o recuperar al disco y sectores físicos principalmente mediante una imagen bitstream (cadenas de bits).
3. Realizar la recuperación lógica de archivos, estructura de particiones o elementos necesarios.
4. Reparación de archivos que puedan haber existido en espacio dañado o sectores para recuperar lo que es posible.

Menciona posibles causas por las cuales un disco duro presente el problema de "clicking" (sonido de golpeteo de las cabezas) y sus posibles soluciones. Indica el procedimiento de cambio de cabezas, platos y motor. E indica cómo distinguir discos duros que sean compatibles para cambio de partes, de acuerdo a las marcas y modelos más comunes.

Las fases presentadas por Moulton no llegan a formar propiamente una metodología, son únicamente buenas prácticas, siendo muy generales y presentando únicamente 4 fases; sin embargo se tomarán como base para el desarrollo de la metodología, ya que cada una de estas fases es de gran importancia y no deben ser omitidas. El manuscrito de Moulton se enfoca a daños físicos, proporcionando una base para este trabajo con respecto a este tipo de daños, y permitiendo la visualización de algunas soluciones.

Capítulo 1. DISCOS DUROS ELECTROMECÁNICOS

En este capítulo se describen los componentes físicos que conforman un *disco duro electromecánico* (DDE), la estructura lógica, es decir, cómo se almacena la información, así como su funcionamiento. De ésta forma se podrán reconocer y esquematizar los factores que pueden producir un daño a nivel físico y lógico, y por lo tanto, ocasionar la pérdida de datos.

1.1. Antecedentes

La industria de los discos duros ha ido creciendo a gran velocidad. A lo largo de 55 años desde el desarrollo del primer DDE, se han creado, desaparecido y fusionado grandes fabricantes.

1.1.1. Reseña de fabricantes de DDEs y sus fusiones.

El comienzo de los discos duros tiene su origen en 1956 en la empresa International Business Machines, mejor conocida como *IBM* [5].

IBM es una empresa fundada en 1889, y en el año 2003 vendió su división de fabricación de discos duros a *Hitachi*, dando origen a la empresa *Hitachi GST (Hitachi Global Storage Technologies)* subsidiaria de *Hitachi, Ltd*, dedicada a la fabricación de discos duros [6]. Actualmente *Hitachi GST* es una empresa líder en tecnología de almacenamiento.

En 1970 surge *Western Digital (WD)* como fabricante de semiconductores, en los 80's ingresa a la industria del almacenamiento y actualmente es el segundo líder de fabricantes de discos duros [7].

En 1979 surge *Seagate* actualmente líder mundial en la fabricación de discos duros, en 1996 se le une la empresa *Conner Peripherals*, la cual fue creada en 1985 [8].

Quantum Corporation surge en 1980 y en el año 2000 la empresa *Maxtor* comienza la transacción de compra de la línea de discos duros *Quantum.* Dicha compra se concreto el 1º de abril del 2001. Actualmente *Quantum* conserva las líneas de almacenamiento y cintas *DLT* [8].

Maxtor es otra empresa que llegó a ser líder en la industria de la fabricación de discos duros, fundada en 1982, y en el año 2006 fue adquirida por *Seagate* [9].

Toshiba es líder mundial en la fabricación de DDEs de 2.5", así como discos duros para automóviles. *Fujitsu* le transfirió su línea de negocios de discos duros el 1º. de octubre de 2009 [10].

1.1.2. Breve historia de los DDEs

La tecnología en los DDEs ha sido desarrollada rápidamente. Los fabricantes invierten en innovar a los DDEs para que sean más estables, y por consiguiente más confiables, con lo cual tratan de disminuir las limitaciones de capacidad de almacenamiento encontradas en el pasado. Los avances más relevantes en los DDEs han sido:

- En 1956 se dio a conocer por *IBM* el primer disco duro comercial, llamado RAMAC (*Random Access Method of Accounting and Control*). Almacenaba 5 millones de caracteres, aproximadamente 5MB, con caracteres de 7 bits. Usaba 50 discos, cada uno de 24 pulgadas de diámetro. Con una transferencia de datos de 8,800 bytes por segundo y giraba a una velocidad de 1,200 rpm (revoluciones por minuto) [5,11].
- En 1961 se dio a conocer por *IBM* el modelo *1301*, el primer disco duro que utilizaba el sistema *air-bearing slider*, en el que las cabezas flotan, lo que permitió mayor capacidad de almacenamiento y confiabilidad [5]. Ya en 1962 *IBM* anuncia el lanzamiento de su *laser diodo*, fundamental para la tecnología de escritura y lectura. Poco tiempo después, en 1963 libera el primer disco duro con discos removibles, el *IBM 1311* [12] y más adelante en 1965 lanza su nuevo disco duro modelo *2310*, con paquetes de discos removibles, famosos en los 60's y 70's [11].
- En 1970 se da a conocer el invento del *floppy disk*, el cual da lugar al almacenamiento portátil [12]. En 1971 se dio a conocer el primer DDE con sistema *closed loop servo control* el *IBM 330 Merlin* que usaba la posición relativa de la cabeza al *Track* [5]. En 1973 *IBM* introdujo el modelo *3340* con dos *spindles* separados, uno permanente y otro removible, cada uno con capacidad de 30MB, por lo que se le refería como 30-30. Esto le ganó el mote de "*Winchester*", por el famoso rifle [5]. En 1979 *IBM* dio a conocer el modelo *3370* que utilizaba cabezas de *thin film*, las cuales fueron estándar durante varios años [11].
- En 1980 *Seagate* presenta el *ST-506* el primer disco 5.25" con *stepper motor* y de 5MB [11]. En 1981 *IBM* introdujo la primera computadora personal, originando con ello que en 1987 surgiera el grabado 1GB por pulgada cuadrada con grabado *magneto-óptico* [12]. En 1983 *Rodime* introdujo el *RO352*, disco de 3.5". Y en 1985 *Quantum* hace lo propio con el *hard-card*, disco duro de 10.5MB montado sobre

una tarjeta de expansión ISA (*Industry Standard Architecture*). En 1986 *Conner Peripherals* da a conocer el modelo *CP340* el primer disco en usar *voice coil actuator* y en 1988 el modelo *CP3022*, que fue el primer disco de 3.5" que usaba una pulgada de altura reducida, llamado de bajo perfil [11].

- En 1990 *IBM* introdujo el modelo *681* con 857MB y cabezas MR (*magneto-resistencia*) y decodificación de datos PRML (*Partial Response and Maximum Likelihood*). En 1991 *IBM* reemplaza la *media de oxido* con *media thin film* en la superficie de los platos. En este mismo año *Integral Peripherals* introduce el primer disco de 1.8" y en 1992 H.P. el primer disco de 1.3" el modelo *C3013A.* En 1997 *Seagate* presenta el primer disco de 7,200 rpm y posteriormente el de 15,000 rpm. En 1998 estuvo disponible el primer *DVD-ROM* y en el mismo año *IBM* dio a conocer las LTO (*Linear Tape Open*) que permite escribir 100GB de datos y *Seagate* el disco de 10,000 rpm [11].
- En el año 2000, *IBM* introduce el *Microdrive* de 1Gb, que pesaba sólo 16 gramos [12], en este mismo año *Seagate* da a conocer el *Barracuda 180,* siendo éste el disco de mayor capacidad 180GB en ese momento. En el 2002 *Seagate* lanza el modelo *Barracuda ATA V*, que es el primer disco con capacidad de 120GB usando sólo dos platos. En el 2004 *Seagate* presenta el modelo *Savvio*, el primer disco duro de 2.5" de clase *Enterprise*. En el 2005 *Seagate* presenta el disco *Barracuda 7200.9* con capacidad de 500GB, la mayor capacidad alcanzada hasta ese momento, en un sólo disco duro, también presenta el primer disco de 2.5" con grabado perpendicular, en el 2006 el primer disco de 750GB y en el 2008 el primer disco de 1.5TB, en tanto *Hitachi* se adelanta en el 2007 y lanza al público el primer disco de 1TB [11].

1.2. Estructura física de los DDEs

Para poder recuperar la información de un DDE, se deben conocer todos sus elementos, es decir, la forma en la que trabajan, como almacenan la información, en general el funcionamiento interno físico y lógico.

1.2.1. Definición de DDE

Un disco duro es un dispositivo electromecánico de almacenamiento no volátil el cual posee la característica de almacenar información por un largo período, aún cuando no tenga suministro de energía. Sus componentes se dividen en 3 categorías: mecánicos, electrónicos y magnéticos (tabla 1.1). Todos ellos contenidos en 2 partes principales: *Head Disk Assembly* (HDA) y *Printed Circuit Board* (PCB).

La información es almacenada en platos circulares recubiertos de un material magnético comúnmente llamado *media*, dichos platos están montados sobre un motor que funciona como eje central, que los hace girar al mismo tiempo. La lectura y escritura de la información se realiza mediante una cabeza de lectura y otra de escritura, que están montadas en un pequeño elemento llamado *slider* [13]. Existe un *slider* por cada cara del plato y éstos, a su vez, están montados sobre unos soportes llamados *suspensions*, los cuales a su vez están montados sobre pequeños brazos conformando el *head-stack*.

Tabla 1.1. Componentes del DDE.

Mecánicos	*Spindle Motor,* Mecanismo *Head Actuator*
Electrónicos	Tarjeta Impresa de Circuitos (PCB), CI preamplificador
Magnéticos	Platos, Cabezas de Lectura/Escritura.

Esta estructura se mueve de forma lateral por el *Voice Coil Motor* (VCM) *Actuator* para posicionar las cabezas en el *track* que será leído o escrito. Cuando a un DDE se le deja de administrar energía, el *slider* es empujado hasta la *landing zone* o *Dynamic load/unload* [13,14], ambas tecnologías sirven para que las cabezas reposen cuando no están en funcionamiento. Los discos más recientes manejan la tecnología del *Dynamic load/unload.*

1.2.2. *Head Disk Assembly* (HDA)

El HDA es la estructura básica del DDE, se compone de un *case* base y de la cubierta (Figura 1.1), ayuda a mantener en niveles bajos la contaminación - debida a partículas como polvo o humo - dentro del DDE. Esto se logra con el reflujo de aire a través de un filtro.

Figura 1.1. HDA completo de un DDE.

Los elementos que están contenidos en el HDA son los platos, cabezas, VCM *Actuator*, Filtros, etc, como se muestra en la Figura 1.2.

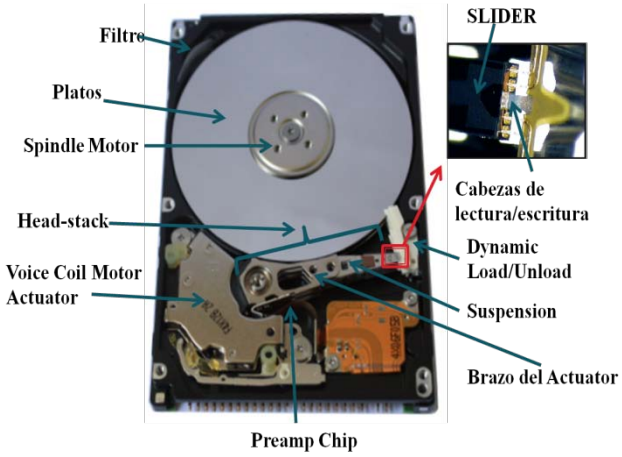


Figura 1.2. Componentes internos de HDA de un DDE.

El HDA es ensamblado en un *clean room* (área con control ambiental de partículas en el aire) [15] de clase 100, es decir, que en un pie cubico de aire no puede haber más de 100 partículas.

1.2.2.1. Platos

Los datos se graban en platos circulares que giran continuamente, este almacenamiento se realiza en ambos lados. Los platos están hechos de aluminio o vidrio, y se recubren en ambos lados con capas de varios materiales, entre ellos la capa de material magnético denominada *media*.

Los platos tienen una abertura circular en el centro, a través de la cual pasa el eje del motor que les hace girar al mismo tiempo a una velocidad angular constante (ω rad/s), y que hace las veces de ensamble. La velocidad relativa entre la cabeza y el *track* de datos depende del Radio (R) en el cual el *track* está localizado (ecuación 1.1).

$$v = \omega R \tag{1.1}$$

Los DDEs de 3.5", típicamente utilizados en equipos de cómputo de escritorio, giran a velocidades de 5,400/7,200 rpm; los de 2.5", usualmente para laptops, a velocidades de 4,200/5,400/7,200 rpm. Los discos de 1.8", para dispositivos de música o minilaptops, a velocidades de 4,200/5,400 rpm. Los DDEs con tecnología SCSI giran a mayores velocidades, de 10,000 rpm o 15,000rpm y generalmente los usan en servidores.

El material de los platos debe ser de cierta textura que permita que las cabezas puedan deslizarse sin tocar la superficie del plato mientras se encuentre girando. Para que las cabezas se "estacionen", existen dos formas: en los DDEs anteriores se colocaba un anillo anular cerca del motor de diferente textura al resto del plato para que las cabezas pudieran utilizar esta área como *landing zone* sin que afectara el funcionamiento de ambos elementos, en esta área no se graba información; en los DDEs más modernos se tienen una pequeña rampa fuera de los platos llamada *Dynamic Load/Unload* que es donde las cabezas se "estacionan".

Los tipos de *media* magnética que se utilizan en los platos son los siguientes [16]:

Thin-Film-Media

En la *thin-film-media* se utilizan procesos como *sputtering* (extracción de átomos de la superficie de un electrodo debido al intercambio de momento con iones que bombardean los átomos de la superficie) o *electroplating* (usualmente llamado "plating", es el depósito de un recubrimiento de metal sobre un objeto, poniendo una carga negativa sobre ella y poniéndola en una solución que contiene sal de metal, la sal de metal contiene iones metálicos con carga positiva que son atraídos por el objeto con carga negativa y son "reducidos" a forma metálica) para depositar la delgada película en los platos.

Cada plato se compone de una capa de Níquel con Fósforo (Ni-P), posteriormente una capa de Cromo (Cr), luego una pequeña capa de material magnético normalmente aleación de Cobalto, luego una capa de Carbón y por último una capa muy delgada llamada de lubricante (Figura 1.3).

La capa de lubricante y la de Carbón sirven como protección del contacto intermitente con las cabezas. La capa de lubricante reduce el "desgaste" de la capa de Carbón. La razón de tener una capa de Carbón es porque incrementa la durabilidad mecánica de los platos y mitiga la corrosión de la capa magnética [12].

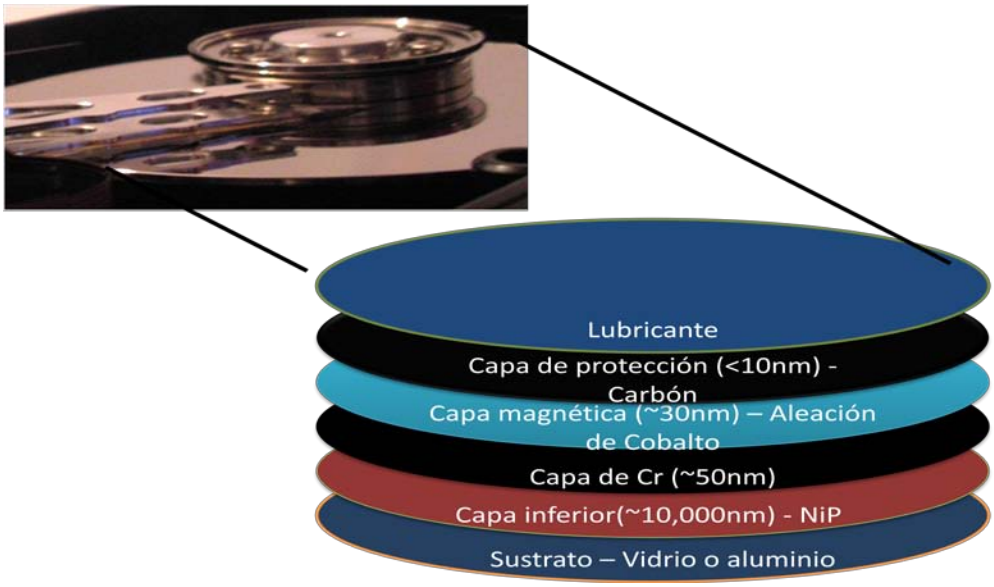


Figura 1.3. *Thin Film Media.*

***Antiferromagnetically Coupled Media* (AFC)**

Debido a que la capacidad en los DDE debe incrementarse, la capa de material magnético debe ser más delgada y la densidad de área incrementarse.

IBM introdujo la tecnología AFC para los platos, la cual consiste en tener dos capas de material magnético de diferente espesor separadas por una capa muy delgada de Rutenio (Figura 1.4), este sándwich produce un acoplamiento antiferromagnético (ordenamiento magnético de los momentos magnéticos en la misma dirección pero sentido inverso) de la parte superior e inferir de las capas magnéticas y permite una estabilidad térmica [17].

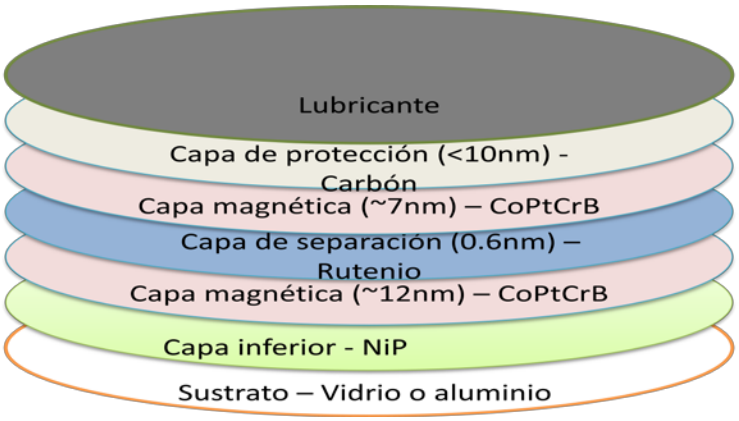


Figura 1.4. *Antiferromagnetically Coupled Media.*

Existen 2 formas de grabar la información, se conoce como grabado perpendicular y grabado longitudinal.

Grabado longitudinal

La grabación longitudinal es el método en el cual se graban los *bits* de datos de tal forma que están alineados horizontalmente con respecto al plato giratorio. La dirección de las cargas magnéticas son horizontales a la *media*, los polos norte y sur de las partículas magnetizadas se alinean paralelamente a la superficie del plato (Figura 1.5).

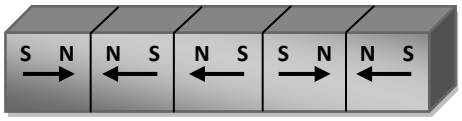


Figura 1.5. Grabado longitudinal.

Grabado Perpendicular

En este tipo de grabación las señales magnéticas se graban alineadas verticalmente a la superficie de los platos (Figura 1.6).

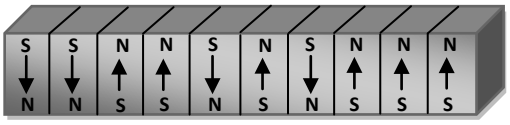


Figura 1.6. Grabado Perpendicular.

Esta tecnología se comenzó a utilizar en el año 2005 por *Toshiba* en DDEs de 1.8" de 160GB, posteriormente se utilizó en DDEs de 2.5" y de 3.5" de capacidades de 750GB o de 1TB, tanto por *Toshiba* como otros fabricantes como *Seagate*, *Hitachi*, etc, [12]. Este método de grabación además de incrementar la densidad de área, también aumenta la resistencia del dominio del efecto superparamagnético (esto es una desestabilización en la orientación de la señal, ocasionando que el valor del bit cambie aleatoriamente, y se origina cuando la señal que representa al *bit* es tan pequeña que su temperatura llega a ser la misma del medio ambiente).

1.2.2.2. Cabezas

La lectura y escritura de los datos se realiza mediante dos cabezas, una de lectura y otra de escritura (Figura 1.7). Se utilizan dos cabezas para poder incrementar la densidad de área y por tanto almacenar más información en espacios más pequeños, así al mejorar la tecnología en una de ellas no se afecta a la otra. Ambas cabezas están montadas sobre un elemento llamado *slider*, el cual provee conectividad eléctrica a ambas cabezas y ayuda a colocar las cabezas en las proximidades de los *bits* magnetizados "volando" sobre la superficie de los platos que están girando. El aire que se mueve junto con los platos giratorios y que es arrastrado entre la superficie del plato y la superficie aerodinámica del *slider* produce un *air bearing* que hace al *slider* "flotar"; a la distancia que se encuentra entre el *slider* flotando y el plato se le llama *flying height*, en el año 2003 esta distancia se encontraba alrededor de 5 nanómetros [13].

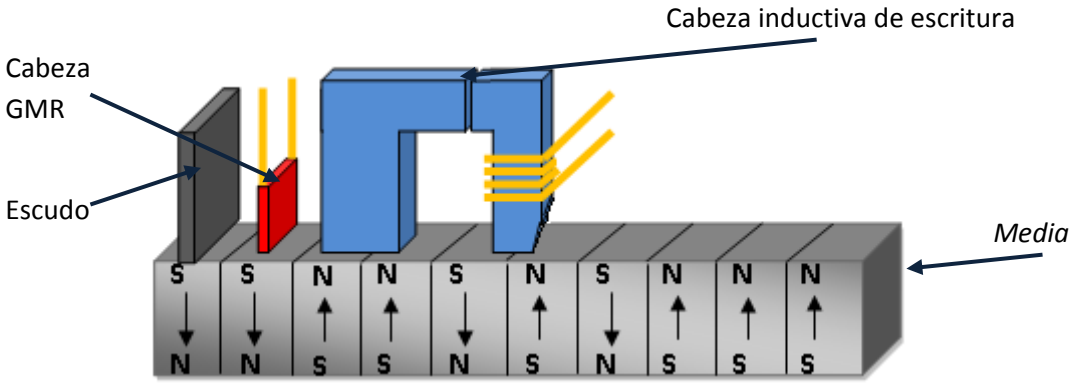


Figura 1.7. Cabezas de lectura y escritura. Hitachi Global Storage Technologies, 2007.

Cabeza de escritura

A este elemento se le llama cabeza *film inductive*, y es una estructura de bobina de *"thin film"* que emite un campo magnético cuando la corriente pasa a través de la bobina y este campo magnético polariza a la *media.* El núcleo de la cabeza tiene un pequeño espacio el cual vuela sobre el plato. La polaridad del campo magnético y por tanto la magnetización de la *media* puede ser revertida, cambiando la polaridad de la corriente que pasa por la bobina y representando un 1 o un 0. Las áreas polarizadas que representan a los *bits* son acomodados en *tracks* circulares concéntricos.

De acuerdo al principio magnético de inducción, un voltaje es producido entre las dos terminales de una bobina cuando es colocada en un campo magnético variable en el tiempo. El voltaje inducido en la bobina del sensor de lectura puede ser expresado matemáticamente como se muestra en la ecuación 1.2.

$$V_{ind} = -N\frac{d\phi}{dt} \tag{1.2}$$

Donde N es el número de vueltas en la bobina y ϕ es el flujo magnético. Como el flujo tiene una distribución espacial, se puede decir que:

$$\frac{d\phi}{dt} = \frac{d\phi}{dx}\frac{dx}{dt} = v\frac{d\phi}{dx} \tag{1.3}$$

Donde '*v*' es la velocidad relativa entre la cabeza y la *media*. La salida del sensor inductivo de lectura es proporcional a la velocidad del *track* de datos con respecto a la cabeza.

Cabeza de lectura

La cabeza encargada de lectura ha cambiado en su tecnología desde su creación, para adaptarse al cambio de tecnología en la *media*. Esta cabeza es más estrecha que un *track* de datos, para evitar que se interfiera con otro *track* durante la lectura.

Las últimas dos tecnologías han sido la *Magneto-Resistencia*, y la *Magneto-Resistencia-Gigante.*

a) ***Magneto-Resistencia* (MR)**

Estas cabezas fueron introducidas al mercado por *IBM* en 1991, en un DDE de 1GB de 3.5". Cuando un alambre pasa a través de un campo magnético, no sólo genera una pequeña corriente sino que la resistencia del alambre también cambia. Las cabezas de lectura estándar usan la cabeza como un pequeño generador, basados en el hecho de que las cabezas generan pulsos de corriente cuando pasan sobre transiciones de flujos magnéticos. Para la creación de las nuevas cabezas de lectura, *IBM* utilizó el hecho de que la resistencia en los alambres de las cabezas también cambia.

Las cabezas MR usan la cabeza como una resistencia. Un circuito pasa un voltaje a través de una cabeza y observa el voltaje que cambia, el cual ocurrirá cuando la resistencia de la cabeza cambie a medida que pasa a través del flujo revertido en la *media*. Este mecanismo resulta en una señal más fuerte y clara de lo que hay en la *media* y habilita el incremento de la densidad [12]. El sensor de magneto-resistencia consiste en una película de Ferrita de Níquel separada por una capa suave magnética (Figura 1.8). La capa de NiFe cambia su resistencia en presencia de un campo magnético. Tiene capas de blindaje que protegen a este sensor de daños por campos magnéticos, en algunos casos este escudo también funciona como un polo del elemento de escritura dando lugar a una cabeza "*merged MR*".

El voltaje a través del sensor *MR* se expresa en la ecuación 1.4:

$$V_{RM} = I_{MR} * R_{MR} \tag{1.4}$$

Donde la resistencia R_{MR} varía como función del campo magnético en la región del sensor.

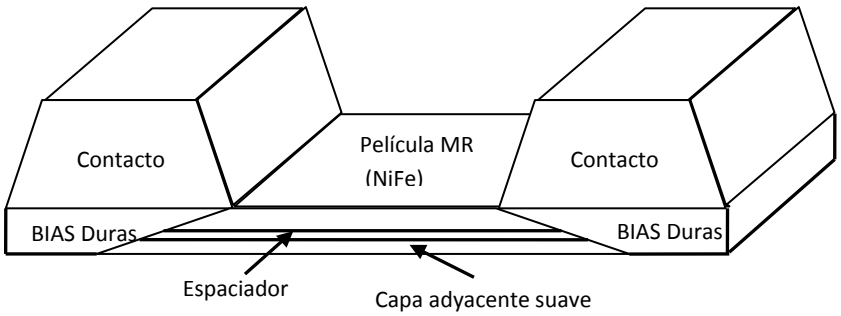


Figura 1.8. Cabeza de lectura MR. Obtenido de (Mueller, 2010).

b) ***Magneto-Resistencia-Gigante*** **(GMR)**

Esta cabeza es más pequeña que las MR pero su nombre radica por el efecto en el cual está basado, el diseño es similar al de las cabezas MR pero tiene 2 películas separadas por una delgada capa de cobre conductor, que reemplazan a la capa de NiFe (Figura 1.9).

La estructura de la cabeza GMR tiene una capa de separación de un metal no magnético entre dos capas de metales magnéticos. Una de estas capas magnéticas está fijada, lo que significa que tiene una orientación magnética forzosa, mientras que la otra es libre, es decir que es libre de cambiar de orientación. Los materiales magnéticos tienden a alienarse en la mima dirección, si la capa de separación es muy delgada la capa libre toma la misma orientación que la capa que la cubre. Se descubrió que la alineación magnética de la capa magnética libre puede periódicamente dar vueltas de un lado a otro para pasar de estar alienada en la misma dirección magnética (relativamente baja resistencia) que la capa que la cubre a ser alienada en la dirección magnética opuesta (relativamente alta resistencia) [12].

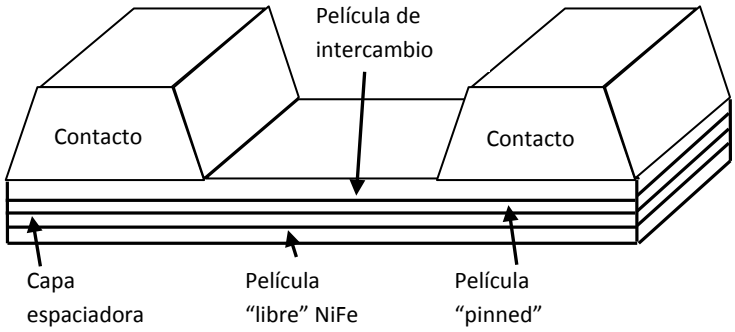


Figura 1.9. Cabeza de lectura GMR. Obtenido de (Mueller, 2010).

Slider

El *slider* es el elemento sobre el cual están montadas las cabezas de lectura y escritura, este elemento es el que flota sobre el plato. Los *sliders* utilizados en los DDEs actualmente son muy pequeños por los que se les llaman *slider femto* o *pico*. Los *sliders* pequeños reducen la masa que transporta el extremo del brazo montado sobre el *head-stack*, el cual proporciona mayor aceleración o desaceleración lo que lleva a tiempos de búsqueda más rápidos.

En los *sliders* convencionales el *flying height* varia de acuerdo a la velocidad de los platos que giran bajo los *sliders*, y la velocidad es mayor en la parte del plato más alejada del

motor; este comportamiento no es deseado ya que al usarse "*zoned bit recording*" (método de formatear al DDE de tal forma que las pistas exteriores puedan contener más sectores que las interiores y con ello cada sector sea del mismo tamaño en todo el plato), lo que se busca es que el *flying height* sea uniforme en todo el plato giratorio para ello los *sliders* más nuevos tienen un diseño especial en la superficie (Figura 1.10). Un *slider Femto* tiene 3 aéreas distintas con cuerpo complejo diseñado para lograr un *flying height* uniforme así como mínimas perdidas de altura bajo condiciones de baja presión [8]. La forma de la superficie del *slider* permite que existan presiones positivas y negativas permitiendo el balance de la fuerza del *suspension* y del brazo del *head-stack*, con lo cual se logra la estabilidad y reducción de variación del *flying height*.

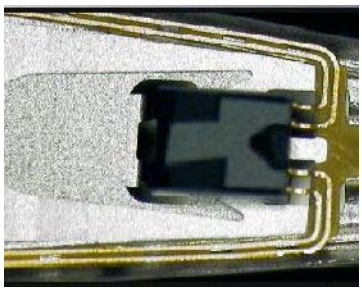


Figura 1.10. *Slider Femto.*

1.2.2.3. *Spindle* Motor

El motor que hace girar a los platos es el *spindle motor*, se le llama así porque está conectado al eje alrededor del cual giran los platos. Se conecta directamente y debe estar libre de ruido y vibraciones, para evitar que estos factores interrumpan las operaciones de lectura y escritura. Se alimenta con 12 volts. Se utilizan unas abrazaderas para sostener los platos al eje del motor, y se usan unos anillos anulares conocidos como "espaciadores" entre cada plato cuando hay más de un plato en el DDE.

La velocidad del *spindle motor* debe estar controlada con precisión, para ello usa un circuito de control con "bucle de retroalimentación" para monitorear y controlar dicha velocidad. Los platos giran en un rango de 3,600 rpm a 15,000 rpm dependiendo de si es IDE o SCSI. La variación en la velocidad puede afectar el rendimiento del DDE; un factor es el cambio en el *flying height*, si este varía afecta la densidad de bit, otro factor es que si la velocidad es

diferente durante el proceso de lectura y de escritura de bits, entonces la razón de bits mientras se lee difiere de la razón real en el cual fueron escritos (Figura 1.11).

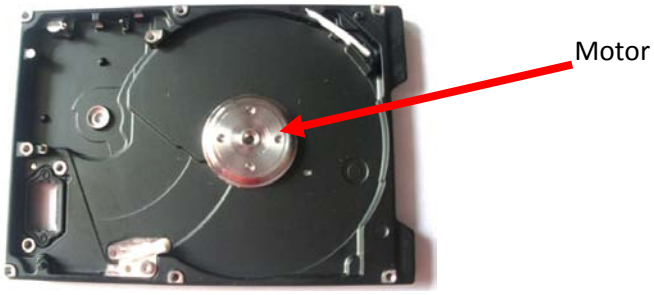


Figura 1.11. *Spindle Motor*

Los DDE usaban motores de *ball bearing* pero al incrementar la capacidad se requirió cambiar de tecnología, la solución fue usar un nuevo tipo de rodamiento llamado *Fluid Dynamic Bearing* (FDB)*;* el cual usa un fluido lubricante de alta viscosidad. Este motor permite mejor resistencia a los sobresaltos, mejora el control de velocidad y reduce la generación de ruido (hasta 20dBA). La mayoría de los DDE actualmente usan motores *FDB* y en algunos diseños de estos DDE se ha logrado disminuir el ruido acústico hasta 4dBA.

En los motores con *ball bearing* existen contactos mecánicos entre el *ball* y el *race* del rodamiento, pero no es posible hacerlos perfecto y libres de defectos. Cualquier contacto con esos defectos inherentes que se encuentran en la geometría de la interfaz del *race ball* y la capa de película lubricante, se producen movimientos laterales en el eje del motor y por tanto en los platos, como dichos movimientos son aleatorios y no sincronizados con la rotación, no pueden ser modelados y compensados, a estos movimientos se les conoce como *Non-Repeatable RunOut* (NRRO). El NRRO es el mayor contribuidor del *Track Mis-Registration* (TMR) que es el error entre la posición de la cabeza de lectura y el centro del *track* cuando el servomecanismo de posicionamiento de cabeza trata de seguir a un *track*. Con el motor de *ball bearing* el NRRO es de un rango de 0.1 micropulgadas. El motor FDB tiene un NRRO con rango de 0.01 micropulgadas [18].

1.2.2.4. Mecanismo posicionador *Head Actuator*

El sistema mecánico que se encarga de controlar el movimiento de las cabezas sobre los platos para ubicarlos sobre el cilindro deseado, es el *head actuator*.

Durante los años 1980 a 1990 se utilizaban los *actuator* "*Stepper motor*", pero al incrementar la densidad de área, este sistema dejo de ser viable, por lo que los DDE actualmente usan un sistema llamada *Voice Coil Motor* (VCM) *Actuator*, el cual fue desarrollado por *IBM* en 1965 [5].

Voice Coil Motor* (VCM) *Actuator

Un VCM *Actuator* trabaja con fuerza electromagnética. El mecanismo está construido en forma similar a una bocina de audio, de ahí el nombre de *voice coil*. En una bocina de audio se usa un imán inmóvil alrededor del *voice coil* al cual está conectado el cono de papel de la bocina. La energización de la bobina causa que se mueva en forma relativa al imán inmóvil, el cual produce sonido desde el cono. En el DDE el VCM *Actuator* tiene una bobina suspendida en el campo magnético producido por un par de imanes permanentes fijados al *case* base del DDE (Figura 1.12). La bobina suspendida es libre de moverse a través de un área restringida (de 0 a 30°). Cuando una corriente pasa a través de una bobina, la atracción o repulsión entre los imanes provoca que la bobina se mueva (esto debido a la Ley de Faraday). El brazo del *actuator* esta unido a la bobina de tal forma que al mover la bobina se mueve el *actuator*. El brazo del *actuator* esta hecho de aluminio del espesor necesario para sostener a las cabezas, una extensión de dicho brazo es conocido como suspensión, sobre el cual está montado el *slider,* en el cable que esta sobre el brazo del *actuator*, se encuentra un Circuito Integrado (CI) preamplificador. Este sistema es más preciso y silencioso que un "*stepper motor*".

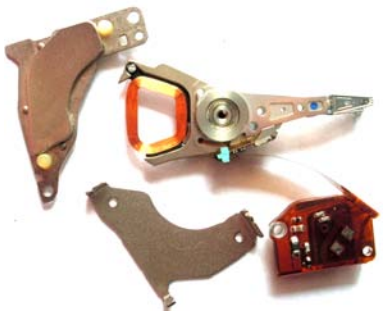


Figura 1.12. Elementos del VCM *Actuator*.

El VCM *Actuator* usa un mecanismo de guía llamado *servo*, para indicarle al *actuator* donde están las cabezas en relación a los cilindros y posicionar las cabezas exactamente en la posición deseada. Este sistema de posicionamiento es llamado mecanismo "*closed loop feedback*". Trabaja mediante el envío de la señal del índice (o *servo*) al posicionamiento electrónico, el cual regresa una señal de retroalimentación que es usada para posicionar las cabezas con precisión.

a) Servo Mecanismo

Un servo mecanismo controla el posicionamiento de forma precisa de las cabezas sobre un cilindro dado. A través de los años han existido tres diseños de servo mecanismo para los DDE (*Wedge Servo, Embedded Servo, Dedicated Servo*) [16], la información para realizar dicha función esta usualmente en una forma especial de un código llamado *gray code* – sistema especial de notación binaria, en el cual cualquier dos números adyacentes son representados por un código que difiere en sólo un lugar de *bit* o posición de columna. Este sistema permite que las cabezas fácilmente lean la información y rápidamente determinen su posición exacta. Para grabar el servo en los platos se utiliza una maquina llamada *servowriter* y es realizado al momento de la fabricación, por lo que no es posible sobreescribir el *servo* incluso con un formato a bajo nivel. Los DDEs actualmente usan el tipo *Embedded.*

b) Recalibración térmica y disk sweep

La mayoría de DDEs con VCM *Actuator* usan un procedimiento de recalibración térmica en intervalos predeterminados mientras están corriendo, esto se hace para eliminar errores de posicionamiento. Este procedimiento implica la búsqueda de cabezas desde el cilindro 0 a algún otro cilindro, una vez por cada cabeza del disco. Mientras esta secuencia ocurre, el circuito de control monitorea cuantas veces la posición del *track* ha sido movida desde la última vez que fue ejecutada la secuencia, y un ajuste de recalibración termina se calcula y almacena en la memoria del disco. Esta información es usada cada vez que el disco posiciona las cabezas para asegurar la exactitud más posible de posicionamiento. La mayoría de los DDEs ejecutan una secuencia de recalibración térmica cada 5 minutos para los primeros 30 minutos a partir de que el disco se ha encendido y cada 25 minutos

posteriormente. La recalibración termina es escondida por el DDE, de tal forma que los procesos de lectura y escritura no se vean alterados.

Algunos DDEs que realizan el procedimiento de calibración térmica también ejecutan una función llamada *disk sweep* o *wear leveling.* Este procedimiento se realiza cuando el DDE ha estado en modo *idle* por un periodo. La función *disk-sweep* mueve las cabezas hasta un cilindro en la porción más alejada del *spindle motor*, ya que es la posición donde la velocidad es mayor y por tanto el *fly height* es más grande; en caso de que el DDE continúe en este modo por otro periodo, entonces las cabezas se mueven a otro cilindro de esta misma área, y este proceso continua mientras el DDE se encuentre encendido pero en modo idle. Esta función fue diseñada por WD para proteger a las cabezas y a la *media* del desgaste o daños que pudieran sufrir al permanecer por un periodo largo en un mismo cilindro. La desventaja de esta función es que se genera ruido durante el movimiento de las cabezas, y este ruido se puede confundir con incorrecto funcionamiento del DDE.

CI Preamplificador

El circuito de preamplificación es parte del Mecanismo posicionador *Head Actuator*, el cual está montado sobre un cable de datos flexible como se muestra en la Figura 1.13. Se le conoce como *preamp.* Es el CI controla las cabezas y las señales que vienen y van hacia ellas.

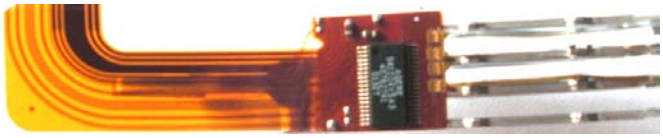


Figura 1.13. CI Preamplificador.

El CI *preamp* se localiza dentro del HDA ya que las señales que utilizan las cabezas son muy tenues y tiene más de 1GHz de frecuencia, así se evita que dichas señales se pierdan al viajar hacia la PCB. El DDE envía señales de control al *preamp* y este selecciona la cabeza que el DDE necesite en ese momento. El DDE tiene seis contactos por cabeza: una es tierra, dos son para los elementos de lectura y escritura, dos son *microactuators* (dispositivos especiales piezoeléctricos o magnéticos que mueven o rotan al slider, ayudan a colocar las cabezas bajo el *track* deseado) y el último contacto es "*heater*" (para ajustar el *fly height*).

1.2.3. *Printed Circuit Board* (PCB)

La PCB contiene a los elementos electrónicos que hacen funcionar al DDE, y se pueden categorizar de acuerdo a su función [5]:

- Para leer/escribir, se les conoce como “canales electrónicos”.
- Para controlar la rotación de los platos y el posicionamiento de las cabezas de lectura/escritura, se les conoce como “canales Servo”.
- Para controlar las operaciones de lectura/escritura de datos, transferencia de datos entre el DDE y el host, es el “control del disco”.
- Para funcionar como interface con el sistema host.
- Memoria: ROM, RAM.

La posición de los elementos así como su existencia varia, de acuerdo a cada fabricante y a cada modelo de DDE. En la Figura 1.14 se muestran dos tarjetas de las marcas *Seagate* y *WD* respectivamente.

Figura 1.14. a) PCB de DDE Seagate b) PCB de DDE marca *WD*.

1.2.3.1. Unidad Microcontroladora

El CI más grande (normalmente), es la unidad microcontroladora (MCU), usualmente consiste de una Unidad Central de Procesamiento, que se encarga de realizar todos los cálculos y es el canal de unidad especial de lectura/escritura, el cual convierte la señal analógica de las cabezas en señal digital, durante el proceso de lectura y codifica la información digital en señal analógica cuando el disco necesita escribir. La MCU tiene puertos de entrada salida, para controlar todo en la PCB y transmitir datos a través de su

interface. En la Figura 1.15 se muestran varios CI MCU para marcas de DDE: *Hitachi, Maxtor y Seagate*; respectivamente de izquierda a derecha.

Figura 1.15. MCU en DDEs de varias marcas.

1.2.3.2. *Firmware*

El área de *Firmware* o área de sistema, es un espacio dedicado para que los DDE almacenen: logs del SMART (*Self Monitoring Analysis and Reporting Technology*), tabla de reasignación de defectos, código de programa, etc. Una parte del *firmware* se encuentra ubicada en la superficie de los platos (en este parte del *firmware* usualmente se guarda el password del DDE).

La otra parte del *firmware* se encuentra en el CI que está en la PCB. Este *firmware*, es el que deja saber al DDE como operar apropiadamente y como leer datos de los platos. Parte de su función es de almacenar información acerca de cuantas cabezas contiene el disco, y como acceder al microcódigo para un exitoso "arranque". Esta información es colocada en la PCB al momento de su fabricación, y es programada de forma muy específica para el DDE en particular para el que fue diseñado.

El CI flash almacena parte del *firmware*. Cuando se aplica poder a un DDE, el CI MCU lee el contenido del CI flash dentro de la memoria y comienza el código. Sin ese código el DDE no puede iniciar. Si no existe el CI flash en la PCB, significa que está localizado dentro del MCU.

1.2.3.3. Memoria

El CI de memoria, es una memoria DDR SDRAM (*Double Data Rate , Synchronous Dynamic Random Access Memory*), son módulos de memoria RAM compuestos por

memorias síncronas, encapsuladas en DIMMs (*Dual In-line Memory Modules*, módulo de memoria en línea doble). El tamaño de la memoria define el tamaño de la cache del DDE, así si el disco tiene una memoria DDR de 32MB, teóricamente significa que el cache será de 32MB. Aunque en realidad el CPU ocupa algo de esta memoria para almacenar módulos del *firmware.* En la Figura 1.16 se muestra el CI de memoria en DDE *Hitachi* y *Toshiba*, respectivamente de izquierda a derecha.

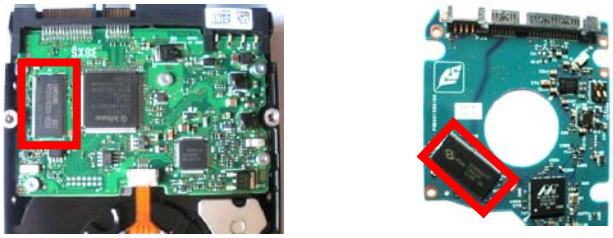


Figura 1.16. CI de Memorias en DDEs *Hitachi* y *Toshiba.*

1.2.3.4. Controlador VCM y *Spindle* Motor

Este CI es el que consume más poder, ya que controla la rotación del *spindle motor*, y el movimiento de las cabezas. El núcleo del controlador VCM puede trabajar a temperatura de 100°C/212°F [19]. La Figura 1.17 muestra el CI de control para VCM y *Spindle motor* de un DDE *WD* y *Maxtor*.

Figura 1.17. Controlador de VCM y *Spindle Motor* de DDE W.D. y Maxtor.

1.2.3.5. *Shock sensor* y *Diodo Transient Voltage Suppression*

El *shock sensor* puede detectar *shocks* excesivos aplicados a un DDE y enviar una señal al controlador VCM. Este controlador, inmediatamente estaciona las cabezas, y

algunas veces detiene la rotación del disco. Esto ayuda a proteger al disco de algún daño, pero no es una garantía. Normalmente se tienen dos sensores de *shock.*

Otra protección es el *diodo Transient Voltage Suppression* (diodo TVS). Protege a la PCB de altos voltajes provenientes de la fuente de poder. Cuando el diodo TVS detecta una subida en el voltaje crea un corto circuito entre el conector de poder y la tierra. Normalmente hay dos diodos TVS en cada PCB para protección de 5V y 12V.

1.3. Estructura lógica de los DDEs

La información es almacenada en cada lado del plato del DDE. La escritura de la información se logra mediante la alternación de la polaridad de la corriente en la bobina de la cabeza de escritura. Como el plato se encuentra girando y las cabezas están en un punto sobre este, la corriente de escritura magnetiza un camino circular.

1.3.1. Organización lógica

Un DDE almacena la información en *tracks* y sectores. Las cabezas leen y escriben los datos en anillos concéntricos llamados *tracks*, los cuales están divididos en segmentos llamados sectores, que contienen normalmente 512 bytes cada uno. Para localizar a los sectores en la superficie del plato, son etiquetados con un número de identificador, cada bloque de datos es asignado con un una dirección lógica de bloque (*Logical Block Address* – LBA), que comienza en 0 y termina en el numero apropiado de acuerdo a la capacidad entera del DDE.

Esta dirección de bloque no es adecuado para un acceso a bajo nivel, para este tipo de accesos se usa número de cabeza, número de cilindro y numero de sector asignado a cada LBA. Cada *track* se divide en sectores usando un patrón de escritura magnético especial para cada disco, este se realiza desde su fabricación. Cada *tracks* contiene un número de segmentos iguales. La alineación idéntica de *tracks* en cada lado de cada plato, juntos forman un cilindro (Figura 1.18).

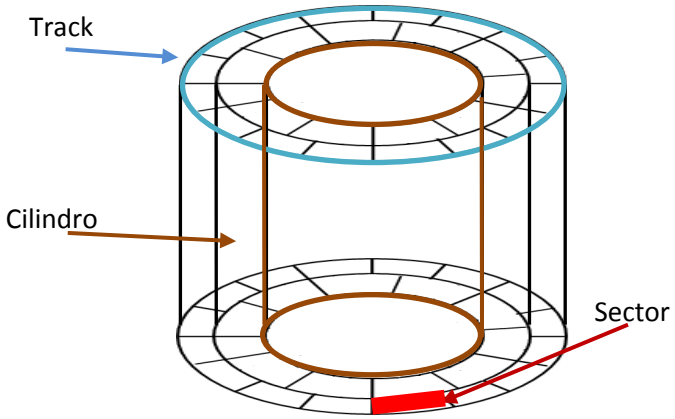


Figura 1.18. Track, cilindros y sectores.

Algunos términos respecto a la organización lógica de los DDE, son [5]:

- Track de datos: Son *tracks* concéntricos circulares en el plato donde cada *bit* binario es almacenado de forma secuencial.
- Track Pitch: Distancia entre 2 *tracks* adyacentes.
- Densidad de Track: Es el inverso del Track Pitch. Es decir el número de *tracks* en una unidad de longitud del radio del plato.
- Densidad de Bit: Número de *bits* grabados por unidad de longitud de un *track*, definido en unidades de *Bits* por Pulgada (*Bits per Inch* - BPI).
- Densidad de Área: Número de *bits* almacenados por unidad de área de la superficie del plato. Es equivalente al producto de densidad de Track y Densidad de Bit; es definido en unidades de *bits* por pulgada cuadrada.
- Tiempo de búsqueda: Es el tiempo que toma el servomecanismo de posicionamiento de cabeza para mover las cabezas de un *track* a otro.
- Tiempo promedio de búsqueda: El tiempo de búsqueda exacto depende de la longitud de la búsqueda, es decir la diferencia entre el *track* inicial y el *track* destino. El tiempo promedio de búsqueda es un promedio del tiempo de búsqueda de todas las posibles longitudes de búsqueda.
- Latencia: el proceso de lectura/escritura no es iniciado inmediatamente después de posicionar la cabeza sobre el *track* destino, ya que la locación exacta del *track* puede no estar bajo la cabeza en ese momento. La lectura/escritura debe esperar antes de que el sector deseado esté disponible, a esta espera se le llama latencia.

- Promedio de latencia: Cada proceso de recuperación de datos tiene diferente latencia. El promedio de latencia es el tiempo igual a la mitad del tiempo requerido para una revolución del plato.
- Tiempo de Acceso: Es el tiempo requerido para recuperar un bloque de datos del plato y es igual a la suma del tiempo de búsqueda y el promedio de la latencia.

1.3.2. Estructura de los datos

Los datos almacenados en los platos del DDE, tienen una estructura, de tal forma que puedan ser interpretados por el sistema.

1.3.2.1. *Master Boot Record*

El Registro Principal de Arranque (*Master Boot Record* - MBR) es el primer sector físico del DDE; cilindro 0, cabeza 0, sector 1 su tamaño es de 512 bytes. Contiene el código de inicio. Se conoce como Sector Principal de Arranque, ya que el Sistema Operativo (SO) lo utiliza para iniciarse. Cuando se inicia el Sistema, el código de inicio en el MBR es cargado automáticamente por el BIOS *(Basic Input/Output System)* y este a su vez se encarga de buscar dentro del mismo MBR la tabla de particiones y ubicar cuál de ellas está marcada como "booteable", para pasarle el control, que se ejecute y cargar el SO.

El esquema del sector MBR se muestra en la tabla 1.2. Los valores de dirección están expresados en código hexadecimal vistos con un editor hexadecimal. Los valores de firma, offset y contenido se visualizan con un editor hexadecimal en "*little endian*", aquí se expresan en "*big endian*" (ejemplo 0xaa55).

Tabla 1.2. Esquema del sector Master Boot Record.

No. de bytes	Dirección	Contenido
440	0000h - 01B7h	Gestor de arranque
4	01B8h - 01BBh	Firma del disco (opcional)
2	01BCh - 01BDh	Usualmente nulos (0x0000)
64	01BEh - 01FDh	Tabla de particiones
2	01FEh - 01FFh	Firma de fin se sector (0xaa55)

Dentro de la sección de *Tabla de Particiones*, pueden existir hasta 4 registros de particiones, cada uno de 16 bytes. La estructura de cada registro se muestra en la tabla 1.3.

Tabla 1.3. Estructura del registro de una partición.

No. de bytes	Offset	Contenido
1	0x00	Bandera de Estado. • 0x80 - indica "booteable" activo • 0x00 - indica no "booteable" • Otro valor - invalido
3	0x01 - 0x03	Dirección del primer sector de la partición , formato CHS (Cylinder, Head, Sector) [1]
	• 0x01	Cabeza
	• 0x02	Sector
	• 0x03	Cilindro
1	0x04	Tipo de partición (los más comunes se muestran en la tabla 1.4)
3	0x05 - 0x07	Dirección del último sector de la partición, formato CHS
	• 0x05	Cabeza
	• 0x06	Sector
	• 0x07	Cilindro
4	0x08 - 0x0B	Primer sector de la partición en formato LBA (Logical Block Address) y "Little indian"
4	0x0C – 0x0F	Número de sectores de la partición, en formato "Little indian"

[1] Los campos están limitados a 1024 cilindros, 255 cabezas y 63 sectores. Si una dirección CHS es demasiado larga para almacenarla, se usan los valores (1023,254,63).

Tabla 1.4. Tipos de particiones más comunes.

Valor	Desarrollador	Descripción
0x00	--	Partición vacía
0x01	Microsoft	DOS, FAT 12
0x04	Microsoft	FAT 16 <32Mb
0x05	Microsoft	Extendida
0x06	Microsoft	FAT 16
0x07	Microsoft	HPFS/NTFS
0x0b	Microsoft	Windows 95 FAT 32
0x0c	Microsoft	Windows 95 FAT 32 (LBA)
0x0e	Microsoft	Windows 95 FAT 16 (LBA)
0x0f	Microsoft	Windows 95 FAT 16 Extendida
0x11	Microsoft	Escondida - FAT 12
0x12	Compaq	Diagnóstico de Compaq
0x14	Microsoft	Escondida - FAT 16
0x82	--	Linux swap space
0x83	--	Cualquier Sistema de Archivos Nativo Linux
0xda	--	Raw data (sin Sistema de Archivos)
0xdf	TeraByte Unlimited	BootIt

Obtenido de (Carrier, 2005).

En la sección *Tabla de particiones* del MBR existe espacio hasta para cuatro particiones, cuando se requieren crear más de cuatro, se podrán crear de una a tres particiones principales y una extendida, la *partición extendida* ocupara el resto del disco, dentro de la *partición extendida* se podrán crear *particiones secundarias*, o incluso *particiones secundarias extendidas*. Dentro de esta última se podrán crear más *particiones secundarias extendidas*, hasta agotar el espacio del disco [20].

Una *partición primaria* es una partición cuya entrada se encuentra en el MBR y contiene un Sistema de Archivos (SAs) u otra estructura de datos.

Una *partición extendida* es una partición cuya entrada está en el MBR y contiene particiones adicionales, cuyas entradas estarán en un Extended Boot Record EBR (Registro de arranque extendido).

Una *partición secundaria extendida* es una partición cuya entrada se encuentra en un EBR y contiene particiones adicionales.

Una *partición secundaría* es una partición cuya entrada se encuentra en un EBR y contiene un sistema de archivos u otra estructura de datos.

La estructura de un EBR se muestra en la tabla 1.5. Es similar a la estructura del MBR, excepto que no tiene el código de gestor de arranque ni el identificador de disco.

Tabla 1.5. Estructura de un EBR.

No. de bytes	Dirección	Contenido
446	0000h - 01BDh	Vacío
64	01BEh - 01FDh	Tabla de particiones
2	01FEh - 01FFh	Firma de fin de sector (0xaa55)

La sección de *tabla de particiones* tiene la misma estructura que la mostrada en la tabla 1.3, excepto que el número del sector inicial de la partición está conformado por el número que indica la tabla de particiones en el offset 0x08 - 0x0B más el número del sector donde está ubicada la *partición extendida* o *partición secundaría extendida*.

Para la *Tabla de particiones* el número de sector de inicio y número de sectores totales de la partición, los valores están en "*Little indian*" y abarcan 4 bytes, en la Figura 1.19 se muestra el valor 0x0000003f" encerrado en color rojo para el sector de inicio y el valor 0x037dff40

encerrado en color verde para el número total de sectores en la partición, para convertir estos valores a sistema decimal, ver anexo 1.

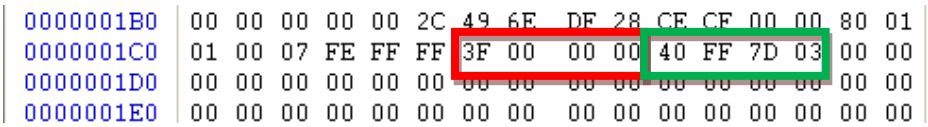


Figura 1.19. Valores en la tabla de particiones.

1.3.2.2. Sistema de Archivos

El sistema de archivos es un método para almacenar y leer datos en un dispositivo de almacenamiento, proporcionan un mecanismo para que los usuarios almacenen datos en jerarquía de archivos y directorios (dependiendo el sistema de archivos). Un SA estructura los datos de tal forma que el sistema sabe dónde encontrarlos. Normalmente el SA es independiente de cualquier equipo especifico, la mayoría de SO manejan su propio SA. Los SA tradicionales proveen métodos para crear, mover, renombrar y eliminar archivos o directorios.

Sistema de archivos FAT32

FAT (*File Allocation Table*) es un sistema de archivos de los más simples ya que tiene un número pequeño de tipos de estructura de datos. Fue el primer sistema de archivos de Microsoft DOS y Windows 9X, actualmente es frecuentemente utilizado en memorias para cámara digital y USB “thumb drives”. Hay dos importantes estructuras de datos: FAT (Fat Allocation Table) y entradas de directorios.

Hay tres diferentes versiones de FAT: FAT12, FAT16 y FAT32. La mayor diferencia entre ellas es el tamaño de las entradas en la estructura FAT. Actualmente la más usada es FAT32.

El concepto básico del sistema de archivos FAT32 es que cada archivo y directorio es asignado en una estructura de datos, llamada entrada de directorio, que contiene el nombre del archivo, el tamaño, inicio de la dirección del contenido del archivo y otros metadatos (datos sobre el archivo). El contenido del archivo y directorio es almacenado en unidades de datos llamados *clusters* (para FAT32 el tamaño es de 4Kb). Si un archivo es almacenado en

más de un *cluster*, el otro *cluster* es encontrado usando la estructura llamada FAT. La estructura FAT es usada para identificar al siguiente *cluster* en un archivo y es también usada para identificar el estado de asignación del *cluster*. La Figura 1.20 ejemplifica la relación entre las estructuras de directorio, *clusters* y estructura de FAT.

A cada *cluster* se le asigna una dirección, la primera dirección del primer *cluster* es dos. No hay *clusters* con direcciones cero y uno. Los *clusters* son alojados en la región del área de datos del sistema de archivos, no en el área reservada para el Sector de arranque o FAT's.

El tamaño máximo para un archivo en este sistema de archivos es de 4GB (2^{32}-1 bytes). El soporte FAT32 en Windows 2000/XP está limitado a DDE de 32GB para la instalación, pero no al uso, ya que se puede acceder a discos de hasta 2 Terabytes.

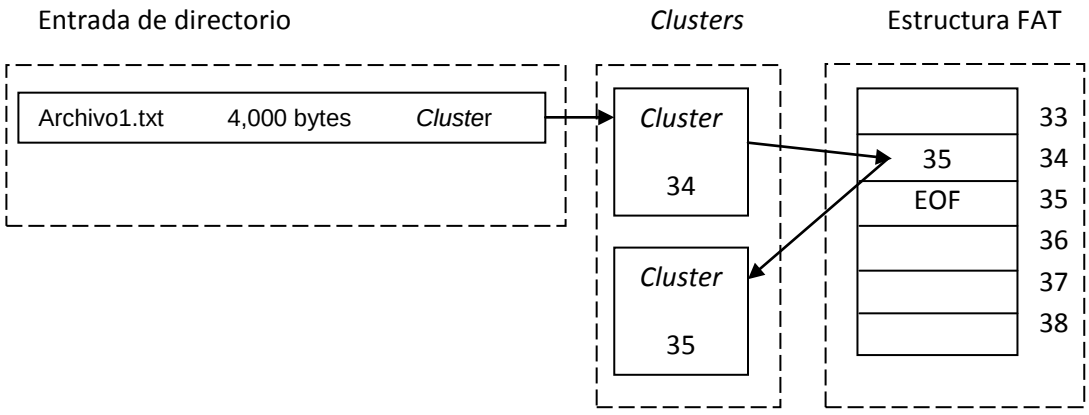


Figura 1.20. Relación entre entradas de directorio, *clusters* y estructura FAT.

FAT32 cuenta con cuatro secciones como se muestra en la Figura 1.21: Sector de arranque (Boot Sector), área de FAT's (Primer FAT/ Segunda FAT, donde la segunda FAT es copia de la primer FAT), área de directorio raíz y el área de datos.

Figura 1.21. Secciones del sistema de archivos FAT32.

Sector de Arranque

El Sector de arranque (Boot Sector) está alojado en el primer sector del sistema de archivo y contiene información de la partición. La estructura del Sector de Arranque se muestra en la tabla 1.6. Existe una copia del sector de arranque, en el sector 6. Las direcciones están expresadas en código hexadecimal vistas con un editor hexadecimal. Y los valores de firma, offset y contenido se visualizan con el editor hexadecimal en "*little endian*", aquí se expresan en "*big endian*".

Tabla 1.6. Estructura del Sector de Arranque FAT32.

# de bytes	Dirección	Contenido
3	0000h - 0002h	Instrucción de salto
8	0003h - 000Ah	Nombre de OEM en ASCII
2	000Bh - 000Ch	Bytes por sector (valores como 512,1024,2048 y 4096)
1	000Dh - 000Dh	Sectores por *cluster* (valores en potencia de 2, tamaño máximo 32Kb)
2	000Eh - 000Fh	Tamaño del área reservada (en sectores)
1	0010h - 0010h	Número de FAT's (normalmente 2)
2	0011h - 0012h	Número máximo de archivos en el Directorio Raíz
2	0013h- 0014h	Valor de 16-bit de números de sectores en el sistema de archivos.
1	0015h - 0015h	Tipo de dispositivo (para fijo 0xf8 y para removible 0xf0)
2	0016h - 0017h	Tamaño de 16 bits en sectores de cada FAT. (para FAT32 - es 0)
2	0018h - 0019h	Sectores por track
2	001Ah - 001Bh	Número de cabezas
4	001Ch - 001Fh	Número de sectores antes del inicio de la partición
4	0020h - 0023h	Valor de 32 bits de número de sectores en el sistema de archivos.
4	0024h - 0027h	Tamaño de 32 bits en sectores de una FAT
2	0028h - 0029h	Define cuantas estructuras múltiples de FAT son escritas
2	002Ah - 002Bh	La mayor o menor número de versión
4	002Ch - 002Fh	El *cluster* donde el directorio raíz se encuentra
2	0030h - 0031h	Sector donde la estructura del FSINFO se encuentra
2	0032h - 0033h	Sector donde el respaldo de la copia del Sector de Arranque es localizado (por default es 6)
12	0034h - 003Fh	Reservado
1	0040h - 0040h	Número de dispositivo BIOS INT13
1	0041h - 0041h	No usado
1	0042h - 0042h	Firma de boot extendido para identificar si los siguientes 2 valores son validos. La firma es 0x29
4	0043h - 0046h	Número de serie de volumen, algunas versiones de Windows calculan este valor basado en la fecha y hora de creación
11	0047h - 0051h	Etiqueta de volumen en ASCII. El usuario escoge este valor al crear el sistema de archivos
8	0052h - 0059h	Tipo de etiqueta del sistema de archivos en ASCII. El valor estándar es "FAT32", pero no es requerido
420	005Ah - 01FDh	No usado

# de bytes	Dirección	Contenido
2	01FEh - 01FFh	Valor de firma de fin de sector (0xaa55)

Obtenido de (Carrier, 2005) adaptación por el autor.

FAT32 FSINFO

El sistema de archivos FAT32 tiene una estructura FSINFO que incluye información acerca de dónde puede el sistema operativo alojar nuevos *clusters.* Es el sector siguiente al Sector de Arranque. La tabla 1.7 muestra la estructura del sector FSINFO.

Tabla 1.7. Estructura del Sector FSINFO en una partición FAT32.

No. de bytes	Dirección	Contenido
4	0200h - 0203h	Firma (0x41615252)
480	0204h - 03E3h	No usado
4	03E4h - 03E7h	Firma (0x61417272)
4	03E8h - 03EBh	Número de *clusters* libres
4	03ECh-003EFh	Siguiente *cluster* libre
12	03F0h - 003FBh	No usado
4	03FCh - 03FFh	Firma 0xaa55

Obtenido de (Carrier, 2005) adaptación por el autor.

FAT'S

La FAT tiene dos propósitos dentro del sistema de archivos FAT: se usa para determinar el estado de asignación de un *cluster*, y para encontrar los *clusters* asignados a un archivo o directorio. Típicamente hay 2 FAT's pero el número real así como el tamaño, está indicado en el Sector de Arranque de la partición FAT. La segunda FAT esta seguida de la primer FAT.

Las tablas consisten en un número de entradas iguales en tamaño y no tienen valores de encabezado o de terminación, cada entrada consiste de 4 bytes. El tamaño de las FAT's depende del sistema de archivos y de la versión. El direccionamiento de las entradas comienza en 0 y cada entrada corresponde al *cluster* con la misma dirección. Si un *cluster* no está asignado tendrá el valor 0. Si está asignado, contendrá la dirección del siguiente *cluster* en el archivo o directorio. Si se trata del último *cluster* del archivo o directorio el valor contenido indicará el final (para FAT32 es un valor mayor a 0x0ffffff8), en caso de que el *cluster* este dañado y no pueda ser asignado, el valor contenido en la FAT deberá ser 0x0ffffff7 para FAT32. El funcionamiento de la FAT se ejemplifica en la Figura 1.22.

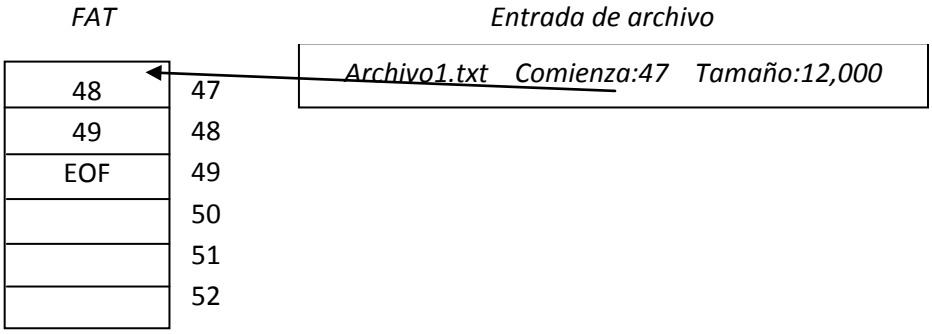


Figura 1.22. Ejemplificación de la FAT.

Entradas de Directorios

Las entradas de directorios contienen el nombre y los metadatos de los archivos o directorios. Se tiene una entrada de directorio por cada archivo o directorio. La estructura de esta entrada se indica en la tabla 1.8. Esta estructura de datos, soporta un nombre de 8 caracteres, y la extensión de 3 caracteres. Si el nombre del archivo es más grande será necesaria una entrada de directorio para nombre largo. Debido a que el campo del tamaño del archivo es de 4 bytes el tamaño máximo para un archivo es de 4GB [21].

Tabla 1.8. Estructura de entrada de directorio.

No. de bytes	Contenido
1	Primer carácter del nombre de archivo en ASCII estado de asignación (0xe5 o 0x00 si no es alojado)
10	Caracteres 2 al 11 del nombre de archivo en ASCII
1	Atributos del archivo (ver tabla 8)
1	Reservado
1	Hora de creación (decimas de segundo)
2	Hora de creación (hora, minutos y segundos)
2	Día de creación
2	Día de acceso
2	2 bytes altos de la primer dirección de *cluster*
2	Hora de escritura (hora, minuto y segundos)
2	Día de escritura
2	2 bytes bajos de la primer dirección de *cluster*
4	Tamaño de archivo (para directorios es 0)

Obtenido de (Carrier, 2005).

Los valores para las banderas de atributos se indican en la tabla 1.9.

Tabla 1.9. Lista de banderas de atributos.

Valor de bandera (bits)	Descripción
0000 0001	Sólo lectura
0000 0010	Archivo escondido
0000 0100	Archivo de sistema
0000 1000	Etiqueta de volumen
0000 1111	Nombre largo de archivo
0001 0000	Directorio
0010 0000	Archivo

Obtenido de (Carrier, 2005).

Entrada de directorio de nombres largos de directorio

Esta estructura es usada cuando los nombres de los archivos o directorios ocupan más de ocho caracteres, y cada entrada normal tendrá adicionalmente una entrada LFN (*Long File Name),* esta entrada precederá a la entrada normal, la estructura se muestra en la tabla 1.10.

Tabla 1.10. Estructura de entrada de directorio LFN.

No. de bytes	Contenido
1	Número de secuencia (ORed con 0x40) y estado de asignación (0xe5 si no está asignado)
10	Caracteres de nombre de archivo 1-5 (en Unicode)
1	Atributos de archivo
1	Reservado
1	Suma de comprobación
12	Caracteres del nombre de archivo 6-11 (en Unicode)
2	Reservado
4	Caracteres de nombre de archivo 12-13 (en Unicode)

Obtenido de (Carrier, 2005).

Sistema de archivos NTFS

NTFS (*New Technologies File System*) es un sistema de archivos diseñado por Microsoft, utilizado para Windows NT/2000/XP/Vista/7, etc. Fue diseñado para la confiabilidad, seguridad y soporte de dispositivos de gran almacenamiento.

Los datos importantes son almacenados en archivos, incluyendo el sistema de archivos básico de administración de datos ($Boot, $MFT, $Bitmap, etc.). El SA es considerado como un área de datos y cualquier sector puede ser asignado a un archivo [21].

Consta de 2 elementos importantes, el primero es el Sector de arranque, que se encuentra ubicado como primer sector del volumen, contiene información sobre el propio volumen y código de inicio. Una copia de este sector se encuentra al final de la partición (Figura 1.23). El segundo elemento importante son las *Master File Tables* (MFT) que son el corazón del volumen, contienen información sobre todos los archivos y directorios. Existe una copia de los primeros 4 registros de la MFT, y se encuentra ubicada acorde al tamaño de la partición.

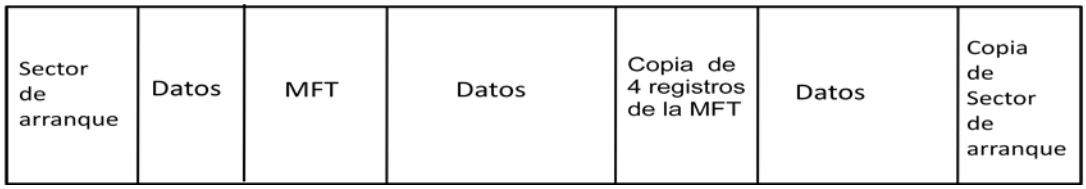


Figura 1.23. Estructura de una partición NTFS.

Sector de Arranque

Cuando se formatea un volumen con NTFS, se asignan los primeros 16 sectores en el archivo $Boot. El primer sector es un Sector de arranque con un código de "bootstrap" (proceso de inicio) y los siguientes 15 sectores son el IPL (*Initial Program Loader*). Para incrementar la confiabilidad del SA el último sector de la partición NTFS contiene una copia del Sector de arranque. El sector de arranque se compone de 6 secciones importantes (tabla 1.11).

Tabla 1.11. Secciones del sector de arranque NTFS.

No. de bytes	Dirección	Contenido
3	0000h - 0002h	Instrucción de salto
8	0003h - 000Ah	ID de OEM
73	000Bh - 0053h	Parámetros del bloque BIOS
426	0054h - 01FDh	Código de Bootstrap
2	01FEh - 01FFh	Firma de fin de sector (0xaa55)

Obtenido de (Carrier, 2005) adaptación por el autor.

La instrucción de salto es hacía el IPL. El ID de OEM es la cadena que indica con que herramienta fue realizado el SA. Los parámetros del bloque BIOS (tabla 1.12), describen la geometría de la partición. El código de Bootstrap es el programa que localiza la memoria y la carga; posteriormente ejecuta el código de inicio de la partición.

Tabla 1.12. Parámetros del bloque BIOS.

No. de bytes	Offset	Contenido
2	0x00	Bytes por sector, normalmente el valor es 512
1	0x02	Sectores por *cluster*
2	0x03	Sectores reservados
3	0x05	Reservado – siempre 0x00
2	0x08	No usado
1	0x10	Tipo de Media
2	0x11	Reservado – siempre 0x00
2	0x13	Sectores por Track
2	0x15	Número de cabezas
4	0x17	Sectores escondidos
4	0x21	No usado
4	0x25	No usado
8	0x29	Total de sectores en la partición
8	0x37	*Cluster* inicial del $MFT
8	0x45	*Cluster* inicial del $MFTmirr
4	0x53	Cluster por FRS (File Record Segment)
4	0x57	*Cluster* por bloque de Index
8	0x61	Número de serie del volumen
4	0x69	Suma de comprobación

Obtenido de (Carrier, 2005).

Parte del trabajo del IPL es de localizar e iniciar el NTLDR, para lo cual requiere leer la MFT y localizar al índice (directorio) raíz, donde encontrará la entrada del NTLDR y leerá los segmentos de registro del archivo NTLDR y lo cargará a la memoria y saltará hacía esta.

Master File Table

La MFT contiene información acerca de todos los archivos y directorios. Cada archivo y directorio tiene al menos una entrada en esta tabla. Las entradas utilizan 1Kb pero sólo los primeros 42 bytes tienen un propósito, los demás bytes son atributos de almacenamiento que tienen propósitos específicos. Algunos atributos son usados para almacenar el nombre del archivo. A las entradas en la tabla, se les llama “registro de archivos”, y a cada una se le

da una dirección basada en su ubicación, comenzando con 0. El tamaño de cada entrada es definido en el Sector de Arranque. MFT es un archivo, como todo lo es en una partición NTFS. Utiliza *clusters* al igual que las FAT's en el sistema de archivos FAT32 [21].

Microsoft reserva las primeras 16 entradas de la MFT para archivos con información del sistema de archivos, la primer entrada es para la propia MFT. Si las entradas reservadas no son usadas sólo contienen información básica y genérica (tabla 1.13). La MFT comienza lo más pequeña posible, pero se expande a medida que se van requiriendo más entradas. Cuando los atributos de un archivo no caben en una sola entrada, se usan múltiples entradas. Si esto ocurre, la primer entrada es llamada "registro de archivo base" o "entrada de MFT base" y cada entrada subsecuente contiene la dirección de la entrada base.

Tabla 1.13. Archivos de metadatos del sistema de archivos NTFS.

Entrada	Nombre del archivo	Descripción
0	$MFT	Entrada de la MFT
1	$MFTmIRR	Respaldo de la primer entradas en la MFT
2	$LogFile	El diario que registra las transacciones de los metadatos
3	$Volume	Información del volumen
4	$AttrDef	Información de los atributos
5	-	El directorio raíz del sistema de archivos
6	$Bitmap	Estado de asignación de cada *cluster* en el sistema de archivos
7	$Boot	El sector de arranque y código de arranque
8	$BadClus	Los *cluster*s que tienen sectores dañados
9	$Secure	Información de la seguridad y control de acceso de los archivos
10	$Upcase	La versión *Uppercase* para cada carácter Unicode
11	$Extended	Un directorio que contiene archivos para extensiones opcionales.

Obtenido de (Carrier, 2005).

Las entradas de las MFTs pueden contener como atributo el contenido del archivo, siempre y cuando este no sea mayor de 700 bytes, y se le llamara "atributo residente". Cuando el archivo es más grande, se convierte en una entrada con atributo "no residente" y se salvará el contenido del archivo en un *cluster* externo. La entrada correspondiente a dicho archivo tendrá las direcciones de la ubicación del archivo. La tabla 1.14 muestra la estructura de una entrada básica MTF. El valor de la firma estándar es "FILE" pero cuando se encuentra un error, la firma es "BAAD".

Tabla 1.14. Estructura de entrada básica MFT.

Rango de Byte	Contenido
0-3	Firma (“FILE”)
4-5	Offset para corrección de arreglos
6-7	Número de entradas en arreglo
8-15	Número de secuencia $LogFile (LSN)
16-17	Valor de secuencia
18-19	Conteo de vinculo
20-21	Offset del primer atributo
22-23	Bandera (en uso y directorio)
24-27	Tamaño usado de la entrada MTF
28-31	Tamaño asignado de la entrada MFT
32-39	Referencia de archivo para el registro de base
40-41	ID del siguiente atributo
42-1023	Valores de atributos y corrección

Obtenido de (Carrier, 2005).

RESUMEN

En este capítulo se describieron los elementos físicos que conforman al DDE, y cómo interactúan entre ellos para poder almacenar la información, mediante campos magnéticos, en los platos que son diseñados para tal fin, esta lectura/escritura se realiza mediante dos cabezas, también se describió la tecnología que se maneja en dichos elementos, y la que todavía se puede encontrar en DDE que existen en el mercado. Asimismo se explicó, el funcionamiento lógico, es decir, a nivel de datos como se logra tener acceso al DDE y poder guardar y recuperar la información en forma de archivos. Se describieron los elementos para el Sistema de archivos NTFS y FAT32.

Capítulo 2. CLASIFICACIÓN DE LOS DAÑOS LÓGICOS Y SU POSIBLE SOLUCIÓN

Los daños en los DDEs pueden tener diferentes causas, que originan la pérdida de datos. En este capítulo se estudian a aquellos denominados como lógicos; se revisarán las causas, la forma en que afectan a la información y se propondrán soluciones. Finalizando con una tabla concreta de los principales daños y las posibles soluciones.

2.1. Tipos de daños lógicos y sus causas

Se dice que un DDE tiene un daño lógico, cuando la estructura física funciona de forma correcta, pero no así la lógica, ocasionando que la información sea no accesible. Un daño lógico puede ser también originado de un daño físico.

Como se explicó en el capítulo 1, se debe contar con el MBR y el sistema de archivos para poder almacenar, organizar y recuperar la información, en caso de que estos elementos fallen, la información (aun cuando exista) no podrá ser accedida. La información por sí misma también puede sufrir daños, sin afectar la estructura. Y en algunos casos se puede dañar tanto la información como el MBR o el sistema de archivos.

A continuación se describirán los principales daños en los elementos de la estructura lógica que ocasiona la pérdida de datos parcial o total. Se usa el programa editor hexadecimal *Winhex* [22] para visualizar la estructura lógica del DDE.

2.1.1. Daño en el MBR/EBR

Dentro de los daños lógicos que pueden afectar al MBR son la alteración o destrucción del código. Estos puede ser ocasionados por:

- Código malicioso del tipo “virus de boot”.
- Falla de poder durante el proceso de escritura, ocasionando que las cabezas escriban en el MBR/EBR.
- Daño físico en el sector MBR/EBR impidiendo su lectura total o parcial.
- Alteración intencional del contenido de los campos o por errores en procesos de restauración de respaldos.
- Cambio en los parámetros de la partición mediante programas, como *diskmgmt.msc*.

Si el código de alguna de las secciones del MBR/EBR no se encuentra correctamente o simplemente no se encuentra, el SO contenido en el DDE no podrá “Iniciar” y los síntomas más comunes serán: un error indicando que el SO no existe, una pantalla azul con mensaje de error, o no ser reconocido como unidad lógica.

De la estructura del MBR en la tabla 1.2, sólo 2 de las 5 secciones (*tabla de particiones* y firma de fin de sector MBR) son importantes para el reconocimiento como unidad "*booteable*" o lógica por un SO externo o por algún programa, estas mismas secciones son importantes en el EBR.

Un SO es capaz de reconocer de forma lógica al DDE conectado como esclavo y a sus particiones aún cuando en el MBR:

1) La sección del gestor de arranque sea alterada o borrada (no será "*booteable*").
2) La firma del DDE sea alterada o borrada. Al conectarlo como esclavo, el SO automáticamente asignará un código.
3) La sección del código nulo (0x0000) contenga código.

2.1.1.1. Daño en la firma 0xaa55

La firma 0xaa55 del MBR/EBR indican el final del dichos sectores. En caso de que la firma no exista o sea alterada (Figura 2.1), el SO no es capaz de leer las tablas de particiones.

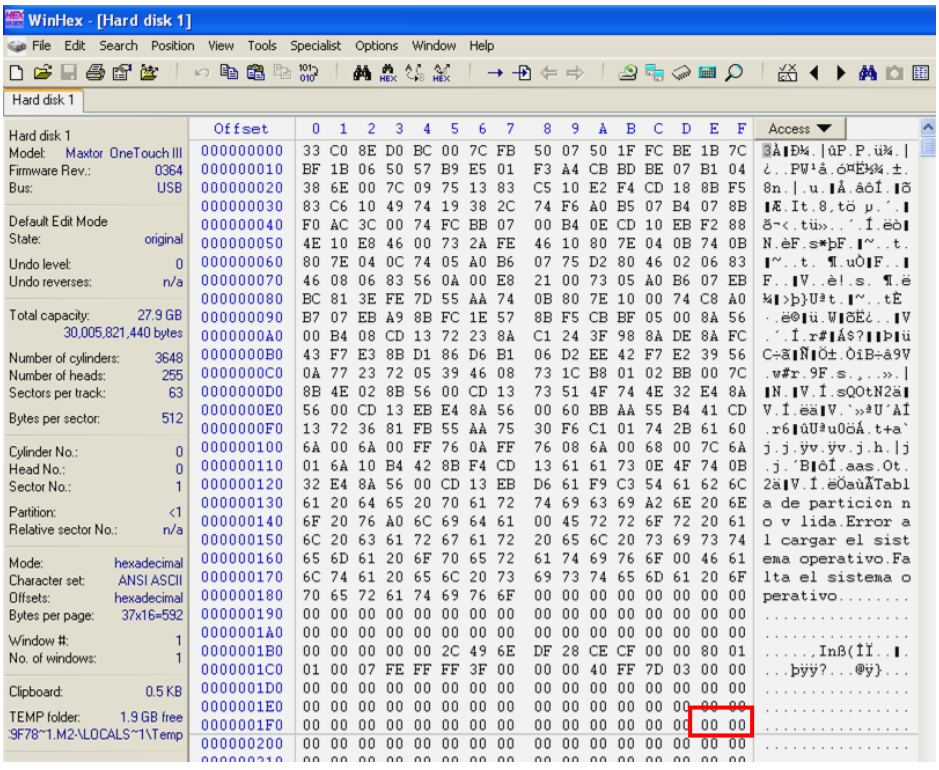


Figura 2.1. MBR sin firma, visualizado con el programa Winhex.

La visualización, con el programa *diskmgmt.msc,* de un disco duro que no contenga dicha firma se muestra en la Figura 2.2.

Figura 2.2. Disco duro sin firma de fin de sector MBR/EBR.

2.1.1.2. Daño en la Tabla de particiones

Si la tabla de particiones no existe (Figura 2.3) el DDE se mostrará en su totalidad como "*unallocated*" (Figura 2.4), y no podrá visualizarse la unidad lógica. El borrado de la tabla de particiones puede realizarse de forma manual (utilizando un editor hexadecimal), o mediante el programa interno del SO *diskmgmt.msc.*

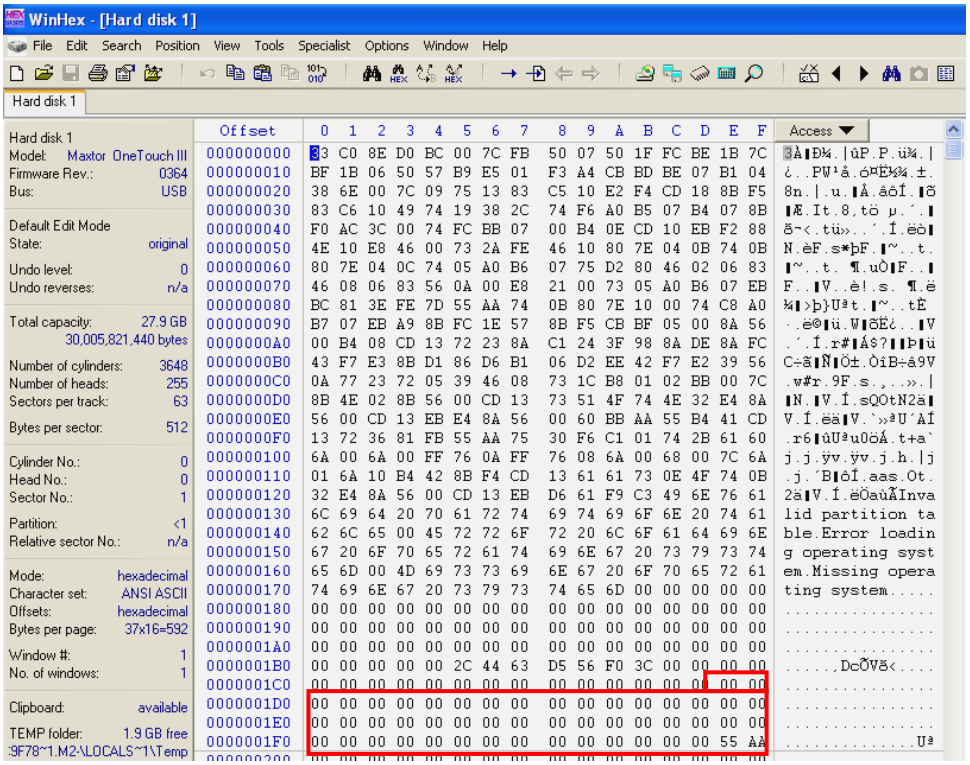


Figura 2.3. MBR sin la tabla de particiones, visualizado con Winhex.

Figura 2.4. Disco duro sin tabla de particiones, visualizado con diskmgmt.msc.

La tabla 2.1 muestra la consecuencia del daño en los campos de la tabla de partición.

Tabla 2.1. Daños y consecuencias en los campos de la tabla de partición.

Campo	Daño	Consecuencia
Bandera de estado	Código erróneo o nulo (0x00)	No afecta al funcionamiento como unidad lógica, sólo cuando es "*booteable*", en cuyo caso no iniciará el SO contenido en la partición
Dirección del primer sector de la partición (formato CHS)	Dirección errónea	No afecta el funcionamiento, ya que el Sistema se basa en la dirección en formato LBA
Tipo de partición	Tipo erróneo o nulo (0x00)	La unidad lógica no será reconocida
Dirección del último sector de la partición (formato CHS)	Dirección errónea	No afecta el funcionamiento, ya que el Sistema se basa en la dirección en formato LBA
Primer sector de la partición (formato LBA)	Valor erróneo	La unidad lógica será inaccesible
Número del total de en la partición	Valor erróneo	La unidad lógica será inaccesible

Si los valores en la *tabla de particiones* son alterados de forma manual, las unidades lógicas se mostrarán de acuerdo a dichos valores, pueden mostrarse de mayor o menor capacidad; pero no serán accesibles.

Si la modificación de las particiones se realizó con *diskmgmt.msc* (Figura 2.5) sin formatear las particiones, sólo se modifica la tabla de particiones correspondiente, el resto de estructura de la partición original como MFT permanecen intactas.

Figura 2.5. Modificación de los tamaños de particiones, sin formatear las unidades lógicas.

Si la partición que se crea es de tipo “extendida”, el primer sector de dicha partición se modificará únicamente agregando la firma 0xaa55 en la dirección 01FEh-01FFh. Si la partición que se crea es “primaria” la información que contenga el primer sector de dicha partición será borrada (llenado con código 0x00) y sólo contendrá la firma 0xaa55 en la dirección 01FEh-01FFh.

2.1.2. Daño en la estructura del Sistema de Archivos

El Sistema de Archivos presenta daño lógico cuando la información contenida en su estructura, ha sido alterada o borrada. Afectando con ello el funcionamiento del SO y por tanto el acceso a la información. Dentro de las principales causas que originan este tipo de daño, están:

- Código malicioso del tipo “virus de *boot”*.
- Falla de poder durante la escritura de archivos, ocasionando que las cabezas escriban en los campos de la estructura del SA.
- Alteración o borrado intencional del contenido en los campos.
- Cambio en los parámetros de la partición mediante programas, como *diskmgmt.msc*.
- Sectores dañados pertenecientes a la estructura del SA.

Los principales síntomas que se derivan de estos daños son: el SO no es capaz de iniciar, las unidades lógicas no son reconocidas o no pueden ser accedidas y pantallas con mensaje de error indicando que no existe SO de inicio.

2.1.2.1. Sistema de archivos FAT

Los elementos críticos para el funcionamiento del SA FAT32 son el Sector de arranque y las FAT’s, ya que en base al sector de arranque se identifica el inicio, el final y el tamaño de la partición, y en base a las FAT’s se identifica la ubicación física de cada archivo.

Sector de Arranque

El daño que puede sufrir un Sector de Arranque es la alteración o ausencia de código en los campos que lo conforman (acorde a la tabla 1.6), no todos ellos son críticos. La tabla 2.2 muestra a los campos críticos para el funcionamiento, así como la consecuencia en caso de que el código sea modificado o borrado.

Tabla 2.2. Campos críticos del Sector de Arranque FAT32.

#	Contenido	Crítico	Consecuencia
1	Instrucción de salto	Si	No permite el acceso a la unidad lógica, aunque es suficiente con que la primer posición tenga el valor “0xeb”
2	Bytes por sector (valores como 512,1024,2048 y 4096)	Si	No permite el acceso a la unidad lógica
3	Sectores por *cluster* (valores en potencia de 2, tamaño máximo 32Kb)	Si	
4	Tamaño del área reservada (en sectores)	Si	
5	Número de FAT’s (normalmente 2)	Si	No permite el acceso a la unidad lógica o el acceso es incorrecto mostrándose código ilegible en el directorio raíz
6	Número máximo de archivos en el Directorio Raíz (normalmente 0x00)	Si	Muestra código ilegible en el directorio raíz
7	Valor de 16-bit de números de sectores en el sistema de archivos.	Si	No afecta al funcionamiento como unidad lógica, sólo cuando es “*booteable*”, en cuyo caso no iniciará el SO contenido en la partición
8	Tipo de dispositivo (para fijo 0xf8 y para removible 0xf0)	Si	No permite el acceso a la unidad lógica si no contiene alguno de los dos valores: 0xf8 y 0xf0
9	Tamaño de 16 bits en sectores de cada FAT. (para FAT32 este campo es 0)	Si	Si tiene algún valor diferente de 0x00, la unidad lógica es inaccesible.
10	Sectores por track	Si	Con código 0x00 – no altera el funcionamiento. Con código diferente al correcto o a 0x00 – la unidad lógica no será accesible
11	Número de cabezas	Si	
12	Número de sectores antes del inicio de la partición	Si	
13	Valor de 32 bits de número de sectores en el sistema de archivos. (normalmente el valor es 0)	Si	No permite el acceso a la unidad lógica
14	Tamaño de 32 bits en sectores de una FAT	Si	
15	Define cuantos estructuras múltiples de FAT son escritas	Si	
16	La mayor o menor número de versión	Si	
17	El *cluster* donde el directorio raíz se encuentra	Si	

	Contenido	Crítico	Consecuencia
18	Número de dispositivo BIOS INT13	Si	No afecta al funcionamiento como unidad lógica, sólo cuando es *"booteable"*, en cuyo caso no iniciará el SO contenido en la partición
19	No usado	Si	No afecta al funcionamiento como unidad lógica, sólo cuando es "booteable", en cuyo caso no iniciará el SO contenido en la partición

En la figura 2.6 se indican los campos descritos en la tabla 2.2, en un sector de arranque visto con un editor hexadecimal.

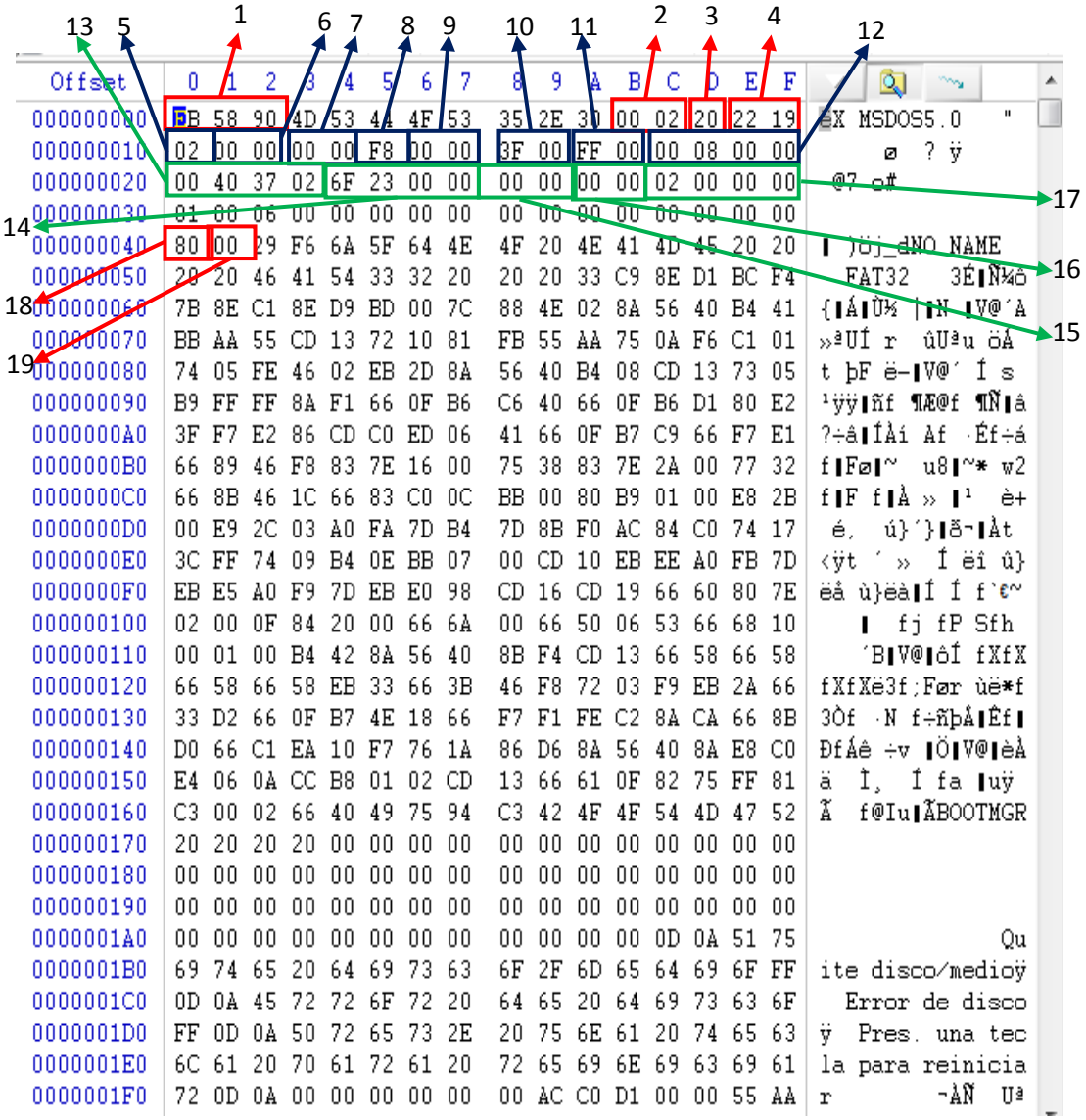


Figura 2.6. Campos críticos del Sector de arranque FAT32.

FAT's

Los daños que pueden sufrir una FAT o ambas, se describen en la tabla 2.3, así como su consecuencia.

Tabla 2.3. Daños de una FAT y sus consecuencias.

Daño	Consecuencia
Borrado total de la FAT1	La unidad lógica es visible, pero no es accesible
Borrado total de ambas FAT's	
Borrado de la FAT1 excepto el inicio: 0x0fffffff0fffffff7fffffff0ffffff8	La unidad lógica es visible, así como el contenido del directorio raíz, pero no se puede tener acceso a los archivos ni directorios
Borrado de ambas FAT's excepto el inicio 0x0fffffff0fffffff7fffffff0ffffff8	
Borrado total de la FAT2	No afecta, ya que el SA se basa en la FAT1 para su funcionamiento
Borrado parcial de la FAT2	
Alteración del contenido en la FAT2	
Borrado parcial de la FAT1	Los archivos serán visibles al igual que los directorios pero serán inaccesibles aquellos para los cuales las entradas en la FAT han sido borradas
Alteración del contenido en la FAT1	
Borrado parcial en ambas FAT's	Los archivos serán visibles al igual que los directorios pero serán inaccesibles aquellos para los cuales las entradas en las FAT's han sido borradas
Alteración del contenido en ambas FAT's	

La alteración de los campos en el sector FSINFO no afecta el funcionamiento del SA.

2.1.2.2. Sistema de archivos NTFS

Los elementos críticos para el correcto funcionamiento de NFTS son: Sector de arranque y MFT.

Sector de Arranque

Si este elemento sufre alteración en su contenido o borrado, tendrá diferentes consecuencias. Algunos campos no son críticos para el funcionamiento del SA, en otros casos dichas acciones tendrán consecuencias graves. La tabla 2.4 y 2.5 describen las secciones del Sector de Arranque y los parámetros del bloque BIOS (en base a la tabla 1.11 y 1.12 respectivamente) que son críticos y la consecuencia de sufrir alteración o borrado del contenido.

Tabla 2.4. Secciones del sector de arranque NTF y consecuencias de los daños.

#	Contenido	Consecuencia de daño
1	Instrucción de salto	No afecta el funcionamiento
2	ID de OEM	No se puede tener acceso a la unidad lógica
	Parámetros del bloque BIOS	Ver tabla 2.5
3	Código de Bootstrap	Es reconocido como unidad lógica pero no será "*booteable*"
4	Firma de fin de sector (0xaa55)	

Tabla 2.5. Parámetros del bloque BIOS y consecuencia de los daños.

#	Contenido	Crítico	Consecuencia de daño
5	Bytes por sector (normalmente el valor es 512)	Si	No permite el acceso a la unidad lógica
6	Sectores por *cluster* (normalmente 0x08)	Si	
7	Sectores reservados	Si	Si tiene algún valor diferente de 0x00, la unidad lógica es inaccesible.
8	Reservado – siempre 0x00	Si	
9	No usado	Si	
10	Tipo de Media	No	Es reconocido como unidad lógica pero no será *"booteable*"
11	Reservado – siempre 0x00	Si	Si tiene algún valor diferente de 0x00, la unidad lógica es inaccesible.
12	Sectores por *track*	No	Es reconocido como unidad lógica pero no será *"booteable*"
13	Número de cabezas	No	
14	Sectores escondidos	No	
15	No usado	Si	Si tiene algún valor diferente de 0x00, la unidad lógica es inaccesible.
16	No usado	No	Es reconocido como unidad lógica pero no será "*booteable"*
17	Total de sectores en la partición	Si	No permite el acceso a la unidad lógica
18	*Cluster* inicial del $MFT	Si	
19	*Cluster* inicial del $MFTmirr	Si	
20	Cluster por FRS (File Record Segment)	Si	
21	*Cluster* por bloque de Index	Si	

En la figura 2.7 se indican los campos descritos en la tabla 2.5, en un sector de arranque visto con un editor hexadecimal.

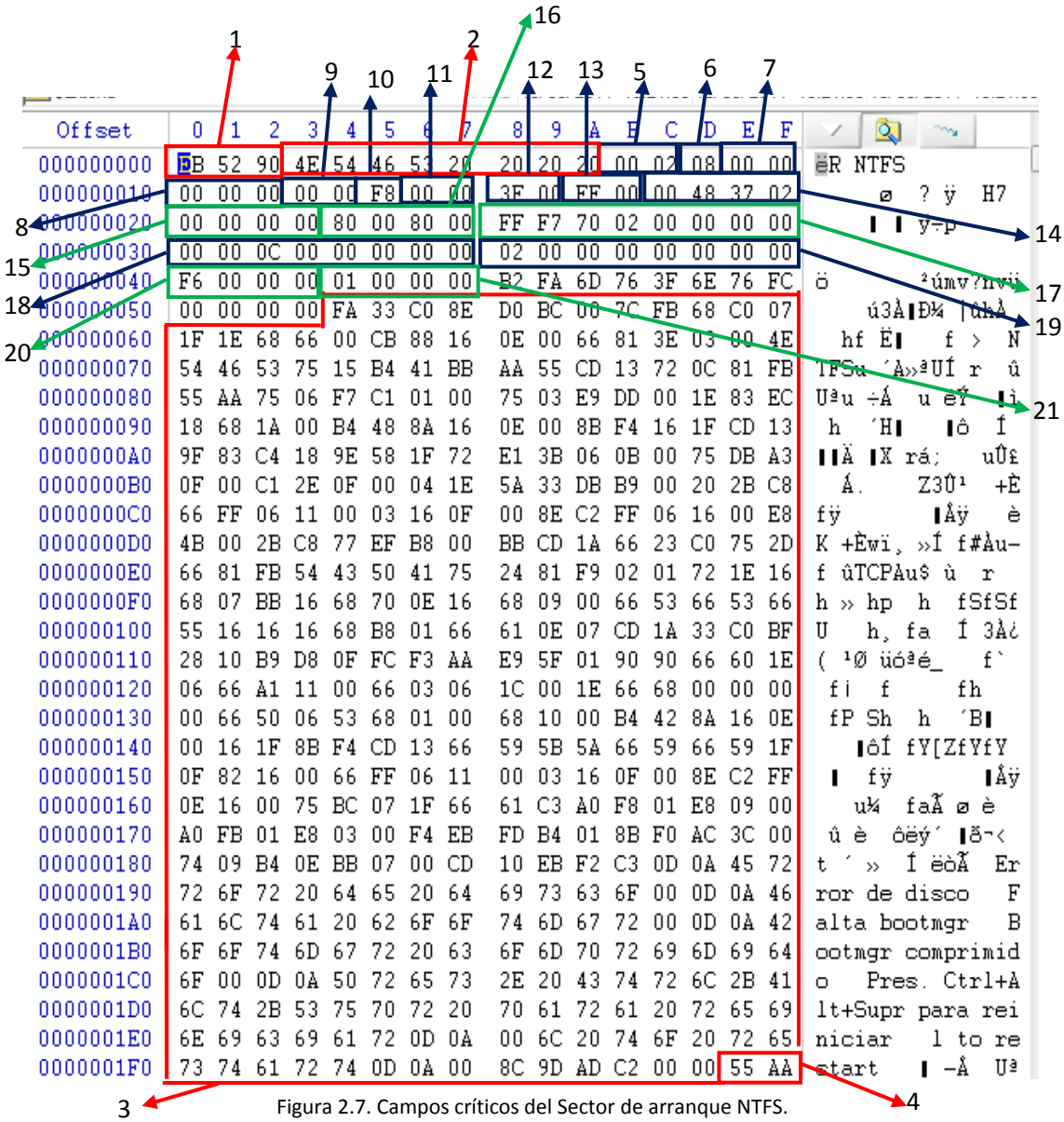


Figura 2.7. Campos críticos del Sector de arranque NTFS.

MFT

Los daños que pueden sufrir una MFT, se describen en la tabla 2.6, así como su consecuencia.

Tabla 2.6. Daños en la MFT y la consecuencia.

Daño	Consecuencia
Borrado total de la MFT	Los archivos y carpetas serán visibles, pero no se podrán acceder
Borrado parcial de la MFT	Los archivos y carpetas afectados serán visibles, pero no se podrán acceder
Alteración del contenido de la MFT	Los archivos y carpetas afectados serán visibles, pero no se podrán acceder

2.1.3. Archivos Borrados

Cuando se borra un archivo con un SO, el contenido de dicho archivo no se borra, el SA únicamente marca al archivo como borrado dentro de la entrada del directorio de archivos. Para cada SA de archivos la marca de borrado es diferente.

El archivo únicamente se borrará cuando su contenido sea sobreescrito con nueva información.

Las causas que pueden originar que un archivo sea borrado son las siguientes:

- Código malicioso como virus, que borre los nombres de archivos en las entradas de directorios.
- Falla de poder durante la escritura de archivos, ocasionando que las cabezas escriban en espacios ocupados por entradas de directorios.
- Errores humanos como borrado intencional o por accidente de los archivos.
- Sectores dañados pertenecientes a las entradas de directorios.
- Errores de software como la restauración errónea de respaldos que borran las entradas de los archivos en los directorios.

El síntoma común de los archivos borrados es que no son visibles dentro de los directorios.

2.1.3.1. FAT 32

Para el SA FAT32 los elementos que son modificados al borrar un archivo son los siguientes:

- Se modifica el nombre del archivo en la entrada de directorio. Se sustituye la primera letra del nombre por el código 0xe5. En la Figura 2.8 la ventana superior muestra la entrada de directorio antes de ser borrado, la ventana inferior después.

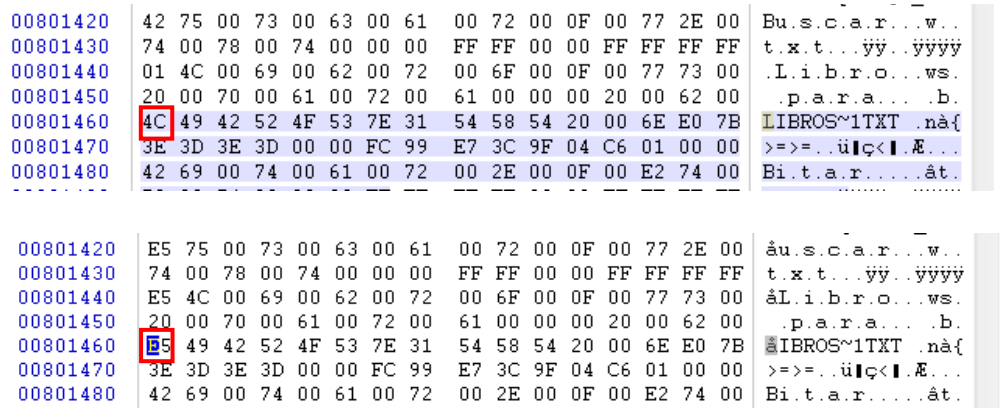


Figura 2.8. Comparación del nombre del archivo en la entrada de directorio.

- En las FAT's, las direcciones que indican los *clusters* que conforman al archivo, son sustituidas por 0x00. La Figura 2.9 muestra en la ventana superior a la primer FAT antes de borrar al archivo y la ventana inferior después.

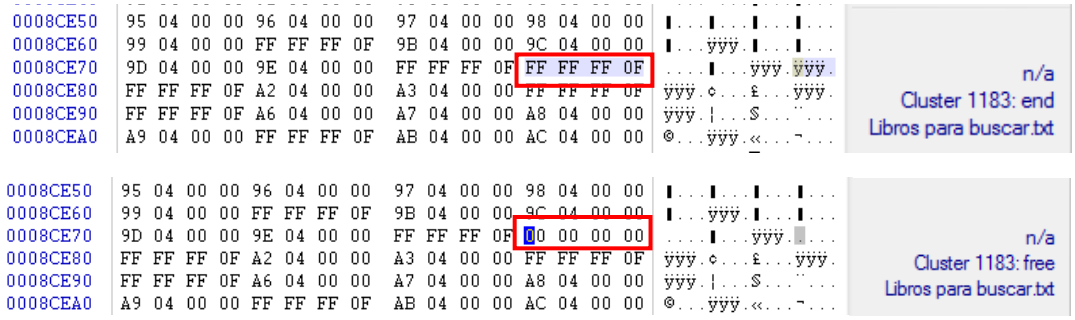


Figura 2.9. Comparación de la primer FAT antes y después de borrar un archivo.

2.1.3.2. NTFS

Como se mencionó en el capítulo 1, un archivo en SA NTFS puede ser almacenado como atributo residente de la entrada MFT o de forma externa a dicha estructura, los cambios que se realizan cuando se borra un archivo, son diferentes para ambas formas.

Para el SA NTFS cuando se borra un archivo, los cambios son los siguientes:

- El nombre del archivo LFN en la entrada MFT de la carpeta donde se ubica el archivo borrado también es borrado y sólo se conserva el "nombre corto". Esto sucede para ambas formas de almacenar al archivo. La Figura 2.10 muestra una comparación

cuando se borra el archivo, en la ventana superior el archivo existe de forma normal, en la ventana superior ha sido borrado.

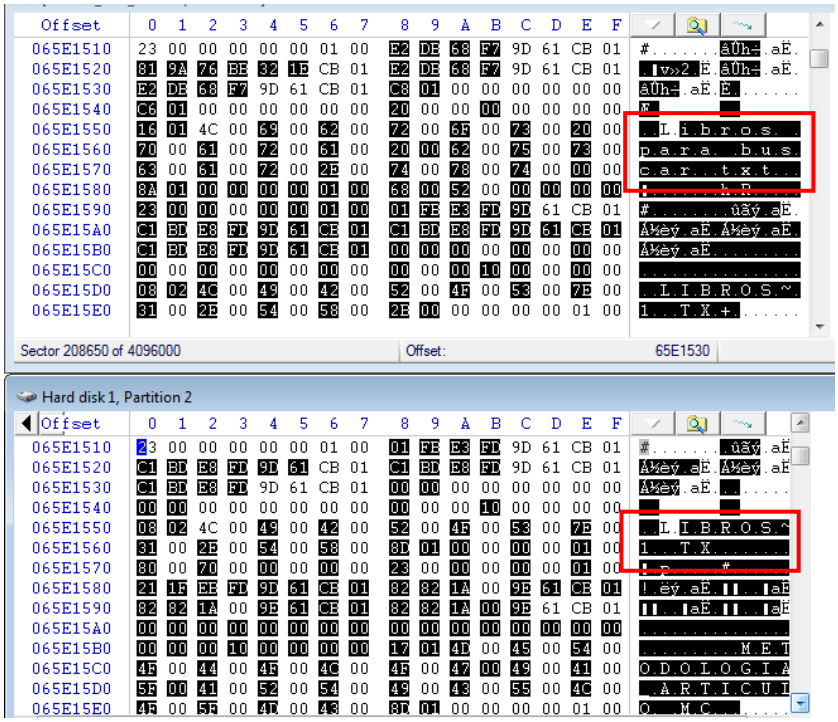


Figura 2.10. Comparación de la entrada MFT de un archivo borrado.

- Si el contenido del archivo está como atributo residente en la entrada de la MFT, el nombre se borra y la información permanece intacta. Si el archivo está como atributo no residente, el nombre del archivo en la entrada de la MFT no es afectada a menos que se vacié la papelera de reciclaje. La Figura 2.11 muestra la entrada MFT cuando el contenido del archivo está como atributo residente y dicho archivo ha sido borrado.

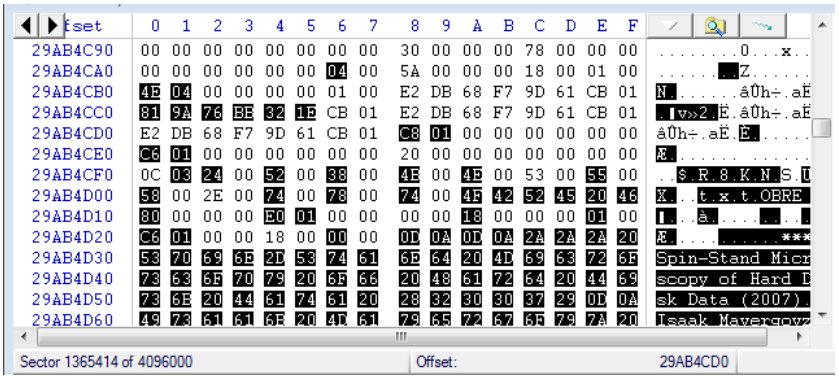


Figura 2.11. Entrada MFT con atributo residente.

La Figura 2.12 muestra el contenido de la papelera de reciclaje cuando el archivo es no residente.

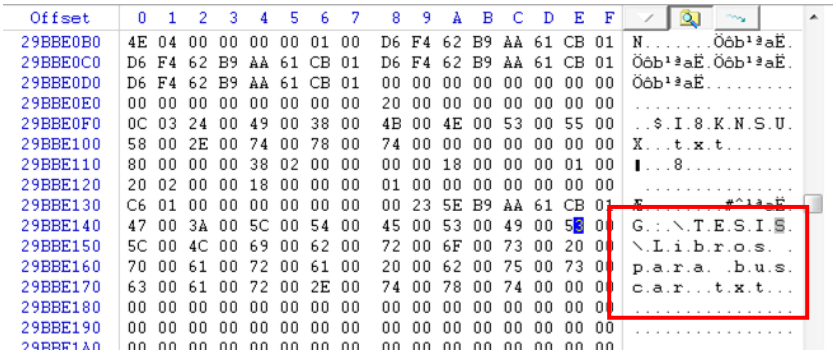


Figura 2.12. Contenido de la papelera de reciclaje.

La Figura 2.13 muestra la entrada MFT cuando tiene atributo no residente y el archivo ha sido borrado incluso de la papelera de reciclaje.

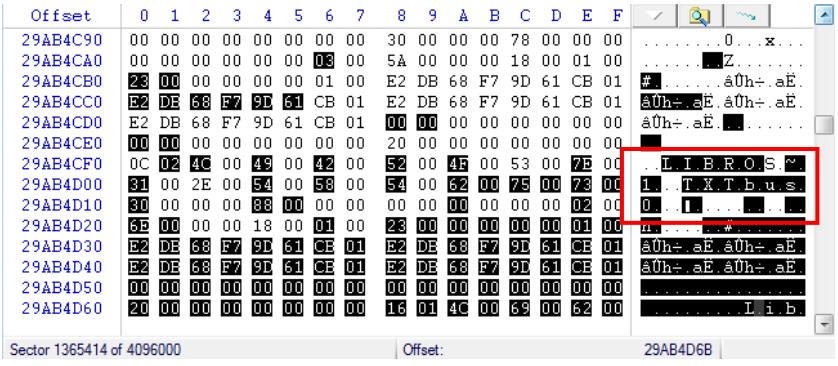


Figura 2.13. Entrada de la MFT cuando el archivo no residente ha sido borrado.

2.1.4. DDE Formateados

Existen 2 tipos de formateo para un DDE, el físico y el lógico. El físico consiste en dividir a los platos en sectores, este proceso se realiza desde su fabricación. El lógico consiste en implantar un SA que asigna sectores a archivos, esta asignación depende del SA.
Los SOs de Microsoft dan dos opciones para realizar el formateo lógico: rápido y completo. Al formatear de forma rápida al DDE o sólo una partición, la información de la estructura del SA es alterada, pero la información como contenido de archivos y entradas de directorios que no pertenecen al directorio raíz, son conservadas. Las unidades lógicas se muestran como nuevas, sin archivos ni directorios. Al realizar el formateo de forma completa, el borrado se hará tanto en la estructura del SA como en la información. Este borrado es de forma permanente ya que la información es sobreescrita con el patrón “0x00”.
La causa principal que ocasionan el formateo lógico de un DDE o de particiones, es el error humano, ya sea intencional o por accidente. Este último se da cuando no se tienen identificadas las posiciones de los DDEs dentro del sistema. Se detecta que una unidad lógica o DDE ha sido formateada porque la estructura del SA funciona correctamente pero el directorio raíz no contiene archivos ni directorios.

2.1.4.1. FAT 32

Los elementos de la estructura del SA de FAT32 que se modifican al formatear son:

1. El Sector de arranque: aquellos campos de la tabla 1.6 que estén relacionados con la fecha de creación. Como se muestra en la Figura 2.14, la ventana superior es el volumen antes del formateo y la ventana inferior es el volumen después del formateo.

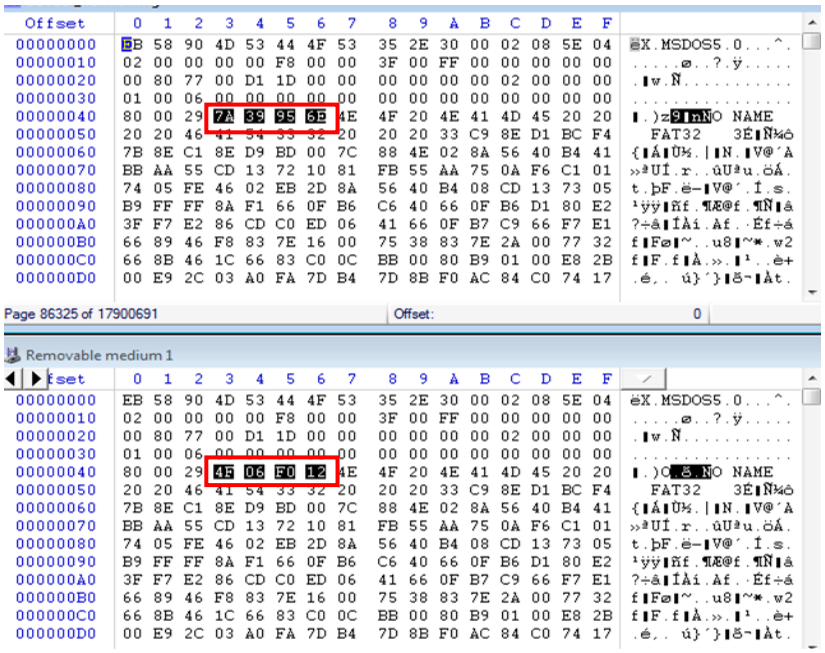


Figura 2.14. Comparación del Sector de Arranque.

2. El sector FSINFO, en el campo del número de *clusters* libres. La Figura 2.15 muestra el cambio.

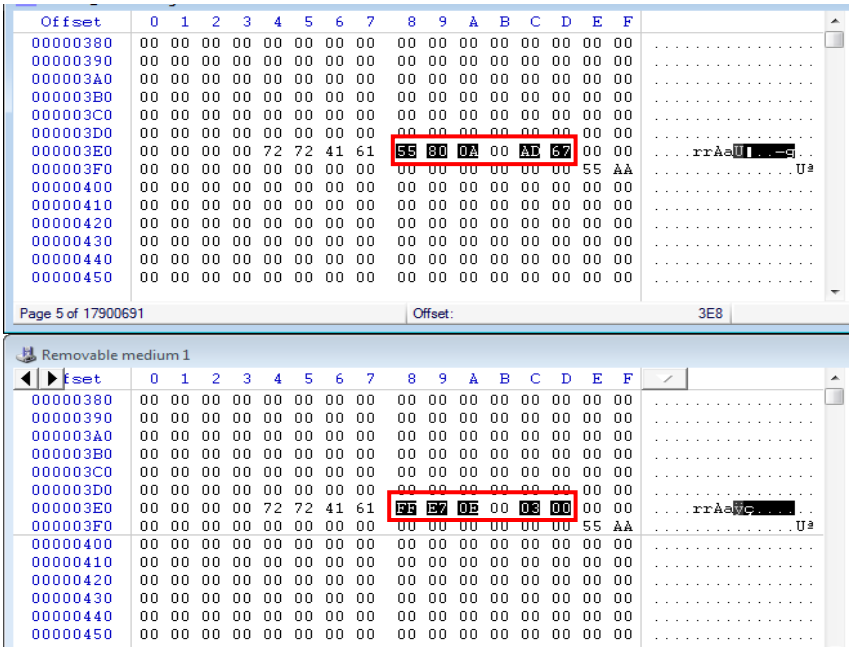


Figura 2.15. Comparación del Sector FSINFO.

3. Las FAT's son borradas. La Figura 2.16 muestra la comparación de la primer FAT. La ventana superior es antes del formateo y la inferior después.

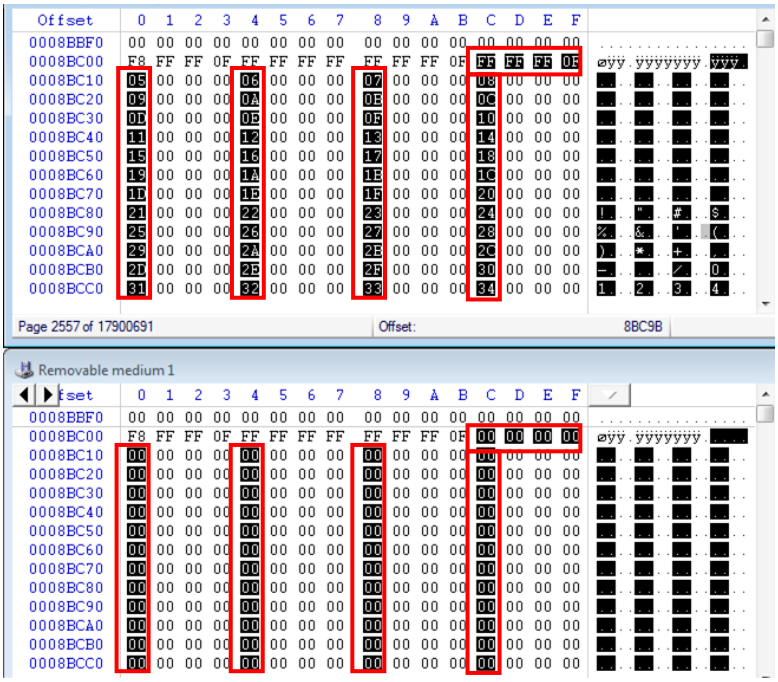


Figura 2.16. Comparación de la primer FAT.

4. El Directorio Raíz es borrado, como se muestra en la Figura 2.17.

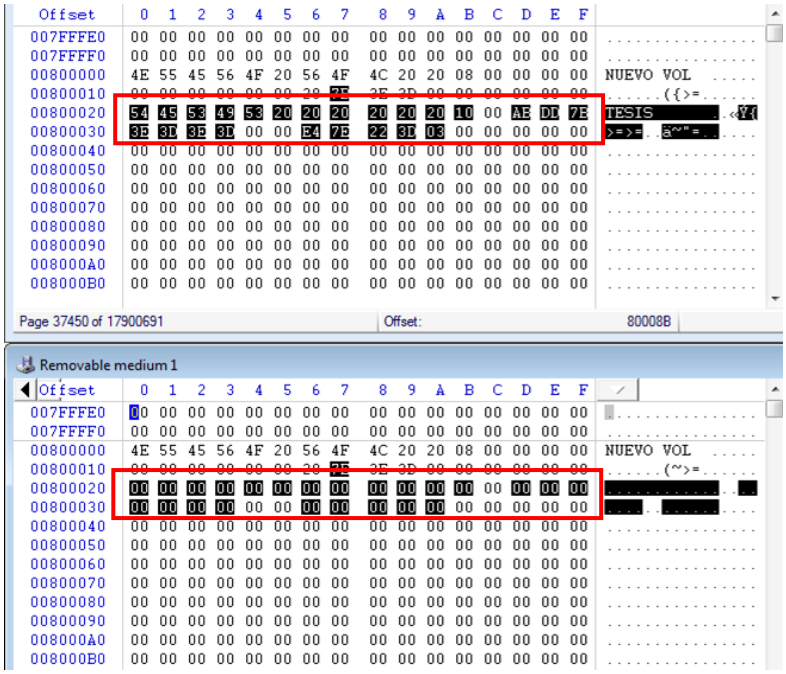


Figura 2.17. Comparación del directorio raíz.

2.1.4.2. NTFS

Los elementos de la estructura del SA de NTFS que se modifican son:

1. El Sector de arranque: aquellos campos de la tabla 1.11 y 1.12 que estén relacionados con la fecha de creación. Como se muestra en la Figura 2.18, la ventana superior es el volumen antes del formateo y la ventana inferior es el volumen después del formateo.

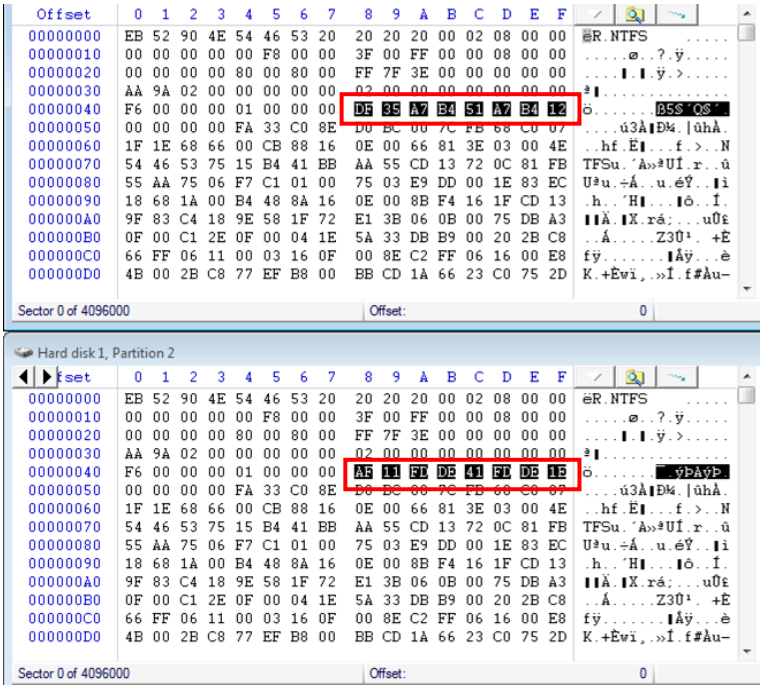


Figura 2.18. Comparación del Sector de arranque.

2. Las primeras 4 entradas de la entrada MFT. La Figura 2.19 muestra la comparación de la primer entrada de la MFT.

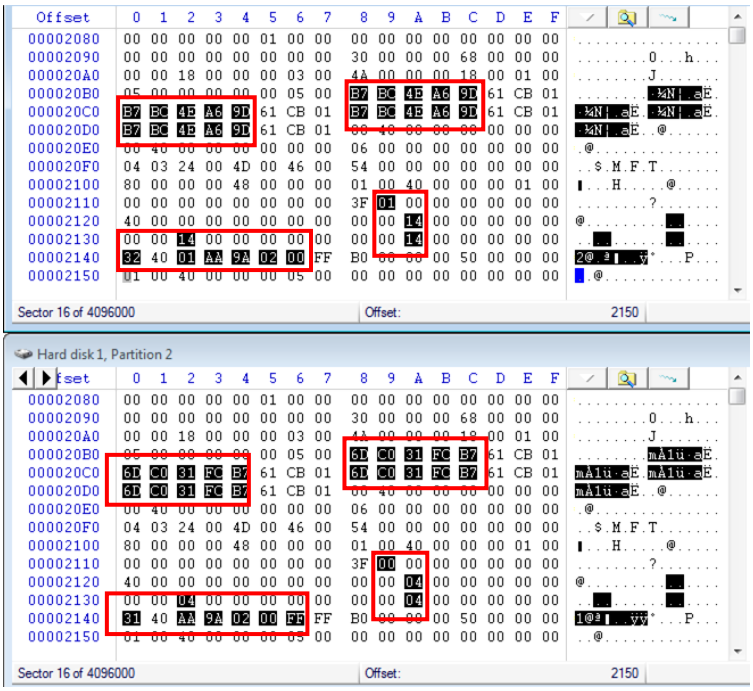


Figura 2.19. Comparación de la entrada MFT en la MFT.

3. La entrada index correspondiente al directorio raíz. La Figura 2.20 muestra la comparación de dicho index.

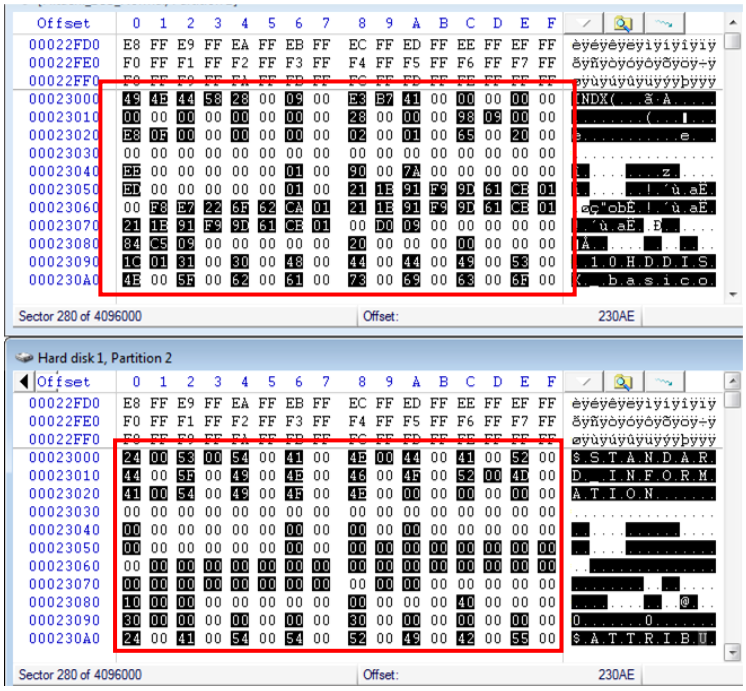


Figura 2.20. Comparación del Index.

2.1.5. Sobreescritura parcial

La sobreescritura parcial se refiere a la modificación parcial del contenido de archivos o entradas de directorios, ya sea por nueva información o código ilegible.

Las causas principales que originan este daño son:

- Código malicioso del tipo "virus de sobreescritura" que altera el contenido del archivo atacado.
- Falla de poder durante la escritura de archivos, ocasionando que las cabezas escriban en el contenido de los archivos.
- Errores humanos, al borrar archivos o formatear al DDE, y posteriormente grabar nueva información.
- Sectores dañados pertenecientes al contenido de un archivo.
- Restauraciones de respaldos de forma incorrecta.

Los síntomas que se presentan cuando se han sobreescrito archivos son: no "*boot*" del SO, no se puede abrir el archivo, al abrir el archivo la información es ilegible o el contenido es incorrecto.

2.2. Métodos y procedimientos para la Recuperación de Información

Existen principalmente tres métodos para recuperar la información cuando un DDE ha sufrido un daño lógico, o cuando este se ha originado de un daño físico. Para una recuperación de información se puede usar uno sólo de estos métodos o los tres.

2.2.1. Reparación manual o mediante software

Cuando parte de la estructura del SA ha sido modificada, se puede realizar una reparación manual o con algún programa especial como MBRFIX [23], Partition Table Doctor (PTD) [24], TestDisk [25], etc, sólo en el caso de que exista suficiente información para

calcular la información faltante/modificada. Esto en base a la información mínima con que el SA puede trabajar y la unidad lógica sea visible.

Para el caso en que la información contenida en los archivos de usuario o SO han sido modificados, la reparación no puede ser posible, y se tendrá que hacer la recuperación mediante la utilización de Software especializado o por "tipo de archivos". La Tabla 2.7, 2.8 y 2.9 indican que elementos pueden ser reparados de forma manual o automática y como se realiza dicha reparación, para el MBR/EBR, el SA FAT32 y SA NTFS respectivamente.

Tabla 2.7. Elementos del MBR que pueden ser reparados.

Elemento	Forma Manual	Forma Automática
Código de inicio	No se puede	El programa *MBRFIX* y *PTD* son capaces de recrear este código de forma automática
Firma	Escribir en el offset 01FEh-01FFh la cadena 0xaa55	El programa *MBRFIX* y *PTD* son capaces de escribir la firma de forma automática en las posiciones correspondientes
Tabla de Particiones	Se identifica el número del sector de arranque de la partición a recrear (dicha posición se escribe en la TP en el campo correspondiente al inicio de la partición en formato LBA). En el Sector de arranque de la partición, se localiza el campo del tamaño de la partición en sectores (offset 20h), y ese valor es escrito en el MBR, en el campo de "número de sectores de la partición". De acuerdo al tipo de partición (tabla 1.3), se coloca el valor en el campo correspondiente en el MBR/EBR. Para el inicio y final de la partición en formato CHS se escribe el código 0x00, ya que el SA se basará en la información en formato LBA	*MBRFix* no es capaz de reconstruir la TP, pero PTD sí lo hace, para ello realiza un escaneo rápido de todo el DDE, en busca de los sectores de arranque

Tabla 2.8. Elementos del SA FAT32 que pueden ser reparados.

Elemento	Forma Manual	Forma Automática
Sector de Arranque	De acuerdo a la estructura, escribir aquellos valores conocidos o basados en el MBR/EBR	El programa *TestDisk* es capaz de reconstruir al sector de arranque con los valores mínimos para que la unidad lógica sea accesible, aunque no "*booteable*"
FAT1	Se localiza la FAT2 y se copia a la FAT1	No es recomendable, ya que puede existir más de un SA.
FAT2	Se localiza la FAT1 y se copia a la FAT2	

En caso de que tanto FAT1 como FAT2 se dañen, no se podrán reconstruir ni manual ni automáticamente.

Tabla 2.9. Elementos del SA NTFS que pueden ser reparados.

Elemento	Forma Manual	Forma Automática
Sector de Arranque	De acuerdo a la estructura, escribir aquellos valores conocidos o basados en el MBR/EBR	El programa *TestDisk* es capaz de reconstruir al sector de arranque con los valores mínimos para que la unidad lógica sea accesible, aunque no "*booteable*"
MFT	No se puede	No es recomendable, ya que puede existir más de un SA.
Entradas de directorio	No se puede	

2.2.2. Utilización de Software especializado

Cuando la reparación de la estructura lógica de un DDE, no ha sido posible o ha sido de forma parcial, se utiliza Software especializado en la recuperación de información. Este software debe ser específico para el SA contenido en el DDE.

De forma general lo que hacen este tipo de programas es: Buscar todos los MBR/EBR validos que encuentre a los largo del DDE, buscar cada uno de los elementos de acuerdo al SA (como Sector de Arranque, FAT's, MFT, etc) de cada una de las particiones especificadas en el MBR/EBR y con aquellos elementos intentar reconstruir cada partición de forma virtual. En caso de que no encuentre MBR validos, buscará los elementos del SA para la reconstrucción. Para la reconstrucción virtual, el programa buscará cada rastro de entradas de directorios. Las búsquedas que se ejecutan son sector por sector sin importar si están vacios o contienen datos, por ello en la mayoría de casos el proceso es lento, más aún si la capacidad del DDE es grande.

Los programas que están enfocados a la recuperación de información tienen la capacidad de obtener archivos borrados u orphans [21]. Estos últimos son archivos que se encuentran en el DDE y que tienen entradas en las FAT's o en la MFT, pero no pertenecen a alguna entrada de directorio existente. Un ejemplo de este tipo de Software es el programa Get Data Back [26] que existe para los Sistemas de archivos NTFS y FAT.

2.2.3. Recuperación "*por tipo de archivo*"

La recuperación "*por tipo de archivo*" es aplicada cuando el MBR/EBR y/o la estructura del sistema de archivos sufrieron un daño y no pueden ser reconstruidos, pero la información no ha sufrido daño alguno y se sabe el tipo de archivo específico que se requiere recuperar.

El procedimiento general para recuperar información "*por tipo de archivo*" es:

1. Identificar el patrón del encabezado de un determinado tipo de archivo, es decir, ubicar los primeros bytes del primer sector del primer *cluster* que conforman al archivo, aquellos que para todos los tipos de archivos son iguales. En la Figura 2.21 se muestra el encabezado para archivos de office y Winzip.
2. A partir de dicho primer *cluster* ubicar el último sector del archivo (depende del tipo de archivo es el patrón del fin de archivo) y calcular cuántos sectores lo conforman.
3. De acuerdo al tamaño calculado del archivo, extraer como archivo, los *clusters* o sectores contiguos. No se recupera el archivo con su nombre real ni el directorio o subdirectorios a los que pertenecía, pero el contenido será visible.

a)

DiscoDuro[1].doc

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	D0	CF	11	E0	A1	B1	1A	E1	00	00	00	00	00	00	00	00	ÐÏ.à¡±.á.....
00000010	00	00	00	00	00	00	00	00	3E	00	03	00	FE	FF	09	00	........>...þÿ..
00000020	06	00	00	00	00	00	00	00	00	00	00	00	02	00	00	00	....
00000030	A3	00	00	00	00	00	00	00	00	10	00	00	A5	00	00	00	£...........¥...
00000040	01	00	00	00	FE	FF	FF	FF	00	00	00	00	A1	00	00	00	....þÿÿÿ....¡...
00000050	A2	00	00	00	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	¢...ÿÿÿÿÿÿÿÿÿÿÿÿ
00000060	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000070	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ

b)

atapwd.zip

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	50	4B	03	04	0A	00	00	00	00	00	3D	6B	4F	2C	5A	19	PK.....=kO,Z.
00000010	78	04	18	00	00	00	18	00	00	00	0B	00	00	00	66	69	x.............fi
00000020	6C	65	5F	69	64	5F	64	69	7A	41	54	41	20	54	6F	6F	le_id_dizATA Too
00000030	6C	73	20	75	74	69	6C	69	74	79	20	76	31	2E	32	0D	ls utility v1.2.
00000040	0A	50	4B	03	04	14	00	00	80	08	00	55	6A	4F	2C	C2	.PK.....€..UjO,Â
00000050	28	8B	1A	5F	4C	00	00	00	AE	00	00	0A	00	00	00	41	(‹._L...®.....A
00000060	54	41	50	57	44	2E	45	58	45	EC	7C	7B	5C	54	C7	DD	TAPWD.EXEì|{\TÇÝ
00000070	F7	9C	3D	BB	67	D7	DD	75	41	50	D4	68	56	D0	6F	D3	÷œ=»gרÝuAPÔhVÐoÓ

Figura 2.21. Encabezado para archivos a) Excel b) Winzip.

El éxito para este tipo de recuperación, depende mucho de la fragmentación del DDE, ya que la extracción de los archivos se hace de manera contigua y no siempre se almacenan así los archivos, principalmente aquellos que tienen un uso continuo.

Existen programas especiales que realizan este tipo de recuperación de datos de forma automática como Recover My Files [27]. La recuperación "*por tipo de archivo*" no siempre es posible, ya que en algunas ocasiones, principalmente bases de datos, sistemas contables o archivos ligados, el nombre real es requerido.

2.3. Clasificación de los daños lógicos

Después de analizar a detalle cada uno de los tipos de daños lógicos que pueden afectar al DDE, se presenta la tabla 2.10, la cual muestra la clasificación concreta de los daños mencionados y posibles soluciones acorde a las vistas en la sección 2.2.

Tabla 2.10. Clasificación de los principales daños lógicos que afectan a un DDE y su posible solución.

Daño	Síntoma	Posible solución
Estructura del MBR/EBR corrupta	-El SO no inicia - La unidad lógica no es reconocida por el propio SO ni por uno externo -Pantalla azul con mensaje de error	-Reparación de la estructura de forma manual o con software especializado -Correr programa especializado para recuperar datos -Recuperación "por tipo de archivo"
Sistema de Archivos corrupto		
Archivos corruptos		
Borrado de archivos	-Archivos faltantes	-Correr programa especializado para recuperar datos -Recuperación "por tipo de archivo"
Formateo	-La unidad lógica se visualiza como nueva	-Reconstruir la estructura original de forma manual o con software especializado -Correr programa especializado para recuperar datos -Recuperación "por tipo de archivo"
Reparticionamiento		
Sobreescritura parcial/total	- El SO no inicia -Los archivos no pueden ser abiertos o contienen código parcial o totalmente ilegible	-Recuperación "por tipo de archivo" -Reparación por tipo de archivo con programa especializado

RESUMEN

En este capítulo se analizaron aquellos daños de tipo lógico que afectan a un DDE, para ello se realizaron ataques, es decir se modificación algunos parámetros y elementos del Sistema de Archivos, y se verifico cuales afectaban al acceso de la unidad lógica, y en cuales casos la información ya no se podría recuperar a 100%.

Los casos más severos, y que permiten un bajo o nulo porcentaje de información recuperada, son cuando la sobreescritura de los datos o de la estructura del SA, está prácticamente al 100%.

Capítulo 3. CLASIFICACIÓN DE LOS DAÑOS FÍSICOS Y SU POSIBLE SOLUCIÓN

En este capítulo se revisarán las causas que originan daño físico en un DDE. Para los daños más comunes y frecuentes encontrados en el grupo de 78 DDEs con diferentes características para esta investigación, se propondrán soluciones. Asimismo se desarrollaron dos herramientas físicas que ayudan en la solución de problemas con motor y firmware. Se finalizará con una tabla referencia de los principales daños y las posibles soluciones.

3.1. Tipos de daños físicos y sus causas

Decimos que un DDE tiene un daño físico cuando uno o varios componentes o elementos no funcionan adecuadamente, ocasionando que la lectura/escritura de los datos no sea posible o se presente de forma intermitente.

Los daños físicos pueden existir por el propio funcionamiento mecánico y electrónico del DDE, aunado a problemas como condiciones ambientales inadecuadas, o hasta errores humanos, entre otros.

La falla de un elemento del DDE genera cambios en el funcionamiento de los demás componentes, agravando el daño e incluso derivando en la pérdida total de la información.

Un daño físico puede ocasionar un daño lógico debido a la incorrecta o nula lectura de sectores, y por consiguiente la obtención parcial o nula de la estructura del SA o de la propia información de usuario.

Se tomó una muestra de 78 DDEs dañados de 2.5" y 3.5", de diferentes características (marca y capacidad) y se detectaron los diferentes tipos de fallas físicas. Estos datos se muestran en la tabla 3.1.

Tabla 3.1. Muestra de 78 DDEs con daños físicos.

MARCA	CAPACIDAD (GB)	CANTIDAD	MARCA	CAPACIDAD (GB)	CANTIDAD
Fujitsu	40	1	**IBM**	12	1
|	60	2		120	1
	120	1	**Maxtor**	4	1
	160	1		6	1
Hitachi	6	1		15	1
	40	5		20	1
	80	4		40	4
	100	1		80	2
	120	1		160	1
	160	1		250	1
	250	1		300	1
	1024	1			

MARCA	CAPACIDAD (GB)	CANTIDAD	MARCA	CAPACIDAD (GB)	CANTIDAD
Quantum	2	1	**Toshiba**	30	1
Samsung	2	1		40	2
	4	1		60	1
	80	1		120	1
	120	1		160	1
Seagate	0.85	2		200	1
	4	2	**W.D.**	1.6	1
	13	1		40	2
	30	1		60	1
	40	4		120	3
	160	3		160	2
	250	1		200	1
	500	2		250	2
	750	1		320	1
	1500	1			

En esta sección se detallan los daños identificados en los 78 DDEs, así como los síntomas que presentan.

3.1.1. Daño en Platos y Cabezas

Una cabeza dañada ocasiona con el tiempo un daño en los platos hasta degradar la *media* (material magnético donde se almacenan los datos), y viceversa. El daño se agrava cuando existen ambos, ya que generalmente deriva en daño visible en la superficie de los platos (*headcrash*), siendo muy difícil recuperar la información o incluso imposible.

3.1.1.1. Daño en platos

Los daños que presentan los platos, pueden ir desde problemas sencillos como la alteración térmica en la *media*, que ocasiona lecturas/escrituras intermitentes o indicación de sectores dañados debido al TMR (*Track Mis-Registration*); o problemas más severos como la alteración o destrucción física total o parcial del material que recubre a los platos (desde la capa de lubricante hasta la *media*), y que ocasionan la presencia real de sectores

dañados o *headcrash*, es decir que se presentan surcos o rayones sobre los platos (Figura 3.1), aún cuando estos no sean visibles a simple vista, la información ya no estará integra. Debido a que es en los platos donde se almacena la información, si estos presentan daño, dependiendo de la severidad, la información se puede perder, al ya no existir o volverse la lectura imposible.

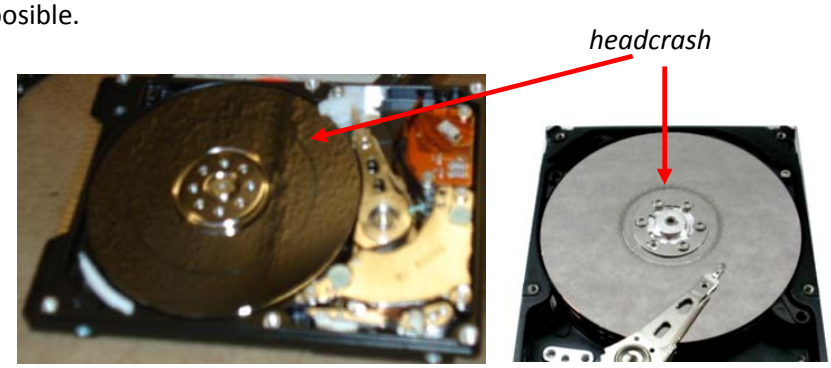


Figura 3.1. Daño visible en superficie del plato superior.

La principal causa que origina estos daños es el cambio del *flying height*, que puede ser ocasionada por:

- Daño en el VCM Actuator, brazos y/o *slider*: ocasionado por caídas o golpes provocados por errores humanos, y que derivan en la pérdida de alineación.
- Problemas en el motor: ocasionados por caídas o golpes, mal funcionamiento del motor provocado por fallas en la energía eléctrica o por trabajar en condiciones ambientales no adecuadas; y que provoca que los platos no roten a la velocidad correcta o que no roten alineados, es decir de forma ondulada.
- Problemas térmicos en los platos: ocasionado por condiciones ambientales no adecuadas. Los materiales que recubre a los platos son sensibles a la temperatura, debido a ello, cuando son expuestos a temperaturas elevadas (fuera de los rangos que soporta el DDE de acuerdo a las especificaciones de cada fabricante, generalmente de 5°C a 55°C), las propiedades magnéticas se pierden y el material se expande, ocasionando que el *flying height* no sea uniforme a través de toda la superficie de los platos. Incluso puede existir un contacto directo entre el *slider* y la *media*, ocasionando *headcrash*.

- Entrada de partículas: la más mínima partícula puede afectar la alineación de las cabezas, ya que una partícula puede llegar a ser más grandes que la distancia ente el slider y la *media*. Estas partículas pueden provenir de polvo o de humo de cigarro.

Otra causa que puede originar destrucción del material de los platos, es la exposición del DDE a desastres naturales como inundaciones o incendios.

Los síntomas que se presentan cuando los platos se han dañado, es la lectura intermitente o nula de los datos; identificación incorrecta del DDE en el BIOS del equipo de cómputo (debido a que no se leyeron correctamente los parámetros en la parte del firmware ubicado en los platos); o sonido de golpeteo de las cabezas (click-click).

Los casos llamados irrecuperables por problemas en los platos, se presentan cuando la destrucción de la *media* abarca una gran área física del plato, al grado de ocasionar la destrucción en las cabezas, o cuando se daña el área física del plato donde se encuentra ubicado el firmware. La Figura 3.2 muestra a un DDE identificado como irrecuperable debido a la severidad del daño en la *media*.

Figura 3.2. DDE con daño severo en la superficie del plato superior (*headcrash* visible), irrecuperable.

3.1.1.2. Daño en cabezas

Los daños que se presentan en las cabezas de los DDE, pueden no ser tan graves, pero generalmente uno de estos daños deriva en otro, esto es cuando el primer daño se ha presentado por un periodo largo, o por que el factor causante sigue presente. Por ejemplo, si los *sliders* llegan a tocar la superficie de los platos, y si este contacto sigue por un periodo largo, el daño será mayor, afectando tanto a las cabezas como a los platos.

Mala alineación de los elementos que sostienen a las cabezas

Si se desalinea el brazo que sostiene al *slider* donde están montadas las cabezas de lectura/escritura, el *flying height* cambia, aún cuando esta desalineación sea mínima. Al cambiar el *flying height* la lectura/escritura se vuelve intermitente debido al TRM. La cercanía entre las cabezas y la *media*, puede ocasionar *headcrash* y por tanto dañar además de las cabezas de lectura/escritura, a la *media*, ocasionando adicionalmente un daño lógico. Esta mala alineación puede ser provocada por un error humano o por un desastre natural (caídas o golpes intencionales o accidentales), una falla eléctrica que afecte al VCM *Actuator* y por tanto al CI *preamp* que controla al *headstack*. Otro causante puede ser debido a las condiciones ambientales inadecuadas, ya que el material de las cabezas al igual que los platos es sensible a la expansión térmica. Si algunas partículas como polvo o humo, llegan a entrar al HDA, y debido a que el tamaño de estas partículas llega a ser más grandes que el *flying height,* al tocar las cabezas también ocasionan mala alineación o dañarlas de forma permanente. En la Figura 3.3 se muestra una comparación simbólica de la diferencia de tamaños que existe entre el *flying height,* que hasta el año 2003 era de 5nm, y el grosor de un cabello que es de aproximadamente 80,000nm [28] y una partícula de polvo puede llegar a hasta 500,000nm [29].

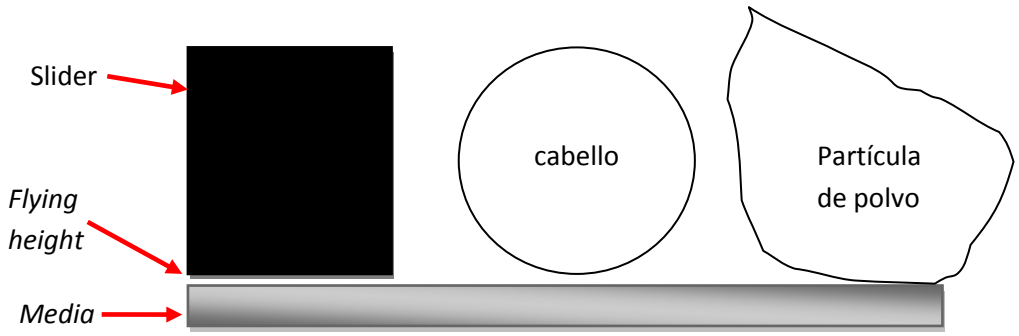


Figura 3.3. *Flying height* vs cabello y partícula de polvo.

Cabezas/*slider* quemados o mojados

Otro daño que pueden llegar a presentar las cabezas/*slider* es cuando se han quemado o mojado y que pierdan sus propiedades, provocando que no se pueda realizar la lectura. Este daño generalmente es ocasionado por un desastre natural y es de los más severos.

Stiction

El *stiction* [30] es la fricción estática, se define como la fuerza que se ejerce por medio de la cual quedan adheridos el *slider* y la superficie del plato, esto debido a la reducción del *flying height* que puede ser ocasionado por una incorrecta alineación de las cabezas. También puede ser ocasionado por una caída o una falla de energía eléctrica. Si los platos se encuentran en rotación y este movimiento es detenido de forma repentina, las cabezas no tienen suficiente tiempo para llegar a su zona de estacionamiento provocando *stiction*.

Desprendimiento de *slider*

El desprendimiento del slider, como su nombre lo indica es cuando el *slider* ya no es sujetado por el brazo que es sostenido por la *suspensión* del *head-stack*. Si el DDE se pone a funcionar en esta condición, se corre el riesgo de que los pequeños alambres que quedan sueltos que sujetaban al *slider*, ocasionen *headcrash*. Este desprendimiento puede ser ocasionado por una caída, por *stiction* mal tratada, por falla en la energía eléctrica aunado al continuo intento de funcionamiento, por condiciones ambientales inadecuadas (partículas adentro del DDE que tocan a las cabezas y las dañan) o incluso por desastres naturales.

Headcrash

Este daño es el más severo hablando de cabezas y platos, debido a que cuando las cabezas entran en contacto con los platos, sin llegar a la *stiction*, producen un desgaste en los platos visible o no, ocasionando rayones o surcos, destruyendo no sólo las capas superficiales como la capa de lubricante y carbón, sino también la capa magnética que es donde se almacena la información. Normalmente este daño surge como consecuencia de otro daño, como mala alineación o desprendimiento del *slider*. También puede ser causado por caídas, fallas de energía eléctrica, condiciones ambientales inadecuadas o desastres naturales.

Los síntomas de esto daños son:

Lectura nula o intermitente, detección incorrecta del DDE en el BIOS del equipo de cómputo, nula rotación del *spindle* motor, sonidos de golpeteo (click-click) o calentamiento en elementos de la PCB.

3.1.2. Daño en el *Spindle* Motor

Anteriormente los DDE usaban motores con ball bearing, y desde 1997 [31] se comenzaron a usar motores FDB (Fluid Dynamic Bearing), ambos tipos de motores son sensibles a fallas ocasionando pérdida de datos.

Ball bearing

Los motores *ball bearing* producen NRRO [18], es decir movimientos internos (vibraciones) del motor que se transmiten a los platos, ocasionando lecturas/escrituras incorrectas, este error se puede presentar por contactos mecánicos internos. Las vibraciones producen ruido acústico, que afecta a la capacidad de posicionamiento en *tracks* de alta densidad, derivando igualmente en una incorrecta lectura/escritura. Si las vibraciones llegan a ser muy grandes, pueden producir que el *flying height* cambie, originando hasta *headcrash*. Estos contactos mecánicos internos pueden ser producidos por el propio desgaste del uso, por altas temperaturas, o por impactos físicos a los DDE, ya sea por accidente o mal intencionados.

En estos motores las cargas de impactos son absorbidas por puntos de contacto entre las *balls* y los *race*, bajo grandes cargas, el *race* se deforma permanente, ocasionando las vibraciones y ruido acústico [31]. Otros factores que los pueden afectar son las fallas de energía eléctrica, en algunas ocasiones puede quemar el motor, ocasionando que se quede pegado (*stuck*) y que no haya rotación.

Fluid Dynamic Bearing

Este tipo de motor fue diseñado para reducir las vibraciones y ruido acústico, y con ellos los problemas que de estos se derivan. Sin embargo existe otro tipo de problema. El aceite lubricante que se utiliza internamente puede cambiar de viscosidad por el sobrecalentamiento, ocasionando problemas internos, de tal forma que el motor comienza a rotar a una velocidad variable o simplemente no rotar.

Los problemas que se presentan en ambos motores también pueden ser ocasionados por desastres naturales como incendios o inundaciones, un temblor puede ocasionar impactos.

Los síntomas característicos de estos daños son: no es reconocido por el BIOS del equipo de cómputo, no gira, gira a una velocidad intermitente, el motor inicia pero luego se detiene o el motor gira pero se escucha un sonido inusual proveniente de la parte interna del motor.

3.1.3. Daño en la PCB

Los daños electrónicos, se presentan en componentes electrónicos, la mayoría de ellos se encuentra en la PCB. Debido a que están ubicados de forma externa al HDA, las condiciones ambientales inadecuadas los pueden afectar más.

La operación más delicada de los componentes es al momento de encender y apagar la alimentación eléctrica del DDE, ya que pasan del estado de reposo al de máximo rendimiento o viceversa, también se puede presentar cuando están trabajando de manera interrumpida o durante largo periodos.

Las PCBs presentan daños a nivel de componentes, pueden quemarse, desoldarse, romperse, o tener corrosión. También se pueden llegar a dañar las pistas.

Todos estos daños pueden ser ocasionados por condiciones ambientales inadecuadas que provocan que se quemen; mala fabricación que ocasionen que la soldadura se caiga y que el CI no haga contacto, o también que se quemen fácilmente; romperse por impactos ya sea por caídas o golpes; tener corrosión por desastres naturales; quemarse por fallas de energía eléctrica o cortos circuitos externos directo hacia los componentes.

Los síntomas que denotan estos daños son: el *spindle* motor no gira o la velocidad de rotación es menor a la adecuada, se calientan algunos componentes o el daño en los componentes es visible. La Figura 3.4 muestra un daño visible en un CI de la PCB.

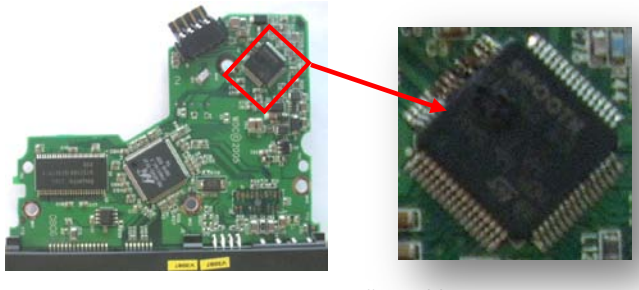


Figura 3.4. Daño visible en PCB.

3.1.4. Daño en el firmware

El firmware es el área del DDE dedicado para almacenamiento de parámetros del propio disco (cuantas cabezas tiene el disco, tablas de reasignación de defectos, etc), y es el que le deja saber al DDE como operar y leer los datos; debido a que se encuentra ubicado en dos áreas (platos y CI en la PCB), se pueden dañar de forma independiente.

Cuando se daña el firmware del CI, el DDE no es reconocido por el BIOS con parámetros correctos, ya sea la marca, modelo, número de serie o capacidad; este tipo de daño se presenta generalmente por un defecto de fábrica (por bugs).

Este tipo de daño se ha presentado en los DDE marca Seagate series 7200.11, y es debido a un proceso en una prueba específica de manufactura, problema conocido por el propio Seagate [32].

Mientras que si se daña el firmware que se localiza en los platos, el DDE no es reconocido por el BIOS, y se presenta por un daño en la *media*, que puede ser originado por daños en la propia *media* o en las cabezas.

3.2. Métodos y herramientas para la recuperación de información

De la muestra conformada por 78 DDEs mostrados en la tabla 3.1, se revisaron y analizaron los daños físicos presentados, así como la severidad del mismo. En base a dicha información se propusieron soluciones para los tipos de daños.

En esta sección se presentan aquellas soluciones por elemento dañado, aplicadas o identificadas para la muestra de DDE obtenidos para esta investigación.

3.2.1. Platos

Los daños que se pueden presentar en los platos de un DDE, pueden variar en severidad. Y de acuerdo a esta severidad se deben aplicar correctivos, cuando la *media* se encuentra en un estado con alta degradación, la recuperación de información se vuelve

imposible, de igual forma, si el área afectada en los platos es el área del firmware. A continuación se presentan algunas soluciones que permitan realizar la lectura de la información, pero si el daño en los platos se originó por otro problema, como daño en motor o PCB, primero se debe corregir dicho problema.

3.2.1.1. Limpieza de los platos

En los casos cuando la falla de lectura se presenta por la entrada de partículas al interior del disco o existen estas particular por presentar inicios de *headcrash*, se debe hacer una limpieza de la *media*.

Esta limpieza se debe realizar con aire comprimido, no se debe hacer con líquidos especiales ya que estos pueden provocar alteración en alguno de los materiales que recubren a los platos.

Para esto, se debe abrir al DDE, dentro de un "clean room" o área limpia, y aplicar el aire comprimido hacia el exterior del HDA, posteriormente se debe cerrar, colocando los tornillos de la tapa de forma alineada.

3.2.1.2. Congelamiento del DDE

Cuando el daño que presenta la *media*, se debe a problemas térmicos, se recomienda enfriar al DDE, a veces no es suficiente con el aire del ambiente, por ello se puede enfriar mediante algún sistema artificial como la exposición continua del aire proveniente de un ventilador, o exponerlo de forma temporal a la temperatura de un congelador.

En el caso de que se exponga al congelador, se debe hace por un periodo corto (10 o 15 minutos) y cubrirlo debidamente, para evitar que se moje y que el daño se agrave. Se recomienda meterlo en bolsas antiestáticas bien cerradas.

3.2.2. Cabezas

Las cabezas de lectura/escritura son elementos sensibles debido a su tamaño, la finalidad de repararlas es para que sean capaces de leer la información contenida en la *media*. Si las cabezas no llegan a funcionar correctamente, aun cuando la información en la *media* no tenga daño, no se podrá recuperar la información.
Algunas soluciones que se pueden aplicar se presentan a continuación.

3.2.2.1. Limpieza de cabezas

Si las cabezas contienen material ajeno al propio derivado del intercambio de material entre el *slider* y las cabezas al entrar en contacto, o por partículas provenientes del exterior; se deben limpiar.
Esta limpieza se debe hacer con un liquido especial “head cleaner” [33]. En el caso de que el DDE tenga un *dynamic load/unload*, se debe aplicar sobre este elemento, como se muestra en la Figura 3.5.

Figura 3.5. Aplicación del “head cleaner” mediante el *dynamic load/unload.*

En el caso de que no exista el *dynamic load/unload*, se debe extraer el *head-stack* completo, y aplicarlo directamente a las cabezas (Figura 3.6.), y volver a ensamblar el *head-stack* al HDA; no se debe aplicar mediante la *media*, ya que este líquido puede alterar sus propiedades.

La extracción del *head-stack* se debe hacer teniendo el debido cuidado de que los *sliders* no entren en contacto.

Figura 3.6. Aplicación del "head cleaner, extrayendo el *head-stack* .

3.2.2.2. Cambio de *head-stack*

Para hacer el cambio de cabezas, se tiene que manipular al *head-stack* completo, debido al tamaño es difícil poder reparar sólo una de las cabezas, aunado a que generalmente al dañarse una cabeza se genera mala alineación en las demás.

Para hacer este cambio, se debe utilizar un DDE donador, el cual debe ser compatible, el anexo 2 muestra una tabla de compatibilidad dependiendo del fabricante. También es importante utilizar las herramientas adecuadas, como guantes para evitar la transmisión de partículas portadas en las manos hacia los platos, cubrebocas, y los desarmadores de los tipos y medidas correctos.

Al momento de empujar a los brazos del *head-stack* hacia afuera de los platos, se debe girar de forma manual al *spindle* motor en sentido contrario a las manecillas del reloj, para facilitar el deslizamiento de los sliders sobre la superficie de los platos, y evitar que se genere *stiction.*

Se debe evitar que durante el cambio, los *sliders* estén en contacto directo, ya que pueden adherirse y ocasionar nuevamente daño en las cabezas, para ellos se recomienda separar los brazos que sostienen a los *sliders* antes de la extracción del *head-stack*, para ellos se puede utilizar un pedazo de material no conductor y del grosor necesario para dicha separación, como papel o foami, la Figura 3.7 muestra la separación de los brazos cuando el DDE cuenta con *dynamic load/unload.*

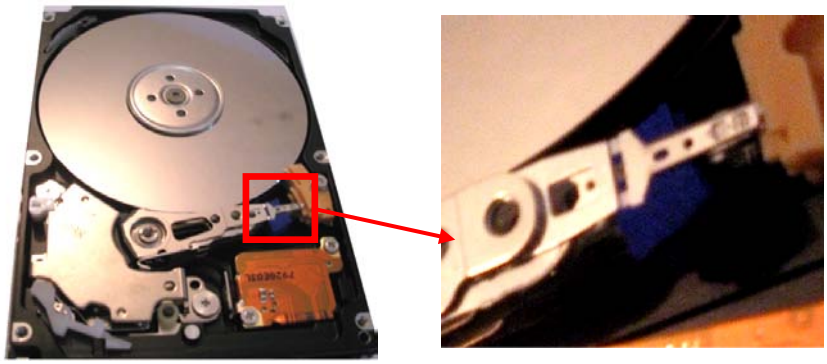


Figura 3.7. Separación de los brazos, cuando el DDE tiene *dynamic load/unload* .

La Figura 3.8 muestra la separación cuando no cuenta con este sistema. Esta extracción de *head-stack*, se hace en ambos discos, tanto en el dañado como en el donador, y se ensambla el *head-stack* donador al DDE del cual queremos recuperar la información. Se debe tener cuidado al momento de ensamblar, cuidando que los tornillos no queden flojos, ya que esto altera la alineación y no tocar los platos.

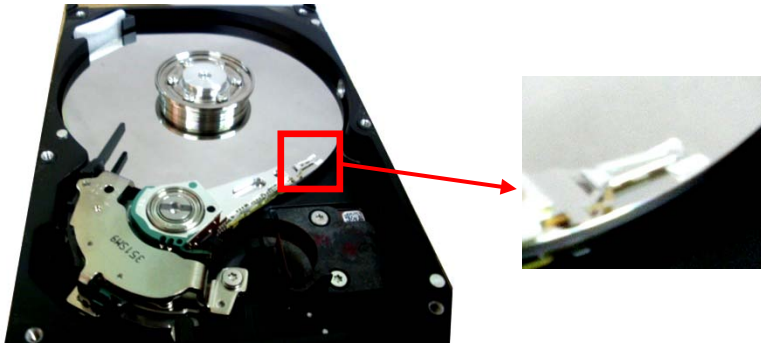


Figura 3.8. Separación de los brazos, cuando el DDE no tiene *dynamic load/unload* .

3.2.3. *Spindle* Motor

Un daño en el *spindle* motor, impacta en la rotación de los platos. El objetivo de reparar al motor es que gire a la velocidad suficiente para que se pueda producir el correcto *flying height* y por tanto las cabezas puedan leer adecuadamente la información. Algunas soluciones que se pueden aplicar para lograr dicho objetivo, se presentan a continuación.

3.2.3.1. Uso de la herramienta “motor unstuck”

Si los platos del DDE rotan a una baja velocidad o no giran, se deben “desatorar”, para lo cual se necesita sujetar al eje del *spindle* motor de tal forma que se tenga la fuerza necesaria para hacerlo rotar de forma manual, esto se logra mediante el uso de una herramienta que se denomina “*motor unstuck*”. Existe una herramienta comercial llamada “*spindle motor unstuck*” [34], para esta investigación se hizo la adaptación utilizando dados y manerales, se desarrollaron dos modelos, para algunas de las marcas de DDEs.

El primero modelo, se muestra en la Figura 3.9 y funciona sujetando al motor mediante los propios tornillos, de tal forma que al aplicar la fuerza sobre el maneral, se logra hacer rotar al motor. La rotación manual tiene que ser en sentido a las manecillas del reloj, cuidando de que las cabezas se encuentren en su zona de estacionamiento.

Se debe rotar manualmente al motor el tiempo necesario, hasta lograr que la fricción se reduzca.

Figura 3.9. Primer modelo del “motor unstuck”.

El segundo modelo, se muestra en la Figura 3.10, y se utiliza cuando no es posible sujetar al eje del motor mediante los tornillos. Este modelo sujeta al motor directamente ocupando el espacio de los tornillo, es decir, se deben quitar al menos dos tornillos del eje del motor, y conectar al “*motor unstuck*” mediante dichos tornillos, y se debe aplicar la fuerza sobre el maneral para hacer rotar al motor hasta que no exista fricción interna o sea mínima.

Figura 3.10. Segundo modelo del "motor unstuck".

3.2.3.2. Lubricación del motor

En los casos cuando el aceite del motor ha cambiado su viscosidad, y por tanto el motor ya no funciona adecuadamente, se debe introducir al motor un poco de aceite lubricante, mediante una pequeña perforación que es lograda por desgaste en la parte opuesta a su eje (puede ser tallando con una navaja o perforado con una broca), como se muestra en la Figura 3.11, para que logre funcionar temporalmente. No todos los motores de los DDEs pueden ser candidatos a esta reparación, debido a la forma en que están construidos y ensamblados al HDA. Generalmente los candidatos a esta reparación son los DDEs marca Toshiba, acorde a la experiencia del autor. La perforación o desgaste que se realice debe ser prácticamente superficial, lo suficiente para poder introducir el aceite y no agravar más el daño; el aceite puede penetrar desde un par de horas hasta un día.

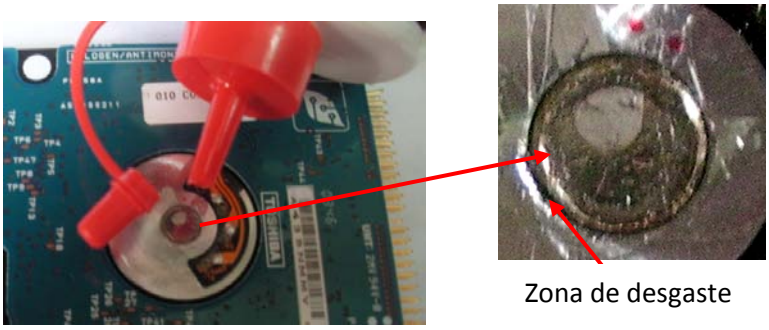


Figura 3.11. Lubricación del motor en un DDE Toshiba, mediante desgaste del material cerca del motor.

3.2.3.3. Migración de platos

Cuando el motor se ha quemado y ninguna de las soluciones anteriores funciona, se puede tomar como opción la migración de platos, es decir, se deben trasladar todos los platos del DDE dañado a otro HDA que sea compatible. La dificultad de esta solución, radica en el traslado del plato sin tocar las superficies, y en el caso de tener más de un plato, esto lo haría más complicado debido a que todos se deban trasladar al mismo tiempo y no perder la alineación, si esto llega a pasar, la recuperación ya no es posible.

Para esta migración se debe utilizar una herramienta que permita el traslado completo de todos los platos al mismo tiempo. En esta investigación dicha herramienta no fue desarrollada.

3.2.4. PCB

La PCB es el componente que controla el funcionamiento del DDE, si esta falla, aún cuando los elementos del HDA se encuentren funcionando de forma apropiada, no se podrá conseguir acceso a la información. Y en algunas ocasiones un daño iniciado en la PCB que no se ha detectado y corregido a tiempo, puede ocasionar un daño en platos, motor o cabezas. A continuación se proponen algunas soluciones que se pueden aplicar al detectar este tipo de daño.

3.2.4.1. Cambio a nivel de componente

Esta solución es aplicable cuando se tiene identificado aquel o aquellos elementos dañados, y que son candidatos a ser cambiados, para ello se requiere contar con una PCB compatible, y deben coincidir los elementos a cambiar. No todos los elementos son candidatos a esta solución, principalmente aquellos elementos que contengan información específica del DDE, como lo es el MCU, o aquel CI que contiene al firmware.

Principalmente los elementos que se dañan más comúnmente son los CI que controlan al motor, ya que este es uno de los primeros en recibir energía eléctrica, aunque hay DDE que

contiene diodos TVS y fusibles que sirven para proteger de fallas de energía. Estos elementos si son candidatos a ser cambiados.

Para aplicar esta solución, además de contar con la PCB compatible, se deben contar con las herramientas adecuadas, como cautín, soldadura, desarmadores, entre otros. Y se debe desensamblar la PCB del HDA, y tener el debido cuidado de no afectar a los elementos aledaños.

3.2.4.2. Cambio total de PCB

Esta solución se recomienda cuando no es posible el cambio a nivel de componente, ya sea porque lo que se quemó son las pistas o el daño es muy grande. Hay que considerar que no todas las marcas de DDE permiten el cambio total de PCB, ya que algunos CI de la PCB guardan información específica y personalizada del DDE, por lo que no es viable dicho cambio.

En otros casos cuando el cambio de PCB es posible, se deben intercambiar aquellos elementos que contiene dicha información crítica, como lo es el caso de algunos modelos de DDEs marca Hitachi. La Figura 3.12 muestra una PCB Hitachi, y se indican aquellos elementos que deben ser cambiados, cuando se hace un cambio total de PCB.

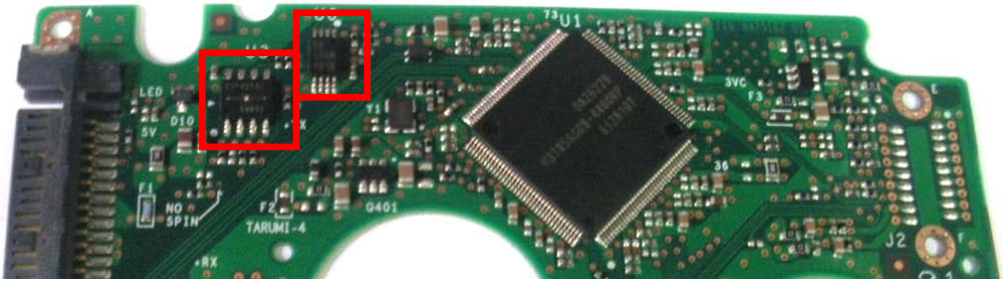


Figura 3.12. PCB de DDE marca Hitachi.

3.2.5. Firmware

Cuando el firmware que se daña es el que se encuentra ubicado en los platos, generalmente se diagnóstica como irrecuperable, ya que no hay forma de reconstruir la información del área del firmware.

Cuando el firmware que se dañó es el que se encuentra ubicado en un CI, la solución que se propone, basada en la solución expresada por algunas personas en internet [35,36], es el reseteo del código firmware.

Para lograr el reseteo se establece una comunicación directa con el DDE. Para ello se utiliza un adaptador RS232 (el cual se conecta al puerto de un equipo de cómputo) y se adecua con un CI MAX232, alimentado con 5Volts, para obtener el voltaje necesario TTL en la recepción y transmisión en el disco duro (de acuerdo al anexo 3).

Se interrumpe la comunicación de la PCB con el HDA, cubriendo la conexión con un trozo de papel y se le conecta la alimentación de poder, así como las entradas RX, TX y tierra del cable (Figura 3.13). El cable rojo es RX, el cable negro en TX, y el cable blanco en tierra.

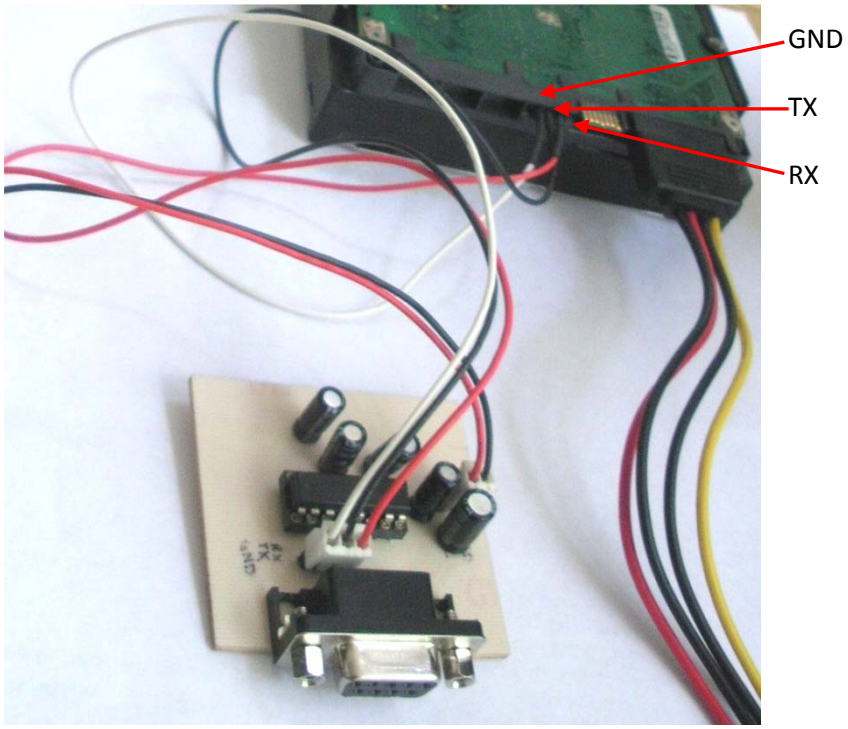


Figura 3.13. Conexión del cable RS232 a la PCB.

Se abre sesión de hyperterminal de Windows del sistema al cual se conecto la PCB, especificando 38,400 bits por segundo, 8 bits de datos, sin paridad, bits de stop 1, y nada en flujo de control. Las instrucciones para el reinicio del firmware son los siguientes:

1. Presionar **CTRL+z** y aparecerá un prompt: *F3 T>*
2. Para acceder al nivel 2, teclear: *F3 T>***/2** (enter)
3. Aparecerá el prompt: *F3 2>*
4. Esperar alrededor de 20 segundos, y teclear: F3 2>**Z** (enter)
5. Aparecerá un mensaje indicando que la rotación se ha detenido e indicará el tiempo esperado y volverá a salir el prompt. Si este mensaje no aparece y aparece un mensaje como:

   LED: 000000CE FAddr: 00280D4D

   Será porque el tiempo que se espero para teclear la letra Z, no fue suficiente, entonces hay que cerrar la sesión de la hypeterminal y volver a comenzar
6. Volver a conectar la PCB al HDA y esperar hasta escuchar la rotación del motor
7. Teclear: *F3 2>***U** (enter)
8. Esperar a que vuelva a salir un mensaje de que la rotación comenzó y el tiempo esperado y volverá a salir el prompt
9. Cambiar el nivel al 1, tecleando: *F3 2>***/1** (enter)
10. Hacer un S.M.A.R.T. erase (crear un sector S.M.A.R.T) tecleando *F3 1>***N1** (enter)
11. Cuando vuelva a aparecer el prompt, apagar el poder en el DDE, esperar unos segundos y volverlo a encender. Y esperar alrededor de 20 segundos.
12. Hacer una regeneración de partición, tecleando: *F3 T>***m0,2,2,0,0,0,0,22** (enter)
13. Después de 15 a 30 segundos, aparecerá un mensaje indicando que el formateo de la partición de usuario ha sido exitoso.
14. Apagar el poder del disco duro, y conectarlo de forma normal al equipo de cómputo de prueba para verificar que el reseteo ha sido exitoso.

3.3. Clasificación de los daños

Después de analizar a detalle cada uno de los tipos de daños físico que se encontraron en el grupo conformado por 78 DDEs, como conclusión se presenta la tabla 3.2, donde se muestra la clasificación concreta de los daños mencionados y una posible solución acorde a las vistas en la sección 3.2.

Tabla 3.2. Clasificación de los principales daños físicos que afectan a un DDE y su posible solución.

Elemento	Daño	Síntoma	Posible Solución
Cabezas	Mala alineación en Cabezas/*slider*	- Incorrecta o nula detección del DDE - Sonidos de lectura forzada - Lectura/escritura intermitente	-Cambiar *head-stack* -Limpiar h*ead-stack* con líquido especial
	Cabezas/*slider* Mojados /quemados		
	Headcrash		
	Desprendimiento del *slider*	- Sonidos de lectura forzada, o click-click	-Cambiar *head-stack*
	Stiction	- Alta temperatura en PCB - Rotación nula en el *spindle Motor*	-Aplicar fuerza horizontal sobre el *head-stack*, moviendo a las cabezas hacia su zona de aterrizaje, y rotanto al *spindle* motor en sentido contrario a las manecillas del reloj
Platos	Sectores dañados	- Lectura/escritura intermitente - Incorrecta o nula detección del DDE - Sonidos de lectura forzada, click-click	-Limpiar *head-stack* con aire comprimido - Congelar al DDE por un periodo corto -Copiar sector por sector, forzando la lectura de los sectores dañados
	Destrucción parcial o total de la *media (headcrash)*		
Motor	Motor "*Stuck*"	- Rotación nula del *spindle Motor* o intermitente	-Aplicar una fuerza al *spindle* motor de forma manual - Usar una herramienta "*Motor unstuck*". -Lubricar al motor con aceite entre el *sleeve* y *shaft* - Migración de platos
	Motor con daño interno (quemado, contacto mecánico, espesamiento del aceite lubricante)	-Vibración -Ruido acústico	
PCB	Componentes quemados o rotos	-Rotación nula del *spindle Motor* -Daño visible -Alta temperatura en componentes	-Cambiar PCB completa -Cambiar a nivel de componente -Refinar la soldadura en componentes
	Corrosión en componentes		
Firmware	Bug en *Firmware*	-Detección errónea -SO no inicia	Reiniciar el *firmware*

RESUMEN

En este capítulo se analizaron posibles soluciones para los daños detectados en la muestra de 78 DDEs. Para la aplicación de dichas soluciones se deben utilizar algunas herramientas que ayuden a aumentar la probabilidad de éxito y a disminuir la posibilidad de agravar el daño. Como en el caso del motor, si no utilizamos el "motor unstuck" de forma correcta, podemos causar daño a la *media*.

Los casos en los cuales la información no se puede recuperar, es cuando se involucran elementos esenciales como la *media* o CIs con información específica del DDE, o cuando no se cuenta con los recursos necesarios, como DDE donador o herramientas físicas.

Capítulo 4. METODOLOGÍA PARA RECUPERAR INFORMACIÓN EN DDEs

La pérdida de información tiene grandes consecuencias, más aun si la información forma parte de la evidencia en un análisis forense informático y por tanto la recuperación de información es requerida. En este capítulo se propone un concepto de recuperación de información basado en la definición de "recuperación". Debido a que no existe una metodología para la recuperación de información en DDEs, en este capítulo se propone una, la cual se basa en mejores prácticas existentes y aplicadas por empresas dedicadas a ofrecer el servicio de recuperación de información.

4.1. Recuperación de Datos

La informática forense es la ciencia que se encarga de identificar, preservar, analizar y presentar evidencia digital en una forma que sea aceptable en un proceso legal [37]. Al llevar a cabo una investigación, si se ha identificado al DDE como el objeto del análisis, pero debido a que presenta un daño lógico o físico, no se puede continuar con la investigación, se requiere realizar el proceso de recuperación de información; para obtener la mayor cantidad de información posible y continuar con el análisis y búsqueda de la evidencia.

La recuperación de información así como la informática forense debe tener su propia metodología, ya que en ambos casos se trabaja con la información, siendo esta el objeto principal de estudio.

El proceso de recuperación de información puede formar parte en un proceso de análisis forense informático, pero también existe por sí mismo. Ya que la información es uno de los activos más importantes no sólo para las compañías sino también para las personas en general.

Concepto de Recuperación de Información

En el diccionario *Online* de Cambridge [38], se define "recuperación" como: *sustantivo*. "El proceso de recuperar algo perdido, en especial salud, capacidad, posesión, etc. ".

Basado en dicho concepto, en este trabajo se define **Recuperación de Información en medios magnéticos** como: "El proceso o acción por el cual se accede a un dispositivo de almacenamiento electrónico o electromecánico dañado, mediante técnicas físicas y/o lógicas, para la extracción de datos"[39].

4.2. Metodología

Debido a que no existe una metodología estándar para el proceso de la Recuperación de Información, que ayude a una adecuada y rápida recuperación, en este trabajo se proporciona una metodología aplicable cuyo objetivo es recuperar la mayor

cantidad de información de forma íntegra. Dicha metodología está basada en mejores prácticas aplicadas por empresas dedicadas a ofrecer el servicio de Recuperación de Datos, como lo son: Forensic Strategy [40], Ontrack Data Recovery [41], ActionFront [42], y a la experiencia laboral del autor en dicho ámbito.

Para ayudar a definir la siguiente metodología se tomaron 10 casos de DDEs que requerían recuperación de información. Las características de los 10 DDE's de los casos, se muestran en la tabla 4.1, así como el tipo de daño que presentaron.

Tabla 4.1. Características de los DDE's de los casos para Recuperación de Información.

Marca	Capacidad (GB)	Tipo de daño, daño especifico y causa
Hitachi	40	Físico – cabezas mal alineadas - fallas de energía eléctrica
	80	Físico - *headcrash* - caída
	120	Físico – cabezas mal alineadas - fallas de energía eléctrica
Maxtor	250	Lógico – Particiones dañadas - error humano
Western Digital	120	Físico – desprendimiento de slider - fallas de energía eléctrica
	120	Físico – desprendimiento de slider y daño en la media- caída
Toshiba	60	Lógico – particiones dañadas - fallas de energía eléctrica
Quantum	80	Lógico - sobreescritura parcial de los datos - error humano
Seagate	40	Lógico - sobreescritura parcial de las particiones - error humano
	250	Físico - Componentes de la PCB dañados - fallas de energía eléctrica

La metodología se conforma de 7 etapas, y cada etapa contiene fases, que se muestran en el diagrama de la Figura 4.1. Al iniciar el proceso de recuperación de información utilizando la metodología propuesta, se debe llenar un documento donde se describen las características del DDE e información concerniente al caso, así como datos de contacto. Y por cada etapa se debe generar un documento donde queden asentados todos los hallazgos y pruebas realizadas, además la hora de inicio y de fin y deberá ser firmada por el examinador o responsable. Toda la documentación se entregará a la persona correspondiente, junto con la información recuperada si es el caso. Los formatos de dichos documentos se muestran en el anexo 4.

Se recomienda que las pruebas se realicen en un equipo de cómputo diferente al equipo original del disco duro, ya que éste también puede tener daño. Las pruebas para los 10 casos, se realizaron en tres equipos de cómputo, los cuales se describen en el anexo 5.

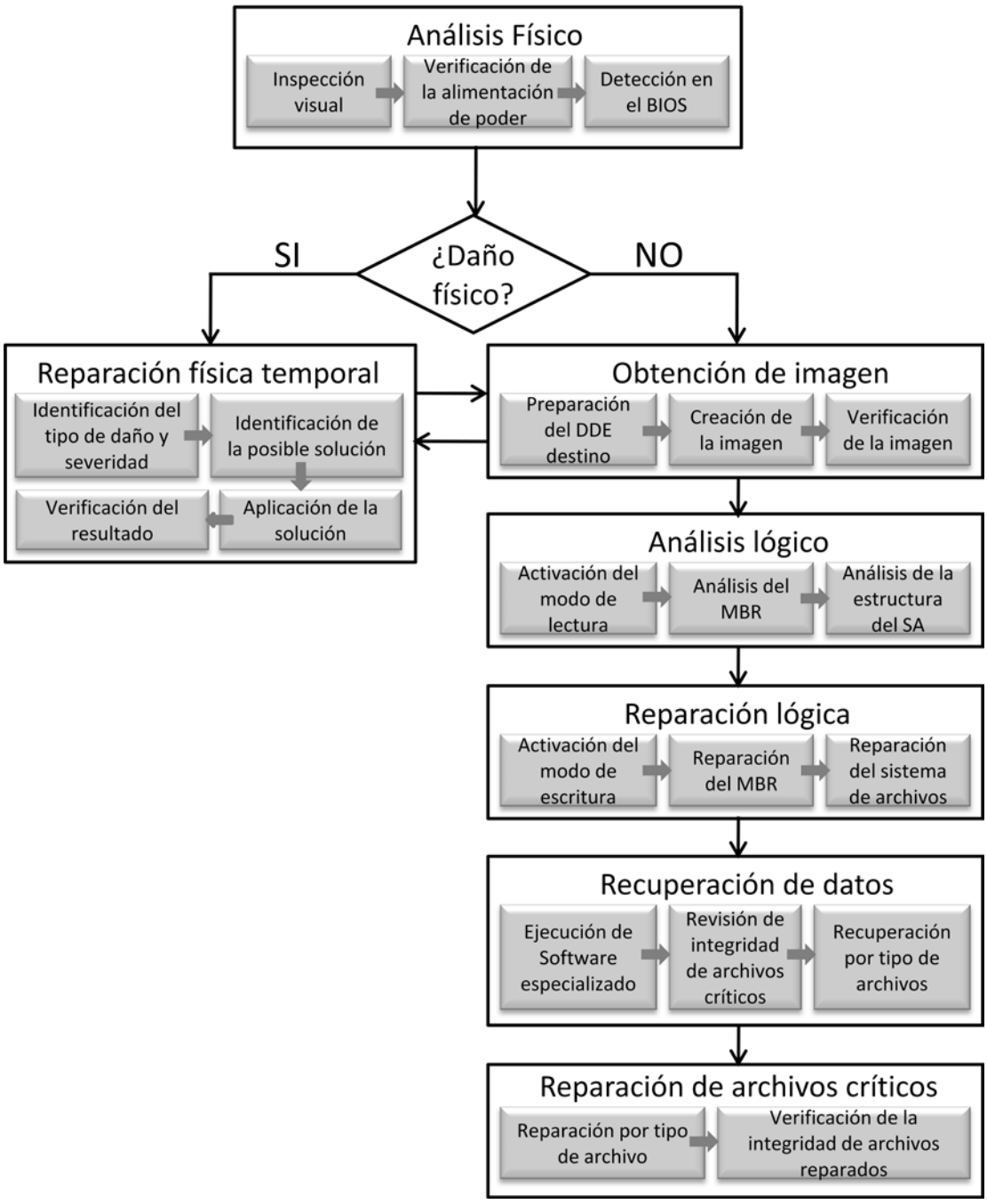


Figura 4.1. Metodología para Recuperar Información en DDEs.

A continuación se describe cada una de las etapas que conforman la metodología, y en cada una de ellas se especifican las fases y herramientas o software necesarios. Y en el anexo 6 y 7 se describen casos reales procesados con la metodología.

4.2.1. Análisis físico

Como su nombre lo indica, en esta etapa se realizará un análisis físico del DDE con la finalidad de evitar agravar el daño, se realiza en 3 fases (Figura 4.2).

Figura 4.2. Fases del análisis físico.

Inspección visual

Primero se realiza una inspección física visual, para descartar la existencia de daño en los componentes ya sea de la PCB o del HDA. Estos daños pueden ser ocasionados por golpes, fallas de poder, etc. Es recomendable desensamblar la PCB del HDA, de esta forma se podrá observar mejor la existencia de fracturas o quemaduras en los Circuitos Integrados (CI), o en algún otro elemento de la PCB.

Verificación de la alimentación de poder

Se verifica que la alimentación de poder sea la adecuada, para lo cual, se conecta el cable de poder de la fuente de alimentación, y se mide el voltaje en las terminales. Para un disco de 3.5" IDE el voltaje entre la terminal 1 y 2 debe ser de +12V y entre la terminal 3 y 4 debe ser +5V (Figura 4.3).

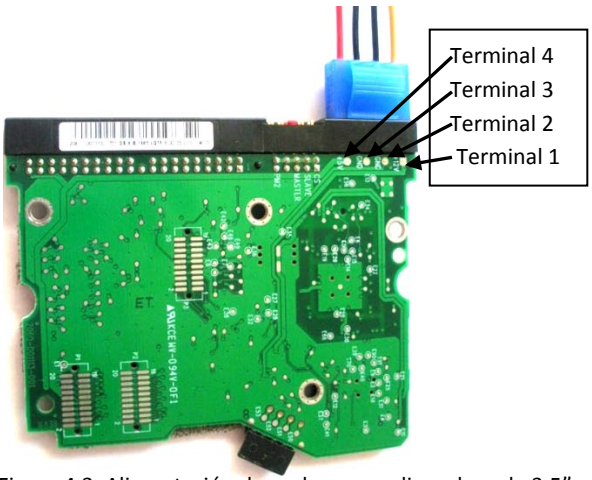


Figura 4.3. Alimentación de poder en un disco duro de 3.5".

En un disco duro 2.5" IDE los pines de poder están junto con los pines de datos. Para un disco SATA los pines de poder se describen en la tabla 4.2.

Tabla 4.2. Descripciones de pines de poder en DDE SATA.

Número de pin	Función
1	3.3V
2	3.3V
3	3.3V
4	Tierra
5	Tierra
6	Tierra
7	5V
8	5V
9	5V
10	Tierra
11	Actividad de inicio de rotación (en discos que lo soportan)
12	Tierra
13	12V
14	12V
15	12V

Para medir el voltaje se hace desde uno de los pines que indiquen el voltaje (3.3V/5V/12V) hacia un pin de tierra (Figura 4.4). La medición se realiza con un multímetro y con la PCB desensamblada del HDA.

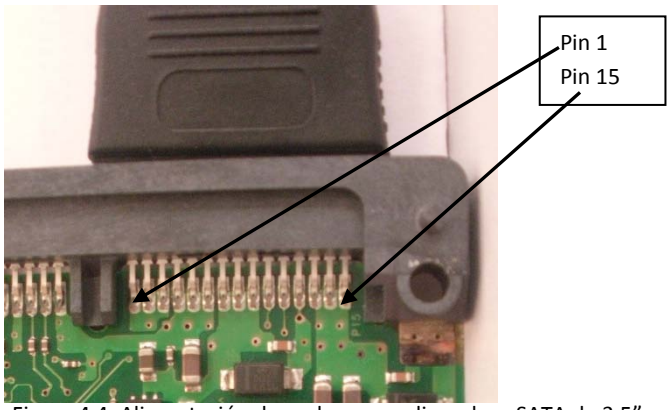


Figura 4.4. Alimentación de poder en un disco duro SATA de 3.5".

Detección en el BIOS

Se verifica que el BIOS (Sistema Básico de Entrada/Salida) de la *Tarjeta Madre* del sistema de prueba, reconozca al DDE de forma correcta y con los parámetros correctos (marca, modelo, capacidad), para lo cual se ensambla la PCB al HDA, y se conecta el cable de alimentación y el cable de datos. Como se muestra en la Figura 4.5.

a) b) c)

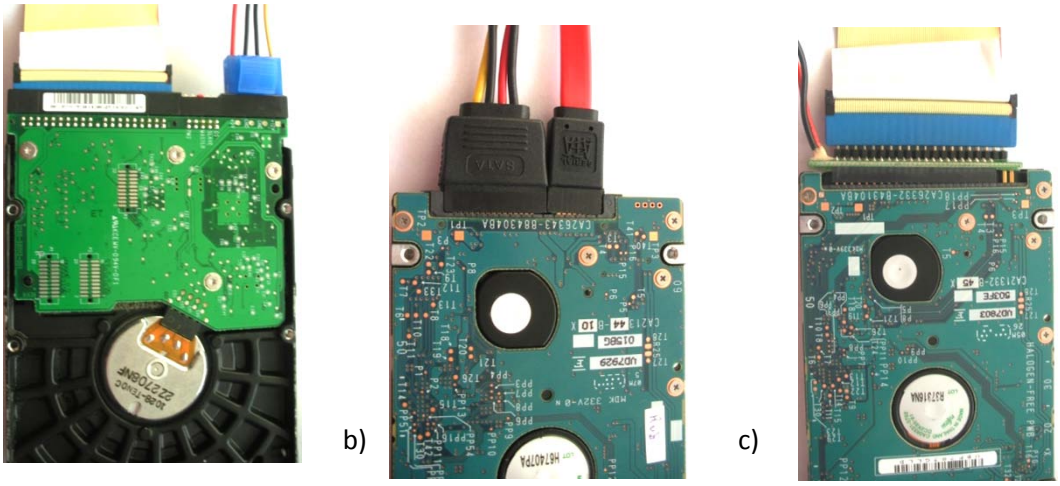


Figura 4.5. Conexión de poder y datos en disco duro a)3.5” IDE, b) 2.5” SATA, c) 2.5” IDE.

Se determina que existe daño físico cuando:

- Existe daño visible en algún componente.
- El voltaje en la conexión de poder no es correcto o es nulo.
- No se escucha o no existe rotación en el motor.
- El DDE no es reconocido por el BIOS, o es reconocido con parámetros erróneos (capacidad, modelo, etc).
- El arranque, lectura o escritura es intermitente.
- Existen sectores dañados.
- Se calienta alguno de los elementos de la PCB.

En caso de que el disco duro no presente daño físico, se continuará en la etapa 3.

4.2.2. Reparación física temporal

La reparación que se le realiza al DDE dañado, generalmente sólo es temporal, porque las condiciones de funcionamiento ideales son alteradas debido a la manipulación a los componentes que ésta reparación requiere. En esta etapa se planean los procedimientos para la reparación temporal, acorde al tipo de daño identificado y su severidad, conforme el capítulo 3. La finalidad es acceder al DDE y obtener una copia fiel, que contenga todos los datos del disco duro. Esta etapa consta de 4 fases (Figura 4.6).

Figura 4.6. Fases de la reparación física temporal.

Identificación del tipo de daño y severidad

En esta fase se deben considerar los síntomas que presenta el DDE, y en base a ellos consultar la tabla 3.2 del capítulo 3, para identificar el tipo de daño. Y verificar si el DDE presenta más de un daño, ya que existen síntomas comunes para diferentes daños. Por ejemplo, si no se escucha rotación en el motor, se puede tratar de un daño en el motor o daño en la PCB (en el CI que controla la rotación). Como se indicó en el capítulo anterior, la falla en alguno de los elementos, puede afectar el funcionamiento de los otros elementos, incrementando con ello, la severidad del daño.

Identificación de la posible solución

En base al daño (s) identificado, se planea la posible o posibles soluciones acorde a la tabla 3.2. Se deben considerar todas las herramientas tanto físicas como de software que se requerirán.

En aquellos casos que requerirán soluciones como reparación de motor/PCB o sustitución de motor, conjunto de cabezas o PCB. Se requieren desarmadores: torx T3-T10, planos y de cruz.

Cuando una sustitución de elementos es necesaria, se requiere un disco donador de partes, dicho disco debe estar funcionando correctamente y ser de la misma marca y modelo del original, aunado a ciertas características adicionales como el número de firmware, dependiendo del fabricante, algunas de las cuales se describen en el anexo 2. Los discos duros remanufacturados no sirven como discos duros donadores [40,43].

Aplicación de la solución

Se aplican la solución previamente definida, en caso de que exista más de una solución, se deben probar todas, hasta que el DDE funcione. En la mayoría de los casos la reparación que se le realiza al DDE es de forma temporal y por tanto el DDE ya no es confiable para su uso posterior.

Las reparaciones que requieran abrir al DDE, se deben realizar en un área limpia, utilizando guantes, cubreboca, y los desarmadores del tamaño y tipo correctos. Se recomienda que se realice en un *clean room* (área con control ambiental de partículas en el aire) [15], ya que la mínima partícula de polvo puede ocasionar daño en las cabezas.

Los DDE que fueron donadores quedaran inutilizables.

Verificación del resultado de la solución

Una vez que se haya reparado de forma temporal al DDE, se conecta al sistema de prueba, el cual ya debe estar listo para la obtención de imagen, y se verifica el acceso aún cuando sea intermitente. En caso de que no se haya logrado el acceso y se hayan agotado las posibilidades de soluciones, se determinará que no es posible la recuperación de información y por consiguiente no se podrá continuar con el análisis forense informático.

4.2.3. Obtención de imagen

Se obtendrá al menos una imagen, la cual es una copia física *bit* a *bit* del DDE dañado y reparado temporalmente, para disminuir la pérdida de datos la imagen se debe hacer del DDE completo, sin importar si se ocupaba parcialmente o si sólo una partición contiene información crítica. El NIST SP-800-86 en su publicación “Guide to Integrating

Forensic Techniques into Incident Response" recomienda realizar una imagen *bit* a *bit* del dispositivo con la evidencia. El autor del presente trabajo basado en su experiencia laboral en el ámbito de la recuperación de datos, recomienda para los casos de análisis forense, realizar 2 imágenes directamente del DDE original; en caso de no ser posible, la primer imagen se obtendrá directamente del DDE original y la segunda se obtendrá de la primer imagen. Asimismo se recomienda que la primer imagen sea almacenada en un DDE y la segunda en otro DDE o en un archivo de imagen. Para el caso de recuperación de datos, con una imagen es suficiente. Esta etapa consta de 3 fases como se muestra en la Figura 4.7. Si durante la obtención de la imagen, el DDE se vuelve a dañar y se cuenta con los elementos necesarios, como otro DDE donador, para volverlo a reparar, se podrá regresar a la etapa anterior: Reparación física temporal.

Figura 4.7. Fases de la obtención de imagen.

Preparación del DDE destino

Se recomienda que la imagen sea creada directamente sobre otro DDE, el cual debe ser por lo menos de la misma capacidad del DDE dañado y previamente debió ser sanitizado [44]. El proceso de sanitización consiste en llenar todos los sectores del DDE con el código 0x00 o con algún patrón aleatorio, esto se hace con la finalidad de evitar mezclar información previamente almacenada en el DDE destino, y de esta forma contaminar la evidencia.

Existen programas como Winhex (Figura 4.8) que permiten realizar este procedimiento, el cual se debe realizar teniendo el debido cuidado para evitar sanitizar al DDE erróneo, ya que al correr este proceso, la información previamente existente será irrecuperable.

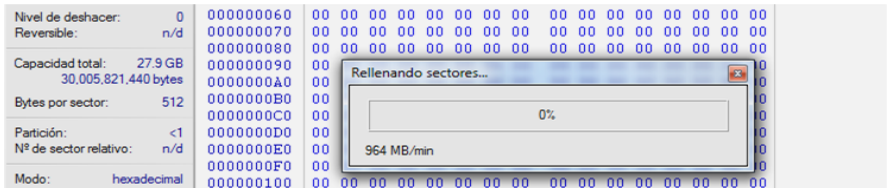


Figura 4.8. Sanitización de un DDE con Winhex.

Creación de la imagen

Se debe obtener el mayor porcentaje de la imagen, en algunas ocasiones no puede ser completada debido a la existencia de sectores dañados o intermitencia en la lectura. La imagen se debe realizar utilizando Software específicamente para generación de imágenes como lo son Winhex, ByteBack (BB) [45], FTK Imager [46], etc, ya que este tipo de software permite comenzar la copia en un punto intermedio del disco, o realizar dicha copia en reversa, la cual tendrá ventajas al no registrar las fallas de ECC (Código de Corrección de Error) [47] en el cache y agilizar la imagen [40].

Para lograr obtener el mayor porcentaje de la imagen, primero se copiaran las áreas que no presenten mayor esfuerzo en la lectura (los sectores no estén dañados), por lo cual es importante que el programa que utilicemos sea capaz de comenzar la copia en cualquier sector del DDE, y posteriormente se forzará al disco a copiar los sectores con problemas, en esta fase se corre el riesgo de que el DDE vuelva a fallar. Se deberá utilizar una bitácora de trabajo para registrar los sectores que se han logrado copiar y aquellos con problemas.

Si el DDE ha fallado nuevamente y se tiene la posibilidad de volver a hacer la reparación, se regresará a la etapa anterior para la reparación temporal. Y al regresar a la obtención de imagen, se comenzará donde se quedo la última vez.

Verificación de la imagen

Una vez que se obtuvo la imagen, incluso si esta no se obtuvo al 100%, se le debe ejecutar una función hash (que es una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc, [48]), la cual dará como resultado un clave que representa a toda la imagen y se utiliza como protección a posibles alteraciones. Si se le genera un hash a la imagen del DDE, y posteriormente se le altera un sólo byte, al volver a obtener el hash, este ya no corresponderá con el primero, lo que indica que la evidencia se ha alterado.

Las funciones hashes recomendadas son MD5 [49] que genera como salida un número de 32 dígitos hexadecimales, o SHA1 [50] que genera como salida un número de 56 dígitos hexadecimales, en el anexo 8 se muestran los algoritmos de ambas funciones. En la Figura 4.9. Se muestra un hash MD5 y un SHA1 para la misma imagen de un DDE de 30GB.

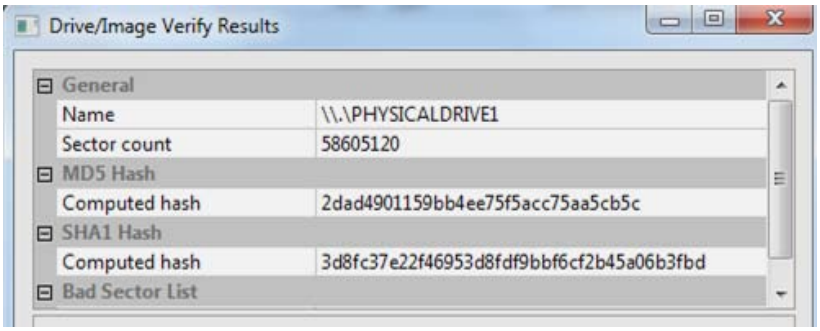


Figura 4.9. Hash MD5 y SHA256 para una imagen de un DDE de 30GB.

La Figura 4.10 muestra los hashes MD5 y SHA1 respectivamente para la misma imagen de 30GB con un sólo byte modificado.

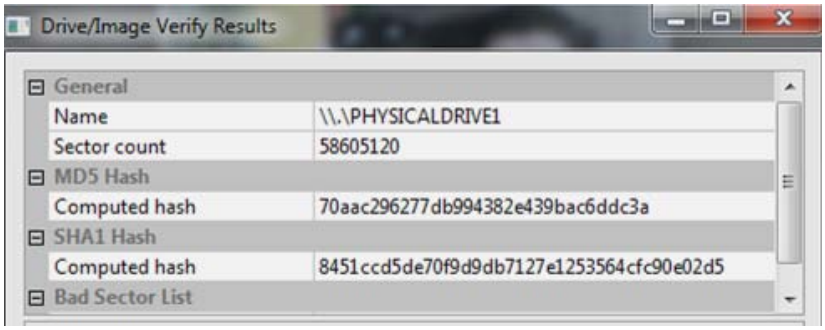


Figura 4.10. Hash MD5 y SHA256 para la imagen de la Figura 4.12 con un byte modificado.

4.2.4. Análisis lógico

Se analiza la imagen obtenida previamente, con la finalidad de identificar los SAs existentes en el DDE, así como aquellos elementos de la estructura lógica que pudieran estar dañados y por consiguiente afectar el funcionamiento lógico y la extracción de los archivos. Esta etapa se realiza en 3 fases como se muestra en la Figura 4.11. Para el análisis lógico se recomienda el uso de un editor hexadecimal, como Winhex.

Figura 4.11. Fases del análisis lógico.

Activación en modo de lectura

Antes de comenzar un análisis lógico, la imagen debe estar protegida contra escritura, para evitar que durante este proceso se altere algún valor ocasionado que la pérdida de información sea mayor, o que se invierta más tiempo reparando elementos de la estructura que no estaban dañados.

La protección contra escritura se puede realizar de dos formas:

1. Mediante Hardware, utilizando un bloqueador de disco duro, en el cual se activa un interruptor que bloquea la escritura (Figura 4.12).

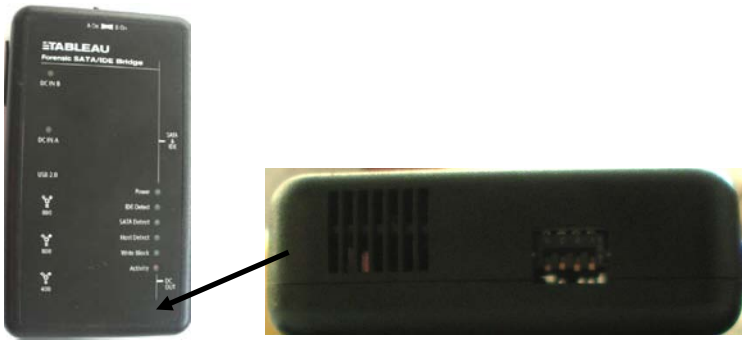


Figura 4.12. Protección contra escritura mediante Hardware.

2. Mediante Software, utilizando un editor hexadecimal como Winhex que permite activar el modo sólo-lectura (Figura 4.13).

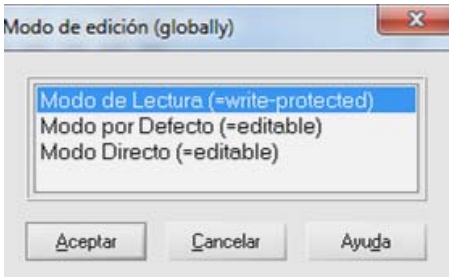


Figura 4.13. Protección contra escritura mediante Software.

Análisis del MBR

El análisis del MBR consiste en conocer cuantas particiones tiene el DDE, los tipos de particiones, es decir, si son FAT32, NTFS, HFS, Ext2, Ext3, etc, así como los tamaños y ubicaciones de cada una. Esto en base a la tabla 1.1 y 1.2 del capítulo 1 que muestran la

descripción del MBR. Los daños que pueden afectar al MBR se indican en la sección 2.1.1 del capítulo 2.

Se recomienda ir tomando nota de cada una de las particiones para su posterior análisis de forma independiente. Los datos relevantes que se obtienen del MBR son: sector de inicio de la partición, número total de sectores en la partición y tipo de partición.

El MBR se ubica en el primer sector, es decir el sector 0. Pero podemos encontrar más MBRs o EBR's en sectores subsecuentes, algunos de ellos podrán ser erróneos. Se recomienda analizar sector por sector hasta encontrar el primer Sector de inicio de partición, y tomar nota de las posiciones de dichos MBR's o EBR's.

Análisis de la estructura del SA

Este análisis consiste en conocer la ubicación de cada elemento de la estructura de cada una de las particiones en el DDE, la estructura es en base a cada SA.

Existen 2 opciones para localizar el primer sector de inicio de una partición, dependiendo del resultado de la fase anterior.

a) Si existe MBR: Validamos que el sector de inicio en formato LBA de la partición indicada en el MBR (basados en la tabla 1.2) corresponda al sector inicial real, en caso de no ser así, este proceso se realizará como si no existiera el MBR.
b) Si no existe MBR: Se busca sector por sector el Sector de inicio de la partición, dependiendo del SA, basado en el formato indicado en la tabla 1.5 para FAT32 o 1.10 para NTFS.

Con la información del primer sector localizamos el final de la partición, utilizando la ecuación 4.1. Y validamos que la ubicación real corresponda.

Para un Sistema de archivos FAT32 y para NTFS se utiliza, la ecuación 4.1.

$$\#\ sector\ final = (\#\ sector\ inicial + \#\ total\ de\ sectores\ en\ la\ partición) \qquad (4.1)$$

Para localizar las FAT's en un SA FAT32, se busca el patrón hexadecimal "F8 FF FF" con ayuda de un editor hexadecimal. En la información del primer sector en un SA NTFS se localiza la ubicación de la MFT y validamos que corresponda la ubicación real. Para calcular el sector de la MFT se utiliza la ecuación 4.2.

$$\#\ sector\ MFT = \#\ sector\ inicial + (\#\ cluster\ de\ MFT * \#\ de\ sectores\ por\ cluster) \quad (4.2)$$

En el anexo 9, se muestran ejemplos de cómo se utilizan las ecuaciones 4.1 y 4.2.

Los daños que afectan a los SA FAT32 y NTFS se describen en la sección 2.1.2 del capítulo 2.

4.2.5. Reparación lógica

Si la etapa anterior da como resultado que la estructura o alguno de sus elementos está dañado, en esta etapa se reparan, de ser posible. La Figura 4.14 muestra las fases de la etapa 5. De todas las modificaciones que se realicen, se debe tomar nota, para llevar el control de los cambios y evitar repetir alguna prueba.

Figura 4.14. Fases de la reparación lógica.

Activación del modo de escritura

Para poder realizar la reparación lógica, se debe activar el modo escritura, esta se realiza dependiendo de cómo se hizo el bloqueo de escritura de la fase 1 de la etapa 4:

1. Mediante Hardware, utilizando un bloqueador de disco duro, en el cual se activa un interruptor que activa la escritura (Figura 4.15).

Figura 4.15. Activación de la escritura mediante Hardware.

2. Mediante Software, utilizando un editor hexadecimal como Winhex que permite activar el modo editable que habilita la escritura (Figura 4.16).

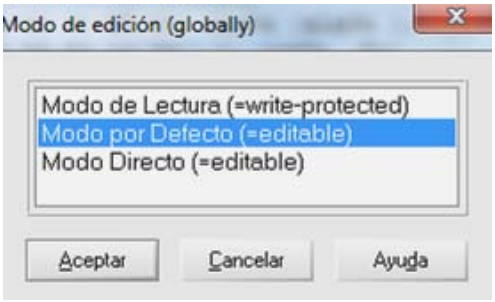


Figura 4.16. Activación de la escritura mediante Software.

Reparación manual o automática del MBR

En caso de haberse encontrado algún daño en el MBR, se realizan las reparaciones correspondientes como se indica en la tabla 2.7 del capítulo 2. En caso de que las reparaciones no sean posibles, se debe continuar la recuperación de información acuerdo a la etapa 6, utilizando Software especializado.

Reparación manual o automática del SA

En caso de haber detectado que la estructura de alguna de las particiones presenta daño, se deben aplicar las soluciones indicadas en las tablas 2.8 y 2.9 para los SAs FAT32 y NTFS respectivamente.

Si las reparaciones no son exitosas, se debe utilizar Software especializado para recuperación de información, como se detalla en la siguiente etapa.

4.2.6. Recuperación de datos

En esta etapa se realiza la Recuperación de Información utilizando Software especializado para estos procesos y acorde a los SAs. Esto se realiza tanto si en la etapa anterior no se tuvo éxito, o si se requiere recuperar archivos borrados o archivos orphans. Las fases se muestran en la Figura 4.17.

Figura 4.17. Fases de la recuperación de datos.

Ejecución de software especializado

El Software especializado se refiere a programas acorde al SA. El funcionamiento de estos programas se describe en forma general en la sección 2.2.2 del capítulo 2. Estos programas recrean la estructura del SA de forma virtual, de tal forma que se puede visualizar previamente la información recuperada antes de copiarla a algún dispositivo de almacenamiento electrónico.

La información recuperada debe ser guardada en un dispositivo diferente sobre el cual se efectuó la recuperación. Puede ser que la cantidad de información obtenida sea mayor a la capacidad del DDE, dependiendo de cuantas veces se hayan borrado archivos o instalado SOs.

Revisión de integridad de archivos críticos

Una vez que se han copiado los archivos recuperados, se verifica la integridad, no es posible hacerlo para cada archivo, por lo que se verifican aquellos que se consideren críticos, es decir, los que pueden contener evidencia.

La revisión consiste en validar que el archivo abra con el programa correspondiente a su extensión y que contenga información legible. En caso de que algún archivo crítico sea identificado como dañado, se debe reparar como se indica en la última etapa.

Recuperación por tipo de archivos

Este tipo de recuperación se describe en la sección 2.2.3 del capítulo 2. Existen programas para realizar este tipo de recuperación, aunque no existe uno para cada tipo de archivo. En caso de que no exista, para algún tipo de archivo específico identificado como crítico, el proceso se realiza de forma manual.

4.2.7. Reparación de archivos críticos

En esta etapa final, se reparan aquellos archivos que no funcionan correctamente y que han sido detectados como críticos. Esta etapa consta de 2 fases como se muestra en la Figura 4. 18.

Figura 4.18. Fases de la reparación de archivos críticos.

Reparación por tipo de archivo

Si algún archivo se identifico como crítico porque posiblemente contiene evidencia, presenta daño; se debe reparar con algún programa especializado para dicho fin. Existen varios programas para reparar varios tipos de archivos, como Recover My Files [26], pero no existe para todos. Para los casos en los que no exista este programa, se debe por lo menos tratar de extraer texto, con la finalidad de obtener una evidencia parcial.

Verificación del correcto funcionamiento de archivos reparados

En esta última fase se valida la integridad del archivo, primero se verifica que pueda ser abierto por el programa al que pertenece, y posteriormente que contenga información legible, ya que dicha información puede ser utilizado como evidencia o puede proporcionar indicios de una evidencia.

4.3. Reporte

Al finalizar el proceso de recuperación de datos, se debe generar un reporte para ser entregado al responsable.

Los elementos que debe contener son los siguientes:

I. Introducción

-Objetivo del proceso de recuperación

-Antecedentes de la problemática

-Identificación del activo objeto del análisis

-Descripción de las herramientas utilizadas durante el análisis

-Fecha de inicio del análisis

-Fecha de término del análisis

II. Metodología del proceso de recuperación de información (con base en documentos obtenidos de cada etapa)

-Descripción del procedimiento y hallazgos del análisis físico

-Descripción del procedimiento y hallazgos de la reparación física temporal

-Descripción del procedimiento y hallazgos de la obtención de imagen

-Descripción del procedimiento y hallazgos de la revisión lógica

-Descripción del procedimiento y hallazgos de la reparación lógica

-Descripción del procedimiento y hallazgos de la recuperación de datos

-Descripción del procedimiento y hallazgos de la reparación de archivos críticos

III. Resultados y conclusión

-Hashes del disco original y de las imágenes

-Cantidad de información recuperada en total y por tipo de archivos

IV. Glosario de los términos técnicos utilizados

V. Anexos (formatos de asentamiento de hallazgos y pruebas de cada etapa descritos en el anexo 4)

RESUMEN

En este capítulo se describieron a detalle todas las etapas así como las fases, que componen a la metodología propuesta para recuperar información. Cuyo objetivo es recuperar la información para su análisis forense, es decir, el DDE o DDEs forman parte de una investigación forense, por lo que el proceso de cadena de custodia concerniente a una metodología de análisis forense, ya se ha llevado a cabo. Al finalizar de aplicar la metodología propuesta, a la información que se logre recuperar, se le dará continuidad con el análisis forense.

Capítulo 5. RESULTADOS

Los resultados del análisis que se realizó sobre la muestra de DDEs que sirvieron para delimitar los daños que afectan físicamente a un DDE, encontrar y proponer soluciones, se describen en este capítulo, así como los resultados obtenidos al aplicar la metodología propuesta en los casos de recuperación de información, para ellos se utilizó un modelo de análisis de regresión multivariada.

5.1. Resultados de la muestra de DDEs para la detección de daños físicos y sus posibles soluciones

Como se mencionó en el capítulo 3, se utilizó una muestra de 78 DDEs de diferentes, marcas, modelos, capacidad y condición de funcionamiento, para analizarlos y determinar sus fallas físicas, la Figura 5.1 muestra una gráfica por marcas y capacidad, de la muestra de dichos DDEs. En el eje X se indican las capacidades de los DDEs expresada en Gigabytes (GB), y en el eje de las Y se indica la cantidad de DDEs.

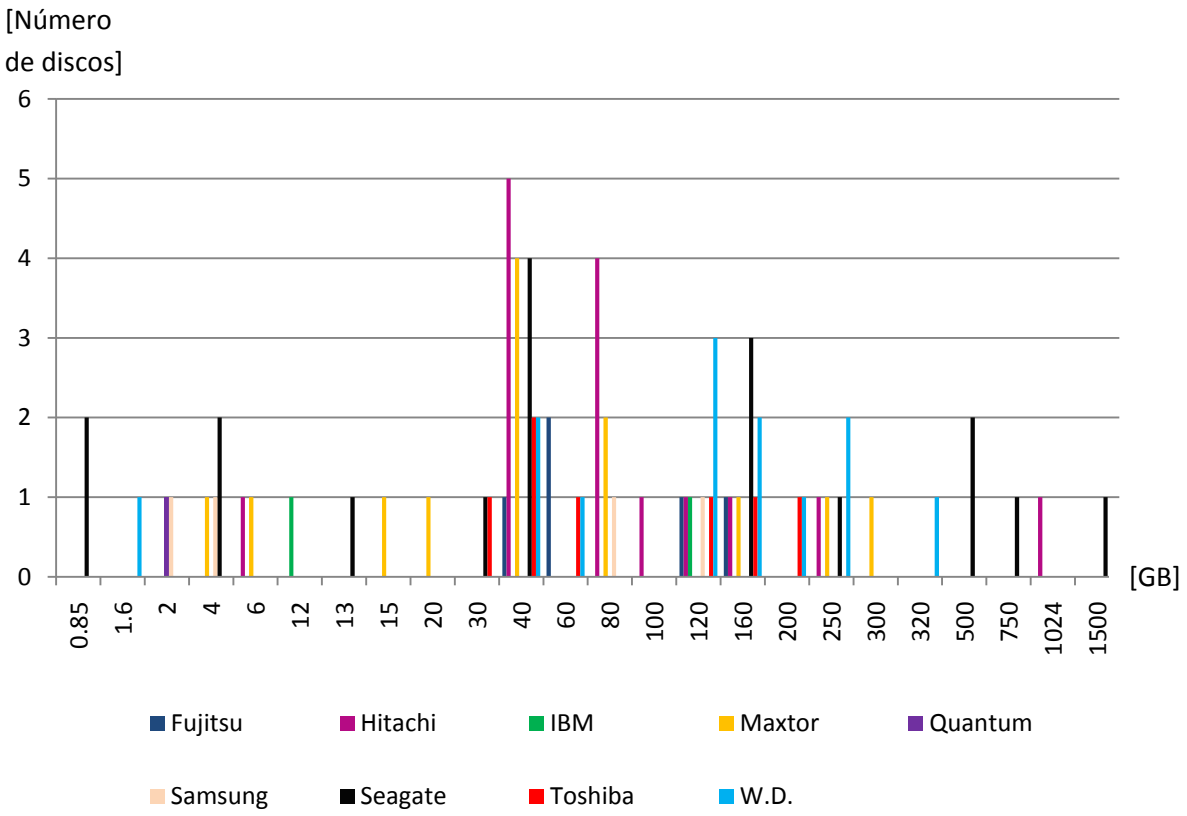


Figura 5.1. Gráfica de la muestra de DDEs por marca y capacidad.

Se observa que el grueso de la muestra está ubicado en la capacidad de 40GB, 120GB y 160GB. Y las marcas que predominan son Seagate y Hitachi, seguidos por Maxtor y W.D.

Se realizó un estudio de los daños que se encontraron en cada uno de los discos, y se englobaron para obtener una clasificación. Cada uno de estos daños puede variar en severidad, es decir, en un DDE que se clasifica como "sectores dañados", el porcentaje de sectores que no se puedan leer y por tanto copiar, determinará si la información es irrecuperable. De igual forma, en un DDE con daño en la PCB, el elemento dañado determinará la posibilidad de recuperar la información; ya que si se llega a dañar un elemento insustituible como el CI con el firmware, el DDE quedará inaccesible y por tanto la información irrecuperable.

11 DDEs presentaron más de una falla, en la tabla 5.1, se describen los discos que presentaron esta condición.

Tabla 5.1. Descripción de DDEs con más de una falla.

MARCA	CAPACIDAD (GB)	FALLAS
Fujitsu	60	Daño en CI de motor y sectores dañados
Maxtor	6	Sectores dañados y sobrescritura
Quantum	2	Cabezas/platos sucios y sectores dañados
Seagate	750	Bug en firmware y daño de la *media*
Seagate	1500	Motor *stuck* y *headcrash* visible
Toshiba	30	Daño interno en motor y *stiction*
Toshiba	120	Sectores dañados y daño en el SA
Toshiba	160	
Hitachi	80	
W.D.	120	Desprendimiento de *slider* y *headcrash* visible
W.D.	60	

La combinación de dos o más daños, tanto físicos como lógicos, requieren la aplicación de más de una solución, lo que repercute en la disminución del porcentaje de posibilidad de recuperar la información. El daño lógico puede generarse al momento de presentarse el daño físico, por ejemplo, cuando las cabezas comienzan a fallar, pueden sobreescribir la estructura del sistema de archivos. Pero también se puede presentar el daño lógico como consecuencia de la recuperación incompleta del daño físico, por ejemplo, cuando un DDE que ha sido reparado temporalmente vuelve a fallar antes de obtener la imagen completa, y ya no es posible volver a repararlo, la estructura y/o información estará incompleta, requiriéndose la recuperación a nivel lógico.

La gráfica de la Figura 5.2 muestra el porcentaje de DDE's del total de la muestra por tipo de falla.

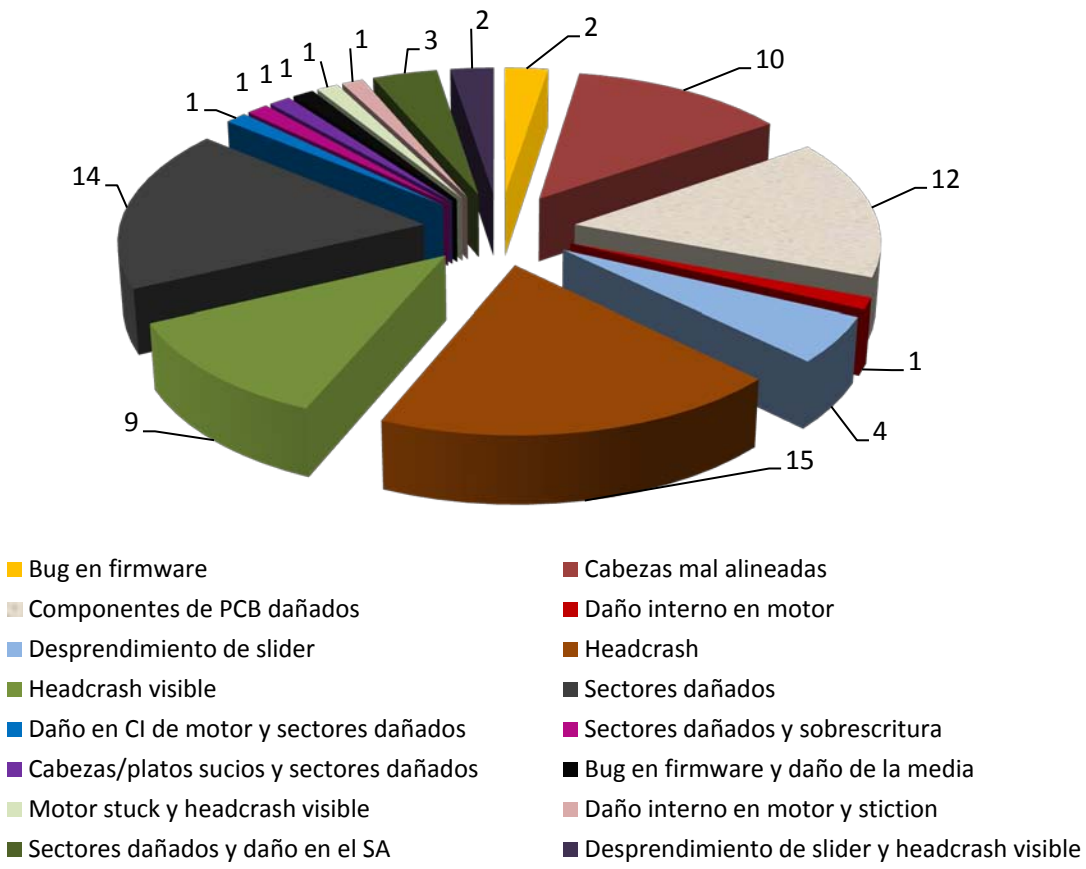


Figura 5.2. Tipos de falla de la muestra de 78 DDEs.

De la Figura 5.2, se observa que el daño con mayor incidencia en la muestra es el *headcrash,* seguido por Sectores dañados. Es decir, los daños que predominaron fueron aquellos que afectan a la *media*.

De los daños que tuvieron menor incidencia fueron las combinaciones de daños, así como aquellos daños que afectan al motor.

La gráfica de la Figura 5.3 muestran los tipos de daños encontrados por marcas de DDE, para los 67 casos que presentan un sólo daño. En el eje de las X se indican los tipos de daños y en el eje Y se indica la cantidad de DDEs.

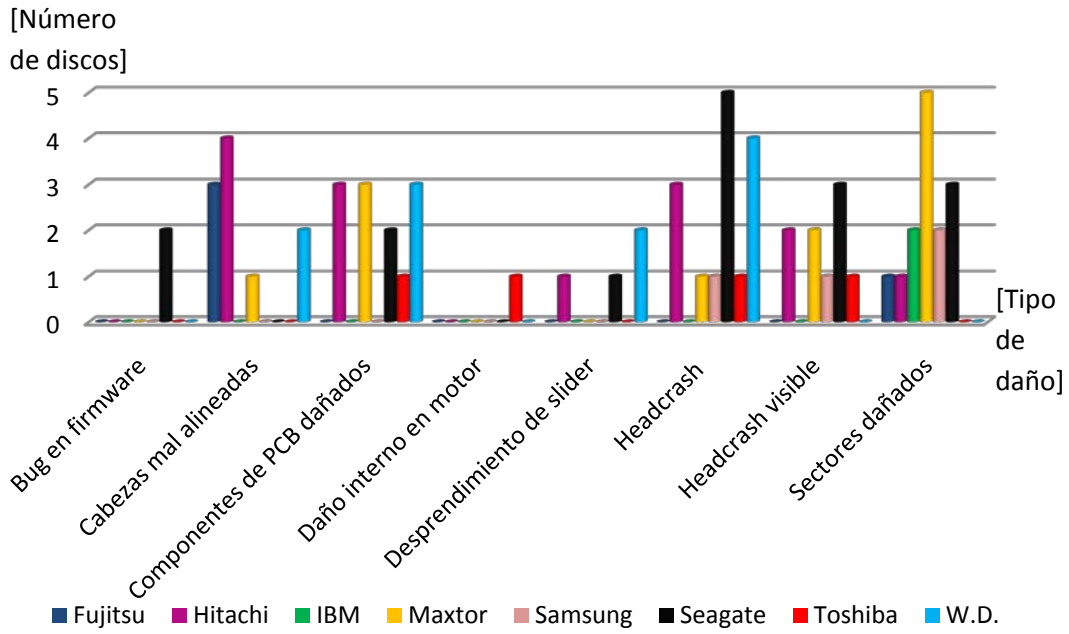


Figura 5.3. Gráficas de los DDEs por tipo de daño y marca.

En la muestra de la gráfica 5.3 los daños más frecuentes son *headcrash* visible/no visible, y sectores dañados. Dentro de estos daños, las marcas que se encuentran son Seagate, Maxtor y Hitachi. Los sectores dañados afectan a varias marcas de discos duros, aunque los más afectados fueron los Maxtor. De los daños con una o dos incidencias, son daño a motor y bug en firmware.

Una vez que se identificaron los daños, se hizo un extremo análisis y estudio para buscar las soluciones apropiadas. En más de una de ellas se encontraron varias posibles soluciones. Se aplicaron dichas soluciones con la finalidad de reparar temporalmente al DDE, pero en la mayoría de casos no se tuvo éxito, debido a que no se contaban con los recursos necesarios, como DDEs donadores (debido a la gran diversidad de modelos), o porque no se contaba con las herramientas necesarias.

La tabla 5.2 muestra la descripción de cada DDE con el daño que presentó, se indican las posibles soluciones y si es que se puede recuperar, y en los casos que no se logró éxito, se describe la causa.

Tabla 5.2. Descripción de DDEs, falla, posibles soluciones, y resultado de la reparación.

MARCA	CAPA-CIDAD (GB)	FALLA (S)	SOLUCIÓN	ÉXI-TO	CAUSA DE NO ÉXITO
Fujitsu	40	Cabezas mal alineadas	Cambio de *head-stack*	no	No se consiguió DDE donador
	60	Daño en CI de motor y sectores dañados	Reparación a nivel de componente y copia física forzada	si	
		Cabezas mal alineadas	Limpieza de la *media* y/o cambio *head-stack*	no	No se consiguió DDE donador. La limpieza no funciono
	120	Sectores dañados	Copia física forzada	si	
	160	Cabezas mal alineadas	Limpieza de la *media* y/o cambio *head-stack*	no	No se consiguió DDE donador. La limpieza no funciono
Hitachi	6	Desprendimiento de *slider*	Cambio de *head-stack*	no	No se consiguió DDE donador
	40	Cabezas mal alineadas	Cambio de *head-stack* y copia física forzada	si	
		Componentes de PCB dañados	Reparación a nivel de componente	si	
		Headcrash visible	Cambio de *head-stack*	no	Si se consiguió DDE donador pero la *media* daño nuevamente a las cabezas
		Headcrash visible	Limpieza de la *media* y/o cambio *head-stack*		No se consiguió DDE donador. La limpieza no funciono
		Sectores dañados	Copia física forzada	si	
	80	Sectores dañados y daño en el SA	Copia física forzada, reparación de estructura y ejecución de software especial para recuperar datos	si	
		Headcrash	Cambio de *head-stack*	no	Daño en la *media*, no funciono cambio de *head-stack*
		Headcrash			No se consiguió DDE donador
		Headcrash			Pocos sectores en buen estado

MARCA	CAPA-CIDAD (GB)	FALLA (S)	SOLUCIÓN	ÉXI-TO	CAUSA DE NO ÉXITO
Hitachi	100	Componentes de PCB dañados	Reparación a nivel de componente y/o cambio de PCB completa	no	No se consiguió PCB compatible
	120	Cabezas mal alineadas	Cambio de *head-stack*		No se consiguió DDE donador
	160	Componentes de PCB dañados	Reparación de fusible	si	
	250	Cabezas mal alineadas	Limpieza de la media y/o cambio *head-stack*	no	No se consiguió DDE donador. La limpieza no funciono
	1024				
IBM	12	Sectores dañados	Copia física forzada	si	
	120				Hay sectores que no se pudieron copiar
Maxtor	4	*Headcrash*	Cambio de *head-stack*	no	No se consiguió DDE donador
	6	Sectores dañados y sobrescritura	Copia física forzada y ejecución de software para recuperar datos		Sobreescritura total
	15	Componentes de PCB dañados	Cambio a nivel de componente o total		No se consiguió PCB compatible
	20		Cambio de PCB completa		
	40	*Headcrash* visible	Cambio de *head-stack*	no	No se consiguió DDE donador
		Headcrash visible			
		Sectores dañados	Copia física forzada	si	
		Sectores dañados			
	80	Sectores dañados	Copia física forzada	si	Hay sectores que no se pudieron copiar
		Sectores dañados		no	Pocos sectores buenos
	160	Sectores dañados	Copia física forzada	si	Hay sectores que no se pudieron copiar
	250	Cabezas mal alineadas	Cambio de *head-stack*	no	No se consiguió DDE donador
	300	Componentes de PCB dañados	Cambio a nivel de componente o total	no	No se consiguió PCB compatible
Quantum	2	Cabezas/platos sucios, sectores dañados	Limpieza de cabezas y copia física forzada	si	

MARCA	CAPA-CIDAD (GB)	FALLA (S)	SOLUCIÓN	ÉXI-TO	CAUSA DE NO ÉXITO
Samsung	2	Sectores dañados	Copia física forzada	si	
	4	*Headcrash*	Cambio de *head-stack*	no	No se consiguió DDE donador
	80	Sectores dañados	Copia física forzada	si	
	120	*Headcrash* visible	Irrecuperable	no	Destrucción de la *media*
Seagate	0.85	*Headcrash* visible	Irrecuperable	no	Destrucción de la *media*
	0.85				
	4	*Headcrash*	Cambio de *head-stack*	no	
		Sectores dañados	Copia física forzada	si	
	13	*Headcrash*	Cambio de *head-stack*	no	No se consiguió DDE donador
	30		Limpieza de *media*		Daño severo en la *media* aunque no es visible
	40	Componentes de PCB dañados	Cambio de PCB completa	no	No se consiguió PCB compatible
		Desprendimiento de *slider*	Limpieza de la *media* y/o cambio *head-stack*	no	No se consiguió DDE donador. La limpieza no funciono
		Headcrash	Cambio de *head-stack*	no	No se consiguió DDE donador
		Headcrash			
	160	*Headcrash* visible	Irrecuperable	no	Destrucción de la *media*
		Sectores dañados	Copia física forzada	si	
		Sectores dañados			
	250	Componentes de PCB dañados	Reparación de PCB a nivel de componente	no	No se consiguió PCB donadora
	500	Bug en firmware	Reseteo de firmware	si	
	500				
	750	Bug en firmware y daño de la *media*	Irrecuperable	no	La *media* donde se ubica el firmware está dañado
	1500	Motor *stuck* y *headcrash* visible	Uso de herramienta "motor unstuck"	no	La *media* estaba destruida

MARCA	CAPA-CIDAD (GB)	FALLA (S)	SOLUCIÓN	ÉXI-TO	CAUSA DE NO ÉXITO
Toshiba	30	Daño interno en motor y *stiction*	Lubricación del motor y/o cambio de HDA	si	Se lubrico el motor, y se hizo copia física forzada
	40	Daño interno en motor			
	40	*Headcrash*	Cambio de *head-stack*	no	Daño severo en la *media* aunque no visible. Cambio de *head-stack* no funciono
	60	*Headcrash* visible	Limpieza de la *media* y/o cambio *head-stack*		Se consiguió DDE donador pero la *media* daño nuevamente a las cabezas
	120	Sectores dañados y daño en el SA	Copia física forzada, reparación de estructura y ejecución de software especial para recuperar datos	si	
	160				Muchos sectores dañados
	200	Componentes de PCB dañados	Reparación a nivel de componente y/o cambio de PCB completa	no	No se consiguió PCB compatible
W.D.	1.6	*Headcrash*	Cambio de *head-stack*	no	No se consiguió DDE donador
	40	Cabezas mal alineadas			
	40	*Headcrash*		si	El daño en la *media* ocasiona daño en cabezas
	60	Desprendimiento de *slider* y *headcrash* visible	Limpieza de la *media* y cambio *head-stack*	no	No se consiguió DDE donador. La limpieza no funciono
	120		Cambio de *head-stack*		No se consiguió DDE donador
	120	Desprendimiento de *slider*	Cambio de *head-stack*	no	No se consiguió DDE donador
	120				
	160	Cabezas mal alineadas			
	160	Componentes de PCB dañados	Cambio a nivel de componentes	no	No se consiguió PCB compatible
	200	*Headcrash*	Cambio de *head-stack*	no	No se consiguió DDE donador
	250				
	250	Componentes de PCB dañados	Cambio de PCB a nivel de componente y/o cambio de *head-stack*	no	No se obtuvo el cautín de aire para cambio de CI
	320				No se consiguió DDE donador

Existen casos en los que no se pudo recuperar la información por la severidad del problema, principalmente por daño en la *media*. La Figura 5.4 muestra una gráfica por marca y capacidad de DDE de los casos determinados como *irrecuperables* por la severidad del daño, más que por la falta de recursos. El daño que predominó en los casos irrecuperables fue el *headcrash* visible, el cual afectó a 4 diferentes marcas de DDE. Los discos Seagate presentan variedad en los tipos de daños. En el eje X se indican las marcas de los discos y en el eje Y el porcentaje que representa cada tipo de daño.

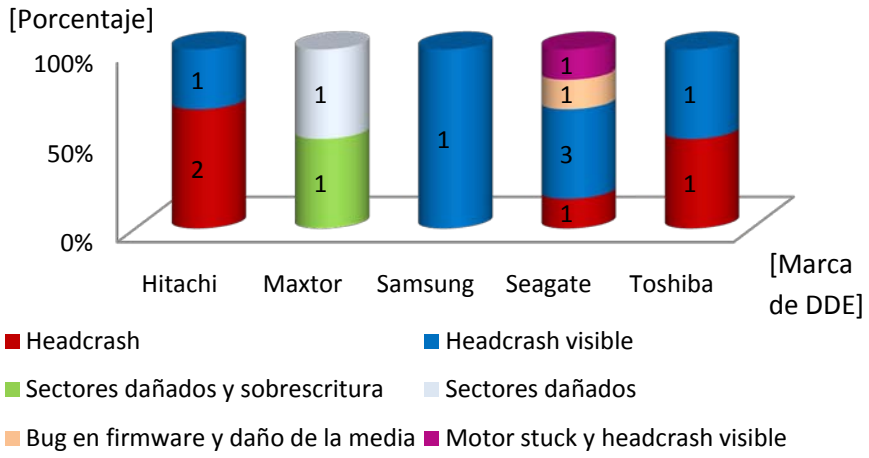


Figura 5.4. Gráficas de los DDEs irrecuperables.

La gráfica de la Figura 5.5 describe los motivos por los que no se tuvo éxito en la reparación del DDE. El motivo principal es por la destrucción de la *media*. En el eje X se indican las marcas de los discos y en el eje Y el porcentaje que representa cada motivo de no éxito.

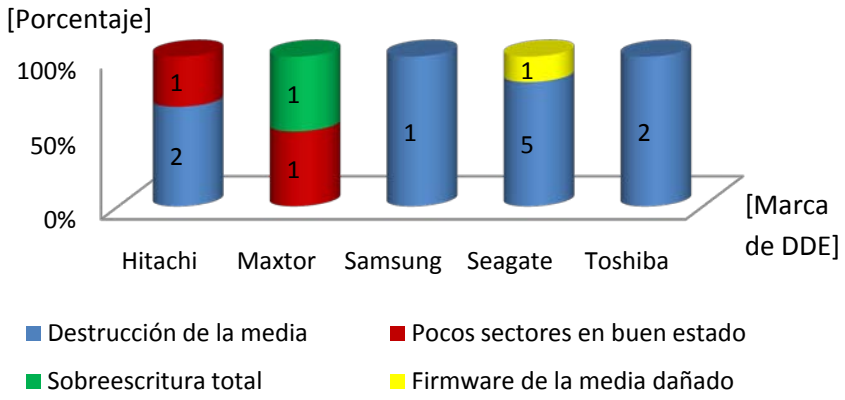


Figura 5.5. Gráficas de la causa de no éxito en los DDEs irrecuperables.

Durante el análisis de los DDEs, se desarrollaron 2 herramientas, para la reparación temporal del DDE dañado. Una de ellas es el denominado “motor unstuck”, llamado así por el daño al que da solución, y la otra herramienta es un cable con conector RS232 para la reparación del firmware en los DDEs marca Seagate. La tabla 5.3 describe los casos en los que se utilizó alguna de las dos herramientas y se indican los casos de éxito, que fueron aquellos que sólo presentaron Bug en el firmware, no así en los casos con dos tipos de daño.

Tabla 5.3. Descripción de casos en los que se aplicaron las herramientas desarrolladas.

MARCA	CAPACIDAD (GB)	FALLA (S)	HERRAMIENTA UTILIZADA	ÉXITO	CAUSA DE NO ÉXITO/CANTIDAD DE INFORMACIÓN RECUPERADA
Seagate	500	Bug en Firmware	Reseteo de firmware con el cable RS232	si	
Seagate	500	Bug en Firmware	Reseteo de firmware con el cable RS232	si	
Seagate	750	Bug en Firmware y daño en la *media*	Reseteo de firmware con el cable RS232	no	Daño visible en la *media*
Seagate	1500	Motor *stuck* y *headcrash* visible	Uso de herramienta "motor unstuck"	no	Daño visible en la *media*

En la Figura 5.6 se muestra la gráfica de los casos en los que se tuvo éxito, de acuerdo a la marca y capacidad del disco, tanto utilizando las herramientas como alguna de las posibles soluciones propuestas. En el eje X se indican las capacidades de los DDEs expresada en Gigabytes (GB), y en el eje de las Y se indica la cantidad de DDEs.

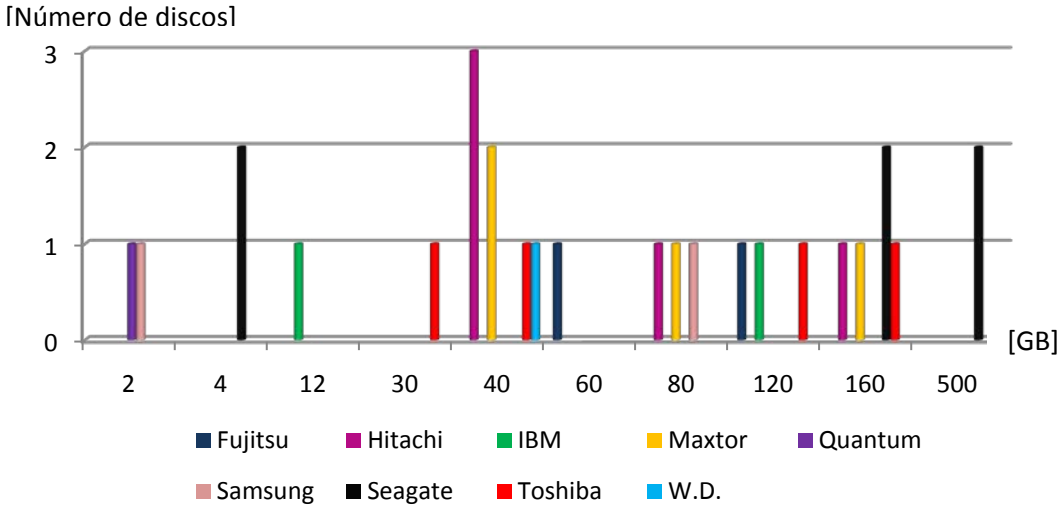


Figura 5.6. Gráficas de los DDEs reparados temporalmente.

La capacidad que predominó en los discos reparados temporalmente fue 40GB, y la marca fue Seagate seguida por Hitachi.

La Figura 5.7 muestra los casos recuperados de acuerdo a la marca y el daño. En el eje X se indican las marcas de DDE, y en el eje Y la cantidad de DDEs de dichas marcas.

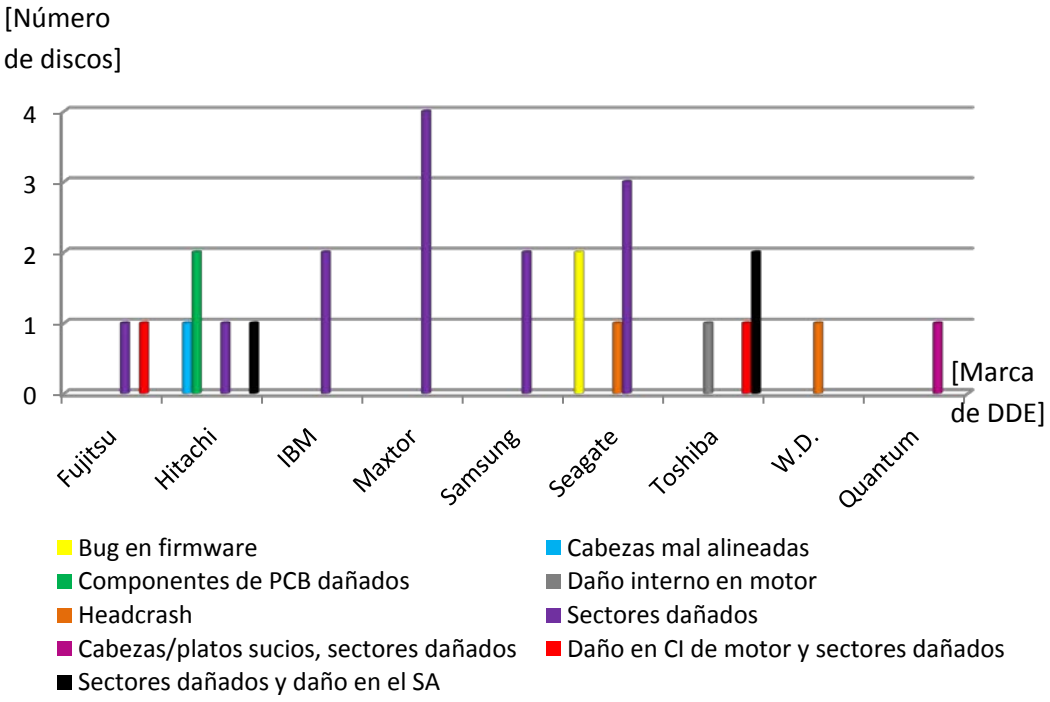


Figura 5.7. Gráficas de los DDEs reparados temporalmente por marca y daño.

Los casos con mayor éxito fueron los que tuvieron sectores dañados y la combinación de sectores dañados con un daño lógico, como lo es el daño en el Sistema de Archivos.

5.2. Resultados de la metodología propuesta

Para la realización del presente trabajo, se recibieron mediante donación, 89 DDEs; de los cuales 78 presentaron daño físico y 11 presentaron daño lógico. Sólo se efectuó el proceso de Recuperación de Información en los primeros 40 DDEs recibidos, ya que en estos casos la Recuperación de información se requería de forma inmediata. Mientras que para los otros 49 casos, la recuperación no era necesaria, adicionalmente a que no pudo realizar la reparación temporal y por consiguiente su recuperación de datos.

De la muestra ahora conformada por sólo 40 DDEs, a los primeros diez recibidos, se les efectuó el proceso de Recuperación de información utilizando mejores prácticas como las establecidas por Scott Moulton [40], estos casos sirvieron como base para establecer y delimitar cada una de las etapas y fases de la metodología descrita en el capítulo 4, la cual se aplicó a los siguientes 30 DDEs recibidos.

La Figura 5.8 muestra una gráfica de la muestra de 40 DDEs por marca y capacidad. En el eje de las X se indican las marcas de los DDEs y en el eje de las Y, la cantidad de DDEs.

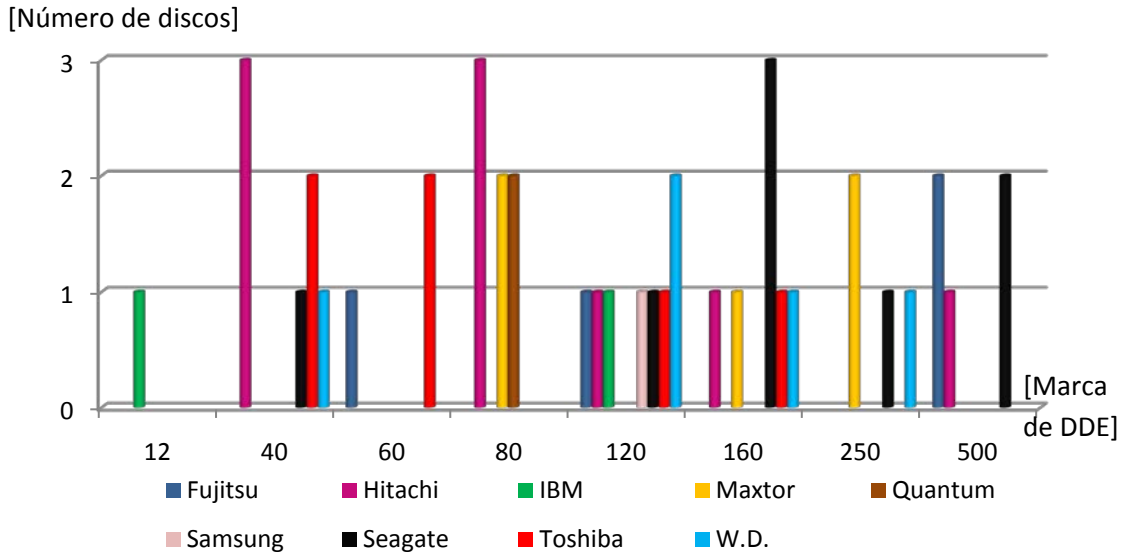


Figura 5.8. Gráfica de 40 DDEs a los cuales se les aplicó el proceso de Recuperación de datos.

La mayoría de DDEs recibidos fue de la marca Hitachi seguida por Seagate y de las capacidades de 120GB, seguidas en igual número de DDEs por 40GB, 80GB y 160GB.

La Figura 5.9 muestra una gráfica con los principales daños presentados en los 40 DDEs recuperados.

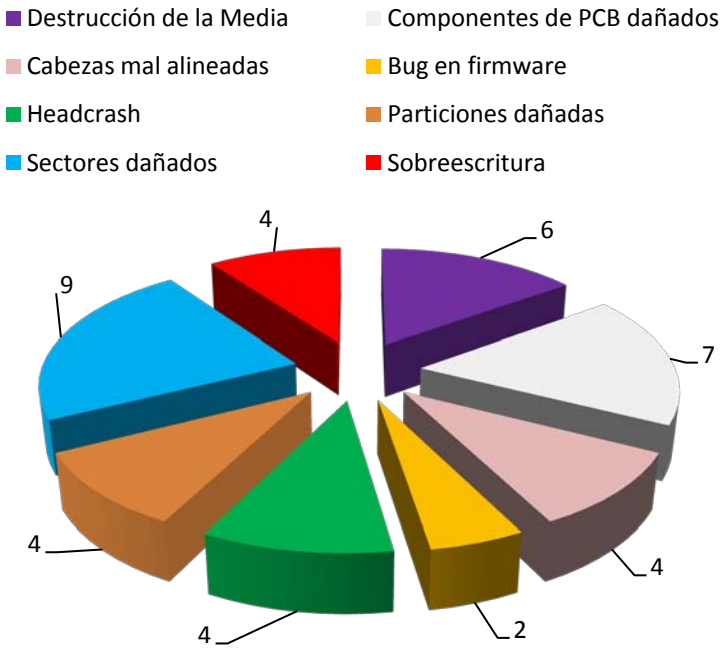


Figura 5.9. Tipos de daños identificados en la muestra de 40 DDEs.

El daño que predomina son los sectores dañados, seguidos por componentes de PCB dañados y destrucción de *media.*

La Figura 5.10 muestra una gráfica donde se indican los diferentes tipos de daño por marcas de DDEs. En el eje de las X de indican las diferentes marcas, y en el eje de las Y se indica la cantidad de DDEs. La marca Hitachi es la que presenta más variedad de tipo de daños, seguida por Seagate y W.D.

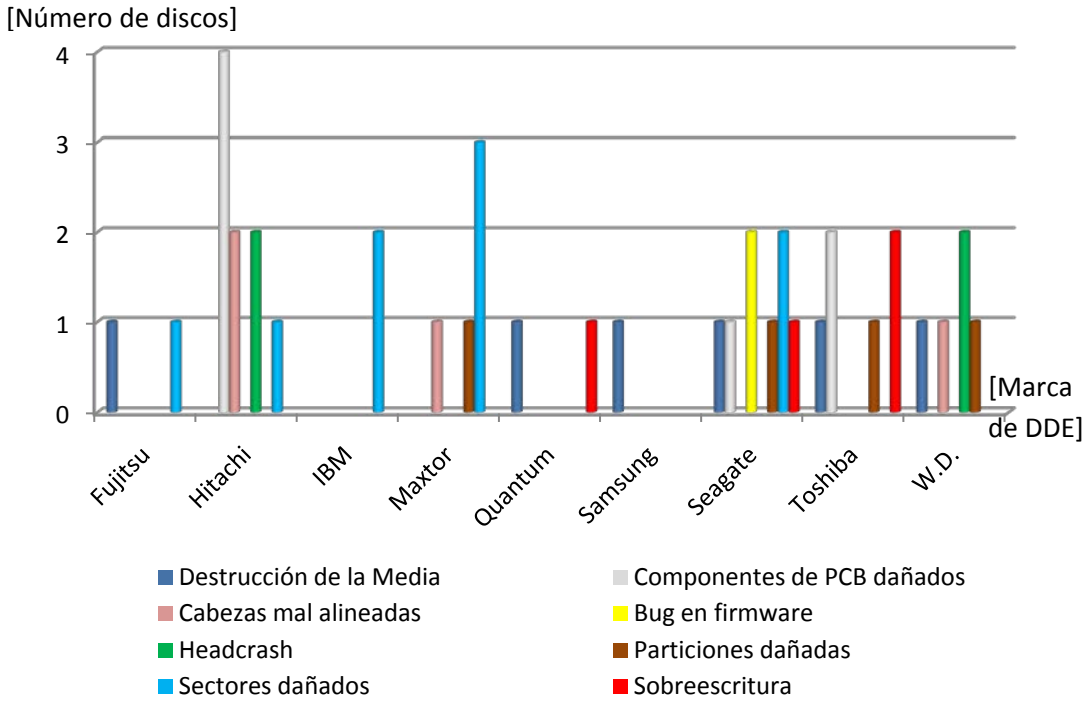


Figura 5.10. Muestra de 40 DDEs por marcas y tipos de daños.

Al finalizar las recuperaciones de datos, se realizó un análisis estadístico a través de un modelo de regresión multivariada sobre la muestra de datos de las 40 Recuperaciones de datos.

Una regresión multivariada es una técnica estadística que puede utilizarse en los análisis para establecer la relación entre una variable criterio y un conjunto de variables independientes o predictoras, cuyos valores son conocidos y no se pueden controlar.

El objetivo del análisis de regresión multivariada es utilizar los valores del conjunto de variables independientes para predecir el valor de la variable dependiente, seleccionada previamente por el investigador. Además de cuantificar la relación entre cada una de las variables independiente con la variable dependiente, mediante ponderaciones, las cuales aseguran la máxima predicción y facilitan la interpretación de la influencia de cada variable en la realización de la predicción [51].

El análisis estadístico realizado fue desarrollado a través de 4 pasos, como se muestra en el diagrama de la Figura 5.11.

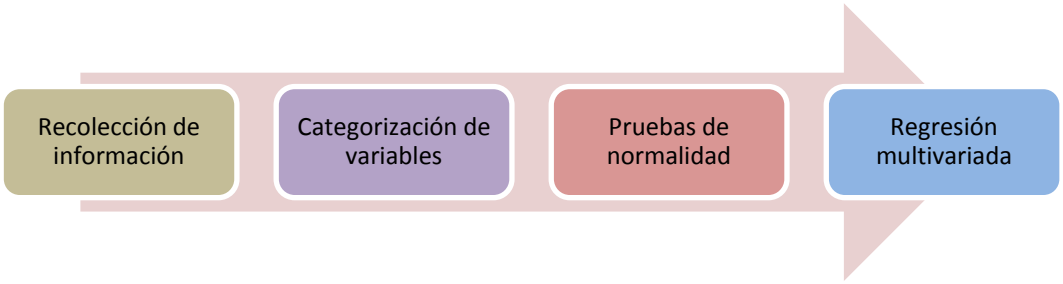


Figura 5.11. Pasos del análisis estadístico de regresión multivariada.

1. **Recolección de Información**

Se recolectó la información de relativa importancia de cada uno de los casos de Recuperación de datos, tales como: marca, capacidad, daño, antigüedad del DDE, entre otros; los cuales se describen a continuación:

Marca: La marca del fabricante del DDE, la muestra obtenida no abarca el total de los fabricantes.

Modelo: El modelo de acuerdo al fabricante. Este dato puede proporcionar información sobre la capacidad del DDE.

Capacidad: La capacidad de almacenamiento del DDE.

No. de serie: El número único con el cual se identifica a cada DDE.

Antigüedad: De acuerdo al año de fabricación de cada DDE de forma independiente.

Tipo de daño: El daño que presentó a nivel físico y lógico, de acuerdo a la clasificación establecida en el capítulo 2 y 3.

Solución: Propuesta de una o varias soluciones para reparar temporalmente al DDE, de acuerdo a los mostrados en el capítulo 2 y 3.

Éxito en la reparación: Se indica sí se tuvo éxito en la reparación temporal del DDE.

Utilización de metodología: Se indica sí se aplico la metodología propuesta del capítulo 4, para la recuperación de datos.

Porcentaje de copia física: Se indica el porcentaje de la copia *bit* a *bit* obtenido del DDE reparado temporalmente.

Cantidad de información recuperada: La cantidad de información expresada en GB, recuperada al finalizar el proceso de recuperación de datos.

Cantidad de información no recuperada: La cantidad de información expresada en GB, no recuperada, al finalizar el proceso de recuperación de datos, de acuerdo a lo indicado por el usuario del DDE.

Tipo de motor: Tipo de motor de acuerdo a la tecnología, es decir, se indica si es *Ball bearing* o *Fluid Dynamic Bearing*.

Tecnología de escritura/lectura: El tipo de tecnología que se utiliza para almacenar la información, es decir, se indica si es perpendicular o longitudinal.

Sistema de Archivos: El sistema de archivos que se utiliza en el DDE para gestionar la información. De acuerdo a la muestra, sólo hubo 2 tipos de SA: NTFS y FAT32.

Las mejores prácticas aplicadas a los diez primeros DDEs, consta de 4 etapas (reparación del disco duro, imagen o copia, recuperación lógica y reparación de archivos dañados), la tabla 5.4 describe los tiempos invertidos en cada una de dichas etapas por cada DDE.

Tabla 5.4. Tiempos de las etapas de las "mejores prácticas" aplicadas a 10 DDEs.

MARCA	CAPACIDAD [GB]	ÉXITO EN RECUPERACIÓN	TIEMPO (HORAS)			
			Etapa 1	Etapa 2	Etapa 3	Etapa 4
Toshiba	60	si	0	3	7	0
Maxtor	250	si	0	12	18	0
Hitachi	40	si	2	5	5	0
Hitachi	80	no	3	3	0	0
Hitachi	120	no	6	0	0	0
W.D.	120	no	1	0	0	0
W.D.	120	no	5	0	0	0
Seagate	40	no	0	2	6	2
Seagate	250	no	4	0	0	0
Quantum	80	si	0	4	10	4

El tiempo invertido en total en el proceso de recuperación de información depende de la capacidad del DDE y del daño. Como se observa en la tabla 5.5, para los DDEs de mayor capacidad se invirtió mayor tiempo en la etapa 1, aun cuando la reparación no tuvo éxito. La única excepción fue para un caso de un DDE de 250GB, en el cual para la etapa 1 no e invirtió tiempo ya que se trató de un daño lógico, no así para las demás etapas, en las que la recuperación y búsqueda de información tuvo que efectuarse sector a sector.

La metodología utilizada para los siguientes 30 casos, consta de 7 etapas (Análisis físico, Reparación física temporal, Obtención de imagen, Análisis lógico, Reparación lógica, Recuperación de datos y Reparación de archivos críticos), la tabla 5.5 describe los tiempos invertidos en cada etapa, para los 30 DDEs.

Tabla 5.5. Tiempos de las etapas de la metodología propuesta aplicadas a 30 DDEs.

MARCA	CAPACI-DAD (GB)	ÉXITO EN RECUPERACIÓN	TIEMPO (HORAS)						
			Etapa 1	Etapa 2	Etapa 3	Etapa 4	Etapa 5	Etapa 6	Etapa 7
Fujitsu	60	si	0.50	1.00	2.00	0.25	0.00	4.00	0.00
Fujitsu	120	si	0.25	0.00	3.50	0.25	0.00	4.00	0.00
Hitachi	160	si	0.25	0.00	2.00	0.50	0.25	2.00	0.00
Hitachi	40	si	0.25	0.25	1.00	0.25	0.00	1.50	0.00
Hitachi	500	si	0.25	0.00	6.00	0.50	0.15	8.00	0.00
Hitachi	80	no	2.00	0.00	0.00	0.00	0.00	0.00	0.00
Hitachi	40	si	0.25	0.00	3.00	0.25	0.00	4.00	0.00
Hitachi	80	si	0.25	0.00	3.00	0.25	0.00	6.00	0.00
IBM	120	si	0.25	0.00	5.00	0.50	0.25	4.00	1.00
IBM	12	si	0.25	0.00	2.00	0.25	0.25	1.00	0.00
Maxtor	250	no	2.00	0.00	0.00	0.00	0.00	0.00	0.00
Maxtor	160	si	0.25	0.00	5.00	0.50	0.25	2.00	0.50
Maxtor	80	no	0.25	1.75	4.00	0.00	0.00	0.00	0.00
Maxtor	80	si	0.25	0.00	3.00	0.50	0.25	2.50	0.50
Quantum	80	si	0.25	0.00	2.00	0.25	0.00	2.00	0.00
Samsung	120	no	1.50	0.00	0.00	0.00	0.00	0.00	0.00
Seagate	500	si	0.50	1.00	8.00	0.25	0.00	7.00	0.00
Seagate	160	no	0.50	0.00	0.00	0.00	0.00	0.00	0.00
Seagate	160	si	0.25	0.00	4.00	0.25	0.00	5.00	0.00
Seagate	160	si	0.25	0.00	10.00	0.25	0.00	5.00	0.00
Seagate	500	si	0.25	0.75	8.00	0.15	0.00	4.00	0.00
Seagate	120	si	0.25	0.00	3.00	0.50	0.50	3.00	0.00
Toshiba	40	si	0.25	0.00	1.00	1.00	0.75	2.00	1.00
Toshiba	120	si	0.15	0.00	18.50	0.50	0.50	5.00	2.00
Toshiba	160	si	0.50	0.00	8.00	0.25	0.50	4.50	0.00
Toshiba	40	no	0.25	0.00	1.00	0.25	0.00	0.00	0.00
Toshiba	60	no	0.25	0.00	1.50	0.25	0.00	0.00	0.00
W.D.	160	no	1.00	0.00	0.00	0.00	0.00	0.00	0.00
W.D.	40	si	0.50	2.00	1.00	0.25	0.00	1.00	0.25
W.D.	250	si	0.25	0.00	4.00	0.50	0.25	4.50	0.50

De la tabla 5.6 se puede observar que las etapas que requieren mayor tiempo son la 3 y 6, ya que en ambos casos no importa cuanta información almacena exista, si no el total de la capacidad de almacenamiento del DDE. En la etapa 3, se crea una imagen bit a bit, por lo que además de influir la capacidad del DDE en el tiempo invertido, también influye la existencia de sectores dañados, estos sectores aumentan el tiempo cuando se configura a los programas (con los que se realiza la imagen) para intentar leer dichos sectores más de una vez, con el objetivo de obtener un mayor porcentaje de la copia. Mientras que en la etapa 6, el tiempo invertido es alto, debido a que se buscan archivos y carpetas en toda la copia del DDE, sector por sector.

Para las demás etapas, el tiempo invertido varía en función del tipo de daño y la solución y/o soluciones aplicadas.

2. Categorización de variables

- Se categoriza cada variable de la información recuperable. Categorizar es el proceso de estandarizar el catalogo de los tipos de daño.

- Se realizó la construcción de la variable de respuesta que es la tasa de recuperación, a la cual se le llama *Recorate*, la cual se obtiene del cociente de la cantidad de información recuperada en bytes y la capacidad del DDE, como se muestra en la ecuación 5.1.

$$Y = \frac{\#\ de\ bytes\ recuperados}{\#\ total\ de\ bytes\ del\ DDE} \tag{5.1}$$

- Se realizó la identificación individual y excluyente de cada marca, tipo de daño y solución para poderlos someter al proceso de regresión multivariable; es decir, para las marcas de discos duros las variables son: mseagate, msamsung, mtoshiba, mwd, mhitachi, mfujitsu, mibm, mmaxtor y mquantum.

La categorización es un requerimiento para poder ejecutar el análisis de regresión multivariada.

3. Pruebas de normalidad

Se realizaron pruebas de normalidad en la variable de respuesta. Se eligió como variable de respuesta a la determinación de la tasa de recuperación (*recorate*), con el objetivo de describir los parámetros de la expresión de la ecuación 5.2:

$$Y = \beta_0 X_1 + \beta_1 X_2 \ldots \beta_{n-1} X_n + \varepsilon \qquad (5.2.)$$

Donde Y es la tasa de recuperación y está en función de las variables independientes $X_1 \ldots X_n$, donde el modelo de regresión multivariada nos deberá identificar los parámetros $\beta_0 \ldots \beta_{n-1}$, y ε es el error sistemático.

Para la prueba de normalidad se utilizó el *modelo de bondad de ajuste* Kolmogórov-Smirnov [52], donde el valor de la significancia para rechazar la hipótesis nula debe ser mayor a 0.10 considerando que la hipótesis nula es cuando la muestra no se ajusta a una distribución normal. En la tabla 5.6 se muestra el estadístico de descripción del modelo Kolmogórov-Smirnov, donde el valor de la significancia es 0.187.

Prueba de Kolmogorov-Smirnov para una muestra

		RecoRate
N		40
Parámetros normales(a,b)	Media	.2983
	Desviación típica	.31524
Diferencias más extremas	Absoluta	.172
	Positiva	.153
	Negativa	-.172
Z de Kolmogorov-Smirnov		1.088
Sig. asintót. (bilateral)		.187

a La distribución de contraste es la Normal.
b Se han calculado a partir de los datos.

Tabla 5.6. Muestra del modelo Kolmogórov-Smirnov.

Dado el valor de significancia que se observa en la tabla 5.6, se puede asegurar que la variable de respuesta tiene un comportamiento normal, lo que nos permite asegurar a través del *teorema de límite central,* que después del elemento 30 de la muestra, la

distribución se comporta estadísticamente como una distribución normal [53], es decir, que una muestra con 30 elementos es suficiente para caracterizar el comportamiento de la variable.

En la gráfica de la figura 5.12, se observa el histograma resultante de la prueba de Kolmogórov-Smirnov, donde se observa la frecuencia del evento de la variable dependiente *recorate*, y se verifica el comportamiento normal ya que no hay una tendencia especifica.

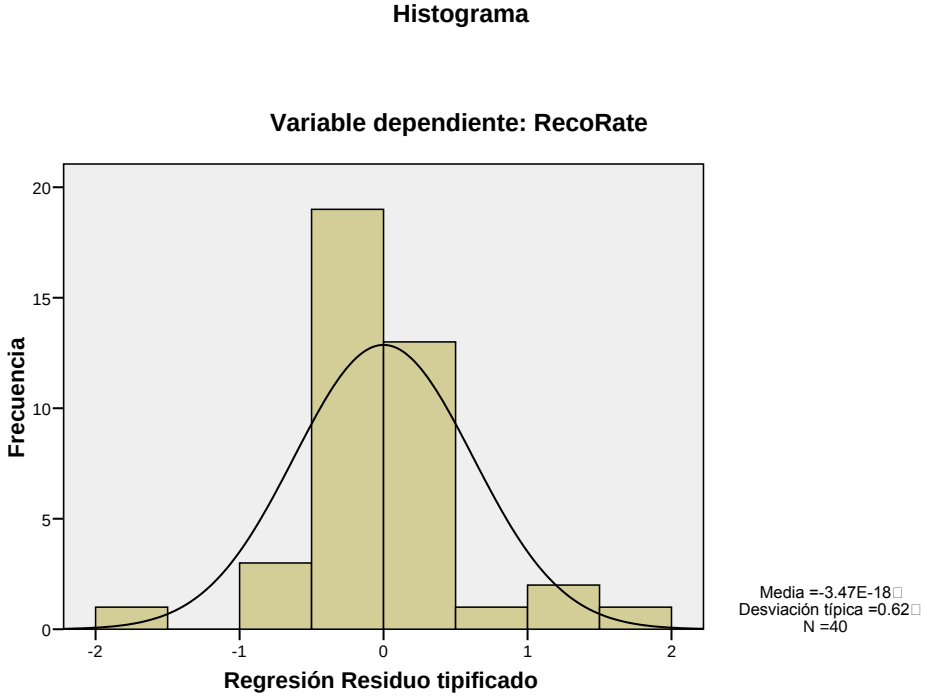


Figura 5.12. Histograma resultante de la prueba de Kolmogórov-Smirnov.

En la gráfica de la figura 5.13 también se puede observar la normalidad de la variable dependiente, ya que la probabilidad acumula observada, se acerca mucho a la esperada (teórica) que va de 0 a 1; tal como se espera del resultado de la prueba de Kolmogórov-Smirnov para una muestra normal.

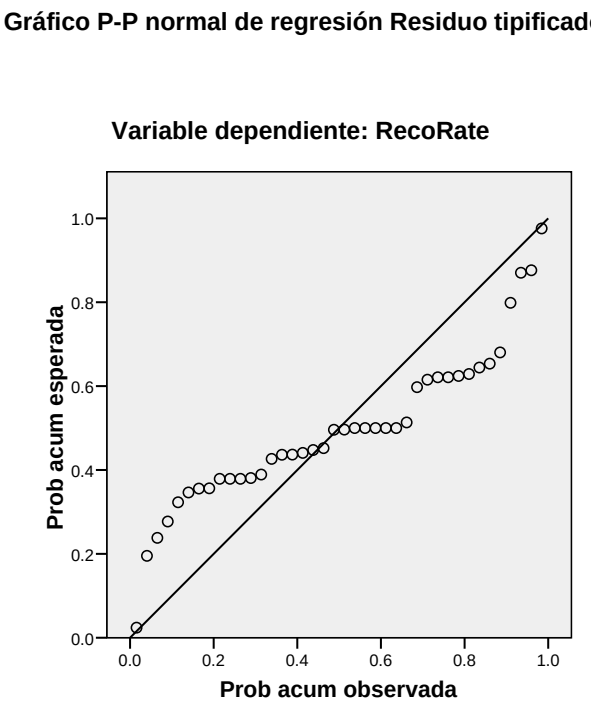


Figura 5.13. Gráfica de la probabilidad acumulada, de la prueba de Kolmogórov-Smirnov.

4. Regresión Multivariada

Una vez obtenidos los datos necesarios, se realizó el proceso de regresión multivariada sobre la muestra de los 40 DDEs, obteniendo los coeficientes β y obteniendo las variables que son significativas para la explicación de la variable dependiente Y (tasa de recuperación); y excluyendo las variables que no explican el comportamiento de los grados de recuperación de los DDEs. Este proceso fue realizado mediante un ANOVA (Analysis of Variance - análisis de la varianza).

Un análisis de varianza es una técnica estadística para el análisis de las mediciones en función de varios tipos de efectos que operan simultáneamente, para decidir qué tipo de efectos son importantes y estimar dichos efectos [54].

En la Tabla 5.7 se muestra el resultado del ANOVA y se indican los modelos. En cada modelo se van incrementando el número de variables independientes que utiliza el análisis para ir comparando la varianza y obtener un valor de significancia; y de esta forma decidir aquellas variables independientes que deban intervenir. El modelo que obtuvo mayor significancia es el que indica el conjunto de variables independientes a utilizar, en este caso, el modelo g.

Tabla 5.7. Modelos del ANOVA.

ANOVA(h)

Modelo	Comp	Suma de cuadrados	Gl	Sig.
a	Regresión	0.845	7	.294(a)
b	Regresión	1.825	12	.166(b)
c	Regresión	1.836	13	.498(c)
d	Regresión	2.161	14	.137(d)
e	Regresión	2.161	15	.561(e)
f	Regresión	2.882	23	.176(f)
g	Regresión	2.914	24	.891(g)

a Variables predictoras: (Constante), TDan8, TDan4, TDan5, TDan3, TDan6, TDan1, TDan2
b Variables predictoras: (Constante), TDan8, TDan4, TDan5, TDan3, TDan6, TDan1, TDan2, Sol5, Sol4, Sol6, Sol1, Sol3
c Variables predictoras: (Constante), TDan8, TDan4, TDan5, TDan3, TDan6, TDan1, TDan2, Sol5, Sol4, Sol6, Sol1, Sol3, Method
d Variables predictoras: (Constante), TDan8, TDan4, TDan5, TDan3, TDan6, TDan1, TDan2, Sol5, Sol4, Sol6, Sol1, Sol3, Method, Recovery
e Variables predictoras: (Constante), TDan8, TDan4, TDan5, TDan3, TDan6, TDan1, TDan2, Sol5, Sol4, Sol6, Sol1, Sol3, Method, Recovery, TWrite
f Variables predictoras: (Constante), TDan8, TDan4, TDan5, TDan3, TDan6, TDan1, TDan2, Sol5, Sol4, Sol6, Sol1, Sol3, Method, Recovery, TWrite, mIBM, mMaxtor, mHitachi, mQuatum, mSamsung, MFujitsu, mWD, mToshiba
g Variables predictoras: (Constante), TDan8, TDan4, TDan5, TDan3, TDan6, TDan1, TDan2, Sol5, Sol4, Sol6, Sol1, Sol3, Method, Recovery, TWrite, mIBM, mMaxtor, mHitachi, mQuatum, mSamsung, MFujitsu, mWD, mToshiba, SA
h Variable dependiente: RecoRate

En la tabla 5.8 se indican los coeficientes finales para cada variable independiente que se obtuvo mediante el ANOVA, dichos coeficientes indican el efecto que causan sobre la variable de respuesta. El valor indicado en Constante, es el error expresado en la ecuación 5.2.

Tabla 5.8. Valores de los coeficientes y error del ANOVA.

Var		B	Error Tip
	(Constante)	0.0346894	0.32
x1	TDan1	0.13767215	0.389
	TDan2	0.06325477	0.617
	TDan3	0.13581172	0.507
	TDan4	0.07627781	0.662
	TDan5	0.10418433	0.49
	TDan6	0.12650955	0.591
	TDan8	0.06325477	0.506
x2	Sol1	0.1020121	0.582
	Sol3	0.11006569	0.617
	Sol4	0.21476232	0.52
	Sol5	0.23623855	0.512
	Sol6	0.12080381	0.655
x3	Method	0.4134546	0.149
x4	Recovery	0.00160927	0.16
x5	TWrite	0.00234321	0.153
x6	mIBM	0.02186947	0.255
	MFujitsu	0.07654313	0.299
	mHitachi	0.02278069	0.205
	mMaxtor	0.07107577	0.196
	mQuatum	0.02278069	0.309
	mToshiba	0.00820105	0.292
	mWD	0.02004701	0.274
	mSamsung	0.01913578	0.389
	mSeagate	0.08018804	0.112
x7	SA	0.00228459	0.194

a Variable dependiente: RecoRate
Modelo 7 Variables predictoras: (Constante), TDan8, TDan6, TDan5, TDan4, TDan3, TDan2, TDan1, Sol6, Sol5, Sol4, Sol3, Sol1, Method, Recovery, TWrite, mIBM, mMaxtor, mHitachi, mQuatum, mSamsung, MFujitsu, mWD, mToshiba,mSeagate, SA
h Variable dependiente: RecoRate

El resultado de la ecuación de la ANOVA es:

$$Y = G(X_1) + H(X_2) + \beta_3 x_3 + \beta_4 x_4 + \beta_5 x_5 + I(X_6) + \beta_7 x_7 + \varepsilon \tag{5.3}$$

Sean:

$$\mathrm{B}_1 = \{\beta_{1,1}, \beta_{1,2}, \beta_{1,3}, \beta_{1,4}, \beta_{1,5}, \beta_{1,6}, \beta_{1,7}, \beta_{1,8}\},$$

$$\mathrm{B}_2 = \{\beta_{2,1}, \beta_{2,2}, \beta_{2,3}, \beta_{2,4}, \beta_{2,5}, \beta_{2,6}\},$$

$$\mathrm{B}_6 = \{\beta_{6,1}, \beta_{6,2}, \beta_{6,3}, \beta_{6,4}, \beta_{6,5}, \beta_{6,6}, \beta_{6,7}, \beta_{6,8}, \beta_{6,9}\},$$

$$X_1 = \{x_{1,1}, x_{1,2}, x_{1,3}, x_{1,4}, x_{1,5}, x_{1,6}, x_{1,7}, x_{1,8}\},$$

$$X_2 = \{x_{2,1}, x_{2,2}, x_{2,3}, x_{2,4}, x_{2,5}, x_{2,6}\},$$

$$X_6 = \{x_{6,1}, x_{6,2}, x_{6,3}, x_{6,4}, x_{6,5}, x_{6,6}, x_{6,7}, x_{6,8}, x_{6,9}\},$$

Se tiene entonces:

$$G(X_1) = \{c : c = \beta_{1,n} x_{1,m} \mid \beta \in \mathrm{B}_1, x \in X_1 \wedge x \neq 0\}$$

n=1,…,8
m=1,…,8

$$H(X_2) = \{c : c = \beta_{2,n} \cdot x_{2,m} \mid \beta \in \mathrm{B}_2, x \in X_2 \wedge x \neq 0\}$$

n=1,…,6
m=1,…,6

$$I(X_6) = \{c : c = \beta_{6,n} x_{6,m} \mid \beta \in \mathrm{B}_6, x \in X_6 \wedge x \neq 0\}$$

n=1,…,9
m=1,…,9

Al sustituir valores obtenidos de la ANOVA en la ecuación 5.3, se obtiene la ecuación 5.4:

$$Y = G(X_1) + H(X_2) + (0.4134546)x_3 + (0.00160927)x_4 + (0.00234321)x_5 + I(X_6) + (0.00228459)x_7 + 0.0346894$$

(5.4)

B_1={0.13767215, 0.06325477, 0.13581172, 0.07627781, 0.10418433, 0.12650955, 0.0, 0.06325477}

B_2={0.1020121, 0.0, 0.11006569, 0.21476232, 0.23623855, 0.12080381}

B_6={mIbm=0.02186947, mFujitsu=0.07654313, mHitachi=0.02278069, mMaxtor=0.07107577, mQuantum=0.02278069, mToshiba=0.00820105, mWD=0.02004701, mSamsung=0.01913578, mSeagate=0.08018804}

Donde:

X_1 corresponde a los tipos de daños.

TDan1: Variable del daño “sectores dañados”.

TDan2: Variable del daño “componente de PCB dañados”.

TDan3: Variable del daño “cabezas mal alineadas”.

TDan4: Variable del daño “bug en firmware”.

TDan5: Variable del daño “*headcrash*”.

TDan6: Variable del daño “particiones dañadas”.

TDan7: Variable del daño “destrucción de la *media*”.

TDan8: Variable del daño “sobreescritura”.

Sólo se puede presentar uno de los daños correspondientes a X_1. Cuando se presente, la X_1 del coeficiente correspondiente, se sustituirá por el valor 1, y las demás por 0.

X_2 corresponde a las soluciones.

Sol1: Variable de la solución “cambio de *headstack*”.

Sol2: Variable de “Irrecuperable”.

Sol3: Variable de la solución “reparación de la estructura lógica”.

Sol4: Variable de la solución “uso de software especializado para recuperar datos”.

Sol5: Variable de la solución “copia física forzada”.

Sol6: Variable de la solución “Reparación a nivel de componente”.

Se puede aplicar sólo una solución para X_2, cuando se aplique la solución, la X_2 del coeficiente correspondiente, se sustituirá por el valor 1, y las demás por el valor 0.

X_3=Method: Variable del uso de la metodología propuesta, con metodología=1, sin metodología=0.

X_4=Recovery: Variable del éxito de la reparación temporal, éxito=1, no éxito=0.

X_5=TWrite: Variable del tipo de escritura/lectura, longitudinal=1, perpendicular=0.

X_7=SA: Se refiere a la variable del Sistema de Archivos, NTFS=1, FAT32=0.

X_6 correspondiente a las marcas de fabricante de DDE.

mIBM: Variable de la marca IBM.

mFujitsu: Variable de la marca Fujitsu.

mHitachi: Variable de la marca Hitachi.

mMaxtor: Variable de la marca Maxtor.

mToshiba: Variable de la marca Toshiba.

mWD: Variable de la marca W.D.

mSeagate: Variable de la marca Seagate.

mSamsung: Variable de la marca Samsung.

mQuantum: Variable de la marca Quantum.

Para los valores de la X_6, de las marcas de fabricante, sólo se puede presentar una; la X_6 del coeficiente de la marca correspondiente, se sustituirá por el valor 1, y las demás por 0.

De la tabla 5.8 se observa que el uso de la metodología propuesta en el capítulo 4, tiene gran impacto sobre la tasa de recuperación, ya que el coeficiente es de 0.4134546, equivaliendo a una contribución del 41.34%. También los tipos de daños tienen alto impacto sobre la tasa de recuperación, pero ellos van ligados a las soluciones, ya que no se puede usar indistintamente las soluciones para todos los tipos de daños, estas combinaciones deben ser a criterio del especialista en recuperación de datos. En el anexo 10 se muestran ejemplos del cálculo de la tasa de recuperación.

RESUMEN

En este capítulo se analizó mediante estadística descriptiva, la muestra de DDEs recibidos para esta investigación. Donde se identificó las marcas de DDEs más recibidos, los tipos de daños previamente clasificados en el capítulo 2 y 3, y las marcas a las cuales afectan más dichos tipos de daños; así como aquellos casos con más de un daño y los casos donde se aplicaron las herramientas desarrolladas para esta investigación.

También se analizaron los resultados obtenidos de los casos de recuperación de datos, para ello se utilizó un modelo de análisis de regresión multivariada, con el cual se predice el comportamiento de la variable de respuesta (tasa de recuperación) mediante el efecto que causan las variables independientes, como lo son: los tipos de daños, solución, sistema de archivos, etc. Se observó que el uso de la metodología propuesta impacta en un 41.34% sobre la tasa de recuperación.

CONCLUSIONES

El proceso de recuperación de información es de gran importancia, ya que la información es uno de los activos más importantes para todas las personas, y si un DDE dañado está involucrado en un análisis forense informático, es necesario repararlo y obtener la información.

La metodología propuesta en este trabajo contempla a detalle cada etapa y fase para recuperar información en un DDE, con lo cual es posible tener mayor número de casos de éxito y recuperar mayor cantidad de información.

El factor tiempo invertido en una recuperación de información, varía en función de la capacidad del disco, del daño y de la cantidad de información almacenada, se observa que al utilizar la metodología propuesta dicho tiempo disminuye en comparación con un caso similar en el cual no se aplica la metodología, ya que se evita realizar procesos iterativos y agravar más el daño. El factor tiempo es crítico cuando lo es para el análisis forense informático, generalmente lo más importante es poder recuperar los datos.

Dentro de las etapas de la metodología, la más relevante es la reparación física temporal; para la reparación temporal se propusieron diferentes soluciones como cambio de *head-stack*, limpieza de cabezas/platos, lubricación del motor, entre otras; para aplicar algunas de las soluciones se requieren herramientas especiales y práctica debido a que no todas las marcas y modelos de DDEs tienen el mismo tipo de arquitectura física.

Para solucionar el problema “stuck” en el *spindle* motor, se desarrolló una herramienta física “motor unstuck”, de la cual se desarrollaron 2 modelos. De la muestra de 78 DDEs, el modelo 1 sirve para discos de marca Seagate, W.D. y algunos Maxtor, y el modelo 2 para discos Quantum y Samsung.

Para dar solución al bug en firmware, se desarrolló una herramienta física, la cual fue determinante para lograr éxito en la reparación de 2 DDEs de marca Seagate y por consiguiente recuperar el 100% de la información.

Otra contribución de gran importancia de la metodología, es la obtención de una imagen *bit* a *bit*, aún cuando no se logre obtener al 100%, en la copia parcial se podrán ejecutar diversos programas especializados que permitan recuperar y analizar archivos parciales, borrados, así como espacio no asignado a archivos; donde puede existir evidencia.

Un factor ajeno a la propia metodología pero que afecta el éxito en la recuperación de información, cuando la solución requiere cambio de elementos, es la obtención del DDE donador, debido a que en algunas ocasiones lo modelos han sido descontinuados, o porque algunas marcas de DDE fabrican discos del mismo modelo pero con estructura interna diferente, haciendo imposible el cambio de elementos.

Otro de los objetivos de este trabajo, fue analizar los resultados obtenidos de los 40 casos de recuperación de datos, mediante un análisis de regresión multivariada; con la finalidad de determinar la tasa de recuperación y con ello establecer un modelo de predicción y su comportamiento para determinar aquellos factores que la afectan.

De dicho análisis se concluye que la metodología propuesta contribuye en la tasa de recuperación en un 41.34%, es decir, que si no se aplica la metodología la cantidad de información que se puede recuperar disminuye en dicho porcentaje.

Existen otros factores que determinan la cantidad de información que puede recuperar y estos se observan e identifican también en el resultado del análisis de regresión multivariada: el tipo de daño y la solución aplicada, ya que hay daños que tienen menor probabilidad de ser recuperados, aún cuando existen más de una solución, el daño propiamente evita que se logre recuperar la información al 100%. En el resultado del modelo de análisis, hay 7 daños y 5 soluciones, pero no se pueden usar de forma indistinta, existe cierta correspondencia entre un daño y una o dos soluciones. Al momento de utilizar la ecuación resultante del análisis, es responsabilidad del experto en recuperación de datos, de verificar dicha correspondencia para obtener la mayor tasa de recuperación.

También se observa, del resultado del análisis, que las marcas de fabricantes no afectan de forma importante al modelo, y debido a que el número de DDEs por cada marca no fue equitativo, implica cierta tendencia hacia las marcas con mayor número de DDEs.

El uso de la metodología es un factor determinante para el éxito en la recuperación de información, ya se consideran tanto a los daños lógicos como físicos, aunado al estudio realizado previamente de los tipos de daños y sus soluciones; y el resultado del análisis de regresión multivariante muestra el impacto que tiene la metodología sobre la cantidad de información que se puede recuperar con un nivel de confianza del 95%.

En 10 casos procesados en base a las “mejores prácticas”, se recuperaron sólo 4 casos y 173Gb de aproximadamente 1,160Gb de los cuales 3 fueron daños lógicos y un daño físico,

mientras que en 30 casos procesados con la metodología propuesta, se recuperaron 22 casos y 1,273.10Gb de aproximadamente 4,452Gb, de los cuales 5 con daño lógico y 17 con daño físico. Se recuperó un 33.3% más de casos cuando se usó la metodología.

Con este trabajo, la metodología y soluciones propuestas así como las herramientas desarrolladas, fijan un precedente para mejorar el análisis forense cuando se ha identificado al DDE como el objeto de análisis y presenta un daño físico o lógico.

TRABAJO A FUTURO

Se debe buscar en el marco legal, que durante un análisis forense, la información recuperada de un disco duro dañado, sea aceptado como evidencia.

EN DAÑOS LÓGICOS

- Se deben buscar mejores técnicas y algoritmos para recuperar *data carving*, es decir, recuperación "por tipo de archivos", para abarcar un mayor número de tipos de archivos.

EN DAÑOS FÍSICOS

- Analizar los tipos de daños en discos duros SCSI y de estado sólido, para complementar la clasificación de tipos de daños.
- Desarrollar más herramientas que ayuden a incrementar el número de casos de éxito en las recuperaciones. Herramientas que ayuden principalmente a la migración de platos, y al cambio de *head-stack.*

MODELO DE ANÁLISIS

- Obtener una muestra de discos duros con mayor variedad en las marcas de discos duros, en los tipos de daños y sistema de archivos, para adaptar el modelo construido en esta investigación, y obtener una mayor exactitud en la predicción de la tasa de recuperación. El modelo construido en esta investigación sólo se basa en 8 tipos de daños de 19 identificados tanto físicos como lógicos, en 9 marcas de fabricantes de DDE, y en 2 sistemas de archivos.

REFERENCIAS

[1] Universidad de California. *How much information 2003?.* Octubre 27, 2003. Recuperado el 16 de junio 2010, de http://www2.sims.berkeley.edu/research/projects/how-much-info-2003/.

[2] eTForecasts. *Computer-in-use Forecast by Country*. 2008. Recuperado el 12 de mayo 2010 de http://www.etforecasts.com/products/ES_cinusev2.htm#toc.

[3] Kroll Ontrack. *Kroll Ontrack survey reveals a high percentage of corporate data loss that is rectified ineffectively.* Minneapolis. Enero 19, 2010. Recuperado el 12 de mayo 2010, de http://www.ontrackdatarecovery.com/data-recovery-press/index.aspx?getPressRelease=61409.

[4] Smith, David M. DeepSpar *Data Recovery Systems. Data loss and Hard Drive Failure: Understanding the Causes and Costs.* Recuperado el 12 de mayo 2010, de http://www.deepspar.com/wp-data-loss.html.

[5] Al Mamun, A., Guo, G. y Bi, C. (2007). *Hard Disk Drive Mechatronics and Control*. CRC Press 2007.

[6] Hitachi, *Hitachi Global Storage Technologies Background*. Recuperado el 17 de agosto 2010, de http://www.hitachigst.com/company/background/background.

[7] Western Digital, *Corporate Information*. Recuperado el 17 de agosto 2010, de http://www.wdc.com/en/company/corpfact.asp.

[8] Seagate, *Seagate Technology Company Milestones.* Recuperado el 25 de enero 2010, de http://www.seagate.com/www/en-us/about/corporate_information/company_milestones/.

[9] Quantum, *Corporation*. Recuperado el 17de agosto 2010, de http://www.fundinguniverse.com/company-histories/Quantum-Corporation-Company-History.html.

[10] Fujitsu, *Hard Disk Drives*. Recuperado el 29 de enero 2010, de http://www.fujitsu.ca/products/hdd/index2.html.

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

[12] Khurshudov, A. (2001). *Essential Guide to Computer Data Storage: From Floppy to DVD*. Prentice Hall Junio 2001.

[13] Jian-Gang, Z. (2003). *New heights for hard disk drives*. Department of Electrical and Computer Engineering and Data Storage Systems Center. Universidad de Carnegie Mellon. Julio/Agosto 2003.

[14] Kim, P. y Suk, M. (2007). *Whitepaper: Ramp Load/Unload Technology in Hard Disk Drives*. Hitachi Global Storage Technologies, 2007.

[15] International Organization for Standardization (ISO). ISO 14644-1, *Cleanrooms and associate controlled environments—Part 1: classification of air cleanliness*, 1999.

[16] Mueller, S. (2010). *Upgrading and Repairing PCs*. 19th Edition. Pearson Education, Inc. 2010.

[17] Do ,H., V., Fullerton, E., E., Margulies, D., T. y Rosen H., J. (2002). *Laminated Magnetic Recording Media with Antiferromagnetially coupled layers as the individual magnetic layers in the laminate*. 2002.

[18] Walker, C. B. (2007). *Whitepaper: Fluid Dynamic Bearing Spindle Motors: Their future in hard disk drives.* Hitachi United Stated Nobember 2007.

[19] Rubtsov, A. (2009). *HDD from inside: Main parts*. Recuperado el 31 de mayo 2010, de http://hddscan.com/doc/HDD_from_inside.html

[20] Wikipedia, *Master Boot Record.* Recuperado el 12 de mayo 2010, de http://en.wikipedia.org/wiki/Master_boot_record.

[21] Carrier, B. (2005.) *File System Forensic Analysis.* Addison Wesley Professional, 2005.

[22] X-Ways Software Technology AC. *Winhex*. Recuperado el 18 de octubre 2010, de http://www.x-ways.net/winhex/index-e.html.

[23] *MBRFix.exe*. Copyright (C) 2004-2009 Systemintegrasjon AS. Recuperado el 18 de octubre 2010, de http://www.sysint.no/nedlasting/mbrfix.htm.

[24] Easeus, *Partition Table Doctor*. Recuperado el 18 de octubre 2010, de http://www.ptdd.com/recover-partition-table.htm.

[25] *Test Disk*. Recuperado el 18 de octubre 2010, de http://www.cgsecurity.org/wiki/TestDisk.

[26] Runtime Software, *Get Data Back.* Recuperado el 18 de octubre 2010, de http://www.runtime.org/data-recovery-software.htm.

[27] Get Data Software Development Company, *Recover My Files*. Recuperado el 18 de octubre 2010, de http://www.recovermyfiles.com/es/.

[28] Wikipedia*, Pelo*. Recuperado el 16 de febrero 2011, de http://es.wikipedia.org/wiki/Pelo.

[29] Wikipedia, *Dust*. Recuperado el 16 de febrero 2011, de http://en.wikipedia.org/wiki/Dust.

[30] Shoji, S. y Ta-Chang F. (2004). *Hard Disk Drive Head-Media System having reduced Stiction and low Fly Height.* Enero 2004.

[31] Paper from Seagate (2001). *FDB Motor technology.* Número de publicación TP-574, Octubre 2001.

[32] MacWorld. *Seagate advierte de problemas con el firmware en las unidades barracuda*. Recuperado el 20 de febrero 2011, de http://www.idg.es/macworld/content.asp?idn=76026.

[33] Wikipedia, *Video Head Cleaner*. Recuperado el 20 de febrero 2011, de http://en.wikipedia.org/wiki/Video_head_cleaner.

[34] HDRC (2010). *Motor unstuck*. Recuperado el 20 de febrero 2011, de http://www.hdrconline.com/spindle_unstuck.php.

[35] MSFN Where people go to know. (2009). *Reparación del ST3500320AS SD15.* Recuperado el 20 de febrero 2011, de http://www.msfn.org/board/topic/128906-reparacion-del-st3500320as-sd15-en-espanol/

[36] Garcia, B. (2009). *Fixing a Seagate 7200.11 Hard Drive*. Recuperado el 20 de febrero 2011, de http://sites.google.com/site/seagatefix/Home.

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

[38] Dictionary Online Cambridge, *Recuperación*. Recuperado el 5 de agosto 2010, de http://dictionary.cambridge.org/.

[39] Pérez-García M, Rosales-García M., A., Pérez-Meana H., M. (2010). Metodología para Recuperación de Información en discos duros electromecánicos dañados para su análisis

forense. *Congreso Internacional sobre Innovación y Desarrollo Tecnológico*. Noviembre 24-26, 2010. Cuernavaca, Morelos, México.

[40] 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.

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

[42] Action Front. *Data Emergency Guide.* Recuperado el 20 de enero 2011, de www.ActionFront.com.

[43] 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-Changing-headstack-Q-and-A/.

[44] Hughes G., F., Commins, D., M. y Coughlin, T. (2009). *Disposal of Disk and Tape Data by Secure Sanitization.* Copublished by the IEEE Computer and Reliability Societies, July/August 2009.

[45] *ByteBack*. Recuperado el 22 de enero 2011, de http://www.toolsthatwork.com/byteback.htm.

[46] *AccessData.* Recuperado el 22 de enero 2011, de http://accessdata.com/support/adownloads.

[47] Machado, M., G. (1998). San José, Cal. *Disk Drive with Improved Error Correction Code*. Mazo 1988.

[48] Wikipedia, *Hash*. Recuperado el 25 de enero 2011, de http://es.wikipedia.org/wiki/Hash.

[49] *Funciones hash*. Recuperado el 10 de enero 2011, de http://foro.elhacker.net/criptografia/funciones_de_hash-t100025.0.html.

[50] Wikipedia, *SHA-1.* Recuperado el 21 de enero 2011, de http://en.wikipedia.org/wiki/SHA-1.

[51] Hair, J., Anderson, R., Tatham, R. y Black, W. (1999). *Análisis multivariante*, 5a. edición. Pearson Prentice Hall Iberia, Madrid, 1999.

[52] Lehmann, E. (1986). *Testing Statistical Hypotheses*. Wiley & Sons, New York.

[53] Canal, N. (2006).*Distribuciones de probabilidad. El Teorema central del límite.* Recuperado el 14 de abril, de http://www.seden.org/files/8-CAP%208.pdf.

[54] Scheffé, H. (1959). *The analysis of Variance*. Wiley & Sons, USA.

[55] *OfficeRecovery*. Recuperado el 5 de abril 2011, de www.officerecovery.com.

[56] Get Data Software Development Company. *Zip Repair*. Recuperado el 5 de abril 2011, de www.ziprepair.com.

SIGLAS

AFC: *Antiferromagnetically Coupled Media* (Media de Acoplamiento Antiferromagnético)
BIOS: *Basic Inpu/Output System* (Sistema Básico de Entrada y Salida)
BPI*: Bits per Inch* (Bits por Pulgada)
CI: Circuito Integrado
DDE: Disco Duro Electromecánico
DDEs: Discos Duros Electromecánicos
DDR: *Double Data Rate* (Velocidad Doble)
DIMMs: *Dual In-line Memory Modules* (Módulos de Memoria en Linea-Dual)
DLT: *Digital Linear Tape* (Cinta Digital de Almacenamiento)
EBR: *Extended Boot Record* (Registro de Inicio Extendido)
ECC: *Error Correcting Code* (Código de Corrección de Error)
EXT2: *Second Extended FileSystem* (Segundo Sistema de Archivos Extendido)
EXT3: *Third Extended Filesystem* (Tercer Sistema de Archives Extendido)
FAT*: File Allocation Table* (Tabla de Asignación de Archivos)
FDB: *Fluid Dynamic Bearing* (Rodamentos de Fluido Dinámico)
FSINFO: *File System Information* (Información del Sistema de Archivos)
GB: Gigabytes
GMR: Magneto Resistencia Gigante
HDA: *Head Disk Assembly* (Ensamble de la Cabeza del Disco)
HFS: *Hierarquical File System* (Sistema de Archivos Jerárquico)
IBM*: International Business Machines*
ID: *Identification* (Identificación)
IPL: *Initial Program Loader* (Cargador del Programa Inicial)
ISA*: Industry Standard Architecture* (Arquitectura Estándard de la Industria)
LBA: *Logical Block Address* (Dirección Lógica del Bloque)
LFN: *Long File Name* (Nombre Largo de Archivo)
LTO: *Linear Tape Open* (Cinta Magnética Almacenamiento de Datos)
MBR: *Master Boot Record* (Registro Principal de Inicio)
MCU: Unidad Microcontroladora
MD5: *Message-Digest Algorithm* 5 (Algoritmo de Resumen del Mensaje 5)
MFT: *Master File Table* (Tabla Principal de Archivos)
MR: Magneto Resistencia
NIST: *National Institute of Standards and Technology* (Instituto Nacional de Estándares y Tecnología)
NRRO: *Non-Repeatable RunOut* (Concentriciad No Repetible)
NTFS: *New Technology File System* (Sistema de Archivos de Nueva Tecnología)
OEM: *Original Equipment Manufacturer* (Fabricante del Equipo Original)

PCB: *Printed Circuit Board* (Tarjeta Impresa de Circuito)
PRLM: *Partial Response and Maximum Likelihood* (Respuesta Parcial y Máxima Verosimilitud)
RAM: *Random Access Memory* (Memoria de Acceso Aleatorio)
RAMAC: *Random Access Method of Accounting and Control* (Método de Acceso Aleatorio de Conteo y Control)
ROM: *Read Only Memory* (Memoria de Sólo Lectura)
RPM (rpm): Revoluciones Por Minuto
SA: Sistema de Archivos
SAs: Sistemas de Archivos
SDRAM: *Synchronous Dynamic Random Access Memory* (Memoria de Acceso Aleatorio de Sincronía Dinámica)
SHA1: *Secure Hashs Algorithm* 1 (Algoritmo de Hash Seguro 1)
SMART: *Self Monitoring Analysis and Reporting Technology* (Tecnología de Reporte y Análisis de Auto Monitoreo)
SO: Sistema Operativo
SOs: Sistemas Operativos
TB: Terabytes
TMR: *Track Mis-Registration* (Mal Registro de Pista)
TVS: *Transient Voltage Suppression* (Supresión de Voltaje Transitorio)
VCM: *Voice Coil Motor* (Motor de Bocina de Voz)

ANEXO 1. CONVERSIÓN HEXADECIMAL-DECIMAL-HEXADECIMAL

A.1. Conversión de números hexadecimales a decimales

Para realizar esta conversión, se multiplica el peso de cada posición por el equivalente decimal del dígito de cada posición, por último se suman los productos.
Donde A=10, B=11, C=12, D=13, E=14 y F=15.

Ejemplo 1:

3F =**3***(16^1)+ **F***(16^0) = (**3***16)+(**15***1)= 48 + 15

=**63**

Ejemplo 2:

037DFF 40 =**3***(16^6)+ 7*(16^5)+ **D***(16^4)+ **F***(16^3)+ **F***(16^2)+ **4***(16^1)+ **0***(16^0)

=(3*16,777,216)+ (7*1,048,576)+(13*65,536)+(15*4,096)+(15*256)+(4*16)+ (0*1)

=50,331,648+7,340,032+851,968+61,440+3,840+64+0

=**58,588,992**

A.2. Conversión de números decimales a hexadecimales

Para realizar este tipo de conversión, se realizan divisiones sucesivas por 16, se obtienen números enteros de dichas divisiones y el sobrante es el valor que formará al hexadecimal.

Ejemplo 1:

63 **=** 63/16= 3 y sobra 15=F

Como 3 ya no es divisible entre 16, 3 se queda como la cifra más significativa

= **3F**

Ejemplo 2:

58,588,992	= 58,588,992/16= 3,661,812 y sobra	0
	= 3,661,812/16= 228,863 y sobra	4
	= 228,863/16 =14,303 y sobra	15=F
	= 14,303/16 = 893 y sobra	15=F
	= 893/16 = 55 y sobra	13=D
	= 55/16 = 3 y sobra	7

Como 3 ya no es divisible entre 16, 3 se queda como la cifra más significativa

= 37DFF40

ANEXO 2. TABLA DE COMPATIBILIDAD DE DDE POR FABRICANTE

A continuación se presenta la tabla A2.1, donde se indican las características que deben ser idénticas entre un DDE dañado y un DDE donador (además de la marca y modelo), para que el intercambio de elementos como *head-stack,* o partes de la PCB pueda funcionar como solución en la recuperación de datos. Estas características son proporcionadas por Scott Moulton en su Scott Moulton's Speech Research Material and Notes on Data Recovery [39] y por Stanislav Korb en su página HDDGURU.COM [42].

Marca	Característica adicional
Quantum (hasta familias Plus AS)	-Número de cabezas (tercer digito del número de serie). -Firmware.
Quantum Plus (AS, D540X, D740X)	-Número de cabezas (tercer digito del número de serie). -Código alfabético HA. -Firmware. -País.
Seagate	-Número de cabezas (tercer símbolo del número de serie). -Firmware. -País.
Fujitsu	-País. -El primer carácter del Firmware (xx-Xxxx)
Fujitsu 2.5"	-Firmware. -País
IBM	-Número de parte. -Firmware. -País. -Código MLC.
Hitachi 2.5"	-Código de Revisión de la PCB. -País.
Hitachi 3.5"	-Firmware. -Número de parte.
Samsung	-Tamaño de buffer. -País.
Maxtor	-Número de cabezas (segundo digito del número de serie). -Tercer dígito del número de serie. -Firmware. -País.
W.D.	-En el código DCM el 5º y 6º número. -Firmware. (Los DDEs con modelo EB o BB que tengan la letra R no se deben usar).

Tabla A2.1. Características de compatibilidad necesarias para un DDE donador.

ANEXO 3. RS232 PARA REPARAR BUG EN FIRMWARE DE DDE SEAGATE.

Para la construcción del adaptador RS232, se utilizó un CI MAX232, al cual se le conectaron 4 capacitores de 4.7µF para que se puedan manejar voltajes TTL. El diagrama utilizado se muestra en la Figura A3.1.

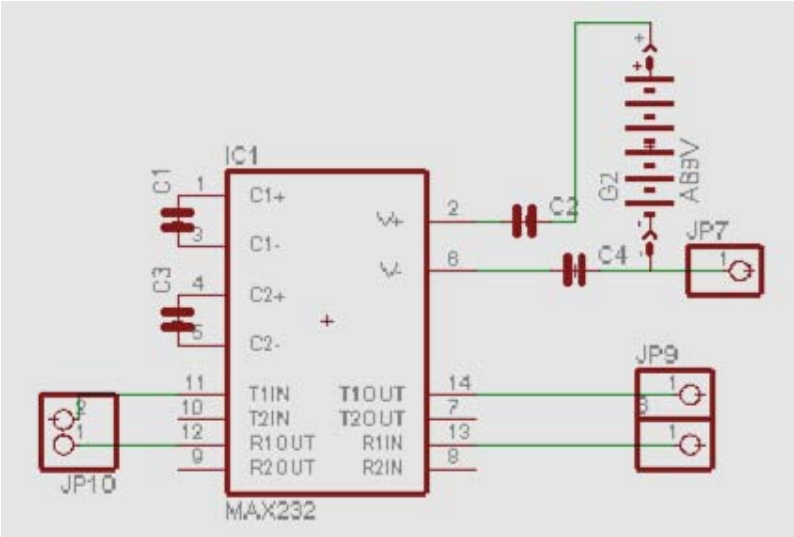


Figura A3.1. Diagrama del MAX232 adaptado al RS232.

Se soldaron todos los elementos del diagrama a un aplaca, donde también se soldó el adaptador RS232 (Figura A3.2), y se dejaron los pines para la alimentación de 5Volts, y los pines que van hacia el DDE: cable rojo RX, cable negro TX y cable blanco tierra.

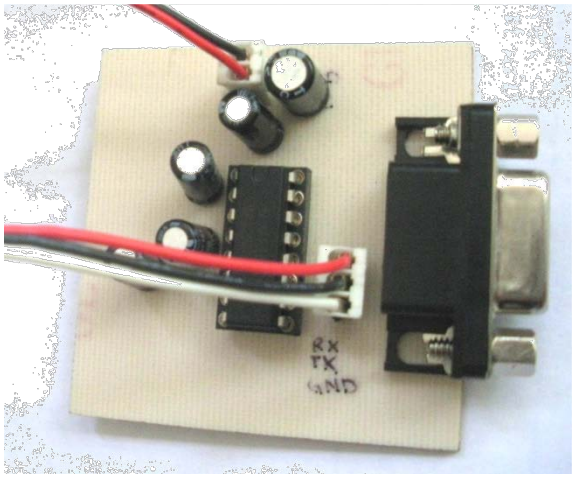


Figura A3.2. Placa del CI 232 con el adaptador RS232.

ANEXO 4. FORMATOS DE LOS ENTREGABLES DE LA METODOLOGÍA.

RECUPERACIÓN DE INFORMACIÓN

No. de caso:		Fecha:	
Nombre del contacto:			
Teléfono del contacto:			
Nombre del examinador:			
Teléfono del contacto:			
Lugar:			

Descripción del dispositivo				
# Elemento	Marca	Modelo	Capacidad	No. de serie

Especificaciones técnicas del dispositivo					
# Elemento	Tipo de Interfaz	Tamaño (pulgadas)	Año de fabricación	Tipo de escritura/lectura	Tipo de motor

Información proporcionada por el cliente				
# Elemento	Sistema operativo	Probable daño	Información almacenada (GB)	Número de particiones

Entrega (nombre completo y firma):		**Recibe (nombre completo y firma):**	

ETAPA 1: ANÁLISIS FÍSICO.

No. de caso:		No. de elemento:	
Lugar de realización del análisis:			
Fecha y hora de inicio de la etapa:			
Fecha y hora de fin de la etapa			

FASE 1: Inspección visual.

Inspección visual del HDA	
Ubicación de golpes visibles:	
Ubicación de etiquetas alteradas:	
Otros hallazgos:	
Inspección visual de la PCB	
Elementos quemados:	
Elementos desoldados:	
Elementos rotos:	
Daño en pistas:	
Otros hallazgos:	

FASE 2: Verificación de la alimentación de poder.

¿Alimentación correcta?:	
¿Se calientan elementos de la PCB? :	
Elementos que se calientan:	
Otros hallazgos:	

FASE 3: Detección en el BIOS.

¿El BIOS detecta al DDE?:	
Parámetros detectados (marca, modelo y no. de serie):	
¿Parámetros correctos? (conforme las especificaciones del DDE) :	
Otros hallazgos:	

Examinador o responsable (nombre completo y firma):	

ETAPA 2: REPARACIÓN FÍSICA TEMPORAL.

No. de caso:		No. de elemento:	
Lugar de realización del análisis:			
Fecha y hora de inicio de la etapa:			
Fecha y hora de fin de la etapa			

FASE 1: Identificación del tipo de daño y severidad.

Síntomas del DDE :			
¿Rota el motor?:		¿Sonido de golpeteo interno de las cabezas?:	
Componente (s) dañado (s), (cabezas, platos, motor, PCB):			
Daño (s) identificado (s):			
Severidad del daño:			
Observaciones:			

FASE 2: Identificación de la posible solución.

Soluciones identificadas :	
Herramientas necesarias:	
¿Se requiere DDE donador? :	
Observaciones:	

FASE 3: Aplicación de la solución.

¿Se obtuvo el DDE donador? (de ser necesario):	
Soluciones aplicadas :	
Herramientas utilizadas:	
Observaciones:	

FASE 4: Verificación del resultado de la solución.

¿Se logro éxito en la reparación temporal?:	
Tipo de solución aplicada con éxito :	
Porque no se logro el éxito:	
Observaciones:	

Examinador o responsable (nombre completo y firma):	

ETAPA 3: OBTENCIÓN DE IMAGEN.

No. de caso:		No. de elemento:	
Lugar de realización del análisis:			
Fecha y hora de inicio de la etapa:			
Fecha y hora de fin de la etapa			

FASE 1: Preparación del disco duro destino.

Parámetros del DDE destino (marca, modelo, capacidad, no. de serie):	
Software utilizado para sanitizar al DDE destino:	
No. de sectores del DDE destino:	
Observaciones:	

FASE 2: Creación de la imagen.

Software para crear imagen:	
Número de imágenes obtenidas:	
Porcentaje obtenido de las imágenes:	
Número de sectores copiados:	
Observaciones:	

FASE 3: Verificación de la imagen.

Se logró el 100% de la (s) imagen (es):	
¿Por qué?:	
Software utilizado para la verificación:	
Tipo de hash (es):	
Hash (es) de la (s) imagen (es):	
Observaciones:	

Examinador o responsable (nombre completo y firma):	

ETAPA 4: ANÁLISIS LÓGICO.

No. de caso:		No. de elemento:	
Lugar de realización del análisis:			
Fecha y hora de inicio de la etapa:			
Fecha y hora de fin de la etapa			

FASE 1: Activación del modo de lectura.

¿Se activó el modo de sólo lectura?:	
¿Se activó con software o hardware?:	
Tipo de software o hardware:	
Observaciones:	

FASE 2: Análisis del MBR.

¿Se logró ubicar el MBR?:		No. de sector del MBR:	
¿La firma del MBR (0xaa55) está dañada?:			
Número de particiones identificadas:			
Sistema de archivos de la (s) partición (es):			
Sector inicial y número de sectores de cada partición:			
Tipo de daño en el MBR:			
Tipo de solución:			
Software para la reparación:			
Observaciones:			

FASE 3: Análisis de la estructura del sistema de archivos.

# de partición	Sistema de archivos	# de sectores totales	Sector inicial	Sector final	Elementos dañados	Posible Solución (es)
Observaciones:						

Examinador o responsable (nombre completo y firma):	

ETAPA 5: REPARACIÓN LÓGICA.

No. de caso:		No. de elemento:	
Lugar de realización del análisis:			
Fecha y hora de inicio de la etapa:			
Fecha y hora de fin de la etapa			

FASE 1: Activación del modo de escritura.

¿Se activó el modo de escritura?:	
¿Se activó con software o hardware?:	
Tipo de software o hardware:	
Observaciones:	

FASE 2: Reparación del MBR.

¿Se logró reparar el MBR?:		¿Por qué?:	
Elementos reparados:			
Software utilizado para la reparación:			
Número de particiones correctas:			
Sistema de archivos de la (s) partición (es):			
Sector inicial y número de sectores de cada partición correcta:			
Observaciones:			

FASE 3: Reparación del sistema de archivos.

# de partición	Solución aplicada	Éxito en la reparación	¿Por qué?	Sector inicial	Sector final	Total de sectores
Observaciones:						

Examinador o responsable (nombre completo y firma):	

ETAPA 6: RECUPERACIÓN DE DATOS.

No. de caso:		No. de elemento:	
Lugar de realización del análisis:			
Fecha y hora de inicio de la etapa:			
Fecha y hora de fin de la etapa			

FASE 1: Ejecución de software especializado.

¿Se requirió ejecutar software especializado para recuperar archivos?:	
Software utilizado:	
Cantidad de información recuperada:	
Observaciones:	

FASE 2: Revisión de la integridad de archivos críticos.

¿Hay archivos críticos dañados?:	
Archivos dañados:	
Sotware para reparar los archivos críticos.	
Observaciones:	

FASE 3: Recuperación "por tipo de archivos".

¿Se requiere la recuperación "por tipo de archivos"?:	
Sotware para la recuperación :	
Tipos de archivos recuperados:	
Observaciones:	

Examinador o responsable (nombre completo y firma):	

ETAPA 7: REPARACIÓN DE ARCHIVOS CRÍTICOS.

No. de caso:		No. de elemento:	
Lugar de realización del análisis:			
Fecha y hora de inicio de la etapa:			
Fecha y hora de fin de la etapa			

FASE 1: Reparación por tipo de archivo.

¿Se requirió la reparación por tipo de archivos?:	
Sotware para reparar por tipo de archivo:	
Tipos de archivos reparados:	
Archivos reparados:	
Observaciones:	

FASE 2: Verificación de la integridad de archivos reparados

¿Se logró reparación por tipo de archivos?:	
Sotware utilizado :	
Cantidad de archivos reparados:	
Cantidad de archivos no reparados:	
Archivos no reparados:	
Observaciones:	

Examinador o responsable (nombre completo y firma):	

ANEXO 5. EQUIPOS DE CÓMPUTO DE PRUEBAS.

Para realizar las pruebas de los DDE dañados con la finalidad de recuperar la información, se utilizaron 3 diferentes equipos de cómputo. Acorde a las características y el daño del DDE se utilizó el equipo adecuado.

EQUIPO 1. De escritorio

- Tarjeta principal Pentium Soyo
- Procesador AMD-K6 (tm)-2/300
- 256MB de memoria RAM
- Conexión para DDE IDE/USB
- Unidad de Floppy

EQUIPO 2. De escritorio

- Tarjeta principal K7N2 Delta Series MS-6570
- Procesador AMD Athlon XP2000 1.6GHz
- 512MB de memoria RAM
- Conexión para DDE IDE/SATA/USB
- Unidad de Floppy

EQUIPO 3. Laptop

- Tarjeta principal Intel
- Procesador Intel Core(TM)2 Duo CPU T6600 2.20GHz
- 3GB de memoria RAM
- Conexión para DDE USB

ANEXO 6. CASO REAL DE RECUPERACIÓN DE DATOS A NIVEL LÓGICO.

DDE marca Hitachi modelo HDS725050KLAT80 500GB, sistema de archivos NTFS, una partición, no contiene sistema operativo por lo que no es unidad de arranque sólo de datos.
Daño en el Master Boot Record (MBR) y en el Sector de Inicio.
Información recuperada: 245GB.

Seguimiento de la metodología:

1. **Análisis físico**

En esta etapa se revisó la estructura física del DDE, para eliminar la posibilidad de un daño físico. Los resultados de las fases de esta etapa se muestran en la tabla A7.1.

Tabla A7.1. Resultados de las fases del Análisis físico.

FASES	RESULTADO
Inspección visual	No se encontró rastros de golpes o abolladuras en el HDA. La PCB tampoco muestra componentes dañados
Verificación de la alimentación de poder	La energía eléctrica en la PCB es correcta y no generó conflictos al conectar la alimentación de poder
Detección en el BIOS	El BIOS del equipo de cómputo de prueba, detectó todos los parámetros de forma correcta.

Al finalizar está etapa, se concluye que el DDE no presenta daños físicos que requieran reparación temporal.

2. **Reparación física temporal**

Los resultados de la etapa anterior revelaron que no existe daño físico, por lo que en ésta etapa no se realizaron reparaciones.

3. **Obtención de imagen**

Se obtuvo una imagen *bit* a *bit* del DDE dañado para realizar las pruebas sobre dicha imagen. Los resultados de las fases, se describen en la tabla A7.2.

Tabla A7.2. Resultados de las fases de la Obtención de Imagen.

FASES	RESULTADO
Preparación del DDE destino	Se sanitizó un DDE de 500GB utilizando el programa "winhex". El número de sectores del DDE destino es igual al DDE dañado
Creación de la imagen	La copia bit a bit se realizó al 100%, utilizando el programa winhex, sin presentar sectores dañados
Verificación de la imagen	Se obtuvo el hashs MD5 y SHA1 para el DDE dañado y para la imagen.

Los algoritmos hash MD5 y SHA1 se obtuvieron con el programa FTK imager [45], para ambos discos duros (original e imagen), se obtuvieron los siguiente hashes:

MD5 hahs: 19ed720fe72725d35e5fb0db638f0633

SHA1 hash: 252fab1c2ff1525d7e5986737ecd141ac1f7205

4. Análisis lógico

Se analizó la estructura del MBR y del SA, debido a que el DDE presentó daño lógico y no era posible visualizar la unidad lógica. Al conectarlo como esclavo bajo un SA NTFS, el sistema indicó que se trataba de una unidad nueva. El análisis se realizó utilizando el programa winhex.

Análisis del MBR:

Se analizó el MBR basados en la tabla 1.2 y 1.3 del capítulo 1. Como se indica en el capítulo 2, los únicos elementos que afectarían el funcionamiento del MBR son la firma y los parámetros de la partición. El análisis del MBR indicó que la firma es correcta, pero en la sección de parámetros de las particiones, se identificaron 2 particiones.

Los parámetros de la primer partición se muestran en la tabla A7.3.

Posición	Valor	Contenido
1BEh	00h	Unidad: no "booteable"
01BFh-01C1h	00h,00h,01h	Cabeza 0, sector 0, cilindro 1, del inicio de la partición
1C2h	07	Tipo de partición: NTFS
1C3h-1C5h	FEh,FFh,FFh	Cabeza 254, sector 255, cilindro 255, del final de la partición
1C6h-1C9h	3Fh 00h 00h 00h	Sector de inicio: 63
1CAh-1CDh	00h 48h 38h 3Ah	Número de sectores en la partición: 976,766,976

Tabla A7.3. Parámetros de la primer partición en el MBR.

De la tabla A7.3 se observa la existencia de una partición de 465GB no activada (no contiene el código 80h en el campo correspondiente en la bandera de estado, en la posición 01B3h), debido a que no es una unidad de arranque que contenga Sistema Operativo, es correcto el valor 00h como bandera de estado.

Los parámetros de la segunda partición en el MBR se indican en la tabla A7.4 e indican una partición de 6.5GB.

Posición	Valor	Contenido
1CEh	00h	Unidad: no “booteable”
01CFh-01D1h	17h,05h,11h	Cabeza 23, sector 5, cilindro 17, del inicio de la partición
1D2h	00	Tipo de partición: vacía
1D3h-1D5h	58h,C2h,FFh	Cabeza 88, sector 194, cilindro 255, del final de la partición
1D6h-1D9h	00h 04h 00h 00h	Sector de inicio: 1024
1DAh-1DDh	A1h D7h CCh 00h	Número de sectores en la partición: 13,424,545

Tabla A7.4. Parámetros de la segunda partición en el MBR.

Los datos incorrectos que se detectaron fueron los parámetros de la segunda partición, ya que se tiene conocimiento de la existencia de sólo una partición que abarca el tamaño total del DDE. Los recuadros rojos indicados en la Figura A7.1 muestran la posición de los campos identificados como erróneos del MBR.

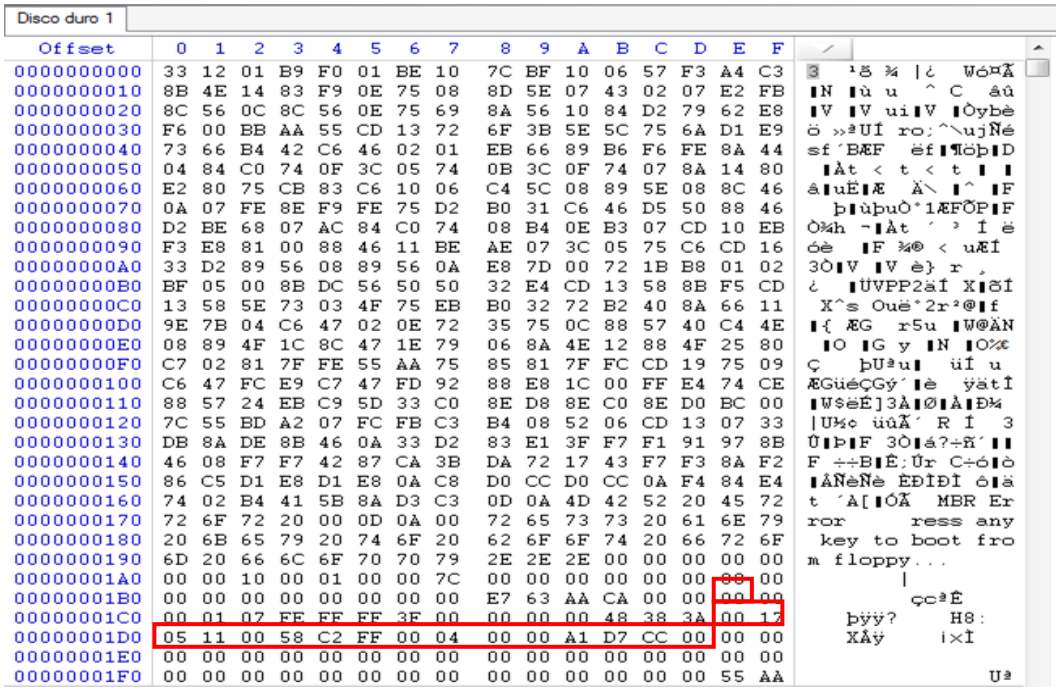


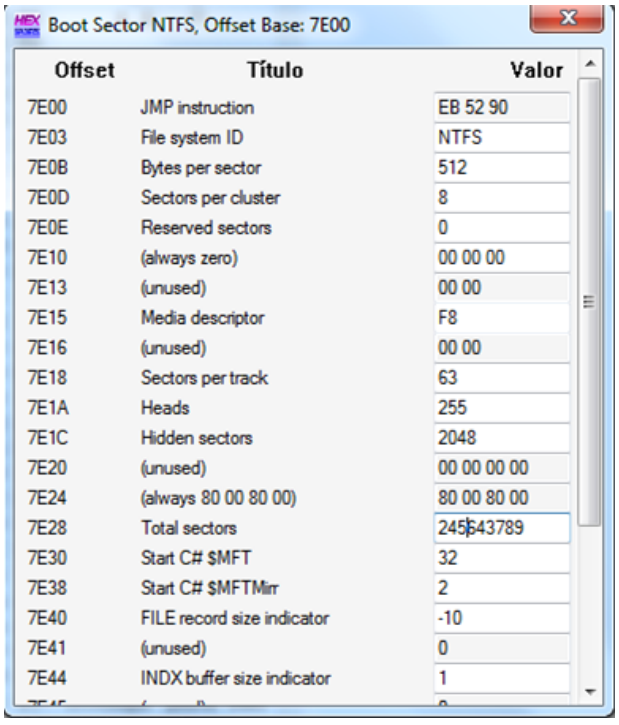
Figura A7.1. Campos erróneos en el MBR.

Se identifica a la partición de 465GB como válida, comienza en el sector 63 y consta de 976,766,976 sectores.

Análisis de la estructura del Sistema de Archivos:

Basados en el MBR, se identificó la posición del sector de inicio de la partición. Físicamente se busco dicha posición, pero el sector de inicio no correspondía al tamaño de la partición indicado en el MBR, ya que se trataba de una partición de aproximadamente 120GB, con inicio de la partición en el sector 2,048.

La Figura A7.2 muestra los parámetros de sector de inicio identificados como erróneo, vistos con el gestor de plantillas de winhex.



Offset	Título	Valor
7E00	JMP instruction	EB 52 90
7E03	File system ID	NTFS
7E0B	Bytes per sector	512
7E0D	Sectors per cluster	8
7E0E	Reserved sectors	0
7E10	(always zero)	00 00 00
7E13	(unused)	00 00
7E15	Media descriptor	F8
7E16	(unused)	00 00
7E18	Sectors per track	63
7E1A	Heads	255
7E1C	Hidden sectors	2048
7E20	(unused)	00 00 00 00
7E24	(always 80 00 80 00)	80 00 80 00
7E28	Total sectors	245243789
7E30	Start C# $MFT	32
7E38	Start C# $MFTMirr	2
7E40	FILE record size indicator	-10
7E41	(unused)	0
7E44	INDX buffer size indicator	1

Figura A7.2. Parámetros identificados como erróneos del Sector de inicio.

Se calculó el número de sector del final de la partición basado en los datos obtenidos del MBR. En el último sector de la partición se localiza la copia del sector de inicio, de esta forma se verifica la información del MBR y del sector de inicio ubicado al principio de la partición.

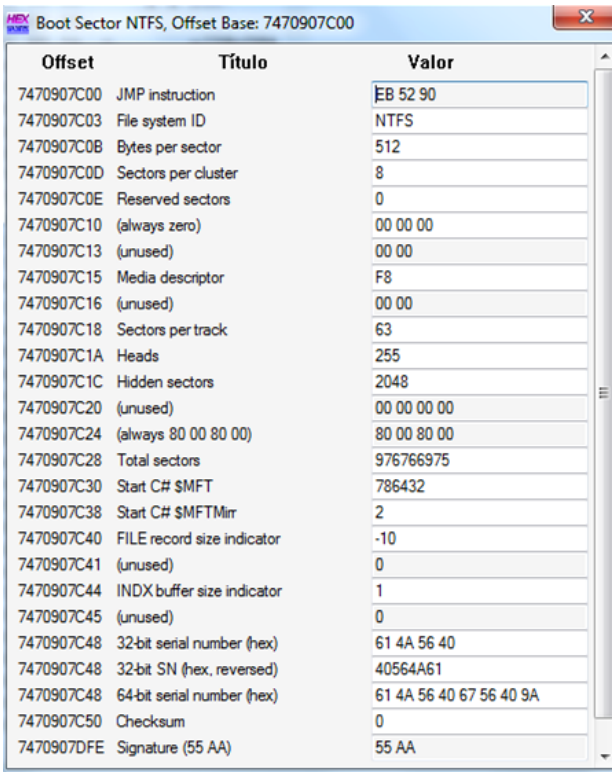
El MBR indica “el número del total de sectores en cada partición”, mientras que en el Sector de inicio de cada partición el número indicado como “el total de sectores en la partición” será menos 1 con respecto al indicado en el MBR, esto es debido a que en el Sector de inicio no se cuenta a sí mismo.

Para aplicar la ecuación 4.1 del capítulo 4, se usó el número de sectores escrito en el MBR menos 1, ya que no se contaba con la información real del Sector de inicio (los datos para aplicar la ecuación se obtienen del MBR, los cuales fueron transcritos a la tabla AI.3):

$$\#\ sector\ final = (\#\ sector\ inicial + \#\ total\ de\ sectores\ en\ la\ partición\ )$$

$$\#\ sector\ final = 976{,}767{,}038$$

Se buscó físicamente la posición del sector calculado y se encontró la copia del Sector de inicio, el cual correspondía al tamaño de la partición de la que se tenía conocimiento. La Figura A7.3 muestra la copia del sector de inicio (el último sector de la partición) ubicada en el sector 976,767,038 vista con el gestor de plantillas de winhex.



Offset	Título	Valor
7470907C00	JMP instruction	EB 52 90
7470907C03	File system ID	NTFS
7470907C0B	Bytes per sector	512
7470907C0D	Sectors per cluster	8
7470907C0E	Reserved sectors	0
7470907C10	(always zero)	00 00 00
7470907C13	(unused)	00 00
7470907C15	Media descriptor	F8
7470907C16	(unused)	00 00
7470907C18	Sectors per track	63
7470907C1A	Heads	255
7470907C1C	Hidden sectors	2048
7470907C20	(unused)	00 00 00 00
7470907C24	(always 80 00 80 00)	80 00 80 00
7470907C28	Total sectors	976766975
7470907C30	Start C# $MFT	786432
7470907C38	Start C# $MFTMirr	2
7470907C40	FILE record size indicator	-10
7470907C41	(unused)	0
7470907C44	INDX buffer size indicator	1
7470907C45	(unused)	0
7470907C48	32-bit serial number (hex)	61 4A 56 40
7470907C48	32-bit SN (hex, reversed)	40564A61
7470907C48	64-bit serial number (hex)	61 4A 56 40 67 56 40 9A
7470907C50	Checksum	0
7470907DFE	Signature (55 AA)	55 AA

Figura A7.3. Copia del Sector de inicio.

Se calculó la posición de la MFT, usando la ecuación 4.2 del capítulo 4:

$$\#\ sector\ MFT = \#\ sector\ inicial + (\#\ cluster\ de\ MFT * \#\ de\ sectores\ por\ cluster)$$
$$\#\ sector\ MFT = (63) + (786{,}432 * 8)$$
$$\#\ sector\ MFT = 6{,}291{,}519$$

Se buscó físicamente la posición de la MFT calculada, para comprobar la integridad de la estructura NTFS y validar los datos indicados en la copia del Sector de inicio. La posición real de la MFT correspondió con la posición indicada en la copia del Sector de inicio.
Los resultados obtenidos de las fases de esta etapa se describen en la tabla A7.5.

Tabla A7.5. Resultados de las fases del Análisis lógico.

FASES	RESULTADO
Activación del modo de lectura	Se activo el modo de lectura mediante Hardware, utilizando un bloqueador de disco duro.
Análisis del MBR	El análisis del MBR reveló la existencia de 2 particiones, únicamente los parámetros de la primer partición eran los correctos
Análisis de la estructura del SA	El sector de inicio de la partición, no correspondía al tamaño de la partición indicado en el MBR, se buscó la copia del sector de inicio, el cual se ubica al final de la partición, se localizo y se validaron los parámetros indicados, tanto tamaño de la partición como ubicación de la MFT

Al finalizar el análisis lógico, se detectó daño en el MBR y en el sector de inicio de la partición, ambos elementos requieren reparación.

5. Reparación lógica

Se repararon los campos detectados como erróneos tanto en el MBR como en la estructura del SA.

Reparación del MBR:

- Del resultado de la etapa anterior, se verificó que los datos de la segunda partición identificados en el MBR no eran correctos, para corregir este problema, únicamente

se sobreescribieron los campos con el valor 00h, es decir se escribió el valor 00h desde la posición 01CEh hasta 01DDh.

- El estado inactivo de la primer partición (identificada como correcta) no se modificó, ya que no es necesario para el funcionamiento como unidad lógica.

Reparación del Sector de Inicio:

Para realizar la reparación del sector de inicio, se copió el respaldo del sector de inicio ubicado en la parte final de la partición. Esta acción fue suficiente, debido a que los parámetros identificados en dicho respaldo eran correctos.

Los resultados obtenidos de las fases de la reparación lógica se muestran en la tabla A7.6.

Tabla A7.6. Resultados de las fases de la Reparación lógica.

FASES	RESULTADO
Activación del modo de escritura	Se activo el modo de escritura utilizando al bloqueador de disco duro
Reparación del MBR	Se reparó el MBR acorde al daño detectado en la etapa anterior
Reparación del SA	Se reparó el Sector de Inicio inicial que faltaba, haciendo uso de la copia del Sector de inicio ubicada al final de la partición

6. Recuperación de datos

Se ejecutó el software GetDataBack NTFS [26] para recuperar aquellos archivos o subdirectorios que quedaron desligados de su directorio, así como archivos borrados. De esta forma se obtuvo la mayor cantidad de información posible. Los resultados de las fases, se describen en la tabla A7.7.

Tabla A7.7. Resultados de las fases de la Recuperación de datos.

FASES	RESULTADO
Ejecución de software especializado	Se ejecuto el programa GDB NTFS, activando la opción de búsqueda de archivos borrados
Revisión de integridad de archivos críticos	Se revisaron los archivos críticos, archivos de Word, Excel y power point. Se estimó que menos del 5% presentaron daño en la integridad, estos archivos fueron los recuperados identificados como borrados.
Recuperación por tipo de archivos	No fue necesaria la búsqueda por tipo de archivos, debido a que la información crítica existía de forma lógica

7. Reparación de archivos críticos

Esta etapa no fue necesaria, debido a que los archivos críticos fueron recuperados de forma íntegra.

En caso de haber requerido la reparación:

1. Se identifican los archivos críticos
2. Se identifican los tipos de archivos, es decir a que programas pertenecen
3. Se identifican los programas de reparación para dichos archivos, como Office Recovery [55], Zip repair [56], etc.
4. Se reparan los archivos con los programas correspondientes
5. Se verifica la integridad del archivo

ANEXO 7. CASO REAL DE RECUPERACIÓN DE DATOS A NIVEL FÍSICO.

DDE marca W.D. modelo WD400EB-00CPF0 40GB, sistema de archivos FAT32, una partición "booteable". Cabezas mal alineadas y daño no visible en la media.
Información recuperada: 6GB.

Seguimiento de la metodología:

1. **Análisis físico**

En esta etapa se revisó la estructura física del disco duro, para detectar daños físicos visibles. Los resultados de las fases se muestran en la tabla A8.1.

Tabla A8.1. Resultados de las fases del Análisis físico.

FASES	RESULTADO
Inspección visual	No se encontró rastros de golpes o abolladuras en el HDA. La PCB tampoco muestra componentes dañados
Verificación de la alimentación de poder	La energía eléctrica en la PCB es correcta y no generó conflictos al conectar la alimentación de poder
Detección en el BIOS	El BIOS del equipo de cómputo de prueba, no detectó al DDE, y se escuchó un sonido de golpeteo de las cabezas (click-click)

Al finalizar está etapa, se concluye que el DDE presenta daño físico, y se requiere la reparación física temporal.

2. **Reparación física temporal**

Debido a la necesidad de una reparación física temporal, se aplicaron todas las fases de esta etapa:

Identificación del tipo de daño y severidad

Acorde a los síntomas descritos en la tabla 3.2 del capítulo 3 (nula detección por el BIOS y sonido click-click), se determinó que podían existir 2 elementos dañados: las cabezas de lectura/escritura o los platos.

Se abrió el DDE en una superficie y área limpia, para verificar la existencia de un *headcrash* visible, para ello se utilizaron desarmadores tipo torx no. 9. Los platos del DDE no presentaron *headcrash* visible (Figura A8.1).

Figura A8.1. Headcrash no visible.

Identificación de la posible solución

Debido a la posibilidad de 2 elementos dañados, las posibles soluciones que se identifican son:

1. Limpieza de los platos
2. Limpieza de cabezas
3. Congelamiento del DDE por un periodo corto
4. Cambio de *head-stack*

Para aplicar las soluciones en el orden descrito previamente, se requirió lo siguiente:

- Liquido “headcleaner”
- Aire comprimido
- Bolsas antiestáticas
- DDE donador, misma marca, modelo, firmware y con el número 5º y 6º del código DCM.

Todos los elementos arriba descritos se pudieron obtener.

Aplicación de la solución

Se aplicó cada una de las soluciones identificadas en la fase anterior, en el orden descrito previamente:

1. Limpieza de los platos: Para limpiar los platos se utilizó el aire comprimido, como se describe en la sección 3.2.1.1. del capítulo 3.
2. Limpieza de las cabezas: Para esta prueba, se utilizó el "headcleaner", debido a que el DDE no tenía *dynamic load/unload* para aplicar el líquido, se desensambló el *head-stack*, como se indica en la sección 3.2.2.1. del capítulo 3. Para la extracción del *head-stack* se utilizaron: desarmadores torx no. 9 y pinzas de plástico. Se utilizó un pequeño trozo de foami, el cual es un material no conductor, para separar los brazos que sostienen a los sliders. Después de aplicar el líquido, se volvió a ensamblar el *head-stack* al HDA, haciendo uso de los desarmadores mencionados.
3. Congelamiento del DDE por un periodo corto: Se metió al DDE completo, armado y cerrado en bolsas antiestáticas, se cerraron y se metieron al congelador por un periodo de 10 minutos (Figura A8.2). Posteriormente se sacó del congelador y de las bolsas antiestáticas.

Figura A8.2. DDE dentro de bolsa antiestática para meter al congelador.

4. Cambió de *head-stack*. Esta prueba se realizar acorde a lo descrito en la sección 3.2.2.2 del capítulo 3. Para esta prueba primero se desensambló el *heads-stack* del DDE dañado, del mismo modo que se realizó para la limpieza de cabezas, (el procedimiento tanto para el disco dañado como para el donador fue el mismo). Se

utilizaron desarmadores torx no. 9 y pinzas de plástico. Al momento de empujar a los brazos del *head-stack* fuera de los platos, se utilizaron pequeños trozos de papel bond, para separar a los sliders, como se muestra en la Figura A8.3:

Figura A8.3. Separación de los *sliders* mediante un trozo de papel.

Posteriormente entre los brazos se introdujo un pequeño trozo de foami, para facilitar la reincorporación de las cabezas hacia los platos, como se muestra en la Figura A8.4:

Figura A8.4. Separación de los *sliders* mediante foami.

Por último se ensambló el *head-stack* del DDE donador al HDA del DDE dañado.

Verificación del resultado de la solución

Se verificaron cada una de las soluciones aplicadas, para comprobar el éxito, es decir, lograr que el BIOS del equipo de cómputo de prueba detectara los parámetros de forma correcta.

1. Limpieza de los platos: No se tuvo éxito, ya que el DDE no fue reconocido.
2. Limpieza de las cabezas: No se tuvo éxito, el DDE no fue reconocido por el BIOS.
3. Congelar al DDE por un periodo de corto: No se tuvo éxito, ya que el DDE no fue reconocido por el BIOS.
4. Cambio de *head-stack*: En esta prueba se tuvo éxito, ya que el DDE fue reconocido por el BIOS con todos los parámetros correctos.

Los resultados de las fases de la Reparación física temporal, se describen en la tabla A8.2.

Tabla A8.2. Resultados de las fases de la Reparación física temporal.

FASES	RESULTADO
Identificación del tipo de daño y severidad	Se detectó como primer daño, un problema en las cabezas de lectura/escritura, lo que impide la identificación del DDE, y por tanto la lectura en cualquier área del DDE
Identificación de la posible solución	Se identificaron 4 soluciones, de las cuales el cambio de *head-stack* fue el que tuvo éxito. Para dicho cambio se requirió un DDE donador. Este DDE se logró conseguir con las características similares al DDE dañado necesarias
Aplicación de la solución	Se realizó el cambio de *head-stack* con éxito
Verificación del resultado de la solución	El DDE reparado temporalmente logró ser detectado por el BIOS del equipo de computo de prueba

Al finalizar esta etapa, se logró éxito en la reparación temporal, por lo que se procedió a efectuar la imagen.

3. Obtención de imagen

Se obtuvo una imagen *bit* a *bit* del DDE dañado para realizar las pruebas sobre dicha imagen.

Creación de la imagen

Para la creación de la imagen se utilizó el programa ByteBack [44]. La imagen se comenzó del principio al final de los sectores del DDE, se logró copiar aproximadamente el 3% del total del DDE, se tuvo que forzar a que se leyeran los sectores, esto se hace configurando al programa para que intente máximo un número determinado de veces de lectura sobre cada sector), en este caso se configuraron máximo 3 intentos. Se copiaron 2,423,235 sectores, posteriormente el disco comenzó a marcar nula lectura de los sectores, por lo cual, se intento copiar en reversa, es decir, del último sector al primero, sin embargo tampoco se logro la lectura. Se intentó leer diferentes áreas del DDE, tanto de reversa como normal, pero la lectura ya no fue posible, incluso el BIOS dejo de detectar nuevamente al DDE.

Los platos volvieron a dañar las cabezas, lo que detona un *headcrash* no visible en los platos.

La Figura A8.5 muestra el hash MD5 y SHA1 de la copia parcial (1.2GB).

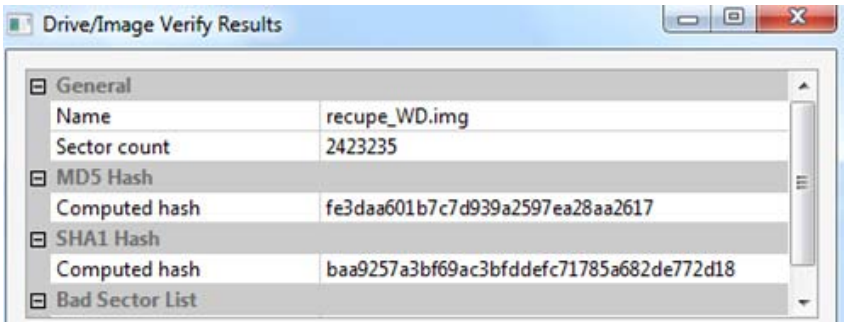


Figura A8.5. Hash MD5 y SHA1 de la copia parcial.

Para intentar obtener un mayor porcentaje de la imagen *bit* a *bit*, se requería de un segundo DDE donador, pero debido a la existencia de daño en la media, había una probabilidad menor al 20% de tener éxito en un segundo cambio de *head-stack*. Adicionalmente a que no se logro obtener un segundo DDE donador.

En la tabla A8.3 se describen los resultados de las fases de esta etapa.

Tabla A8.3. Resultados de las fases de la Obtención de imagen.

FASES	RESULTADO
Preparación del DDE destino	Se sanitizó un DDE de 60GB utilizando el programa Winhex. El número de sectores del DDE destino es mayor al DDE dañado
Creación de la imagen	Únicamente se logro obtener una copia *bit* a *bit* del 3%, utilizando el programa ByteBack. La existencia de daño en la media no visible, ocasiono nuevamente daño en las cabezas de lectura/escritura, impidiendo nuevamente el reconocimiento del DDE por el BIOS
Verificación de la imagen	Se obtuvo el hashs MD5 y SHA1 para la imagen parcial. Para el DDE dañado no se pudo obtener debido a que se volvió a dañar

4. Análisis lógico

Se analizó la imagen parcial, debido al poco porcentaje de dicha imagen obtenido, no fue posible visualizar la unidad lógica. Los resultados de las fases de esta etapa se muestran en la tabla A8.4.

Tabla A8.4. Resultados de las fases del Análisis lógico.

FASES	RESULTADO
Activación del modo de lectura	Se activo el modo de lectura mediante Software, utilizando el programa Winhex.
Análisis del MBR	El análisis del MBR reveló la existencia de una partición de 37.26GB, con el tamaño correspondiente al tamaño del DDE dañado
Análisis de la estructura del SA	El sector de inicio de la partición identificada, muestra el tamaño de la partición correcto, así como las FAT's.

Al finalizar el análisis lógico, se detecto que tanto la MBR como el sector de inicio y FAT's, no presentaban daño lógico, ya que ambas correspondían a una partición de 37.26GB. Los sectores dañados se ubican en el área de datos. La Figura A8.6 muestra al MBR y al Sector de inicio vistos por winhex en el gesto de plantilla.

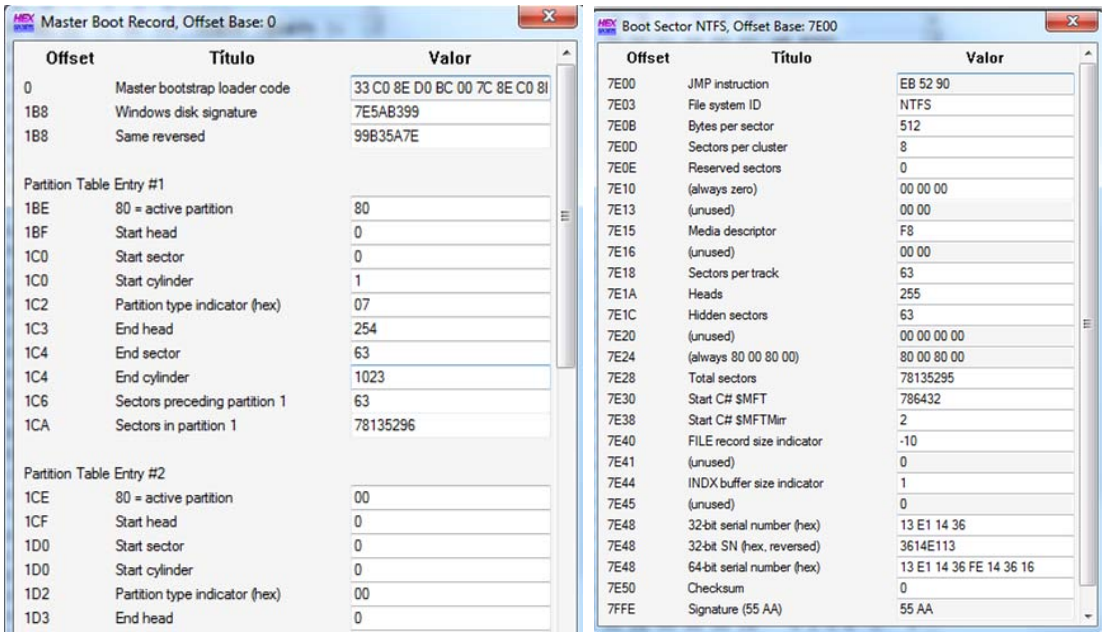


Figura A8.6. MBR y Sector de inicio vistos por winhex.

5. Reparación lógica

Debido a que el análisis lógico revelo que la estructura lógica funciona correctamente, no fue necesario efectuar algún tipo de reparación.

6. Recuperación de datos

Se ejecutó el software GetDataBack FAT [26] para recuperar aquellos archivos o subdirectorios que pudiesen existir en la imagen parcial, y que pudieran estar desligados de su directorio, así como archivos borrados. La estructura del SA estaba incompleta, el programa fue capaz de reconstruir algunos archivos y carpetas con nombres.

Se recuperaron con GDB 1,421archivos=2.13GB.

Se corrió el proceso de recuperación de archivos "recuperación por tipo de archivos", utilizando el programa Recovery My Files [27].

Se logró obtener 2,923archivos= 3.93GB.

Entre ambas recuperaciones se obtuvo 4,344 archivos=6GB

En la tabla A8.5 se describen los resultados de las fases de esta etapa.

Tabla A8.5. Resultados de las fases de la Recuperación de datos.

FASES	RESULTADO
Ejecución de software especializado	Se ejecuto el programa GDB FAT, activando la opción de búsqueda de archivos borrados y búsqueda exhaustiva
Revisión de integridad de archivos críticos	Se revisaron los archivos obtenidos con la finalidad de encontrar archivos críticos que conservaran su nombre real y ubicación. Los archivos críticos eran: Word, Excel y power point. Se encontraron pocos archivos críticos y varios del sistema operativo, por lo que era necesaria la recuperación por tipo de archivos.
Recuperación por tipo de archivos	Esta búsqueda se efectuó ejecutando el programa Recover My Files, indicando que buscara archivos de Word, Excel, power point, winzip, acrobat, e imágenes como jpg, tif, bmp

7. Reparación de archivos críticos

Esta etapa no fue necesaria, debido a que los archivos recuperados por tipo de archivos, fueron recuperados de forma íntegra.

ANEXO 8. FUNCIÓN DE INTEGRIDAD HASH.

Una función hash es una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc, resumir o identificar un dato a través de la probabilidad, utilizando una función hash o algoritmo hash [48].

El algoritmo para un hash MD5 se muestra en la Figura A5.1 [49]:

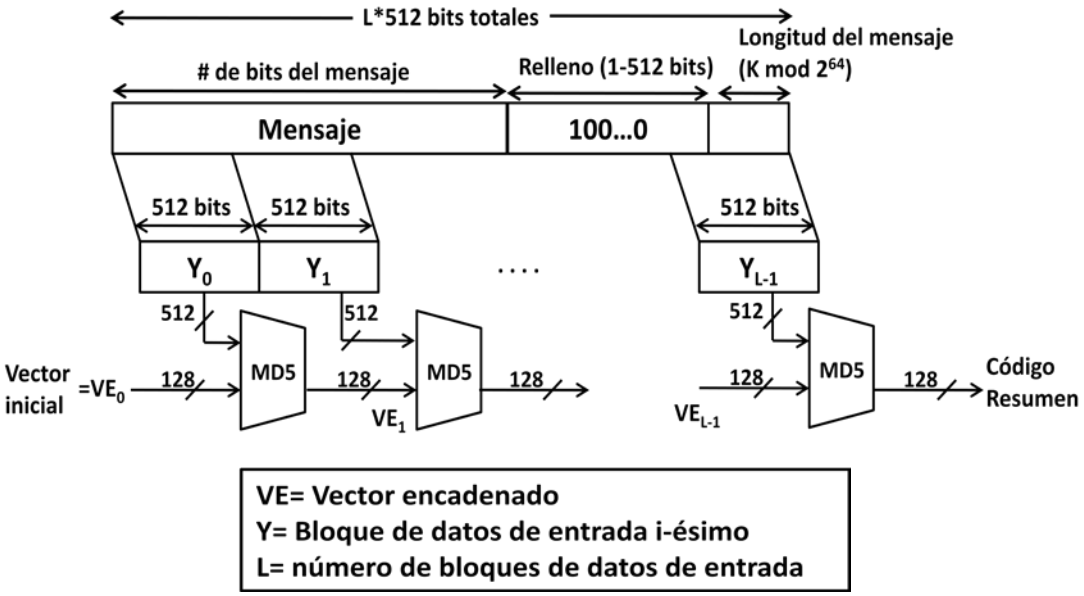


Figura A5.1. Algoritmo hash MD5.

El algoritmo para un hash SHA-1 se muestra en la Figura A5.2 [50]:

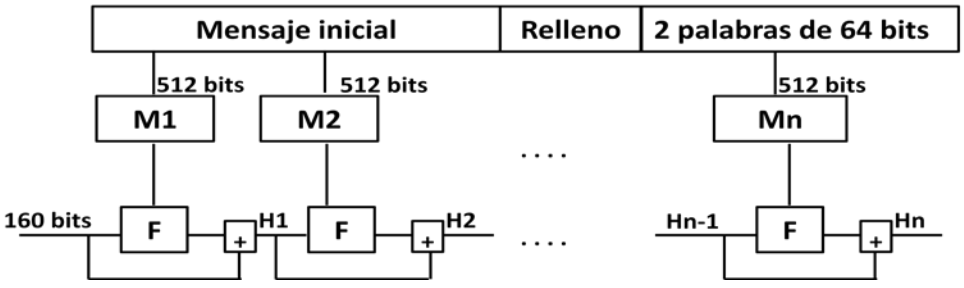
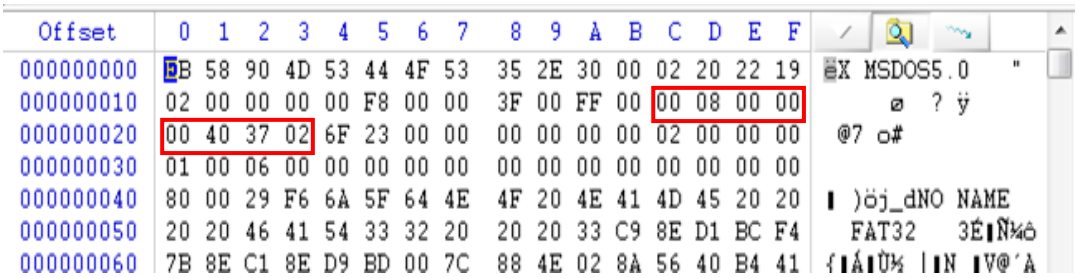


Figura A5.2. Algoritmo hash SHA-1.

ANEXO 9. EJEMPLOS DEL CÁLCULO DEL SECTOR FINAL DE UNA PARTICIÓN, DE LA MFT Y DE LA FAT.

6.1. Calculo del sector final para SA FAT32.

En la Figura A6.1 se muestra un sector de inicio de un SA FAT32, visto en un editor hexadecimal.



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
000000000	EB	58	90	4D	53	44	4F	53	35	2E	30	00	02	20	22	19
000000010	02	00	00	00	00	F8	00	00	3F	00	FF	00	00	08	00	00
000000020	00	40	37	02	6F	23	00	00	00	00	00	00	02	00	00	00
000000030	01	00	06	00	00	00	00	00	00	00	00	00	00	00	00	00
000000040	80	00	29	F6	6A	5F	64	4E	4F	20	4E	41	4D	45	20	20
000000050	20	20	46	41	54	33	32	20	20	20	33	C9	8E	D1	BC	F4
000000060	7B	8E	C1	8E	D9	BD	00	7C	88	4E	02	8A	56	40	B4	41

Figura A6.1. Sector de inicio FAT32.

Del capítulo 1, de la tabla 1.6 verificamos la posición del sector inicial, el cual corresponde al campo “Número de sectores antes del inicio de la partición” ubicado en posición 001Ch-001Fh , y el total de sectores en la partición que corresponde al campo “Valor de 32 bits de número de sectores en el sistema de archivos” ubicado en la posición 0020h-0023h. Para poder calcular el sector final, se transforman los números hexadecimales a decimales acorde el Anexo 1 (los valores en el editor hexadecimal están expresados en “little indian”)

- Sector inicial= 00 08 00 00, expresado en “big indian”=00 00 08 00, expresado en valor decimal= 2048.
- Sectores en la partición=00 40 37 02, expresado en “big indian”=02 37 40 00, expresado en valor decimal= 37175296.

Por último se aplica del capítulo 4, la ecuación 4.1.

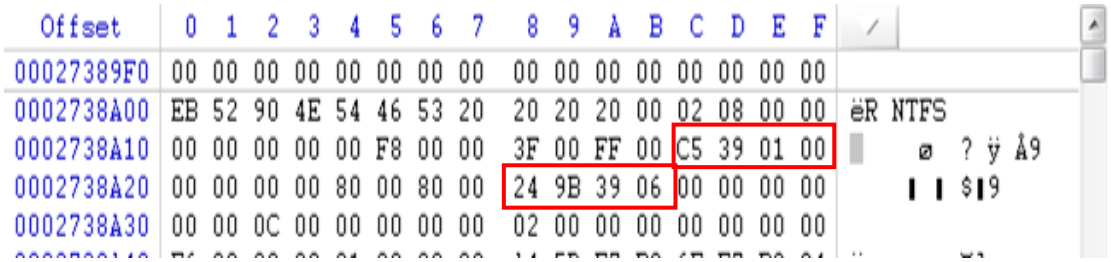
$$\#\ sector\ final = (\#\ sector\ inicial + \#\ total\ de\ sectores\ en\ la\ partición\ )$$

$$\#\ sector\ final = (2{,}048 + 37{,}175{,}296\ )$$

$$\#\ sector\ final = 37{,}177{,}344$$

6.2. Calculo del sector final para SA NTFS.

En la Figura A6.2 se muestra un sector de inicio de un SA NTFS, visto en un editor hexadecimal.



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00027389F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0002738A00	EB	52	90	4E	54	46	53	20	20	20	20	00	02	08	00	00
0002738A10	00	00	00	00	00	F8	00	00	3F	00	FF	00	C5	39	01	00
0002738A20	00	00	00	00	80	00	80	00	24	9B	39	06	00	00	00	00
0002738A30	00	00	0C	00	00	00	00	00	02	00	00	00	00	00	00	00

Figura A6.2. Sector de inicio NTFS.

Del capítulo 1, de la tabla 1.12 verificamos la posición del sector inicial, el cual corresponde al campo “Sectores escondidos” en el offset 17 a partir del inicio de los parámetros del bloque BIOS, y el total de sectores en la partición que corresponde al campo “Total de sectores en la partición” ubicado en el offset 29 a partir del inicio de los parámetros del bloque BIOS. Se transforman los números hexadecimales a decimales acorde el anexo 1 (los valores en el editor hexadecimal están expresados en “little indian”).

- Sector inicial= C5 39 01 00, expresado en “big indian”=00 01 39 C5, expresado en valor decimal= 80325.
- Sectores en la partición=24 9B 39 06, expresado en “big indian”=06 39 9B 24, expresado en valor decimal= 104,438,564.

Por último se aplica la ecuación 4.1 del capítulo 4:

$$\#\ sector\ final = (\#\ sector\ inicial + \#\ total\ de\ sectores\ en\ la\ partición\ )$$

$$\#\ sector\ final = (80{,}325 + 104{,}438{,}564\ )$$

$$\#\ sector\ final = 104{,}518{,}889$$

6.3. Calculo del sector de ubicación de la MFT.

Del sector de arranque de la Figura A6.3, ubicamos acorde a la tabla 1.12 del capítulo 1, el sector inicial (como se indica en la sección 6.2), el número de cluster de la MFT ubicado en el offset 37 a partir del inicio de los parámetros del bloque BIOS, y el número de sectores por cluster ubicado en el offset 2 a partir del inicio de los parámetros del bloque BIOS. Los valores hexadecimales se convierten a decimales.

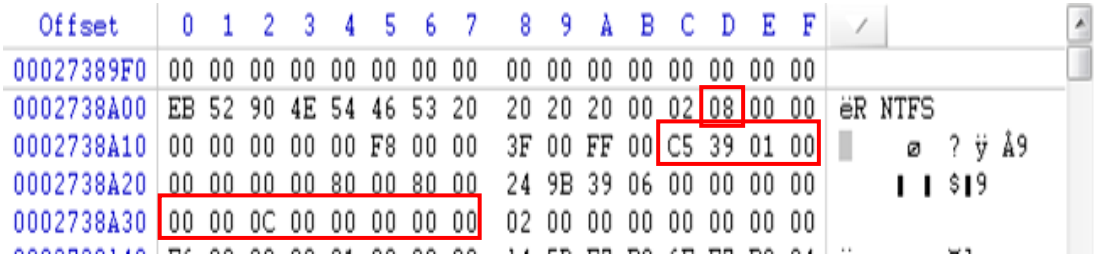


Figura A6.3. Sector de inicio NTFS.

- Sector inicial= C5 39 01 00, expresado en “big indian”=00 01 39 C5, expresado en valor decimal= 80,325.
- Número de cluster de la MFT= 00 00 0C 00 00 00 00 00, expresado en “big indian”=00 00 00 00 00 0C 00 00, expresado en valor decimal= 786,432.
- Número de sectores por cluster= 08, expresado en “big indian”= 08, expresado en valor decimal= 8.

Por último se aplica la ecuación 4.2 del capítulo 4.

$$\#\ sector\ MFT = \#\ sector\ inicial + (\#\ cluster\ de\ MFT * \#\ de\ sectores\ por\ cluster)$$

$$\#\ sector\ MFT = 80{,}325 + (786{,}432 * 8)$$

$$\#\ sector\ MFT = 80{,}325 + (6{,}291{,}456)$$

$$\#\ sector\ MFT = 6{,}371{,}781$$

ANEXO 10. EJEMPLOS DE CÁLCULO DE LA TASA DE RECUPERACIÓN.

Para el cálculo de la tasa de recuperación, se utiliza la ecuación 5.4 del capítulo 5; se verifican los valores de las variables X's para sustituir por 1 ó 0, y de esta forma sumar los coeficientes. Para X_1 (daños), X_2 (soluciones), X_6 (marcas), sólo se elige un coeficiente.

EJEMPLO 1:

Disco duro marca Hitachi de 120GB, con cabezas mal alineadas que requiere cambio de *head-stack*, se logró conseguir DDE donador compatible, con tipo de escritura/lectura longitudinal, y sistema de archivos NTFS.

Sustituyendo en la ecuación 5.4 con los valores de las variables X's:

$$Y = G(X_1) + H(X_2) + (0.4134546)x_3 + (0.00160927)x_4 + (0.00234321)x_5 + I(X_6) + (0.00228459)x_7 + 0.0346894$$

$$Y = (0.13581172)(1) + (0.1020121)(1) + (0.4134546)(1) + (\ 0.00160927)(1) + (0.00234321)(1) + (0.02278069)(1) + (0.00228459)(1) + 0.0346894$$

$$Y = 0.13581172 + 0.1020121 + 0.4134546 + 0.00160927 + 0.00234321 + 0.02278069 + 0.00228459 + 0.0346894$$

Tasa de recuperación= 0.71498558

EJEMPLO 2:

Disco duro marca Fujitsu de 500GB, con particiones dañadas que requiere reparación de la estructura, con tipo de escritura/lectura perpendicular, y sistema de archivos NTFS.

Sustituyendo en la ecuación 5.4 con los valores de las variables X's:

$$Y = G(X_1) + H(X_2) + (0.4134546)x_3 + (0.00160927)x_4 + (0.00234321)x_5 + I(X_6) + (0.00228459)x_7 + 0.0346894$$

$$Y = (0.12650955)(1) + (0.11006569)(1) + (0.4134546)(1) + (\ 0.00160927)(1) + (0.00234321)(0) + (0.07654313)(1) + (0.00228459)(1) + 0.0346894$$

$$Y = 0.12650955 + 0.11006569 + 0.4134546 + 0.00160927 + 0.07654313 + 0.00228459 + 0.0346894$$

Tasa de recuperación= 0.76515623

ANEXO 11. PUBLICACIONES.

Congresos internacionales

Maricarmen Pérez-García, Marcos A. Rosales-García, Héctor M. Pérez-Meana. "Main damages classification in Electromechanical Hard Disk Drives and the possible solutions". 1st. International Congress on Instrumentation and Applied Sciences. Octubre 26-29, 21010 Cancún, Q.R.

Maricarmen Pérez-García, Marcos A. Rosales-García, Héctor M. Pérez-Meana. "Metodología para Recuperación de Información en discos duros electromecánicos dañados para su análisis forense". VIII Congreso Internacional sobre Innovación y Desarrollo Tecnológico. Noviembre 24-26, 2010. Cuernavaca, Morelos.

Congresos nacionales

Alejandro Padrón Godínez, Maricarmen Pérez García, Nicolás Solano Luna. "Generación de políticas de Seguridad Informática". SOMI XXIV Congreso de Instrumentación. Mérida Yucatán, Octubre 2009.

CCADET
CENTRO DE CIENCIAS APLICADAS Y DESARROLLO TECNOLOGICO

1ST INTERNATIONAL CONGRESS ON INSTRUMENTATION AND APPLIED SCIENCES

CONACYT

FRESENIUS KABI

Centro de Ciencias Aplicadas y Desarrollo Tecnologico of the Universidad Nacional Autonoma de Mexico

CERTIFICATE OF PARTICIPATION

This is to certify that

M. Pérez-García, M. A. Rosales-García and H. Pérez-Meana

attended the congress and presented the paper

Main damages classification in Electromechanical Hard Disk Drives and the possible solutions

at the 1ST INTERNATIONAL CONGRESS ON INSTRUMENTATION AND APPLIED SCIENCES

CANCUN, Q.R., MEXICO, OCTOBER 26-29, 2010

Dr. José Manuel Saniger-Blesa
HONORARY CHAIR

Dr. Gabriel Ascanio
CHAIR

Main damages classification in Electromechanical Hard Disk Drives and the possible solutions

M. Pérez-García, M. A. Rosales-García, H. Pérez-Meana

mperezg0808@ipn.mx

SEPI ESIME Culhuacan
Avenida Santa Ana #1000 Col. San Francisco Culhuacan.
Deleg. Coyoacán, C.P. 04430, México D.F.

Abstract: When an Electromechanical Hard Disk Drive has a failure and the information in that device is valuable, it is important to determinate the type of damage to implement the most appropriate solution to recover the information. Despite the technological advances made in electromechanical hard disk drives, they still fail, some failures can become predictable but most of them not. Hard Disk Drives are found in laptops, desktop computers and Servers; they are sensitive to damages because of its own nature of mechanic and electronic functionality, its working environment conditions, human errors, among other. This paper describes the main causes that affect the Electromechanical Hard Disk Drives and its consequences, in order to provide a classification of damages and the possible solutions. The classification is based in logical and physical damages, as physical damage is failure in electromechanical elements; as logical damage is corruption of the *file system* structure, deletion of files, overwritten, etc. Sometimes a physical damage require as solution a change of elements as *head-stack*, *motor*, or some chips of the *Printed Circuit Board*, when it happen a donor electromechanical Hard Disk Drive is needed, this must be the same model as the damaged. A logical damage normally requires as solution Software that can analyze the Electromechanical Hard Disk Drive sector by sector.

I. Introduction

Over the last years, the information stored in electronic devices is one of the most important assets, not only for companies, for all people too. Ninety-two percent of new generated information is stored in electronic devices, mostly Hard Disk Drives (HDD) [1], as these are found in Servers, desktop computers and laptop. This information can be a simple user file, a picture, the payroll of a company or software that controls the entire production line.

Electromechanical Hard Disk Drive (EHDD) is sensitive to damages because of its own nature of mechanic and electronic functionality, its working environment conditions, human errors, among other. Damage in EHDD can cause data loss, and this problem worsens as more valuable information is, also if there are no backups or these are incomplete or obsolete.

There have been done some researches to predict failures in EHDD, some of them based on Bayesians method as the Hamerly and Elkan [2] or some based on algorithms Murray et al [3]. Although there are some kind of damages that are not predictable as falls, brownouts, power loss, power surge or malicious persons.

This paper outlines the main causes that affect an EHDD and consequences that arise, to provide damages classification and possible solutions. This classification will be useful during the process of Data Recovery, when an EHDD had a fail, it helps to identify the kind of damage and the correct process and tools that will be used.

CIINDET 2010
HACIA UN DESARROLLO SUSTENTABLE CON TECNOLOGÍA PROPIA

IEEE
SECCIÓN MORELOS

CONSTANCIA

Artículo: ***"Metodología para recuperación de información en discos duros electromecánicos dañados para su análisis forense."***

Autores: **Maricarmen Pérez García, Marcos Arturo Rosales García, Héctor Manuel Pérez Meana.**

Id. artículo: **690**
Área: **Sistemas Computacionales**

El Comité Técnico del VIII Congreso Internacional Sobre Innovación y Desarrollo Tecnológico CIINDET 2010, que se llevó a cabo en la ciudad de Cuernavaca, Morelos, México, del 24 al 26 de noviembre de 2010, hace constar que el artículo citado fue presentado de acuerdo con el programa técnico del congreso e incluido en las memorias del mismo.

La presente constancia se expide para los fines legales que a los autores convengan.

Cuernavaca, Morelos, México a 26 de Noviembre de 2010.

Atentamente

M.C. Humberto Hernández García
Presidente del Comité Técnico CIINDET 2010

CONGRESO INTERNACIONAL SOBRE INNOVACION Y DESARROLLO TECNOLOGICO
CIINDET

CIINDET 2010

HACIA UN DESARROLLO SUSTENTABLE
CON TECNOLOGÍA PROPIA

IEEE
Sección Morelos

La Sección Morelos del
Instituto de Ingenieros en Electricidad y en Electrónica

Otorga el presente

Reconocimiento

A: **Maricarmen Pérez García**

Por su participación como

C O N G R E S I S T A

Durante el VIII Congreso Internacional sobre Innovación
y Desarrollo Tecnológico, realizado del 24 al 26 de noviembre del 2010,
en la ciudad de Cuernavaca, Morelos, México.

M.C. Julio A. Hernández Galicia
Presidente IEEE Sección Morelos

VIII CONGRESO INTERNACIONAL SOBRE INNOVACION Y DESARROLLO TECNOLOGICO

Innovaciones inteligentes para las sociedades modernas

CIINDET 2010

VIII Congreso Internacional sobre Innovación y Desarrollo Tecnológico, 24 al 26 de noviembre de 2010, Cuernavaca Morelos, México.

Metodología para recuperación de información en discos duros electromecánicos dañados para su análisis forense

M. Pérez-García, M. A. Rosales-García, H. M. Pérez-Meana

Resumen: Al llevar a cabo una investigación de informática forense en un disco duro electromecánico se puede presentar el caso que dicho disco tenga un daño lógico ó físico, no permitiendo el análisis en busca de evidencia, requiriéndose realizar el proceso de recuperación de información. La recuperación de información así como la informática forense debe tener su propia metodología, ya que en ambos casos se trabaja con la información, siendo esta el objeto principal de estudio. Debido a que no existe una metodología definida para este proceso que ayude a una adecuada y rápida recuperación, el propósito de este trabajo es proporcionar una metodología aplicable cuyo objetivo sea recuperar la mayor cantidad de información de forma íntegra. Los resultados muestran que aplicando esta metodología aumenta el número de casos de éxito y la cantidad de información recuperada.
Palabras Clave: Discos duros electromecánicos, daños físicos y lógicos, *headcrahs, stiction, fly height.*
Abstract: During an investigation of Computer Forensic in an electromechanical hard disk drive, could happen that the hard disk has a physical or logical damage, turning the analysis for searching evidence become impossible, a process of Data Recovery will be required. The Data Recovery on damaged hard disk drive and the Computer Forensic must have its own methodology, since in both cases the experts handle with information, which it is the target of the analysis. Due the absence of a defined methodology for this process which helps to an adequate and earlier recovery, the purpose of this paper is to provide an applicable methodology which objective is to recover as much reliable data as possible. The results show that applying this methodology, the number of success cases and the amount of information recovered are increased.
Keywords: Electromechanical hard disk drive, physical and logical damages, *headcrahs, stiction, fly height.*

Maricarmen Pérez García, mperezg0808@ipn.mx.
Marcos Arturo Rosales García, marosales@ipn.mx.
Héctor Manuel Pérez Meana, hmperezm@ipn.mx.
SEPI ESIME Culhuacan, IPN.
Avenida Santa Ana #1000 Col. San Francisco Culhuacan, Deleg. Coyoacán. C.P. 04430, México D.F.

Se agradece al Consejo Nacional de Ciencia y Tecnología (CONACYT) y al Instituto Politécnico Nacional (IPN) por el apoyo recibido, durante la realización del presente trabajo.

Introducción

La informática forense es la ciencia que se encarga de identificar, preservar, analizar y presentar evidencia digital en una forma que sea aceptable en un proceso legal [1].
De manera general las etapas que se realizan durante el análisis forense informático sobre un Disco Duro Electromecánico (DDE) son:

- Identificación: Se identifican los DDEs involucrados en el caso y se conocen los detalles del mismo.
- Preservación: Se obtiene una imagen *bit* a *bit* del DDE para trabajar sobre esta y resguardar al DDE original, en esa etapa damos por hecho que el DDE funciona de forma correcta. Sin embargo puede ocurrir el caso que dicho disco tenga un daño lógico ó físico, lo que implica recuperar previamente la información que se va a analizar, requiriéndose realizar el proceso de recuperación de información.
- Análisis: Se realiza la búsqueda de la evidencia del incidente y se analiza.
- Presentación: Se presentan en forma escrita mediante un reporte, los resultados obtenidos de la investigación.

La recuperación de información, así como la Informática forense, debe tener una metodología y ser realizada por expertos de manera que permita recuperar la información y llevar a cabo una investigación de forma correcta.
Existen diferentes metodologías para realizar un análisis forense informático, tales como las metodologías del "National Institute of Standards and Technology" [2], de la "European Network of Forensic Science Institute" [3], del "National Institute of Justice" de los Estados Unidos [4], entre otras. Sin embargo ya que no existen metodologías conocidas para la

SOMI XXIV
Congreso de Instrumentación

Mérida Yucatán, México, Octubre 2009

La Sociedad Mexicana de Instrumentación

Otorga la presente

CONSTANCIA

a: Alejandro Padrón Godínez, Maricarmen Pérez García, Nicolas Solano Luna

Por haber presentado en el Congreso de Instrumentación SOMI XXIV su trabajo:

Generación de políticas de seguridad informática

Dr. José Manuel Saniger Blesa
PRESIDENTE

Dr. Gabriel Ascanio Gasca
SECRETARIO EJECUTIVO

SOMI XXIV Congreso de Instrumentación
Mérida, Yucatán, del 14 al 16 de octubre de 2009

GENERACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

Alejandro Padrón G., Maricarmen Pérez García*, Nicolás Solano Luna**
Grupo Académico de Modelado y Simulación de Procesos, CCADET
Universidad Nacional Autónoma de México. Apartado Postal 70 - 186, Coyoacán, C. P. 04510, México D. F.,
Tel.: (01) 5622 8602, Ext.:1183, Fax: (01) 5622 8653,
* ESIME – Culhuacán, IPN
** Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán
e-mail: alejandro.padron@ccadet.unam.mx

Resumen

Una política de Seguridad es el conjunto de lineamientos que regirá el buen uso de los recursos informáticos dentro de una Organización, describiendo tanto los derechos como las obligaciones a que están sujetos los diferentes tipos de equipos y usuarios, así como las normas de conducta y buen uso de los recursos. En este trabajo se presenta la generación de políticas que van de lo global, pasando por los temas o tópicos específicos a políticas de aplicaciones específicas que planean aspectos estratégicos para la estabilidad de una Organización. Estas políticas se aplican sobre actividades o activos en la Organización, como control de acceso físico y lógico, análisis de riesgos, software, selección de personal, estado físico y disponibilidad de equipamiento, clasificación de la información, resguardo y respaldo de la misma, procedimientos (comportamientos) y difusión y publicación de las mismas tanto como su revisión periódica por las altas gerencias de la Organización. Las políticas antes mencionadas deben estar disponibles para todos los usuarios y clientes. Su cumplimiento debe estar referido en los requerimientos y acuerdos de nivel de servicio de ITIL (Information Technologies Infrastructure Library), así como en los contratos.

a) Políticas globales

Se usan para crear la visión general y la dirección que tomará la organización.

Política no. 1.

Tema: Análisis de Riesgos

Aplica: Todo administrador de Tecnologías de la Información (TI)

Descripción: "El administrador de sistemas de TI es responsable de realizar un análisis de riesgos (AR) del sistema o sistemas de TI de *alto impacto* para la empresa de los que están a su cargo administrativo, con una periodicidad de al menos un año".

Sanción: El incumplimiento de esta política podrá causar una observación administrativa conforme lo determine el comité de seguridad informática.

Vigencia: Esta política entrará en vigor a partir del 6 de febrero del 2010.

Revisión: Anual.

Política no. 2.

Tema: Control de Acceso Físico

Aplica: Encargado del área de Mantenimiento