HERRAMIENTAS PARA LA RECUPERACION

1 OBJETIVO

El objetivo de la presente clase es conocer y aprender a utilizar las herramientas disponibles en el mercado para la recuperación de información, ya sea que la misma haya sido borrada por algún desperfecto técnico, por el descuido de un usuario, por una mala maniobra del técnico, o por el ataque de un virus.

No esta dentro de las premisas de esta clase el abocarnos al estudio de un producto en particular, sino a conocer genéricamente cuales son las herramientas con las que cuenta un técnico hoy en día para el desarrollo de esta tarea, ya sean estas comerciales o de distribución gratuita.

Dado que las cuestiones conceptuales para la comprensión del funcionamiento de dichas herramientas ya han sido abordadas oportunamente en capacitaciones anteriores y que dichos conceptos han sido aplicados en profundidad en las clases 9 y 10, durante la presente clase no se definirá ni profundizará sobre ninguno de estos conceptos, y se los dará por sabidos.

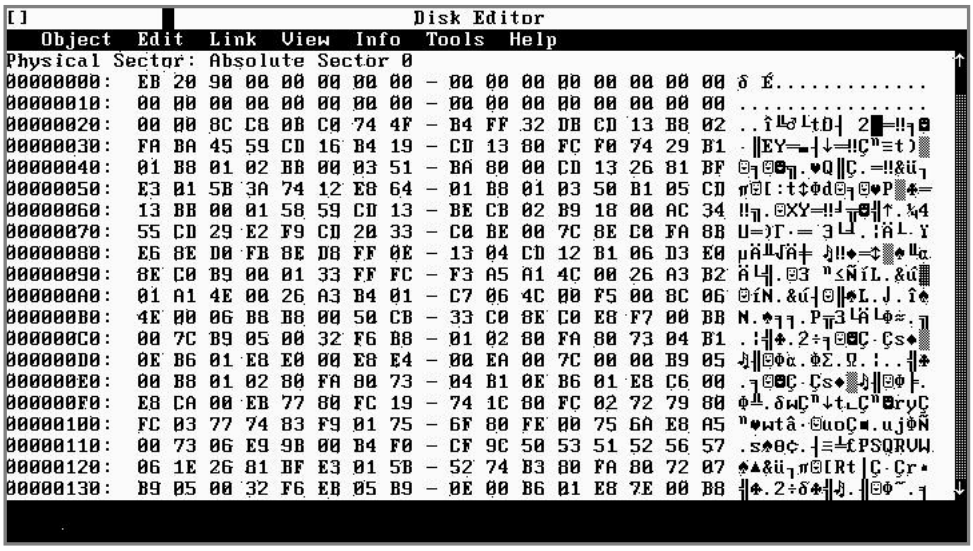
2 POSIBLES DAÑOS

2.1 DAÑOS EN EL MBR

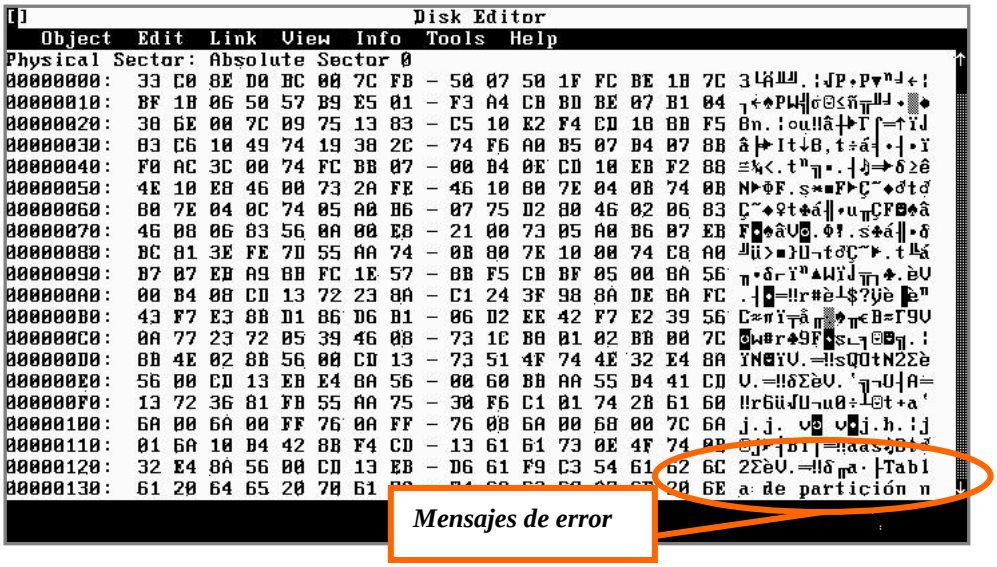
Cuando el problema esta centrado en el MBR será imposible iniciar o acceder a datos localizados en un disco rígido, estos daños pueden ser ocasionados por algunos tipos de virus, borrados accidentales a través de un software de particionado o cualquier otro tipo de error posible. Si bien tenemos herramientas y conocimientos para confirmar con certeza que el daño está ubicado en este sector tan crítico para un disco, será necesario muchas veces recurrir a software específico que realice una verificación de diversos sectores de la unidad e intente reconocer información conocida o relevante, de manera de poder volver a reconstruir la información perdida para luego dejarlo en un estado igual o similar al original.

En la primera de las capturas inferiores podemos ver el MBR de un disco rígido con Windows XP instalado sobre un sistema de archivos NTFS infectado por el virus Urkel, la segunda muestra el estado de un MBR normal.

Desde la visualización del MBR infectado por Urkel solo podemos especular que en la zona dedicada a los mensajes de error no se encuentran estos y por lo tanto podemos inferir que fue modificado por un virus.



En la segunda imagen podemos ver un MBR normal y dentro de él los típicos mensajes de error.



2.2 DAÑOS EN EL SECTOR DE ARRANQUE (BOOT SECTOR)

De la misma manera que el caso anterior cualquier falla en este sector dejará al disco imposibilitado de arrancar, lo que nosotros llamamos montar el volumen y acceder al sistema de archivos, por lo que deberemos realizar alguna tarea de reconstrucción o reparación para volver a acceder al sistema.

2.3 DAÑOS EN LAS TABLAS DE ASIGNACIÓN DE ARCHIVOS

Cuando se producen fallas en sectores de un disco rígido que pertenecen al área de que contienen las tablas FAT, estas quedarán inutilizadas para poder cumplir su función específicas, esto mismo sucedería en el caso de NTFS con la MFT, por lo que será imposible acceder a los datos contenidos en el disco afectado. Un problema que tiene FAT es que ubica sus tablas en un determinado grupo de sectores fijos y no pueden ser movidas una vez creadas, por lo que si un disco sufriera daños físicos en un sector destinado a la FAT quedaría inutilizado para su uso normal. Contrariamente a lo dicho anteriormente la MFT puede estar ubicada o movida a cualquier lugar de la partición, por lo que no tiene el problema de FAT.

Para efectuar un correcto diagnóstico del problema podemos recurrir a programas tales como el Norton Diskedit o el Winhexa y realizar una inspección del BR de forma de verificar su validez o los daños visibles (inexistencia, borrado, falta de la firma, datos "basura" o mensajes incorrectos)

3 HERRAMIENTAS PARA LA RECUPERACION DE INFORMACIÓN

Cuando nos referimos a este tipo de herramientas, hablamos de software capaz de facilitarnos la tarea de recuperar información que de otro modo sería dada por perdida. Hay que tener muy en cuenta que los daños físicos de los discos rígidos hacen imposible la tarea de recuperación de datos mediante cualquier tipo de software, por lo tanto, a continuación estaremos hablando de daños a nivel lógico. Los problemas que pueden causar pérdidas de información van desde los simples borrados accidentales (con vaciado de la papelera de reciclaje incluida) a fallas producidas por virus que incluyen corrupción o borrado de los sectores de arranque del disco rígido (MBR y Boot Sector), de las tablas de asignación de archivos FAT, MFT, el directorio raíz, etc.

Estas herramientas proveen la funcionalidad de escanear los diferentes sectores del disco rígido en busca de información útil o recuperable, dándonos la posibilidad en la mayoría de los casos de revertir situaciones desfavorables que incluyen la perdida de datos.

Para que la recuperación de datos sea lo más efectiva posible existen ciertas reglas básicas que deberán observarse para obtener los mejores resultados, por lo tanto si nos enfrentamos a una situación de este tipo deberán seguirse las siguientes pautas:

- Apagar inmediatamente la computadora.
- No intentar arrancar la PC en vano reiniciando reiteradamente si vemos que es imposible arrancar la computadora.
- No instalar ni desinstalar ningún programa sobre el disco rígido afectado (esto incluye a cualquier tipo de software de recuperación de datos)
- No alterar de ninguna manera la estructura de directorios o datos de la unidad afectada.
- Tratar en la medida de lo posible de realizar una imagen completa de la unidad con algún software adecuado (llámese Symantec Ghost o cualquier otro similar).

3.1 TEST DISK

TestDisk es una herramienta gratuita (Freeware) que fue diseñada para ayudar a recuperar particiones perdidas y/o a reparar discos con sectores de arranque dañados, siempre y cuando estos problemas sean causados por algún tipo de software, ciertos virus o errores humanos (borrados accidentales de tabla de particiones por ejemplo). TestDisk interroga al BIOS para detectar los discos rígidos instalados y sus características (tamaño LBA y geometría CHS) y realiza un chequeo rápido de la estructura de los mismos, comparándolos con las tablas de partición para detectar errores en alguna entrada. Si la tabla de la partición tiene errores puede repararlos. Si la unidad no tiene particiones visibles o la tabla de particiones esta totalmente vacía, TestDisk puede buscar sobre el disco particiones y crear una tabla nueva e incluso reconstruir el MBR por completo si es necesario. Sin embargo, el programa muestra al usuario la lista de las posibles particiones encontradas por TestDisk y da la opción de seleccionar cual fue nuestra partición o particiones perdidas. En algunos casos, especialmente después de iniciar una búsqueda detallada, pueden verse datos de particiones viejas que han sido suprimidas y sobrescritas anteriormente, por lo tanto será necesario ser cuidadoso y tener la información correcta sobre el último estado conocido a la hora de elegir la partición válida.

Como dato complementario podemos remarcar la rapidez con que desarrolla el análisis de un disco duro de 40 GB, ya que una búsqueda completa tarda menos de 30 segundos.

Testdisk puede ejecutarse bajo los siguientes sistemas operativos: DOS (modo real o desde una ventana de DOS de Windows 9x), Windows NT4, 2000, XP, 2003, Linux, FreeBSD, NetBSD, OpenBSD, SunOS y MacOS. Existen versiones del producto para DOS, Win32 y Linux. Igualmente el programa encuentra particiones para todos los sistemas de archivos siguientes:

- BeFS (BeOS)
- BSD disklabel (FreeBSD/OpenBSD/NetBSD)
- CramFS (Sistema de archivos comprimido)
- DOS/Windows FAT12, FAT16 y FAT32
- HFS, Hierarchical File System
- JFS, IBM's Journaled File System
- Linux Ext2 y Ext3
- Linux Raid
- Linux Swap (versiones 1 y 2)
- LVM y LVM2, Linux Logical Volume Manager
- Netware NSS
- NTFS (Windows NT/2K/XP/2003)
- ReiserFS 3.5 y 3.6

Testdisk puede bajarse de forma gratuita desde el sitio: http://www.cgsecurity.org/

3.2 WINTERNALS ADMINISTRATOR'S PAK

Administrator's Pak es una completa suite de herramientas que posibilitan la tarea de reparar sistemas no iniciables o bloqueados, restaurar datos perdidos, quitar remotamente virus o spyware de sistemas infectados y diagnosticar sistemas y redes. Administrator's Pak incluye las siguientes utilidades: ERD Commander 2005, Remote Recover, NTFSDOS Professional, Crash Analyzer Wizard, FileRestore, Filemon Enterprise Edition, Regmon Enterprise Edition, AD Explorer, Insight for Active Directory, y TCP Tools.

3.2.1 ERD

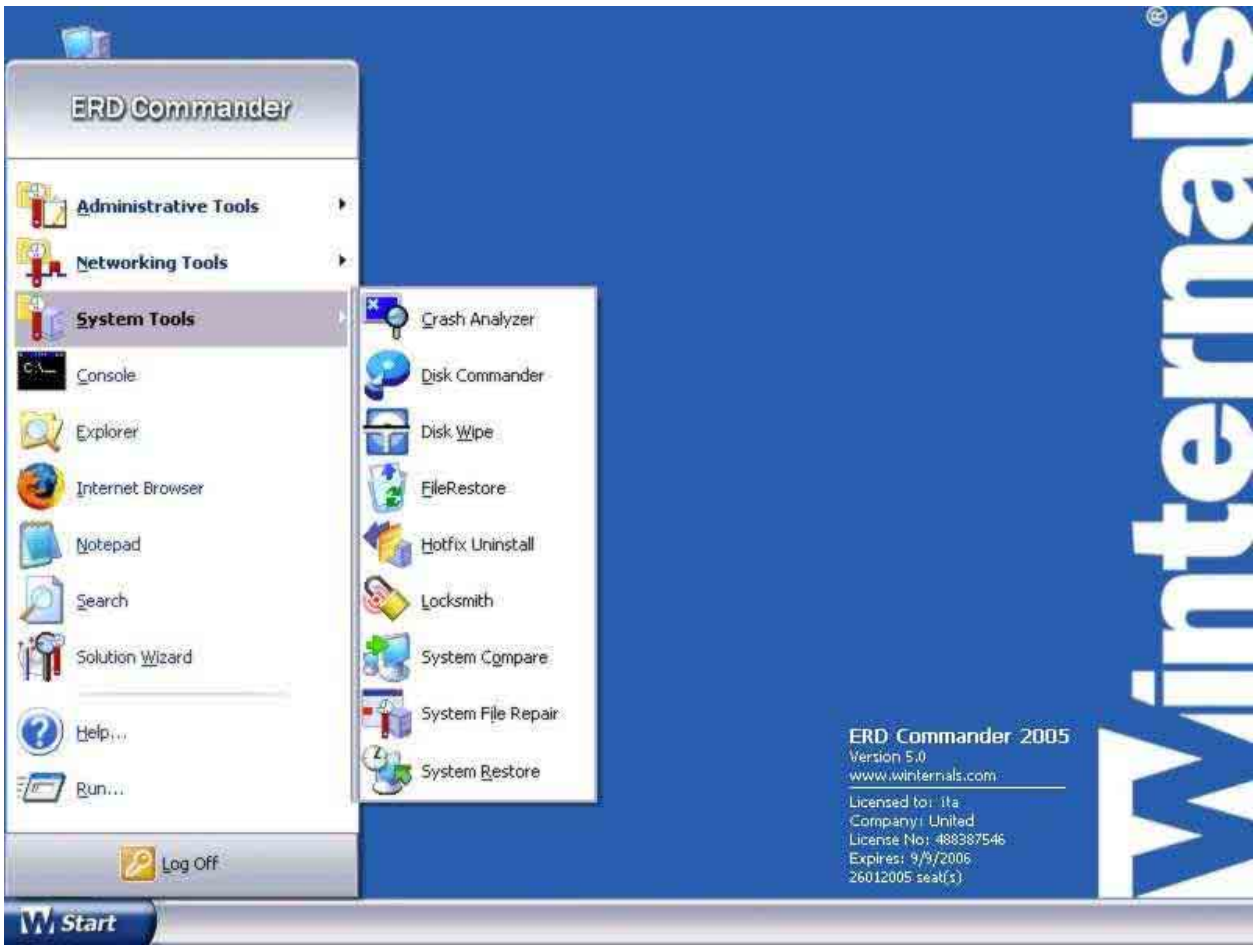
Este producto es de gran utilidad cuando un servidor o un puesto de trabajo de línea NT/2000/XP o 2003 Server no logra arrancar. Esta basado en ***WinPE*** (sistema operativo reducido de 32 bits de Microsoft) y se inicia directamente desde un CD.

De esta manera se tiene acceso completo a la instalación y los datos del sistema desde un ambiente de reparación, de manera de poder diagnosticar y reparar problemas usando las herramientas situadas en el menú inicio de ERD. Adicionalmente el producto incluye todo lo necesario para tener acceso a la red, posibilitándonos acceder a la misma y guardar datos en unidades de red.

Dentro del entorno de este programa tenemos acceso a diferentes utilidades para reparación y análisis de sistemas tales como:

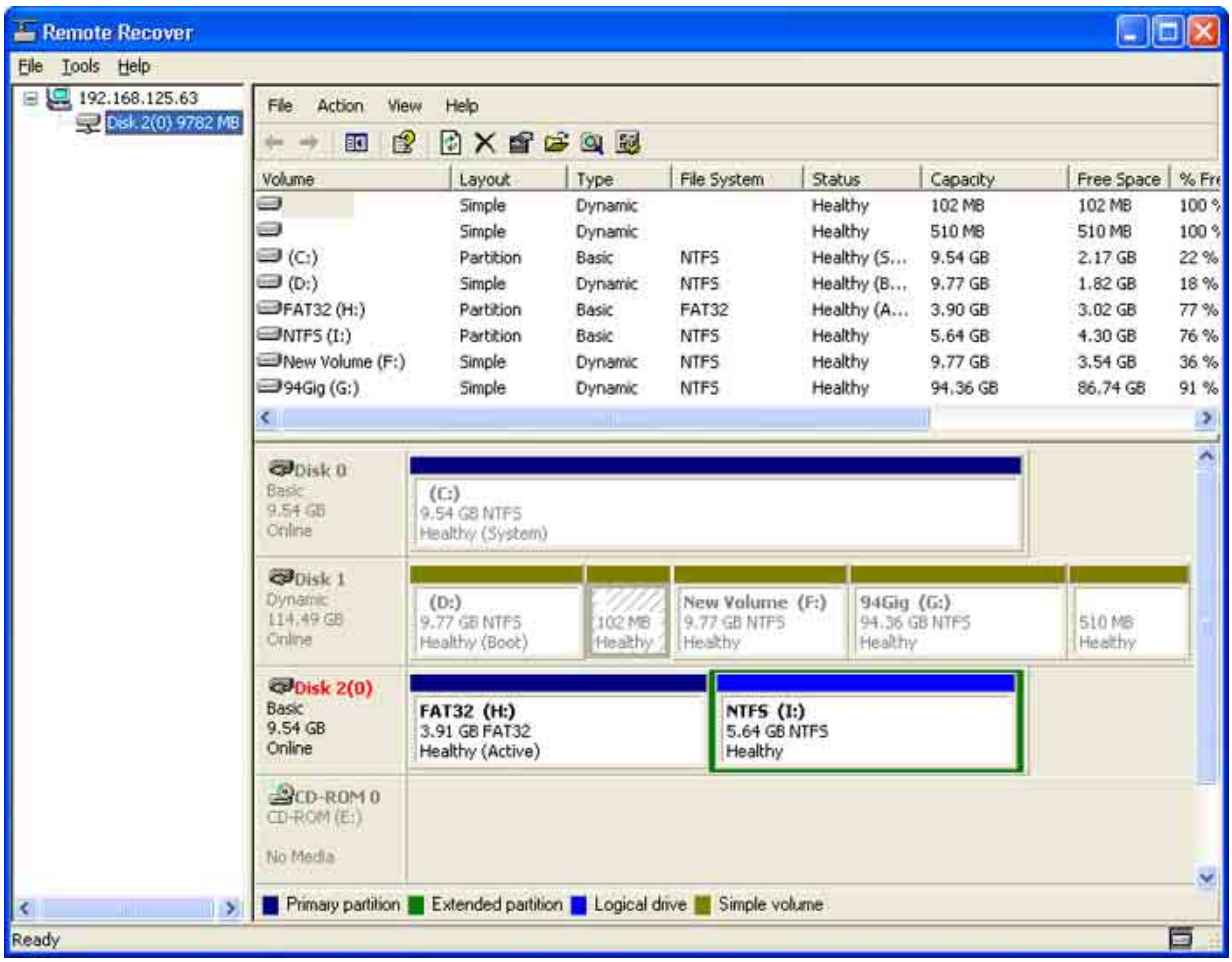
- ***Crash Analyzer*** analiza el sistema en busca de problemas que causen colgaduras.
- ***Disk Wipe*** se usa para borrar irreversiblemente información de discos rígidos.
- ***Locksmith*** reasigna passwords de Administrador perdidos.
- ***Filerestore*** permite localizar y recuperar archivos borrados.
- ***Diskcommander*** analiza y recupera información de discos rígidos dañados.
    - Provee acceso a la consola de puntos de restauración de Windows.
    - Detecta y elimina spyware o malware en sistemas Windows.
    - Provee un navegador para acceso a Internet.
    - Identifica y recupera automáticamente archivos críticos del sistema corruptos.
    - Provee un administrador de discos rígidos similar al de Windows XP.
- ***Registry Editor*** accede y edita el registro de sistema Windows no iniciables.
- Contiene una consola de acceso a Servicios y Drivers.
- Posee una interfaz de comandos compatible.
- Incluye una consola de administración de red.

Todas estas utilidades están disponibles desde el menú inicio del sistema ERD.



3.2.2 Remote recover

Esta utilidad permite reparar sistemas no booteables a través de la red. Remote recover posibilita el acceso vía red a discos rígidos de computadoras remotas como si estuvieran instalados en la propia PC, arrancando la PC remota mediante un CD, disquete o con PXE, de esta manera se pueden recuperar datos, remover virus o hasta instalar sistemas operativos en la otra PC.



3.2.3 NTFSDOS Professional

Mediante NTFSDOS se podrán generar disquetes booteable con acceso completo a volúmenes NTFS, pudiéndose reparar problemas de configuración o archivos corruptos en sistemas NT, 2000, XP y 2003 Server.

3.2.4 Crash Analyzer Wizard

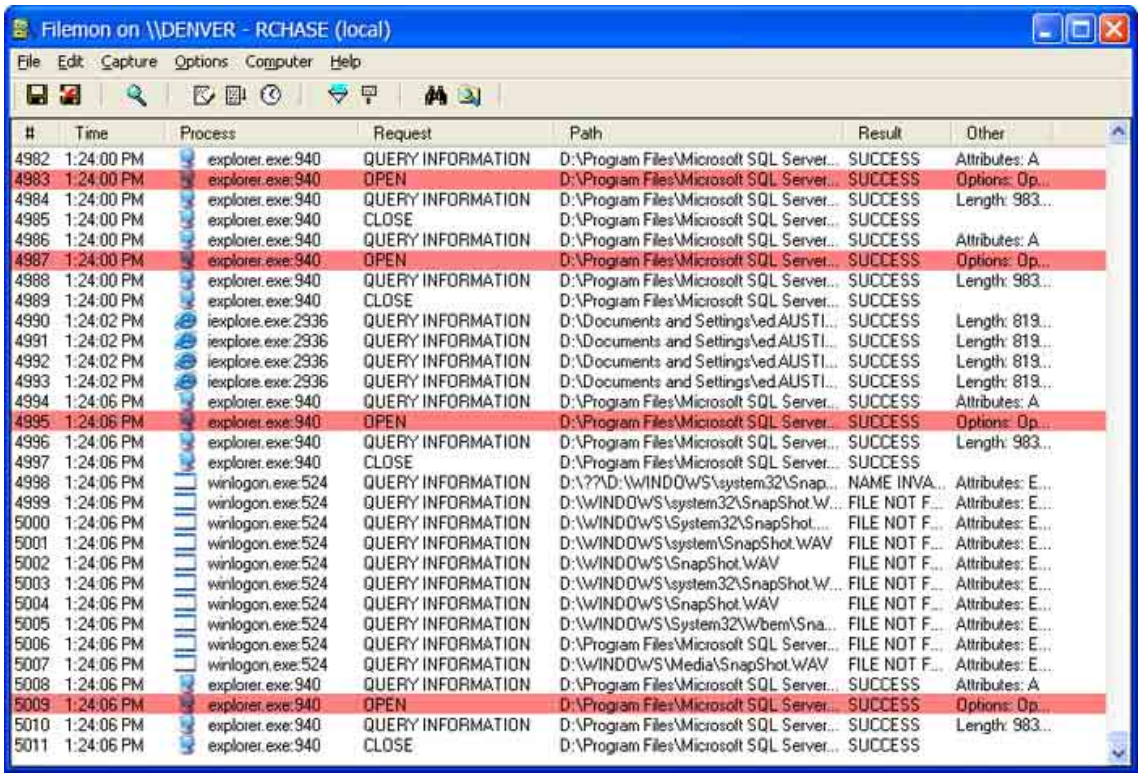
Esta utilidad permite determinar la mayoría de las causas de colgaduras, mediante el uso de un asistente que analiza el archivo de volcado generado por el sistema operativo.

3.2.5 FileRestore

Esta herramienta se utiliza para recuperar de forma simple archivos borrados o perdidos en la computadora, incluso aquellos que hayan sido quitados de la papelera de reciclaje.

3.2.6 Filemon Enterprise Edition

Su función es detectar remotamente problemas en sistemas de archivos de cualquier m'quina dentro de una red, permitiendo tener información en tiempo real de todos los accesos a sistemas de archivos sobre una computadora en particular.



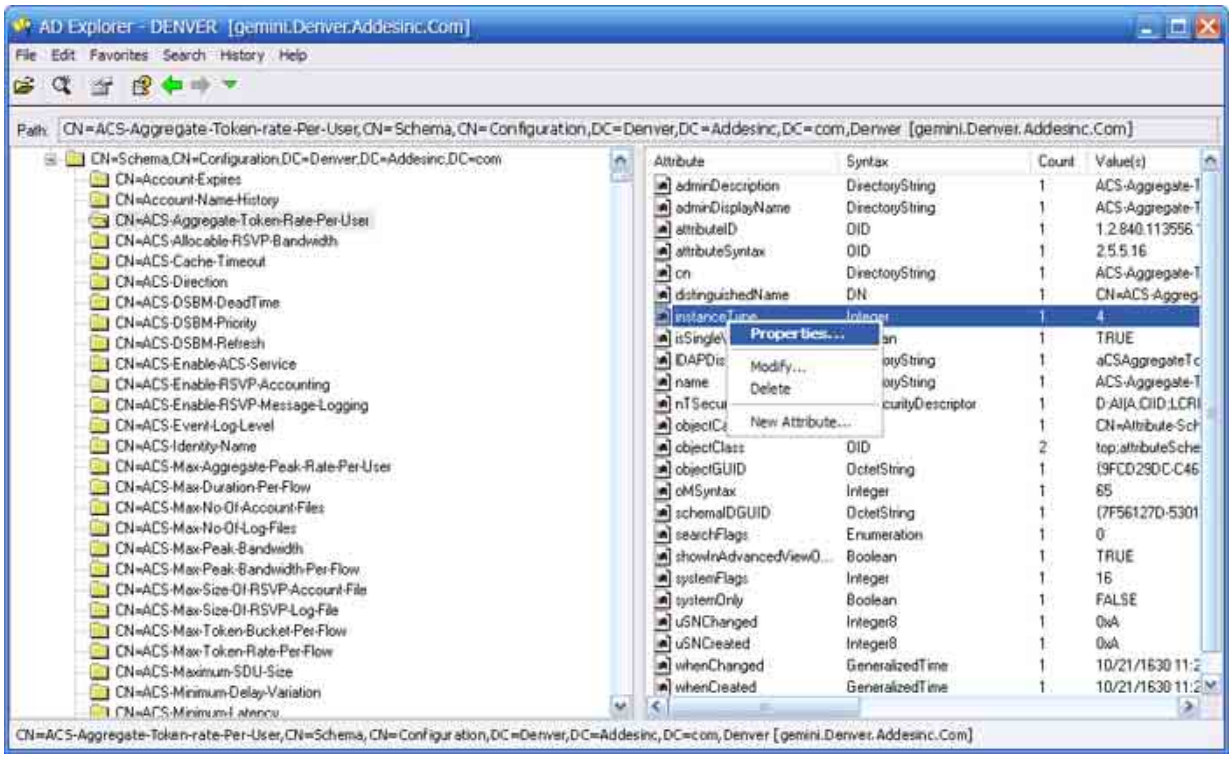
#	Time	Process	Request	Path	Result	Other
4982	1:24:00 PM	explorer.exe:940	QUERY INFORMATION	D:\Program Files\Microsoft SQL Server...	SUCCESS	Attributes: A
4983	1:24:00 PM	explorer.exe:940	OPEN	D:\Program Files\Microsoft SQL Server...	SUCCESS	Options: Op...
4984	1:24:00 PM	explorer.exe:940	QUERY INFORMATION	D:\Program Files\Microsoft SQL Server...	SUCCESS	Length: 983...
4985	1:24:00 PM	explorer.exe:940	CLOSE	D:\Program Files\Microsoft SQL Server...	SUCCESS	
4986	1:24:00 PM	explorer.exe:940	QUERY INFORMATION	D:\Program Files\Microsoft SQL Server...	SUCCESS	Attributes: A
4987	1:24:00 PM	explorer.exe:940	OPEN	D:\Program Files\Microsoft SQL Server...	SUCCESS	Options: Op...
4988	1:24:00 PM	explorer.exe:940	QUERY INFORMATION	D:\Program Files\Microsoft SQL Server...	SUCCESS	Length: 983...
4989	1:24:00 PM	explorer.exe:940	CLOSE	D:\Program Files\Microsoft SQL Server...	SUCCESS	
4990	1:24:02 PM	iexplore.exe:2936	QUERY INFORMATION	D:\Documents and Settings\ed.AUSTI...	SUCCESS	Length: 819...
4991	1:24:02 PM	iexplore.exe:2936	QUERY INFORMATION	D:\Documents and Settings\ed.AUSTI...	SUCCESS	Length: 819...
4992	1:24:02 PM	iexplore.exe:2936	QUERY INFORMATION	D:\Documents and Settings\ed.AUSTI...	SUCCESS	Length: 819...
4993	1:24:02 PM	iexplore.exe:2936	QUERY INFORMATION	D:\Documents and Settings\ed.AUSTI...	SUCCESS	Length: 819...
4994	1:24:06 PM	explorer.exe:940	QUERY INFORMATION	D:\Program Files\Microsoft SQL Server...	SUCCESS	Attributes: A
4995	1:24:06 PM	explorer.exe:940	OPEN	D:\Program Files\Microsoft SQL Server...	SUCCESS	Options: Op...
4996	1:24:06 PM	explorer.exe:940	QUERY INFORMATION	D:\Program Files\Microsoft SQL Server...	SUCCESS	Length: 983...
4997	1:24:06 PM	explorer.exe:940	CLOSE	D:\Program Files\Microsoft SQL Server...	SUCCESS	
4998	1:24:06 PM	winlogon.exe:524	QUERY INFORMATION	D:\??\D:\WINDOWS\system32\Snap...	NAME INVA...	Attributes: E...
4999	1:24:06 PM	winlogon.exe:524	QUERY INFORMATION	D:\WINDOWS\system32\SnapShot.W...	FILE NOT F...	Attributes: E...
5000	1:24:06 PM	winlogon.exe:524	QUERY INFORMATION	D:\WINDOWS\System32\SnapShot....	FILE NOT F...	Attributes: E...
5001	1:24:06 PM	winlogon.exe:524	QUERY INFORMATION	D:\WINDOWS\system\SnapShot.WAV	FILE NOT F...	Attributes: E...
5002	1:24:06 PM	winlogon.exe:524	QUERY INFORMATION	D:\WINDOWS\SnapShot.WAV	FILE NOT F...	Attributes: E...
5003	1:24:06 PM	winlogon.exe:524	QUERY INFORMATION	D:\WINDOWS\system32\SnapShot.W...	FILE NOT F...	Attributes: E...
5004	1:24:06 PM	winlogon.exe:524	QUERY INFORMATION	D:\WINDOWS\SnapShot.WAV	FILE NOT F...	Attributes: E...
5005	1:24:06 PM	winlogon.exe:524	QUERY INFORMATION	D:\WINDOWS\System32\Wbem\Sna...	FILE NOT F...	Attributes: E...
5006	1:24:06 PM	winlogon.exe:524	QUERY INFORMATION	D:\Program Files\Microsoft SQL Server...	FILE NOT F...	Attributes: E...
5007	1:24:06 PM	winlogon.exe:524	QUERY INFORMATION	D:\WINDOWS\Media\SnapShot.WAV	FILE NOT F...	Attributes: E...
5008	1:24:06 PM	explorer.exe:940	QUERY INFORMATION	D:\Program Files\Microsoft SQL Server...	SUCCESS	Attributes: A
5009	1:24:06 PM	explorer.exe:940	OPEN	D:\Program Files\Microsoft SQL Server...	SUCCESS	Options: Op...
5010	1:24:06 PM	explorer.exe:940	QUERY INFORMATION	D:\Program Files\Microsoft SQL Server...	SUCCESS	Length: 983...
5011	1:24:06 PM	explorer.exe:940	CLOSE	D:\Program Files\Microsoft SQL Server...	SUCCESS	

3.2.7 Regmon Enterprise Edition

Regmon se utiliza para diagnosticar problemas asociados con actividades del registro de Windows de cualquier computadora de una red, brindando información en tiempo real de actividades de registro del sistema remoto.

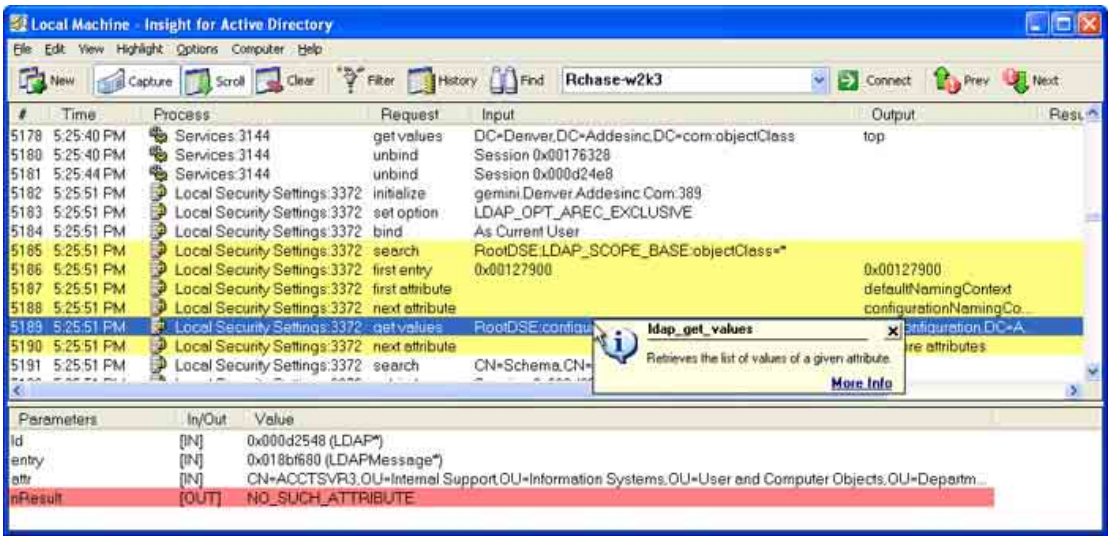
3.2.8 AD Explorer

Este programa tiene la función de permitirnos encontrar, modificar, agregar y borrar objetos y atributos de Active Directory.



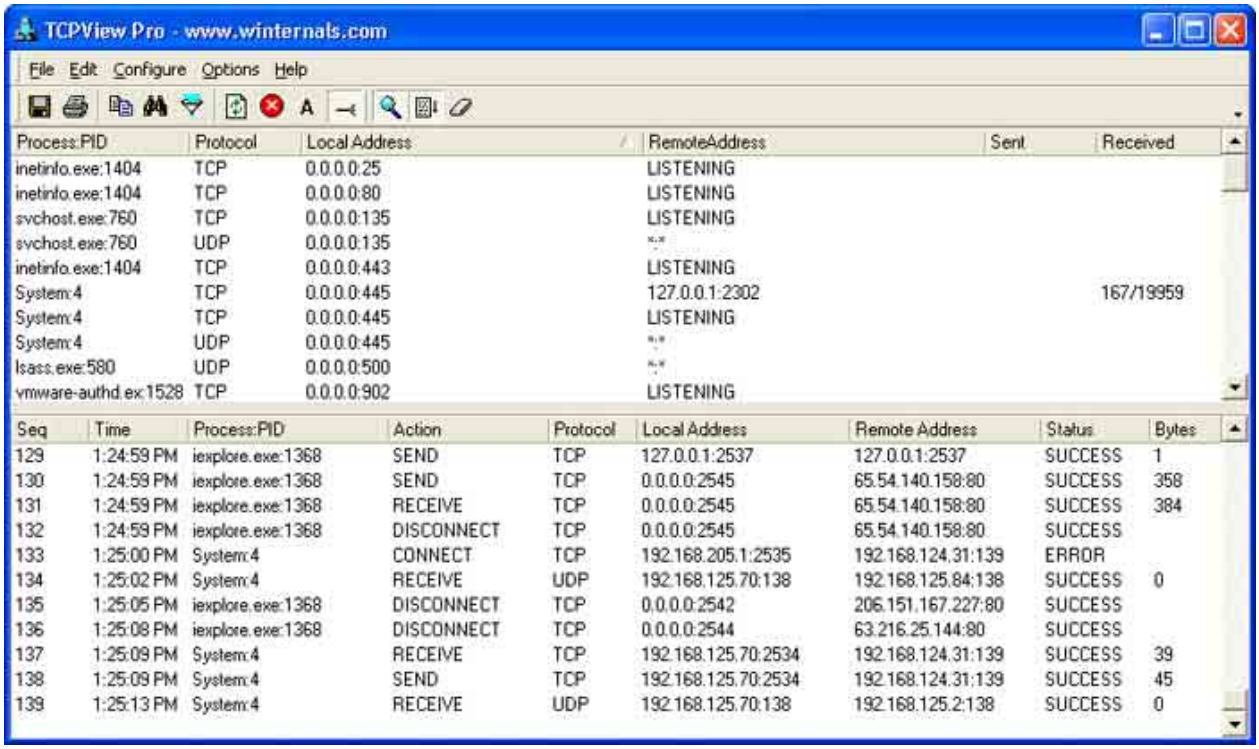
3.2.9 Insight for Active Directory

Insight for Active Directory se usa para identificar conflictos que ocurran en aplicaciones de misión critica tales como servidores de e-mail, y bases de datos, proveyendo de información en tiempo real de las actividades internas y transacciones que se realizan dentro de Active Directory en la maquina local.



3.2.10 TCP Tools

Esta suite de herramientas incluye TCPView Professional y TCPVstat, herramientas de suma utilidad para diagnóstico y seguimiento de errores en redes TCP/IP. TCP Tools brinda información de actividad, procesos y configuración de toda una red basada en estos protocolos.



Sitio web del fabricante: www.winternals.com

3.3 R-STUDIO

R-Studio es una familia de programas muy poderosos y efectivos para la recuperación de datos que utiliza las más modernas tecnologías. Permite recuperar información de sistemas de archivos FreeBSD/OpenBSD/NetBSD, de particiones FAT12/16/32, NTFS, NTFS5 (creado o modificado por Windows 2000/XP/2003), volúmenes Ext2FS / Ext3FS y UFS1 / UFS2. Funciona sobre discos locales y unidades accesibles a través de la red.

Características de **R-Studio**:

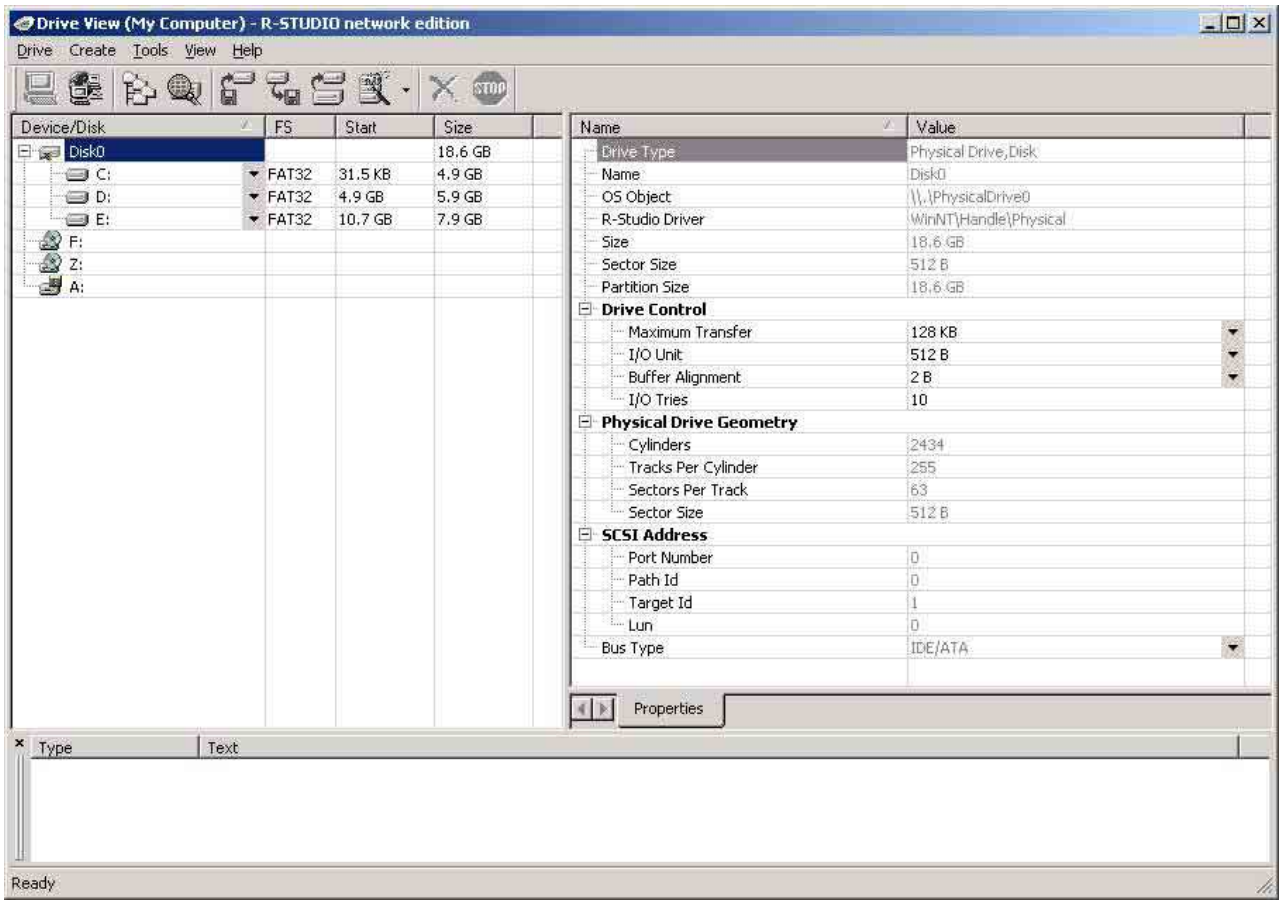
- Trabaja sobre sistemas operativos: Win9x, Me, NT, 2000, XP y 2003 Server.
- Recupera datos en equipos de la red con sistemas Win95/98/ME/NT/2000/XP/2003, Linux y UNIX.
- Reconoce y analiza discos dinámicos (Windows 2000/XP/2003), Básicos y BSD (Unix).

- Recupera datos desde volúmenes RAID dañados.
- Crea archivos Imagen de unidades de disco, particiones o segmentos de las mismas para luego poder ser analizadas como discos convencionales.
- Recupera desde particiones borradas, dañadas y encriptadas (NTFS 5).
- Recobra información borrada y eliminada de la papelera de reciclaje, perdida por ataques de virus o fallas de energía.
- Recompone datos luego de formateos, aun aquellos realizados con diferente sistema de archivos.
- Puede salvar la información recuperada en cualquier unidad accesible por el sistema operativo (incluidas unidades de red).
- El disco o su contenido puede ser visualizado y editado mediante el editor hexadecimal.

R-studio posee dos modos de operación:

Open drive files: realiza una búsqueda sobre particiones válidas o reconocidas de una unidad de disco, analizando la MFT en particiones NTFS y las tablas FAT en particiones FAT. Luego de la búsqueda se muestra una lista con registros encontrados en las tablas. Los archivos borrados recientemente pueden recuperarse inmediatamente. En el caso de no hallarse la información buscada el disco deberá ser escaneado (**Disk Scan**).

Disk Scan: Este modo se utiliza para recuperar información de particiones perdidas, dañadas, formateadas o corruptas. R-Studio realiza un escaneo de la superficie del disco intentando reconocer estructuras de datos válidas. Luego de la búsqueda el programa muestra una lista de particiones encontradas (tener en cuenta que en el caso de discos reformateados pueden aparecer mas de una partición encontrada).



Sitio web del fabricante: www.r-studio.com

NOTAS