

UF5-Manteniment d'equips microinformàtics.

NF1-Manteniment d'equips microinformàtics.

NF1.1 Manteniment del maquinari.

>> **NF1.2 Salvaguarda i recuperació de la informació.**

NF1.3 Malware: Virus i altres amenaces de seguretat.

Introducció

- Les dades dels sistemes informàtics estan sotmeses a perills de tot tipus.
 - **Amenaces de seguretat física**
 - Fallades del subministrament elèctric
 - Inclemències meteorològiques (inundacions, desastres naturals, etc.)
 - Fallada dispositius d'enmagatzematge
 - Fallades del sistema d'aire condicionat
 - Incendis
 - Accés no autoritzat (hacker, cracker, ...).
 - Errors humans

Introducció

– Atacs informàtics

- Suplantació d'identitat (spoofing)
- Denegació de serveis
- Enginyeria social
- Explotació de vulnerabilitat informàtica
- Programes nocius

– Programes nocius (els veurem més endavant)

- Virus
- Troià (Trojan horses)
- Cuc (Worms)
- Programari espia (Spyware)
- Porta falsa (Backdoors)
- Programes salami o tècnica del salami
- Bomba lògica

Còpies de seguretat o backups

- Una còpia de seguretat (backup en anglès) fa referència a la còpia d'informació que es realitza per tal de ser restaurada en cas de pèrdua de dades o en cas de ser requerida en posterioritat.
- Les còpies de seguretat han esdevingut una part crítica de la planificació informàtica de les empreses i més concretament de la seva política de seguretat i és una de les principals mesures que s'adopten per a protegir-se d'incidents de seguretat informàtica.



ALGUNS DRETS RESERVATS.

Joan Coll i Teixidor
Marc Nicolau i Reixach

Còpies de seguretat o backups

- Les còpies es solen fer amb mitjans d'emmagatzemament extraïbles que poden guardar-se físicament separats dels ordinadors on es realitzen les còpies (discos durs externs, CD-ROMs, cintes magnètiques DAT, etc).
- Tot i així, cada cop s'utilitzen més -especialment en grans servidors i empreses- sistemes de còpia de seguretat remota que realitzen les còpies de forma automàtica a través de la xarxa en servidors de la mateixa organització o mitjançant una empresa externa.



ALGUNS DRETS RESERVATS.

Joan Coll i Teixidor
Marc Nicolau i Reixach

Tipus de còpia

- Còpia de seguretat de sistema
 - Té com a objectiu poder rearrencar un sistema després d'un incident de seguretat i per tant realitzen una còpia dels fitxers del sistema operatiu i del programari instal·lat. La restauració d'aquest tipus de còpia permet tornar a tenir un ordinador en funcionament després d'un desastre.
- Còpia de seguretat de dades
 - Sols preté recuperar informació i realitza còpies de fitxers de dades o bases de dades.
- Còpia imatge
 - Copia tot el disc tan si són fitxers de sistema com de dades.
- Les petites còpies d'usuari es poden fer manualment amb l'ús de copiar/enganxar a un disc extern, amb còpia a CD/DVD, amb l'ajut de compressors d'arxius però per empreses s'utilitza programari i maquinari dedicat a còpies de seguretat o backup

Què s'hauria de copiar?

- Totes les dades que ens siguin imprescindibles, sobretot els que generen els usuaris (documents de text, fulls de càlcul, bases de dades, fotografies...). En el cas d'arxius multimèdia, és ideal copiar-los en CD o DVD i eliminar del disc dur els que no s'utilitzen habitualment.
- També hem de fer còpies de seguretat del correu electrònic i dels contactes.
- És molt important que fem còpia de seguretat dels CD's de sistema operatiu (ens els portàtils nous pot estar en una partició) i dels drivers, tant de la placa mare com d'altres perifèrics.
 - No solen ser necessàries còpies de seguretat d'instal·ladors de programes opensource o gratuïts que estiguin canviant de versió cada poc temps i es puguin descarregar per Internet.
 - Tampoc no ens serveix fer còpies de programes ja instal·lats ja que és probable que els haguem de reinstal·lar però sí que hauriem de fer còpia de les dades generades amb aquests programes.

Models de còpies de seguretat professionals

- 1) Còpia de seguretat completa (full backup)
 - Realitza una còpia de tots els fitxers seleccionats i es sol fer sobre conjunts molt grans d'arxius.
 - Cada vegada que es realitza comença un cicle de còpies de seguretat que no finalitzarà fins que es realitzi una altra còpia completa dels arxius.
- 2) Còpia de seguretat diferencial (differential backup)
 - Es copien exclusivament aquells fitxers que han sofert canvis des de la còpia de seguretat completa; sempre copia si hi ha hagut canvis en la còpia completa, de tal manera que cada vegada que es faci aquesta còpia diferencial es copiaran els fitxers modificats des de la completa, encara que s'haguessin copiat en una diferencial anterior.
- 3) Còpia de seguretat incremental o progressiva (incremental backup)
 - La primera vegada que s'executa copia les diferències respecte a la còpia completa, les altres vegades només copia les modificacions existents des de la darrera còpia progressiva.

Estratègies per triar el model de còpia de seguretat

- El backup incremental és el backup més ràpid i requereix el mínim espai en el suport d'emmagatzematge. No obstant, els backups incrementals també requereixen el temps més llarg i més suports per restaurar.
- Els backups incrementals s'haurien d'utilitzar només en entorns on els temps de backup o el suport d'emmagatzematge sigui molt limitat. **Per molts entorns, un backup complet setmanal i un backup diferencial diari són una bona opció.**
 - Exemple:
 - Si es fa un backup complet el diumenge, amb backups incrementals cada nit i el sistema cau el dijous, necessitarem restaurar el backup complet de diumenge amb els backups incrementals de dilluns, dimarts i dimecres.
 - En canvi, si fem un backup complet el diumenge i una còpia diferencial cada nit, quan el sistema caigui en dijous, només haurem de restaurar el backup complet de diumenge i només la còpia diferencial de dimecres.

Planificació de les còpies de seguretat

- Per tal de decidir quina tecnologia s'utilitza per a les còpies de seguretat caldrà tenir en compte:
 - El volum de dades a copiar
 - El cost econòmic del mitjans d'emmagatzemament utilitzat i s'escau del seu manteniment.
 - L'operativitat de la solució escollida tant pel que fa al temps de còpia com el de recuperació.
- Algunes decisions que s'hauran de prendre seran:
 - La periodicitat i horari de les còpies. Com més alta la freqüència major capacitat de recuperació es tindrà.
 - El número de còpies. Si es realitza més d'una còpia i aquestes desen en ubicacions separades s'augmentarà la seguretat.
 - La compressió de les dades redueix el volum a copiar, però incrementa el temps de còpia.
 - Sistema de còpia i mitjà d'emmagatzemament.
 - Model de còpia: Còpia completa, diferencial o incremental.

Precaucions

- Hem d'evitar sobre escriure una còpia de seguretat amb una altra ja que en el cas de que necessitessim recuperar un arxiu és necessari que estiguem segurs que tenim una còpia neta d'aquest arxiu. Si guardem diferents còpies en un CD haurien d'estar en carpetes diferents.
- No s'han de fer còpies en el mateix disc dur (encara que siguin particions diferents). Si es fa malbé el disc dur no servirà de res ja que no podrem accedir a les còpies.
- Encara que tinguem un sistema RAID 1 (discs durs miralls) cal fer una còpia de seguretat de les dades, ja que si un arxiu es corrompeix, el modifiquem, eliminem o s'infecta, estarà en el mateix estat en els dos discos. Un sistema RAID ens garanteix la integritat (depenent del tipus de RAID) de les dades davant una errada del disc però no dels altres supòsits.
- Per què siguin útils, les còpies de seguretat han d'estar correctament etiquetades. Hem d'etiquetar de forma clara la data i l'hora d'aquestes còpies.

Precaucions

- S'hauria de considerar que la substitució d'equips pot ser més o menys costosa, però es totalment factible en curt temps , ja que per una empresa és molt més important la informació que tenen els equips que els mateixos equips.
- La normativa de la Llei de protecció de dades estableix que s'han de guardar còpies de seguretat en llocs diferents que no estigui a la mateixa empresa (perill catàstrofes). En el cas d'empreses amb diferents seus interconnectades (per una VPN, per exemple) una bona solució podria ser que cada centre faci una còpia de seguretat externa. També es poden contractar serveis externs
- Per la normativa també és molt important la confidencialitat de les dades. Per això les còpies de seguretat s'haurien de guardar en llocs segurs, destruint els suports cada cert temps (en el cas de CD's o DVD's). Existien màquines específiques per això. També es poden encriptar les dades o protegir els continguts per contrasenya



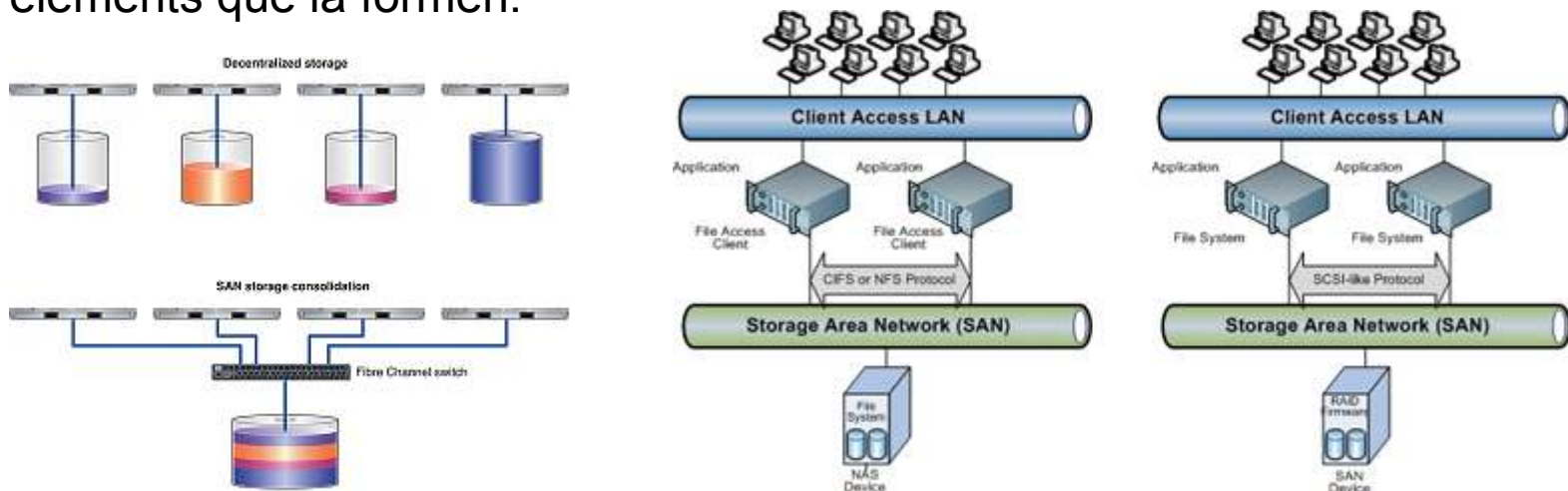
Maquinari per fer còpies de seguretat

- Cintes DLT, LTO, DAT/DDS, S-AIT, VXA
- Discs durs, discs òptics, discs d'estat sòlid (SSD)
- Servidor d'emmagatzematge locals i remots



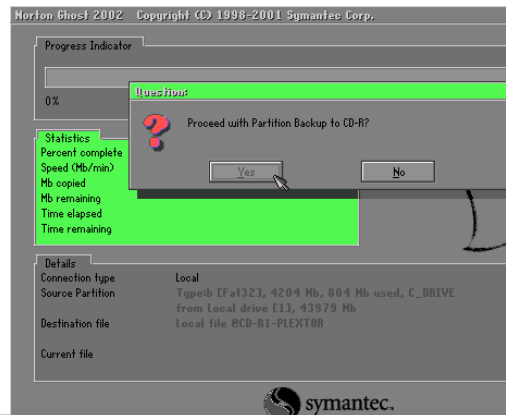
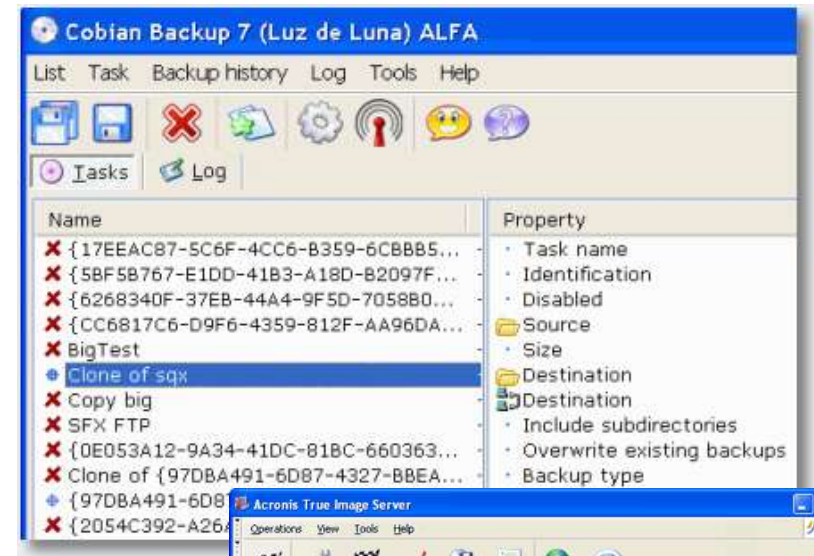
Xarxes d'emmagatzematge

- NAS (Network Attached Storage) és una tecnologia d'emmagatzematge dedicada a compartir la capacitat d'emmagatzematge d'un ordinador (Servidor) amb altres ordinadors personals o servidors clients mitjançant una xarxa (normalment TCP/IP), amb l'ús de NFS, FTP, TFTP...
- SAN (Storage Area Network) o xarxa d'àrea d'emmagatzematge, és una xarxa concebuda per connectar servidors, arrays de discos i llibrerías de suport principalment, sol estar basada en tecnologia iSCSI o fibre channel. La seva funció és la de connectar de forma ràpida, segura i confiables els diferents elements que la formen.



Programari per fer còpies de seguretat

- Opensource
 - Cobian Backup 8
 - Bacula
 - Amanda
 - Partition Image
 - Ghost for Unix (G4U)
- Comercials:
 - Symantec Norton Ghost
 - Symantec Veritas NetBackup
 - Acronis True Image Server
- Freeware
 - HDClone
 - DrivelImage XML



Errors de discs durs

- Síntomes típics errors de disc

Se ha encontrado un problema y windows ha sido apagado para evitar daños al equipo.

KERNEL_DATA_INPAGE_ERROR

Si esta es la primera vez que ve esta pantalla de error de detención, reinicie su equipo. Si esta pantalla aparece otra vez, siga los siguientes pasos:

Compruebe que cualquier hardware o software está correctamente instalado. Si es una nueva instalación, contacte con su proveedor de hardware o software para obtener actualizaciones de windows que pueda necesitar.

Si los problemas continúan, deshabilite o elimine cualquier nuevo hardware o software instalado. Deshabilite las opciones de memoria de la BIOS como caché o vigilancia. Si necesita utilizar el modo a prueba de errores para quitar o deshabilitar componentes, reinicie su equipo, presione F8 para seleccionar opciones de inicio avanzadas y, a continuación, seleccione modo a prueba de errores.

Información técnica:

*** STOP: 0x0000007A (0xC03D0CF98, 0xC000000E, 0xF73E63B4, 0x1686C860)

*** atapi.sys - Address F73E63B4 base at F73D9000, DateStamp 41107b4d

Empezando el volcado de memoria física
Descarga de memoria física completa.
Póngase en contacto con su administrador de sistema o grupo de soporte técnico para obtener

Pri Master Hard Disk:S.M.A.R.T. Status BAD, Backup and Replace
Press <F4> to Resume

Se ha encontrado un problema y windows ha sido apagado para evitar daños al equipo.

KERNEL_DATA_INPAGE_ERROR

The screenshot shows the Windows XP Event Viewer. The left pane displays a list of events, including several 'Information' events and one 'Error' event from the 'ntfs' source. The right pane shows the 'Properties of Event' dialog for the selected error event, dated 15/11/2006 at 10:47:46. The event type is 'Error' and the source is 'ntfs'. The description states: 'La estructura del archivo sistema en el disco está dañada e inutilizable. Ejecute el programa chkdsk en el volumen C:.' (The file system structure on the disk is damaged and unusable. Run the chkdsk program on the volume C:.)

Evento	Fecha	Hora	Origen	Id. suceso
Información	15/11/2006	10:47:53	Service Control Manager	Nir
Error	15/11/2006	10:47:46	ntfs	Dis
Información	15/11/2006	10:47:44	Service Control Manager	Nir
Información	15/11/2006	10:47:38	Service Control Manager	Nir
Información	15/11/2006			
Información	15/11/2006			
Información	15/11/2006			
Información	15/11/2006			
Información	15/11/2006			
Información	15/11/2006			
Información	15/11/2006			
Información	15/11/2006			
Información	15/11/2006			
Información	15/11/2006			
Información	15/11/2006			

Propiedades de Suceso

Suceso:

Fecha: 15/11/2006 Origen: ntfs

Hora: 10:47:46 Categoría: Disco

Tipo: Error Id. suceso: 55

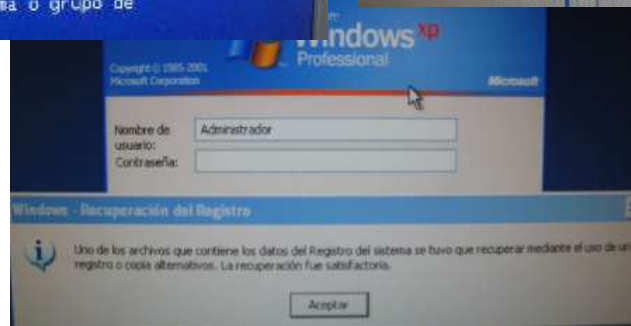
Usuario: No disponible

Equipo: ASTERDC

Descripción:

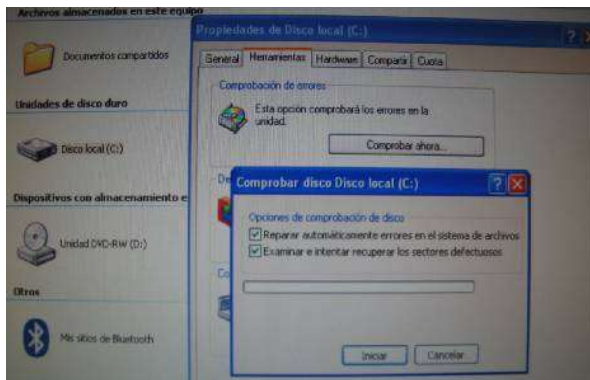
La estructura del archivo sistema en el disco está dañada e inutilizable. Ejecute el programa chkdsk en el volumen C:.

Para obtener más información, vea el Centro de ayuda y soporte técnico en <http://go.microsoft.com/fwlink/events.asp>



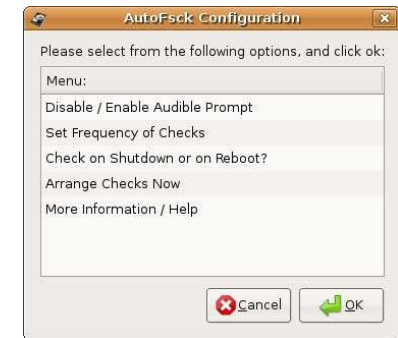
Programari per recuperar discs durs

- Si hi ha errors en el disc dur existeix programari del sistema per intentar recuperar informació.
 - CHKDSK (Errors fixers Windows)
 - FIXMBR (arranc Master Boot Record-MBR Windows)
 - fsck (Linux)



necesita ser comprobado para ver coherencias. Se
comprobación de disco, pero se recomienda
windows comprobará ahora el disco.

```
CHKDSK está comprobando archivos (etapa 1 de 5)...  
Comprobación de archivos terminada.  
CHKDSK está comprobando índices (etapa 2 de 5)...  
Eliminando la entrada hidphone.tsp, en el índice $I30 del archivo 29.  
Eliminando la entrada hnetcfg.dll, en el índice $I30 del archivo 29.  
Eliminando la entrada KB896358, en el índice $I30 del archivo 11340.  
Eliminando la entrada update.ver, en el índice $I30 del archivo 11466.  
Eliminando la entrada time.h, en el índice $I30 del archivo 36754.  
Comprobación de índices terminada.  
CHKDSK está recuperando archivos perdidos.  
CHKDSK está comprobando descriptores de seguridad (etapa 3 de 5)...  
Comprobación de descriptores de seguridad terminada.  
CHKDSK está comprobando los datos de archivo (etapa 4 de 5)...  
Windows ha reemplazado clústeres dañados en el archivo $I82  
de nombre \DOCUME~1\LOCALS~1\NTUSER.DAT.
```



FIXMBR sólo se admite en equipos basados en x86.

```
C:\WINDOWS>fixmbr
```

```
** ADVERTENCIA **
```

Este equipo parece tener un registro de inicio principal
no estándar o no válido.

FIXMBR puede dañar sus tablas de particiones si continúa.

Esto podría ocasionar que todas las particiones del
disco duro actual queden inaccesibles.

Si no tiene problemas para obtener acceso a su unidad,
no continúe.

¿Está seguro de que quiere escribir un nuevo registro de arranque (MBR)? s
Escribiendo el nuevo registro de arranque (MBR) en la unidad física
\\Device\\Harddisk0\\Partition0.

Se ha escrito correctamente el nuevo registro de inicio principal.

Programari per recuperar discs durs

- Si el programari del sistema no és suficient o per error es formata o borren fitxers, existeix programari específic per intentar recuperar informació.
 - RecoverMyFiles
 - HD Tune
 - Handy Recovery
 - SeaTools (Seagate)
 - Grescue (Linux)

ST3120022A (120 GB)

35 °C

Benchmark Info Health Error Scan

Start

Quick Scan

Legend:

- 45 MB
- Ok
- Damaged

Damaged Blocks: 0

Scanning Speed: 30.3 MB/s

Searching Lost Partitions

Time elapsed: 01:17
Time left: 54:38
Position: 875 Mb

Found partitions:

- NTFS(7.9MB - 22.6GB) size: 22.6GB (cluster: 4096)
- NTFS(22.6GB - 37.3GB) size: 14.6GB (cluster: 4096)
- NTFS(37.3GB - 52.0GB) size: 14.6GB (cluster: 4096)
- FAT32(0.2GB - 1.2GB) size: 1.0GB (cluster: 1024)
- FAT16(0.3GB - 0.3GB) size: 0.1GB (cluster: 4096)
- FAT32(0.3GB - 1.2GB) size: 1.0GB (cluster: 1024)

You can select these partitions from the list in the left program window and recover files from them.

Save partitions info

Stop

Verificación de disco

Resultados de la comprobación:

Ejecutar: 15/11/2009 10:00:00

Master principal: ST3120022A
Modelo: 3J52M9C0
Número de serie: 120.0 GBytes
Capacidad: 120.0 GBytes

Resultado de la comprobación: Rutina de autocomprobación completada con un error de alerta S.M.A.R.T.

Cualquier unidad que informe sobre la existencia de un error S.M.A.R.T. puede fallar en cualquier momento. Por esta razón, se recomienda realizar una copia de seguridad de los datos almacenados en estas unidades lo antes posible. Si desea obtener más info

Error S.M.A.R.T. detectado

Una de las unidades de disco Seagate ha devuelto una alerta S.M.A.R.T. o no ha podido realizar la autocomprobación.

¿Desea verificar la garantía y obtener un número de devolución RMA en línea?

Si No

File Edit Help

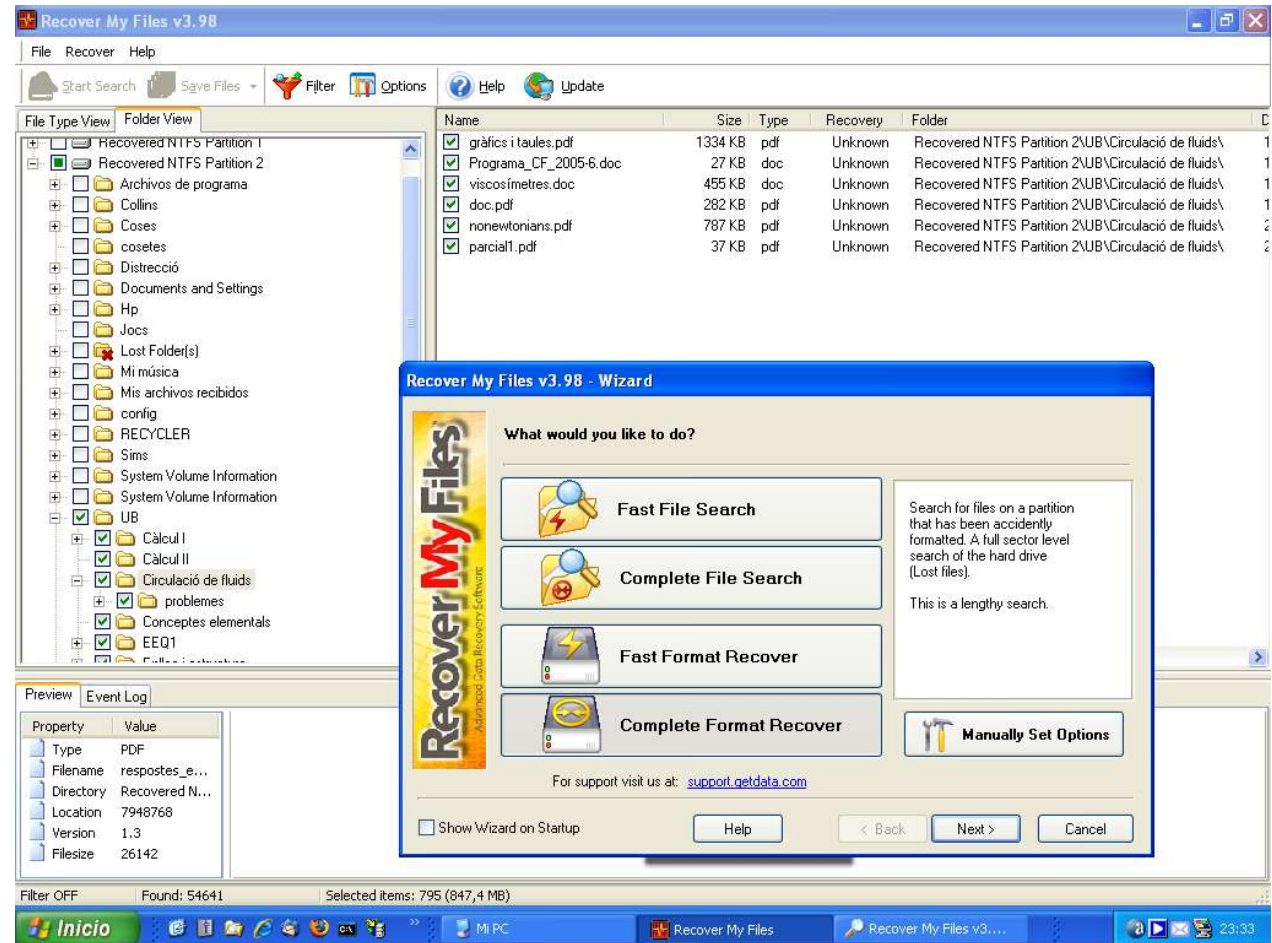
GRescue Started 0.1.1

DEVICE SELECTED : /dev/scd0
DEVICE SELECTED : /dev/sdb1

ID	Current	Worst	Threshold	Data	Status
(01) Raw Read Error Rate	57	53	6	65391972	Ok
(03) Spin Up Time	96	96	0	0	Ok
(04) Start/Stop Count	100	100	20	156	Ok
(05) Reallocated Sector Count	91	91	36	362	Ok
(07) Seek Error Rate	86	60	30	443782	Ok
(09) Power On Hours Count	88	88	0	11273	Ok
(0A) Spin Retry Count	100	100	97	0	Ok
(0C) Power Cycle Count	100	100	20	866	Ok
(C2) Temperature	35	55	0	35	Ok
(C3) Hardware ECC Recovered	57	53	0	65391972	Ok
(C5) Current Pending Sector	100	100	0	52	Ok
(C6) Offline Uncorrectable	100	100	0	52	Ok
(C7) Ultra DMA CRC Error Count	200	194	0	12	Ok
(C8) Write Error Rate	100	253	0	0	Ok
(CA) Unknown attribute	95	249	0	4	Ok

Programari per recuperar discs durs

- RecoverMyFiles



Disc dur recuperat després de l'explosió del Columbia



- Després de tractar els plats amb un producte químic i muntar-lo en un nou disc, es van poder recuperar el 99% de les dades que s'havien gravat en el transbordador Columbia que es va desintegrar el 2003 amb 8 tripulants (no va ser possible en 2 altres discs durs que es van trobar)

