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 metereològiques (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.

Còpies de seguretat o backups

- Les còpies es solen fer amb mitjans d'emmagatzemament extraíbles 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.

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 si 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'enmagatzematge. 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'enmagatzematge 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 sobreescriure 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 corrumpeix, el modifiquem, eliminem o s'infecta, estarà en el mateix estat en els dos discos. Un sistema RAID ens garantitza 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, destruïnt els suports cada cert temps (en el cas de CD's o DVD's). Existen màquines específiques per això. També es poden encriptar les dades o protegir els continguts per contrasenya

Maquinari per fer còpies de seguretat

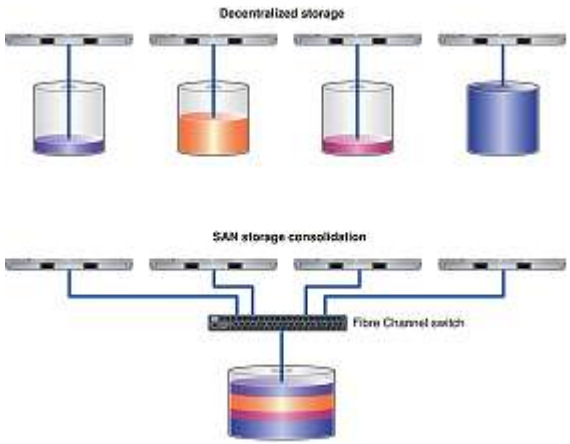
- Cintes DLT, LTO, DAT/DDS, S-AIT, VXA
- Discs durs, discs òptics, discs d'estat sòlid (SSD)
- Servidor d'enmagatzematge locals i remots

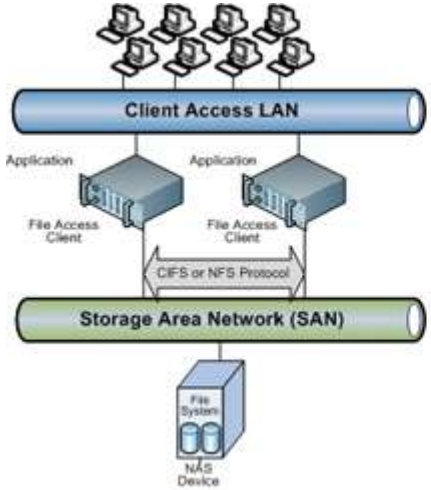


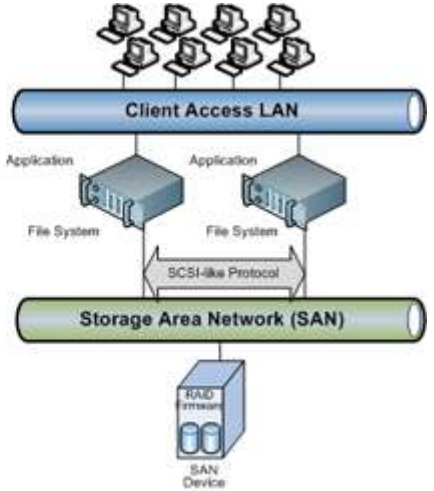



Xarxes d'enmagatzematge

- NAS (Network Attached Storage) és una tecnología d'enmagatzematge dedicada a compartir la capacitat d'enmagatzematge 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.

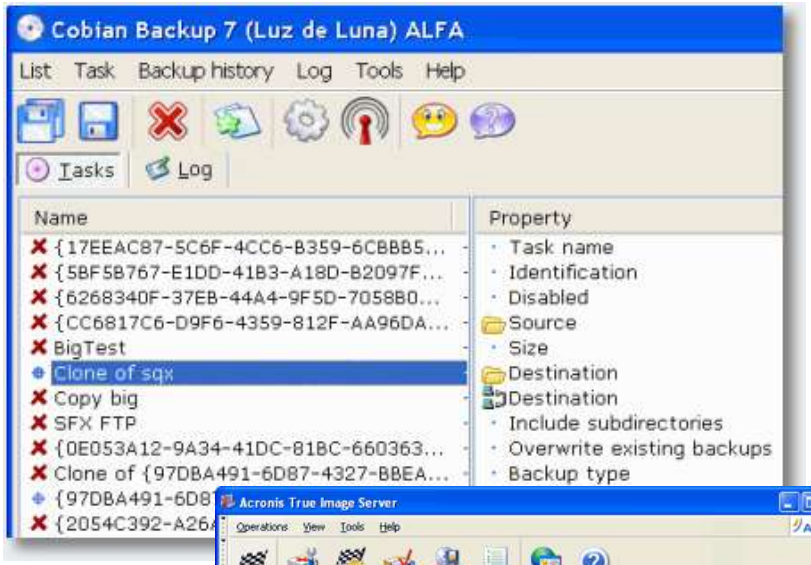


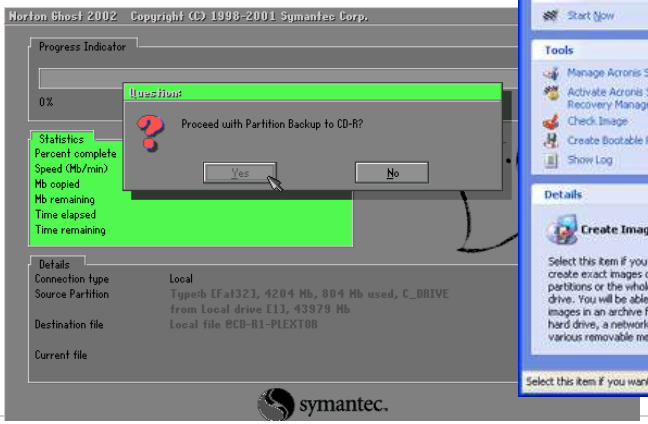




Programari per fer còpies de seguretat

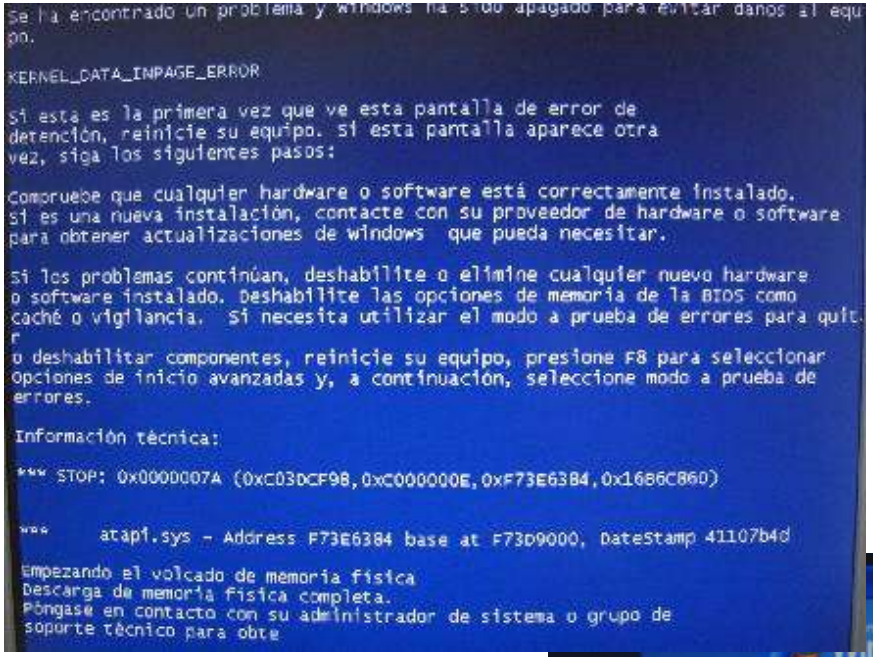
- Opensource
  - Cobian Backup 8
  - Bacula
  - Amanda
  - Partition Image
  - Ghost for Unix (G4U)
- Comercials:
  - Symantec Northon Ghost
  - Symantec Veritas NetBackup
  - Acronis True Image Server
- Freeware
  - HDClone
  - DriveImage XML

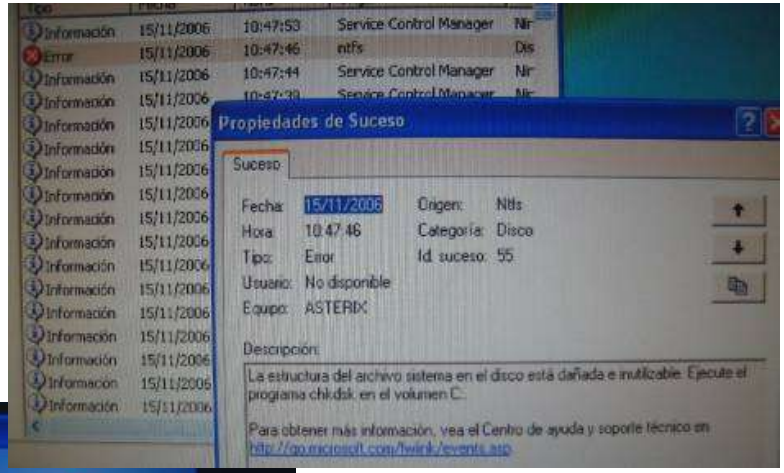




Errors de discs durs

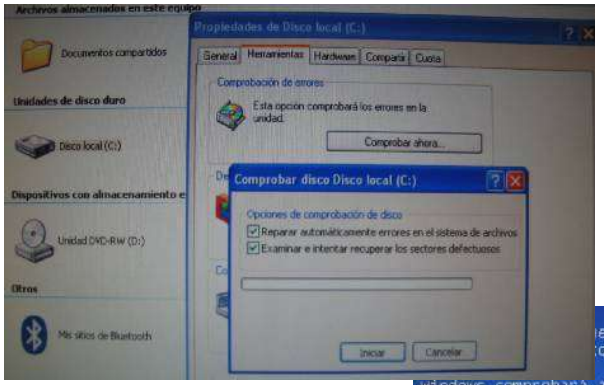
- Símptomes típics errors de disc

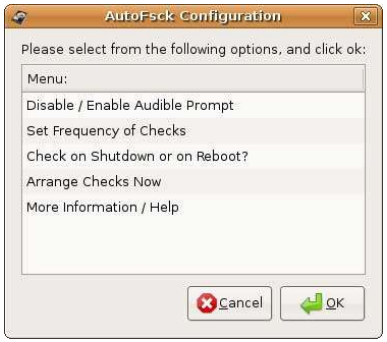


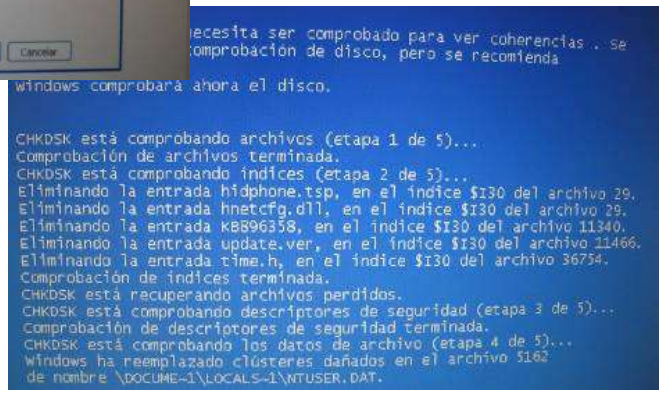


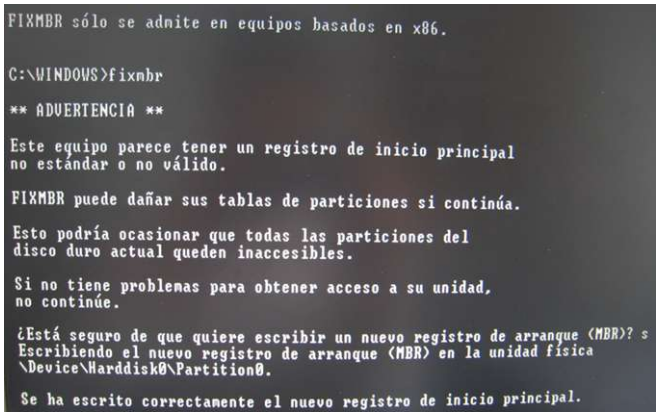
Programari per recuperar discs durs

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



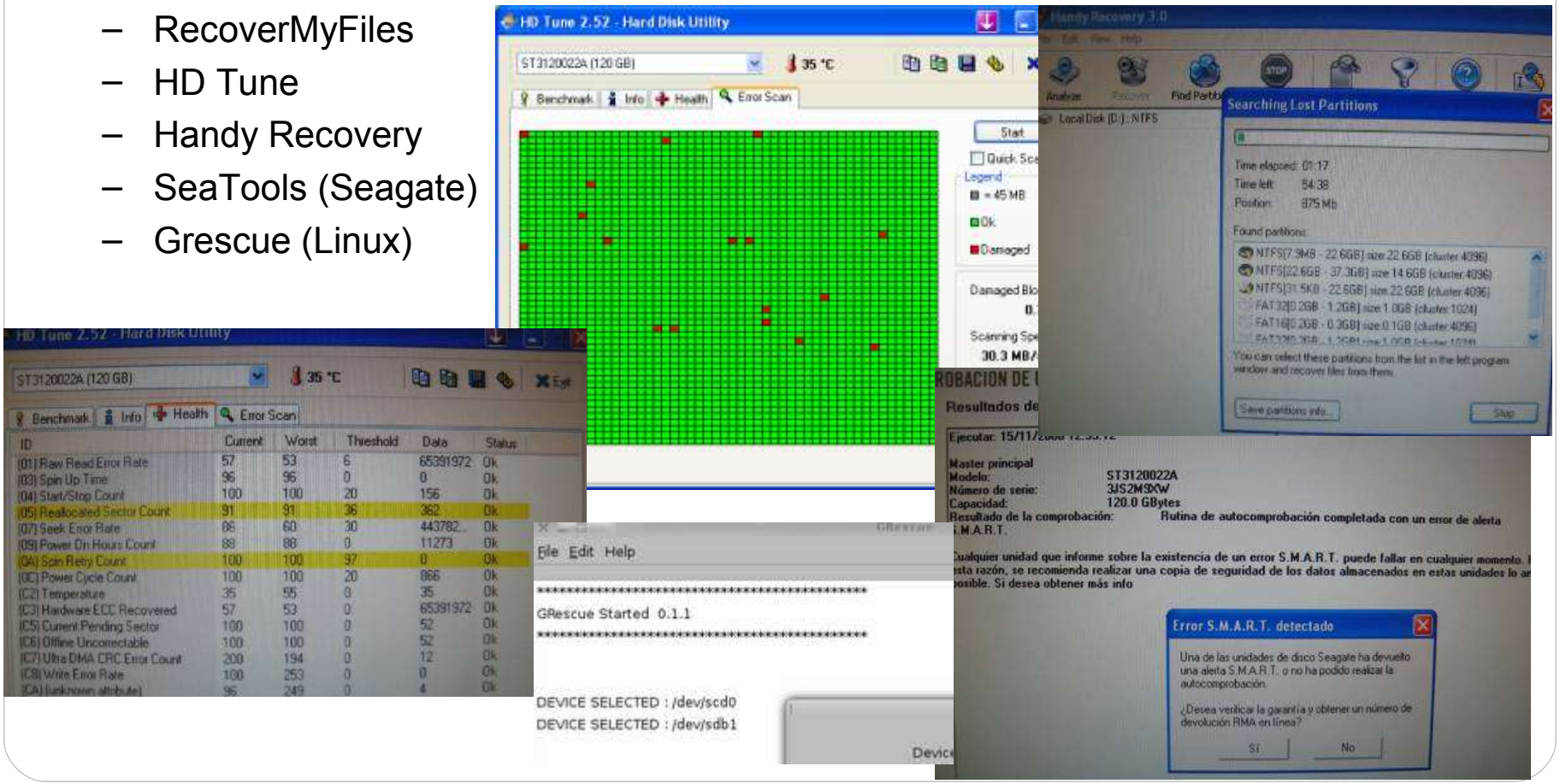






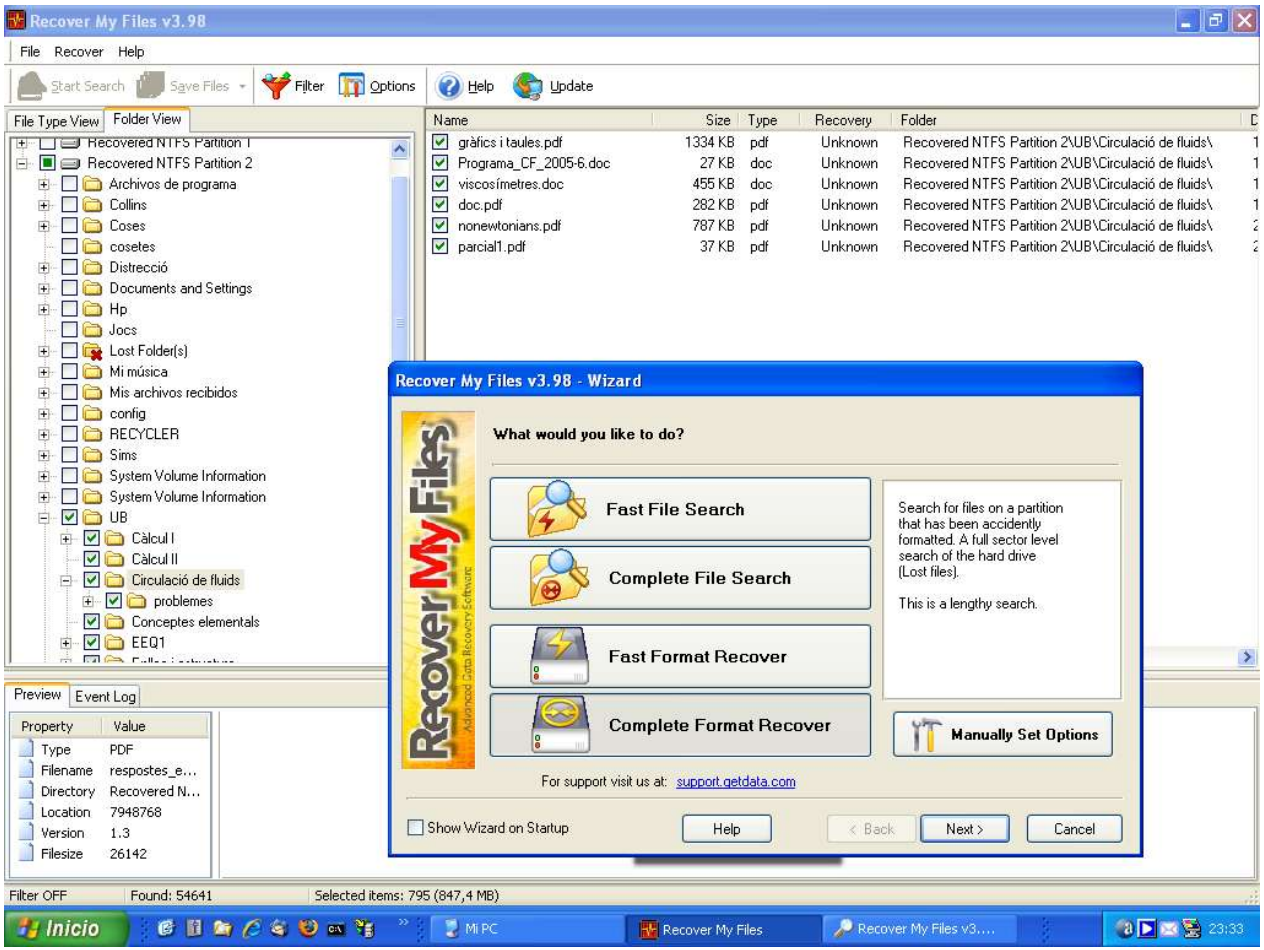
Programari per recuperar discs durs

- 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)



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)