TESTDISK ETAPE PAR ETAPE

http://www.cgsecurity.org/wiki/TestDisk_Etape_par_Etape

Téléchargement :
http://www.cgsecurity.org/wiki/TestDisk_Download

Description du problème

Le disque dur de 36 Go comportait initialement 3 partitions. Malheureusement

- le secteur de boot de la partition NTFS primaire a été endommagé, et
- une partition logique NTFS a été supprimée.

Les étapes pour récupérer une partition FAT32 à la place de la partition NTFS de cet exemple sont absolument identiques.

D'autres exemples de récupération de données sont aussi disponibles. Pour plus d'information sur les FAT12, FAT16, ext2/ext3/ext4, HFS+, ReiserFS et d'autres types de partition, lire Exécuter TestDisk.

Symptômes

Si la partition primaire de ce disque contenait le système d'exploitation, celui-ci ne pourrait plus démarrer à cause de son secteur de boot corrompu. Si ce disque était un disque secondaire (disque de données) ou si vous connectez ce disque sur un autre ordinateur en disque secondaire, les symptômes suivants seraient observés:

1. L'explorateur Windows (`Windows Explorer`) ou le Gestionnaire de disque (`Disk Manager`) affichent la première partition comme *raw* (non formatée) et Windows propose: `Le disque dans le lecteur E: est non formaté, voulez-vous le formater maintenant?`
   [Vous ne devez *jamais* formater le disque si vous voulez récupérer des données]
2. Une partition logique est manquante. Dans l'explorateur Windows, ce volume logique n'est plus visible. Le Gestionnaire de disque de Windows affiche désormais de l'`espace non alloué` là où était la partition.

Lancer TestDisk

Si TestDisk n'est pas encore installé, téléchargez-le depuis Télécharger TestDisk. Extraire les fichiers de l'archive, y compris les sous répertoires.

Pour récupérer des partitions perdues ou réparer un système de fichier d'un disque dur, de clés USB, Smart Card..., vous devez avoir suffisamment de droits pour accéder directement aux périphériques.

- Sous Dos, exécuter `testdisk.exe`

- Sous Windows, exécuter TestDisk (par exemple, `testdisk-6.13/testdisk_win.exe`) depuis un compte dans le groupe Administrateur. Sous Vista, utiliser le clic droit `run as administrator` pour lancer TestDisk.
- Sous Unix/Linux/BSD, vous avez besoin d'être root pour exécuter TestDisk (par exemple, `sudo testdisk-6.13/testdisk_static`)
- Sous MacOSX, si vous n'êtes pas root, TestDisk (par exemple, `testdisk-6.13/testdisk`) va redémarrer lui-même en utilisant sudo après confirmation de votre part.
- Sous OS/2, TestDisk ne gère pas les périphériques physiques, uniquement les images disques, désolé.

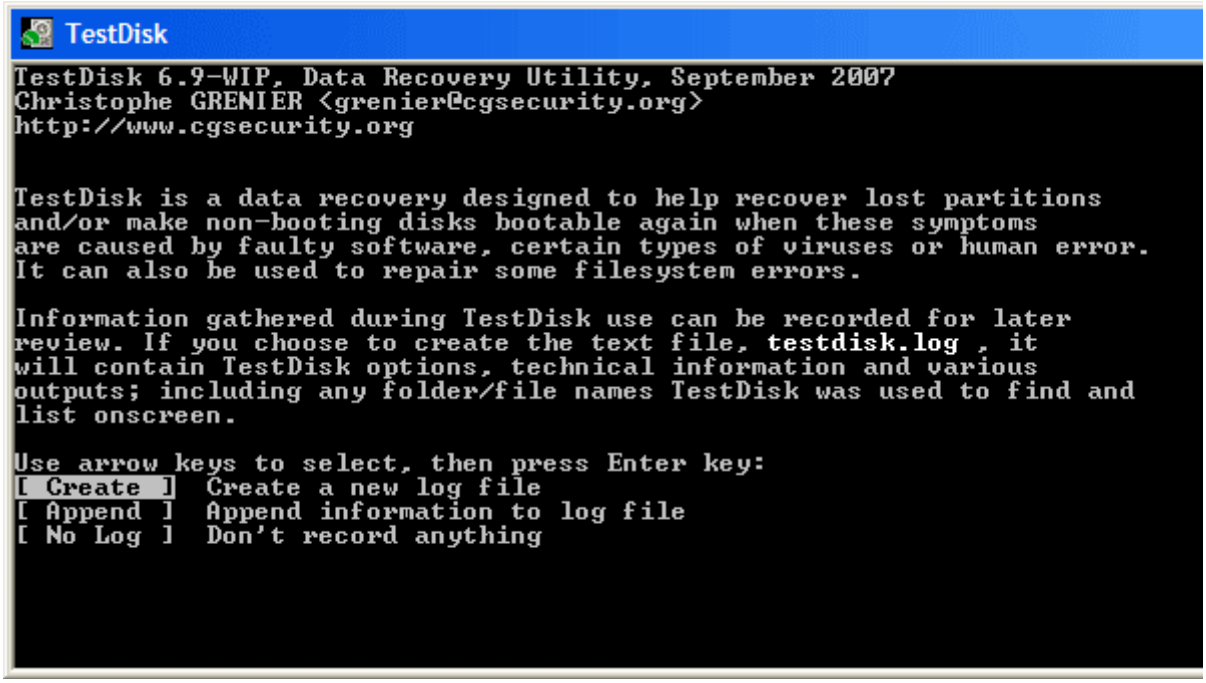
Pour travailler sur une image disque, utiliser

- `testdisk image.dd` pour analyser une image brute d'un disque (`raw image`)
- `testdisk image.E01` pour exploiter une image Encase EWF
- `testdisk 'image.E??'` si l'image Encase est découpée en plusieurs fichiers.

Pour réparer un système de fichier non listé par TestDisk, exécuter `testdisk périphérique`, par exemple:

- `testdisk /dev/mapper/truecrypt0` pour réparer le secteur de boot NTFS ou FAT32 d'une partition TrueCrypt. La même méthode s'applique aussi aux systèmes de fichiers (ext2/ext3/ext4/...) chiffrés par cryptsetup/dm-crypt/LUKS.
- `testdisk /dev/md0` pour réparer un système de fichiers utilisant un RAID logiciel sous Linux.

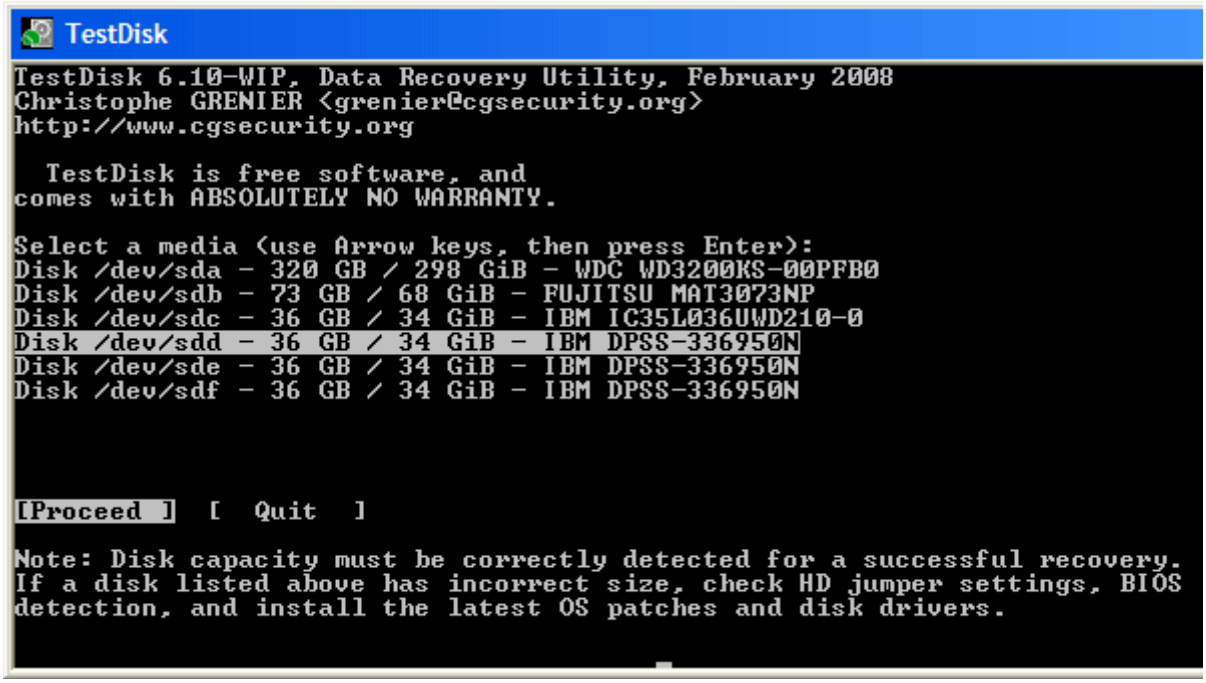
Creation d'un log



- Choisir Create pour créer un fichier log contenant diverses informations techniques et résultats produits par TestDisk. S'il existait, le fichier sera écrasé.
- Append permet d'ajouter au fichier log les résultats de l'opération courante aux résultats précédents.
- None: aucun log n'est créé, utile si vous utilisez TestDisk depuis un média en lecture seule (CD, DVD...) et que vous n'avez nulle part où créer ce fichier.
- Appuyer sur la touche Entrée pour continuer.

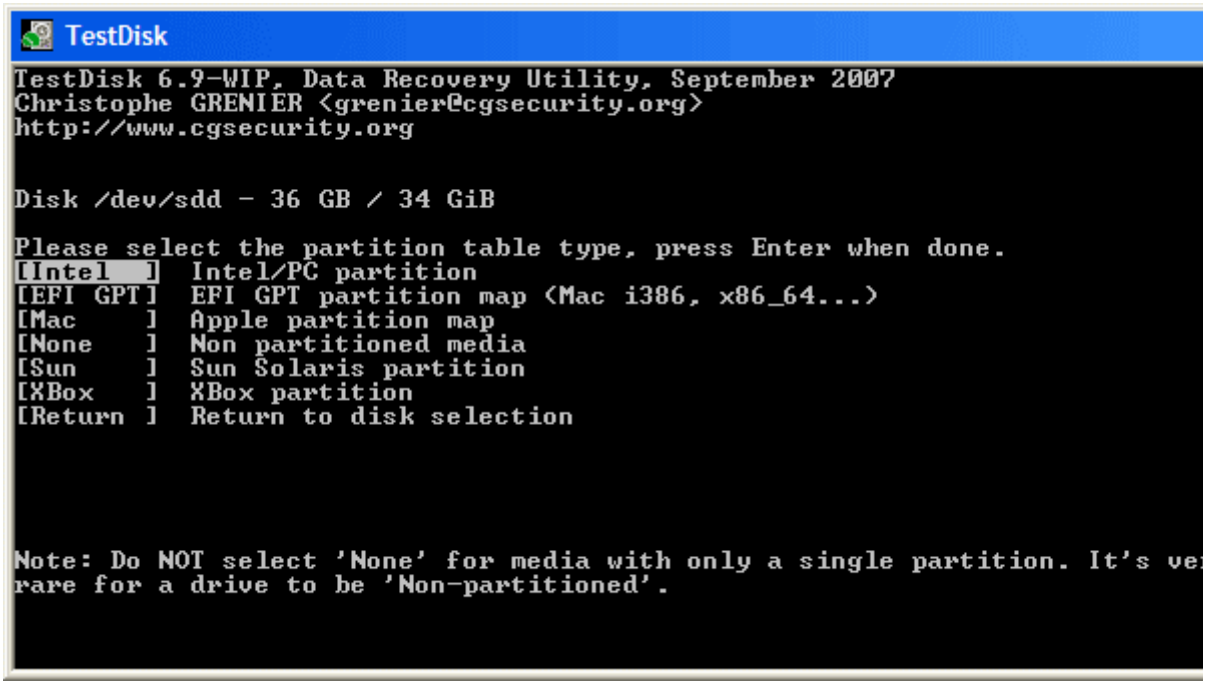
Sélection du disque

Tous les médias (disque dur, CD-ROM...) doivent être détectés par TestDisk et listés avec la bonne capacité:



- Utiliser les touches fléchées haut/bas pour sélectionner le disque avec les partitions perdues ou un système de fichier endommagé.
- Appuyer sur la touche Entrée pour continuer.

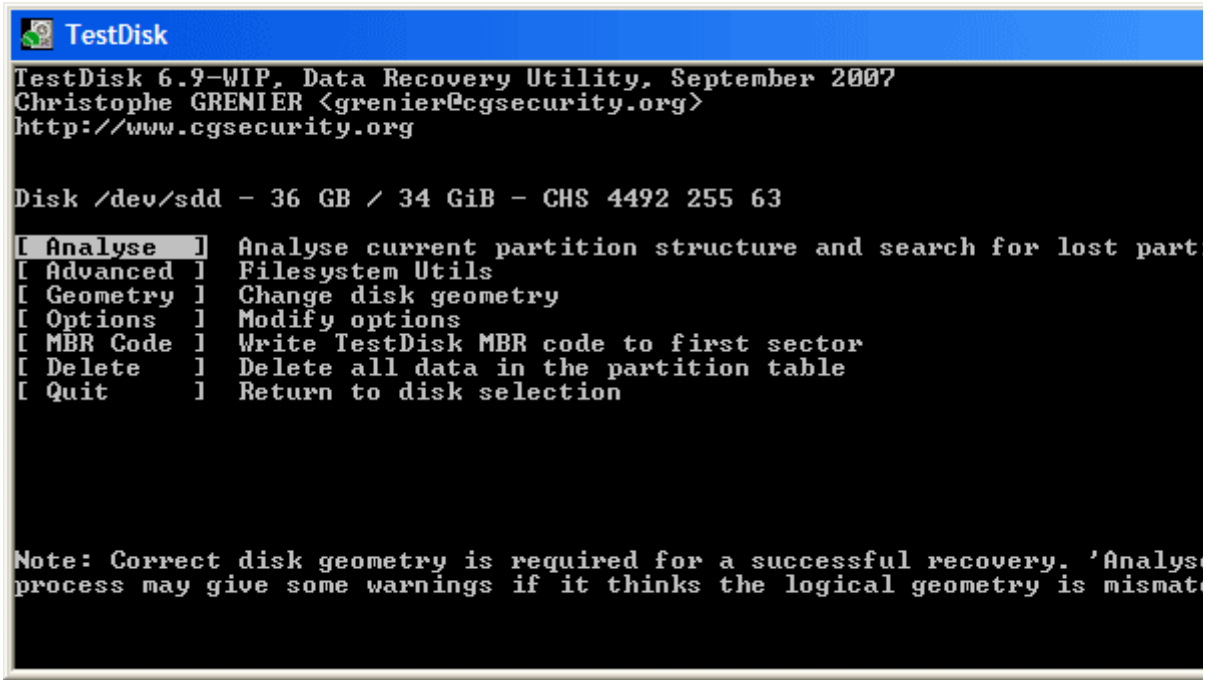
Sélection du type de la table des partitions



Sélectionner le type de la table des partitions, en principe la valeur par défaut est la bonne, car TestDisk effectue une auto détection.

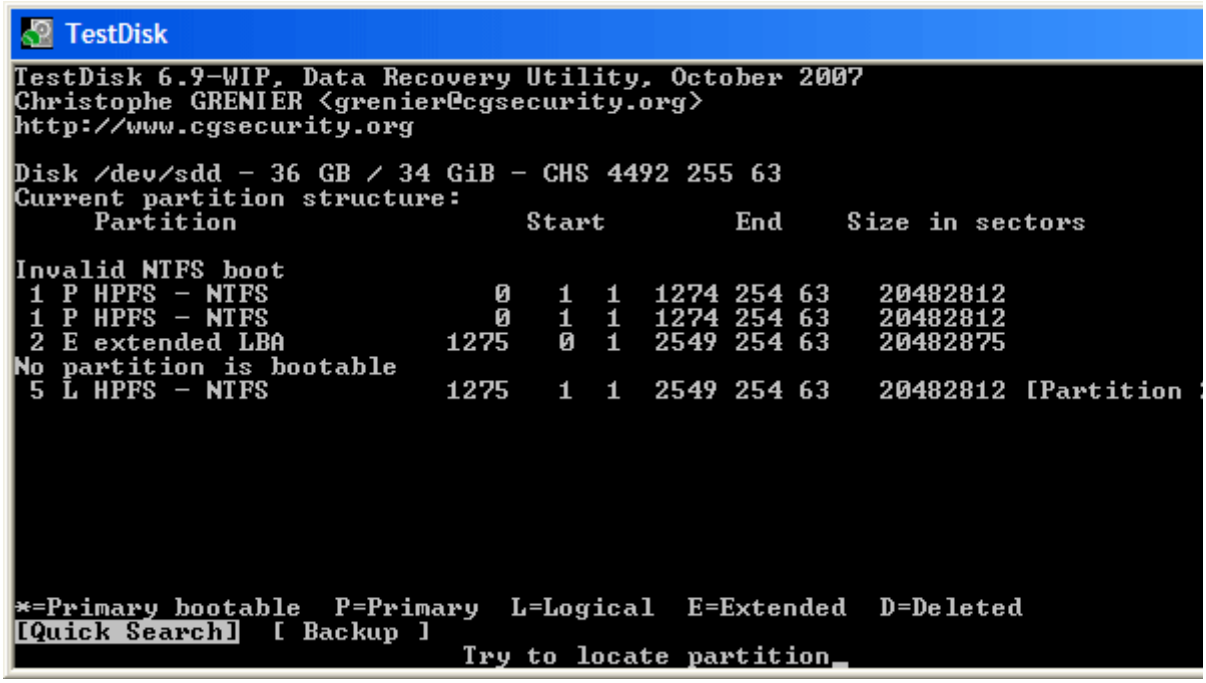
Etat de la table des partitions

TestDisk affiche un menu: (voir le détail du menu de TestDisk).



- Sélectionner le menu Analyse (menu par défaut) et appuyer sur la touche Entrée pour vérifier la structure de la table des partitions.

Le contenu de la table des partitions est affiché. Remarquez que les partitions effacées sont absentes de cette liste, des problèmes peuvent être signalés.



La première partition est listée deux fois ce qui indique que le système de fichier est corrompu ou que l'entrée de table de partition est invalide,
`Invalid NTFS boot` indique plus clairement que le secteur de boot NTFS est défectueux, il s'agit donc d'un système de fichier corrompu.
Seule une partition logique nommée Partition 2 est présente dans la partition étendue, une partition logique est donc manquante.

- Confirmer avec ***Quick Search*** pour continuer.

Recherche rapide des partitions

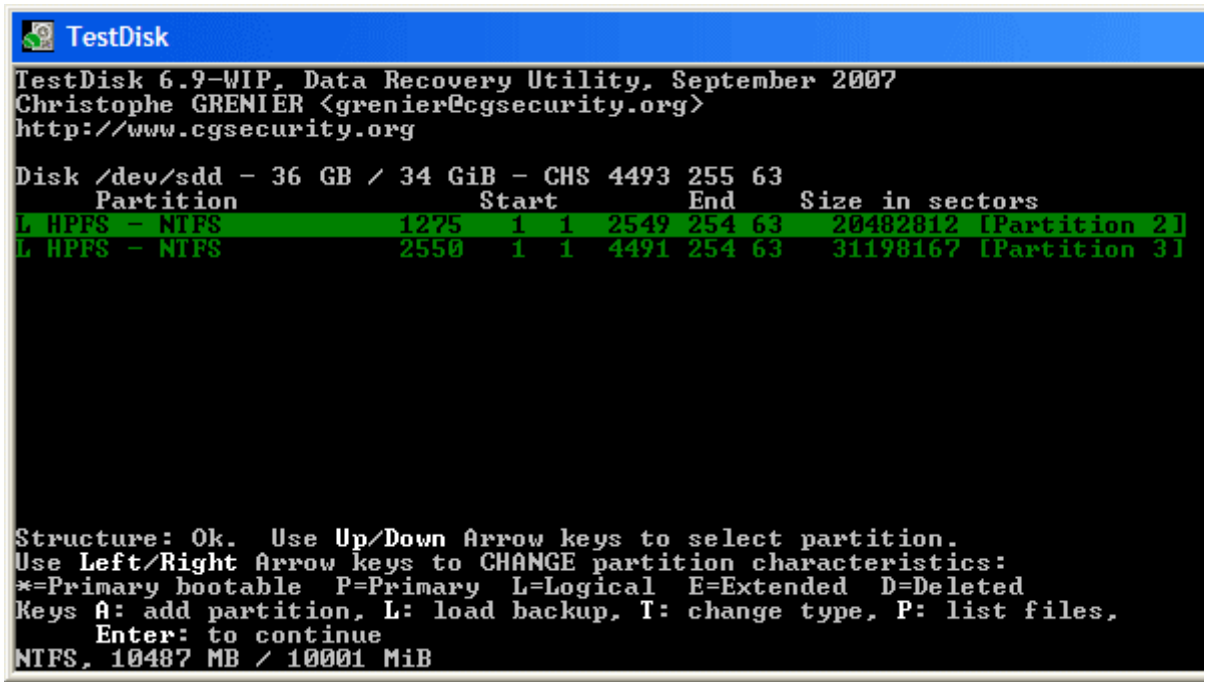
---

vista check

- Si des partitions ont été créées sous Windows Vista ou en cas de doute, répondez par `y` pour confirmer.

TestDisk affiche les premiers résultats en temps réel.  (cliquer sur la miniature pour agrandir l'image).

Durant la recherche rapide, TestDisk retrouve deux partitions dont la partition manquante nommée ***`Partition 3`***.

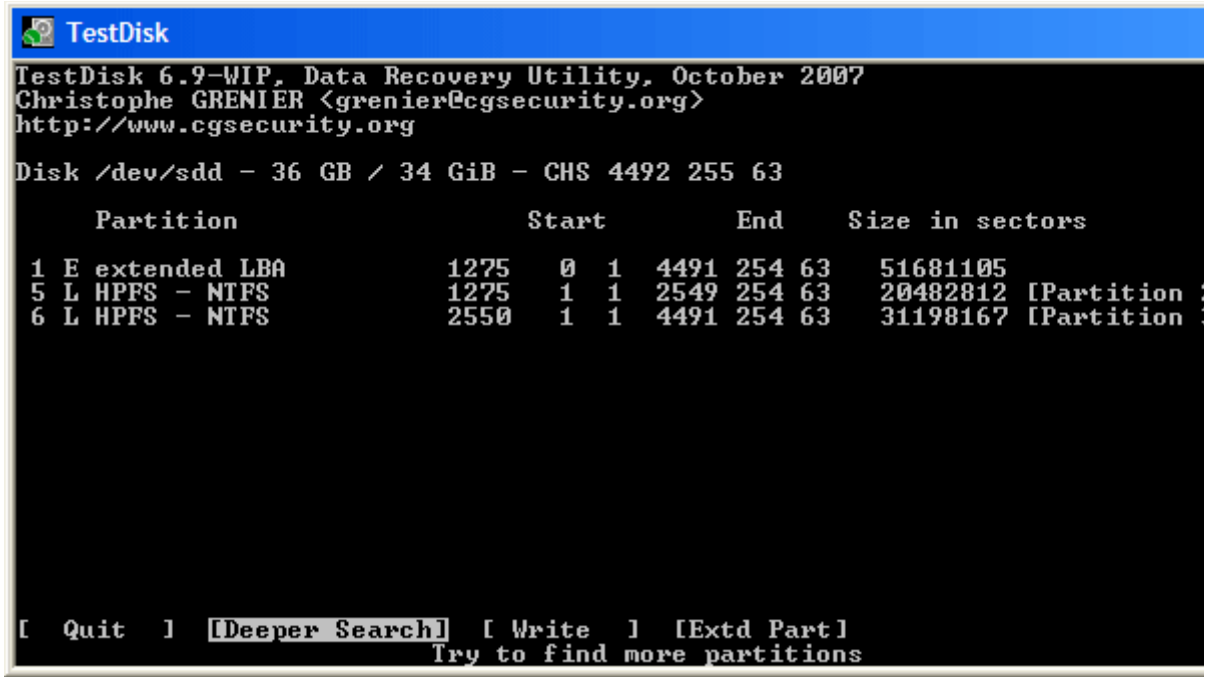


- Mettre en surbrillance cette partition et presser la touche ***p*** pour lister les fichiers (Utiliser *q* pour quitter et retourner à cet écran).

Tous les répertoires et les fichiers doivent être correctement listés.

- Appuyer sur la touche Entrée pour continuer.

Réécrire la table des partitions ou rechercher plus de partitions?



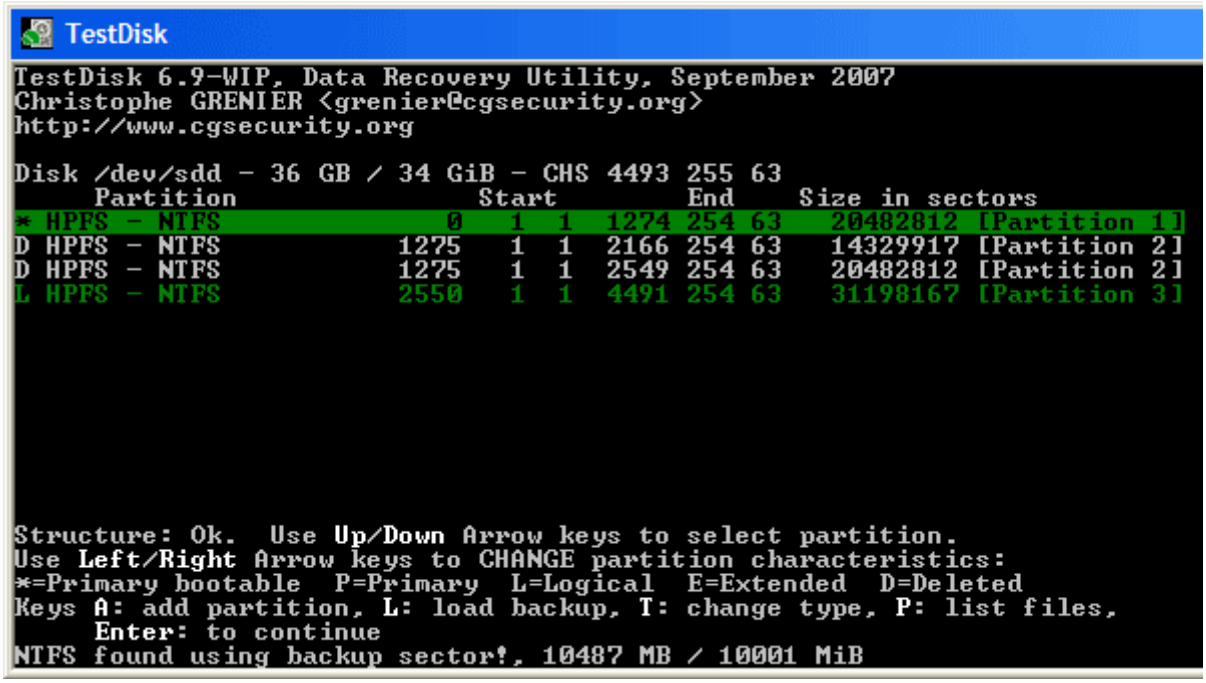
- ***Si toutes les partitions ont été trouvées*** et que les fichiers sont correctement listés, sélectionner **Write** dans le menu pour écrire la nouvelle table des partitions. Le menu `Extd Part` (si présent) vous permet de jouer sur la taille de la partition étendue: elle peut utiliser la totalité de l'espace disponible ou bien le minimum requis.
- ***Comme une partition, la première, est toujours manquante***, choisissons ***Deeper Search*** puis touche `Entrée` pour continuer.

Une partition est toujours manquante: Recherche approfondie

Deeper Search va aussi rechercher la présence de sauvegarde du secteur de boot des systèmes FAT32 et des systèmes de fichiers NTFS, les sauvegardes des `superblocks` ext2/ext3/ext4 ainsi plus de partitions peuvent être retrouvées.

TestDisk scanne chaque cylindre  (cliquer sur la miniature pour agrandir l'image).

Après la recherche approfondie, les résultats sont affichés:
La première partition ***"Partition 1"*** a été trouvée à l'aide de la sauvegarde du secteur de boot. Sur la dernière ligne de l'écran, le message ***"NTFS found using backup sector!"*** et la taille de la partition sont affichés. La partition ***"Partition 2"*** est affichée deux fois avec des tailles différentes.
Ces deux partitions sont affichées avec le statut **D**(eleted) parce qu'elles se chevauchent.

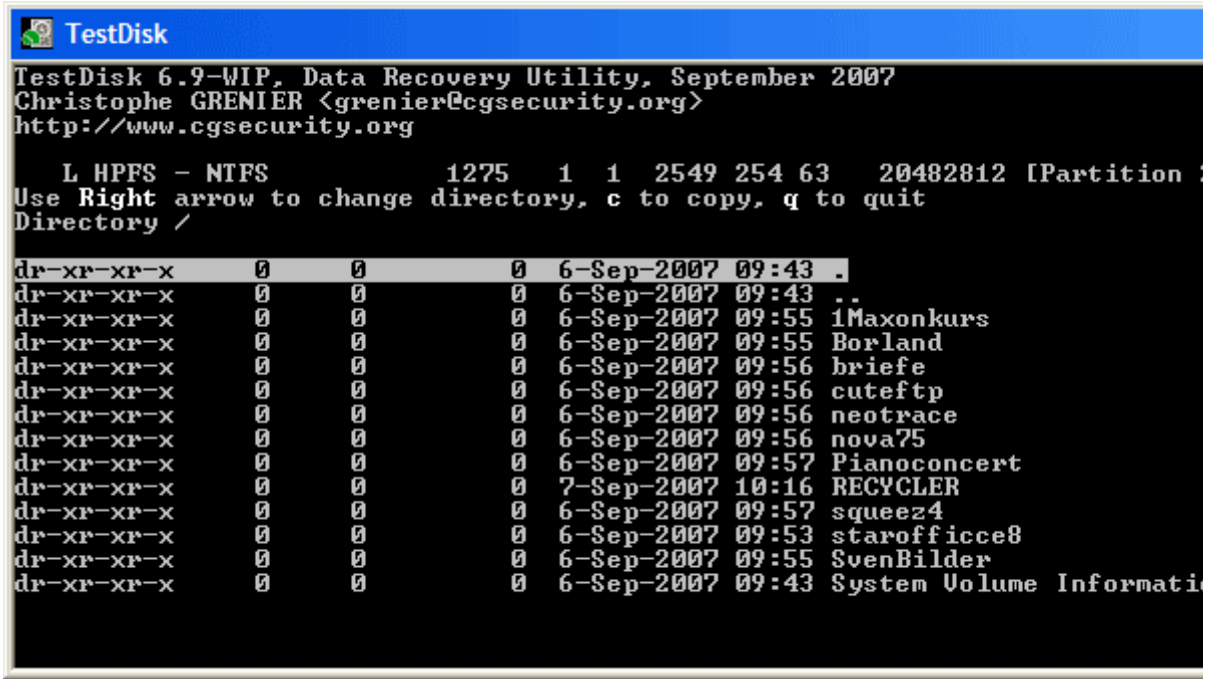


- Sélectionner la première partition `Partition 2` et utiliser ***p*** pour lister les fichiers.

Le système de fichier de la partition logique du dessus (nommé Partition 2) est endommagé

(cliquer sur la miniature pour agrandir l'image).

- Appuyer sur la touche `q` pour revenir à l'écran précédent.
- Laisser la partition `Partition 2` dont le système de fichier est illisible marqué comme `D(deleted)`.
- Sélectionner la seconde partition `Partition 2` en dessous
- Utiliser p pour lister ces fichiers



Cela marche, les fichiers sont bien affichés, vous avez trouvé la bonne partition !

- Utiliser les flèches droite/gauche pour naviguer dans les répertoires et lister vos fichiers pour plus de vérifications

Remarque: L'affichage d'un répertoire d'une partition FAT est limité à 10 clusters, certains fichiers peuvent donc ne pas apparaitre, mais cela n'affecte en rien la possibilité d'y accéder une fois la partition récupérée.

- Presser q pour quitter et revenir à l'écran précédent.

- Une partition peut être dans l'état P=primaire, *=amorçable, L=logique et D=effacé.

A l'aide des flèches gauche/droite, changer le statut de la partition sélectionnée (que l'on souhaite récupérer) en ***L(ogical)***.

sélection partitions à récupérer

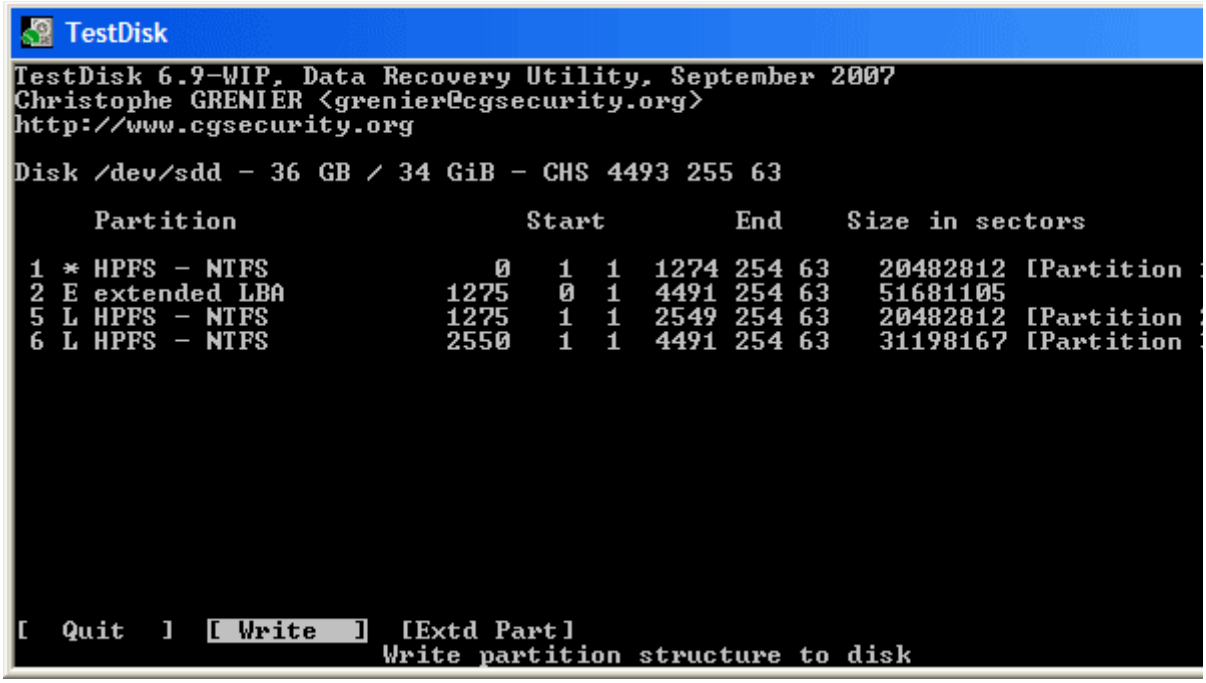
Conseil: lisez ***Reconnaître les partitions primaires et logiques*** si vous avez besoin d'aide pour distinguer les partitions primaires et les partitions logiques.
Note: Si une partition est listée *(bootable) mais que vous n'avez pas

besoin de démarrer depuis cette partition, vous pouvez la changer en partition primaire *P*rimary.

- Appuyer sur la touche `Entrée` pour continuer.

Récupération de la table des partitions

Il est désormais possible de réécrire le partitionnement: table des partitions et partitions étendues.
Note: La partition étendue est créée automatiquement en fonction des partitions logiques.

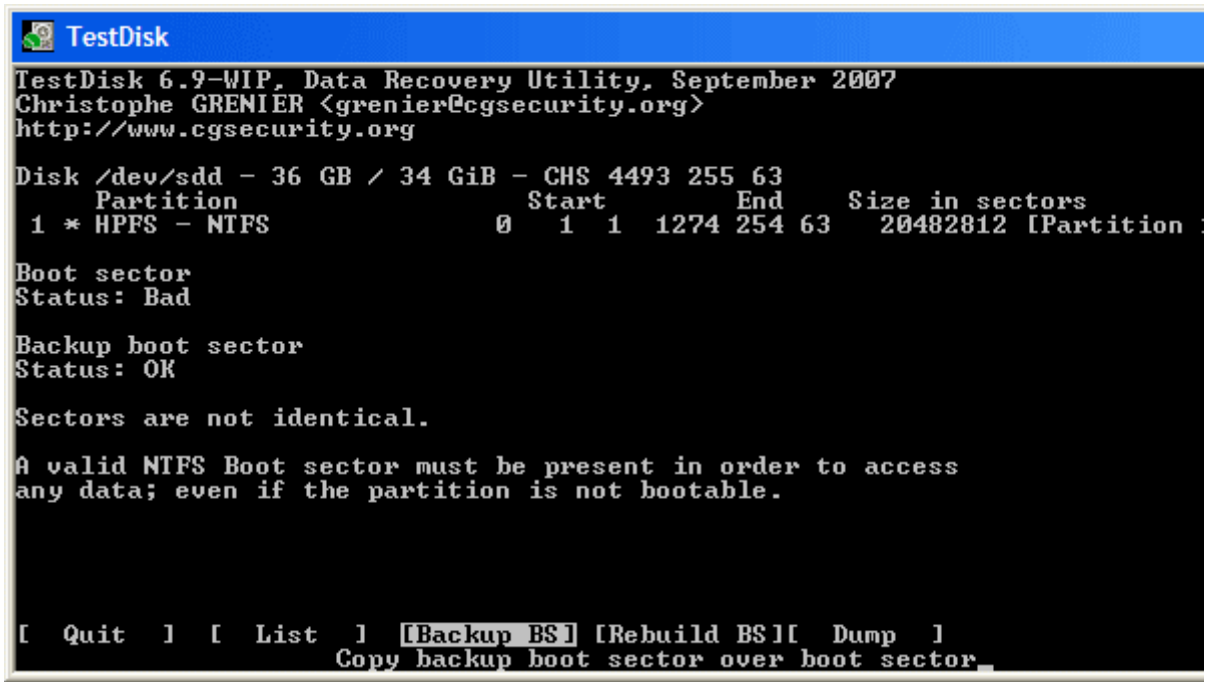


- Sélectionner ***Write***, valider puis confirmer l'écriture avec `y`.

Maintenant, toutes les partitions figurent dans la table des partitions, un problème de réglé.

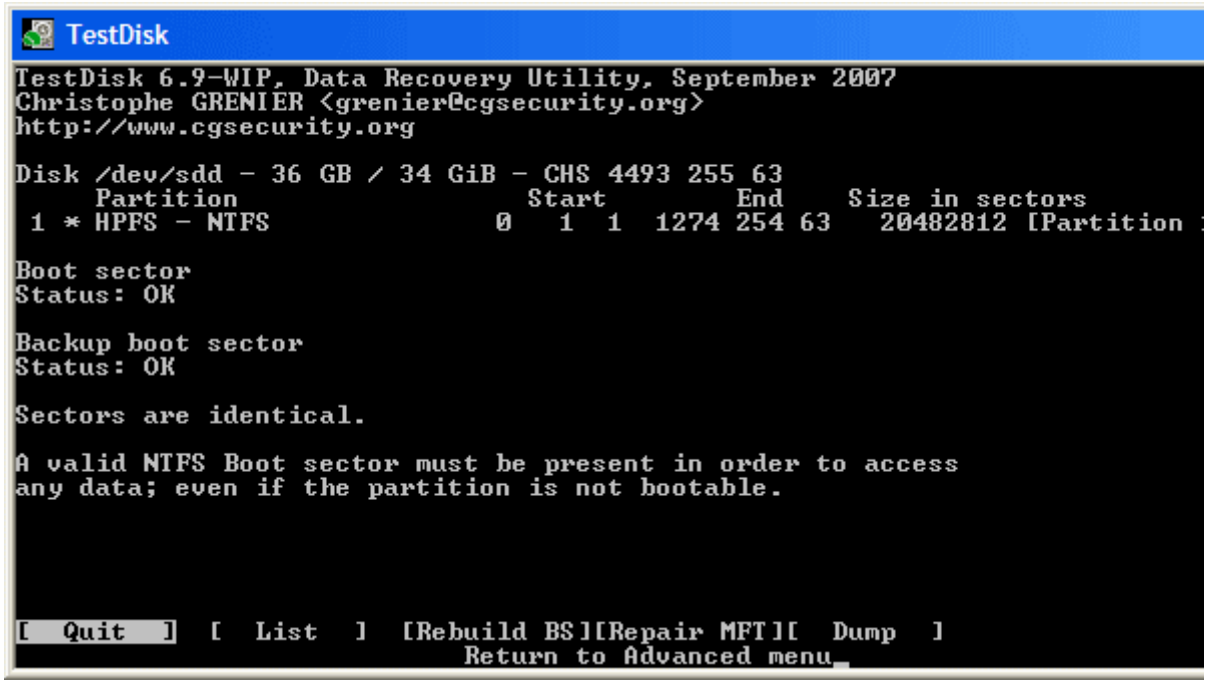
Récupération du secteur de boot NTFS

Le secteur de boot de la première partition nommée `Partition 1` est encore endommagé. Il est temps de le réparer. Le statut du secteur de boot NTFS est incorrect (`bad`) mais sa sauvegarde (backup boot sector) est valide. Ces secteurs ne sont pas identiques.



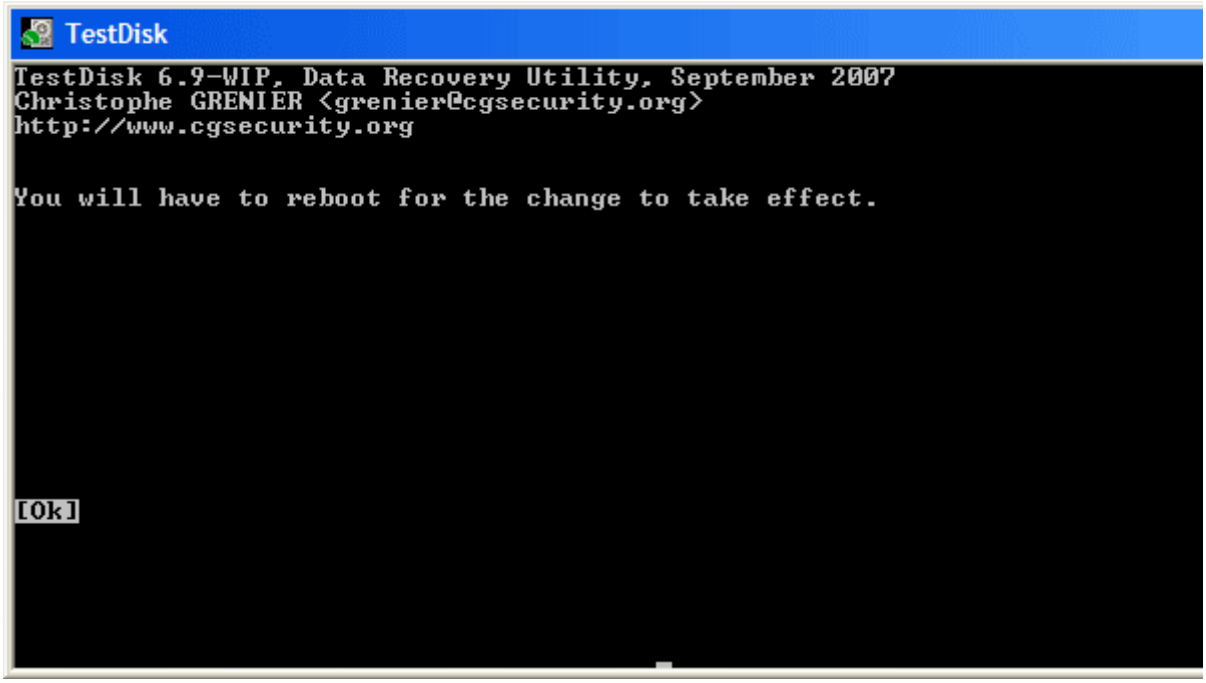
- Pour restaurer le secteur de boot (Copie de la sauvegarde du secteur de boot à l'emplacement du secteur de boot d'origine), sélectionner ***Backup BS***, valider avec la touche Entrée, confirmer par y, acquitter le message de réussite Ok.

Pour plus d'informations sur la réparation d'un secteur de boot, consulter Réparation d'une partition NTFS ou Réparation d'une partition FAT. Le message suivant est affiché:



Le secteur de boot et sa sauvegarde sont tout deux valides et identiques l'un à l'autre: le secteur de boot NTFS a été récupéré avec succès.

- Utiliser Entrée pour quitter.



- TestDisk affiche ***You have to restart your Computer to access your data***, appuyez sur Entrée une dernière fois et redémarrez votre ordinateur.

Récupération de fichiers effacés

TestDisk peut récupérer

- des fichiers et répertoires effacés pour les systèmes de fichiers FAT12, FAT16 et FAT32,
- fichiers supprimés des partitions ext2,
- fichiers effacés des partitions NTFS depuis la version 6.11.

Si cela ne fonctionne pas ou pour d'autres systèmes de fichiers, essayer PhotoRec, un utilitaire de récupération de fichiers à base de signature.

Retourner à la page principe de TestDisk.