

Datenwiederherstellung mit Photorec

Einleitung

Hallo zusammen. Nach etwas längerer Zeit gibt es wieder einmal ein Tutorial von mir. Heute werden wir uns mit Photorec, einer „Datarecovery Software“ befassen. Vielleicht habt ihr ja schon einmal versehentlich eine Formatierung ausgelöst, wart Opfer eines Virenangriffs, welcher das Partitionsformat beschädigte, oder ihr habt schon schmerzliche Erfahrungen mit einer Festplatte gemacht, welche plötzlich defekte Sektoren aufwies...

Von den Daten fehlt plötzlich jede Spur und man sucht verzweifelt nach einem Backup, welches natürlich nicht existiert!

Doch sind die Daten wirklich alle gnadenlos verschwunden?

In letzter Zeit hat mich diese Frage immer wieder beschäftigt, was mich im einen oder anderen Fall dazu brachte auf Recherche zu gehen.



Lasst euch nicht abschrecken von dem Bild. ;-)

Ich habe mich absichtlich für eine sehr eindrückliche, aber auch etwas überspitzte Illustration entschieden...

Was ist Photorec und wo bekomme ich es her?

Photorec ist eine Datenrettungssoftware, welche dazu entworfen wurde, um verlorene Dateien wiederherzustellen. Insbesondere wird die Suche nach digitalen Bildern unterstützt, findet aber auch zahlreiche andere Dateiformate. Die gesamte Liste der wiederherstellbaren Dateiformate unter PhotoRec beinhaltet mehr als 80 Dateierweiterungen. Photorec ignoriert das Dateisystem, so dass es sogar nach einer Formatierung funktioniert oder wenn die Partition schwer beschädigt ist. Photorec ist sicher, da die Software nicht versuchen wird auf ein Laufwerk, von dem versucht wird verlorene Dateien wiederherzustellen zu schreiben.



Photorec ist Open Source und unterstützt eine breite Palette an Plattformen. ☺
Ihr könnt es unter <http://www.cgsecurity.org> downloaden

Was ist Filecarving?

Bei den meisten Dateisystemen werden Dateien beim Löschen oder Formatieren nicht wirklich physikalisch gelöscht. Es wird nur der Zeiger auf die entsprechende Datei gelöscht. Eine Ausnahme bieten da so genannte „Shredder“ oder „Wipe“ Programme, welche die Festplatte mit beliebigen Speichermustern überschreiben, um eine Rekonstruktion der Daten zu verhindern.

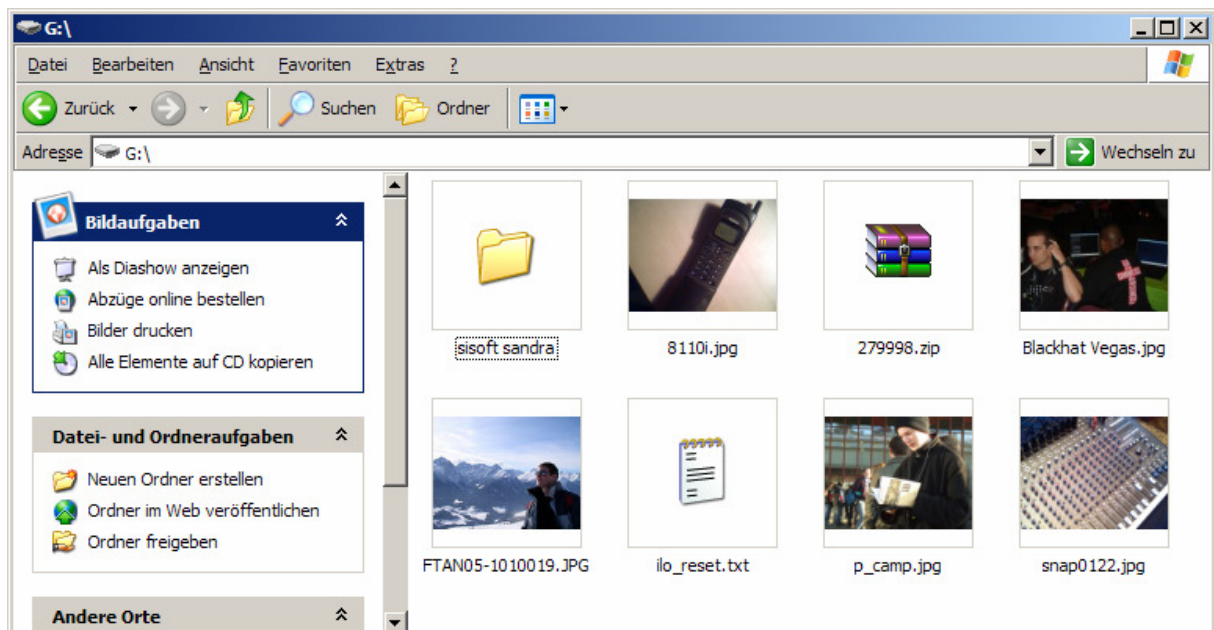
Falls kein „Shredder-Tool“ angewendet wurde, stellt das Dateisystem die gelöschten Dateien als freien Speicherplatz zur Verfügung. Die Daten sind aber meist zum grössten Teil noch vorhanden, sofern sie nicht wieder überschrieben wurden.

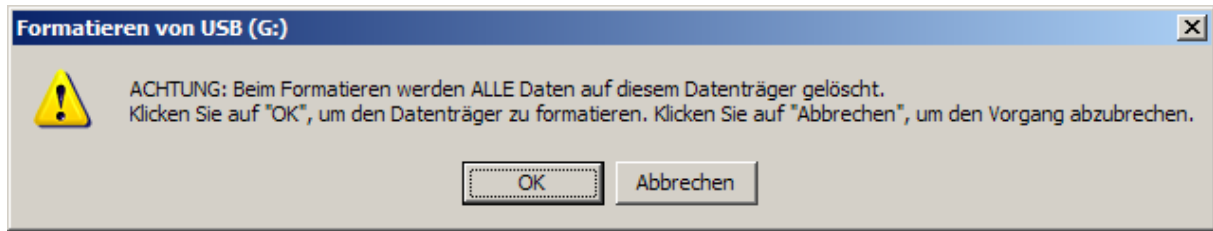
Wird nun eine Festplatte nach genau diesem Prinzip byte für byte gescannt, dann spricht man von Filecarving.

Wir wenden Photorec an

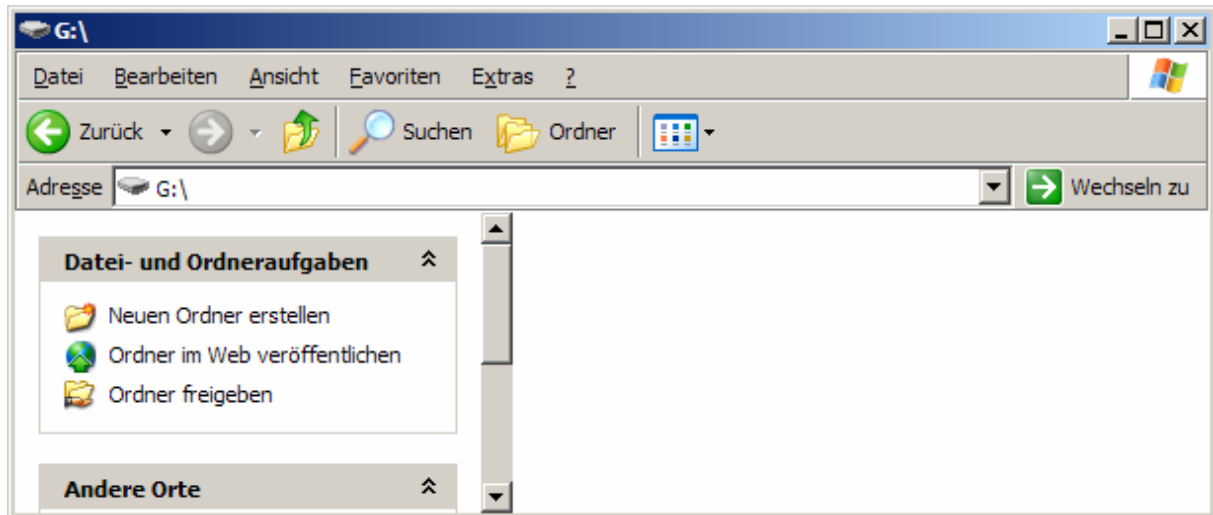
Damit ich Photorec testen kann, muss ein Datenträger zum testen her. Da ich es nicht unbedingt bevorzugte meine eigene Festplatte zu formatieren, habe ich mich für einen Datenträger mit lediglich 16MB Kapazität entschieden. Es handelt sich dabei um einen Werbegeschenk USB-Stick ;-)

Da ich ihn noch nicht in die runde Ablage gelegt habe, missbrauche ich ihn nun für meinen Test. Man findet schliesslich gerade genügend Kapazität um ein paar Bilder, komprimierte Archive und Textdateien abzuspeichern.

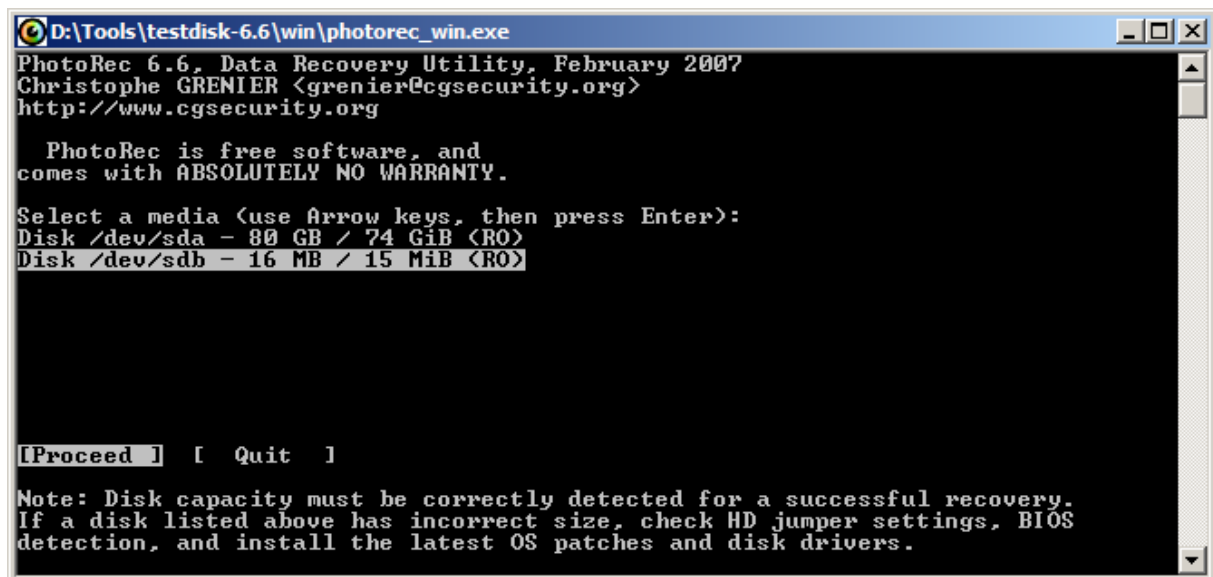




Bevor ich mich Photorec widme, formatiere ich den USB-Stick komplett und vergewissere mich, dass die Daten wirklich alle gelöscht sind.



Entpackt Photorec in ein beliebiges Verzeichnis eurer Wahl und führt die Datei **photorec_win.exe** aus. Wie Ihr sehen könnt handelt es sich um eine Konsolenbasierende Anwendung. Nun sollten die in unserem System installierten Datenträger aufgelistet werden. Ich erkenne meinen USB-Stick mit den stolzen 16MB Kapazität, den ich nun auswähle um fortzufahren.



```

D:\Tools\testdisk-6.6\win\photorec_win.exe
PhotoRec 6.6, Data Recovery Utility, February 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sdb - 16 MB / 15 MiB <R0>

Please select the partition table type, press Enter when done.
[Intel] Intel/PC partition
[Mac] Apple partition map
[None] Non partitioned media
[Sun] Sun Solaris partition
[XBox] XBox partition
[Return] Return to disk selection_

Note: Do NOT select 'None' for media with only a single partition. It's very
rare for a drive to be 'Non-partitioned'.

```

Nun haben wir die Möglichkeit, den Partitionstyp auszuwählen. In meinem Fall wähle ich hier Intel/PC partition aus.

Unterstützte Partitionsformate sind beispielsweise FAT, NTFS, EXT2, EXT3, HFS+ und ReiserFS.

Bevor ich den Suchvorgang starte, habe ich noch die Möglichkeit einige Optionen vorzunehmen oder Filter zu setzen.

```

D:\Tools\testdisk-6.6\win\photorec_win.exe
PhotoRec 6.6, Data Recovery Utility, February 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sdb - 16 MB / 15 MiB <R0>

Partition          Start      End      Size in sectors
D empty            0  0  1      1 254 63      32130 [Whole disk]
1 * FAT12          0  0  8      2   6 11      32512 [NO NAME]

[ Search ] [Options] [File Opt] [ Quit ]_

```

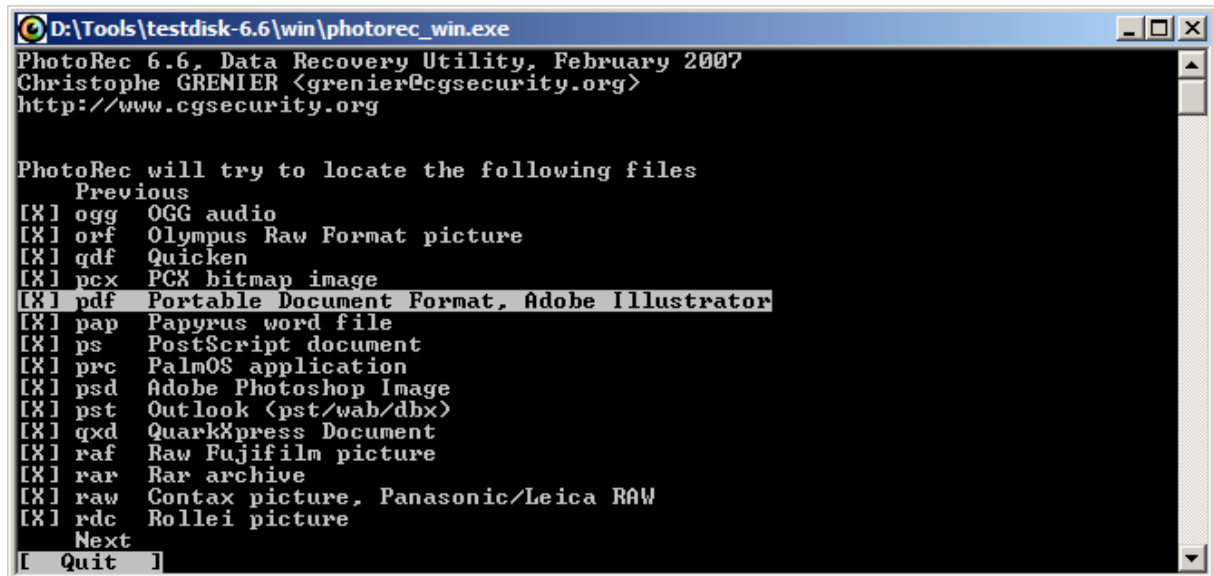
Die Optionsmöglichkeiten belasse ich so wie sie standardmässig vorgeschlagen werden. Man könnte hier beispielsweise einstellen, ob man korrupte Dateien überspringen möchte, ob ein Expertenmodus aktiviert werden soll oder wie tief das Tool den Datenträger durchsuchen soll.

```

Paranoid : Yes
Allow partial last cylinder : No
Keep corrupted files : No
Mode expert : No
Low memory: No
Quit_

```

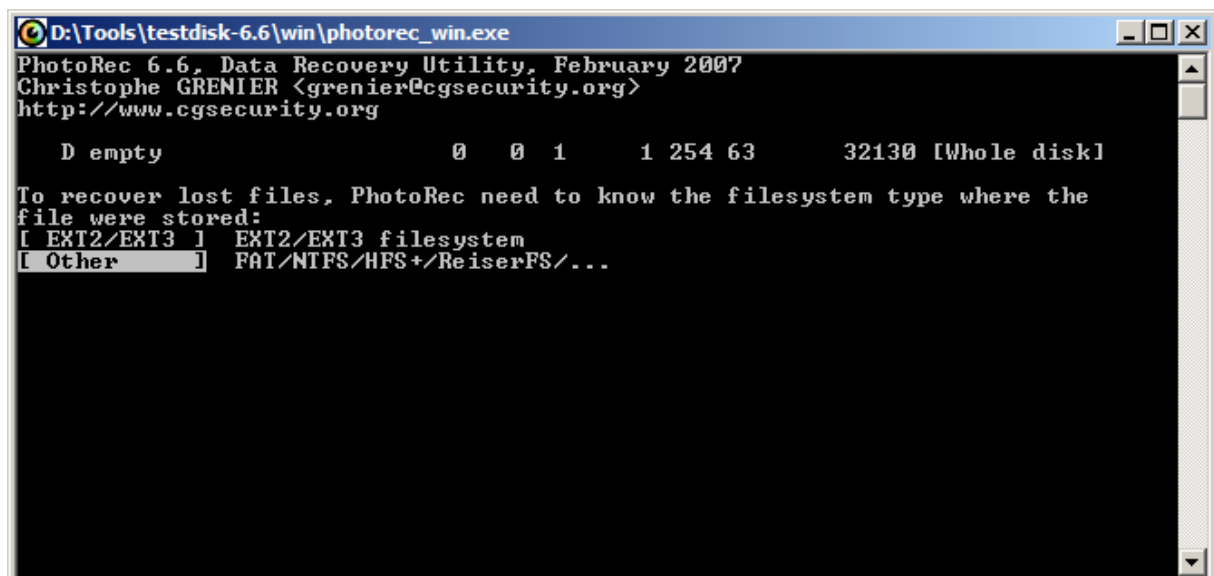
Etwas interessanter dürften die „Fileoptionen“ sein, da man hier einerseits die Vielfalt der Dateierweiterungen sieht, welche Photorec unterstützt und man andererseits auch Filter setzen kann, um die Dateisuche einzuschränken.



```
D:\Tools\testdisk-6.6\win\photorec_win.exe
PhotoRec 6.6, Data Recovery Utility, February 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

PhotoRec will try to locate the following files
  Previous
[X] ogg  OGG audio
[X] orf  Olympus Raw Format picture
[X] qdf  Quicken
[X] pcx  PCX bitmap image
[X] pdf  Portable Document Format, Adobe Illustrator
[X] pap  Papyrus word file
[X] ps   PostScript document
[X] prc  PalmOS application
[X] psd  Adobe Photoshop Image
[X] pst  Outlook (pst/wab/dbx)
[X] qxd  QuarkXpress Document
[X] raf  Raw Fujifilm picture
[X] rar  Rar archive
[X] raw  Contax picture, Panasonic/Leica RAW
[X] rdc  Rollei picture
  Next
[ Quit ]
```

Nachdem ich alles eingestellt habe, beginne ich mit dem Suchvorgang und gebe Photorec an, dass es sich um eine FAT Partition handelt.



```
D:\Tools\testdisk-6.6\win\photorec_win.exe
PhotoRec 6.6, Data Recovery Utility, February 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

  D empty          0  0  1      1 254 63      32130 [Whole disk]

To recover lost files, PhotoRec need to know the filesystem type where the
file were stored:
[ EXT2/EXT3 ]  EXT2/EXT3 filesystem
[ Other      ]  FAT/NTFS/HFS+/ReiserFS/...
```

Nun fragt das Tool nach, wo es gefundene Daten ablegen soll. Man hat hier die Möglichkeit ein eigenes Verzeichnis zu wählen oder die Daten im vorgeschlagenen Verzeichnis von Photorec abzulegen.

```
D:\Tools\testdisk-6.6\win\photorec_win.exe
PhotoRec 6.6, Data Recovery Utility, February 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Do you want to save recovered files in d:\Tools\testdisk-6.6\win ? [Y/N]

To select another directory, use the arrow keys.
drwx----- 400 401 0 5-Jul-2007 12:00 .
drwx----- 400 401 0 20-Jun-2007 16:24 ..
drwx----- 400 401 0 20-Jun-2007 16:24 c
drwx----- 400 401 0 20-Jun-2007 17:13 recup_dir.1
```

Nun beginnt das Tool nach den verlorenen Dateien zu suchen. Bei 16MB geht die Suche relativ schnell. Je nach Datenträgergröße kann dieser Vorgang aber etwas mehr Zeit in Anspruch nehmen...

```
D:\Tools\testdisk-6.6\win\photorec_win.exe
PhotoRec 6.6, Data Recovery Utility, February 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

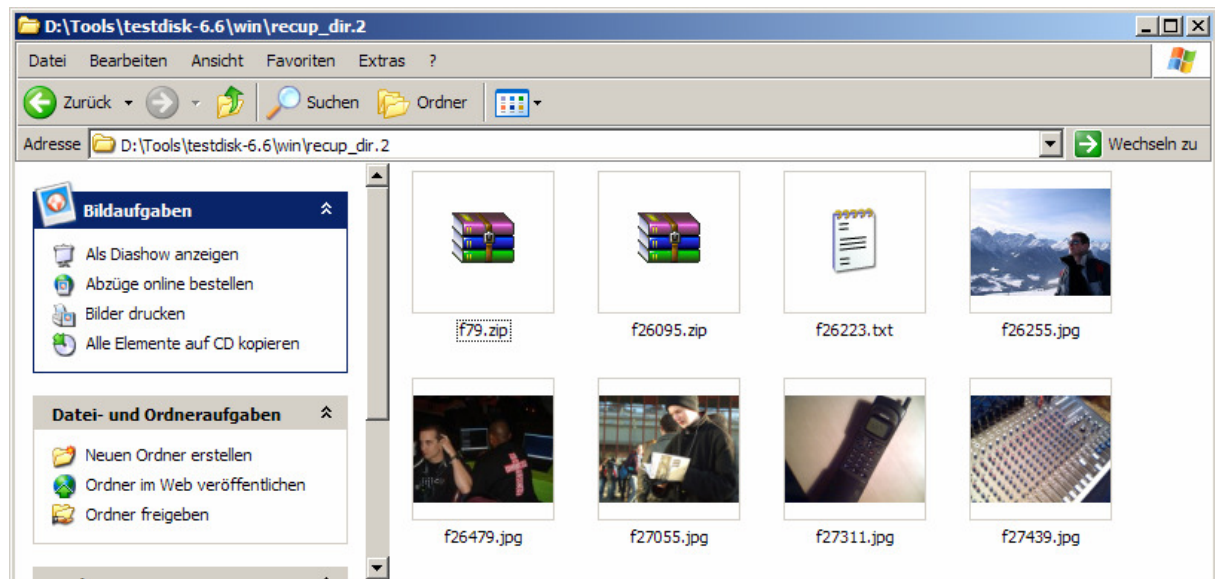
Disk /dev/sdb - 16 MB / 15 MiB (RO)
Partition      Start      End      Size in sectors
D empty        0 0 1      1 254 63      32130 [Whole disk]

Pass 1 - Reading sector      31119/32130, 7 files found
Elapsed time 0h00m51s - Estimated time for achievement 0h00m01
jpg: 4 recovered
zip: 2 recovered
txt: 1 recovered

Stop
```

Nach dem Suchvorgang erhalte ich eine Meldung, wie viele Dateien wiederhergestellt wurden. Ich wechsele ins entsprechende Verzeichnis und bin gespannt, was dabei herausgekommen ist.

```
8 files saved in /cygdrive/d/Tools/testdisk-6.6/win/recup_dir directory.
Recovery completed.
jpg: 5 recovered
zip: 2 recovered
txt: 1 recovered
```



Das Ergebnis ist erfreulich, da alle gelöschten Daten wieder zum Vorschein gekommen sind. Was nicht rekonstruiert wird ist eine allenfalls vorhandene Ordnerstruktur. Dies finde ich aber nicht weiter tragisch, da die gefundenen Daten mit Sicherheit mehr wert sind wie eine korrekte Ordnerstruktur ohne Inhalte. Eine Datenwiederherstellung bei einer Festplatte, welche defekte Sektoren aufweist, dürfte aber nach wie vor sehr kritisch sein. Besonders wenn die Festplatte „kratzen-de“ Geräusche aufweist, dann hilft wohl nur noch beten ;-)

Internet Links

<http://www.cgsecurity.org>
<http://www.irongeek.com>
<http://de.wikipedia.org/Datenrettung>

So, nun wäre ich am Ende meines Tutorials angelangt.
Viel Erfolg bei der Datenwiederherstellung und bis zum nächsten Manual!

© 7/2007 by Daniel Müller
Mail: daniel85@gmx.ch
HP: <http://www.daniel85.ch.vu>

Grüsse an alle Mitglieder von Computec!