



Die Kommandozeile unter Windows

Datum: 06.12.2007 | [ältere Artikel](#)



Klein, stark, schwarz: Die Rede ist nicht vom Espresso nach dem Essen, sondern von der Kommandozeile unter Windows, in Fachkreisen auch Shell genannt. Das unscheinbare, schwarze Fenster ist mehr als ein Relikt aus alten DOS-Zeiten und kann – bei Kenntnis aller Möglichkeiten – dem Windows-Profi viel Klickarbeit ersparen. Im folgenden Artikel stellen wir die wichtigsten Befehle und Möglichkeiten im Umgang mit der Windows-Shell dar.

DOS, kein DOS

Einer unserer ältesten Artikel "[Überleben am DOS-Prompt](#)" ist auch heute noch in den Top20 der meist abgerufenen Artikel auf WinTotal. PCDParker beschrieb damals, mit welchen Befehlen Dateioperationen in Shell/DOS ausgeführt werden. Alte DOS-Hasen sind mit dem Befehlen auch heute noch sicher vertraut. Die Vielzahl unserer Leser ist aber ohne Maus und Explorer oft aufgeschmissen und für solche Hilfestellungen dankbar.

Doch die Shell ist – entgegen ihrem Aussehen – kein DOS, sondern eine native Win32-Anwendung und bietet mehr als einfache Dateioperationen. Wie auf Linux-Systemen üblich, kann über die Shell viel mehr angestellt und abgefragt werden als die meisten User überhaupt wissen.

Microsoft hat übrigens den Nachfolger der aktuellen eingeführt, welche sich Windows PowerShell nennt. Als objektorientierter Nachfolger von Cmd.exe setzt sie ganz auf .NET und bietet für Entwickler und Administratoren viele nützliche Neuigkeiten. Weitere Infos zu Microsoft PowerShell finden Sie auf der [Homepage zur PowerShell](#) sowie als [Download auf WinTotal](#).

Willkommen in der Shell

Die Kommandozeile, in der Folge nun nur noch Shell genannt, starten Sie wie folgt:

Die Windows-Shell ist als ausführbare Datei cmd.exe im System32-Ordner von Windows zu finden. Sie starten die Shell über Start -> Ausführen ([Windows-Taste]+[R]) -> cmd.

Für Windows Vista:

Sie können "[Ausführen](#)" im Startmenü wieder herstellen oder in die Suche einfach **cmd** eingeben.

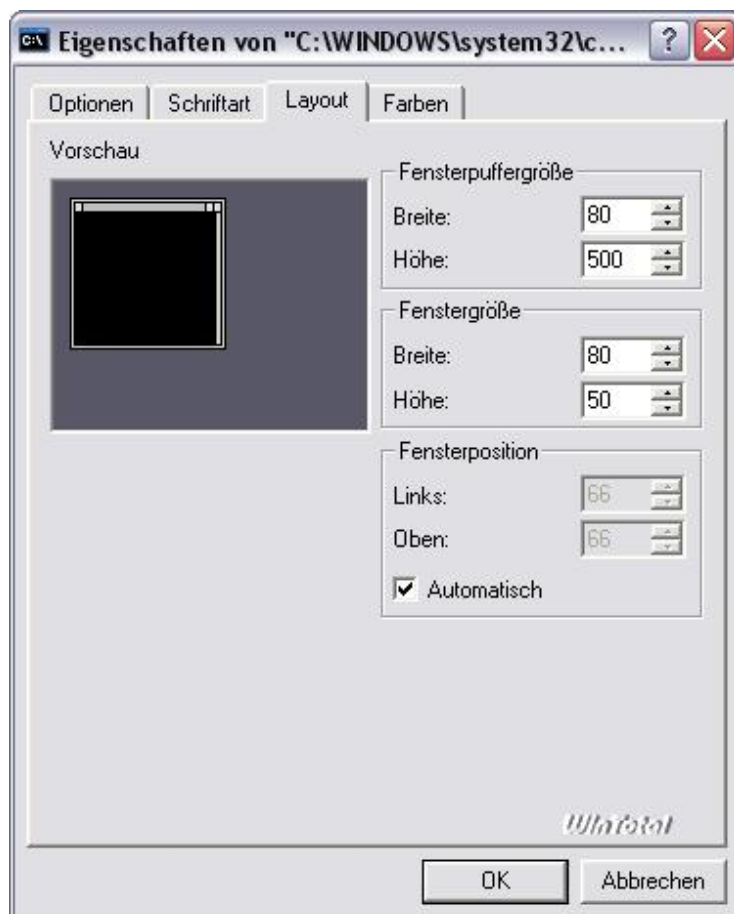
Windows Vista-Nutzer müssen die Eingabe zudem mit [STRG]+[ALT]+[Enter] abschließen, um in der Shell Administratorrechte zu haben ([siehe Tipp](#)), sofern UAC nicht generell abgeschaltet wurde.

Die Shell öffnet sich im Regelfall im aktuellen Pfad des Benutzers oder im System32-Ordner. Die Stelle, an der Sie etwas eingeben können, nennt man Prompt.



Die Shell, am Prompt Laufwerk P:
Klick aufs Bild zum Vergrößern

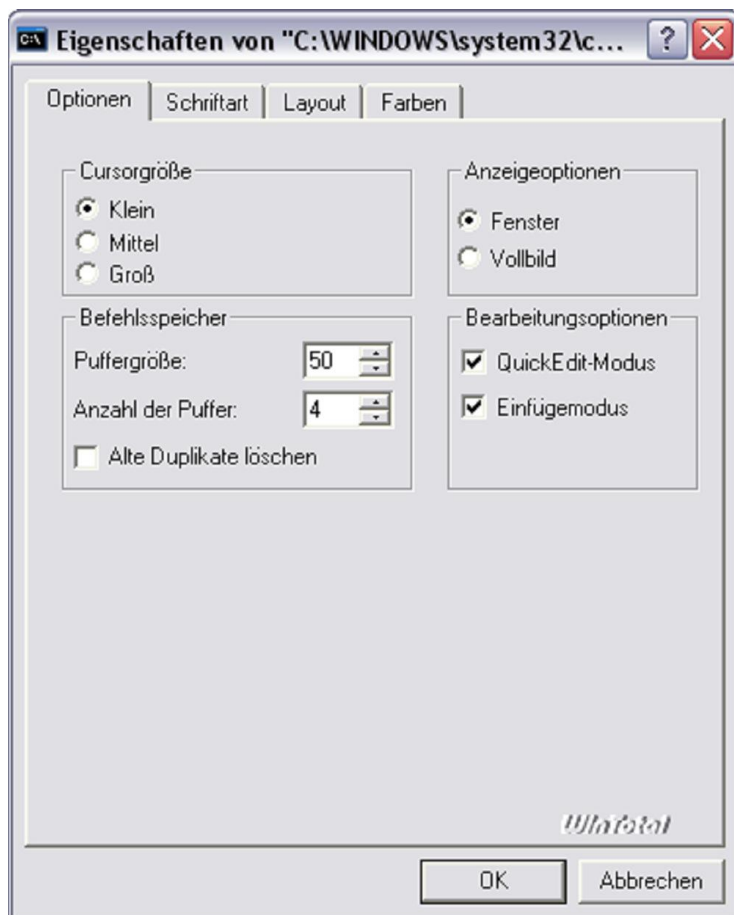
Zunächst können Sie die Shell nach eigenen Wünschen anpassen. Dazu klicken Sie mit der linken oder rechten Maustaste auf das Icon oben links in der Shell. Im erscheinenden Menü können Sie unter Eigenschaften das Erscheinungsbild und Verhalten der Shell bestimmen.



Layouteigenschaften der Kommandozeile
Klick aufs Bild zum Vergrößern

Neben Farbwahl, Fenster -oder Vollbildansicht, können Sie unter Layout die Fenstergröße und Fensterpuffergröße anpassen: 50 Zeichen in der Höhe und eine Pufferhöhe (zum Zurückscrollen) von 500 Zeichen sollten es schon sein. Die Breite sollte man in beiden Optionen bei 80 Zeichen belassen.

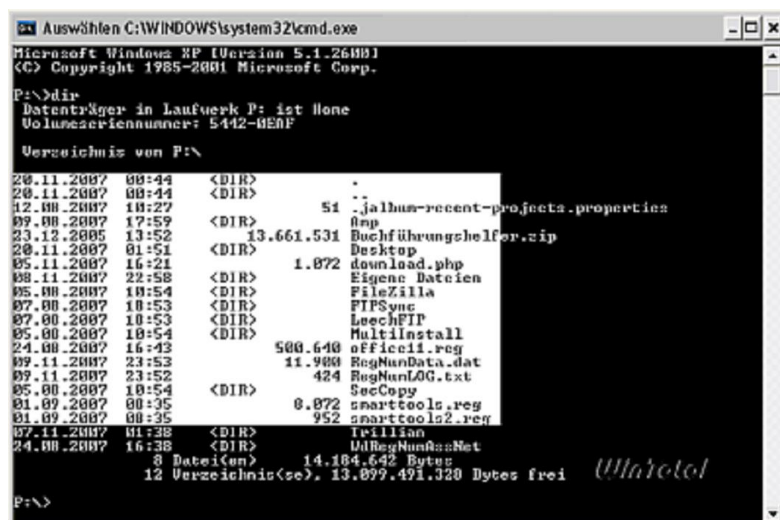
Unter den Optionen finden sich die Bearbeitungsoptionen *QuickEdit-Modus* und *Einfügemodus*.



QuickEdit-Modus und Einfügemodus

Klick aufs Bild zum Vergrößern

Mit dem QuickEdit-Modus können Sie mit gedrückter Maustaste den Text in der Shell erfassen. Drücken Sie anschließend RETURN, wird der markierte Text in die Zwischenablage übernommen. Wenn man das nicht aktivieren will, kann man über das Kontextmenü in der Shell "Markieren" wählen. Der Rest ist dann identisch.



QuickEdit-Modus

Klick aufs Bild zum Vergrößern

Der aktivierte Einfügemodus ermöglicht es, noch Text an der Kommandozeile einzufügen, ohne den rechts davon befindlichen Text zu überschreiben. Die Funktion ist aus der Textbearbeitung her meist bekannt.

Die Shell bietet darüber hinaus viele Komfortfunktionen, wie man sie von dem alten Doskey-Programm her noch kennt:

Mit F3 beispielsweise wird der zuletzt verwendete Befehl erneut am Prompt eingegeben. Mit F8 können Sie durch die zuletzt verwendeten Befehle blättern, mit F7 sehen Sie die History und mit F9 können Sie die Befehlsnummer (laut History) direkt aufrufen.

```

C:\WINDOWS\system32\cmd.exe

[191]: KB925902 - Update
[192]: KB926239 - Update
[193]: KB926255 - Update
[194]: KB926436 - Update
[195]: KB927729 - Update
[196]: KB927802 - Update
[197]: KB927891 - Update
[198]: KB928255 - Update
[199]: KB928043 - Update
[200]: KB929123 - Update
[201]: KB929969 - Update

0: dir
1: getnet
2: netstat
3: sysinfo
4: systeminfo

Netzwerkkarte(n): 2 Netzwerkadapter installiert.
[01]: 1394-Netzwerkadapter
Verbindungsname: 1394-Verbindung
[02]: 3Con Gigabit NIC
Verbindungsname: LAN-Verbindung
DHCP aktiviert: Ja
DHCP-Server: 192.168.1.1
IP-Adresse(n)
[01]: 192.168.1.2?

F:\>systeminfo

```

History und Co.

Klick aufs Bild zum Vergrößern

Die Pfeiltasten haben in der Shell auch eine Bedeutung. Nach oben ruft in umgekehrter Reihenfolge die letzten Befehle auf. Nach rechts stellt Zeichen des letzten Befehls wieder her.

Eine Übersicht über alle Tastaturkürzel und deren Verwendung finden Sie in der Onlinehilfe von Windows XP unter dem Stichwort "Doskey".

In der folgenden Tabelle sind die **doskey**-Bearbeitungsfunktionen und ihre Funktionen aufgeführt:

Taste oder Tastenkombination	Beschreibung
NACH-LINKS-TASTE	Bewegt die Einfügemarke ein Zeichen nach links.
NACH-RECHTS-TASTE	Bewegt die Einfügemarke ein Zeichen nach rechts.
STRG+NACH-LINKS-TASTE	Bewegt die Einfügemarke ein Wort nach links.
STRG+NACH-RECHTS-TASTE	Bewegt die Einfügemarke ein Wort nach rechts.
POS1	Bewegt die Einfügemarke an den Anfang der Zeile.
ENDE	Bewegt die Einfügemarke an das Ende der Zeile.
ESC	Löscht den Befehl aus der Anzeige.
F1	Kopiert ein Zeichen aus derselben Spalte im Zeilenspeicher in die entsprechende Spalte des Eingabeaufforderungsfensters. (Der Zeilenspeicher ist ein Pufferspeicher, der den zuletzt eingegebenen Befehl enthält.)
F2	Sucht vorwärts im Zeilenspeicher nach dem nächsten Auftreten des Zeichens, das Sie nach dem Drücken von F2 eingeben. Doskey.exe fügt den Text bis zum (jedoch nicht einschließlich des) angegebenen Zeichen(s) aus dem Zeilenspeicher ein.
F3	Kopiert den Rest des Zeilenspeichers in die Befehlszeile. Doskey.exe beginnt mit dem Kopieren der Zeichen an der Position im Zeilenspeicher, die der Position der Einfügemarke in der Befehlszeile entspricht.
F4	Löscht Zeichen vom ersten Zeichen nach der Einfügemarke an bis zu dem von Ihnen angegebenen Zeichen. Um diese Bearbeitungsfunktion zu verwenden, drücken Sie F4 und geben dann ein Zeichen ein. Doskey.exe löscht die Zeichen von der Position der aktuellen Einfügemarke an bis zum ersten angegebenen Zeichen.
F5	Kopiert den aktuellen Zeilenspeicher in die aktuelle Befehlszeile.
F6	Plaziert ein Dateiendezeichen (STRG+Z) an der aktuellen Position der Einfügemarke.
F7	Zeigt in einem Popupfeld alle gespeicherten Befehle an. Wählen Sie mit NACH-OBEN und NACH-UNTEN den gewünschten Befehl aus, und drücken Sie zum Ausführen des Befehls die EINGABETASTE. Sie können auch die vor dem Befehl stehende Nummer zusammen mit der Taste F9 verwenden.
ALT+F7	Löscht alle gespeicherten Befehle.
F8	Zeigt alle Befehle im Puffer an, die mit den Zeichen des aktuellen Befehls beginnen.
F9	Fordert Sie zur Eingabe einer Befehlsnummer auf und zeigt dann den Befehl an, der mit der angegebenen Nummer verknüpft ist. Mit der EINGABETASTE können Sie den Befehl ausführen. Um alle Nummern und die entsprechenden Befehle anzuzeigen, drücken Sie F7.
ALT+F10	Löscht alle Makrodefinitionen.

• Verwenden von **doskey** innerhalb eines Programms

Doskey, alle Funktionen

Klick aufs Bild zum Vergrößern

Integration ins Kontextmenü

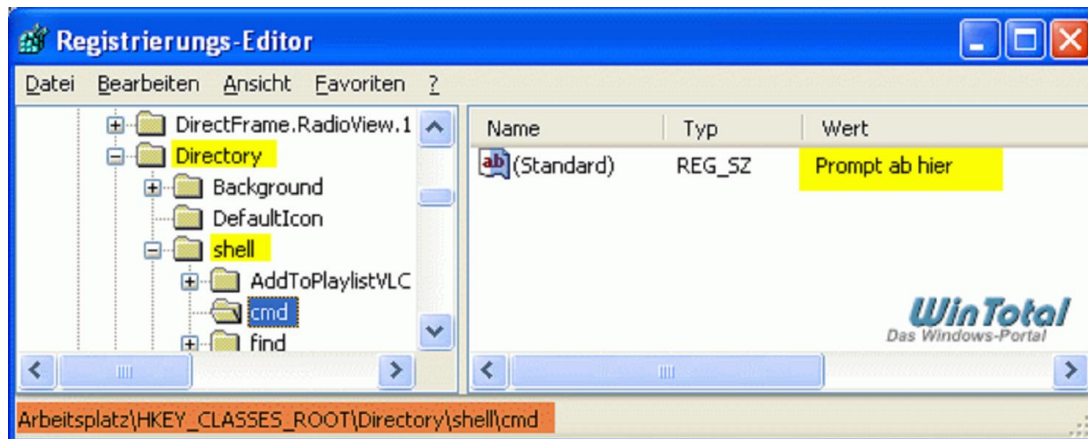
Wie bereits dargestellt, öffnet sich die Shell immer im Ordner des Benutzers oder im System32-Ordner. Wollen Sie in einen anderen Ordner wechseln, müssen Sie ggf. das Laufwerk und dann den Pfad mit dem Befehl **cd** bzw. **chdir** wechseln. Über einen Registry-Eintrag können Sie aber einen Kontextmenüeintrag für den Explorer erstellen, welcher die Shell in dem gerade ausgewählten Ordner öffnet.

Hierzu erstellt man in der Registry unter

HKEY_CLASSES_ROOT\Directory\shell
und

`HKEY_CLASSES_ROOT\Directory\shell`

einen neuen Schlüssel mit dem Namen **cmd** und darin als *Standard-SZ* einen Text wie **“Prompt ab hier“**. Weiter muss man unterhalb von dem erstellten cmd-Schlüssel einen weiteren Schlüssel mit dem Namen **command** erstellen und darin eine neue Zeichenfolge (Name nichts eingeben = Standard) mit dem Wert **cmd.exe /k “cd %L“** anlegen. [Download als gezipptes Reg-File](#).



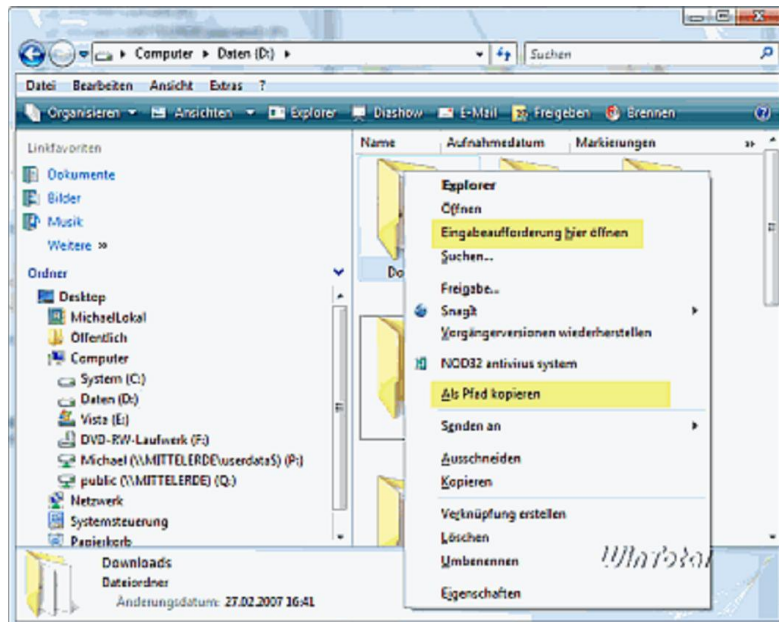
CMD in das Kontextmenü

Klick aufs Bild zum Vergrößern

Der Parameter `/k` weist die Shell an, den folgenden Befehl auszuführen und dann auf neue Befehle zu warten. `Cd%L` wechselt dabei in den aktuell selektierten Pfad.

Besonderheit Windows Vista

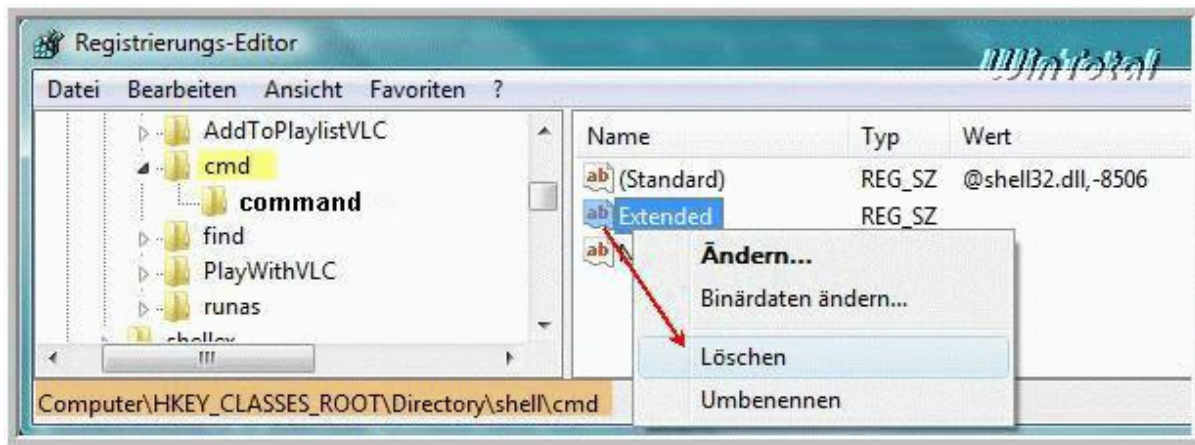
Der Explorer von Windows Vista bietet die gleiche Funktion als Neuerung. Wenn Sie im rechten Fenster des Explorers die Umschalttaste gedrückt halten und dabei die rechte Maustaste drücken, können Sie die Eingabeaufforderung auch direkt über **“Eingabeaufforderung hier öffnen“** ansteuern. Auf gleichem Weg können Sie den aktuellen Pfad eines markierten Verzeichnisses über **“Als Pfad kopieren“** in die Zwischenablage legen.



Eingabeaufforderung im Kontextmenü unter Vista

Klick aufs Bild zum Vergrößern

Wer den Eintrag **“Eingabeaufforderung hier öffnen“** dauerhaft im Kontextmenü haben möchte und nicht nur bei Shift-Rechtsklick, muss bei Vista in der Registry unter `HKEY_CLASSES_ROOT\Directory\shell\cmd` den Eintrag *Extended* löschen.



Eingabeaufforderung im Kontextmenü unter Vista dauerhaft
Klick aufs Bild zum Vergrößern

Wenn man das auch fürs Kontextmenü der Festplatten haben will, muss man unter Vista in der Registry unter `HKEY_CLASSES_ROOT\Drive\shell\cmd` ebenfalls den Eintrag `Extended` löschen.

Weitere Möglichkeiten zur Pfadübergabe und Vervollständigung

Die Shell bietet unter Windows XP noch weitere Möglichkeiten, um den Pfad zu übernehmen: Zum einen können Sie per Drag and Drop Pfadangaben aus dem Explorer in das Shellfenster ziehen. Geben Sie davor `cd` am Prompt ein, wechselt die Shell nach dem Drag and Drop des Pfades und einem Return in diesen. Bei Windows Vista funktioniert diese Feature nicht mehr.

Als weiteres Feature bietet die Shell seit Windows XP eine Autovervollständigung über die Tab-Taste. Wenn Sie beispielsweise in das Verzeichnis "Dokumente und Einstellungen" wechseln möchten und sich im Root `C:\` befinden, reicht `cd Dok`. Die Shell vervollständigt dann den Pfad. Gibt es keine genaue Übereinstimmung (z.B. `System` und `System32`), können Sie auch mehrfach TAB drücken.

Infos zum Umgang mit den Befehlen

Normalerweise liefert jeder Befehl ein Ergebnis oder führt eine Aktion aus. Sie können die Ausgabe eines Befehls aber auch in eine Datei (z.B. für Diagnosezwecke) ausleiten, mehrere Befehle verknüpfen oder komplexe Abfragen als Batch-Datei (Endung `.bat` oder `.cmd`) automatisiert bestimmte Aufgaben abarbeiten lassen. Gerade die letzte Option wird für Netzwerke oft genutzt, um beim Login für bestimmte Benutzer Netzwerkfreigaben als Laufwerke zu verbinden, Patches ggf. aufzuspielen, den Standarddrucker festzulegen usw.

Seitenweise anzeigen

Manche Befehle erschlagen den Anwender mit Infos oder Dateilisten am Shell. Mit der Ergänzung `|more` hinter dem Befehl stoppt die Ausgabe nach jeder Seite – z.B. `dir c:\windows |more`

Ausleiten in eine Datei

Der Befehl `netstat -a` listet alle Verbindungen und abgehörte Ports auf. Mit der Ergänzung `netstat -a > c:\Logfiles\liste.txt` wird die Ausgabe in eine Textdatei `liste.txt` in den Ordner `Logfiles` ausgeleitet. Diese Umleitung funktioniert mit allen Befehlen, welche ein Ergebnis ausgeben und bietet sich immer an, wenn die Menge an Informationen in der Shell zu unübersichtlich wird. Wenn Sie keinen speziellen Ordner für die Ausleitung in eine Datei angeben, wird die Textdatei im aktuellen Verzeichnis der Shell geschrieben, von der aus der Befehl aufgerufen wurde.

Wenn Sie **zwei statt einer** Spitzklammer angeben, wird das Ergebnis an die benannte Datei **angehängt**, ohne den Inhalt zu löschen. Sie können mit diesem Kniff fortlaufende Logfiles anlegen

```
netstat -a >> c:\Logfiles\liste.txt
```

Ausleiten auf den Drucker

Die Ausleitung funktioniert natürlich auch zum Drucker. Hinter der Spitzklammer müssen Sie dazu den Druckeranschluss nennen, also z.B. `lpt1`. Die richtige Syntax lautet dann `netstat -a > lpt1`

Für Netzwerk- oder USB-Drucker muss man sich aber mit einem Trick behelfen: Die Ausgabe erfolgt hier über Notepad, welches auf dem Standarddrucker ausdruckt. Hierzu verwenden wir das Hilfsprogramm `start`, welches aus der Shell heraus auch Fensterprogramme mit Parametern aufrufen kann (siehe [start](#)). Die Syntax lautet dann `start /w notepad /p datei.txt` (ggf. mit Pfad).

Kombination von Befehlen

Mit dem **&**-Zeichen können Sie Befehle kombinieren. Die Befehle werden dann nacheinander abgearbeitet.

`netstat -a > ausgabe.txt & start /w notepad /p ausgabe.txt`

gibt z.B. die `netstat -a` Ausgabe auf die Datei `ausgabe.txt` aus, welche dann von Notepad auf dem Standard-Drucker gedruckt wird.

Über **Klammern** können Sie Befehle auch logisch zusammenfassen:

`(date /t & Time /t & netstat -a) > ausgabe.txt & start /w notepad /p ausgabe.txt`

Das Datum, die Uhrzeit und der Netstat-Befehl werden in die Datei `ausgabe.txt` geschrieben und dann gedruckt.

Für kleinere Operationen macht dies noch Sinn. Bei komplexeren Abläufen dürfte eine Batch-Datei, welche sich noch kommentieren lässt, aber die bessere Wahl sein.

Batchdateien

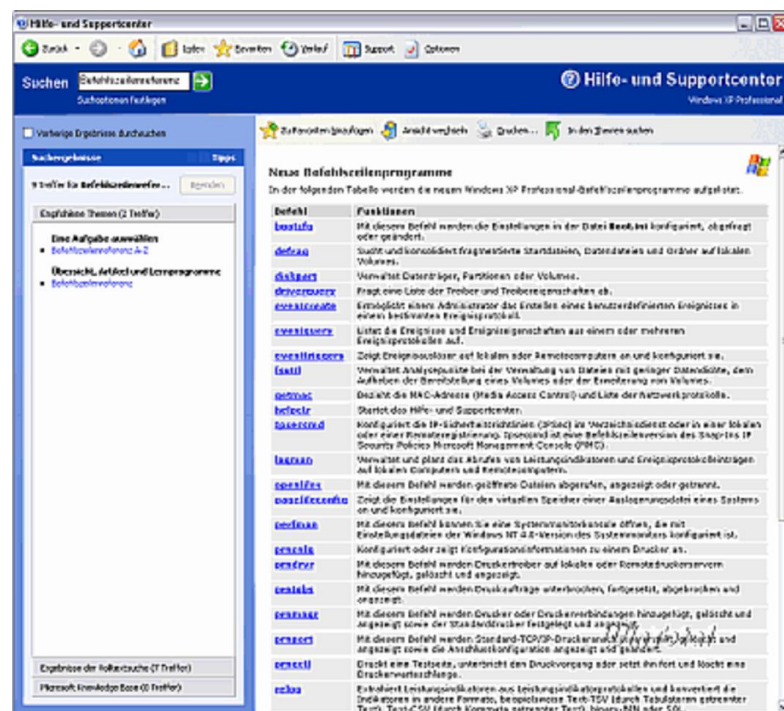
Die bekannteste aller Batchdateien war und ist die `autoexec.bat`. Sie war unter DOS zusammen mit der `config.sys` für den Start des Systems verantwortlich und beinhaltete neben dem Start von Treibern auch ggf. Abfragen und Variablen. Das Thema Batchdateien ist sehr komplex und würde den Rahmen dieses Artikels sprengen. Die Windows-Hilfe führt mit den Ergebnissen der Suche mit dem Begriff "Batchdateien" bzw. mit der Befehlsübersicht eine Fülle von Informationen zu Batchdateien, deren Erstellung, Einsatz von Abfragen und Variablen usw. Weiterführende Links zu dem Thema finden Sie am Ende des Artikels.

Kleine Befehlsübersicht

Der klassische `help`-Befehl zeigt nur die Windows-Standardbefehle an.

Eine komplette Übersicht unter Windows XP erhalten Sie über die Windows-Hilfe (*Befehlszeilenreferenz* als Suchbegriff eingeben) oder [online](#) (Version für Windows XP).

Bei Windows Vista wurden die Inhalte leider nicht mehr in die Hilfe aufgenommen und der Link in der Onlinehilfe selbst führt ins Leere.



Befehlszeilenreferenz unter Windows XP

Klick auf Bild zum Vergrößern

Während einige Befehle ein oder mehrere Argumente und Parameter erwarten, starten andere Befehle eigenständige Programme mit weiteren Befehlen, z.B. `diskpart`.

Zu jedem Befehl können Sie die komplette Syntax mit `befehl/?` anzeigen lassen.

In der Folge haben wir zu den wichtigsten Bereichen Befehle und deren Anwendung kurz beschrieben. Die Befehle sind thematisch gruppiert. Beachten Sie bitte, dass wir nur einen kleinen Teil der Befehle hier präsentieren. Für weitere Informationen schauen Sie sich bitte für den jeweiligen Befehl die Dokumentation in der Onlinehilfe bzw. am Prompt über `befehl /?` an. Zusätzliche Angaben finden Sie auch im Abschnitt "Weiterführende Weblinks und Buchtipps" am Ende des Artikels.

Allgemeine Befehle

CLS

CLS (Clear Screen) löscht den Bildschirm innerhalb der Konsole.

Echo

Der Echo-Befehl findet häufig in Batch-Dateien Verwendung und gibt Meldungen aus oder unterdrückt diese (echo off). Im Zusammenhang mit der Abfrage von Variablen ist Echo aber auch als einfacher Befehl sehr hilfreich. So können Sie z.B. mit `echo %computername%` direkt den Namen der Arbeitsstation abfragen, mit `echo %temp%` den Temp-Pfad, mit `echo %appdata%` den Pfad für den Ordner Anwendungsdaten oder mit `echo %systemroot%` den Pfad des Windows-Verzeichnisses.



```
C:\WINDOWS\system32\cmd.exe

P:\>echo %userdomain%
WINTOTAL

P:\>echo %computername%
PENTIUM

P:\>echo %logonserver%
\\MITTELERDE
```

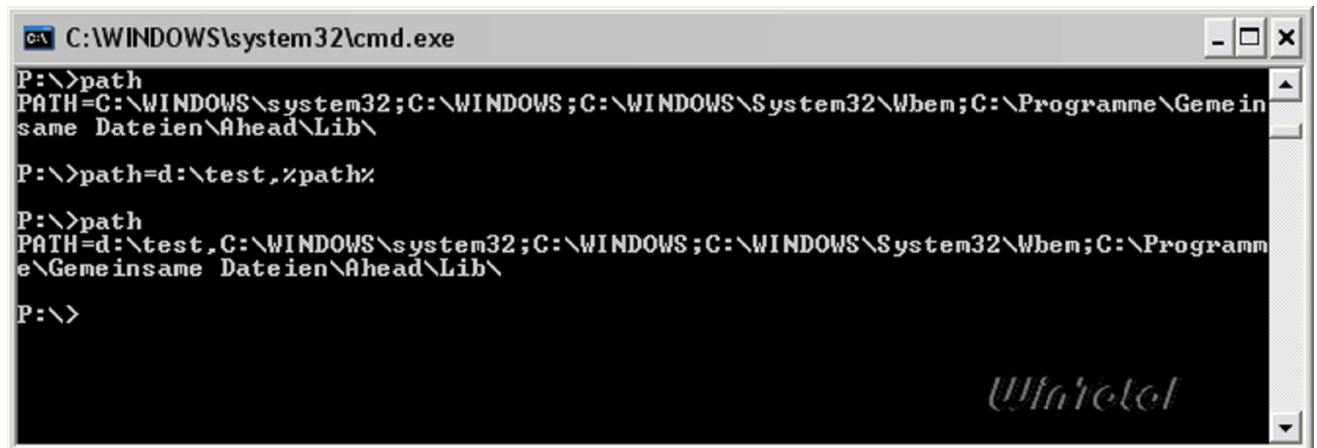
Echo

Klick aufs Bild zum Vergrößern

Eine Übersicht über alle möglichen Variablen und deren Werte erhalten Sie durch die Eingabe von `set` am Prompt (siehe weiter unten).

Path

Mit dem Path-Befehl können Sie die festgelegten Verzeichnispfade angeben, in denen die Shell nach ausführbaren Programmen sucht, wenn Sie deren Namen eingeben. `Path` ohne Angabe von Parametern gibt zunächst die Pfadangaben aus, die schon hinterlegt sind. Weitere Pfade können Sie über `path=C:\PFAD;%path%` hinzufügen. Die Angabe von `;%path%` bewirkt, dass der bisherige Pfad nicht mit dem neuen komplett überschrieben, sondern ergänzt wird. Haben Sie z.B. eigene Batchdateien im Ordner BATCH auf C:\, können Sie diesen Ordner über `path=c:\Batch;%path%` mit aufnehmen und können ab dann an jeder Stelle auf den Laufwerken die Batch-Datei starten, ohne erst in den entsprechenden Ordner zu wechseln.



```
C:\WINDOWS\system32\cmd.exe

P:\>path
PATH=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\Programme\Gene in
same Dateien Ahead\Lib\

P:\>path=d:\test,%path%

P:\>path
PATH=d:\test,C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\Programm
e\Gemeinsame Dateien Ahead\Lib\

P:\>
```

Path

Klick aufs Bild zum Vergrößern

Achtung: Sobald Sie die Shell schließen, werden die hinzugefügten Path-Pfade verworfen. Für einen dauerhaften Einsatz müssen die Path-Anweisungen daher in der Systemsteuerung unter `System -> Erweitert -> Umgebungsvariablen` angegeben werden. Sie können die Path-Anweisung hier auf den Benutzer bezogen oder systemweit festlegen.



Path systemweit setzen

Klick aufs Bild zum Vergrößern

Set

Der Set-Befehl ohne Parameter zeigt die aktuellen Umgebungsvariablen an, welche Sie auch mit [Echo](#) einzeln abfragen können.

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

P:\>set
ALLUSERSPROFILE=C:\Dokumente und Einstellungen\All Users
APPDATA=\mittel Erde\userdata$\Michael\Anwendungsdaten
CLIENTNAME=Console
CommonProgramFiles=C:\Programme\Gemeinsame Dateien
COMPUTERNAME=PENTIUM
ComSpec=C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_CHECK=NO
HOMEDRIVE=P:
HOMEPATH=\
HOMESHARE=\mittel Erde\userdata$\Michael
LOGONSERUER=\MITTELERDE
NUMBER_OF_PROCESSORS=2
OS=Windows_NT
Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\Programme\Gemeinsame Dateien Ahead\Lib\
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 15 Model 2 Stepping 9, GenuineIntel
PROCESSOR_LEVEL=15
PROCESSOR_REVISION=0209
ProgramFiles=C:\Programme
PROMPT=$P$G
SESSIONNAME=Console
SystemDrive=C:
SystemRoot=C:\WINDOWS
TEMP=d:\temp
TMP=d:\temp
USERDNSDOMAIN=WINTOTAL.LOCAL
USERDOMAIN=WINTOTAL
USERNAME=Michael
USERPROFILE=C:\Dokumente und Einstellungen\Michael
windir=C:\WINDOWS

P:\>_

```

set

Klick aufs Bild zum Vergrößern

Darüber hinaus bietet der Set-Befehl die Möglichkeit, neue Umgebungsvariablen zu setzen oder deren Wert zu überschreiben.

Reg (+Unterbefehl)

Mit dem REG-Befehl haben Sie direkt die Möglichkeit, auf die Registry von Windows zuzugreifen, Werte auszulesen, zu löschen, neu anzulegen oder zu überschreiben. Der REG-Befehl erwartet einen Unterbefehl (Reg ADD, Reg DELETE, Reg COPY, Reg QUERY...), um bestimmte Operationen im Zusammenhang mit der Registrierdatenbank auszuführen. Sie können sich für jeden Unterbefehl die genaue Syntax anzeigen lassen, z.B: **reg add /?**

```

C:\WINDOWS\system32\cmd.exe
P:\>reg add /?

Konsolenregistrierungsprogramm für Windows - Version 3.0
Copyright (C) Microsoft Corp. 1981-2001. Alle Rechte vorbehalten

REG ADD Schlüssel [/v Wert] [/ve] [/t Typ] [/s Trennzeichen] [/d Daten] [/f]

Schlüssel [ \Computer\ ] Vollst.Schlüssel
Computer Remotecomputer; ohne Standardeinstellungen des
Computer. Nur HKLM und HKU sind verfügbar.
Vollst.Schlüssel STAMMSCHLÜSSEL\Unterschlüssel
STAMMSCHLÜSSEL [ HKLM | HKCU | HKCR | HKU | HKCC ]
Unterschlüssel Vollst. Name eines Registrierungsschlüssels
unter dem STAMMSCHLÜSSEL.

/v Hinzuzufügender Wert unter dem Schlüssel.
/ve Fügt einen leeren Wert hinzu <no name>.
/t Datentypen für Registrierungsschlüssel
[ REG_SZ | REG_MULTI_SZ | REG_DWORD_BIG_ENDIAN |
REG_DWORD | REG_BINARY | REG_DWORD_LITTLE_ENDIAN |
REG_NONE | REG_EXPAND_SZ ]
Bei Auslassung wird REG_SZ verwendet
/s Bestimmt das Trennzeichen in der Datenzeichenfolge für
REG_MULTI_SZ. Bei Auslassung wird "\0" verwendet.
/d Zuzuordnende Daten für den hinzuzufügenden Registrierungswert.
/f Erzwingt das Überschreiben des vorhandenen Registrierungseintrags.

Beispiele:

REG ADD \ABC\HKLM\Software\MyCo
Fügt den Schlüssel HKLM\Software\MyCo zu Remotecomputer ABC hinzu.

REG ADD HKLM\Software\MyCo /v Data /t REG_BINARY /d fe340ead
Fügt einen Wert hinzu <Name: Data, Typ: REG_BINARY, Daten: fe340ead>.

REG ADD HKLM\Software\MyCo /v MRU /t REG_MULTI_SZ /d fax\0mail
Fügt Wert hinzu <Name: MRU, Typ: REG_MULTI_SZ, Daten: fax\0mail\0\0>

REG ADD HKLM\Software\MyCo /v Path /t REG_EXPAND_SZ /d %%systemroot%%
Fügt einen Wert hinzu <Name: Path, Typ: REG_EXPAND_SZ, Daten:
%systemroot%>.
Hinweis: Verwenden Sie das doppelte Prozentzeichen < %% > innerhalb der
Erweiterungszeichenfolge.

P:\>

```

reg add

Klick aufs Bild zum Vergrößern

Für alle Hauptschlüssel in der Registry werden mit reg folgende Abkürzungen verwendet:

- HLKLM (Hkey_Local_Machine)
- HKCU (Hkey_Current_User)
- HKCS (Hkey_Classes_Root)
- HKCC (Hkey_Current_Config)

So führt der Befehl

```
reg add HKLM\Software\Microsoft\Windows\CurrentVersion /v backuppath /t REG_SZ /d P:\storage
```

Folgendes aus:

Im Schlüssel `HKLM\Software\Microsoft\Windows\CurrentVersion` wird ein neuer Wert (`/v`) mit dem Namen `backuppath` angelegt, welcher als Datentyp (`/t`) `REG_SZ` (Zeichenfolge) den Wert (`/d`) `P:\storage` erhält.

```

C:\WINDOWS\system32\cmd.exe
P:\>reg add HKLM\Software\Microsoft\Windows\CurrentVersion /v backuppath /t REG_SZ /d P:\storage
Der Vorgang wurde erfolgreich ausgeführt.
P:\>

```

reg add Beispiel

Klick aufs Bild zum Vergrößern

Der Befehl `reg add HKLM\Software\Microsoft\Windows\CurrentVersion\backupinfo` fügt dagegen einen neuen Unterschlüssel mit dem Namen `backupinfo` ein, der zuvor noch nicht existierte.

Hinweis: Oft ist es einfacher, mit dem GUI-Programm **regedit** und dessen Schaltern `/s` für den Import bzw. `/a` für den Export Werte in die Registry einzutragen bzw. zu exportieren.

start

Mit dem Start-Befehl können Sie einen neuen Prozess aus der Shell heraus starten, im Regelfall ein Windows-Programm. Durch weitere Parameter können Sie die Priorität des Prozesses sowie ein minimiertes oder maximiertes Fenster zur Ansicht festlegen.

`start /w notepad /p datei.txt` startet beispielsweise Notepad und wartet (`/w`) auf dessen Beendigung. Der Parameter `/p` an Notepad druckt die `datei.txt`.

Dateioperationen

Cipher

Das Dateisystem NTFS bietet auch die Möglichkeit, Dateien zu verschlüsseln bzw. zu entschlüsseln. Zudem können Sie mit `cipher` auch die privaten Schlüssel und Zertifikate exportieren, um ggf. auch ohne den bestehenden Account die Daten wieder unverschlüsselt öffnen zu können. Der Parameter `/e` verschlüsselt und `/d` entschlüsselt die Dateien wieder.

Beispiel: `cipher /e c:\Privates` verschlüsselt den Ordner Privates und die darin befindlichen Ordner und Dateien

Beispiel: `cipher /e /c:\Privates *.doc` verschlüsselt alle DOC-Dateien im Ordner Privates.

Weitere Informationen zur Verschlüsselung unter Windows bietet der gesonderte Artikel „[Dateiverschlüsselung](#)“.

Caccls

Der `Caccls`-Befehl bietet die Möglichkeit, über die Shell Sicherheitseinstellungen für Dateien und Ordner zu setzen. Normalerweise bedienen Sie hierzu die Registerkarte “Sicherheit” in den Eigenschaften eines Ordners oder einer Datei. Mit `Caccls` können Sie diese Rechte aber auch über die Shell setzen – unter Windows XP Home übrigens der einzige Weg (ohne entsprechende Erweiterungen und Patches).

`Caccls e:\Dokumente*.* /p Kinder:N` entzieht beispielsweise dem Account “Kinder” alle Rechte für den Ordner Dokumente.

In der **Support.cab** (siehe Artikelende) findet sich das Kommandozeilenprogramm **Xcaccls**, welches weitere Möglichkeiten im Zusammenhang mit den Sicherheitseinstellungen bietet.

Compact

Mit dem `Compact`-Befehl können Sie die im NTFS-Dateisystem enthaltene Komprimierungsfunktion nutzen und Dateien und Ordner packen (`/c`) bzw. entpacken (`/u`). Wenn Sie ganze Verzeichnisse komprimieren möchten, lautet die Syntax: `compact /c /s c:\Privates` (für den Ordner “Privates” unter C:\).

Expand

Der `Expand`-Befehl kann Dateien aus den von Windows genutzten CAB-Dateien extrahieren.

Mit `expand -d Cab-Datei` bekommen Sie den Inhalt einer CAB-Datei angezeigt. `Expand Cab-Datei -f:Dateien Ziel` entpackt die angegebenen Dateien aus der Cab-Datei an das festgelegte Ziel.

Hinweis: Leider kann Windows selbst keine gängigen Archive (ZIP, RAR etc.) über die Kommandozeile entpacken. Hier müssen Sie sich mit Fremdmitteln helfen. Eine sehr gute Variante ist das Kommandozeilenprogramm des kostenlosen [7-Zip](#). Legen Sie den Inhalt entpackt in einen vom “Path” mit genutzten Ordner (z.B. Windows etc.). Sie können dann bequem aus der Shell heraus fast alle Archivdateien entpacken oder eigene erstellen.

```

C:\WINDOWS\system32\cmd.exe

Q:\Tools\cmds>7za

7-Zip (A) 4.42 Copyright (c) 1999-2006 Igor Pavlov 2006-05-14

Usage: 7za <command> [<switches>...] <archive_name> [<file_names>...]
      [<@listfiles...>]

<Commands>
  a: Add files to archive
  d: Delete files from archive
  e: Extract files from archive (without using directory names)
  l: List contents of archive
  t: Test integrity of archive
  u: Update files to archive
  x: eXtract files with full paths

<Switches>
  -ai[r[-!0]]<@listfile!&wildcard>: Include archives
  -ax[r[-!0]]<@listfile!&wildcard>: eXclude archives
  -bd: Disable percentage indicator
  -i[r[-!0]]<@listfile!&wildcard>: Include filenames
  -m<Parameters>: set compression Method
  -o<Directory>: set Output directory
  -p<Password>: set Password
  -r[-!0]: Recurse subdirectories
  -scs<UTF-8 | WIN | DOS>: set charset for list files
  -sfx<name>]: Create SFX archive
  -si<name>]: read data from stdin
  -slt: show technical information for l (List) command
  -so: write data to stdout
  -t<Type>: Set type of archive
  -v<Size>[b|k|m|g]: Create volumes
  -u[-!p#]!q#!r#!x#!y#!z#!!&newArchiveName]: Update options
  -w<path>]: assign Work directory. Empty path means a temporary directory
  -x[r[-!0]]<@listfile!&wildcard>: eXclude filenames
  -y: assume Yes on all queries

Q:\Tools\cmds>_
  
```

Möglichkeiten von 7za

Klick aufs Bild zum Vergrößern

Rename

Mit dem Rename-Befehl, kurz ren, können Sie auf einen Rutsch mehrere Dateien umbenennen. Dazu geben Sie z.B. *ren *.nfo *.txt* ein, um alle nfo-Dateien in txt-Dateien umzubenednen. Achtung: Eine Konvertierung in das neue Format findet aber nicht statt.

Copy

Der Copy-Befehl kopiert eine Datei in ein anderes Verzeichnis oder in dasselbe Verzeichnis, aber unter einem anderen Namen. Er eignet sich aber nicht für tieferegreifende Kopieraktionen (siehe hierfür XCopy).

copy WinTotal.txt a: (kopiert die WinTotal.txt auf das Laufwerk a)

copy WinTotal. c:\temp* (kopiert alle Dateien mit dem Namen WinTotal in das Verzeichnis c:\temp)

copy c:\temp.txt d:\windows* (kopiert alle Dateien mit der Endung txt im c:\temp-Verzeichnis in das Windows-Verzeichnis auf dem Laufwerk d)

Move

Der Windows-User würde zu diesem Befehl "Ausschneiden" sagen. Prinzipiell ist dieser Befehl mit dem copy-Befehl identisch, nur wird die Quelldatei VERSCHOBEN und nicht kopiert. *move *.* a:* alle Dateien werden zum Laufwerk a verschoben.

XCopy

Der XCopy-Befehl ist die aufgebohrte Variante des Copy-Befehls und kann ganze Verzeichnisbäume kopieren. Dazu stehen zahlreiche Parameter zur Verfügung. /e kopiert auch Unterverzeichnisse (egal ob leer oder nicht); /y unterdrückt die Aufforderung, die Datei auf dem Ziel zu überschreiben etc.

XCopy "c:\Dokumente und Einstellungen\ap73mi\Favoriten.*" "\\mittelerde\Sicherungen\ap73mi\favoriten" /e /y*

sichert z.B. alle Favoriten vom Benutzer ap73mi zum Ordner "Sicherungen/ap73mi/favoriten/" auf dem Server "Mittelerde".

Benutzer- und Clientverwaltung

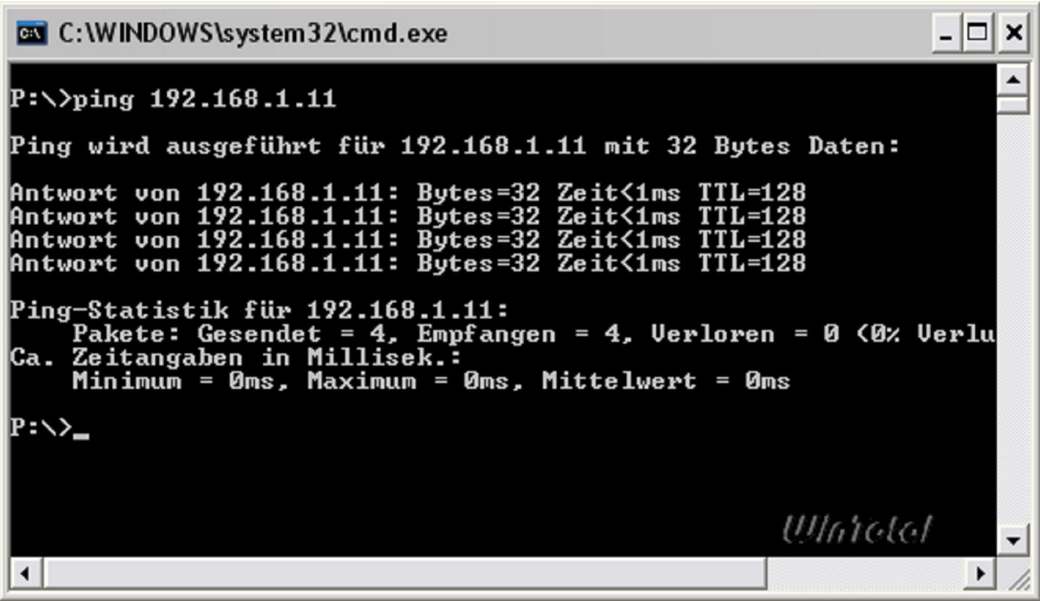
Runas

Mit dem Befehl `runas /user:Username Programm` starten Sie ein Programm im Kontext eines anderen Benutzers. Sie können mit diesem Befehl z.B. auch als eingeschränkter Benutzer ein Programm im Kontext des Administrators ausführen, ohne sich als Admin anzumelden. Ersetzen Sie hierbei Username durch den Screenname des Administrators. Das notwendige Passwort wird beim ersten Aufruf abgefragt und dann hinterlegt, wenn als Parameter noch `/savecred` mit angegeben wird.

Netzwerk

Ping

Der Ping-Befehl ist simpel, aber einer der wichtigsten zur Diagnose in Netzwerken. Mit dem Ping-Befehl senden Sie eine Anfrage an eine IP oder einen Rechnernamen. Der Befehl sendet per Default 4 Signale an die Gegenstelle, listet jede Auslieferung aus und fasst das Ganze am Ende statistisch zusammen. So können Sie schnell prüfen, ob das Netzwerk überhaupt funktioniert und beispielsweise der Router überhaupt erreichbar ist. Ein Ping zum eigenen Rechner (127.0.0.1) bringt oft Klarheit, falls der TCP/IP-Stack auf dem Rechner nicht richtig funktioniert.



```
C:\WINDOWS\system32\cmd.exe

P:\>ping 192.168.1.11

Ping wird ausgeführt für 192.168.1.11 mit 32 Bytes Daten:

Antwort von 192.168.1.11: Bytes=32 Zeit<1ms TTL=128
Antwort von 192.168.1.11: Bytes=32 Zeit<1ms TTL=128
Antwort von 192.168.1.11: Bytes=32 Zeit<1ms TTL=128
Antwort von 192.168.1.11: Bytes=32 Zeit<1ms TTL=128

Ping-Statistik für 192.168.1.11:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlu
Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms

P:\>_
```

Ping

[Klick aufs Bild zum Vergrößern](#)

Ipconfig

IPconfig zeigt die IP-Konfiguration des Rechners an. Sie sehen die lokale IP, Subnetzmaske und den Gateway, welchen im Heimnetzen meist der Router darstellt. Sehen Sie hier einen anderen Gateway oder finden den Rechner in einem anderen Adressraum über die IP, könnte eine gestörte Kommunikation mit dem Router bzw. dessen DHCP-Server vorliegen.

```

C:\WINDOWS\system32\cmd.exe

P:\>ipconfig

Windows-IP-Konfiguration

Ethernetadapter LAN-Verbindung:

    Verbindungsspezifisches DNS-Suffix: wintotal.local
    IP-Adresse . . . . . : 192.168.1.27
    Subnetzmaske . . . . . : 255.255.255.0
    Standardgateway . . . . . : 192.168.1.1

P:\>
  
```

Ipconfig

Klick aufs Bild zum Vergrößern

Der erweiterte Befehl `ipconfig /all` gibt darüber detailliert Auskunft.

```

C:\WINDOWS\system32\cmd.exe

P:\>ipconfig

Windows-IP-Konfiguration

Ethernetadapter LAN-Verbindung:

    Verbindungsspezifisches DNS-Suffix: wintotal.local
    IP-Adresse . . . . . : 192.168.1.27
    Subnetzmaske . . . . . : 255.255.255.0
    Standardgateway . . . . . : 192.168.1.1

P:\>ipconfig /all

Windows-IP-Konfiguration

    Hostname . . . . . : pentium
    Primäres DNS-Suffix . . . . . : wintotal.local
    Knotentyp . . . . . : Hybrid
    IP-Routing aktiviert . . . . . : Nein
    WINS-Proxy aktiviert . . . . . : Nein
    DNS-Suffixsuchliste . . . . . : wintotal.local
                                        wintotal.local

Ethernetadapter LAN-Verbindung:

    Verbindungsspezifisches DNS-Suffix: wintotal.local
    Beschreibung . . . . . : 3Com Gigabit NIC
    Physikalische Adresse . . . . . : 00-0C-6E-EB-7E-A6
    DHCP aktiviert . . . . . : Ja
    Autokonfiguration aktiviert . . . . . : Ja
    IP-Adresse . . . . . : 192.168.1.27
    Subnetzmaske . . . . . : 255.255.255.0
    Standardgateway . . . . . : 192.168.1.1
    DHCP-Server . . . . . : 192.168.1.11
  
```

Ipconfig /all

Klick aufs Bild zum Vergrößern

War der Rechner beim Starten noch nicht mit dem LAN verbunden, findet dieser keinen DHCP-Server und verwendet dann eine selbst gewählte IP, die nicht unbedingt im gleichen Adressraum liegen muss. Gerade bei WLAN-Verbindungen kann dies vorkommen. Um einen Neustart zu vermeiden, können Sie mit `ipconfig /renew` das System anweisen, eine neue Initialisierung vorzunehmen. Der Rechner sucht nun erneut nach einem DHCP-Server und bekommt von diesem (meist Router) eine IP-Adresse sowie die Subnetzmaske und den Gateway übermittelt.

Mit `ipconfig /release` können Sie die IP-Bindung auflösen, per Parameter auch nur für einzelne Netzwerkverbindungen, wenn der Rechner z.B. per LAN und WLAN mit anderen Netzen verbunden ist. Mit `ipconfig /flushdns` leeren Sie den DNS-Auflösungscache.

tracert

Der Tracert-Befehl erwartet eine IP oder einen Rechnernamen. Im Anschluss listet der Befehl als Ergebnis auf, welche Wege das Signal vom Rechner bis zum Ziel nimmt. Sie sehen die Anzahl der Zwischenstationen im Netz und deren Verzögerung.

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

P:\>tracert

Syntax: tracert [-d] [-h Abschnitte max] [-j Hostliste] [-w Zeitlimit]
        Zielname

Optionen:
    -d                Adressen nicht in Hostnamen auflösen
    -h Abschnitte max  Max. Anzahl an Abschnitten bei Zielsuche
    -j Hostliste       "Loose Source Route" gemäß Hostliste
    -w Zeitlimit       Zeitlimit in Millisekunden für eine Antwort

P:\>tracert wintotal.de

Routenverfolgung zu wintotal.de [213.133.111.171] über maximal 30 Abschnitte:

  1  <1 ms    <1 ms    <1 ms    192.168.1.1
  2  41 ms    79 ms    43 ms    217.0.118.44
  3  39 ms    38 ms    39 ms    87.186.240.250
  4  41 ms    41 ms    41 ms    f-ee2.F.DE.net.DTAG.DE [62.154.15.14]
  5  44 ms    44 ms    70 ms    dtag-gw.hetzner.de [193.159.226.2]
  6  45 ms    45 ms    44 ms    hos-bb1.juniper1.rz4.hetzner.de [213.239.240.200]
  7  45 ms    44 ms    44 ms    et.1.16.rs3k4.rz3.hetzner.de [213.239.244.6]
  8  45 ms    45 ms    44 ms    wintotal.de [213.133.111.171]

Ablaufverfolgung beendet.

P:\>_
  
```

tracert

Klick aufs Bild zum Vergrößern

netstat

Mit dem Befehl netstat listet die Shell alle aktiven Netzwerkverbindungen mit Angabe von Protokoll, Remoteadresse, Port und Status auf. Mit dem Parameter `-a` listet Netstat alle Protokolle und serverseitigen Verbindungen auf, `netstat -n` listet dagegen die Verbindungen mit numerischen IP-Adressen statt Rechnernamen auf.


```

C:\WINDOWS\system32\cmd.exe
P:\>netstat -a

Aktive Verbindungen

Proto Lokale Adresse Remoteadresse Status
TCP pentium:epmap pentium.wintotal.local:0 ABHÖREN
TCP pentium:microsoft-ds pentium.wintotal.local:0 ABHÖREN
TCP pentium:2869 pentium.wintotal.local:0 ABHÖREN
TCP pentium:3678 pentium.wintotal.local:0 ABHÖREN
TCP pentium:1042 pentium.wintotal.local:0 ABHÖREN
TCP pentium:2738 localhost:2739 HERGESTELLT
TCP pentium:2739 localhost:2738 HERGESTELLT
TCP pentium:2740 localhost:2741 HERGESTELLT
TCP pentium:2741 localhost:2740 HERGESTELLT
TCP pentium:nethios-ssn pentium.wintotal.local:0 ABHÖREN
TCP pentium:1059 mittelerte.wintotal.local:nethios-ssn HERGEST
LT
TCP pentium:3680 64.12.28.64:5190 HERGESTELLT
TCP pentium:3682 64.12.25.8:5190 HERGESTELLT
TCP pentium:3683 oam-d20c.blue.aol.com:5190 HERGESTELLT
TCP pentium:4013 p5482D394.dip.t-dialin.net:ftp SCHLIESSEN_WAR
N
TCP pentium:4196 212.243.221.222:http HERGESTELLT
UDP pentium:microsoft-ds **:
UDP pentium:isakmp **:
UDP pentium:1025 **:
UDP pentium:1026 **:
UDP pentium:1040 **:
UDP pentium:1529 **:
UDP pentium:3708 **:
UDP pentium:4500 **:
UDP pentium:ntp **:
UDP pentium:1027 **:
UDP pentium:1046 **:
UDP pentium:1900 **:

```

netstat -a

Klick aufs Bild zum Vergrößern

Sie können die Ausgabe auch auf bestimmte Protokolle (UDP, TCP) beschränken, netstat -n -p tcp, listet z.B. nur die TCP-Verbindungen auf.

```

C:\WINDOWS\system32\cmd.exe
P:\>netstat -n -p tcp

Aktive Verbindungen

Proto Lokale Adresse Remoteadresse Status
TCP 192.168.1.27:1062 192.168.1.11:139 HERGESTELLT
TCP 192.168.1.27:1181 62.245.236.178:80 HERGESTELLT
TCP 192.168.1.27:1414 194.64.234.118:80 SCHLIESSEN_WARTEN
TCP 192.168.1.27:1415 212.162.62.43:80 ZULETZT_ACK
TCP 192.168.1.27:1423 194.97.107.23:80 WARTEND
TCP 192.168.1.27:1424 194.97.107.23:80 WARTEND
TCP 192.168.1.27:1425 85.214.47.214:80 WARTEND
TCP 192.168.1.27:1429 195.157.98.220:80 SCHLIESSEN_WARTEN
TCP 192.168.1.27:1430 80.87.128.122:80 SCHLIESSEN_WARTEN
TCP 192.168.1.27:1433 212.162.62.43:80 SCHLIESSEN_WARTEN

```

netstat nur TCP

Klick aufs Bild zum Vergrößern

net (+Unterbefehl)

Der net-Befehl ist einer der mächtigsten Konfigurationsbefehle unter Windows für das Netzwerk. Mit dem net-Befehl können Sie Dateifreigaben oder Benutzerkonten beeinflussen, Informationen über das Netzwerk abrufen und vieles mehr.

Mit `net help` erhalten Sie eine Auflistung aller Unterbefehle und `net UNTERBEFEHL help` zeigt letztlich die benötigten Parameter an.

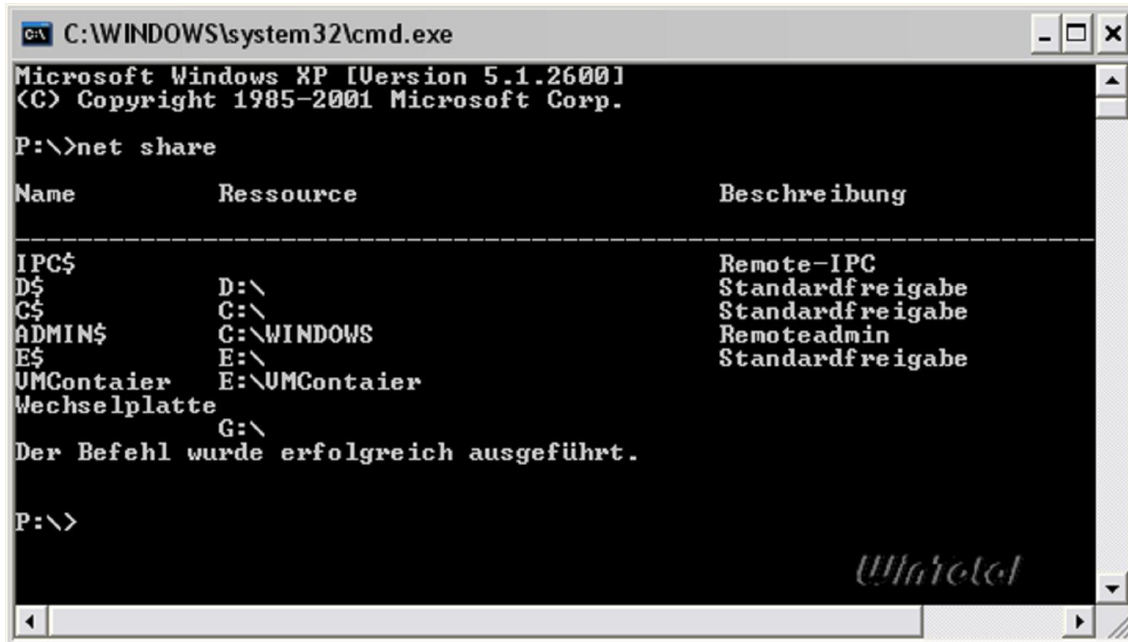
Interessant sind hierbei die zahlreichen Unterbefehle, z.B.

Net time (Zeitverwaltung)

Net user, localgroup, group (Benutzerverwaltung)
 Net share, use, file, session (verwaltet Dateifreigaben)
 Net config, statistics, view (Informationen zum Netz und Netzdiensten)
 Net start, pause, continue, stop (Konfiguration der Windows-Dienste)
 Net send (Mitteilungen im Netzwerk versenden)
 Net computer (Rechner in Domäne aufnehmen)

Beispiele:

Net share zeigt alle Freigaben an.



```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

P:\>net share

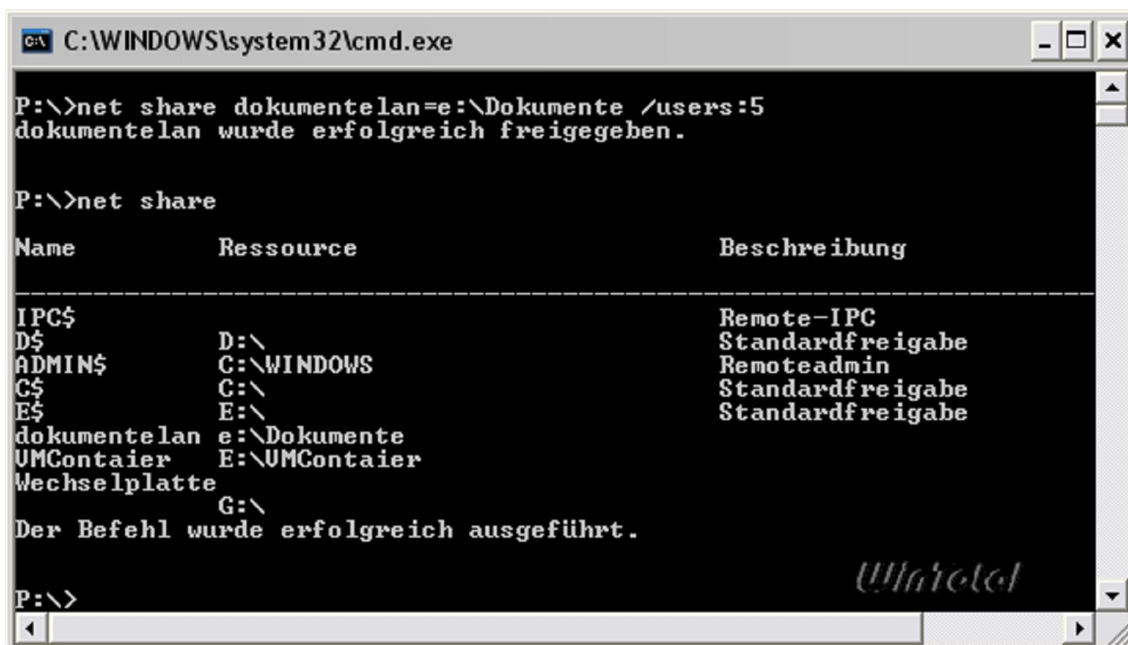
Name                Ressource            Beschreibung
-----
IPC$                 Remote-IPC
D$                   D:\                  Standardfreigabe
C$                   C:\                  Standardfreigabe
ADMIN$               C:\WINDOWS          Remoteadmin
E$                   E:\                  Standardfreigabe
UMContaier          E:\UMContaier
Wechselplatte       G:\
Der Befehl wurde erfolgreich ausgeführt.

P:\>
  
```

net share

Klick aufs Bild zum Vergrößern

Mit *net share dokumentelan=e:\Dokumente /users:5* wird der Ordner e:\Dokumente im Netzwerk als „dokumentelan“ für maximal 5 User gleichzeitig freigegeben.



```

C:\WINDOWS\system32\cmd.exe

P:\>net share dokumentelan=e:\Dokumente /users:5
dokumentelan wurde erfolgreich freigegeben.

P:\>net share

Name                Ressource            Beschreibung
-----
IPC$                 Remote-IPC
D$                   D:\                  Standardfreigabe
ADMIN$               C:\WINDOWS          Remoteadmin
C$                   C:\                  Standardfreigabe
E$                   E:\                  Standardfreigabe
dokumentelan       e:\Dokumente
UMContaier          E:\UMContaier
Wechselplatte       G:\
Der Befehl wurde erfolgreich ausgeführt.

P:\>
  
```

net share

Klick aufs Bild zum Vergrößern

net use q:\mittelerde\public bindet die Freigabe public auf dem Server Mittelerde als Laufwerk Q in das System ein.

Mit der Ergänzung */delete* wird die Bindung von use oder die Freigabe von share wieder aufgehoben.

Zusätzlich kann als Option noch */savecred* bei *net use* und *net share* dazu benutzt werden, um die Anmeldeinformationen zur Nutzung der Freigabe zu speichern. Beim erneuten Herstellen der Verbindung müssen die Anmeldeinformationen dann nicht mehr angegeben werden.

Informationen

sc

Der net-Befehl kann zwar auch auf die Dienste Einfluss nehmen, sc bietet aber weitere Funktionen. Mit dem sc-Befehl haben Sie weitreichenden Zugriff auf die Windows Services und Dienste. Sie können sich mit sc beispielsweise alle laufenden Dienste anzeigen lassen, deren Startverhalten ändern usw.

Sc query state= all listet z.B. alle installierten Dienste auf. Hier finden Sie auch die Zuordnung des internen Dienstnamens zur Bezeichnung in der Computerverwaltung. Der interne Name wird benötigt, wenn man Dienste mit *net stop dienstname* stoppen oder den Start eines Dienstes mit *sc config dienst start= disabled* verhindern möchte.

Getmac

Wer einen WLAN-Router betreibt, kann meist in einer MAC-Liste dort festlegen, welche Clients sich verbinden dürfen. Die MAC-Adresse des WLAN-Adapters erfahren Sie mit dem Befehl getmac. Die Ausgabe kann über Parameter auch formatiert werden.

Systeminfo

Mit dem simplen Befehl *Systeminfo* gibt die Shell relevante Informationen zum verwendeten System aus. Sie erfahren dort neben Angaben zum Netzwerk und dem verwendeten System auch Angaben zum Computer selbst sowie zu installierten Hotfixes. Die Ausgabe kann über Parameter auch formatiert werden und eignet sich zur Ausgabe in eine Datei (z.B. *systeminfo /fo csv >c:\logfile\systeminfo.txt* gibt eine CSV-Liste aus).

```

C:\WINDOWS\system32\cmd.exe

P:\>systeminfo

Hostname: PENTIUM
Betriebssystemname: Microsoft Windows XP Professional
Betriebssystemversion: 5.1.2600 Service Pack 2 Build 2600
Betriebssystemhersteller: Microsoft Corporation
Betriebssystemkonfiguration: Mitglied der Domäne/Arbeitsgruppe
Buildtyp von Betriebssystem: Multiprocessor Free
Registrierter Benutzer: Michael Appelt
Registrierte Organisation: Redaktion WinTotal
Produktkennung:
Ursprüngliches Installationsdatum: 19.12.2005, 15:31:02
Systembetriebszeit: 0 Tage, 5 Stunden, 13 Minuten, 43 Sekunden
Systemhersteller: To Be Filled By O.E.M.
Systemmodell: To Be Filled By O.E.M.
Systemtyp: X86-based PC
Prozessor(en): 2 Prozessor(en) installiert.
[01]: x86 Family 15 Model 2 Stepping 9
[02]: x86 Family 15 Model 2 Stepping 9
enuineIntel ~2598 MHz
enuineIntel ~2598 MHz
BIOS-Version: A M I - 9000420
Windows-Verzeichnis: C:\WINDOWS
System-Verzeichnis: C:\WINDOWS\system32
Startgerät: \Device\HarddiskVolume1
Systemgebietsschema: de;Deutsch (Deutschland)
Eingabebereichsschema: de;Deutsch (Deutschland)
Zeitzone: Nicht verfügbar
Gesamter physikalischer Speicher: 1.535 MB
Verfügbarer physikalischer Speicher: 1.012 MB
Virtueller Speicher: Maximale Größe: 2.048 MB
Virtueller Speicher: Verfügbar: 2.008 MB
Virtueller Speicher: Zurzeit verwendet: 40 MB
Auslagerungsdateipfad(e): D:\pagefile.sys
  
```

Systeminfo

Klick aufs Bild zum Vergrößern

Tasklist

Mit dem Tasklist-Befehl bekommen Sie alle laufenden Prozesse mit der ProzessID (PID) in einer Liste angezeigt. Mit dem Parameter */M* bekommen Sie auch die zu jedem Prozess geladenen DLLs angezeigt, mit */V* sehen Sie weitere Informationen wie den Benutzerkontext des Prozesses.

Abbildname	PID	Sitzungsname	Sitz.-Nr.	Speichernutzung
System Idle Process	0	Console	0	16 K
System	4	Console	0	220 K
smss.exe	932	Console	0	400 K
csrss.exe	1048	Console	0	5.508 K
winlogon.exe	1832	Console	0	3.924 K
services.exe	1880	Console	0	3.384 K
lsass.exe	1892	Console	0	1.660 K
svchost.exe	1272	Console	0	5.152 K
svchost.exe	1368	Console	0	4.024 K
svchost.exe	1504	Console	0	23.436 K
svchost.exe	1568	Console	0	3.644 K
svchost.exe	1776	Console	0	7.324 K
BRS021A.EXE	1716	Console	0	1.224 K
BRS031A.EXE	1932	Console	0	2.156 K
spoolsv.exe	1952	Console	0	7.240 K
schedu12.exe	420	Console	0	1.704 K
LSExec.exe	608	Console	0	2.548 K
hed32kui.exe	692	Console	0	24.252 K
msvc32.exe	704	Console	0	3.624 K
RichView.exe	728	Console	0	2.796 K
svchost.exe	848	Console	0	5.524 K
alg.exe	1812	Console	0	3.964 K
explorer.exe	2528	Console	0	32.620 K
TrueImageMonitor.exe	3276	Console	0	3.092 K
schedhlp.exe	3480	Console	0	2.556 K
daemon.exe	3424	Console	0	3.324 K
CIHELPER.EXE	3752	Console	0	6.304 K
svchost.exe	4828	Console	0	3.408 K
svchost.exe	468	Console	0	2.368 K
hed32kui.exe	532	Console	0	1.628 K
svchost.exe	1124	Console	0	3.664 K
ctfmon.exe	000	Console	0	4.004 K
DesktopSearchService.exe	720	Console	0	14.556 K
psd.exe	1484	Console	0	9.052 K
Paint.exe	1168	Console	0	3.000 K
GhostTrp.exe	1782	Console	0	9.012 K
FSNGive.exe	2828	Console	0	4.440 K
NINMUORD.EXE	616	Console	0	127.332 K
OUTLOOK.EXE	3212	Console	0	70.224 K
cmd.exe	2688	Console	0	2.632 K
Snagit32.exe	4068	Console	0	12.884 K
tschli.exe	3200	Console	0	36.076 K
Snagit32.exe	1336	Console	0	2.344 K
tasklist.exe	3952	Console	0	4.480 K
uniprvse.exe	2124	Console	0	5.620 K

Tasklist

Klick aufs Bild zum Vergrößern

Tasklist unterstützt auch Filter für Abfragen und formatierte Ausgaben. Zudem können Sie auch die Tasks von entfernten Rechnern im LAN abfragen oder mit `taskkill` beenden (siehe folgend).

Gerade in einer Batch-Datei kann es interessant sein, diese Ausgabe in eine Datei umzuleiten und diese Datei dann mittels `find` auf bestimmte Prozesse überprüfen zu lassen.

Über `taskkill /im` kann dann der gefundene Prozess abgeschossen werden.

Taskkill

Der Befehl `Taskkill` ergänzt den Befehl `tasklist`. Mit dem Parameter `/PID ID` können Sie einen Prozess unter Angabe der Prozess-ID beenden. Alternativ können Sie auch `taskkill /im` angeben, um den Prozess zu beenden.

Shutdown

Vor einigen Jahren gab es einen Virus, welcher den Rechner durch einen Programmfehler nach 30 Sekunden automatisch herunterfuhr. Mit dem Befehl `shutdown -a` können Sie ein Herunterfahren abbrechen oder mit `shutdown -s` herunterfahren. `shutdown -r` startet den Rechner neu. Der Parameter `-f` beendet die laufenden Programme ohne Rückfrage. Der Befehl `Shutdown` lässt sich auch auf andere Rechner im LAN anwenden. Die Syntax für einen Reboot eines Netzwerkrechners lautet dann `shutdown -r -m//immerkiste`.

Assoc

Der `Assoc`-Befehl listet ohne Parameter alle registrierten Erweiterungen und den dazu gehörenden Dateityp auf. Wenn Sie den `Assoc`-Befehl mit einer Erweiterung angeben, erhalten Sie den Dateityp – z.B. `Assoc .doc`. Wenn Sie `assoc` mit dem Dateityp angeben, erhalten Sie die erweiterte Angabe zu dem Dateityp.

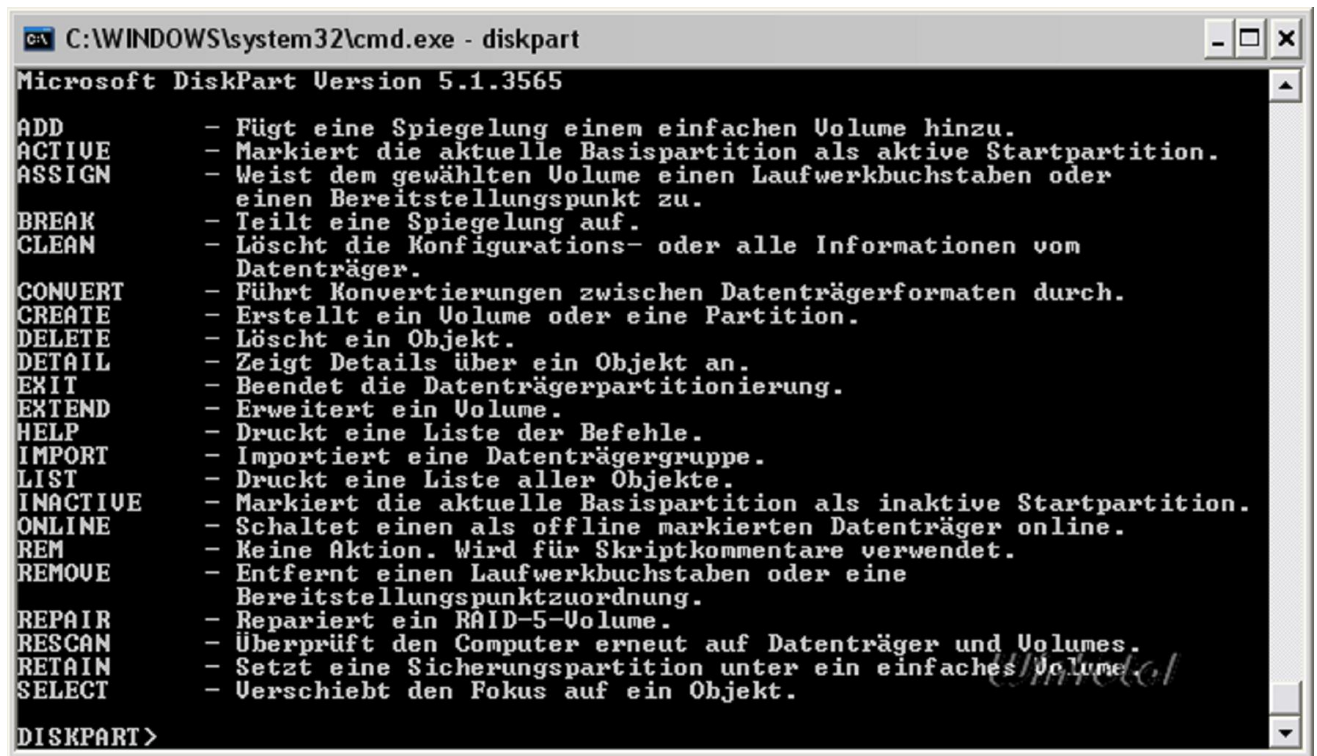
Driverquery

Mit `Driverquery` erhalten Sie eine Liste aller installierten Geräte und Systemtreiber. Mit dem Parameter `/V` wird die Auflistung noch etwas ausführlicher.

Laufwerksmanagement

Diskpart

Diskpart ist kein Befehl, sondern ein eigenständiges Programm zur Verwaltung von Datenträgern. Mit Diskpart können Sie Partitionen erstellen und löschen, Partitionen aktiv setzen, Basis-Datenträger in dynamische Datenträger konvertieren usw.



```

C:\WINDOWS\system32\cmd.exe - diskpart
Microsoft DiskPart Version 5.1.3565

ADD          - Fügt eine Spiegelung einem einfachen Volume hinzu.
ACTIVE      - Markiert die aktuelle Basispartition als aktive Startpartition.
ASSIGN      - Weist dem gewählten Volume einen Laufwerksbuchstaben oder
              einen Bereitstellungspunkt zu.
BREAK       - Teilt eine Spiegelung auf.
CLEAN       - Löscht die Konfigurations- oder alle Informationen vom
              Datenträger.
CONVERT     - Führt Konvertierungen zwischen Datenträgerformaten durch.
CREATE      - Erstellt ein Volume oder eine Partition.
DELETE      - Löscht ein Objekt.
DETAIL      - Zeigt Details über ein Objekt an.
EXIT        - Beendet die Datenträgerpartitionierung.
EXTEND      - Erweitert ein Volume.
HELP        - Druckt eine Liste der Befehle.
IMPORT      - Importiert eine Datenträgergruppe.
LIST        - Druckt eine Liste aller Objekte.
INACTIVE    - Markiert die aktuelle Basispartition als inaktive Startpartition.
ONLINE      - Schaltet einen als offline markierten Datenträger online.
REM         - Keine Aktion. Wird für Skriptkommentare verwendet.
REMOVE      - Entfernt einen Laufwerksbuchstaben oder eine
              Bereitstellungspunktzuordnung.
REPAIR      - Repariert ein RAID-5-Volume.
RESCAN     - Überprüft den Computer erneut auf Datenträger und Volumes.
RETAIN      - Setzt eine Sicherungspartition unter ein einfaches Volume.
SELECT      - Verschiebt den Fokus auf ein Objekt.

DISKPART>
  
```

Diskpart

Klick aufs Bild zum Vergrößern

[Unter Windows Vista können Sie mit Diskpart sogar Partitionen nachträglich in der Größe verkleinern.](#)

Convert

Externe Festplatten sind häufig mit FAT32 formatiert. Mit dem convert-Befehl können Sie das Dateisystem z.B. auf NTFS ändern, ohne das Laufwerk neu formatieren oder die Daten darauf erst sichern zu müssen. Der Befehl `convert e: /fs:ntfs` konvertiert das Laufwerk E in das dem Dateisystem NTFS.

Defrag

Mit dem Befehl Defrag kann die interne Defragmentierung über die Shell gestartet werden. Der Parameter `-a` gibt den Grad der Fragmentierung an. `-f` erzwingt die Defragmentierung auch bei wenig verfügbarem Festplattenspeicher.

Subst

Der Subst-Befehl gerät langsam in Vergessenheit, ist aber gerade bei fehlgeleiteten Installern immer wieder eine Hilfe.

Mit dem Subst-Befehl können Sie einen beliebigen Pfad als weiteres Laufwerk in Windows einbinden.

`Subst k: d:\temp` bindet z.B. den Pfad `d:\temp` als virtuelles Laufwerk K ein. Die Anwendungsgebiete solcher Laufwerke sind ganz verschieden. In der Praxis kommt es aber immer wieder mal vor, dass ein Installer oder Uninstaller auf ein Laufwerk zugreifen will, welches gar nicht mehr existiert, aber vielleicht mal dar war. In diesen Fällen kann der Subst-Befehl helfen, indem man z.B. den Temp-Pfad einfach auf das gewünschte Laufwerk legt.

Mit `Subst ohne Parameter` bekommen Sie alle virtuellen Laufwerke angezeigt und der Parameter `/d` hebt die Zuordnung wieder auf.

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

P:\>subst
P:\>subst /?
Weist einem Pfad eine Laufwerkbezeichnung zu.

SUBST [Laufwerk1: [Laufwerk2:]Pfad]
SUBST Laufwerk1: /D

Laufwerk1:      Laufwerkbezeichnung, die dem Pfad zugewiesen werden soll.
[Laufwerk2:]Pfad Laufwerk und Pfad, die durch Laufwerk1: angesprochen
                  werden sollen.
/D              Hebt die Zuordnung für das (virtuelle) Laufwerk1 wieder auf.

SUBST ohne Parameter zeigt die mit SUBST erstellten, virtuellen Laufwerke an.

P:\>subst k: d:\temp
P:\>K:
K:\>dir
Datenträger in Laufwerk K: ist Temp
Volumeseriennummer: F9F2-0662

Verzeichnis von K:\

03.12.2007  17:34    <DIR>          .
03.12.2007  17:34    <DIR>          ..
26.11.2007  22:42             104.857.600  1.h2t
26.10.2007  20:16             31.232  26adj966.doc

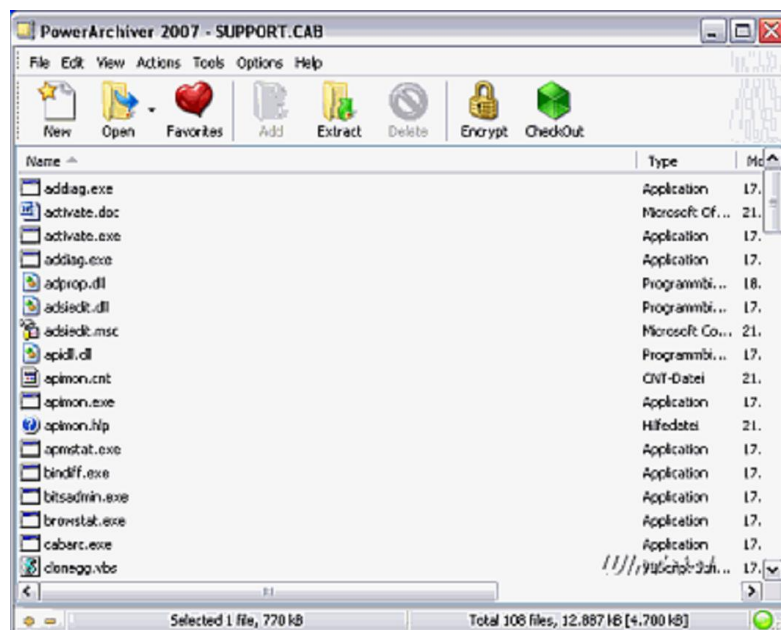
```

subst

Klick aufs Bild zum Vergrößern

Weitere Befehle in der Support.cab

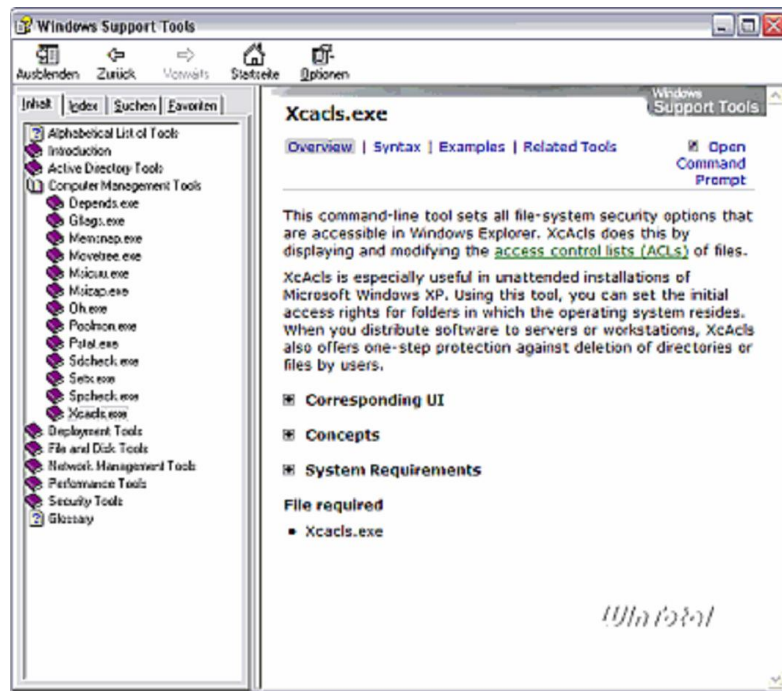
Auf der Windows XP-CD befindet sich im Ordner *SupportTools* die Datei *support.cab*. Sie enthält weitere Hilfsprogramme, von denen einige auch in der Kommandozeile laufen. Man erkennt diese EXE-Dateien am "einfachen"-Programmicon. Kopieren Sie diese Dateien in einen Ordner, welcher von den Pfad-Angaben erfasst wird, damit Sie auf diese Befehle von jeder Stelle des Systems zugreifen können.



support.cab

Klick aufs Bild zum Vergrößern

Eine Beschreibung der Support-Tools finden Sie in der Datei *supptools.chm* innerhalb der *support.cab*.



suptools.chm

Klick aufs Bild zum Vergrößern

Der hier beschriebene Befehl **xcaccls.exe** ist beispielsweise die erweiterte Variante von **cacls.exe** und bietet wesentlich mehr Möglichkeiten zur Verwaltung der Sicherheitseinstellungen.

Weitere Tools

Microsoft bietet noch weiteres Futter für CMD-Freunde, z.B. die **Windows Server 2003 Resource Kit Tools**. Sie beinhalten eine Sammlung von Tools – speziell für Administratoren – für die Registry, Active Directory und sonstiges. Viele der Befehle lassen sich auch unter Windows 2000, XP und Vista einsetzen. [Download über WinTotal](#).

In der Toolsammlung ist auch **Robocopy** enthalten, welches sich auch unter Windows 2000 und XP nutzen lässt. Wir haben einen gesonderten [Artikel zum Tool Robocopy auf WinTotal](#).

Ergänzende Downloads

Die **Sysinternals-Tools** wurden vor einiger Zeit von Microsoft übernommen. Auf der neuen Eingangsseite sind diese thematisch zusammengefasst und werden auch als Suite (nicht alle Programme enthalten) zum Download angeboten. Neben vielen Helferlein mit einer GUI finden sich auch Perlen für den Einsatz in der Kommandozeile: [Link zu Microsoft Sysinternals](#).

Die **GNU Utilities for Win32** erweitern die Kommandozeile von Windows um viele aus dem Unix-Umfeld bekannte Tools, darunter auch Befehle zum Packen und Entpacken von RAR- und ZIP-Archiven etc.

Damit die Befehle bequem aus der CMD gestartet werden können, sollten diese nach dem Entpacken aus dem Ordner `usr\local\wbin` in ein Systemverzeichnis kopiert oder optional der Pfad der GNU utilities in die Path-Anweisung mit aufgenommen werden.

Weiterführende Weblinks

- <http://www.ss64.com/nt/>
- <http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/ntcmds.mspx?mfr=true>
- <http://de.wikibooks.org/wiki/Batch-Programmierung>
- [Microsoft Command-line Reference – A-Z List](#)

Buchtipps

- [Windows-Befehle für XP & Server 2003 – kurz & gut](#)
- [Windows Befehle für Vista und Server 2003](#)
- [Windows PowerShell – kurz & gut](#)
- [Windows 2003 Shell Scripting](#)

- [Scripting für Administratoren](#)
- [Microsoft Windows-Befehlszeilenverwaltung](#)

Tags: **BEFEHLE** **CMD** **DOSKEY** **EINGABEAUFFORDERUNG** **KOMMANDOZEILE** **POWERSHELL** **PROMPT**
SHELL

© 2014 WinTotal.de