* **Windows:**
  + - Unter Windows ist den Dateisystemen ein Laufwerksbuchstabe zugeordnet, wie C:, D: oder X:. Jeder Buchstabe steht für ein Dateisystem.
    - Jedes Dateisystem hat ein Stammverzeichnis, dem alle Verzeichnisse in diesem Dateisystem untergeordnet sind.
    - Unterverzeichnis von C: wird mit einem umgekehrten Schrägstrich markiert. Also C:\.
    - Es gibt auch versteckte Dateien. Sehen kann man die: >Ansicht > Ausgeblendete Elemente.
    - Infos zu Dateien: Rechter Mausklick > „Eigenschaften“ > „Allgemein“: Dateiname, Dateityp, die Anwendung mit der die Datei geöffnet wird und den Pfad, wo die Datei zu finden ist, die Dateigröße (tatsächliche Datenmenge) und die Größe auf dem Datenträger. Wann wurde die Datei erstellt, wann zuletzt geändert und zuletzt aufgerufen. Ebenfalls kann man einstellen ob die Datei Schreibgeschützt sein soll und ob es eine Versteckte Datei sein soll.
    - Weiter kann man oben die Tabs „Sicherheit“, „Details“ und „Vorgängerversionen“ sehen.
    - **Windows (PowerShell):**
    - Unter Windows gibt es zwei Befehlszeilen, sogenannte CLIs: „Command Prompt: cmd.exe“ und „PowerShell: powershell.exe“
    - Viele PowerShell-Befehle sind Aliasse für gängige Befehle in anderen Shells. Alias = Spitzname für einen Befehl.
    - **Aufrufen der PowerShell-CLI:** Suche in der Anwendungsliste nach „PowerShell“ > „Windows PowerShell“ starten.
    - Dateien und Verzeichnisse auflisten: „**Ls**“ oder „**list directory**“ und den entsprechenden Pfad: „ls C:\Users\user\Desktop“
    - Der Pfad ist nicht Teil des Befehls, sondern ein **Befehlsparameter.** Ein Parameter ist ein Wert, der den Befehl näher beschreibt.
  + **Windows: Zwei wichtige Pfadtypen:**
    - Absolute Pfade beginnen im Hauptverzeichnis.
    - Ein relativer Pfad, ist der Pfad vom aktuellen Verzeichnis
  + **Windows: Ändern von Verzeichnissen in der Befehlszeilenschnittstelle:**
    - Mit dem Befehl „cd“ können wir in ein anderes Verzeichnis wechseln.
    - Dazu müssen wir den Pfad eingeben, zu dem wir wechseln möchten.
    - Wechsel mit einem absoluten Pfad:

„cd C:\Benutzer\cindy\Dokumente

* + - Wechsel mit einem relativen Pfad:

„cd ..“ oder „cd ..\Cindy“

* + - Es gibt eine integrierte Funktion: Vervollständigung mit der TAB-Taste. Damit werden Dateinamen und Verzeichnisse automatisch vervollständigt.
  + **Windows: Erstellen Sie Verzeichnisse in der GUI & CLI:**
    - Mit dem Befehl „mkdir“ und dem Namen deines neuen Verzeichnisses, erstellst du einen neuen Ordner.
    - „mkdir Projekt\_Trainee“
    - Bei dem Ordnernamen sind keine Leerzeichen erlaubt.
    - Stattdessen kann man: mkdir „Projekt Trainee“ oder mkdir Projekt` Trainee`
  + **Windows: Befehlsverlauf:**
    - Funktion „history“
    - Mit den Pfeiltasten kann man hier nach oben scrollen und einen Befehl erneut ausführen oder ihn verändert ausführen.
  + **Windows: Kopieren von Dateien und Verzeichnissen:**
    - Cp = Kopieren
    - Man kann mit Platzhalterzeichen mehrere Dateien nach einem bestimmten Muster auswählen.
    - Wenn wir alle PDF Dateien in einem Ordner Kopieren wollen:

Cp \*.pdf C:\ Zielpfad“. Das „\*“ steht für „irgendwas“. Also suche alle Dateien, die .pdf enthalten.

* + - Möchte ich etwas bestimmtes Kopieren: „cp „Name der Datei oder des Verzeichnisses“ C:\ Zielpfad“
    - Kopieren wir einen Ordner mit dem Befehl „cp“, wird der Inhalt nicht mit kopiert.
    - Dafür muss man einen Befehlsparameter verwenden: „cp „Name der Datei oder des Verzeichnisses“ C:\ Zielpfad –Recurse -Verbose“
  + **Windows: Verschieben und Umbenennen von Dateien, Verzeichnissen:**
    - Zum Umbenennen benutze ich den Befehl „mv“
    - „mv .\blue\_document.txt yellow\_document.txt“
    - Damit habe ich die Datei “Blue\_document.txt” umbenannt in “yellow\_document.txt”
    - „mv .\yellow\_document.txt C:\Zielordner\“
    - Damit habe ich die Datei in einen anderen Ordner verschoben
    - Das geht auch mit \*. Also „mv \*\_document.txt C:\Zielordner“
  + **Windows: Entfernen von Dateien und Verzeichnissen:**
    - Zum Löschen „rm“
    - Rm ~\Dateiname
    - Bei wichtigen Dateien, haben nur autorisierte Nutzer haben die Berechtigung zu löschen.
    - Bei Berechtigung muss man „rm ~\Importen-file **–force**“ eingeben, um die Datei zu löschen.
    - Wenn ich ein ganzes Verzeichnis löschen möchte, fragt PowerShell nach, ob man sich sicher ist. Oder man benutzt **„-Recurse**“, dann weiß Powershell, dass man sich dem bewusst ist und fragt nicht mehr nach.
  + Windows: Anzeigen vom Dateiinhalt:
    - Mit „more“ oder „cat“
    - Bei „more“ = Mit der Eingabetaste wird der Dateiinhalt um eine Zeile weiterbewegt. Mit der Leertaste wird die Datei um eine Seite weitergeblättert. Mit „q“ verlassen sie „more“ und gelangen zurück zu „Shell“
* **Aliasse und echte Befehle:**
  + Aliasse sind Spitznamen für echte Befehle. Man muss weniger schreiben und kommt somit schneller ans Ziel.
  + Es gibt nicht für alle Befehle einen Alias
  + Oder man benutzt cmd.exe-Befehle
  + Cmd.exe-Befehle sind Befehle aus dem früheren MD-DOS von Windows.
* **GUI-Optionen:**
  + Unter Windows gibt es den Windows-Suchdienst.
  + Dieser sieht die Dateien auf deinem Computer regelmäßig durch.
  + Daraufhin erstellt er eine Liste in einer Datenbank, mit Namen und Eigenschafen der gefundenen Dateien.
  + Da dieser Dienst sehr Zeit- und Arbeitsaufwendig ist, ist dieser bei den meisten nicht installiert oder deaktiviert.
  + Standartmäßig suchen Sie mit dem Windows-Suchdienst Dateien nach deren Namen, dem Pfad, der letzten Änderung, der Größe oder anderen Details. Standartmäßig ist aber keine wortsuche in diesen Dateien möglich.
  + Um den Dienst zu aktivieren: Suche nach Indizierung > Indizierungsoption > Benutzer > Erweitert > Dateitypen > Eigenschaften und Dateiinhalte indizieren > ok
  + Nun kann ich in meinem Benutzerverzeichnis nach Dateien, die ein bestimmtes Wort enthalten suchen.
  + Dies kann ich ebenso in Notepad++ machen.
* Notizen:
  + Es gibt 3 verschiedene I/O-Streams: stdout, stdin, stderr
  + > = Umleitungsoperator. Mit ihm lässt sich die Standartausgabe weiterleiten.
  + | = Pipe-Operator. Die Ausgabe eines Befehls an die Eingabe eines anderen Befehls senden. (Ausgabeumleitung)
  + Stderr = I/O-Umleiter. (Input/Output-Umleiter).
  + Alle Ausgabestreams werden nummeriert:

1. Stdout – für Standartausgabe (the output)
2. Stderr – Standartfehler/ Fehlermeldungen (the error)
   * Mit dem I/O-Umleiter können erwartete Standartfehlermeldungen umgeleitet werden.
   * Diesen kann man auf „$null“ umleiten. Ins nichts sozusagen ins schwarze Loch.
   * „rm Dateiname 2>$null“

* **Übersicht Befehle (Cmdlets) für Powershell:**

|  |  |
| --- | --- |
| Befehlsaliasse | Bedeutung |
| Ls oder list directory | Dateien und Verzeichnisse auflisten |
| Get-Help Ls | Eine Beschreibung der Parameter des Is-Befehls |
| Get-Help Ls –Full | Detailliertere Beschreibung der Parameter des Is-Befehls |
| Ls -Force | Versteckte Dateien sehen |
| Pwd oder print working directory | Gibt an, in welchem Verzeichnis man sich gerade befindet |
| Cd oder change directory | Wenn man ein anderes Verzeichnis aufrufen möchte |
| Cd .. | Man geht in das übergeordnete Verzeichnis. (z.B. von „C:\User\Sarah\Dokumente“ in „C:\Unser\Sarah“) |
| Cd ~ | Pfad des Basisverzeichnisses. |
| Mkdir oder make directory | Neues Verzeichnis erstellen |
| History | Zeigt mir eine Liste von den zuvor eingegebenen Befehlen an |
| STRG + R oder # | Den Verlauf Ihrer bisher verwendeten Befehle durchsuchen. |
| Clear | Damit wird nicht der Verlauf, sondern nur die Bildschirmausgabe gelöscht. |
| CP oder Copie Paste | Kopieren |
| \* | Irgendwas. |
| -Recurse | Führt den Verzeichnisinhalt auf |
| -Verbose | In Verbindung mit cp. Also cp-Verbose, wird für jedes kopierte Verzeichnis eine Zeile ausgegeben. |
| Mv oder Move/ moveItem | Damit kann man Dateien umbenennen oder verschieben |
| Rm oder remove | Löschen von Dateien oder Verzeichnissen |
| Cat | Damit wird der Inhalt einer Datei angezeigt |
| More | Zeigt den Dateiinhalt an. Seite für Seite indem er immer eine Leerzeile zeigt, wo eine Seite zuende ist. „more“ ist ein eigenes Programm. Mit der Eingabetaste wird der Dateiinhalt um eine Zeile weiterbewegt. Mit der Leertaste wird die Datei um eine Seite weitergeblättert. Mit „q“ verlassen sie „more“ und gelangen zurück zu „Shell“ |
| -Head | Zeigt mir den Anfang einer Datei (cat Dateiname –Head 10) Zeigt mir die ersten 10 Zeilen der Datei an. |
| -Tail | Zeigt mir das Ende einer Datei an (cat Dateiname –Tail 10) letzten 10 Zeilen. |
| Start Notepad++ | Startet den Notepad++ Editor mit der gewünschten Datei. (Start Notepad++ Dateiname) |

|  |  |
| --- | --- |
| Echte Befehle | Bedeutung |
| Get-Help | Mehr Informationen zu Befehlen. |
| Get-Alias | Welcher echter PowerShell-Befehl ausgeführt wird. |
| Get-ChildItem (ls) | Listet wie „ls“ die Verzeichnisse und Dateien auf |
| Get-Command | Sie sehen alle PowerShell Befehle aller Module, die momentan in Ihrem System verfügbar sind. |
| Sls oder select-string | Wörter, Zeichenfolge oder Dateien suchen. |
| -Filter | Ls „C:\Program Files\“ -Recurse –Filter \*.exe = Zeigt mir alle .exe Dateien an. Der –Filter filtert nach Dateinamen. |
| Echo (Alias) für Write-Output | Gibt die Tastatureingabe auf dem Bildschirm wieder. So fügt man Wörter einer Datei zu?! |
| Get-Help about\_redirection |  |
| Get-localUser | Auflistung der Nutzerkonten. |
| Get-localGroup | Auflistung der Gruppen auf dem lokalen Computer |
| Get-LocalGroupMember | Kann man sehen wer alles in einer Gruppe drin ist. (z.B. in der Benutzer Gruppe) Get-LocalGroupMember Benutzer |
| Net | Passwort ändern |
| /logonpasswordchg: yes | Damit kann man einstellen, dass ein bestimmter Nutzer sein Passwort beim nächsten Anmelden ändern soll. |
| New-LocalUser | Neuen Benutzer hinzufügen |
| /add |  |
| icacls | Ich kann sehen, welche Nutzerkonten Zugriff auf meinen Desktop haben |
| Icacls Zielordner /grant ‚Everyone: (OI(CI)(R)‘ | Jemanden den Zugriff auf Dateien erlauben. Everyone steht dafür, dass jeder die Berechtigung bekommen soll. Statt Everyone Authenticated Users für einen bestimmten Benutzer. |
| Compress-Archive -Path | Ein Archiv erstellen (ZIP) |
| Get-PackageSource | Prüfen ob Softwarequellen Startklar sind |
| Install-Package | Sysinternals und die entsprechenden Abhängigkeiten tatsächlich installieren |
| Find-Package sysinternals –includeDependencies |  |
| Get-Package | Prüfen, ob ein installiertes Packet vorhanden ist |
| Uninstall-Package –name | Paket Deinstallieren |
| Diskpart | Öffnen die Festplatte |
| List disk | Auflistung der Platte (Speicherplatz) |
| Select disk | Wir wählen eine Festplatte aus |
| Create partition primary | Eine leere Partition für unser Dateisystem wird erstellt |
| Active | Markieren |
| Format FS=NTFS label=name quick | Formatierung eines Datenträgers mit dem Filesystem NTFS. USB-Laufwerk |
| Mklink | Symbolischen link erzeugen (Einen Shortcut, der lesbar für Shell ist) (Linux=Softlink) |
| Mklink /H | Hardlink erstellen. Hardlinks bleiben bestehen, selbst wenn das Original sich ändert oder gelöscht wird. |
| /F | Prüfung, etwaige Probleme zu beheben |
| Smss.exe (Session Manager Subsystem) | Dieser Prozess, richtet einige Elemente ein, die das Betriebssystem benötigt. |
| Winlogon.exe | Anmeldeprozess |
| Csrss.exe (Client/Server Runtime Subsystem) | Er sorgt für die Ausführung der Benutzeroberfläche und der Befehlszeile |
| Taskkill | Damit lässt sich ein Prozess auffinden und auf mehrere Arten anhalten |
| Ps –x | Man sieht eine Liste aller auf dem System ausgeführten Prozesse. (l. n. r. > **PID** = Prozess-ID; **TTY** =das mit dem Prozess verknüpfte Terminal; **STA**=Prozessstatus(R=running, T=stopped, S=interruptible sleep); **TIME**=die gesamte CPU-Zeit, die ein Prozess bisher in Anspruch genommen hat; **COMMAND**=Name des Befehls, welcher ausgeführt wird.) |
| Ps –ef | „e“= werden alle Prozesse abgerufen, auch die von anderen Nutzern. „f“ zeigt die gesamten Details zu einem Prozess. (l. n. r. **UID**=Nutzer-ID der Person, die den Prozess gestartet hat; **PID**=Prozess-ID; **PPID**=die ID des bergeordneten Prozessen; **C**=Anzahl der diesem Prozess untergeordneten Prozesse; **STIME**=ist die Startzeit des Prozesses; **TTY**=das mit dem Prozess verknüpfte Terminal; **TIME**=die gesamte CPU-Zeit, die ein Prozess bisher in Anspruch genommen hat; **CMD**=Name des ausgeführten Befehls.) |
| Ps –ef I grep | Ob ein Prozess ausgeführt wird |
| SIGINT (signal interrupt) | Signalunterbrechung (strg + C) |
| Get-Desk-Prozess |  |
| Process Explorer | Um laufende Prozesse zu prüfen |
| Get-Process | Informationen zu jedem aktuell vom System ausgeführten Prozess. |
| Get-Process I Sort CPU –descending I Select –first 3 –property ID, ProcessName, CPU | So sieht man die 3 Hauptverbraucher von CPU-Systemressourcen |
| Eventvwr.msc (In Suchen eingeben) | Protokoll des Computers |