

Bedienungsanleitung SimpleBackup

Version 2.0.5

Thomas Agustoni

1. Inhaltsverzeichnis

1. Inhaltsverzeichnis.....	1
2. Was ist SimpleBackup?	1
3. Installation	2
4. Erster Start von SimpleBackup	2
5. Weitere Parameter zum Backup-Lauf	3
6. Konfiguration	4
7. Viewer	4
8. Beeinflussung Backup-Lauf	5
9. Dateien verschieben und umbenennen	7
10. Systemvoraussetzungen	7

2. Was ist SimpleBackup?

SimpleBackup ist eine Backup-Software mit diesen Eigenschaften:

- Das Backupmedium ist eine normale (von Vorteil externe) Harddisk oder ein USB-Stick, welche(r) mit NTFS formatiert sein muss.
- SimpleBackup erstellt pro Backup-Lauf eine vollständige Datensicherung (full backup) und legt die zugehörigen Daten pro Lauf in einem separaten Verzeichnis auf dem Backupmedium ab. Damit kann man später Daten ohne spezielle Software wiederherstellen, indem man sich den gewünschten Backupstand vom Backupmedium mit herkömmlichen Werkzeugen (z. B. Windows Explorer) kopiert.
- Auch wenn SimpleBackup eine vollständige Datensicherung erstellt, sind die gespeicherten Datenmengen moderat. Genaugenommen sichert SimpleBackup nur neue Dateien. Bestehende werden einfach als sogenannter „Hard Link“ auf das Backupmedium geschrieben. „Hard Links“ sind Dateiverweise, wo zwei oder mehr vermeintlich unabhängige Dateien (bzw. eben Dateiverweise) auf denselben Inhalt zeigen. Ändert man den Inhalt einer solchen Datei, ändert automatisch auch der Inhalt der anderen Datei. Windows bietet die Eigenschaft von „Hard Links“ nicht offiziell an, auch wenn diese mit direktem Zugriff auf Systemroutinen angelegt werden können. Dazu muss der verwendete Datenträger zwingend mit NTFS formatiert sein; FAT bietet diese Möglichkeit nicht.
- Es empfiehlt sich, das Backupmedium zu verschlüsseln, so dass bei dessen Verlust niemand auf die darauf gespeicherten Daten zugreifen kann. SimpleBackup unterstützt den Einsatz von TrueCrypt oder VeraCrypt (Verschlüsselungssoftware, Open Source).

3. Installation

setup.exe

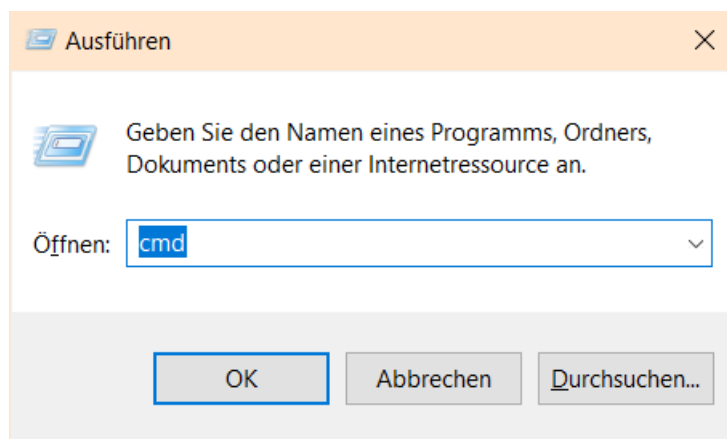
installiert SimpleBackup. Während der Installation muss SimpleBackup.Setup.msi im selben Verzeichnis wie setup.exe liegen.

4. Erster Start von SimpleBackup

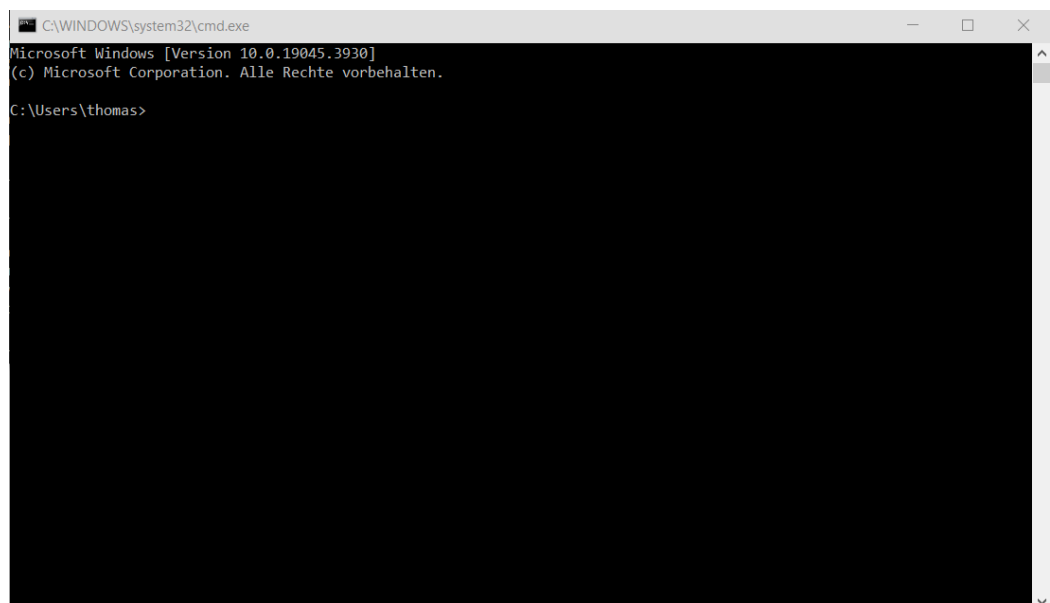
SimpleBackup.CommandLine

startet SimpleBackup ab der Kommandozeile. Ein Kommandozeilenfenster (Command Shell) öffnet man am einfachsten mit

<Win>-R



cmd<Return>



```
>cd /d C:\Program Files\Thomas\SimpleBackup2
```

wechselt in das Programmverzeichnis. Deutsche Windowsversionen verwenden „Programme“ anstelle von „Program Files“.

```
>SimpleBackup.CommandLine.exe
```

startet SimpleBackup ohne Parameter, womit nur die Parameterliste angezeigt wird. Ein sinnvoller Backup-Start sieht beispielsweise so aus:

```
>SimpleBackup.CommandLine.exe -s D:\Daten -t P:\Backup --gui --hide
```

Damit werden die Dateien aus D:\Daten (-s) nach P:\Backup (-t) gesichert. --gui zeigt grafisch den Sicherungsverlauf an und --hide verbirgt die Kommandozeile, bis das Sicherungsfenster geschlossen wird.

Kommandozeilenprompt Das Zeichen > in den obenstehenden (und auch nachfolgenden) Anweisungen muss nicht getippt werden. Es steht stellvertretend für den ganzen Kommandozeilenprompt, beispielsweise für

```
C:\Program Files\Thomas\SimpleBackup2>
```

Start automatisieren Hat man das passende Startkommando inkl. Parameter gefunden, legt man es am besten in einer Batch-Datei ab, so dass man den Backuplauf jederzeit auf die gleiche Art starten kann. Legt man eine Verknüpfung zu dieser Batch-Datei auf dem Desktop ab, braucht man nur noch darauf zu klicken, um den Backuplauf zu starten.

5. Weitere Parameter zum Backup-Lauf

Den Backup-Lauf startet man ab der Kommandozeile:

```
>SimpleBackup.CommandLine -s sourceDir -t targetDir
```

Mehrere Quell- und Zielverzeichnisse schreibt man am besten in eine Datei und bindet sie mit -f ein:

```
[Source]
D:\Daten
D:\Install
```

```
[Backup]
P:\Backup
```

SimpleBackup unterstützt die Verschlüsselung des Ziel-Laufwerkes mit TrueCrypt oder VeraCrypt. Mit der Anweisung --autoenc muss der Benutzer vor dem Backup-Lauf das Passwort für die Entschlüsselung eingeben. SimpleBackup kümmert sich darum, dass das Ziel-Laufwerk unter dem passenden Laufwerksbuchstaben (hier: P:) eingebunden wird. Dazu benötigt SimpleBackup einige Angaben, siehe nachfolgend im Abschnitt „Konfiguration“.

Ein Viewer, der den Backup-Fortschritt anzeigt, lässt sich mit --gui auch gleich starten:

```
>SimpleBackup.CommandLine -f StartBackupFiles.txt --autoenc --gui
```

6. Konfiguration

%userprofile%\AppData\Roaming\SimpleBackup2

enthält die Konfigurationsdatei SimpleBackup2-Settings.xlsx und Log-Dateien. Die Konfigurationsdatei gibt

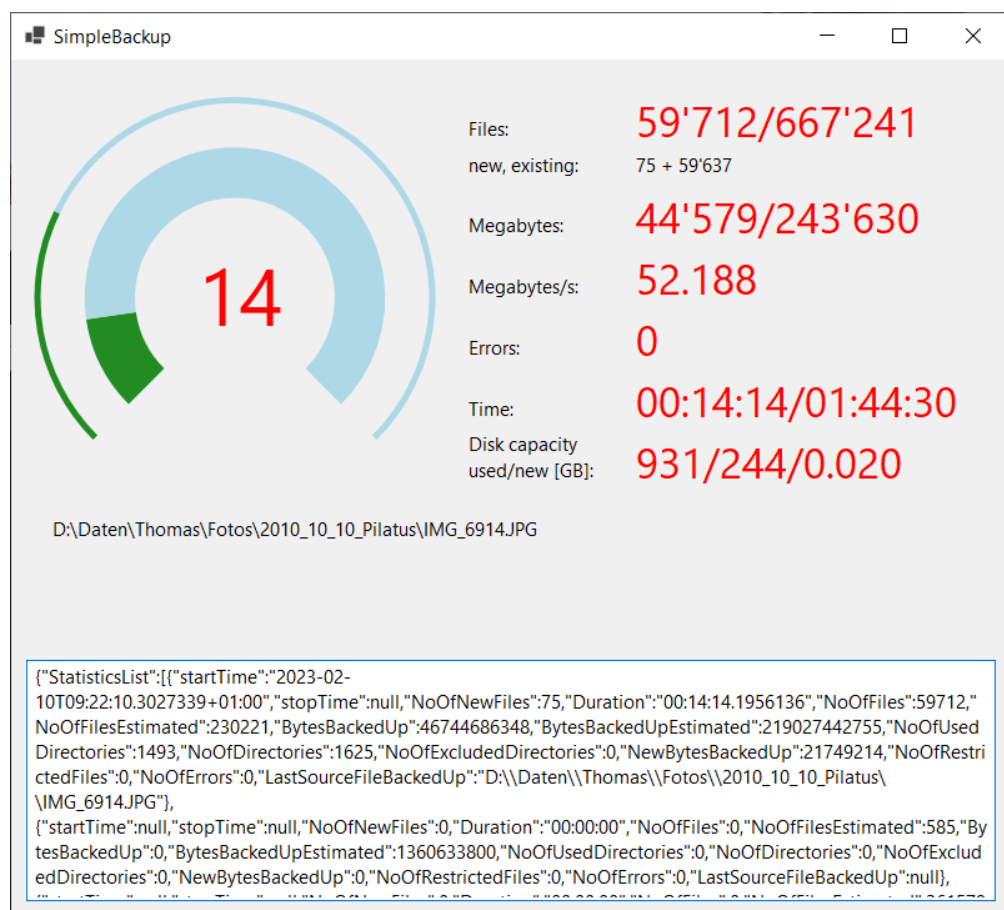
- im Arbeitsblatt „Backup“ Auskunft über erledigte Backup-Läufe.
- Das Arbeitsblatt „Volume“ enthält die Seriennummern externer Ziel-Laufwerke. SimpleBackup verwendet für TrueCrypt oder VeraCrypt die dort notierten Volumes (z. B. \Device\Harddisk2\Partition1 oder einfach nur Partition1). Soll TrueCrypt verwendet werden, ist das ebenfalls einzutragen. Andernfalls verwendet SimpleBackup VeraCrypt.

%userprofile%\AppData\Roaming\SimpleBackup2\SourceTarget

enthält Dateien, die Quell- und Zielverzeichnisse festlegen. SimpleBackup sucht -f spezifizierte Dateien zuerst im Startverzeichnis. Wenn sie dort nicht existieren, sucht SimpleBackup im globalen Verzeichnis SourceTarget.

7. Viewer

Der SimpleBackup.Viewer zeigt den Backup-Fortschritt an. Er lässt sich direkt oder mit Hilfe des Kommandozeilenparameters --gui (siehe oben) starten. Das ist auch möglich, wenn der Backup-Lauf bereits gestartet ist.



Das Viewer-Fenster ist gleichzeitig mit dem Kommandozeilenfenster sichtbar. Letzteres lässt sich bei Bedarf mit `--hide` verbergen. Wenn nach Abschluss des Backup-Prozesses der Viewer geschlossen wird, erscheint das Kommandozeilenfenster wieder. Mit `--hidegui` verschwindet der Viewer im Tray. Mit dem Parameter `--quitgui` wird das Viewer-Fenster automatisch geschlossen, sobald der Backup-Prozess beendet ist.

Solange der Backup-Prozess läuft, verschwindet der Viewer im Tray, falls man ihn schliesst oder auf die Taste `<Esc>` drückt. Von dort kann er auch wieder geöffnet werden.

8. Beeinflussung Backup-Lauf

siba.conf

SimpleBackup bietet die Möglichkeit, mit Konfigurationsdateien das Backup-Verhalten zu steuern. So können beispielsweise einzelne Dateien vom Backup-Prozess ausgeschlossen werden. Dazu legt man im Verzeichnis der betroffenen Datei zusätzlich eine Konfigurationsdatei `siba.conf` an, welche die Ausschluss-Anweisungen enthält. Der Inhalt von `siba.conf` bezieht sich nur auf Dateien und Verzeichnisse, die im gleichen Verzeichnis wie `siba.conf` liegen. Natürlich sind beispielsweise bei einem ausgeschlossenen Verzeichnis auch dessen Inhalt inkl. Unterverzeichnissen ausgeschlossen. Verfügbar sind folgende Optionen:

```
exclude [Dateiname|Verzeichnis]
```

Diese Anweisung schliesst die angegebene Datei bzw. das angegebene Verzeichnis (inkl. Unterverzeichnissen) vom Backup-Prozess aus.

```
include [Dateiname|Verzeichnis]
```

Diese Anweisung schliesst die angegebene Datei bzw. das angegebene Verzeichnis (inkl. Unterverzeichnissen) in den Backup-Prozess ein. Andere Dateien und Verzeichnisse sind damit ausgeschlossen. Sobald `siba.conf` eine einzige `include`-Anweisung enthält, werden allfällige `exclude`-Anweisungen ignoriert.

Mit `exclude`-Anweisungen lässt sich `siba.conf` nur ausschliessen, wenn die Datei ohne den Einsatz von Wildcards ausgeschlossen wird. Bei der Verwendung von `include`-Anweisungen ist sie immer eingeschlossen.

```
restrict [Dateiname] </d:3 /w:1 /m:1 /y:1000>
```

Diese Anweisung beschränkt die Anzahl gesicherter Dateistände auf eine bestimmte Anzahl Versionen. Die optionalen Parameter `d`, `w`, `m` und `y` legen fest, wieviele Versionen erhalten bleiben sollen. `d:3` beispielsweise weist SimpleBackup an, von der angegebenen Datei die drei neusten Tagesversionen zurückzubehalten. Alle anderen Versionen werden gelöscht. Dazu erstellt SimpleBackup intern eine Liste mit den Tagen, an welchen eine Sicherung durchgeführt wurde. Von dieser Liste wählt SimpleBackup im oben erwähnten Beispiel die jüngsten drei Tage und innerhalb eines Tages - falls pro Tag mehrere Backups vorliegen - die jeweils neuste Tagesversion aus. Alle anderen Versionen werden dann noch auf Wochen-, Monats- und Jahresanweisungen geprüft. Die am Schluss verbleibenden, d. h. nicht markierten Dateien werden gelöscht.

`/d:x` x: Anzahl neuster Tagesläufe, welche aufbewahrt werden sollen
Defaultwert: 3

`/w:x` x: Anzahl neuster Wochenläufe, welche aufbewahrt werden sollen
Defaultwert: 1

`/m:x` x: Anzahl neuster Monatsläufe, welche aufbewahrt werden sollen
Defaultwert: 1

/y:x x: Anzahl neuester Jahresläufe, welche aufbewahrt werden sollen
Defaultwert: 1000, d. h. in jedem Jahr soll eine Version erhalten bleiben

Die Defaultwerte gelten dann, wenn ein expliziter Wert fehlt, beispielsweise:

```
restrict [Dateiname] /d /y
```

Die Anweisung `restrict` funktioniert auch im Nachhinein noch. Sobald sie erfasst ist, stellt SimpleBackup sicher, dass nur die gewünschte Anzahl Versionen der betroffenen Datei erhalten bleibt.

```
process [Dateiname] [Verarbeitungsname] -unlock
    [Befehl]
    [Befehl]
...
```

Diese Anweisung führt die spezifizierten Befehle (eingerückt mit einem Tabzeichen) durch, bevor die angegebene Quelldatei gesichert wird. Damit lassen sich beispielsweise gesperrte Dateien vor der Sicherung entsperren. Eine SQLite-Datenbank, die in Gebrauch ist, kann wegen der Dateisperre nicht gesichert werden. Der Kommandozeilenbefehl `sqlite3 abc.sqlite ".backup abc-back.sqlite"` öffnet `abc.sqlite` und erstellt davon die konsistente Kopie `abc-back.sqlite`. Letztere lässt sich sichern. Für diesen Fall empfiehlt sich folgende Anweisung in `siba.conf`:

```
process *.sqlite %1.%guid1 -unlock
    sqlite3 %1 ".backup %1.%guid1"
```

`*.sqlite`: Der Befehl soll auf alle diese Dateien im aktuellen Verzeichnis angewendet werden.

`%1` steht für den Namen der aktuellen Datei, z. B. `abc.sqlite`.

`%guid1` steht für eine GUID, die pro Datei neu generiert wird. Es stehen `%guid1` bis `%guid9` zur Verfügung.

Der Parameter `-unlock` weist SimpleBackup an, den Befehl `sqlite3...` nur auszuführen, falls die Quelldatei gesperrt ist.

Für `abc.sqlite` heisst das:

- `sqlite3 abc.sqlite ".backup abc.sqlite.a293865fnjiowd"`
- Sichere `abc.sqlite.a293865fnjiowd` nach `Backup\...\abc.sqlite`
- Lösche `abc.sqlite.a293865fnjiowd`

SimpleBackup ignoriert Zeilen in `siba.conf`, welche nicht mit `exclude`, `include`, `restrict` oder `process` beginnen. Ebenso wird in einer Zeile sämtlicher Text ab einem Rautezeichen (`#`) ignoriert. Somit ist es möglich, Kommentare einzufügen.

`exclude/include/process` erlauben Wildcards (`*`, `?`); bei `restrict` werden sie ignoriert.

`exclude/restrict/process` (nicht aber `include`) unterstützen die Option `-r`. Damit werden die Regeln auch in den Unterverzeichnissen angewendet.

desktop.ini

Unter Windows gibt es Sonderverzeichnisse, die speziell gekennzeichnet sind. Dazu gehört beispielsweise „Eigene Dateien“, in welchem normalerweise die eigenen Daten abgelegt sind. Oft möchte man genau diese Daten sichern. Auf dem Sicherungsmedium legt SimpleBackup Zielverzeichnisse an, die mit dem Sicherungsdatum benannt sind, z.B. 2015-05-21-23-58-41. Weil nun „Eigene Dateien“ ein Sonderverzeichnis ist, wird Windows auch 2015-05-21-23-58-41 als Sonderverzeichnis betrachten und im Explorer nur „Eigene Dateien“ darstellen. Damit werden sich mit der Zeit auf dem Sicherungsmedium viele gleichnamige Verzeichnisse anhäufen, was unübersichtlich ist.

Dieses Problem lässt sich lösen, indem man die Datei desktop.ini im Verzeichnis „Eigene Dateien“ mit Hilfe von siba.conf vom Sicherungsvorgang ausschliesst. Dazu trägt man dort `exclude desktop.ini` ein.

9. Dateien verschieben und umbenennen

Es ist möglich, Dateien im Quellverzeichnis beliebig zu verschieben oder umzubenennen. SimpleBackup sucht auf dem Backupmedium nach Dateien mit gleichem Inhalt, auch wenn diese in einem anderen Unterverzeichnis oder unter einem anderen Namen abgelegt sind. Stimmt der Inhalt überein, legt SimpleBackup wiederum zwischen den beiden identischen Dateien einen „Hard Link“ an.

Damit der Suchaufwand für SimpleBackup nicht zu gross wird, beschränkt sich die Suche nach identischen Dateien auf die letzten drei Backup-Läufe.

10. Systemvoraussetzungen

- Windows 10
- TrueCrypt 7.1 oder VeraCrypt installiert, falls Verschlüsselung erwünscht