

**Letzte größere Änderung: 28.05.2007 (Letzte kleinere: 13.06.07) (Vorgenommene Änderungen/Erweiterungen siehe changelog)**

**1) Einleitende Worte**

**2) Installation**

**a) Download & Installation**

**b) Deutsche Sprachdatei downloaden & einbinden**

**3) Mithilfe von Truecrypt Volumen erstellen**

**a) Normale Volumen**

**b) Versteckte Volumen**

**4) Volumen einbinden und öffnen**

**a) Normale Volumen**

**b) Versteckte Volumen**

**5) Traveller Mode (Truecrypt mobil)**

**6) Batch Dateien (Starten von Truecrypt automatisieren)**

**a) Einfache Batch Datei, zum starten eines Volumens mit Windows start**

**b) Programm zum starten beliebig vieler Volumen mit Windows start**

**c) Bessere Batch Datei zum variablem starten von (fast) beliebig vielen Volumen(inarbeit)**

**7) Allgemeines**

**8) Header sichern (evtl. letzte Rettung für Daten)**

**9) Probleme und Lösungen**

**10) Ausblick zum Tutorial (kommende Ergänzungen ect.), rechtliches & Changelog**

**1) Einleitende Worte**

Zur Bedeutung und Wichtigkeit von Verschlüsselung heutzutage muss ich den meisten von euch vermutlich nichts mehr sagen, trotzdem möchte ich einige an die verlieren, welche immer noch der Meinung sind sie hätten "nichts zu verbergen":

**Spoiler:**

Damit ich nie mehr Sätze wie "Ich würde ja gern verschlüsseln, aber das ist soooo kompliziert." hören muss, liefere ich hiermit die DAU freundliche "Verschlüsselung mit Truecrypt" Anleitung.

Für ultimative Sicherheit sollte eine Vollverschlüsselung eingesetzt werden ([Anleitung Vollverschlüsselung mit DCPPE](#)) in Kombination mit Truecrypt. Warum dies am besten ist könnt ihr [\\*hier\\*](#) nachlesen.

An alle die "einfach nur verschlüsseln wollen":

Um einen Container zu erstellen dessen Inhalt verschlüsselt ist reicht es 2),3)a) und 4)a) durchzugehen. Der Rest der Anleitung ist für alle mit gehobenen Ansprüchen und für eine einfache Verschlüsselung nicht notwendig.

## 2) Installation

### a) Truecrypt Download & Installation

**Spoiler:**

[Truecrypt](#) runterladen! ([Offizielle Website](#))

Die neuste Version für Windows gibt es [\\*hier\\*](#).

Zum entpacken der Datei wird ein [Zip Entpacker](#) benötigt wie beispielsweise [Winzip \(download\)](#)

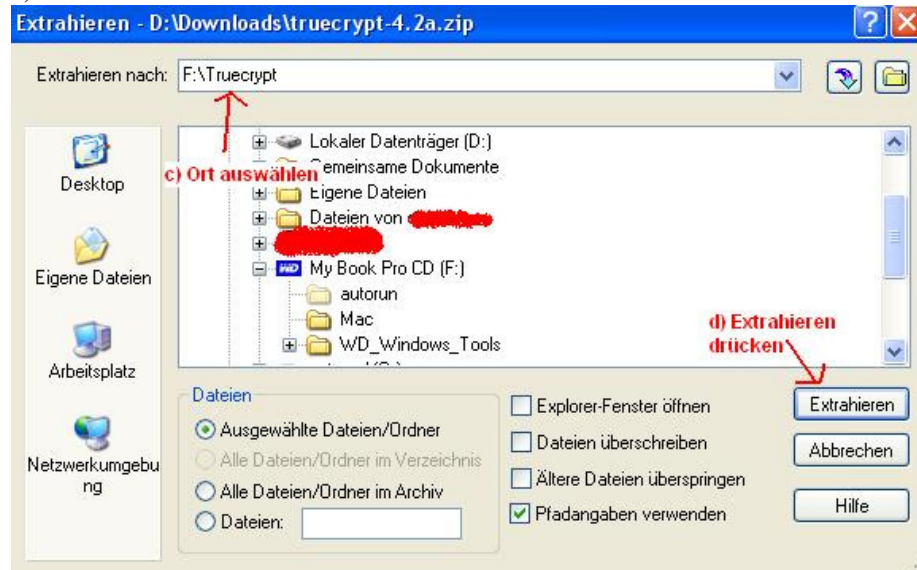
a) Alle Dateien markieren

b) Extrahieren (Entpacken) drücken



c) Ziel auswählen in welches Truecrypt entpackt werden soll

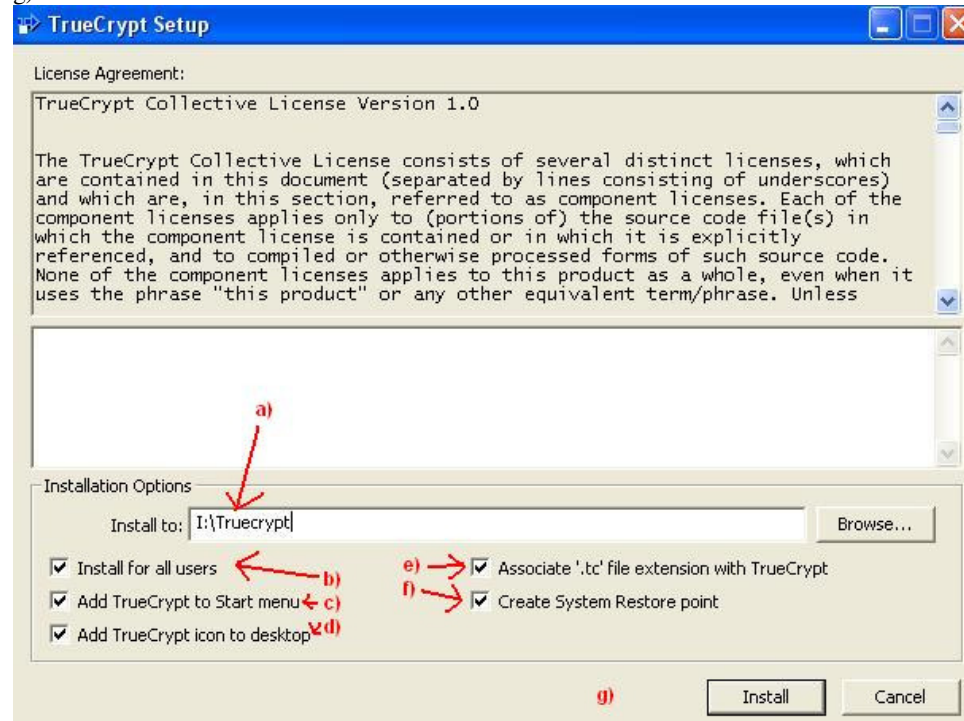
d) extrahieren drücken



Nun geht es ans installieren, geht in das Verzeichnis in welches ihr Truecrypt entpackt habt und startet die "TrueCrypt Setup.exe"

Als erstes sollte man die License Agreement lesen (und verstehen!)

- Das Ziel in welches Truecrypt installiert werden soll eingeben
- sollen alle Benutzer des Computers in den Genuss von Truecrypt kommen?
- Soll ein Startmenü eintrag erstellt werden?
- oder ein Desktopverknüpfung?
- aktivieren, damit .tc Dateien automatisch mit Truecrypt geöffnet werden (empfehlenswert)
- ebenfalls aktivieren, damit man (sollte mal etwas schiefgehen) sein System wieder reparieren kann
- Install drücken!



Nach erfolgreicher Installation die Nachricht darüber mit OK quittieren und das Installationsprogramm mit Exit beenden!

Sowohl die Zip Datei welche wir zuerst heruntergeladen haben, als auch die Dateien die wir entpackt haben, brauchen wir nun nicht mehr und können gelöscht werden.

## b) Sprachdatei Downloaden & Einbinden

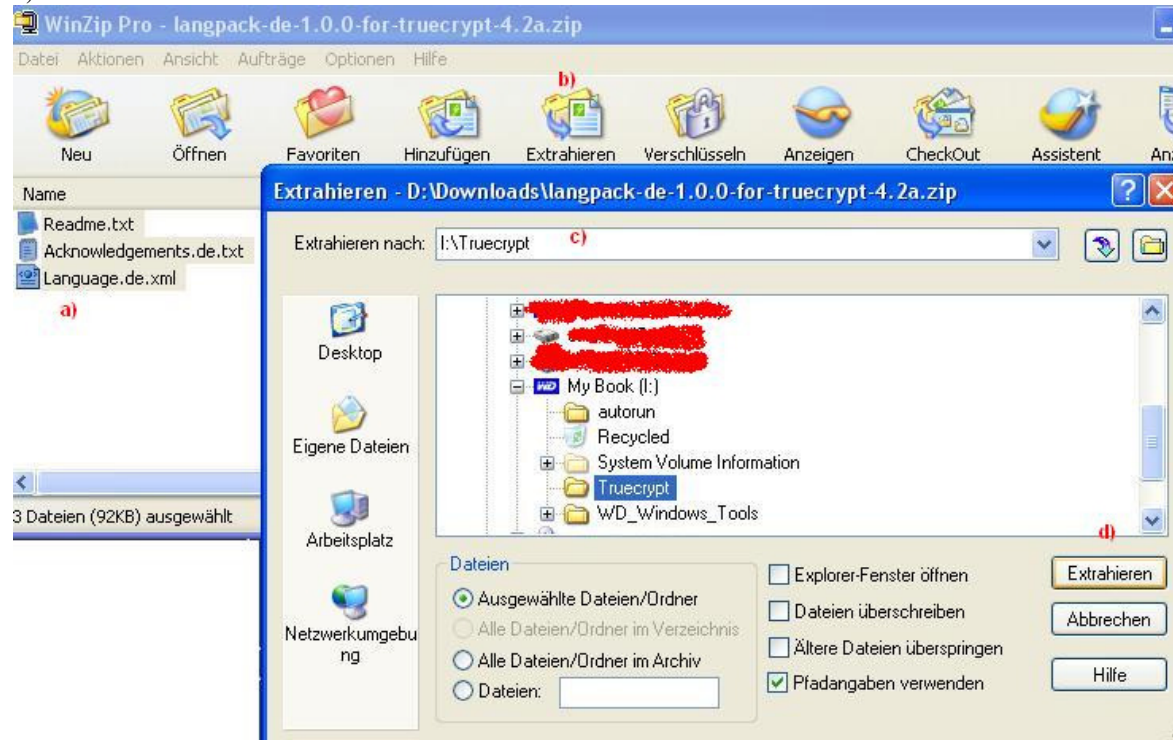
**Spoiler:**

Um Truecrypt auf Deutsch benutzen zu können benötigen wir noch die passende [Sprachdatei](#) ([hier](#) der Direktlink zur deutschen 1.0.0, welche mit Truecrypt 4.3 funktioniert) Diese entpacken wir in das Verzeichnis in welches wir Truecrypt installiert haben(in diesem befindet sich die Datei "Truecrypt.exe", Standard: C:\Programme\Truecrypt) .

- markieren
- extrahieren

c) Ziel wählen

d) extrahieren

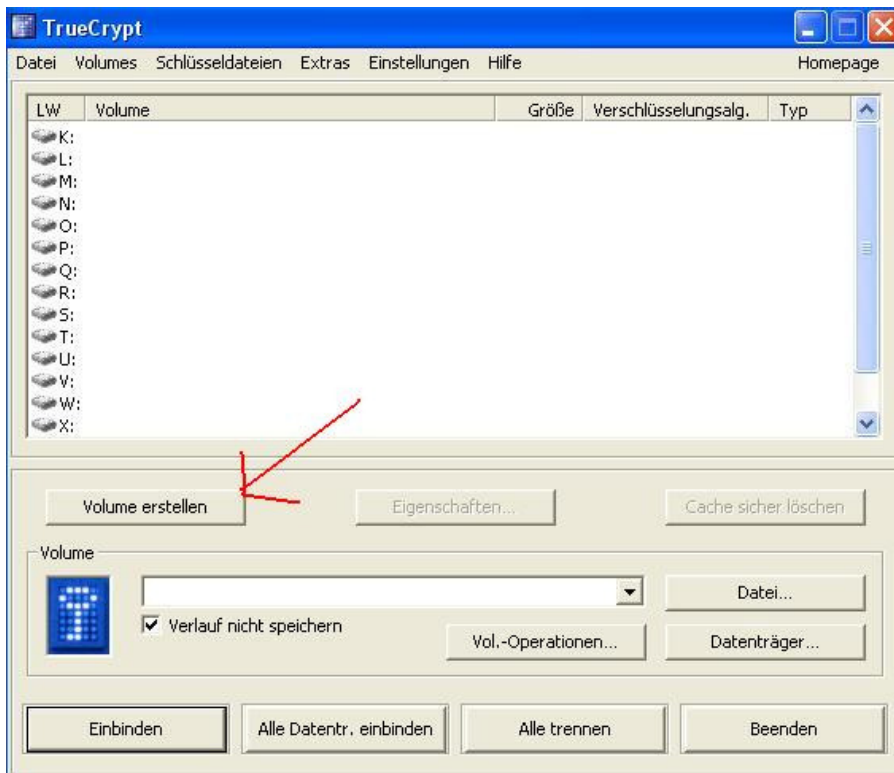


Truecrypt sollte die deutsche Sprachdatei automatisch erkennen und von nun an auf Deutsch starten.  
(sonst muss dieses unter settings->languages von hand umgestellt werden)

### 3) Mithilfe von Truecrypt Volumen erstellen

**Spoiler:**

Die Vorbereitungen sind abgeschlossen, mit einem Doppelklick auf die Truecrypt.exe starten wir das Programm. In dem sich öffnendem Fenster "Volumen erstellen" anklicken.



Es besteht die Möglichkeit ein normales oder verstecktes Volumen zu erstellen. Im Punkt "Wofür steht versteckt" erfährt ihr genaueres über die beiden Möglichkeiten. Für den Anfänger mit Truecrypt bzw. für jede Person die nur private Daten vor unberechtigtem Zugriff schützen möchte reicht ein normales Volumen. Ein verstecktes Volumen lohnt sich nur falls Gefahr besteht, dass, nachdem die [Festplatte](#) weg ist, Druck aufgebaut wird und man gezwungen werden soll das Passwort herauszugeben. Anzumerken ist noch das eine versteckte Partition keinerlei Geschwindigkeitsverlust darstellt.

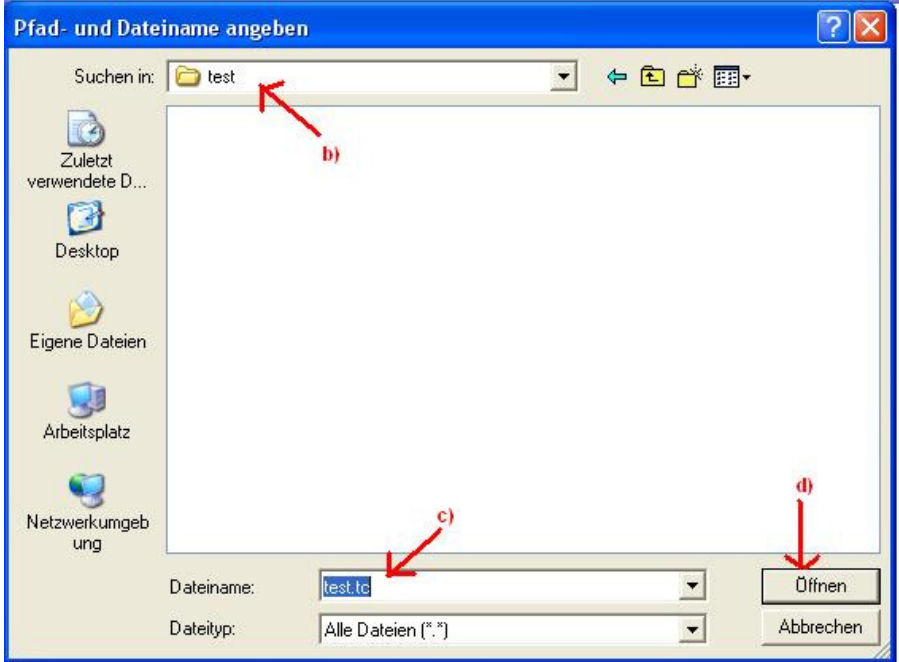
#### a) normales Volumen erstellen

**Spoiler:**

Den Punkt "normales Volumen erstellen" anwählen und Weiter klicken

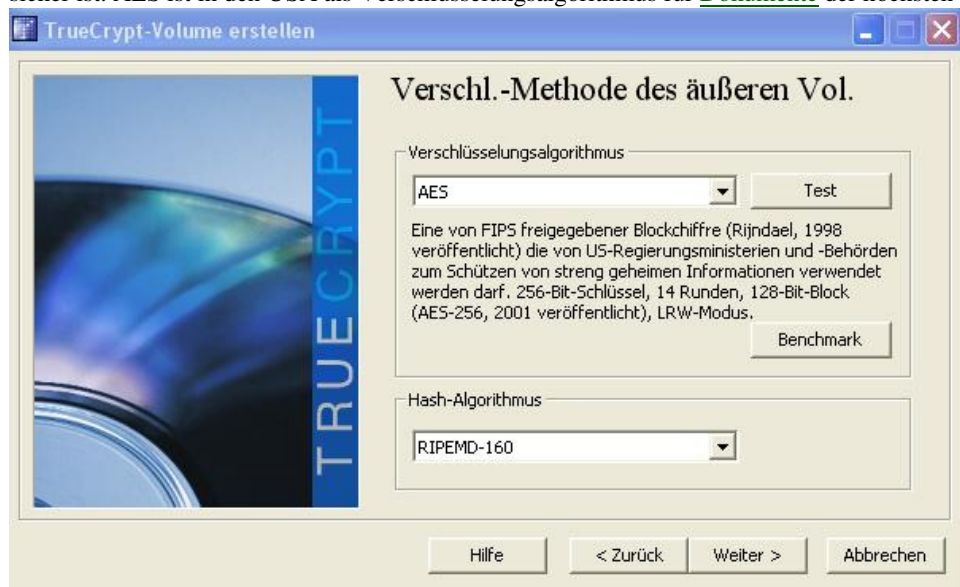


- Als nächstes auf Datei klicken
- Den Ort auswählen an welchem das Volumen erstellt werden soll
- Irgendeinen Namen eingeben (wenn an den Namen ".tc" angehängt wird kann die Datei später mithilfe eines Doppelklicks sofort mit Truecrypt eingebunden werden)
- Öffnen anklicken
- Weiter anklicken

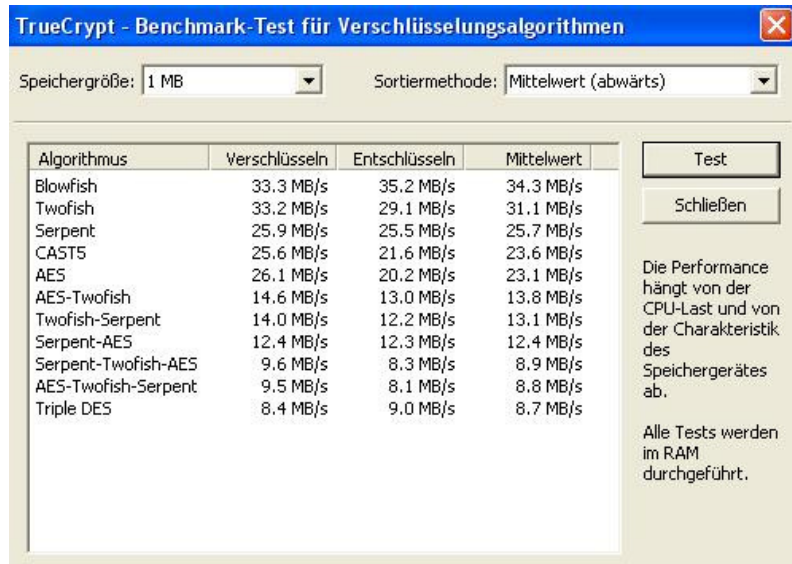


Hier ist es möglich den Verschlüsselungsalgorithmus auszuwählen.

Informationen zu den verschiedenen Verschlüsselungen gibt es unter anderem in der [Wikipedia](#), zum Beispiel zu [AES](#), [DES](#) oder [Blowfish](#). Zu den Verschlüsselungen ist zu sagen, dass sie momentan alle sicher sind. Einige jedoch vermutlich in näherer Zukunft knackbar werden als andere. Andererseits gilt es zu bedenken das eine stärkere Verschlüsselung meist auch mit einem größeren Zeitaufwand Hand in Hand geht. Ich empfehle AES, da es eine noch akzeptable Geschwindigkeit bietet und andererseits sehr sicher ist. AES ist in den USA als Verschlüsselungsalgorithmus für [Dokumente](#) der höchsten Geheimhaltungsstufe zugelassen.



Es lohnt sich definitiv einmal den Benchmark Button zu drücken und sich die verschiedenen Algorithmen im Vergleich anzugucken.



Als nächstes muss die Größe des Volumens festgelegt werden. Die Größe des Volumens kann hinterher nicht mehr verändert werden, das Volumen sollte also großzügig dimensioniert sein (besonders in Musik oder Bildersammlungen welche permanent wachsen!)

Es besteht zwar ebenfalls die Möglichkeit die Größe des Volumen dynamisch zu verwalten, doch davon sollte abgesehen werden! Das dynamische verwalten der Größe verringert die Sicherheit, die Performance wird spürbar verschlechtert und es besteht die Gefahr das verschlüsselte Daten unbeabsichtigt zerstört werden.

Die Wahl wird mit einem Klick auf weiter quittiert.



Nun kommt man zur Wahl ob ein Kennwort und/oder eine Schlüsseldatei Verwendung finden soll. Beides hat vor und Nachteile.

Ein Schlüssel ist sehr komfortabel zu handhaben, sollte allerdings besser nicht alleine zum verschlüsseln benutzt werden, da sonst die Sicherheit leidet. Es sollte IMMER, sofern nur ein Schlüssel verwendet wird, wenigstens ein kurzes Kennwort ebenfalls Verwendung finden, da sonst, durch simples ausprobieren sämtlicher Dateien als Schlüssel, der Schutz geknackt wäre! Eine Schlüsseldatei sollte außerdem immer an mehreren Stellen hinterlegt werden, damit nicht sobald der USB-Stick kaputt ist alle Daten unentschlüsselbar verloren sind.

Ein Kennwort ist zwar (wenn es sicher ist) recht lang und häufig nicht einfach zu merken, bietet aber eine größere Sicherheit als nur eine Schlüsseldatei, das Kennwort darf keinesfalls auf ein Blatt geschrieben im Schreibtisch liegen, oder auf der Tastaturunterseite stehen (wie in Firmen immer wieder zu sehen). Am sichersten ist es natürlich beides zusammen zu verwenden. Soll beides zusammen verwendet werden muss erst eine Schlüsseldatei erstellt werden und dann bevor auf weiter geklickt wird noch ein Kennwort eingeben werden.

Schlüsseldatei

**Spoiler:**

Kennwort

**Spoiler:**

Es sollte hier unbedingt NTFS gewählt werden, damit auch Dateien mit mehr als 4 GB verwaltet werden können (wie Imagedateien von UrlaubsDVDs). Danach auf Formatieren klicken.

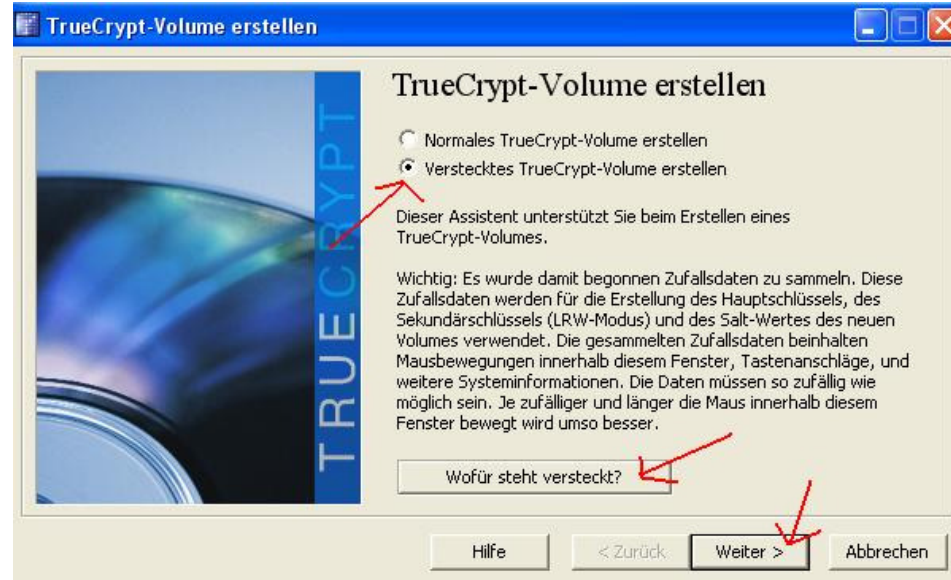
Das Formatieren selbst kann einige Zeit dauern wenn dies erledigt ist wurde erfolgreich ein verschlüsseltes Volumen erzeugt!

**Re: Anleitung, Info und How-To: Truecrypt Verschlüsselung**

---

**b) versteckte Volumen erstellen****Spoiler:** 

Den Punkt verstecktes Volumen erstellen auswählen und auf Weiter klicken.



Da noch kein normales Volumen erstellt wurde müsst ihr "normales und anschließend verstecktes Volumen erstellen" wählen. Dann auf weiter klicken.



## 6) Batch Dateien (Starten von Truecrypt automatisieren)

**Spoiler:**

Zuerst ein Wort zu Batch Dateien:

Diese sind kleine Programme die sehr leicht mithilfe eines Texteditors, wie Notepad, erstellt und bearbeitet werden können. Sobald eine Batch Datei per Doppelklick geöffnet wird führt sie die Befehle aus die in ihr stehen. Hier sollen Batch Dateien verwendet werden um das Starten von Truecrypt zu vereinfachen und zu automatisieren. Das Ideale Ergebnis wäre erreicht- wenn nach dem System start nur noch einmal das Passwort eingegeben werden muss und alle Volumen automatisch gemountet werden! (Die Passwort Eingabe darf aus Sicherheitsgründen keinesfalls ebenfalls von der Batch Datei erledigt werden, da damit die Sicherheit massivst gefährdet wäre!)

Da das Programmieren von Batch Dateien ein wenig Übung erfordert biete ich eine einfache Batch Datei an und eine fortgeschrittenere, welche auch kompliziertere Wünsche erfüllt (Danke an [Leoric](#) für seine wunderbare Batch Datei!).

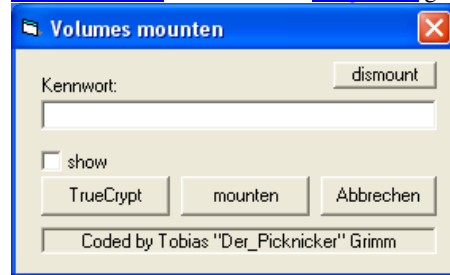
### a) Einfache Batch Datei, zum starten eines Volumens mit Windows start

**Spoiler:**

### b) Programm zum starten beliebig vieler Volumen mit Windows start

**Spoiler:**

[Der Picknicker](#) hat ein feines [Programm](#) geschrieben um euch das einbinden nochmals zu vereinfachen ([Download](#)).



Anleitung liegt bei. Fragen zum Tool bitte [hier](#) stellen. Um das Programm mit Windows start zu starten, müsst ihr zur exe eine Verknüpfung erstellen und diese unter Start->Programme->Autostart einfügen.

Habe im [Programmieren](#) subforum darum gebeten das sich das tool ein kundiger nochmal anschaut was auch [geschehen ist](#).

### c) Bessere Batch Datei zum variablem starten von (fast) beliebig vielen Volumen(inarbeit)

**Spoiler:**

inarbeit

[dies](#) wird in kürze eingepflegt, batch um mehrere volumen mit gleichem pw mit nur einer pw eingabe einzubinden. thx an Leoric für die nutzungserlaubniss.

inarbeit

## 7) Allgemeines

**Spoiler:**

Die Volumen werden als normale Laufwerke im Windows Explorer bzw. im Arbeitsplatz angezeigt und benehmen sich auch genau wie solche.

Die Laufwerke können mithilfe des "Alle Trennen" Buttons auch wieder "ausgebunden" werden, dies geschieht ebenfalls sobald der Rechner aus ist, es empfiehlt sich also eine Steckdosenleiste mit Schalter an den Computer anzuschließen, so das dieser im Fall der Fälle schnell vom Strom zu trennen ist.

## 8) Header sichern (evtl. letzte Rettung für Daten)

**Spoiler:**

Jeder der schon länger im Schutz & Anonymitätsforum mitliest hat bestimmt schon mal den Fall gesehen das ein User nicht mehr an seine Daten herankam und ihm empfohlen wurde den [Header](#) zurückzuspielen, den er doch gesichert haben müsse. Hier also nun nochmal an alle wie es geht: