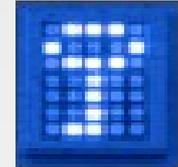


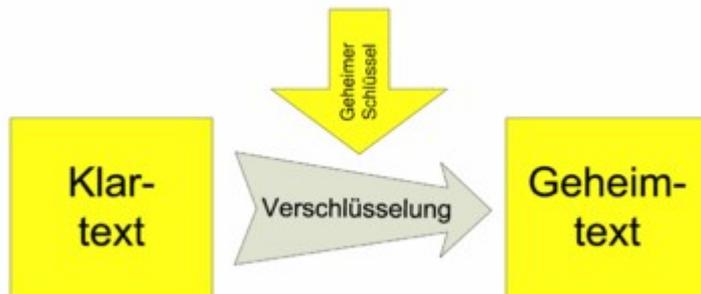
# LUSC Workshopweekend 2008

## Verschlüsselung mit Truecrypt



**Vielen Dank für die Installation des Bundestrojaners**

**Bitte lehnen Sie sich zurück und entspannen Sie sich während  
Ihre Daten zur weiteren Verwertung an uns übermittelt werden**



# Truecrypt – Verschlüsselung



## Zusammenfassung Teil 1

- Was ist Truecrypt ?
- Warum Truecrypt ?
- Was macht die Software?
- Verschiedene Varianten
- Anwendungsmöglichkeiten
- Grundlagen 1, 2 und 3
- Installation

# Truecrypt – Verschlüsselung



## Zusammenfassung Teil 2

- Sichere Passwörter
- Zukunftsaussichten
- Vorteile / Nachteile
- Alternativen
- LUKS / dm-crypt / cryptsetup
- Webadressen

# Truecrypt – Verschlüsselung



## Was ist Truecrypt?

- Open Source Verschlüsselungssoftware
- Grafische Benutzeroberfläche
- Einfache intuitive Bedienung
- Viele verschiedene Einsatzbereiche

# Truecrypt – Verschlüsselung



## Warum Truecrypt?

- Niemand muss meine Daten sehen können – Schäuble lässt grüssen
- Daten sind bei physikalischem Zugriff auf den PC geschützt
- Daten sind bei Verlust (z.B. Laptop oder USB Stick) geschützt (zumindest bis das Passwort geknackt ist, was schonmal bis zu 10 Jahre dauern kann)
- 100 prozentigen Schutz gibt es NICHT

# Truecrypt – Verschlüsselung



## Was macht die Software?

- Durch Kryptografische Tools wie Truecrypt wird Klartext in unleserliche Zeichenfolgen umgewandelt
- Für die Ver- und Entschlüsselung muss der gleiche Algorithmus angewendet werden
- Sichere und relativ lange Passwörter sind das A und O für sichere Verschlüsselung

# Truecrypt – Verschlüsselung



## Verschiedene Varianten

- Linux Ubuntu x86.deb oder x64.deb (“dmsetup” muss nachinstalliert werden)
- OpenSuse x86.rpm oder x64.rpm
- MAC OS X 10.5 Leopard oder 10.4 Tiger
- MS Windows 2000/XP/Vista
- Unter Debian Lenny kann das Ubuntu Paket verwendet werden (es müssen noch 3 Programme nachinstalliert werden)
- Alle verschiedenen Varianten sind untereinander kompatibel

# Truecrypt – Verschlüsselung



## Anwendungsmöglichkeiten

- Komplette Platte oder Systempartition verschlüsseln
- Verzeichnisse / Ordner verschlüsseln
- Einzelne Dateien verschlüsseln
- Spezielle Installation für USB Sticks
- Versteckte Container können seit Version 6.0 eingerichtet werden

# Truecrypt – Verschlüsselung

## Grundlagen I



- **Zwei verschiedene Arbeitsweisen**
  - **Komplette Partition verschlüsseln**
    - Partition muss neu formatiert werden
    - Truecrypt ist immer im Hintergrund aktiv (wenn auf diese Partition zugegriffen wird)
  - **Verschlüsselte Container anlegen**
    - z.B. als Dateien, Verzeichnisse, Partitionen oder auf USB Sticks/Festplatten
    - Geeignet für unverschlüsselte Partitionen um verschlüsselte Bereiche für sensible Daten anzulegen
    - Müssen ebenfalls formatiert werden

# Truecrypt – Verschlüsselung



## Grundlagen II

- **Booten von Truecrypt Volumes?**
  - Funktioniert leider nicht, da die Bootpartition während des Bootvorganges nicht verschlüsselt sein darf
  - Der Bootloader muss den Kern von der Systempartition in den Speicher laden, damit der Prozessor ihn ausführen kann. Ist dieser Bereich verschlüsselt, wäre dies nicht mehr möglich

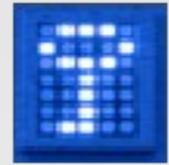
# Truecrypt – Verschlüsselung



## Grundlagen III

- **Hidden Volumes**
  - Versteckte Truecrypt Container
  - Extra Passwort für Hidden Container
  - Nachteil: Man sollte nicht mehr in den äußeren Container schreiben
  - Der äußere Container muss FAT formatiert sein
  - Vorteil: Muss man das Truecrypt Passwort herausgeben, bleiben die Daten im Hidden Container unsichtbar

# Truecrypt – Verschlüsselung

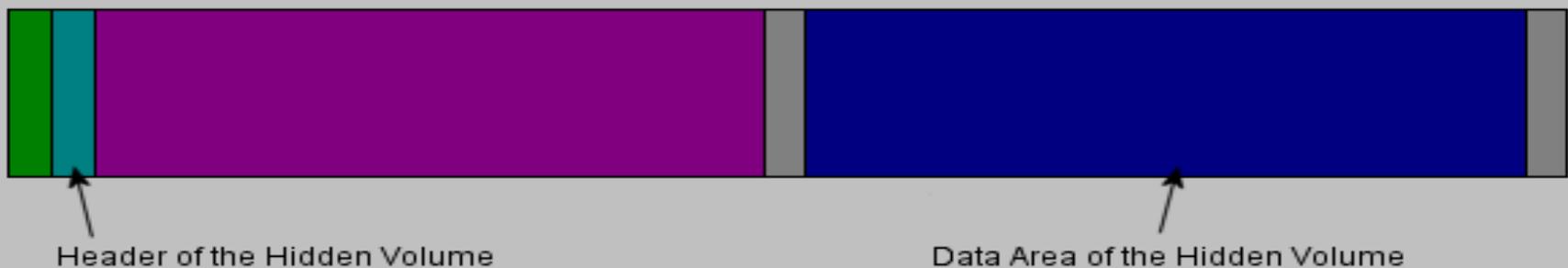


## Grafik Hidden Volumes

**A standard TrueCrypt volume**



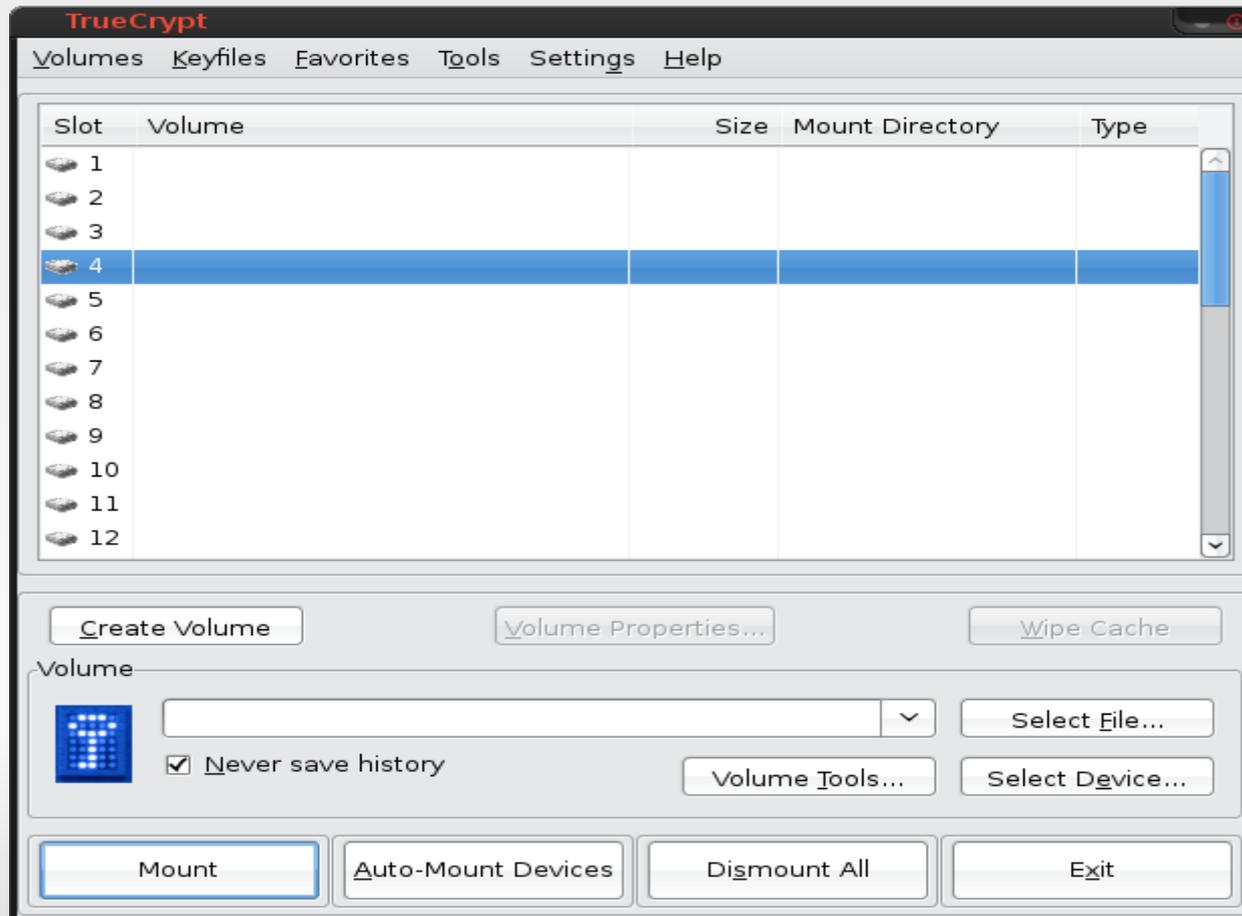
**The standard TrueCrypt volume after a hidden volume was created within it**



# Truecrypt – Verschlüsselung



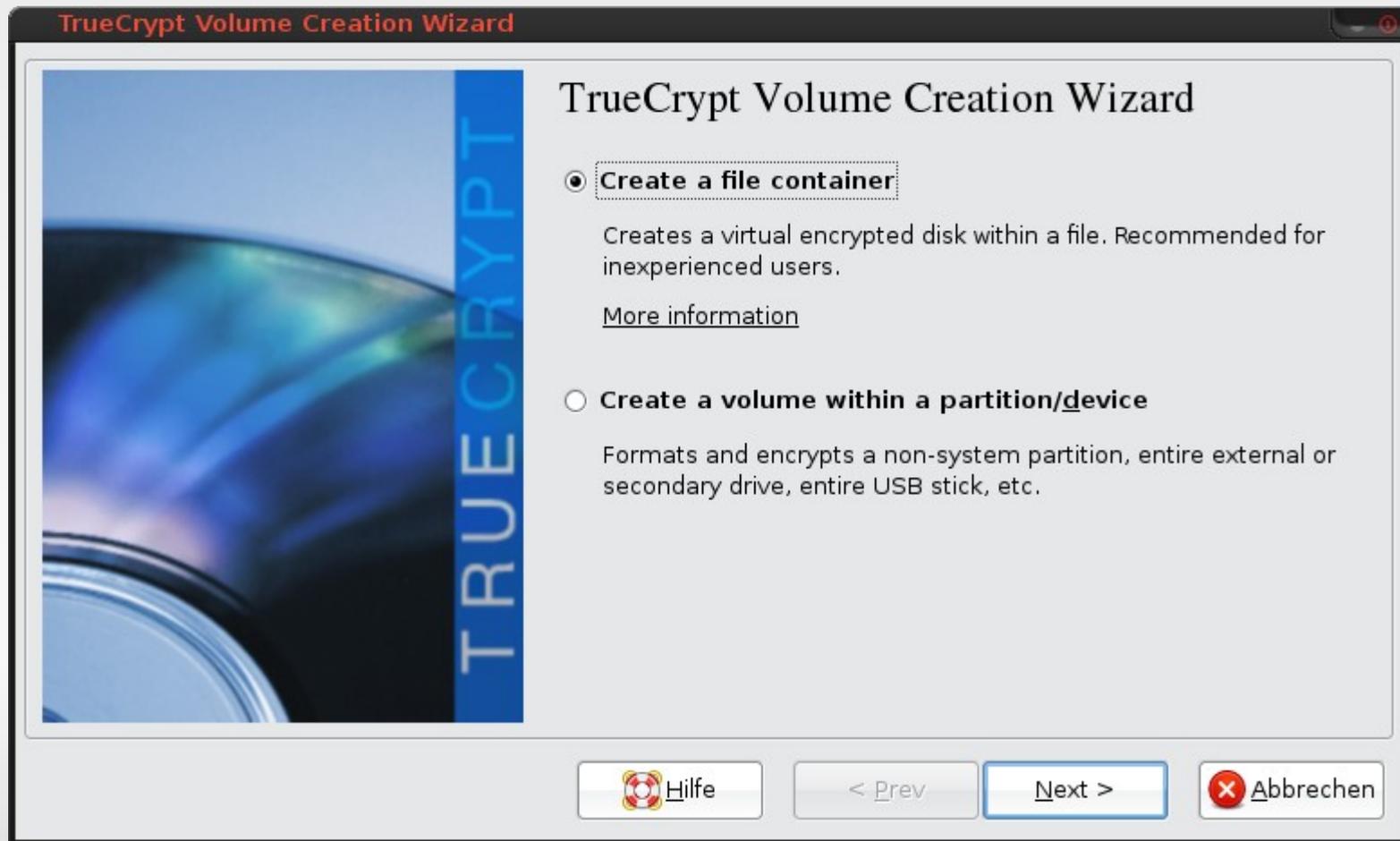
## Installation



# Truecrypt – Verschlüsselung



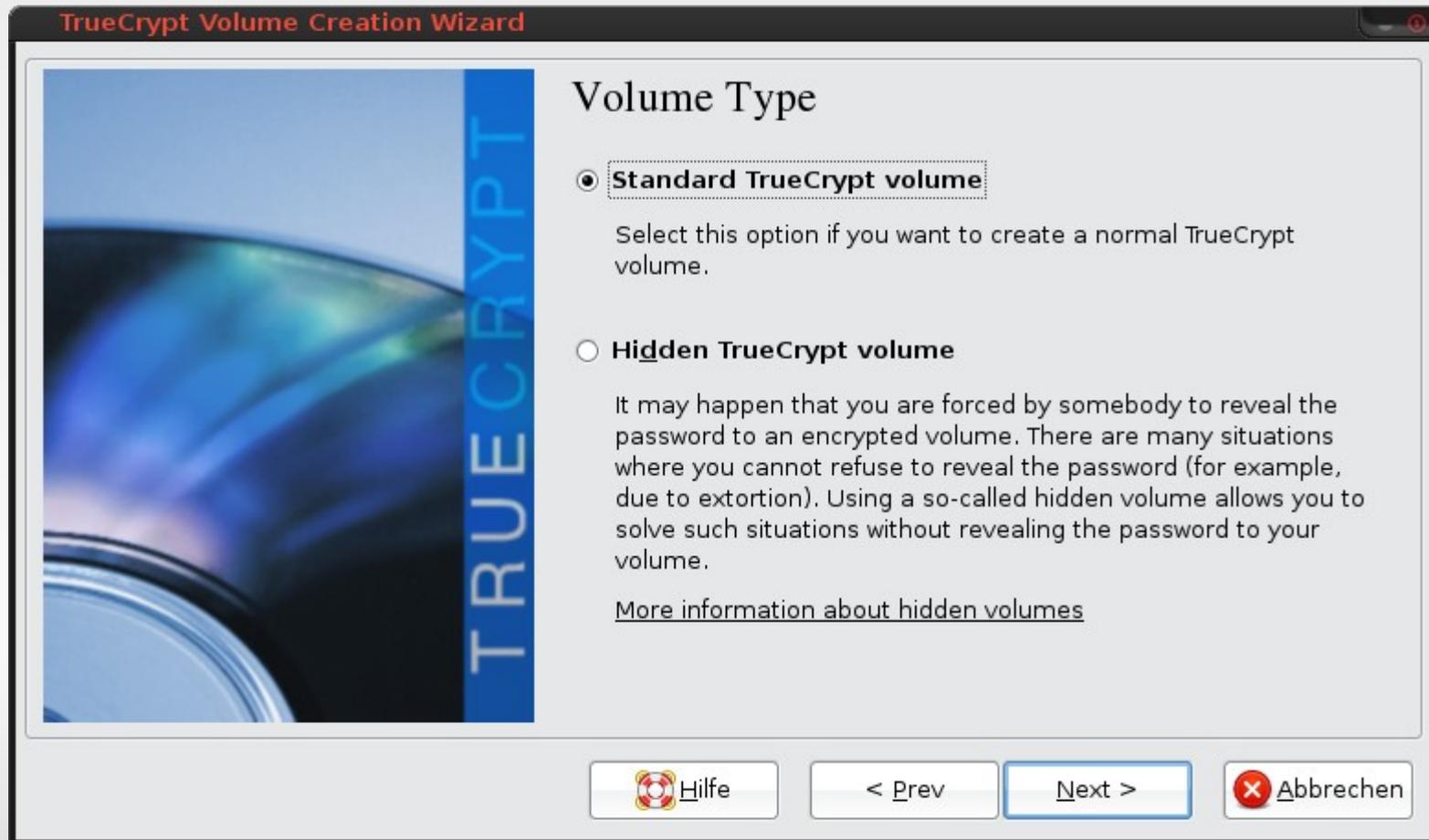
## Installation



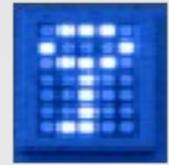
# Truecrypt – Verschlüsselung



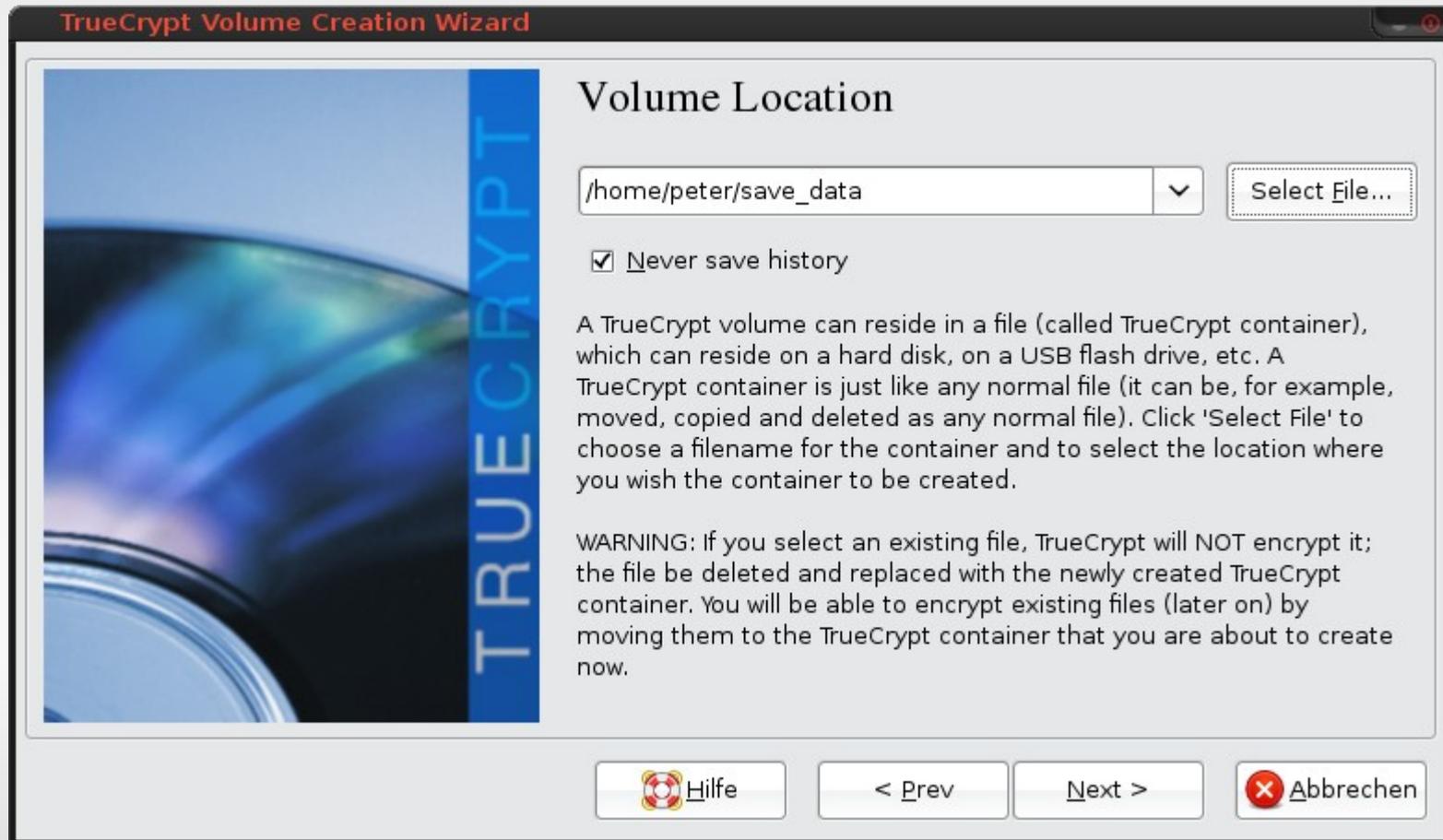
## Installation



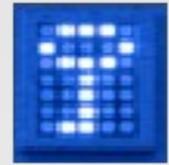
# Truecrypt – Verschlüsselung



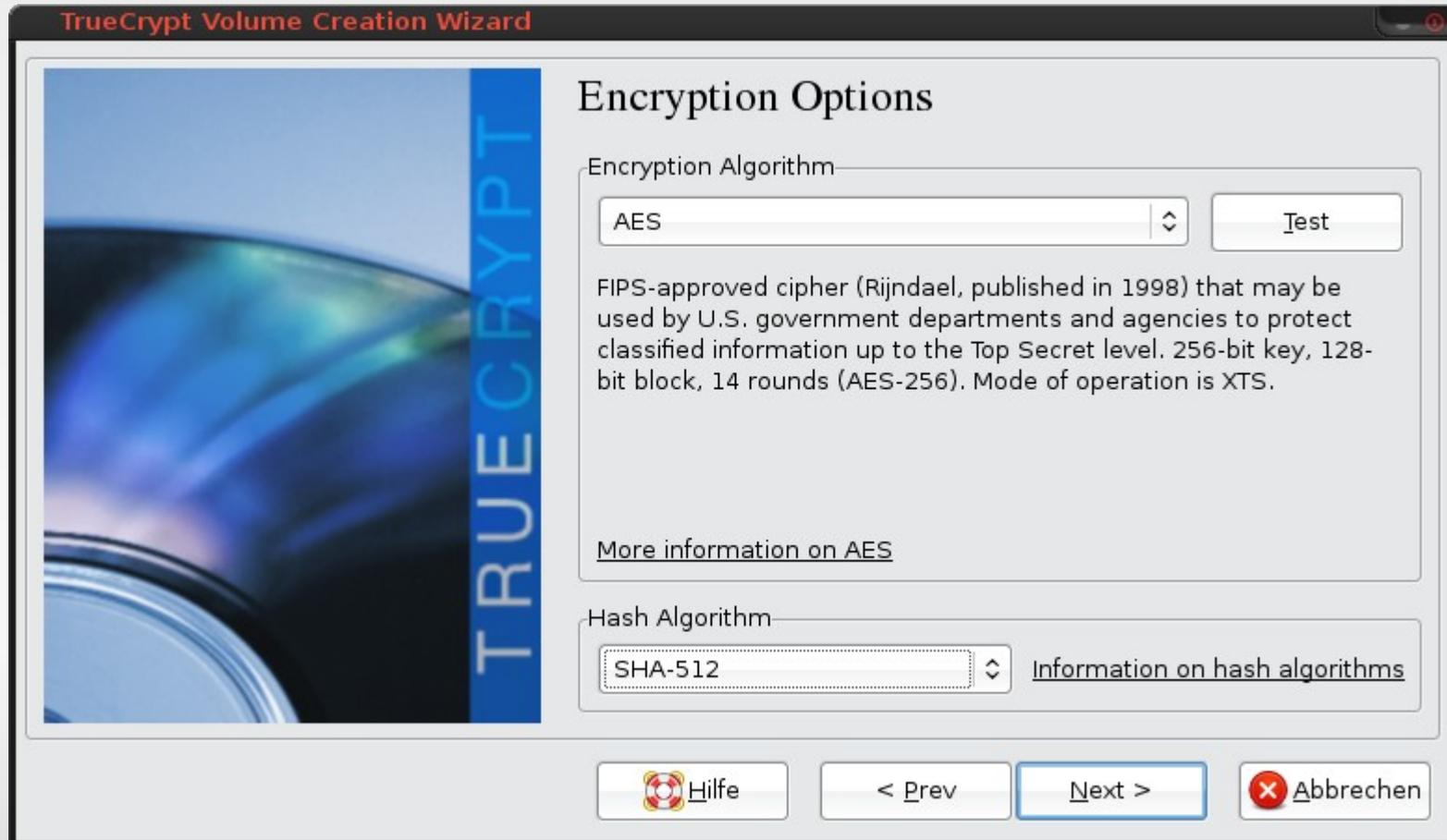
## Installation



# Truecrypt – Verschlüsselung



## Installation



# Truecrypt – Verschlüsselung



## Installation

TrueCrypt Volume Creation Wizard



### Volume Size

**Free space available: 51,3 GB**

Please specify the size of the container to create.

If you create a dynamic (sparse-file) container, this parameter will specify its maximum size.

Note that the minimum possible size of a FAT volume is 275 KB. The minimum possible size of an NTFS volume is 2829 KB.

 Hilfe    Abbrechen

# Truecrypt – Verschlüsselung



## Installation

TrueCrypt Volume Creation Wizard

### Volume Password

Password:

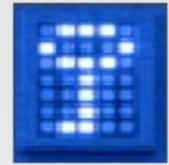
Confirm password:

Display password

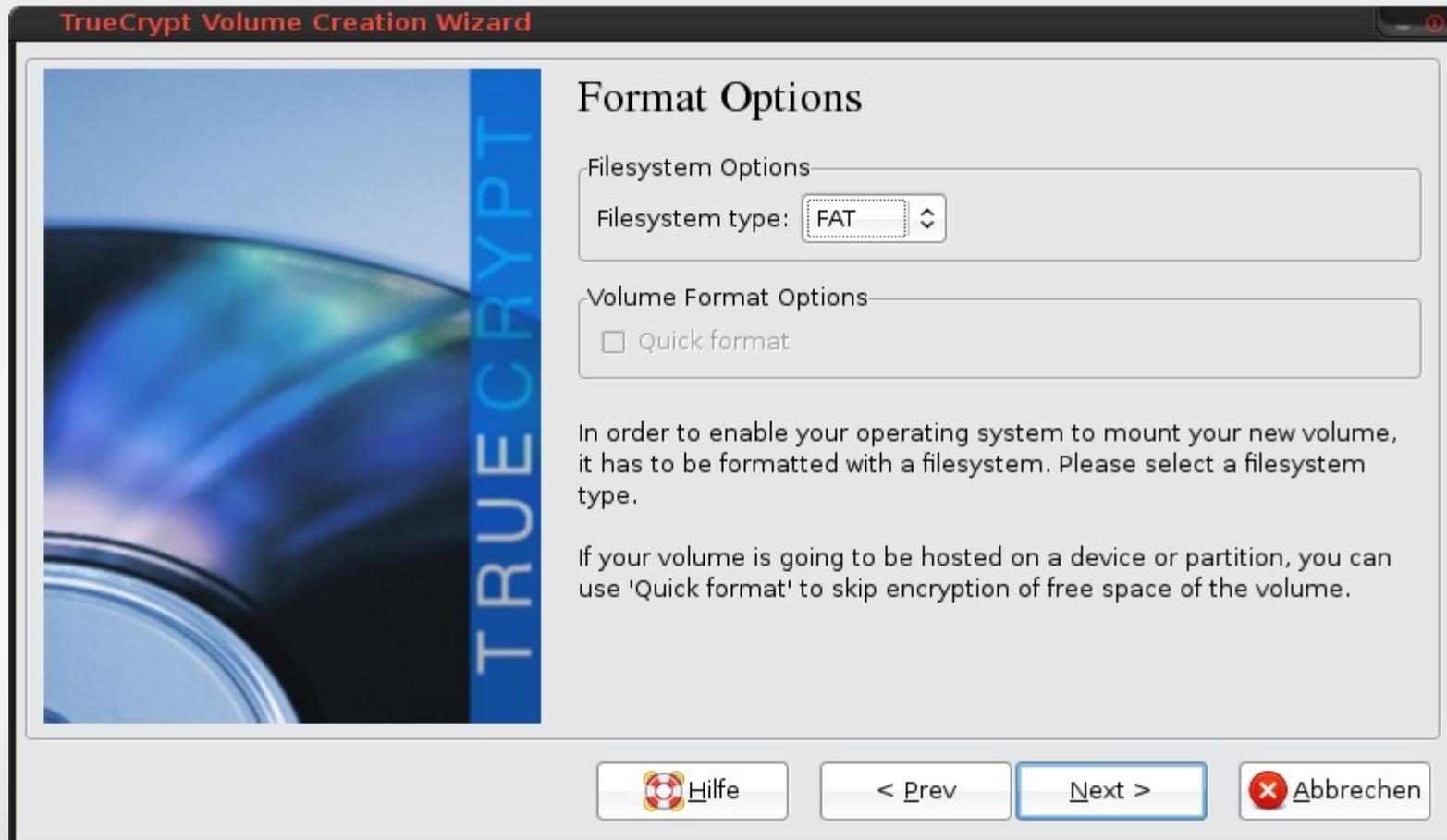
Use keyfiles

It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = \$ \* + etc. We recommend choosing a password consisting of more than 20 characters (the longer, the better). The maximum possible length is 64 characters.

# Truecrypt – Verschlüsselung



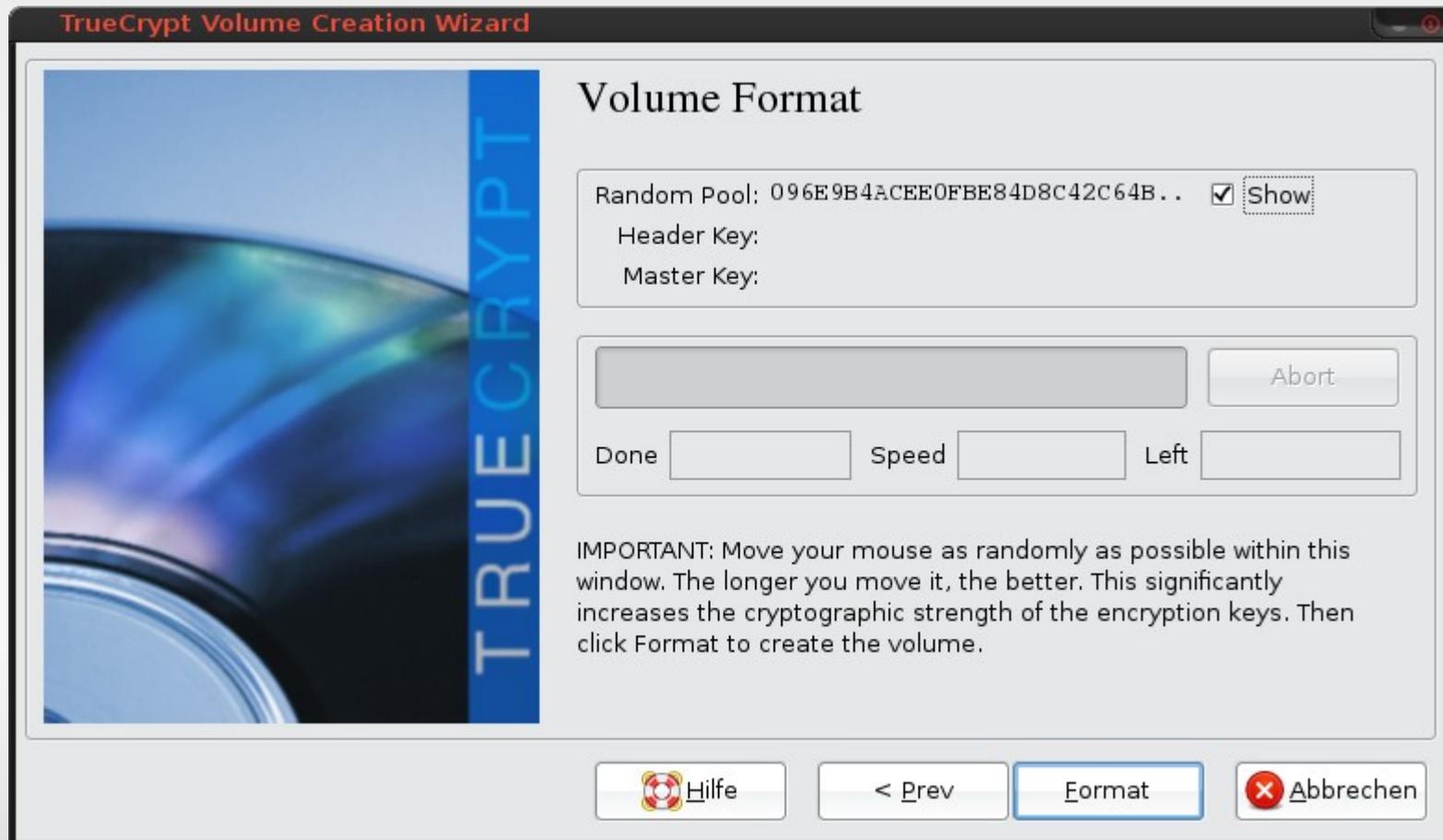
## Installation



# Truecrypt - Verschlüsselung



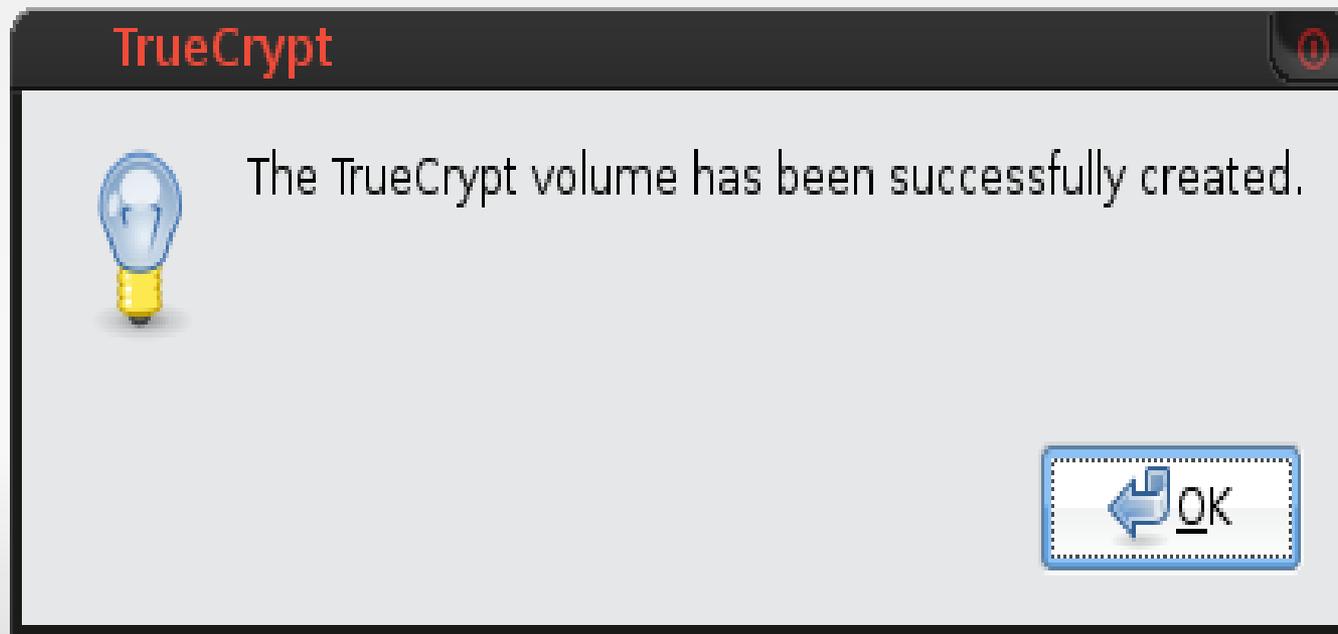
## Installation



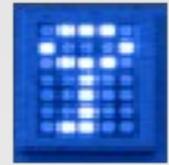
# Truecrypt – Verschlüsselung



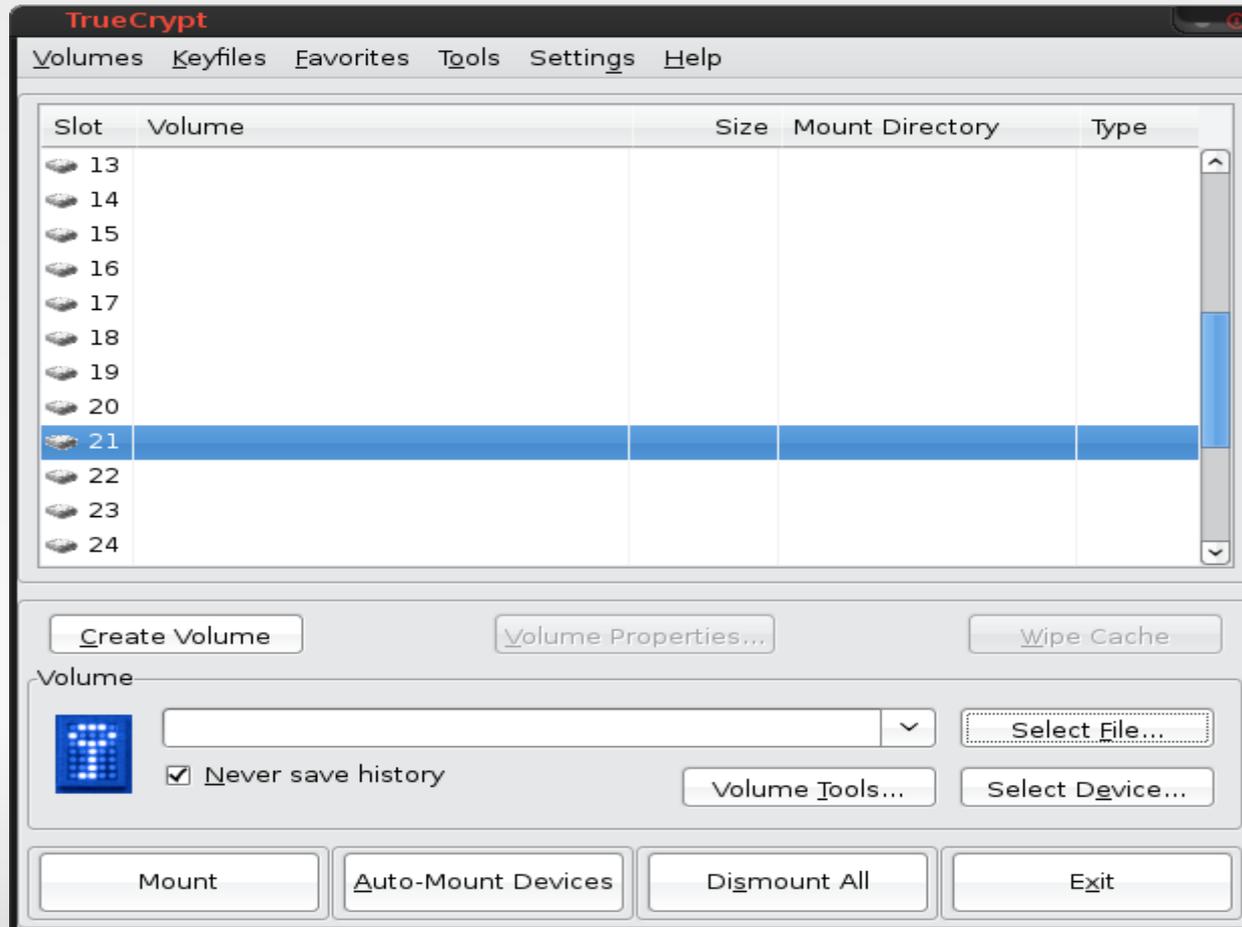
## Installation



# Truecrypt – Verschlüsselung



## Installation



# Truecrypt – Verschlüsselung



## Installation

Enter password for "/home/peter/save\_data"

Password:

Cache passwords and keyfiles in memory

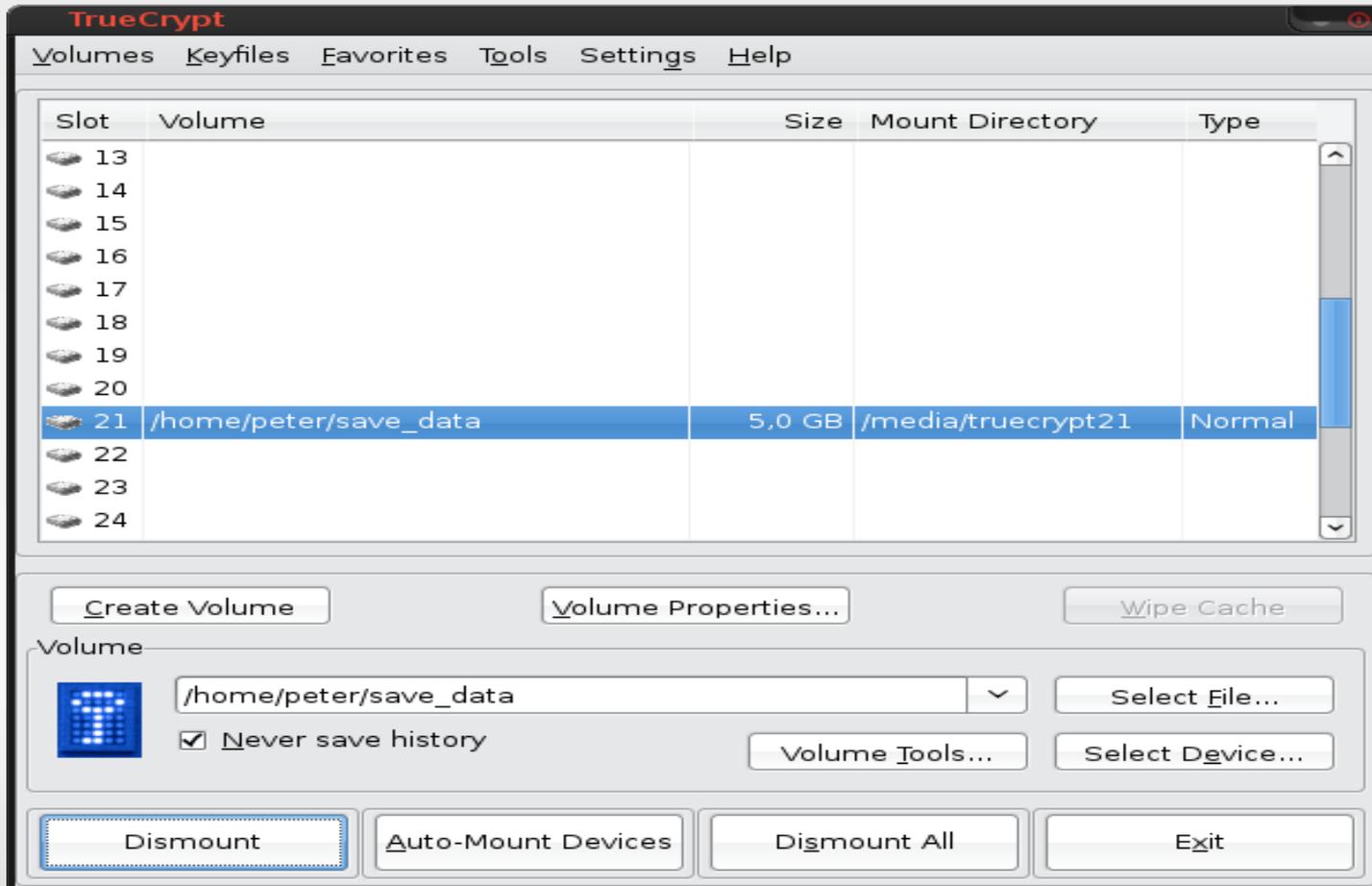
Display password

Use keyfiles

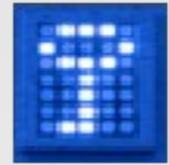
# Truecrypt – Verschlüsselung



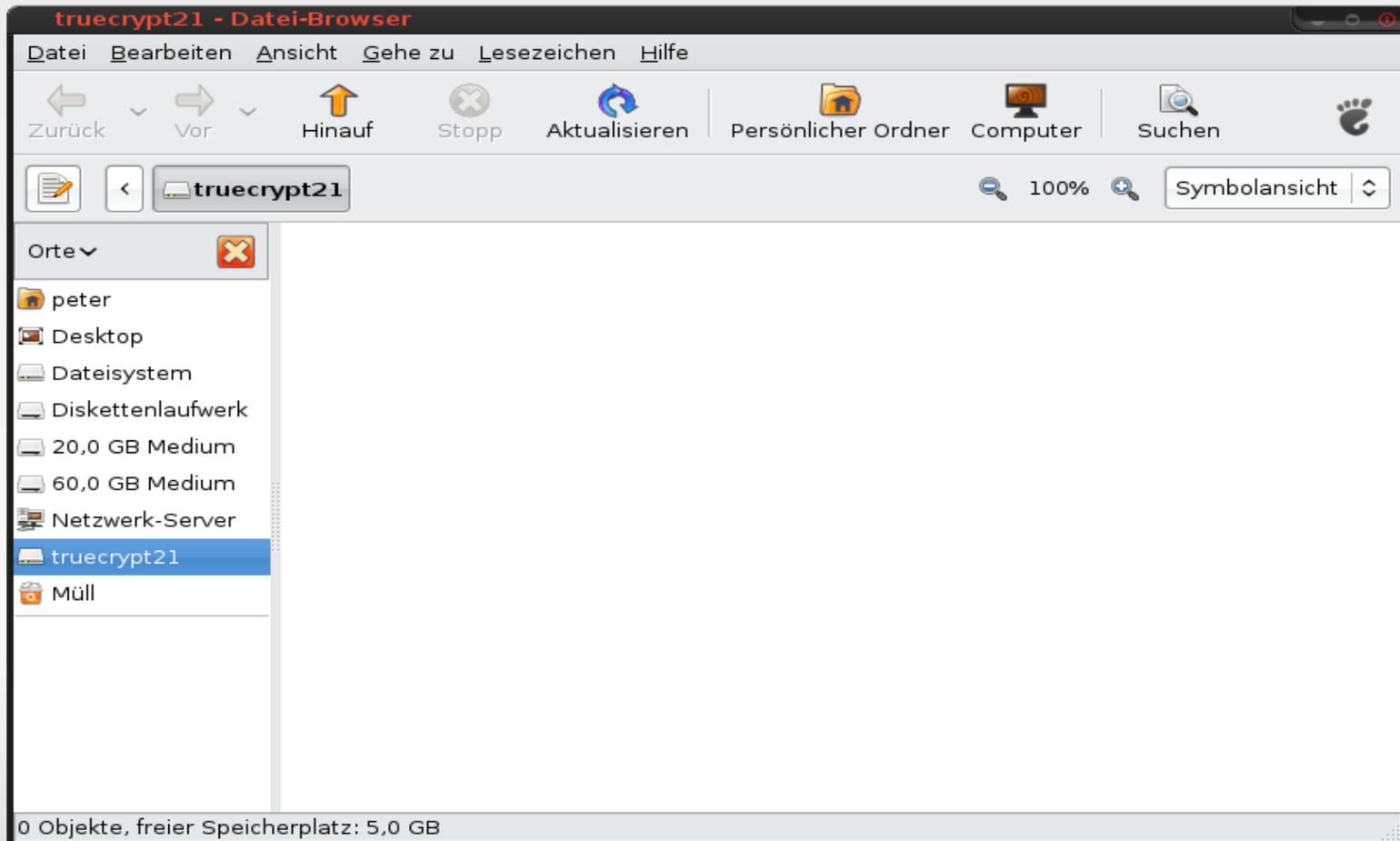
## Installation



# Truecrypt – Verschlüsselung



## Installation



# Truecrypt – Verschlüsselung



## Sichere Passwörter

- Das A und O sind sichere Passwörter
- Wörterbucheinträge oder Geburtsdaten sind tabu
- Sichere Passwörter bestehen aus Groß- und Kleinbuchstaben sowie Sonderzeichen
- Je länger und komplizierter desto besser/sicherer
- Unter Linux mit pwgen Passwörter erstellen
- Für das OS aus Redmond gibt es auch diverse Password Generator

# Truecrypt – Verschlüsselung



## Zukunftsaussichten

- z.Zt. Version 6.0 mit Hidden Container und Systempartitionsverschlüsselung
- Geplant ist ein Zusatztool welches alle Daten im Hidden Container unter vordefinierten Bedingungen löscht
- Es wird auch daran gearbeitet mit anderen Filesystemen z.B. Ext2 oder Ext3 arbeiten zu können
- Verschiedene neuere Verschlüsselungs Standards sollen in Zukunft integriert werden

# Truecrypt – Verschlüsselung



## Vorteile Truecrypt

- Software ist Open Source
- Funktioniert Betriebssystem übergreifend
- Einfache und leicht verständliche GUI
- Spezielle Tools um USB Sticks/Platten zu verschlüsseln
- Hidden Container (unsichtbar für Angreifer)
- Vom Header können relativ einfach Sicherungen gemacht werden (**sehr sehr wichtig!**)

# Truecrypt – Verschlüsselung



## Nachteile Truecrypt

- Pakete nur für einzelne Linux Distributionen vorhanden
- Derzeit nur mit FAT und NTFS Dateisystemen kompatibel
- Bei Verlust des Passwortes sind die Daten weg
- Geringerer Datendurchsatz durch Verschlüsselung
- Risiko eines Bitfehlers im Header. Danach kann das File nicht mehr geöffnet werden

# Truecrypt – Verschlüsselung



## Alternativen?

- Die beste Alternative ist LUKS (Linux Unified Key Setup). On-Disk Specification unter Linux, welche den genauen Aufbau des Containers beschreibt
- Enc FS (unter Linux)
- Drive Crypt (unter MS Windows)
- Wirkliche Plattformübergreifende Alternativen gibt es derzeit noch nicht

# Truecrypt – Verschlüsselung



## LUKS

- **Linux Unified Key Setup**
  - Ermöglicht die Verschlüsselung von kompletten Festplatten oder Partitionen unter Linux
  - Es sollten nicht nur /home, sondern auch die Swap Partition, /tmp, /var sowie Teile des /etc Verzeichnisses verschlüsselt werden
  - Durch den Verzicht des Verschlüsseln der Partition /boot, kann von diesen Partitionen auch gebootet werden

# Truecrypt – Verschlüsselung



## dm-crypt

- **dm-crypt**
  - Cryptotarget für den device-mapper (dm) im Linuxkernel
  - Device-mapper implementiert u.a. auch Software-Raid oder LVM im Kernel
  - Baut eine zusätzliche Schicht zwischen verschlüsselten Roh Daten und dem Dateisystem auf
  - Ermöglicht die Erstellung von virtuellen verschlüsselten Blockgeräten
  - Ist nicht an einen Verschlüsselungsalgorithmus gebunden

# Truecrypt – Verschlüsselung



## cryptsetup I

- **Was ist cryptsetup?**
  - Tool, welches den device-mapper im Kernel „geeignet“ konfiguriert
  - Leitet aus einem Passwort einen kryptographischen Key ab und übergibt ihn dem Kernel
    - Verfahren PBKDF2 (password based key derivation function 2)

# Truecrypt – Verschlüsselung



## cryptsetup II

- **Zwei wichtige Bereiche**
  - Schlüsselgenerierung (wie wird der Schlüssel berechnet)
  - Verschlüsselungsverfahren (Algorithmus und Modus)

# Truecrypt – Verschlüsselung



## LUKS/dm-crypt/cryptsetup

- Da dies eine sehr komplexe Thematik ist, sollte man sich den Artikel „Geheime Niederschrift“ mal anschauen. Dort wird noch einmal sehr genau auf o.g. Stichpunkte eingegangen
- [www.linux-magazin.de/heft\\_abo/ausgaben/2005/08/geheime\\_niederschrift](http://www.linux-magazin.de/heft_abo/ausgaben/2005/08/geheime_niederschrift)

# Truecrypt – Verschlüsselung



## Webadressen

- [www.truecrypt.org](http://www.truecrypt.org)
- [www.truecrypt.de.vu](http://www.truecrypt.de.vu)
- [www.fixmbr.de/truecrypt-anleitung](http://www.fixmbr.de/truecrypt-anleitung)
- [forums.truecrypt.org](http://forums.truecrypt.org)
- [wikipedia.de](http://wikipedia.de)
- <http://aldev.de/59-usb-stick-mit-truecrypt-verschluesseln>

# Truecrypt – Verschlüsselung



**Vielen Dank für die Aufmerksamkeit  
Noch Fragen?**

