

Festplattenverschlüsselung mit TrueCrypt

Crypto-Workshop VHS Tübingen

Kurt Jaeger, pi@opsec.eu

<http://cccs.de/>

Tübingen, 15. März 2014

Übersicht

- ▶ Warum ?
- ▶ Warum TrueCrypt ?
- ▶ Verwendung
- ▶ Fortgeschrittene Themen

Warum ?

- ▶ Einzelne Dateien verschlüsseln ist aufwendig
- ▶ Zum Bearbeiten muss man sie entschlüsseln
- ▶ Davon bleiben Spuren auf dem Laufwerk
- ▶ Daher: Verschlüsselte Dateisysteme sind besser

Was ist...

- ▶ ein Laufwerk ? Festplatte, CD oder USB-Stick
- ▶ eine Partition ? Zusammenhängender Abschnitt auf einem Laufwerk
- ▶ eine System-Partition ? Systemwichtige Software enthalten
- ▶ ein Dateisystem ? Verwaltungsinformationen, um Dateien abzulegen
- ▶ eine Datei ? Eine Folge von Zeichen
- ▶ und mehr: Dateiname, Besitzer, Rechte, Metadaten...

Warum TrueCrypt ?

- ▶ Open Source
- ▶ Windows, Mac, Linux
- ▶ Stellt verschlüsselte Laufwerke bereit
- ▶ Wird als sicher betrachtet
- ▶ Schon lange in Entwicklung und Gebrauch (10 Jahre)
- ▶ Abstreitbarkeit
- ▶ Tarnbetriebssystem (nur Windows)

Aber:

- ▶ <http://istruecryptauditedyet.com/>
- ▶ Offenes Problem: Unsicheres Betriebssystem!

Aber Vorsicht

A CRYPTO NERD'S IMAGINATION:

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR
CLUSTER TO CRACK IT.

NO GOOD! IT'S
4096-BIT RSA!

BLAST! OUR
EVIL PLAN
IS FOILED!



WHAT WOULD ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH
THIS \$5 WRENCH UNTIL
HE TELLS US THE PASSWORD.

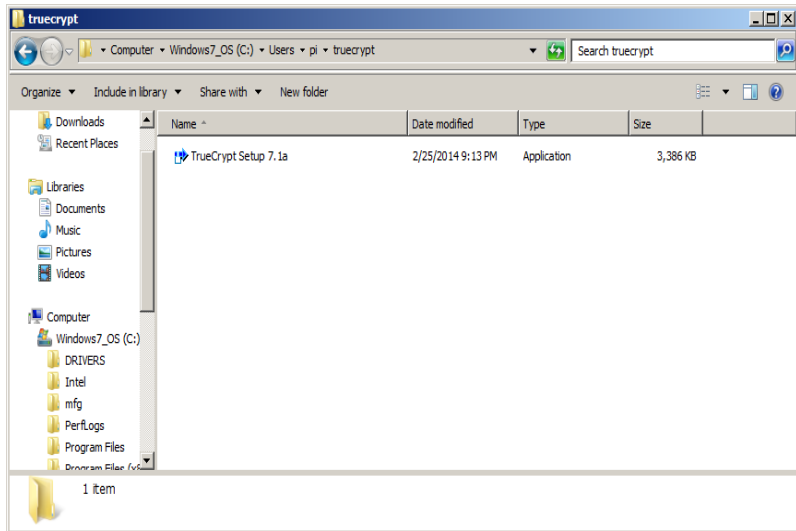
GOT IT.



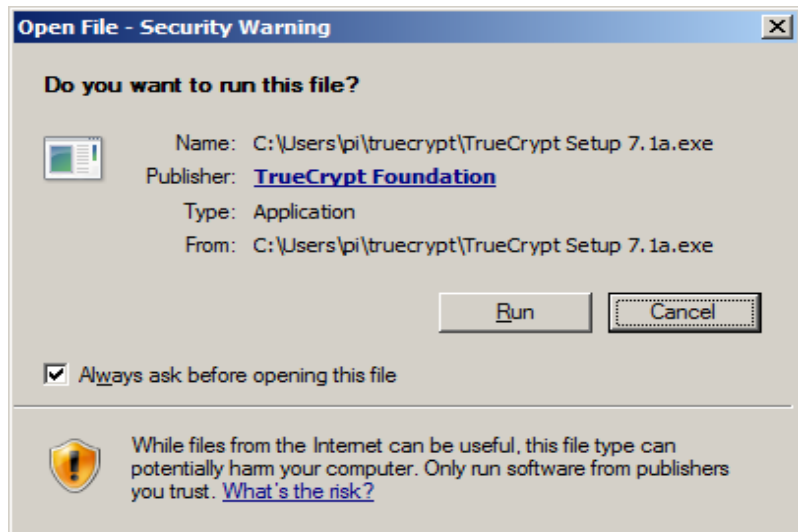
Verwendung

- ▶ Runterladen
- ▶ Installation
- ▶ Anlegen eines Beispiel-Volumes/Laufwerks/Partition
- ▶ Zugriff auf Beispiel-Laufwerk
- ▶ Datei darauf ablegen
- ▶ Zugriff beenden

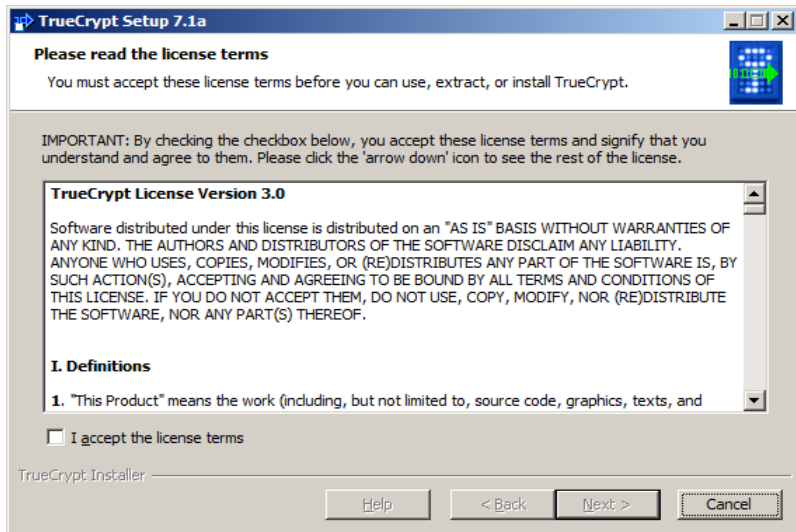
Heruntergeladene Datei



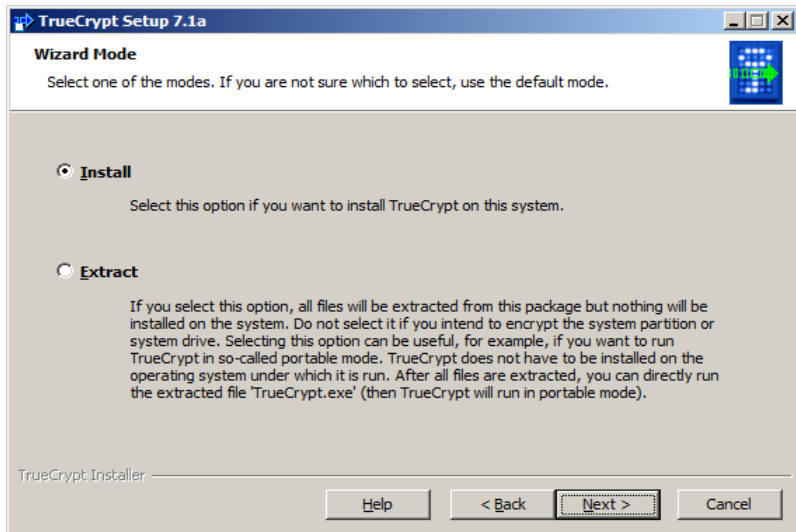
Start der Installation



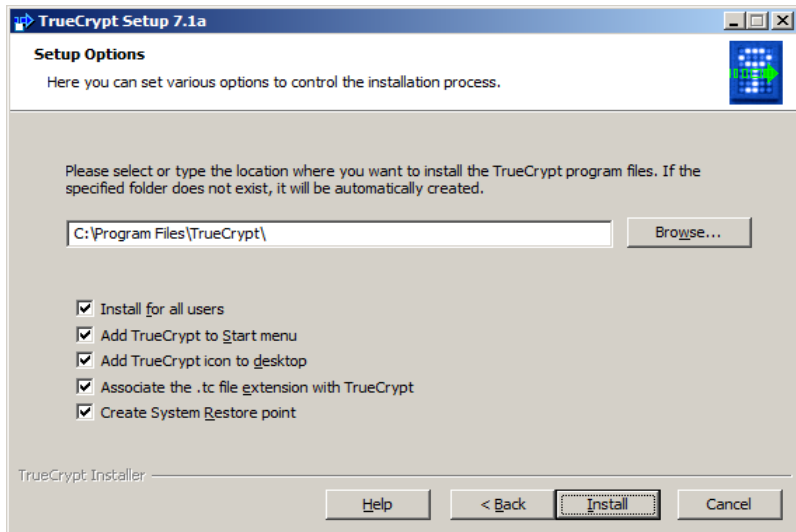
Lizenzabfrage



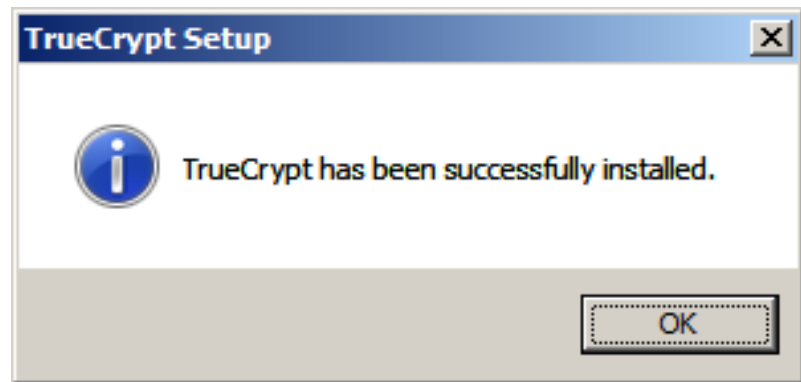
Installation



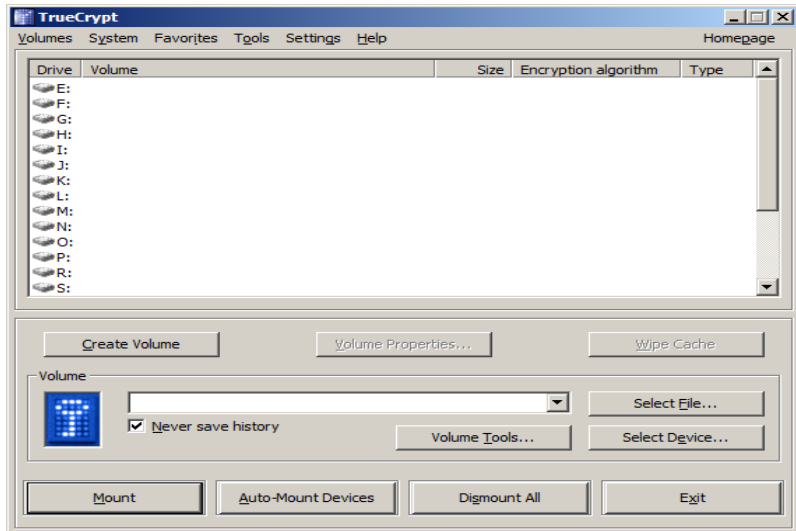
Optionen



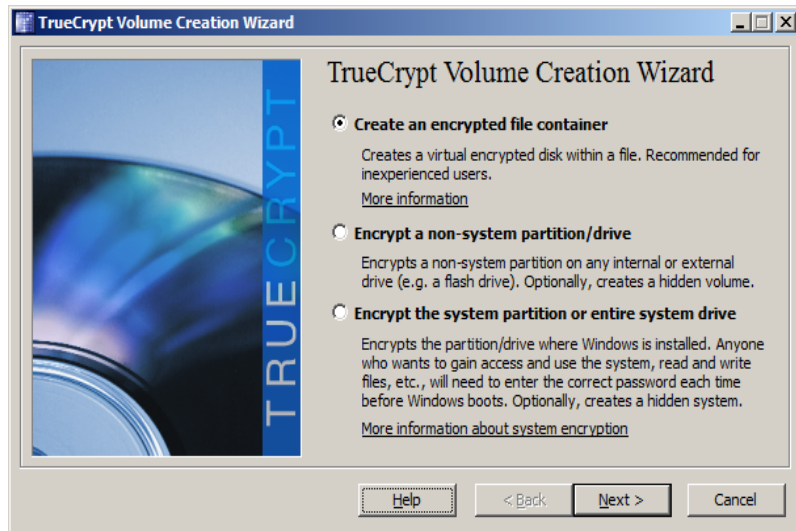
Installation erfolgreich



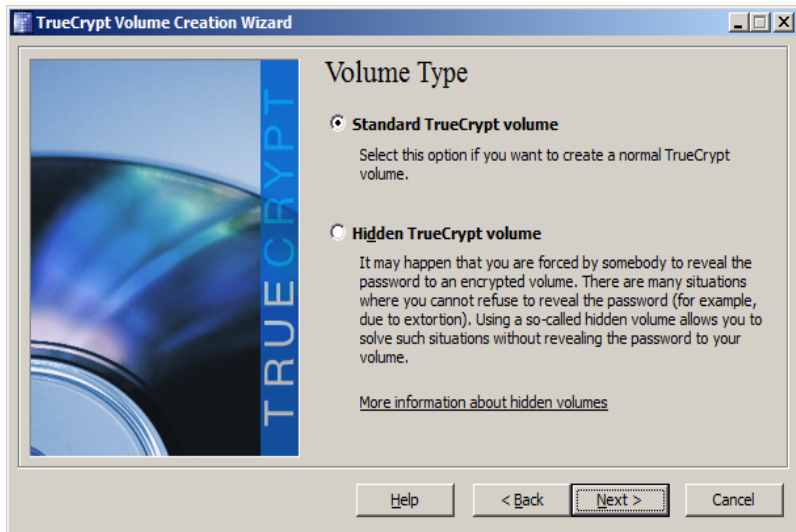
Erster Start von TrueCrypt



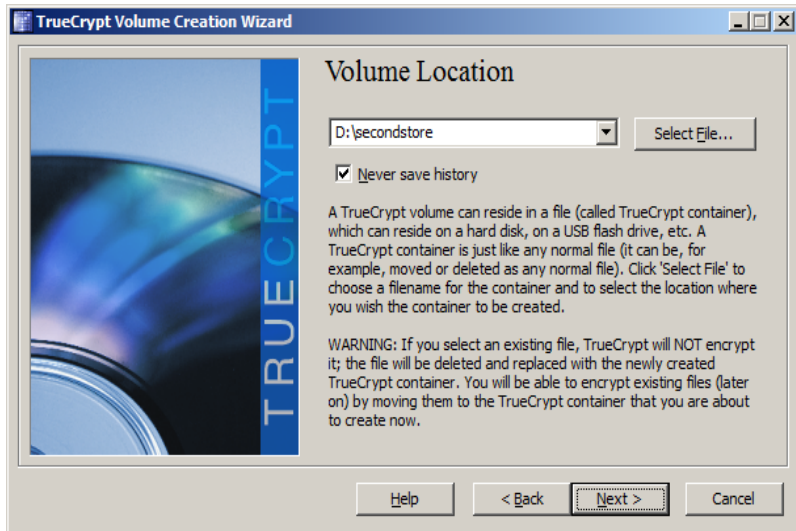
Anlegen eines verschlüsselten Laufwerks



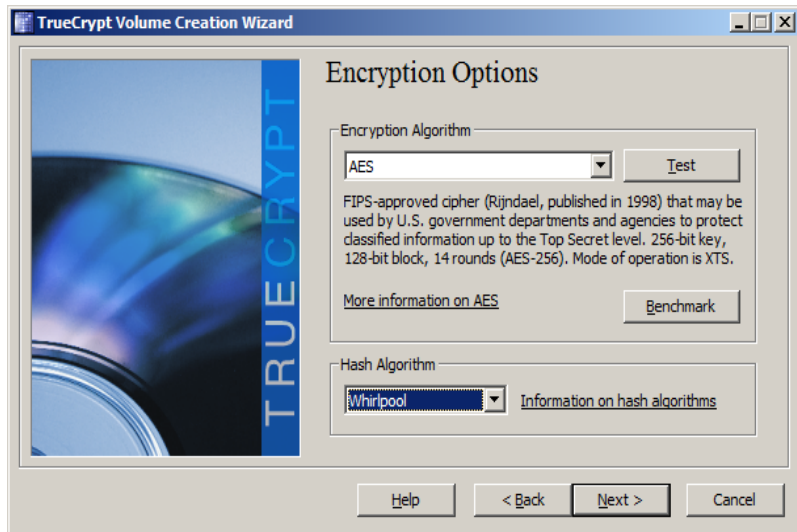
Volume Type



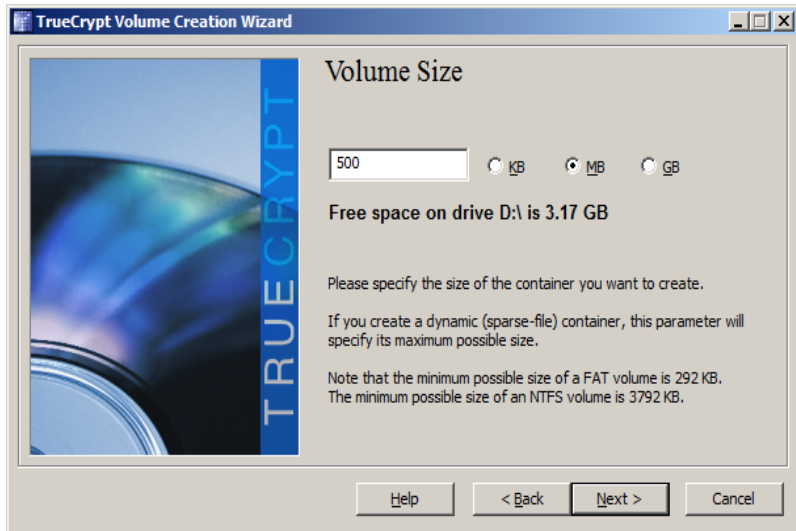
Volume Location



Verschlüsselungsoptionen



Grösse des verschlüsselten Laufwerks



WICHTIG: Passwort

TrueCrypt Volume Creation Wizard

Volume Password

Password:

Confirm:

☐ Use keyfiles

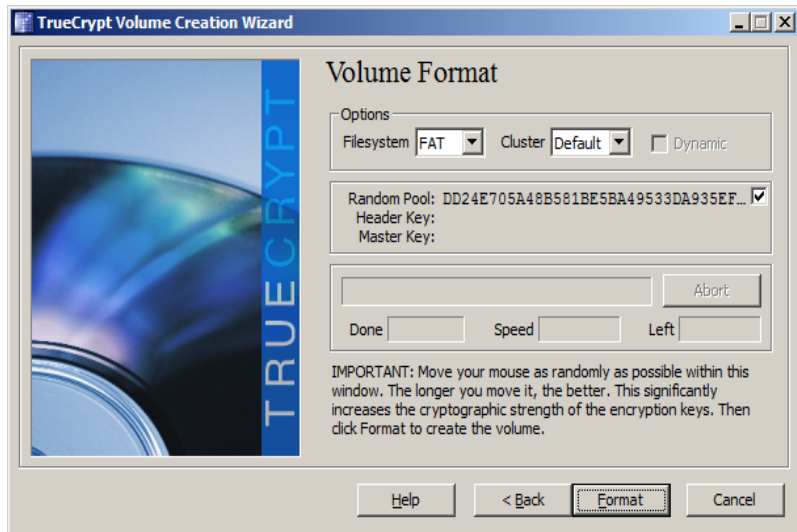
☒ Display password

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.

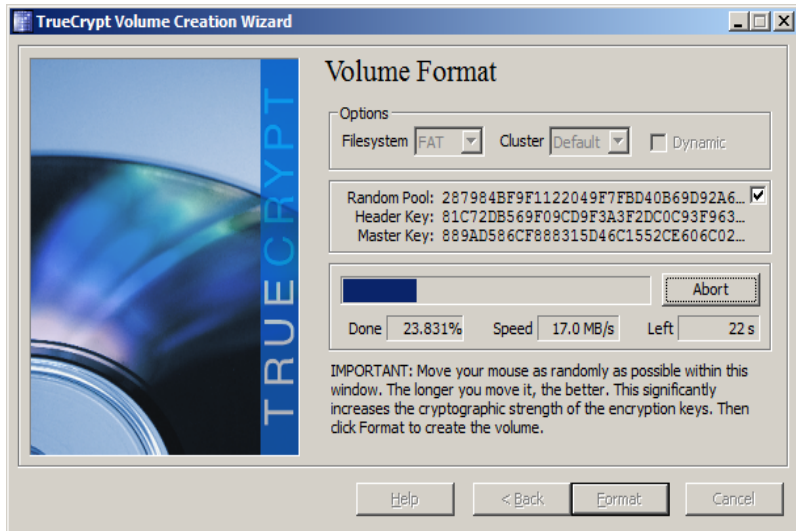
Warnung!



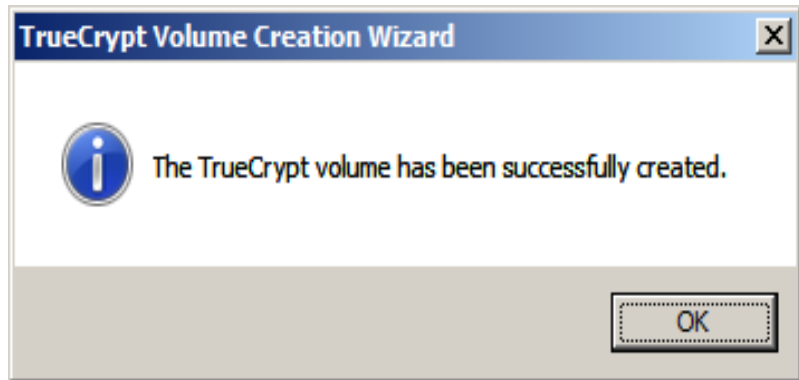
Formatierung des verschlüsselten Laufwerks



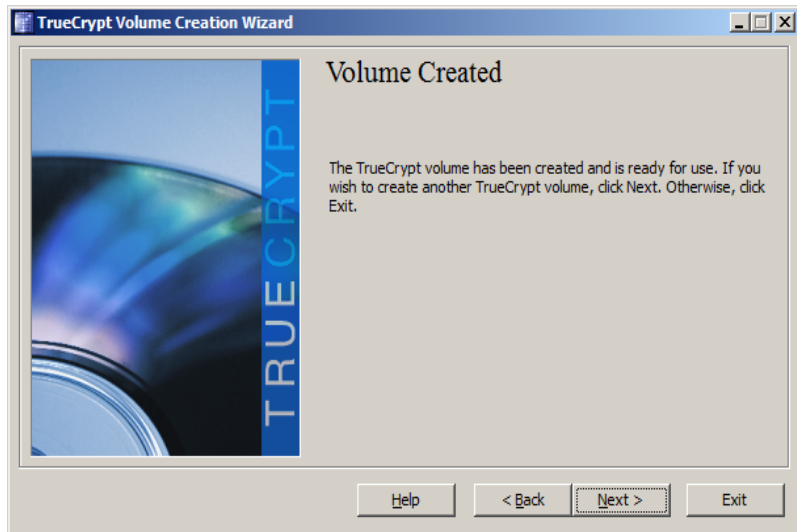
Laufende Formatierung



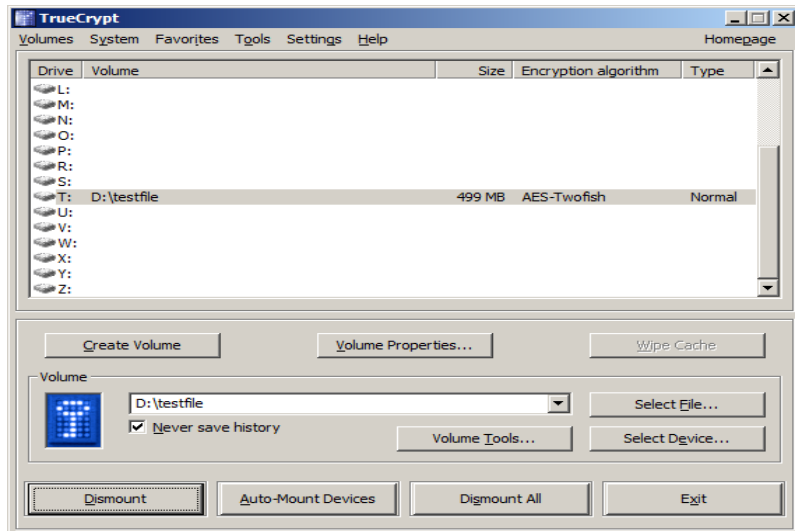
Erfolgreich angelegt



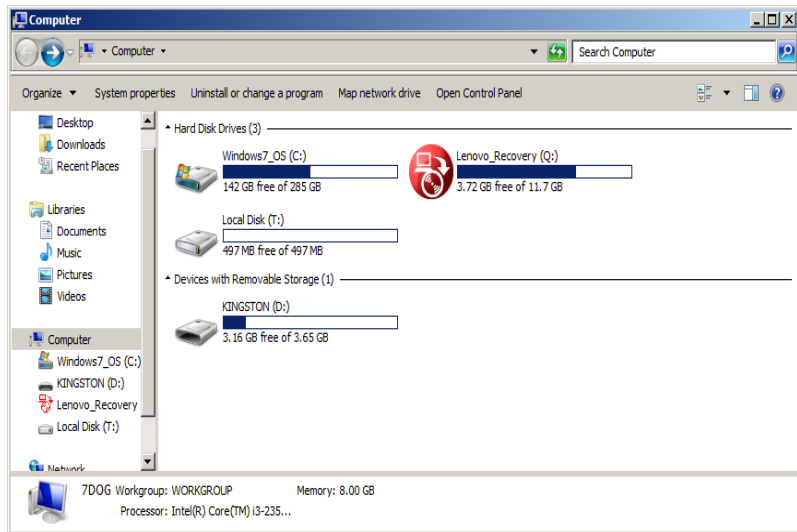
Ausgang nicht verpassen



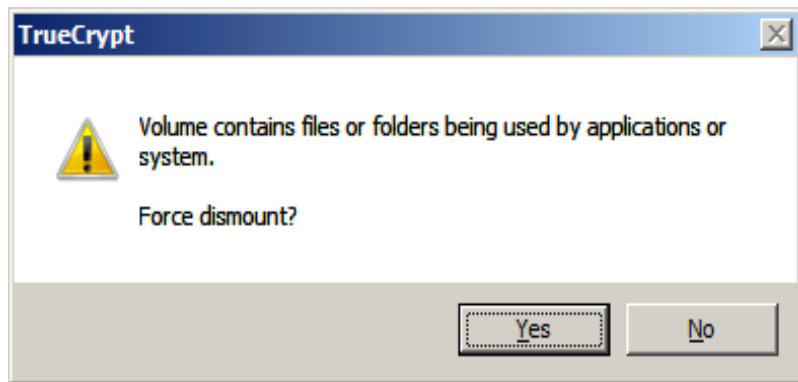
Zugriff auf Beispiel-Laufwerk



Laufwerk ist sichtbar



Zugriff beenden



Fortgeschrittene Themen

- ▶ Non-System-Partitionen
- ▶ System-Partitionen
- ▶ <http://www.truecrypt.org/docs/security-model>
- ▶ Abstreitbarkeit: Plausible Deniability
- ▶ Tarnbetriebssystem
- ▶ Prüfung bzgl. Verschlüsselungserfolg
Sysinternals Suite, DiskView
- ▶ SSDs
- ▶ Forensics
<http://volatility-labs.blogspot.com/2014/01/truecrypt-master-key-extraction-and.html>

SSD

- ▶ Solid State Disk
- ▶ Flash Speicher
- ▶ Jede Speicherzelle verträgt nur kleine (10000) Zahl Schreibvorgänge
- ▶ Lösung: gleichmässiges Beschreiben, Wear-Leveling
- ▶ Problem: Löschen ist langsam
- ▶ Problem: Überschreiben schreibt Daten woanders hin, alte Daten bleiben gespeichert
- ▶ Geschwindigkeit nimmt ab