DATEI- UND FESTPLATTENVERSCHLÜSSELUNG

MIT TRUECRYPT

„The lesson here is that it is insufficient to protect ourselves with laws;
we need to protect ourselves with mathematics.
Encryption is too important to be left solely to governments.“

Bruce Schneier, 1996

PIRATEN PARTEI

ELZPIRATEN EMMENDINGEN

INHALT

- Wieso sollte ich Dateien verschlüsseln?
- Was sollte man beim Verschlüsseln beachten?
- Weshalb sollte ich TrueCrypt einsetzen?
- Wie erstelle ich eine Container-Datei?
- Wie verwende ich eine Container-Datei?
- Wie greife ich unterwegs auf meine Daten zu?

WIESO SOLLTE ICH DATEIEN VERSCHLÜSSELN?

- Schutz vor Diebstahl oder Verlust mobiler Rechner und Datenträger
- Teilen eines Rechners mit weiteren Personen (Familienmitglieder, WG-Mitbewohner, …)
- Hardware-Reparaturdienste erhalten kaputte Geräte inkl. darauf gespeicherter Daten
- Nutzung eines Cloud-Anbieters

WIESO SOLLTE ICH DATEIEN VERSCHLÜSSELN?

- Problemloser Wiederverkauf eines Datenträgers (Vorsicht bei Flash-Speichern)
- (Unrechtmäßige) Durchsuchungen von Wohnungen oder Smartphones durch Polizeibehörden
- Daten elektronischer Geräte können ohne Verdacht beim Grenzübertritt von Behörden eingesehen und kopiert werden (z.B. USA)

WAS SOLLTE MAN BEIM VERSCHLÜSSELN BEACHTEN?

- Ein laufendes System ist u.a. anfällig für:
  - Ausspähen des Passwortes während der Eingabe (Blick über die Schulter, Überwachungskamera, Keylogger, ...)

  - Ausspionieren von Daten durch Trojaner während der Container entschlüsselt ist
  - Das direkte Auslesen des Schlüssels aus dem Speicher mit Hilfe eines FireWire-Anschlusses
  - Das Auslesen des Schlüssels aus dem Speicher nach Tiefkühlen und Entfernen der RAM-Bausteine

WAS SOLLTE MAN BEIM VERSCHLÜSSELN BEACHTEN?

- Verschlüsselung steht und fällt mit der Wahl des richtigen Passwortes
  - Zu kurze Passworte lassen sich mittels Brute-Force-Attacke ermitteln
  - Zu einfache sind anfällig für Wörterbuchangriffe
  - Ein sicheres Passwort sollte dennoch merkbar sein
  - Passwortverlust = Datenverlust
  - Niemals unverschlüsselt Passwörter auf der Festplatte ablegen (SpyWare, Trojaner)

WAS SOLLTE MAN BEIM VERSCHLÜSSELN BEACHTEN?

- Zwang zur Herausgabe des Passwortes
  - Erpressung
  - Strafverfolgung (in GB droht Beugehaft, sollte Beweismaterial auf einem verschlüsselten Datenträger vermutet werden)
  - Gegenmaßnahme: Verschlüsselter Container im verschlüsselten Container (Abstreitbarkeit)

WAS SOLLTE MAN BEIM VERSCHLÜSSELN BEACHTEN?

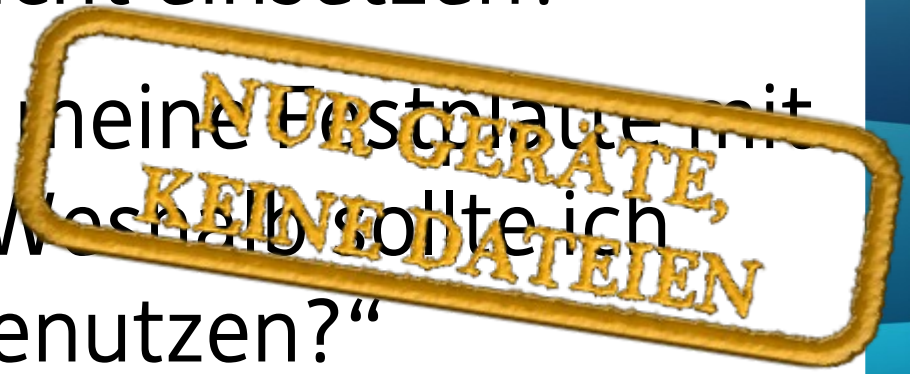
- Datensicherung
  - Ist grundsätzlich sinnvoll ;-)
  - TrueCrypt aktualisiert das Datum des Containers in der Grundeinstellung nicht
  - Backup-Software, die nur das Änderungsdatum einer Datei als Sicherungskriterium verwendet, ignoriert somit den Container
  - Die Windows-Version von TrueCrypt erlaubt es jedoch, das Verhalten zu ändern

WESHALB SOLLTE ICH TRUECRYPT EINSETZEN?

- „Ich bin Windows-Nutzer. Wieso sollte ich nicht EFS (Encrypting File System) oder BitLocker* verwenden?“ (* nur in speziellen Windows-Editionen enthalten)
- „Zum Lieferumfang meines Mac OS X gehört die Verschlüsselungssoftware FileVault. Warum sollte ich diese nicht einsetzen?“
- „Als Linux-User habe ich meine Festplatte mit dm-crypt verschlüsselt. Weshalb sollte ich stattdessen TrueCrypt benutzen?“

WESHALB SOLLTE ICH TRUECRYPT EINSETZEN?

- „Ich bin Windows-Nutzer. Wieso sollte ich nicht EFS (Encrypting File System) oder BitLocker* verwenden?“ (* nur in speziellen Windows-Editionen enthalten)
- „Zum Lieferumfang meines Mac OS X gehört die Verschlüsselungssoftware FileVault. Warum sollte ich diese nicht einsetzen?“
- „Als Linux-User habe ich meine Festplatte mit dm-crypt verschlüsselt. Weshalb sollte ich stattdessen TrueCrypt benutzen?“



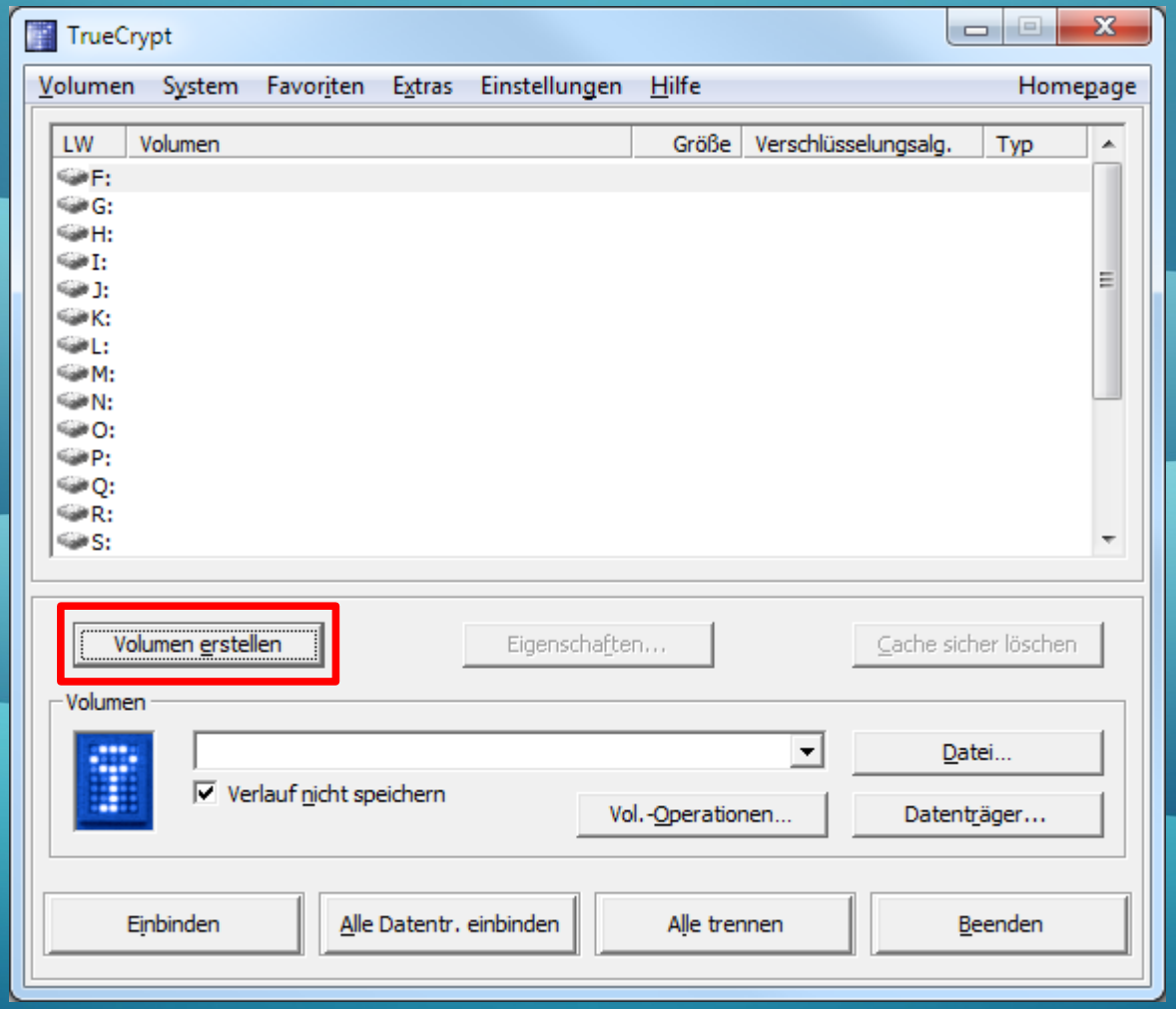
WESHALB SOLLTE ICH TRUECRYPT EINSETZEN?

- Der Programm-Code von TrueCrypt kann von jedem eingesehen werden (Open Source)
- Fehler, aber auch bewusst platzierte Hintertüren können somit entdeckt werden
- Das Ubuntu Privacy Remix Team hat 2011 eine Sicherheitsanalyse des TrueCrypt 7.0a Codes vorgenommen
- TrueCrypt 7.1a (Windows) wurde nachweislich aus dem öffentlichen Quellcode erstellt

WESHALB SOLLTE ICH TRUECRYPT EINSETZEN?

- The TrueCrypt Audit Project strebt an, das Vertrauen in TrueCrypt weiter zu steigern
  - Per Crowdfunding wurden bisher über 60K $ gesammelt, um ein öffentliches Audit des Quelltextes durch Sicherheitsunternehmen (inkl. Bruce Schneier) zu ermöglichen
  - Da die TrueCrypt-Lizenz inkompatibel zu etablierten Open-Source-Lizenzen ist, soll diese ebenfalls angepasst werden

CONTAINER-DATEI ERSTELLEN



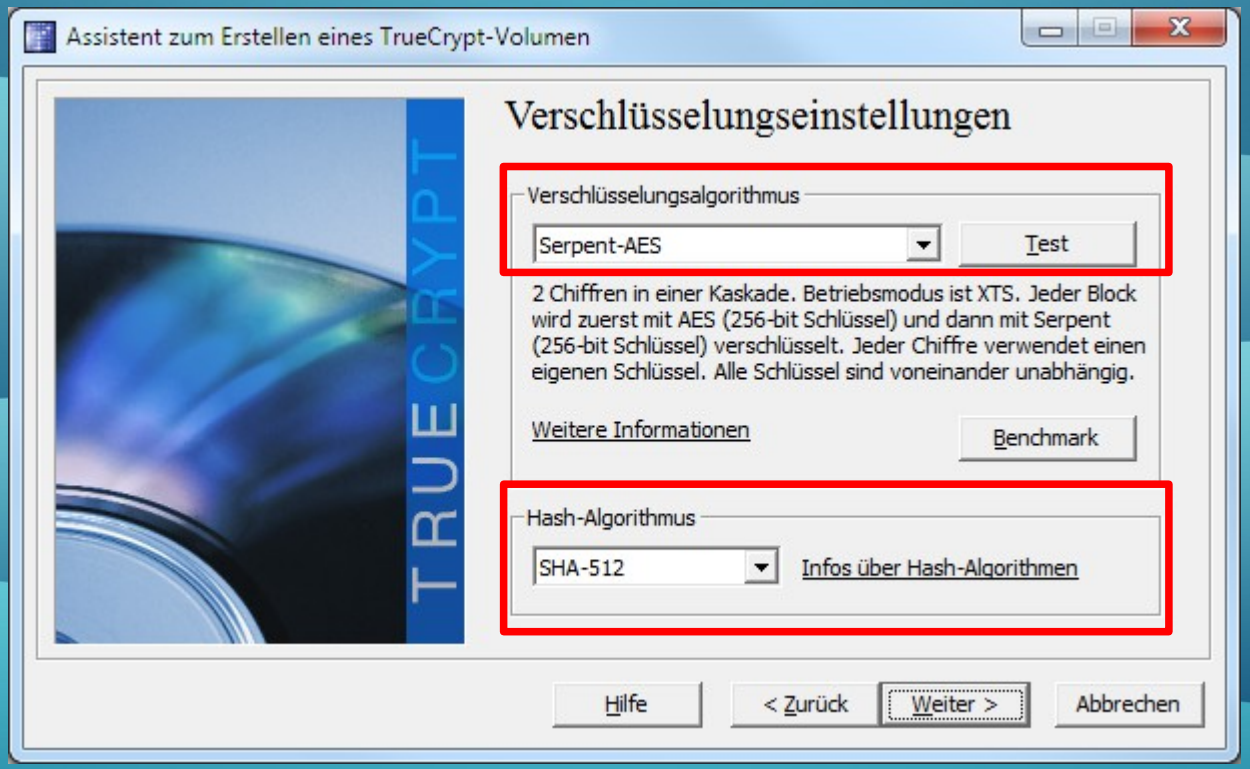
Für die folgenden Screenshots wurde die Windows-Version von TrueCrypt 7.1a verwendet. Die dargestellten Einstellungen dienen als Empfehlung.

CONTAINER-DATEI ERSTELLEN

CONTAINER-DATEI ERSTELLEN

CONTAINER-DATEI ERSTELLEN

CONTAINER-DATEI ERSTELLEN



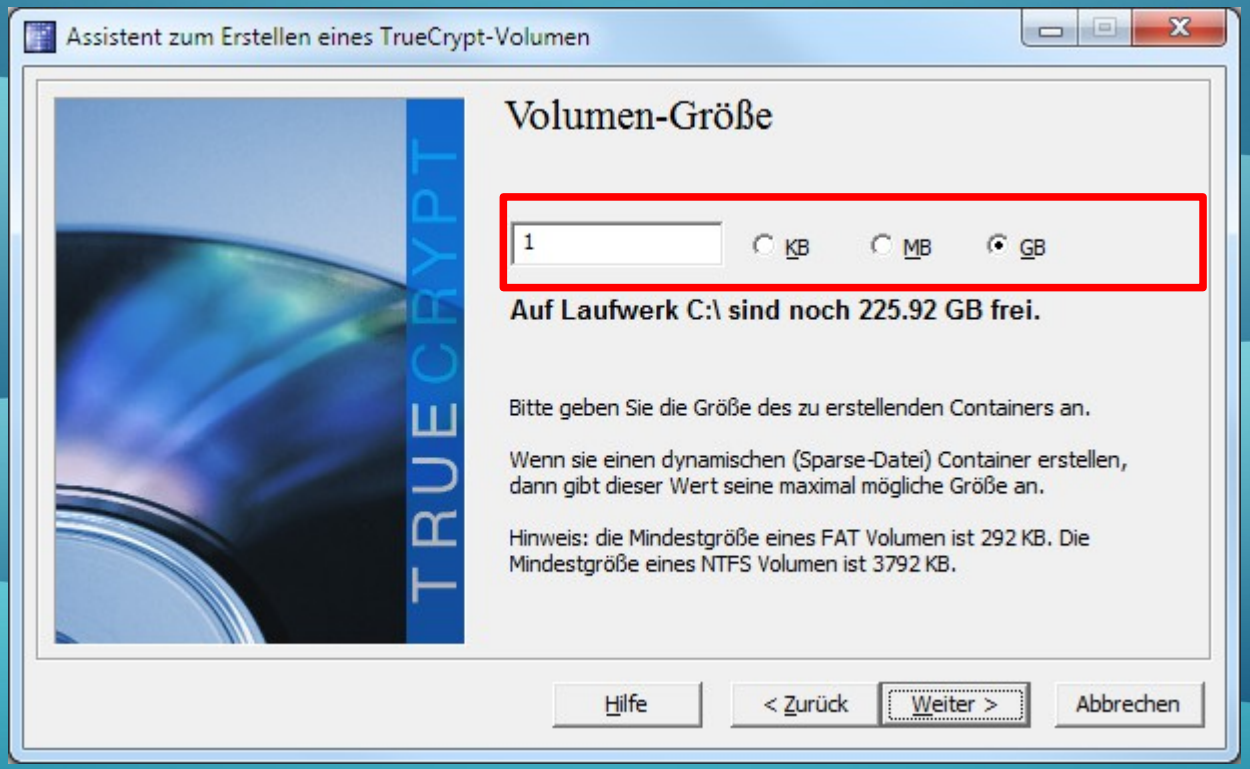
CONTAINER-DATEI ERSTELLEN

- Verschlüsselungsalgorithmus
  - 3 Algorithmen und 8 Kombination möglich
  - AES am schnellsten
  - AES-Twofish-Serpent am langsamsten
  - Standard sollte derzeit Serpent-AES sein
  - Geschwindigkeitssteigerung durch:
    - AES-hardwarebeschleunigte Prozessoren
    - Mehr Prozessorkerne

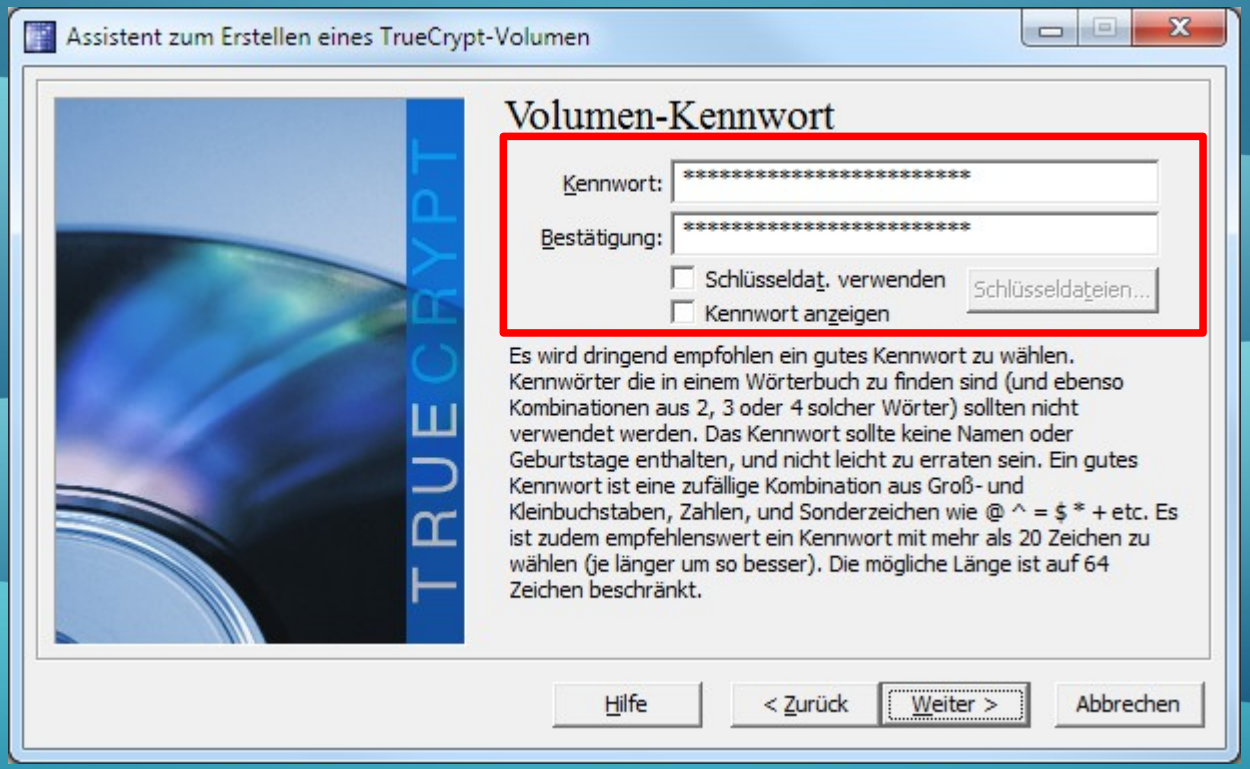
CONTAINER-DATEI ERSTELLEN

- Hash-Algorithmus
  - SHA-512 stammt von der **NSA**!!!
  - Dennoch nutzen, denn der Algorithmus ist sehr gut untersucht und gilt als sehr sicher

CONTAINER-DATEI ERSTELLEN



CONTAINER-DATEI ERSTELLEN



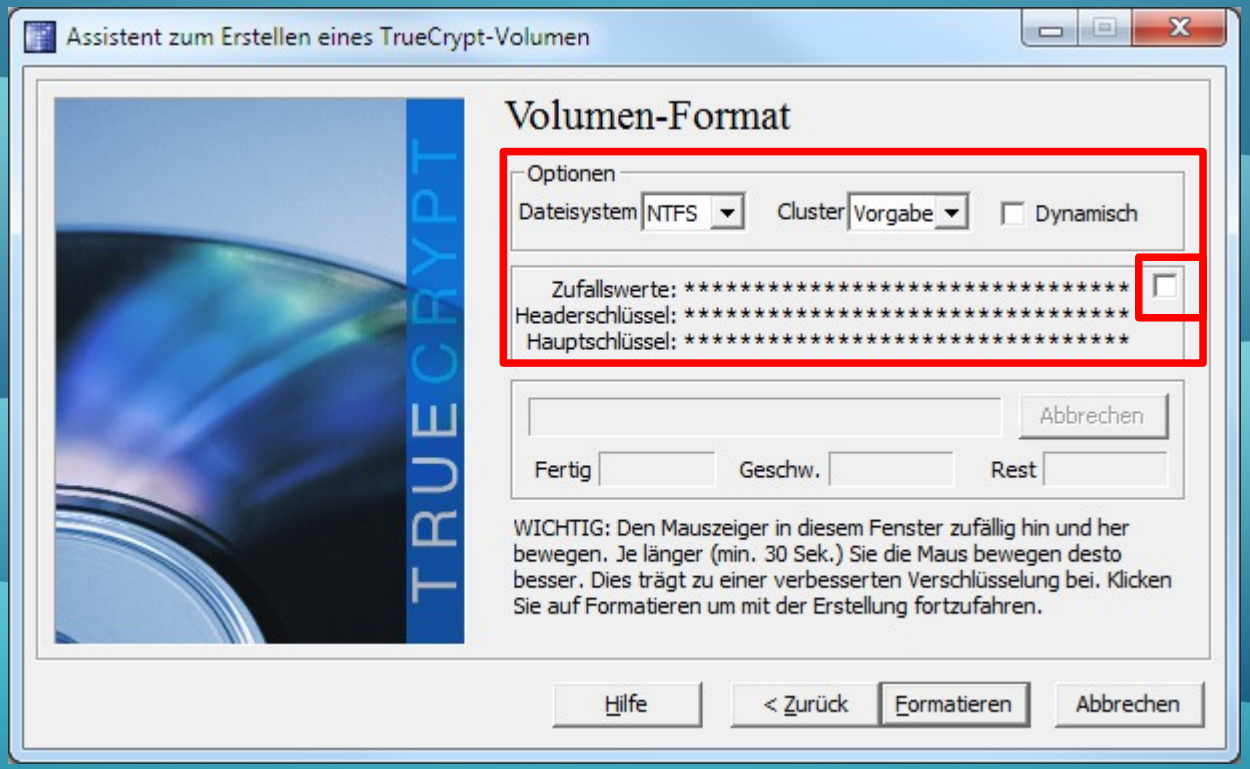
CONTAINER-DATEI ERSTELLEN

- Neben Passwörtern können auch Schlüsseldateien verwendet werden
- Erschwert Brute Force-Attacken
- Verwendung von Security Tokens oder Smart Cards möglich
- Unterschiedliche Schlüsseldateien lassen sich auf verschiedene Benutzer verteilen, so dass man Container nur öffnen kann, wenn alle ihre Schlüsseldatei dazu beitragen

CONTAINER-DATEI ERSTELLEN

- Schlüsseldateie/n sollte/n komprimierte Daten enthalten (z.B. JPG, MP3, ZIP)
- Besser: Schlüsseldateien mit Zufallsdaten von TrueCrypt erzeugen lassen
- **Achtung!** Angriff auf Schlüsseldateien bekannt (siehe Sicherheitsanalyse von TrueCrypt 7.0a)
- Darum **grundsätzlich** ein Passwort und **nie** nur alleinig Schlüsseldateien verwenden

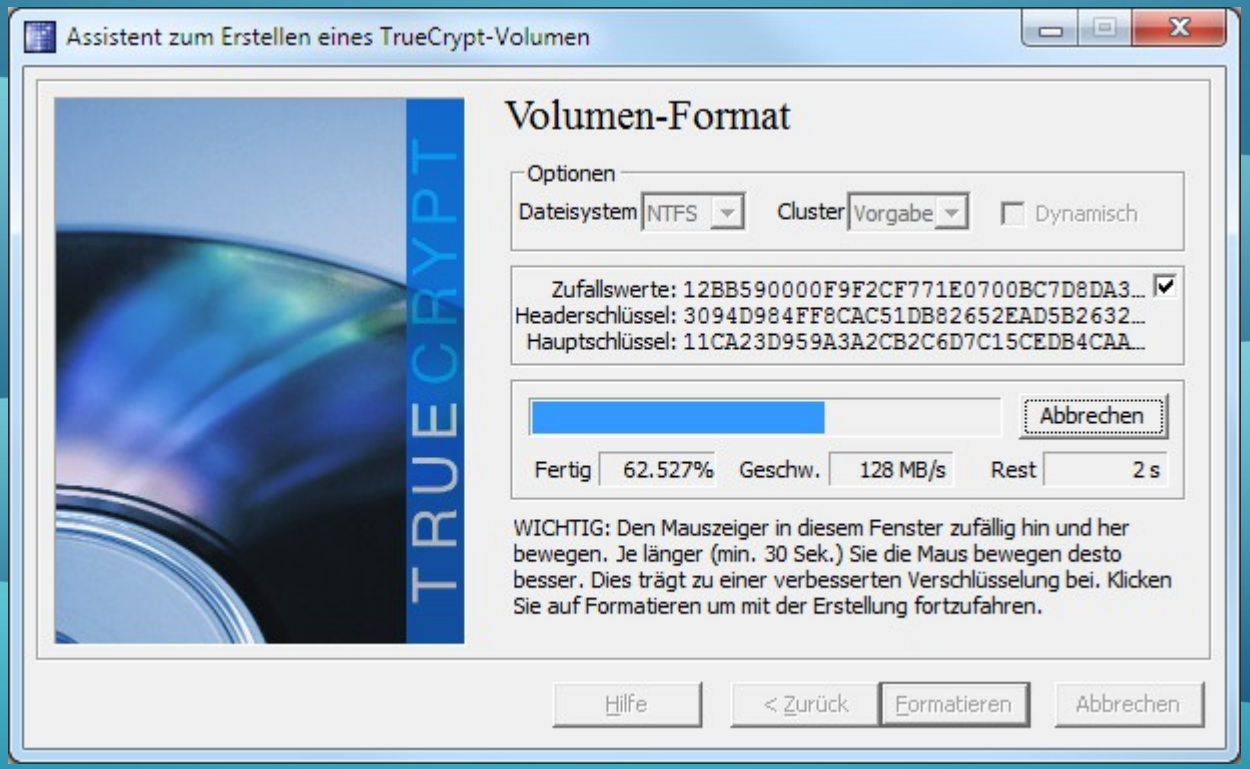
CONTAINER-DATEI ERSTELLEN



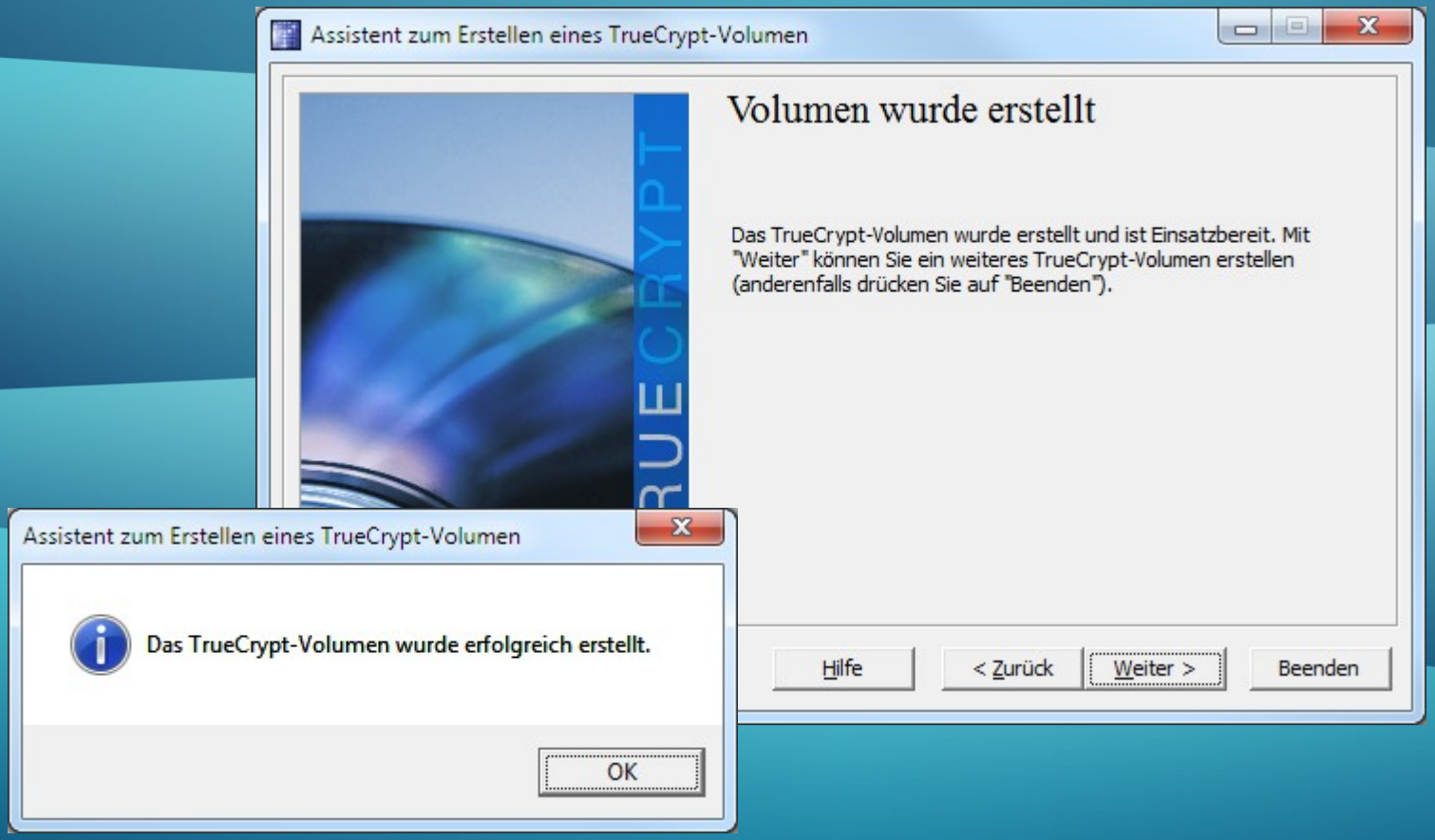
CONTAINER-DATEI ERSTELLEN

- Für größtmögliche Interoperabilität sollte man FAT32 oder NTFS als Dateisystem wählen
- Aus Sicherheitsgründen auf folgendes achten:
  - Bei NTFS unbedingt auf dynamische Partitionsgrößen verzichten
  - NTFS (und andere Journaling File Systems) am besten nur bei Komplettverschlüsselung einsetzen
  - FAT32 am sichersten, mit der Einschränkung, dass eine Datei max. 4 GiB - 1 Byte groß sein kann

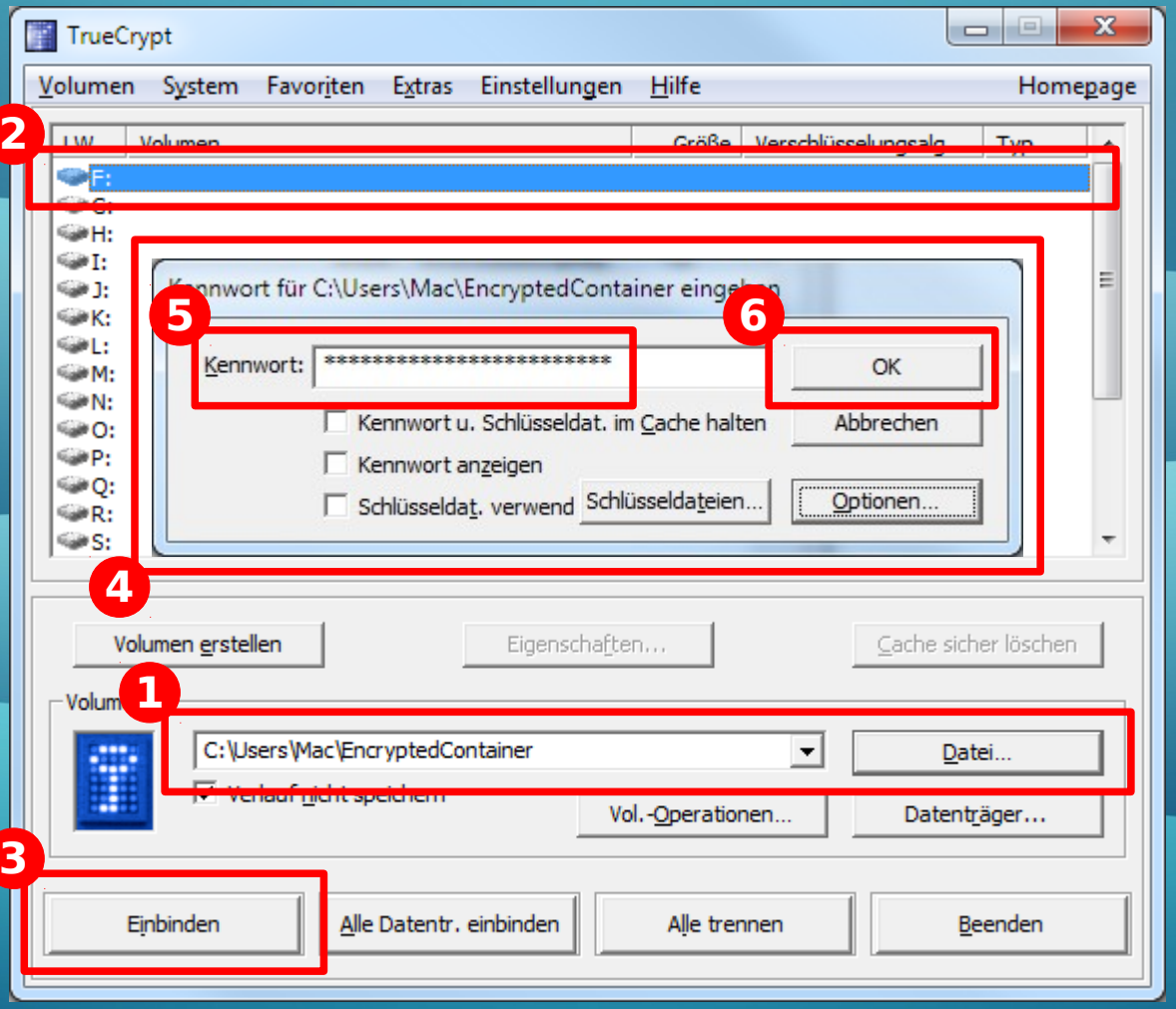
CONTAINER-DATEI ERSTELLEN



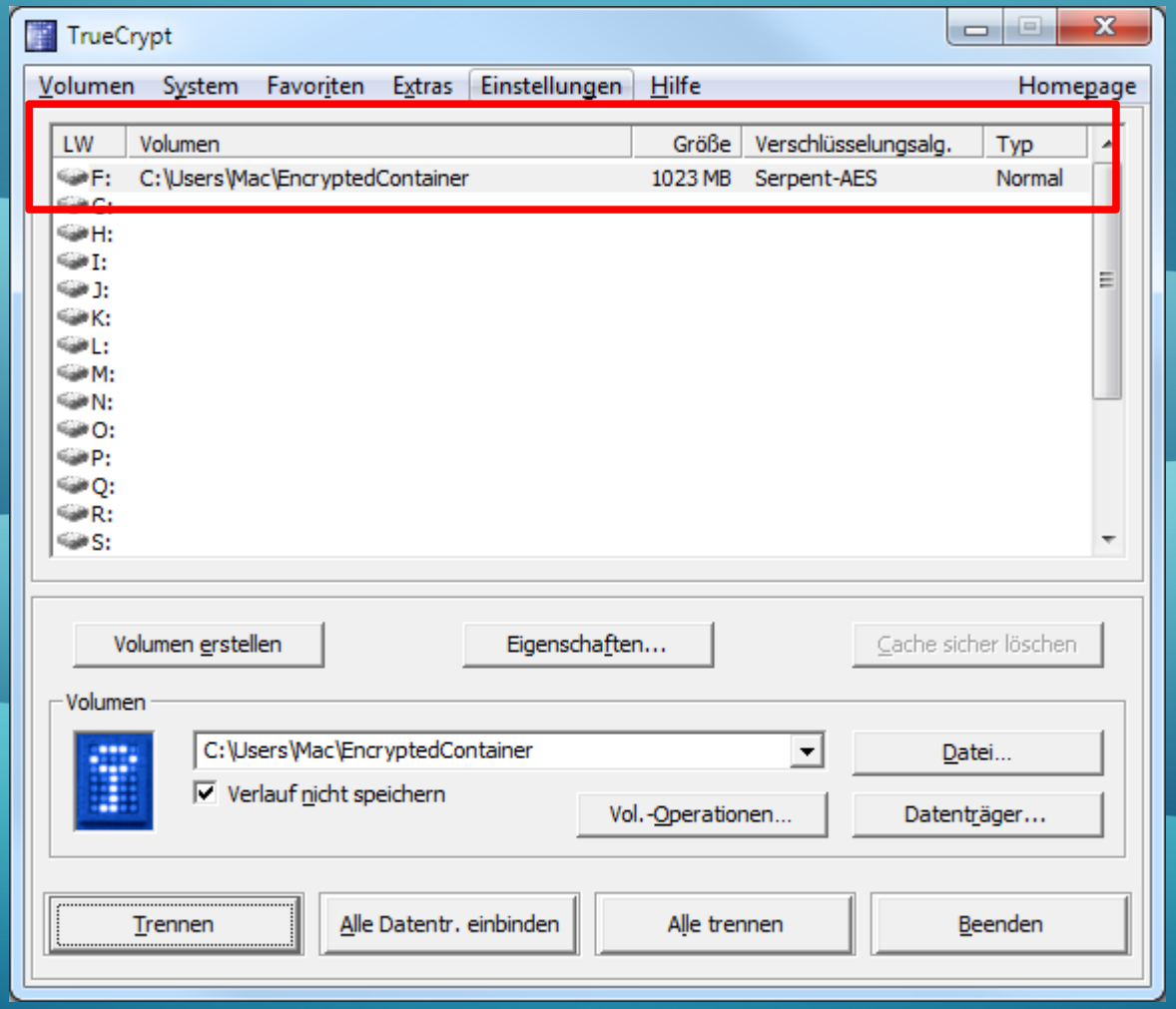
CONTAINER-DATEI ERSTELLEN



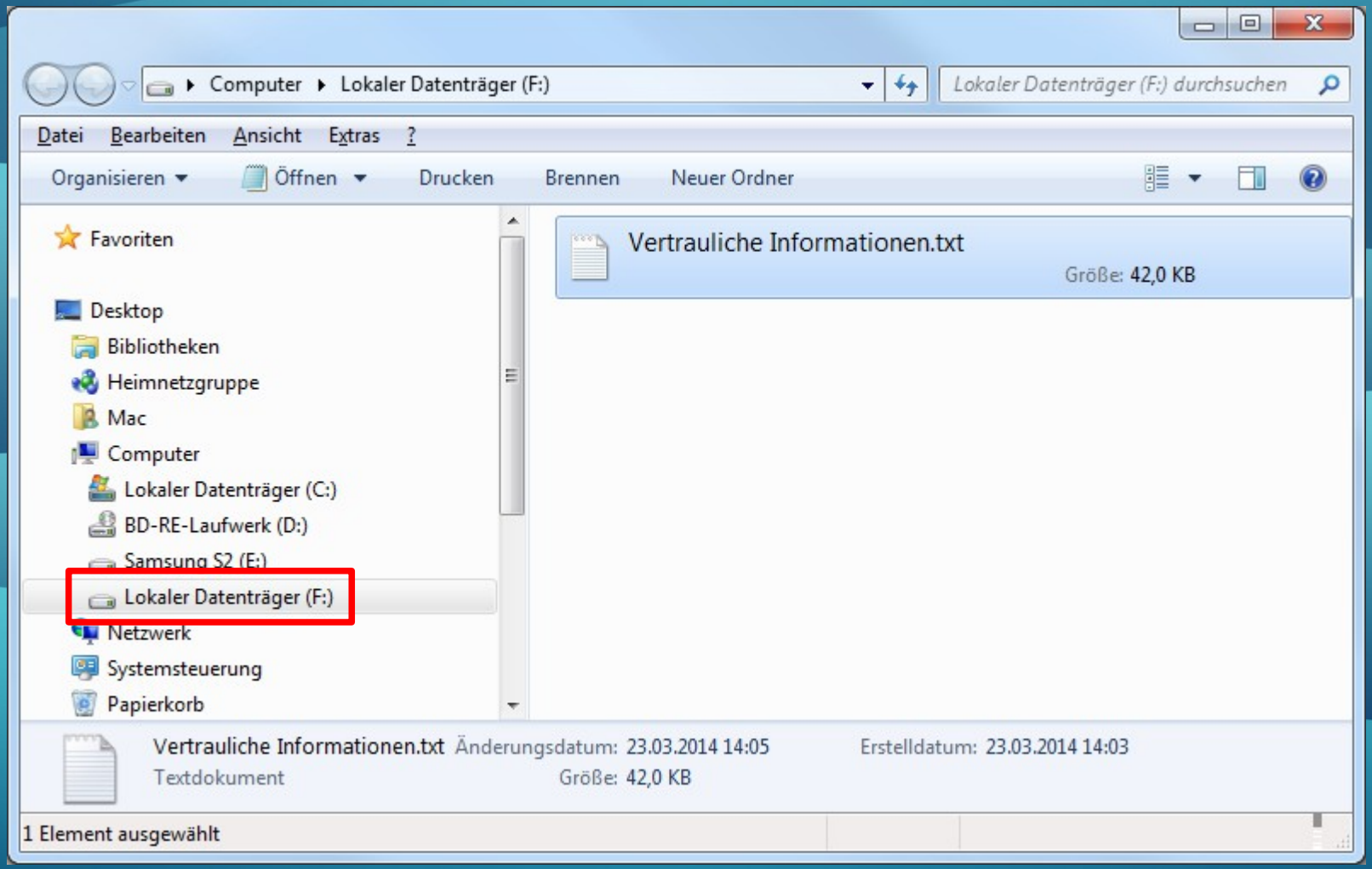
CONTAINER-DATEI VERWENDEN



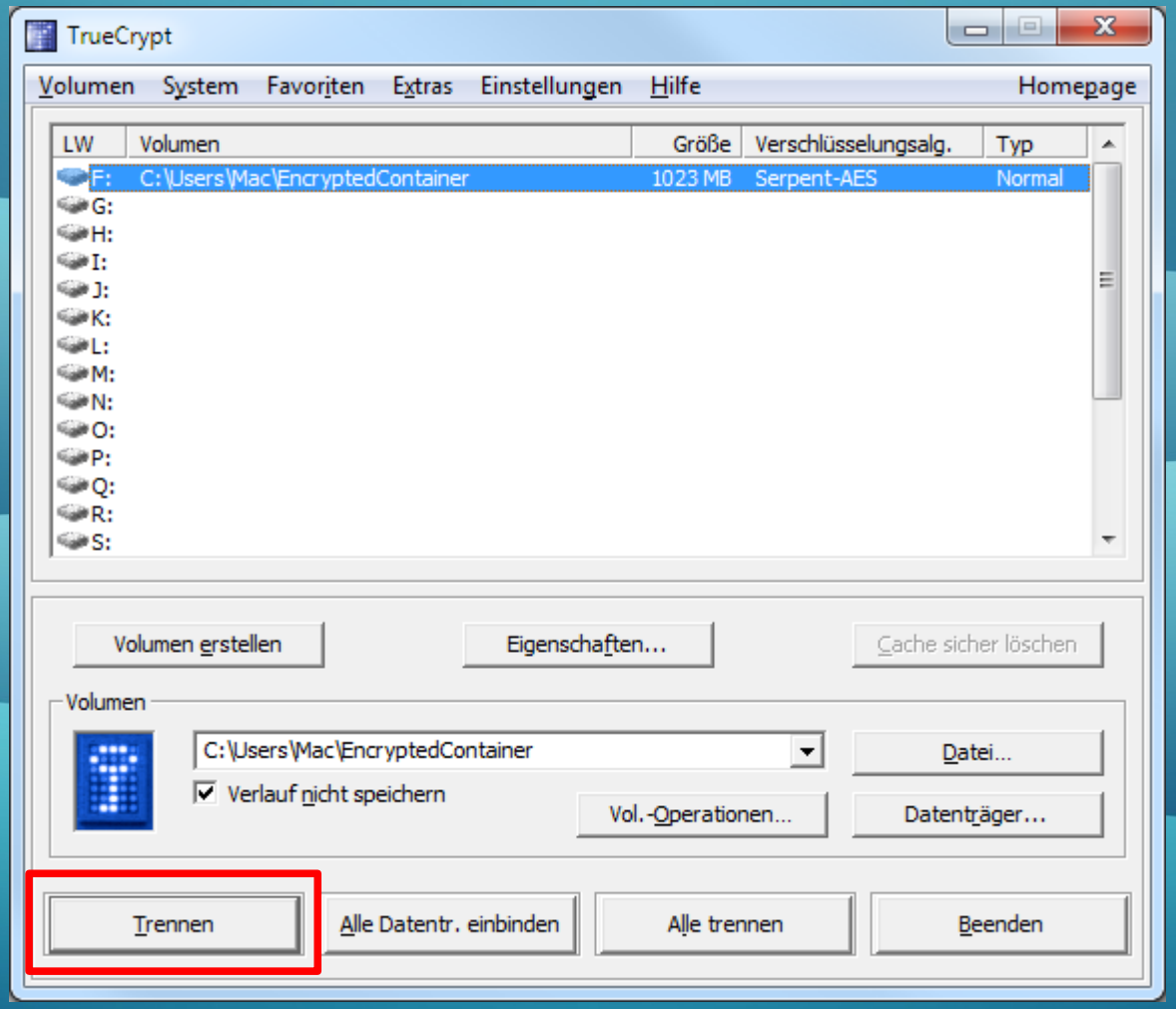
CONTAINER-DATEI VERWENDEN



CONTAINER-DATEI VERWENDEN



CONTAINER-DATEI VERWENDEN



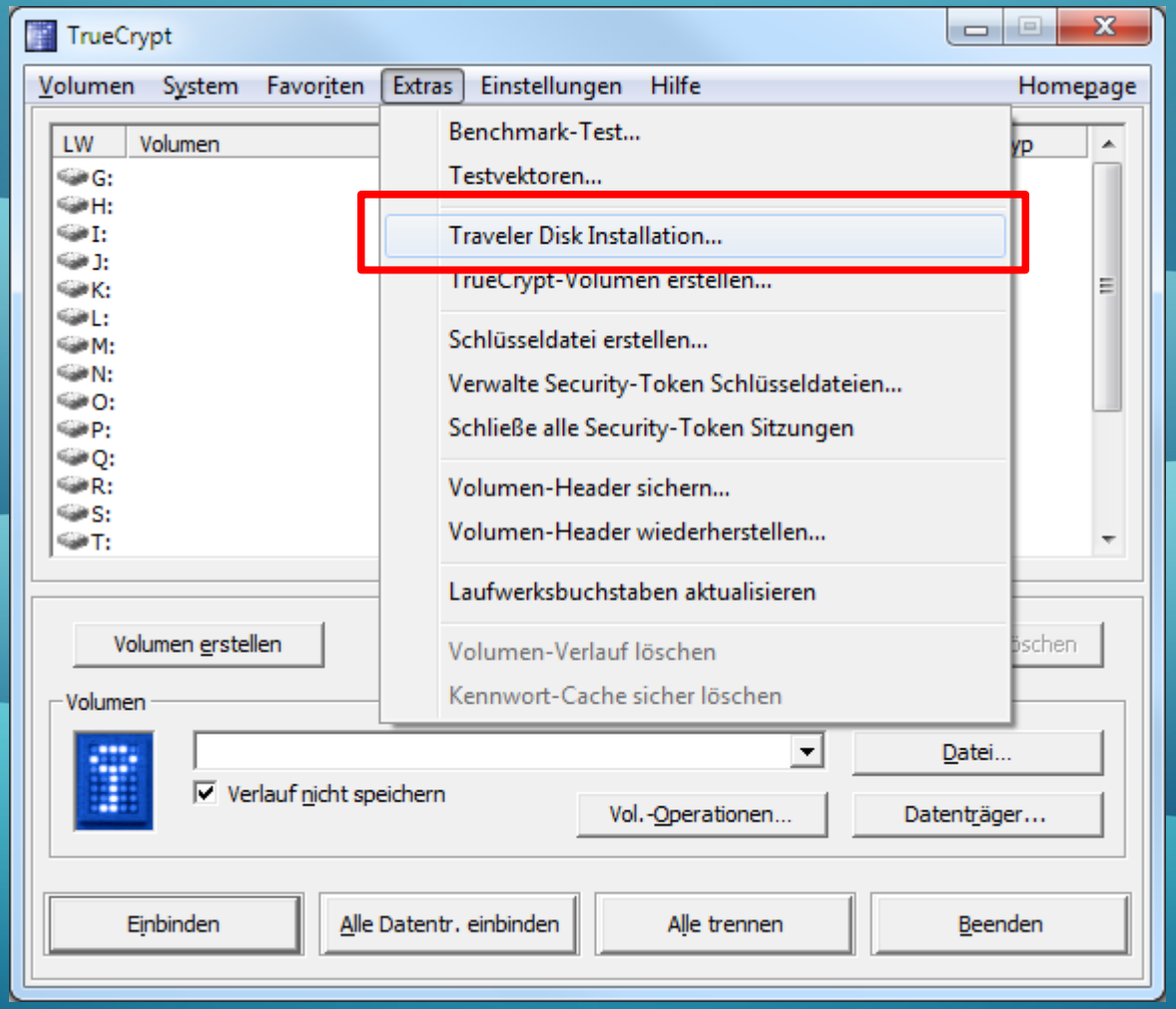
CONTAINER-DATEI TO GO

- „Und was mache ich, wenn ich nun an einem fremden Rechner sitze und dort auf die verschlüsselten Dateien meiner mobilen Festplatte zugreifen möchte?“
- „Du erstellst dir eine Traveler Disk.“
  - Die Windows-Variante enthält einen Assistenten
  - Bei den Mac OS X- und Linux-Versionen genügt es die ausführbare Programmdatei auf den (mobilen) Zieldatenträger zu kopieren

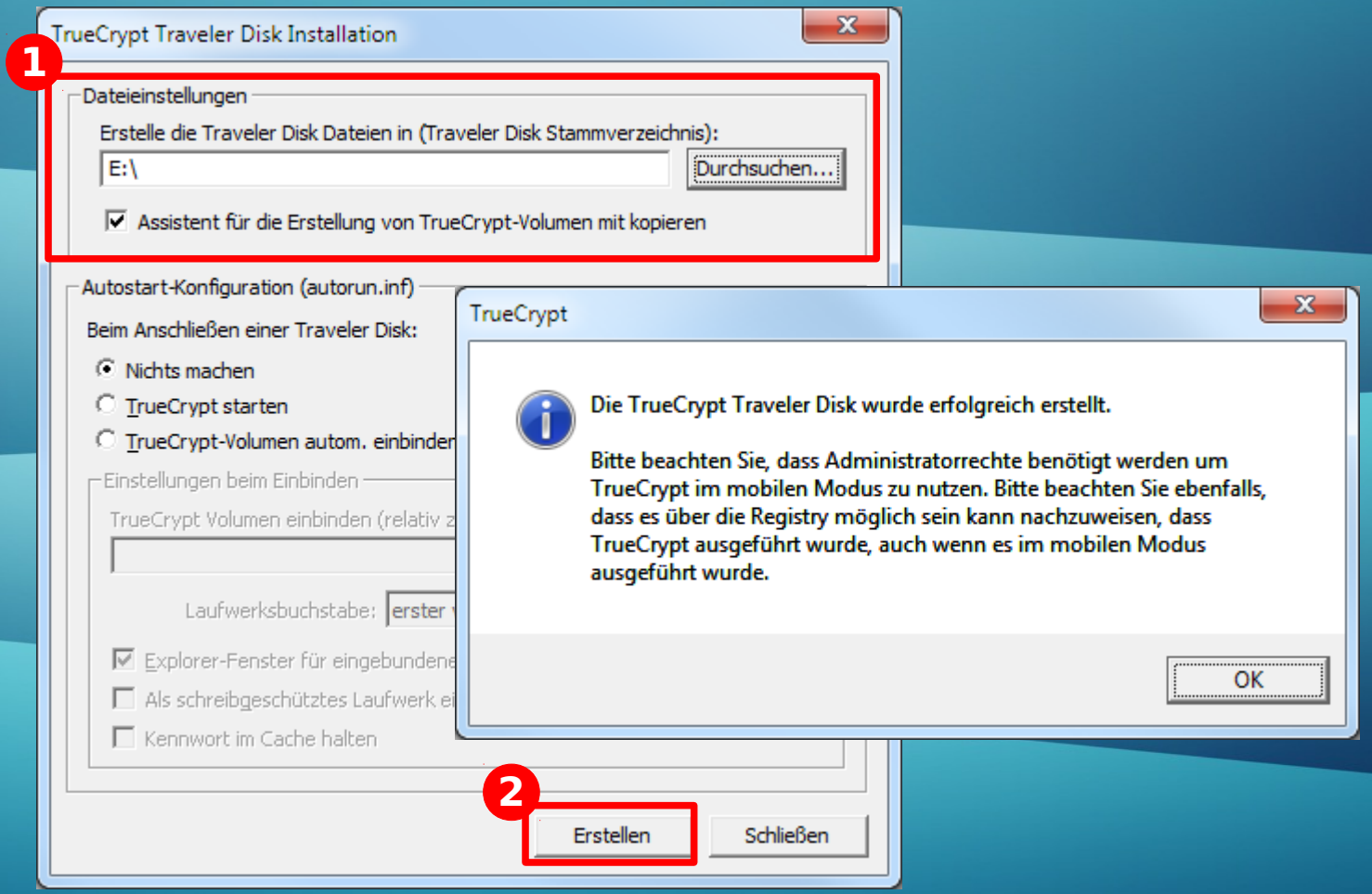
CONTAINER-DATEI TO GO

- Am besten alle drei portablen Versionen auf das Zielmedium mit dem Container kopieren, um im Falle des Falles handlungsfähig zu sein
- Hinweis: Im sogenannten „Portable Mode“ benötigt TrueCrypt Administrationsrechte!

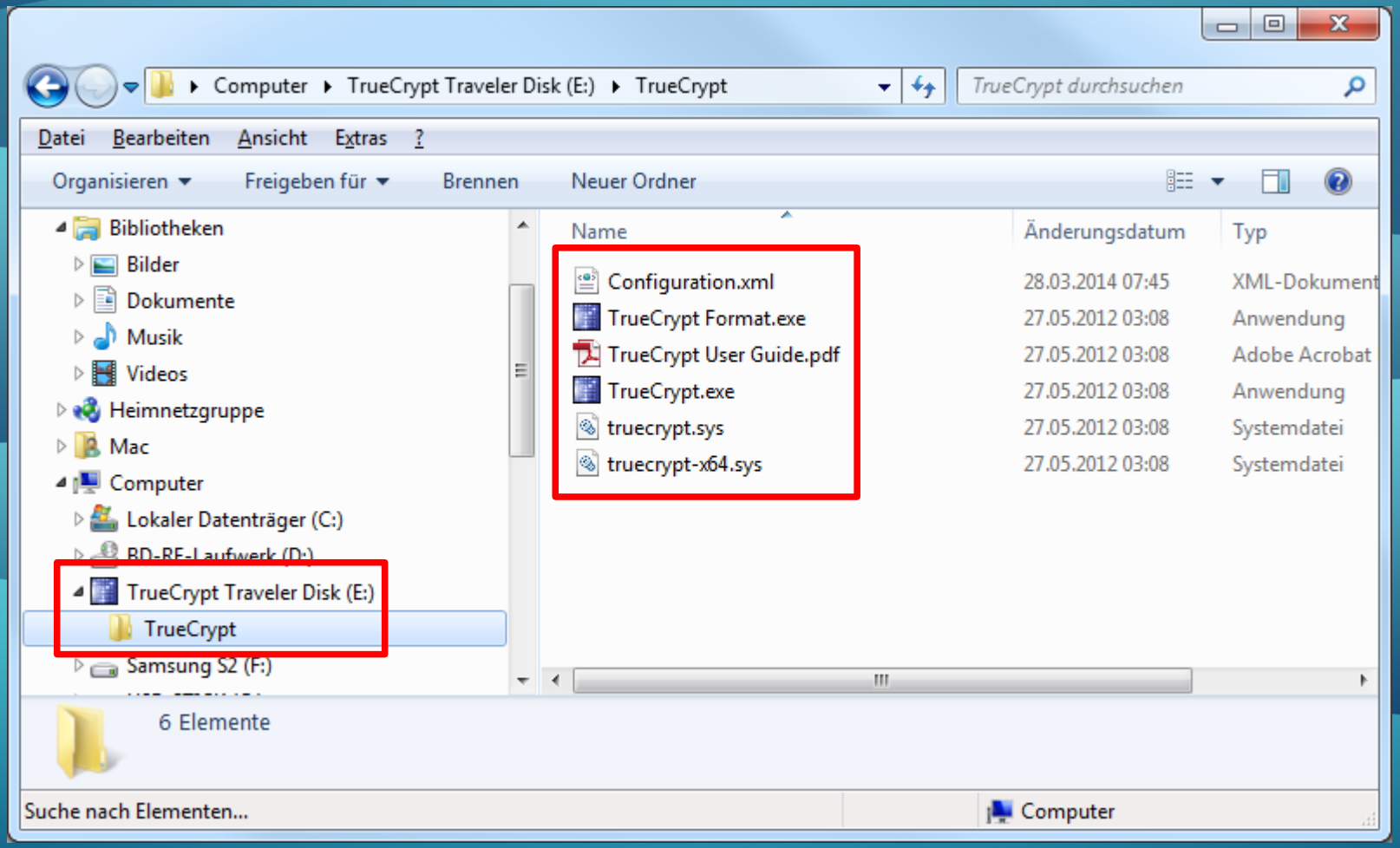
CONTAINER-DATEI TO GO



CONTAINER-DATEI TO GO



CONTAINER-DATEI TO GO



DISCLAIMER

- Dieser Vortrag enthält Vereinfachungen.
- Er ist nach bestem Wissen und Gewissen erstellt, kann aber Fehler enthalten und erhebt deshalb keinen allgemeinen Wahrheitsanspruch.
- Fragt und forscht im Zweifelsfall selbst nach. Die Verantwortung liegt bei Euch.

FRAGEN?

QUELLEN

- TrueCrypt
  - Website des Projekts
  - Downloadseite des Programms
  - Downloadseite der Sprachpakete
  - Dokumentation (engl.)
  - Sicherheitsanalyse von TrueCrypt 7.0a mit einem Angriff auf das Schlüssel-Datei-Verfahren
  - The TrueCrypt Audit Project
- Presse-/Blog-Artikel
  - Nur noch wenige Staaten beschränken die Benutzung starker Verschlüsselung (Telepolis)
  - Nicht immer mit geheimen Informationen (Telepolis)
  - Millionen Briten von Datenpanne betroffen (heise online)
  - Britischen Behörden gehen erneut Millionen Daten verloren (heise online)

QUELLEN

- Presse-/Blog-Artikel
  - Daten von hunderttausenden Patienten sind in Großbritannien verloren gegangen (heise online)
  - E-Mail-Adresse gekapert – Hausdurchsuchung (law blog)
  - Britische Behörden vermissen Datenträger mit Informationen über gefährliche Straftäter (heise online)
  - Verschlüsselung der Festplatte – Wofür das denn? (weigandtLabs)
  - Daten verschlüsselt: Ab in den Knast! (ZDF-Blog Hyperland)
  - Einreisebestimmungen: Wie man die US-Grenze mit seinen Daten überschreitet (Golem.de)
  - Wie mein Smartphone von der Polizei durchsucht wurde (Blog von Andreas Baum)
  - USA: Verfassung wird mit Grenzkontrollen ausgehebelt (heise online)
  - Der Weg zu einem verlässlicheren TrueCrypt (heise online)
  - Verschlüsselungssoftware TrueCrypt: Ein Zweifel weniger (heise online)

QUELLEN

- Presse-/Blog-Artikel
  - US-Gericht: Laptops dürfen ohne Verdacht durchsucht werden (Deutsche Wirtschafts Nachrichten)
- Wikipedia
  - BitLocker
  - Encrypting File System
  - Festplattenverschlüsselung
  - FileVault
  - FireWire
  - Glaubhafte Abstreitbarkeit
  - Kaltstartattacke
  - Social Engineering
  - Solid-State-Drive

QUELLEN

- Wikipedia
  - TrueCrypt
  - Ubuntu Privacy Remix
- Verschlüsselung bei Solid-State-Drives (SSD)
  - SSD verschlüsseln (heise online)
  - Secure-Erase (ubuntuusers.de-Wiki)
  - Verschlüsselung (ubuntuusers.de-Wiki)
- Sonstiges
  - Die etwas andere Art der RAM-Analyse (computer-forensik.org)
  - M 2.167 Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten (BSI)
  - System verschlüsseln (ubuntuusers.de-Wiki)