Bildungsakademie Mittweida e.V.

COMPUTERSICHERHEIT II

COMPUTERKURS 2017

DANIEL MEERWALD

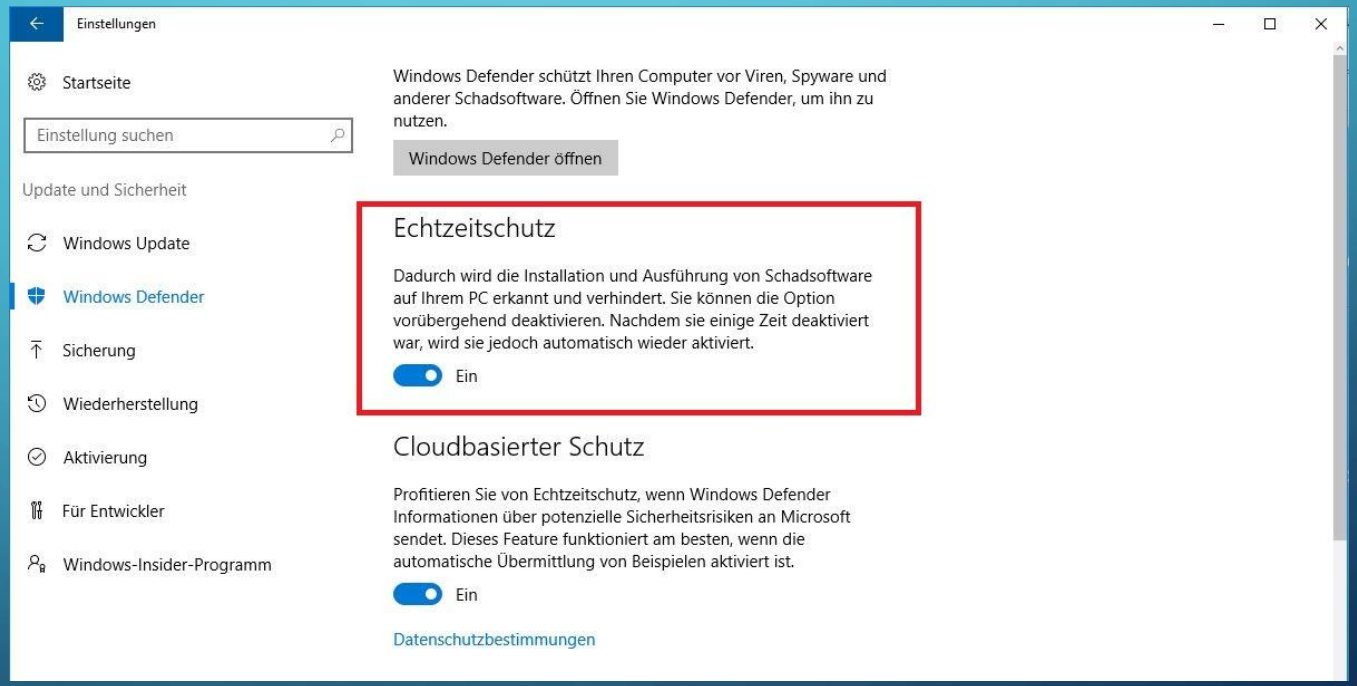
INHALT

- Windows Defender Aktivieren
- Kaspersky Virus Removal Tool und Kaspersky Rescue Disk 10
- Phishing E-Mails erkennen
- Daten verschlüsseln

WINDOWS DEFENDER AKTIVIEREN

Bildungsakademie Mittweida e.V.

- Unter Windows 10:
  1. Wählen Sie die Schaltfläche Start und dann Einstellungen > Update und Sicherheit aus.
  2. Wählen Sie Windows Defender aus und aktivieren oder deaktivieren Sie den Echtzeitschutz.



WINDOWS DEFENDER AKTIVIEREN

Bildungsakademie Mittweida e.V.

- Unter Windows Vista und Windows 7:
  - Sofern kein anderer Virenschutz vorhanden, sollte der Windows Defender unter Windows 7 bereits aktiviert sein.
  - Um den Defender zu einem vollwertigen Virenschutz aufzuwerten, muss aber noch Microsoft Security Essentials installiert werden
  - Die Downloadlinks lauten wie folgt:
    - Für 64Bit Systeme:
      - https://download.microsoft.com/download/0/2/C/02C8AB73-0774-4975-826F-9E8A0FD7F65D/DEDE/amd64/MSEInstall.exe
    - Für 32Bit Systeme:
      - https://download.microsoft.com/download/0/2/C/02C8AB73-0774-4975-826F-9E8A0FD7F65D/DEDE/x86/MSEInstall.exe

KASPERSKY VIRUS REMOVAL TOOL UND KASPERSKY RESCUE DISK 10

Bildungsakademie Mittweida e.V.

- Das Kaspersky Virus Removal Tool (KVRT) ist ein ziemlich mächtiges Tool um gezielt Schadware von ihrem System zu durchsuchen auf dem Standard eines der führenden Unternehmen in Sachen Virenschutz.
  - Vorteil: Das Tool ist kostenfrei und immer top Aktuell
  - Nachteil: Das Tool ist nur ein Tool und kein Antivirensystem. Es muss von Ihnen gestartet werden und durchsucht darauf hin den von Ihnen definierten Speicher nach Schadsoftware.
- Einsatzgebiete:
  - Kleinere Suchläufe auf Verdacht, Durchsuchen von fremden USB-Sticks, Checken einzelner Dateien denen Sie nicht vertrauen

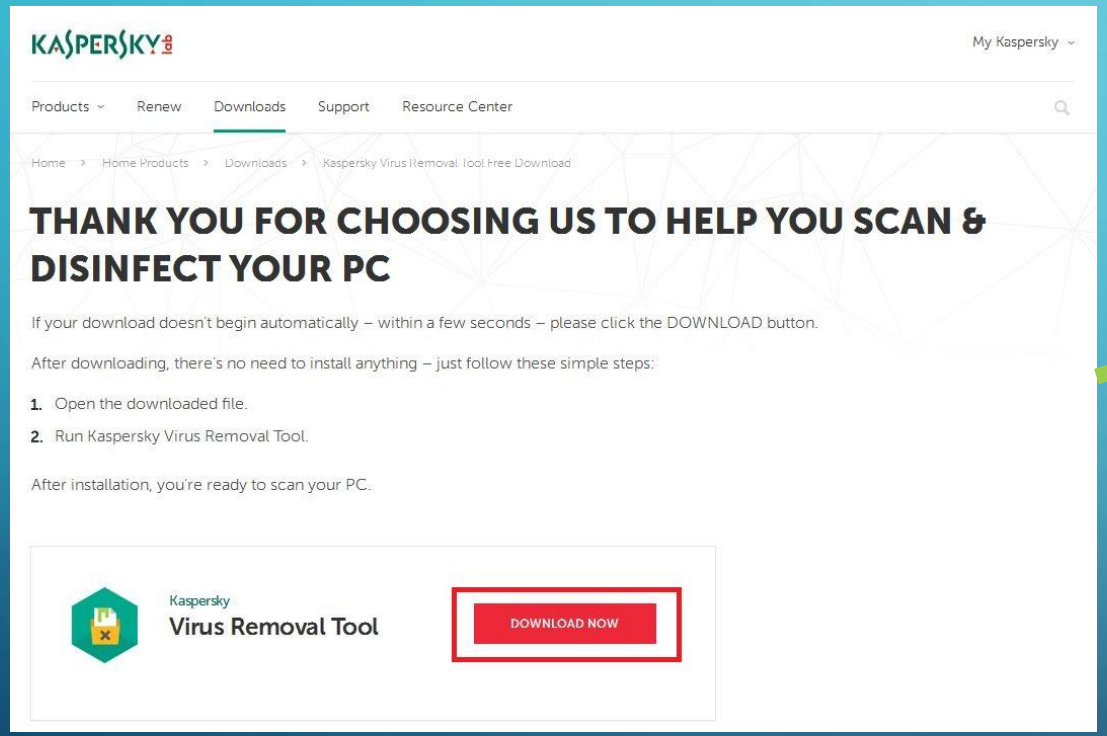
KASPERSKY VIRUS REMOVAL TOOL UND KASPERSKY RESCUE DISK 10

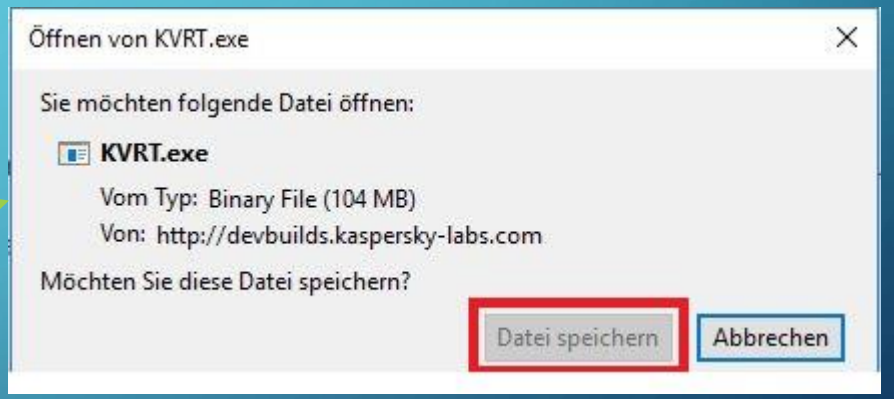
Bildungsakademie Mittweida e.V.

- Kaspersky Rescue Disk 10 (KRD10) ist ein sogenanntes **Live-System** das ihren gesamten Computer nach Schadsoftware durchsucht und dabei Windows nicht startet. Das gibt dem Virus deutlich weniger Chancen, dem „Desinfizieren“ zu entgehen. Die erfolgsrate von KRD10 ist deutlich höher als von jedem Virensystem das auf Windows arbeitet.
  - Vorteil: Höchste Säuberungsrate
  - Nachteil: Relativ langsam, Benötigt Neustart des Systems
- Einsatzgebiete:
  - Zum kompletten Desinfizieren eines Systems nach Virenbefall, ins besondere wenn der Virenscanner den Virus wiederholt nicht vollständig entfernen konnte

KASPERSKY VIRUS REMOVAL TOOL

- Downloadlink:
  - https://www.kaspersky.com/downloads/thank-you/free-virus-removal-tool?form=1

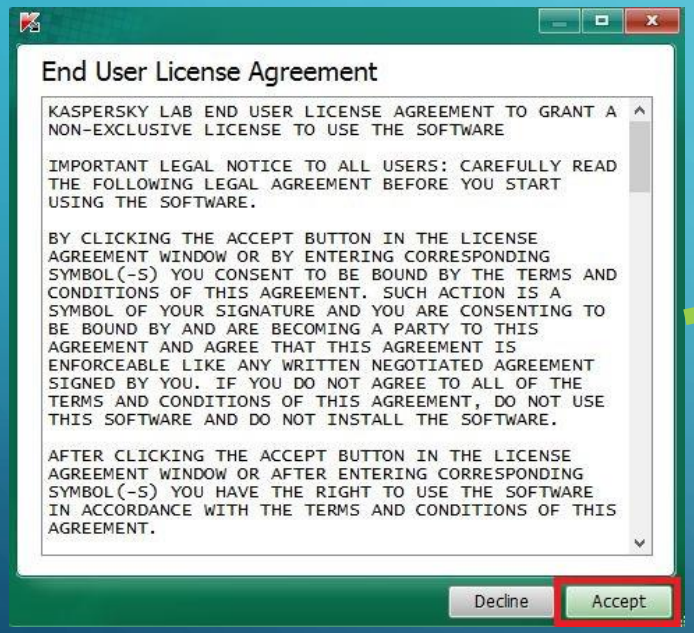


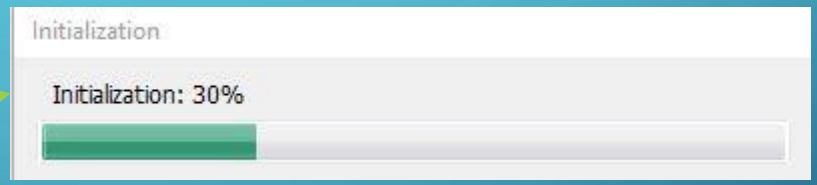


KASPERSKY VIRUS REMOVAL TOOL

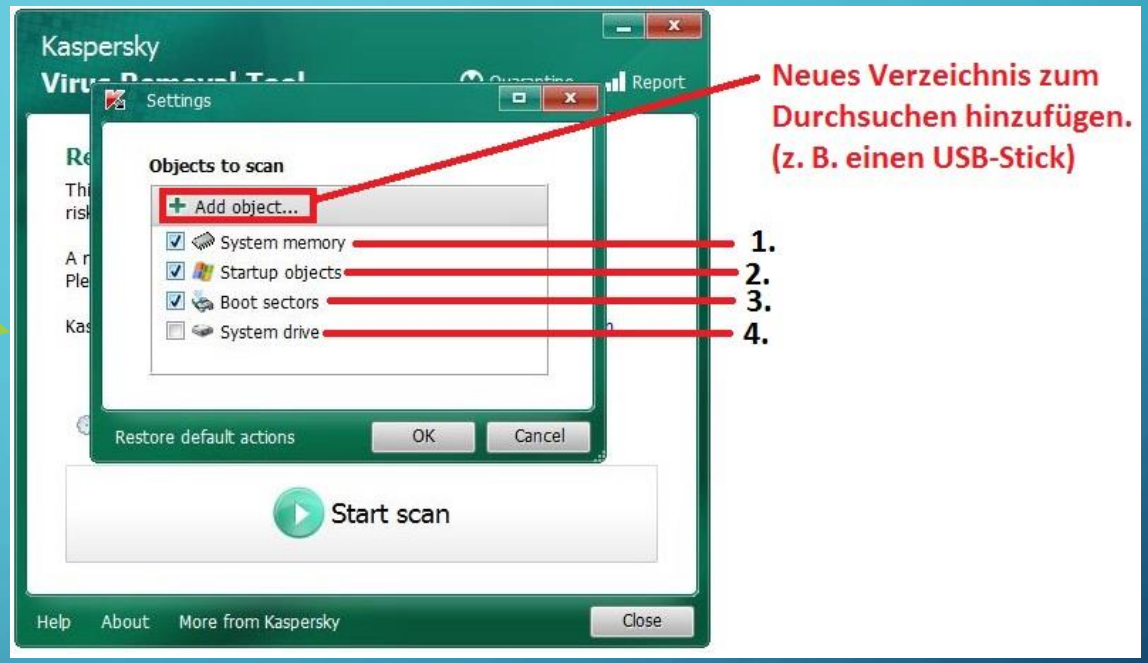
Bildungsakademie Mittweida e.V.

- Die „End-Nutzer-Vereinbarung“ muss akzeptiert werden, danach „Initialisiert“ das Tool sich, dabei holt es die neusten Updates aus dem Internet. Dieser Vorgang kann ein paar Minuten Dauern.



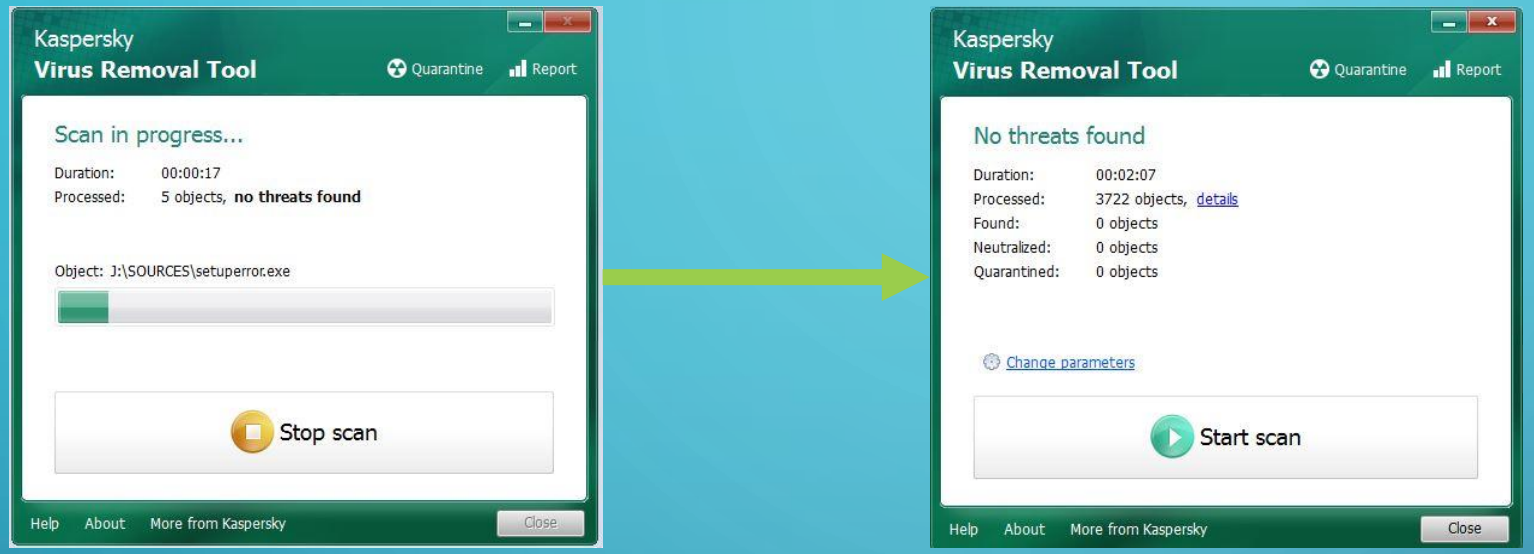


KASPERSKY VIRUS REMOVAL TOOL



1. System RAM durchsuchen, sollte immer an sein.
2. Objekte im Systemstart, sollte auch immer an sein.
3. Objekte im Startbereich der Festplatte, sollte auch immer an sein.
4. Durchsuchen der Festplatte, auf der das System ist. Sinnvoll bei vollständigem Suchlauf, es müssen ggf. andere Vorhandene Festplatten über die Schaltfläche „Add object“ hinzugefügt werden

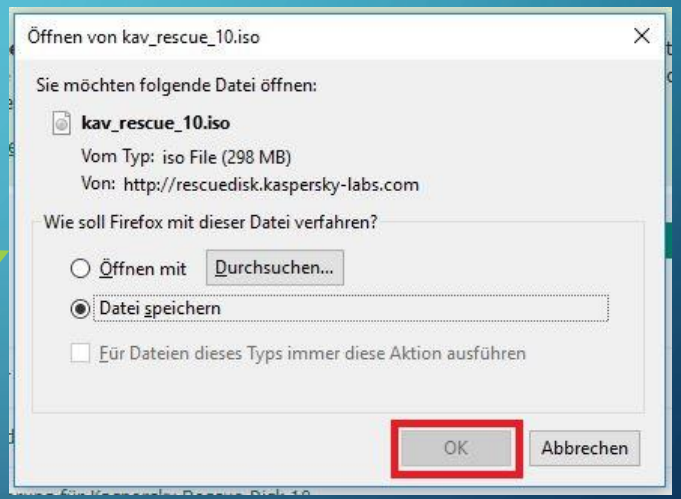
KASPERSKY VIRUS REMOVAL TOOL



- Nach Start (links) des Scans durchsucht das Tool alle angegebenen Pfade.
- Nachdem es fertig ist (rechts) erhalten Sie eine Auflistung aller Funde und Möglichkeiten geboten um darauf zu reagieren, falls etwas gefunden wurde.

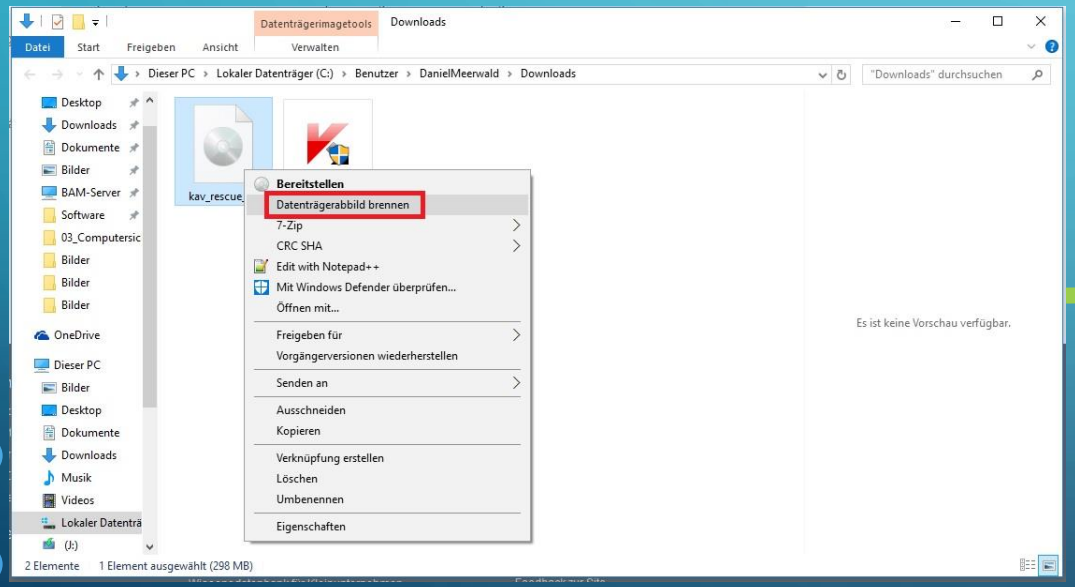
KASPERSKY RESCUE DISK 10

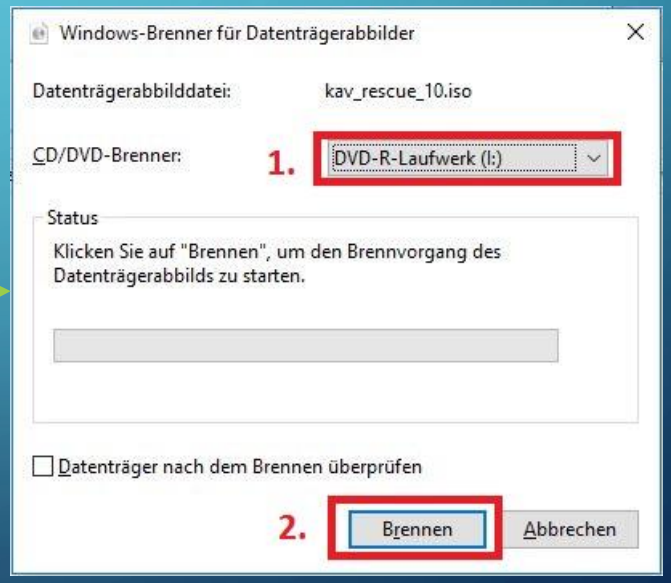
- Downloadlink:
  - https://support.kaspersky.com/de/viruses/rescuedisk



KASPERSKY RESCUE DISK 10

- Nach erfolgreichem Download muss KRD10 auf einen Bootfähigen USB-Stick gepackt werden oder als CD gebrannt werden. Die einfachere Variante ist hier die CD zu brennen. Clicken sie dafür mit der rechten Maustaste auf die fertig herunter geladene „kav_rescue_10.iso“ Datei und dann auf „Datenträgerabbild brennen“ (links). Danach wählen Sie das Brennerlaufwerk mit der Leeren CD und clicken anschließend auf „Brennen“ (rechts).





KASPERSKY RESCUE DISK 10

Bildungsakademie Mittweida e.V.

- Um die Disk nach erfolgreichem Brennen zu benutzen, legen Sie diese in eines der DVD/CD Laufwerke Ihres PC‘s. Anschließend schalten Sie den PC aus warten etwa eine Minute und schalten ihn dann wieder ein.
- Während des Hochfahrens des PC‘s wird ihnen die Möglichkeit geboten „eine beliebige Taste zu drücken um von der CD zu starten“. Diese Anweisung ist recht schnell wieder vom Bildschirm verschwunden, weshalb die Taste Rechtzeitig gedrückt werden muss. Falls Sie es verpassen, PC nochmals ausschalten und nochmals wieder einschalten.
- Nachdem von der CD gestartet wird, müssen Sie ihre Sprache auswählen und welche Version von KRD10 gestartet werden soll.

KASPERSKY RESCUE DISK 10

Bildungsakademie Mittweida e.V.

- Wählen Sie hier „Grafikmodus“ und KRD10 wird Sie grafisch durch die Säuberung ihres Systems führen.
- Nachdem KRD10 gestartet ist, wird ein Menü angezeigt, das dem vom KVRT sehr stark ähnelt.

PHISHING E-MAILS ERKENNEN

Bildungsakademie Mittweida e.V.

- **Wikipedia definiert:** Unter dem Begriff **Phishing** (Neologismus von *fishing*, engl. für ‚Angeln') versteht man Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen.
- Die Angebote in Phishing-Emails sind also nie wirkliche Angebote. Es soll an Ihre Daten gekommen werden und am besten auch noch Geld von Ihnen gezahlt werden, aber die Waren würde nie ankommen.

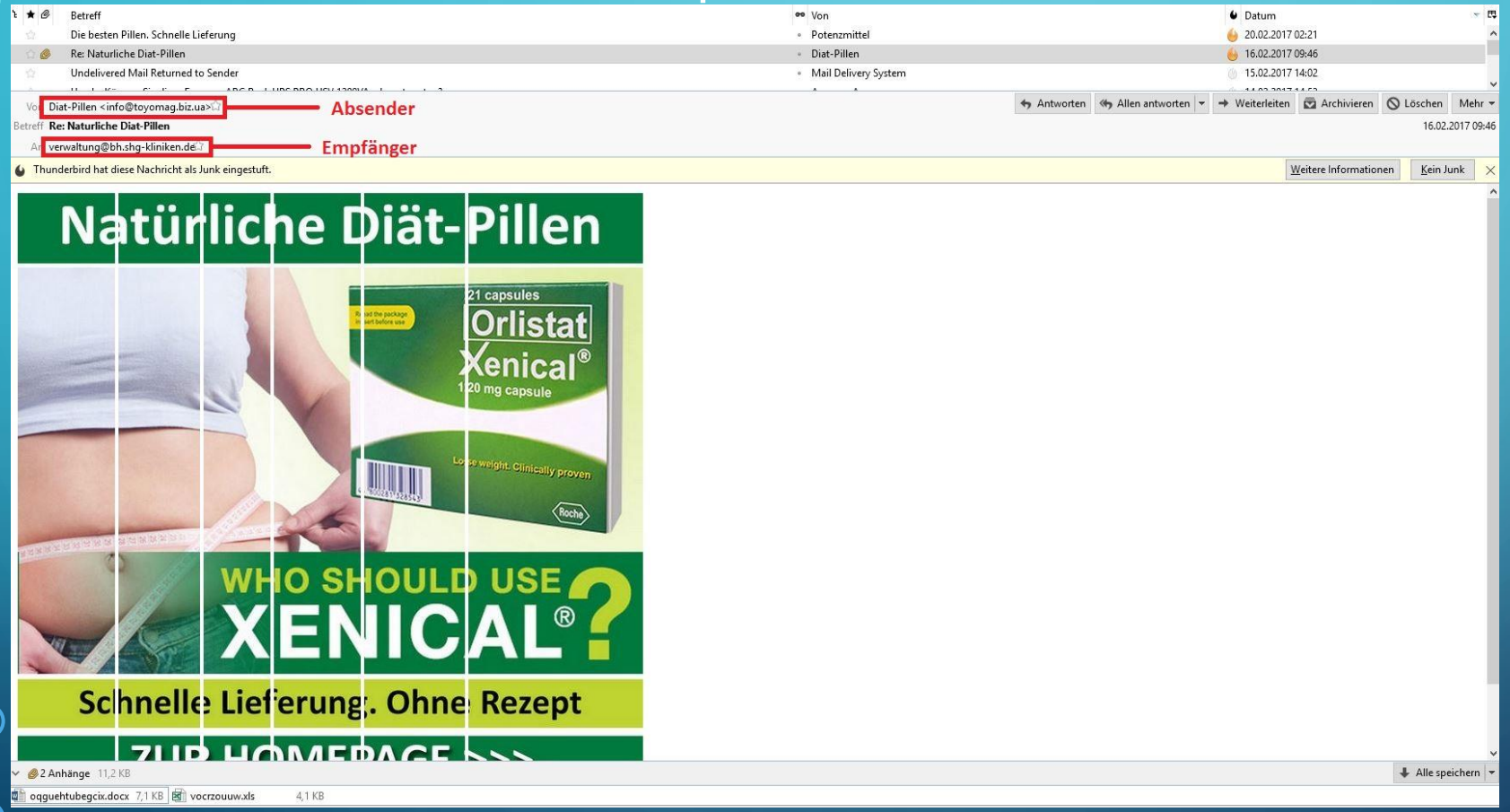
PHISHING E-MAILS ERKENNEN

Bildungsakademie Mittweida e.V.

- Hier wird damit gelockt, das man Viagra Rezeptfrei kaufen kann. Dies ist natürlich nicht möglich, weshalb viele die Chance wittern hier doch ohne ein Rezept an besagtes mittel zu kommen und gehen damit dem Angreifer in die Falle. Alle Angebote die nicht „normal“ sind oder sich in Grauzonen befinden oder zu gut klingen um wahr zu sein sind meist Phishing Emails

PHISHING E-MAILS ERKENNEN

- In unserem Nächsten Beispiel achten wir einmal auf Absender und Empfänger.



Unser Email Programm versucht auf einfache Weise über Schlüsselwörter oder Ähnliches für uns diese Betrügerischen Mails zu sortieren. In diesem Fall hat es Recht und die Mail als „Junk“ (dt. Müll) eingestuft.
Ab und an werden aber auch vertrauenswürdige Mails als „Junk“ eingestuft.

PHISHING E-MAILS ERKENNEN

Bildungsakademie Mittweida e.V.

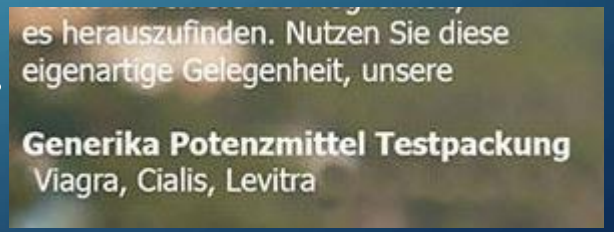
- Wie wir sehen können ist der Absender eine Kryptische Email Adresse, die wir nicht zuordnen können. Interessanter Weise ist der eigentliche Empfänger ebenfalls eine Seltsame E-Mail nämlich: verwaltung@bh.shg-kliniken.de
- Beides deutet auf einen Betrugsversuch hin. Die Mail wurde offenbar auf Masse produziert und an verwaltung@bh.shg-kliniken.de geschickt. Diese haben die Mail dann zu uns weiter geleitet. Betrugsemails können aber genau so gut an Sie direkt adressiert sein.
- Am besten überprüfen Sie also ob die Absende-Email seltsam ist. **Phishing Mails haben meist Kryptische oder seltsam klingende Absender.**

PHISHING E-MAILS ERKENNEN

Bildungsakademie Mittweida e.V.

- Des Weiteren ist der Inhalt solcher Mails meist dubios, Sie sollen ja mit einem Angebot gelockt werden, das Sie nirgendwo anders bekommen können.
- Ein weiterer Hinweis sind Anhänge mit Kryptischen Namen oder angehängte Dokumente ohne sinnvollen Verweis aus der Email auf den Anhang.

- Zuletzt sind solche Mails meist von nicht-Muttersprachlern verfasst und schlecht übersetzt oder enthalten viele Rechtschreibfehler.



DATEIEN VERSCHLÜSSELN

Bildungsakademie Mittweida e.V.

- Das verschlüsseln von Dateien kann viele Gründe haben. Nicht nur Kriminelle verschlüsseln Ihre Dateien weil sie Illegale Inhalte enthalten.
- Jedem steht das Recht zu seine Dateien zu verschlüsseln und so vor dem unbefugten Zugriff anderer zu schützen. So wie das Türschloss in Ihrem Haus.
- Verschlüsseln kann viele Gründe haben:
  - Verwahren von Wichtigen Dokumenten wie: Urkunden, Verträge, Zugangsdaten
  - Schützen von Persönlichen Daten wie: Urlaubsbilder, Geistiges Eigentum
  - Schutz ihrer Arbeit wie: Das Buch an dem grade geschrieben wird, unfertige Kunst, etc.

DATEIEN VERSCHLÜSSELN

Bildungsakademie Mittweida e.V.

- Beim Verschlüsseln von Daten werden diese mit einem Schlüsselwort, dem Passwort, vermischt um so eine unkenntliche Datei zu erhalten, welche sich nur mit besagtem Passwort wieder so lesen lässt, wie sie ursprünglich war.
- Viele Systeme bieten mehr oder minder gute/sichere Möglichkeiten um schnell und einfach ihre Daten vor dem flüchtigen Zugriff anderer zu schützen.
- Für geübte Eindringlinge sind diese Methoden doch meistens kein Hindernis und es ist bekannt, dass Behörden wie der BND oder das FBI sich Hintertüren in vielen solcher Programmen erkaufen.
- Deshalb stelle ich ihnen hier ein Programm vor das getestet wurde und „Quelloffen“ ist. Damit ist garantiert, das die Verschlüsselung selbst keine Lücken enthält und das Programm in keiner Weise eine Hintertür eingebaut hat.

DATEIEN VERSCHLÜSSELN MIT TRUECRYPT

Bildungsakademie Mittweida e.V.

- Truecrypt ist ein Tool, das uns eine Art verschlüsselten Ordner erstellen lässt, in dem wir nach Eingabe des Passwortes, wie bei einem USB-Stick, darauf zugreifen können und Dateien hinzufügen, entfernen oder verändern können.
- Dabei muss die Größe dieses „virtuellen Sticks“ vorher festgelegt werden und ist hinterher nicht mehr zu verändern.
- Truecrypt lässt uns darüber hinaus auch echt, physische Laufwerke, wie einen USB-Stick, vollständig verschlüsseln.
- Zum Benutzen der Dateien muss immer eine Version von Truecrypt gestartet werden um besagte Verschlüsselungen zu öffnen.

DATEIEN VERSCHLÜSSELN MIT TRUECRYPT

Bildungsakademie Mittweida e.V.

- Truecrypt kommt in Fest installierbaren Versionen und mit einer Portablen Version, die nicht installiert werden muss.
- Nachdem das FBI wiederholt die entwickler von Truecrypt unter druck gesetzt hat, haben diese die Weiterentwicklung beendet, da ihr Programm auf dem heutigen stand der Technik nicht zu knacken ist. Deshalb müssen wir uns einer anderen Downloadseite bedienen.
- Link:
  - https://www.heise.de/download/product/truecrypt-25104

DATEIEN VERSCHLÜSSELN MIT TRUECRYPT

Bildungsakademie Mittweida e.V.

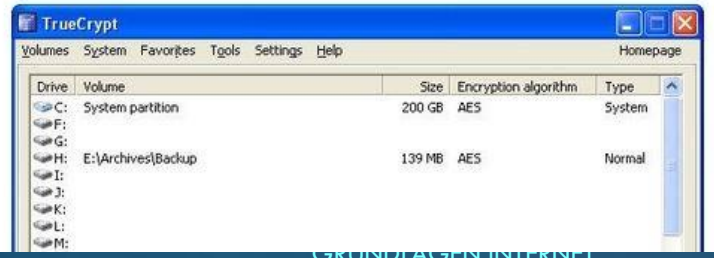
TrueCrypt

TrueCrypt Foundation

Hinweis: Die aktuelle Version 7.2 der Verschlüsselungs-Software TrueCrypt schränkt den Funktionsumfang drastisch ein. Sie wurde von den Entwicklern nur noch zum Umstieg auf andere Programme wie Bitlocker bereit gestellt. Wir bieten hier weiterhin die vollständige Vorgängerversion 7.1a zum Download an. In unserem Themen-Special finden Sie zudem interessante Alternativen zu TrueCrypt.

Für geschützte Daten auf dem eigenen Rechner sorgt das Verschlüsselungs-Werkzeug **TrueCrypt**. Mit umfangreichen Encryption-Funktionen kann man seine Daten vor unbefugtem Zugriff schützen - für die Sicherheit im Alltag, aber auch für den Fall, dass der Laptop oder das externe Laufwerk einmal verloren geht oder gestohlen wird.

TrueCrypt



Zum Download

4,5

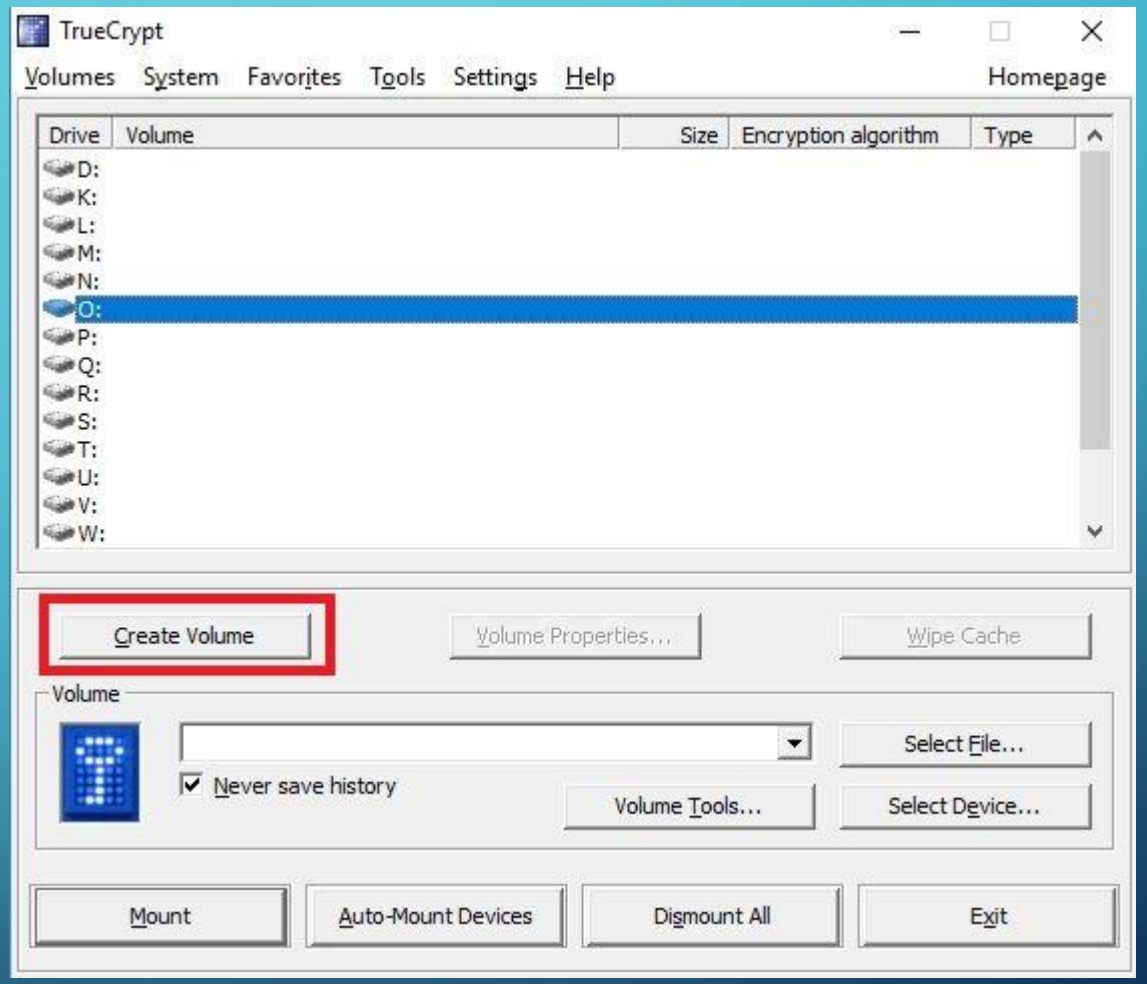
398 Stimmen

5 330
4 23
3 10
2 3
1 32

Hersteller:	» Zur Website
Preis:	kostenlos
Lizenz:	Open Source
Betriebssystem:	Linux, OS X, keine näheren Angaben, Windows XP, Windows Vista, Windows 7, Windows 8
Download-Größe:	2349 KByte bis 9303 KByte
Downloadrang:	18

DATEIEN VERSCHLÜSSELN MIT TRUECRYPT

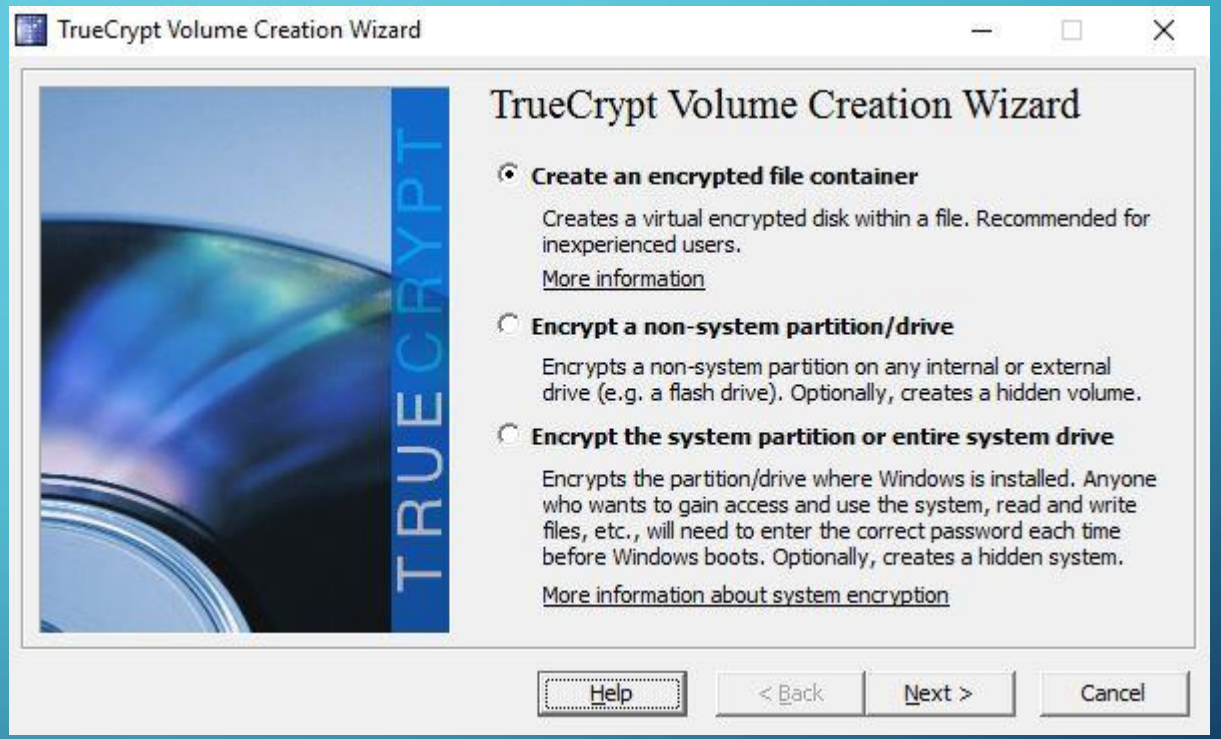
- Zunächst müssen wir ein Volumen erstellen, dafür clicken wir auf die Schaltfläche: „Create Volume“



DATEIEN VERSCHLÜSSELN MIT TRUECRYPT

Bildungsakademie Mittweida e.V.

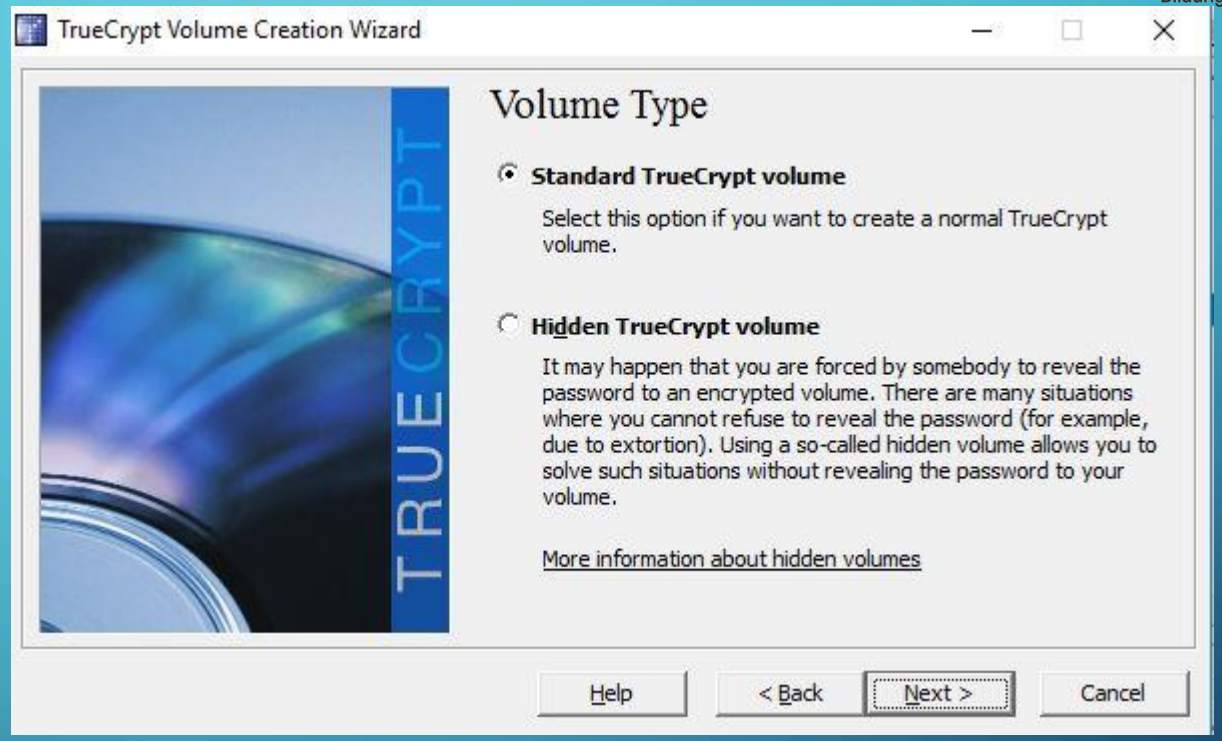
- Wir lassen die Standardeinstellungen hier stehen und bestätigen mit „Next“



DATEIEN VERSCHLÜSSELN MIT TRUECRYPT

Bildungsakademie Mittweida e.V.

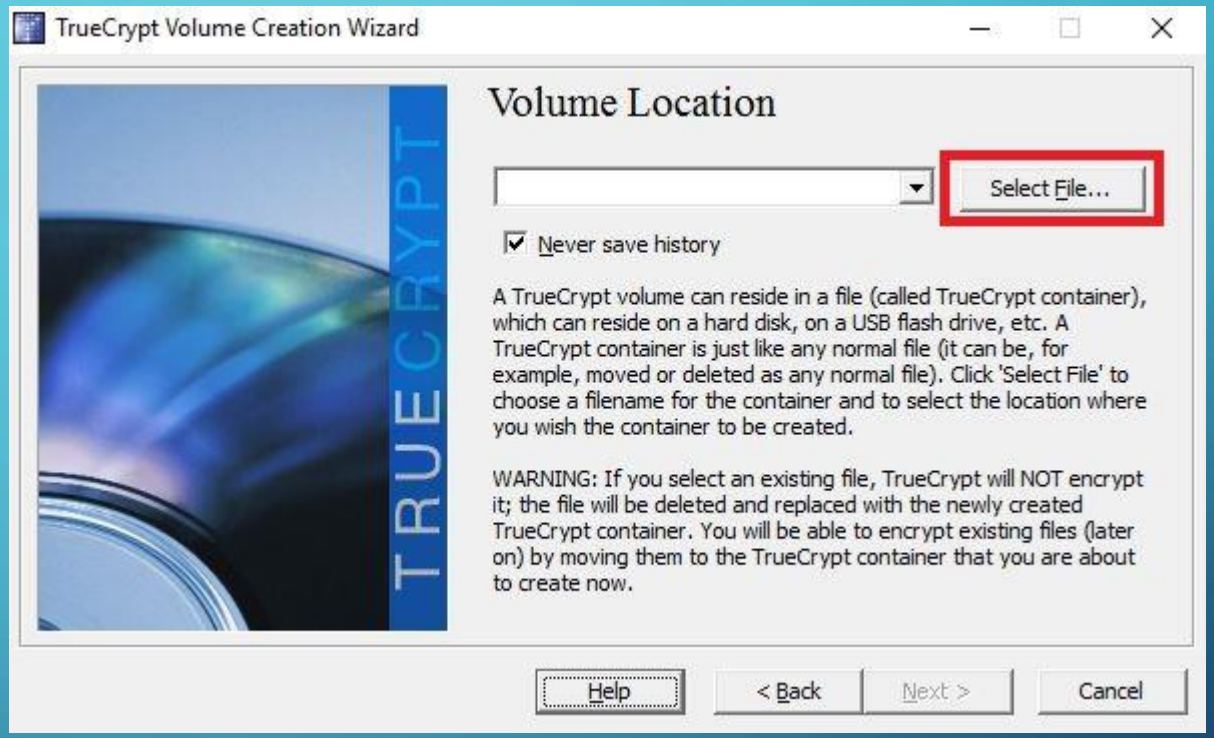
- Wir lassen die Standardeinstellungen hier stehen und bestätigen mit „Next“



DATEIEN VERSCHLÜSSELN MIT TRUECRYPT

Bildungsakademie Mittweida e.V.

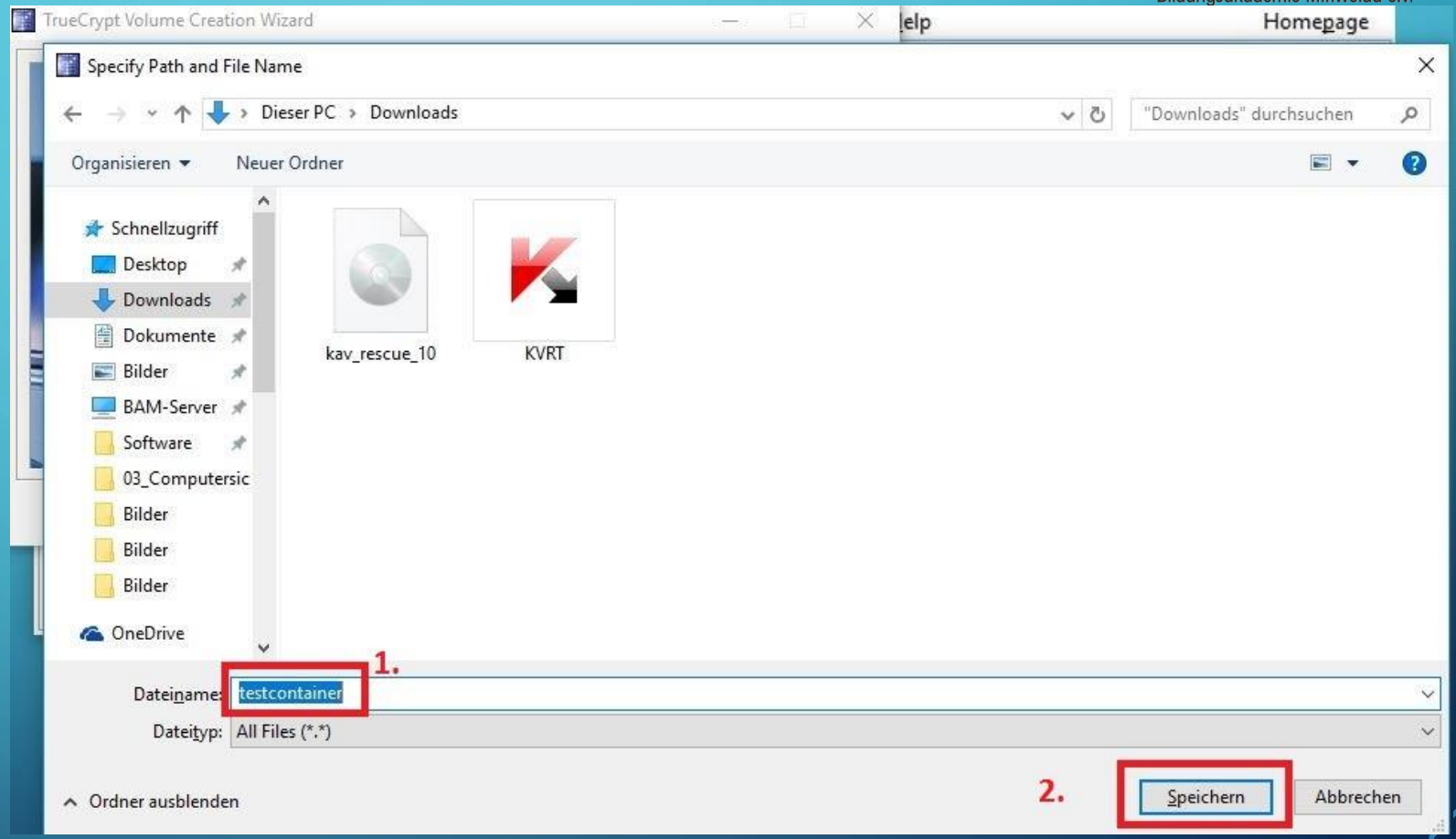
- Wir müssen eine Datei erstellen und benennen in die der Verschlüsselte Container eingebaut wird.



DATEIEN VERSCHLÜSSELN MIT TRUECRYPT

Bildungsakademie Mittweida e.V.

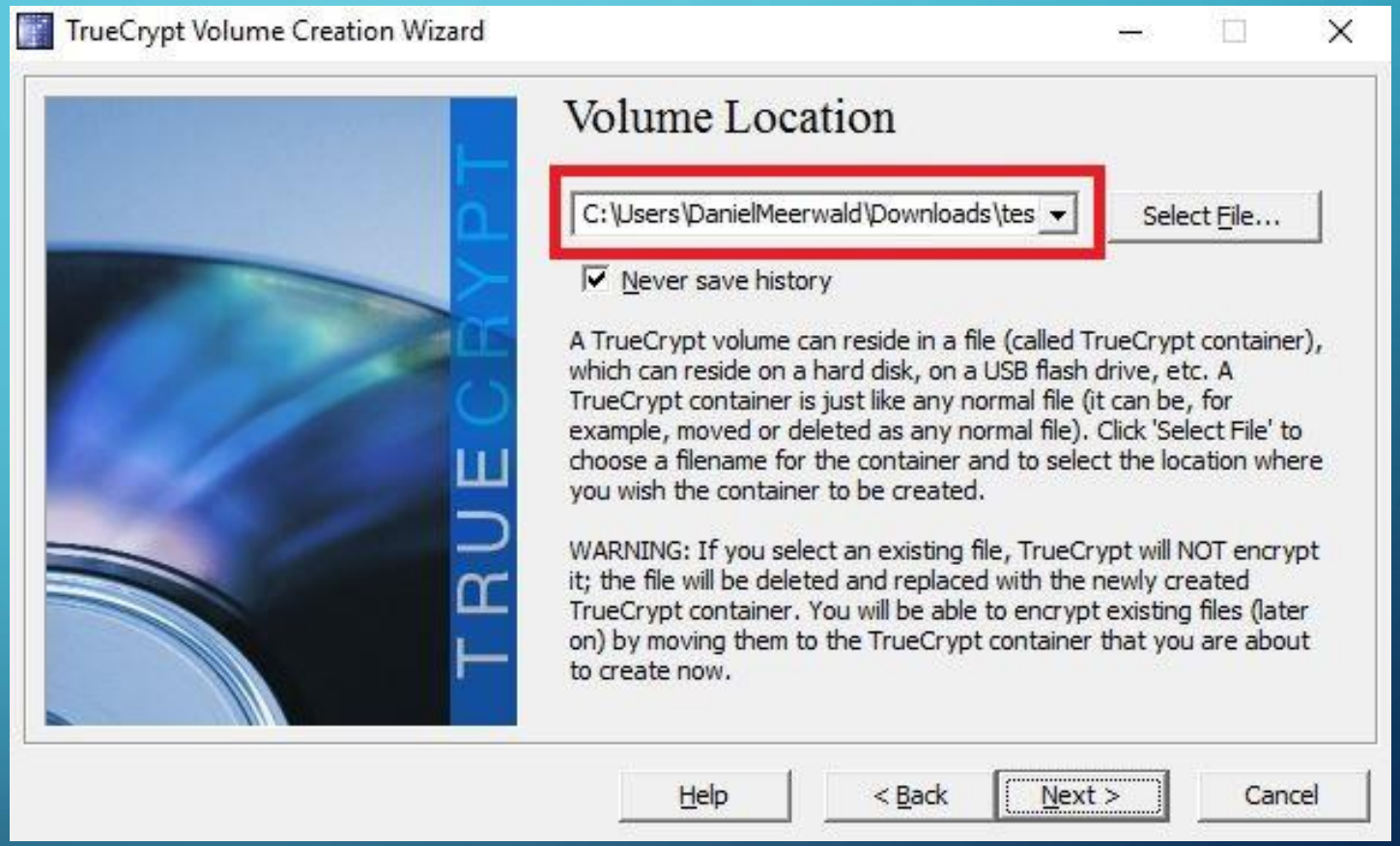
- Ein Dateiname (1.) muss angegeben werden, anschließen clicken wir auf „Speichern“ (2.)



DATEIEN VERSCHLÜSSELN MIT TRUECRYPT

Bildungsakademie Mittweida e.V.

- Danach gelangen wir wieder in dieses Menü, der Pfad zu unserer Datei ist nun eingetragen. Wir bestätigen wieder mit „Next“.



DATEIEN VERSCHLÜSSELN MIT TRUECRYPT

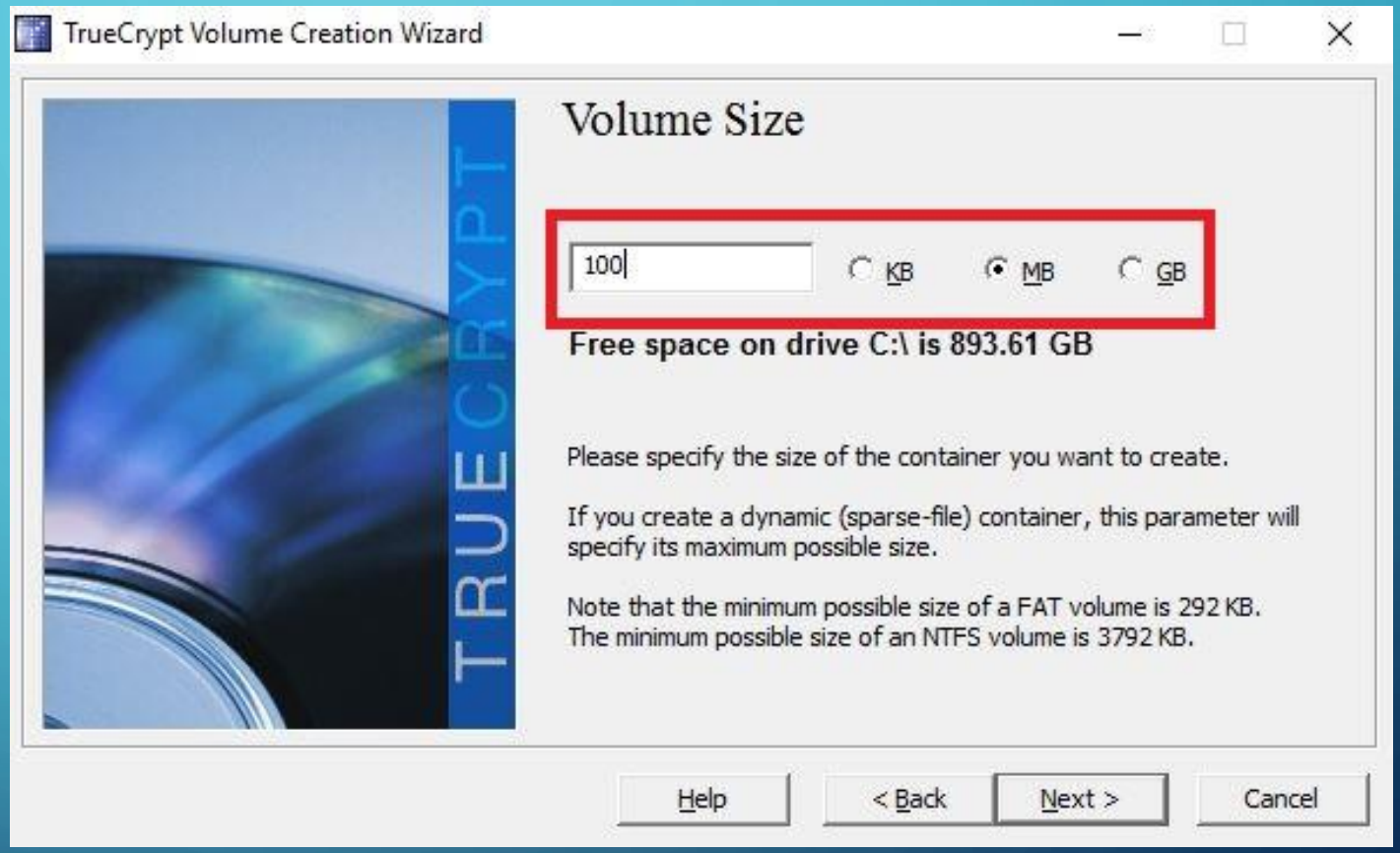
Bildungsakademie Mittweida e.V.

- Wir lassen die Standardeinstellungen hier stehen und bestätigen mit „Next“

DATEIEN VERSCHLÜSSELN MIT TRUECRYPT

Bildungsakademie Mittweida e.V.

- Nun müssen wir die Größe unseres „Virtuellen USB-Sticks“ wählen. Wie bei einem echten Stick, kann diese später nicht verändert werden. Dann clicken wir wieder „Next“.



DATEIEN VERSCHLÜSSELN MIT TRUECRYPT

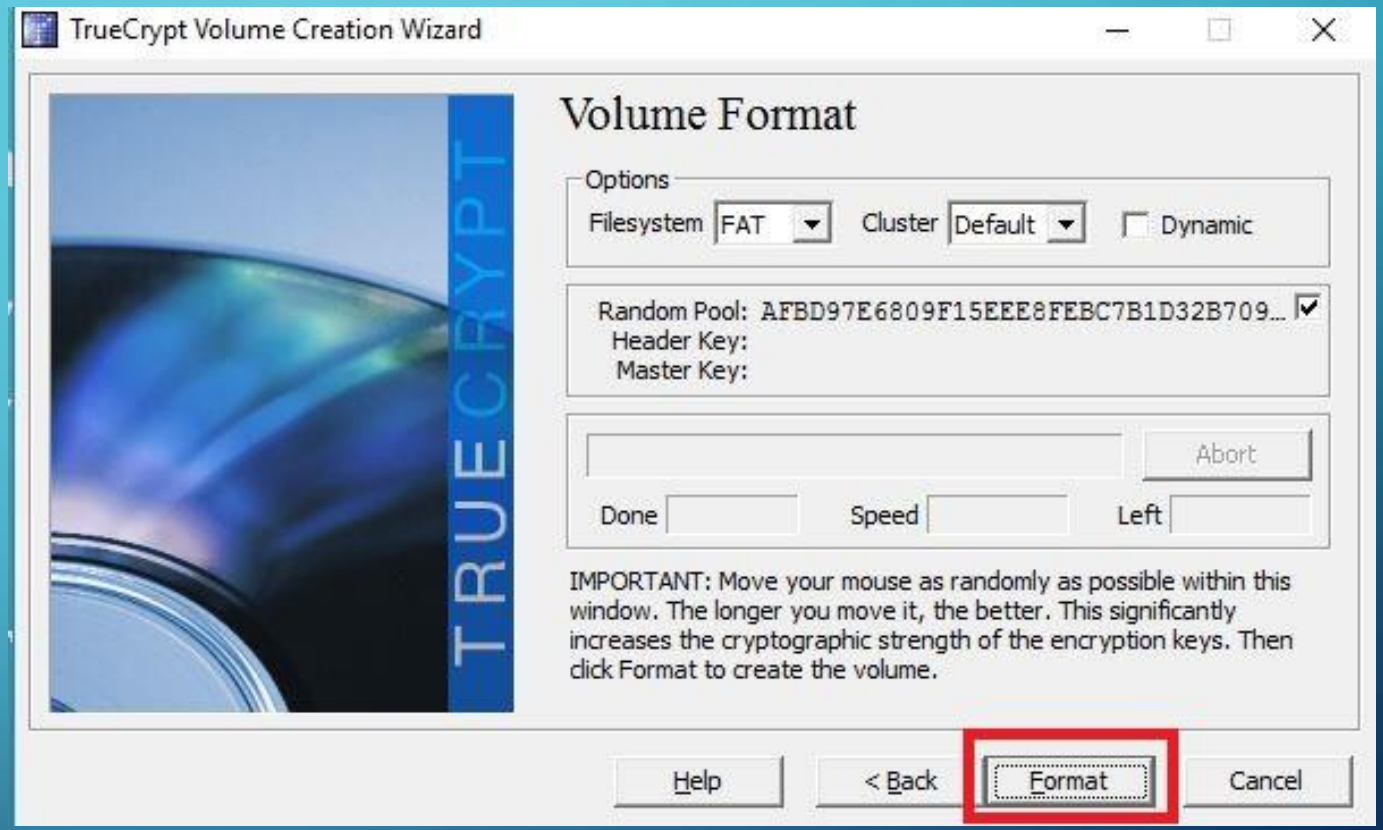
Bildungsakademie Mittweida e.V.

- Nun müssen wir ein Passwort wählen, und dieses zur Sicherheit 2 mal eintragen. In „Computersicherheit“ vom 14.02.2017 können Sie noch einmal nachlesen wie man ein sicheres Passwort erstellt. Truecrypt warnt Sie auch, falls ihr Passwort zu schwach erscheint. Danach wir wieder „Next“.

DATEIEN VERSCHLÜSSELN MIT TRUECRYPT

Bildungsakademie Mittweida e.V.

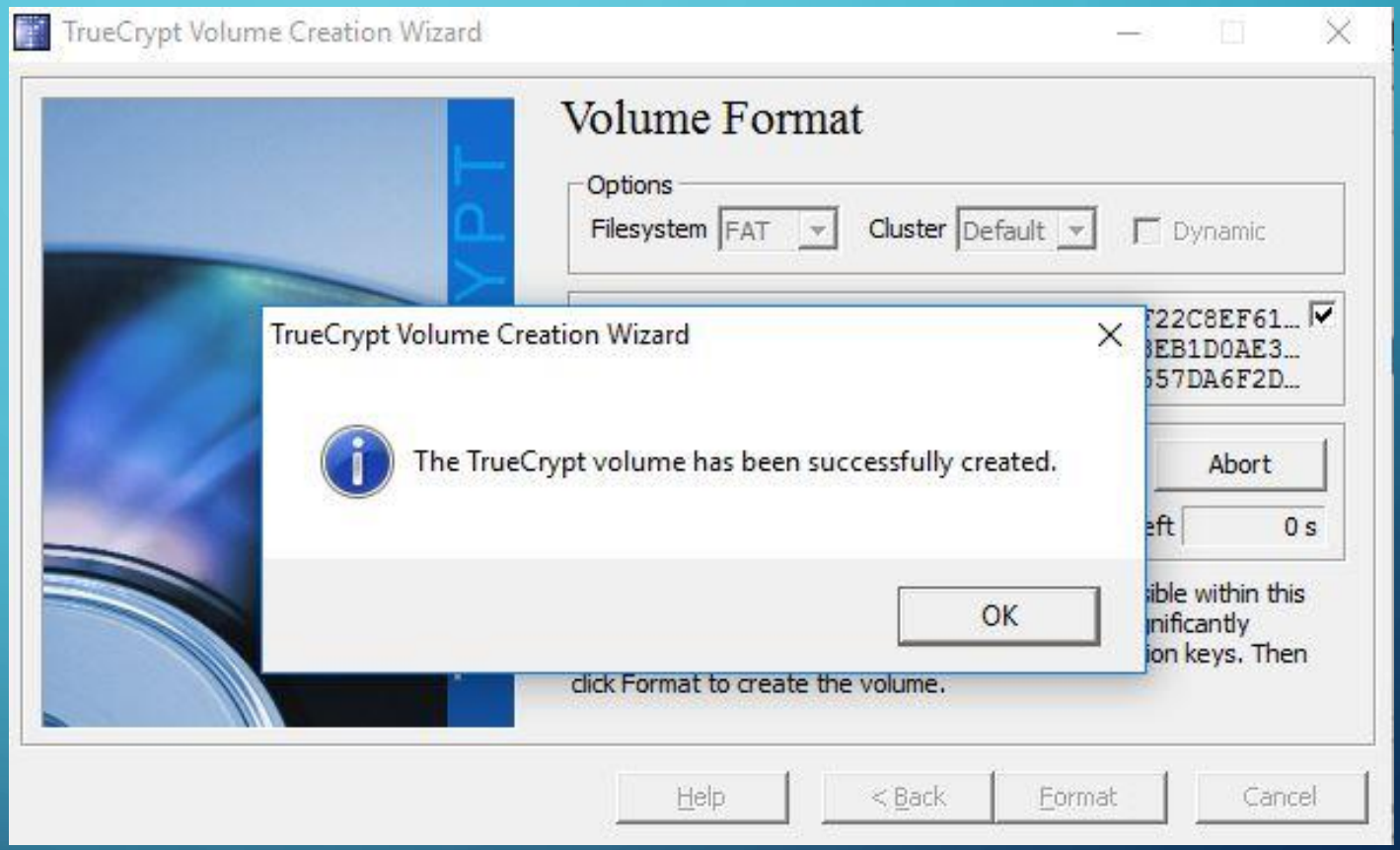
- Nun wird die Datei angelegt und Verschlüsselt, wir bestätigen den Vorgang mit „Format“l.



DATEIEN VERSCHLÜSSELN MIT TRUECRYPT

Bildungsakademie Mittweida e.V.

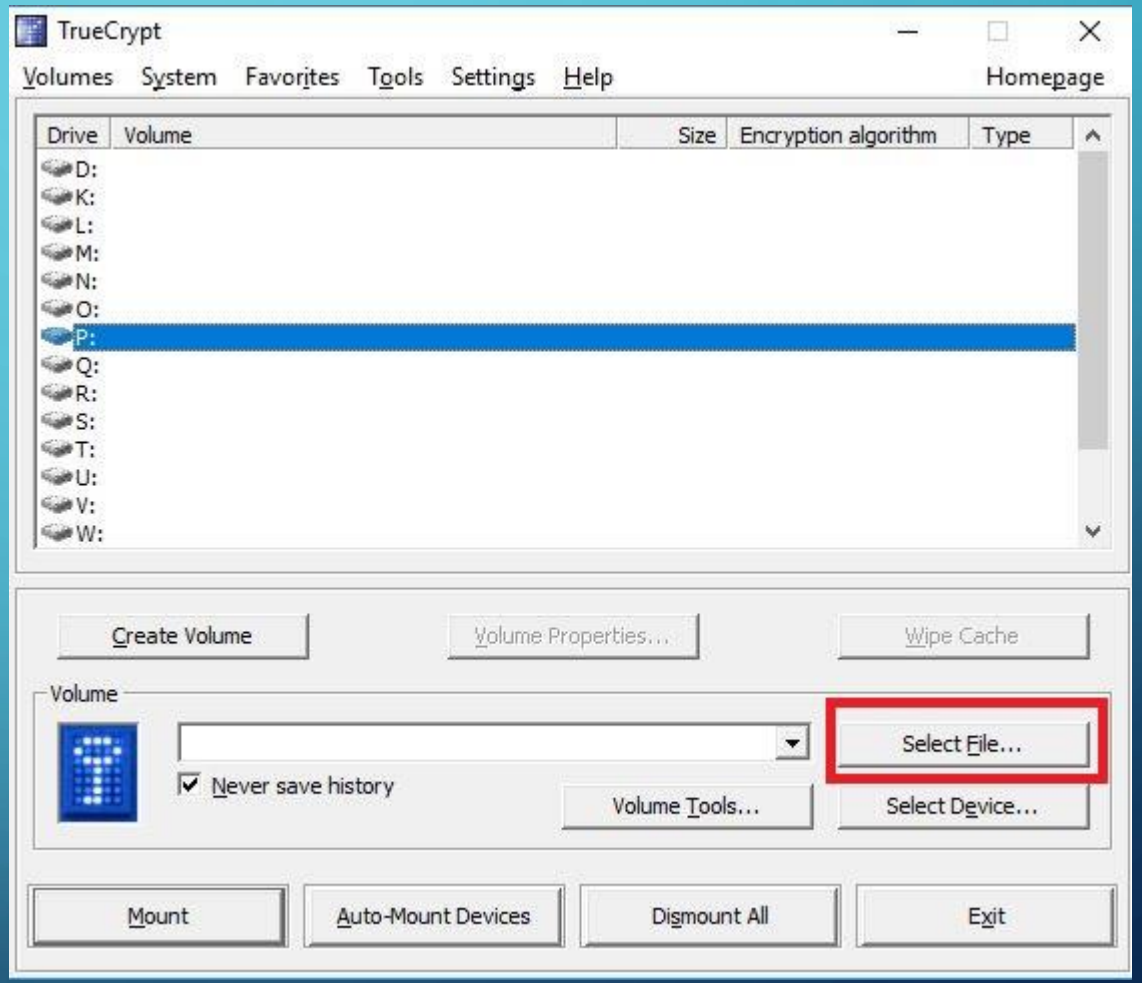
- Ist der Vorgang abgeschlossen sehen Sie diesen Bildschirm. Bestätigen Sie mit „OK“ und clicken anschließend unten rechts auf „Exit“.



DATEIEN VERSCHLÜSSELN MIT TRUECRYPT

Bildungsakademie Mittweida e.V.

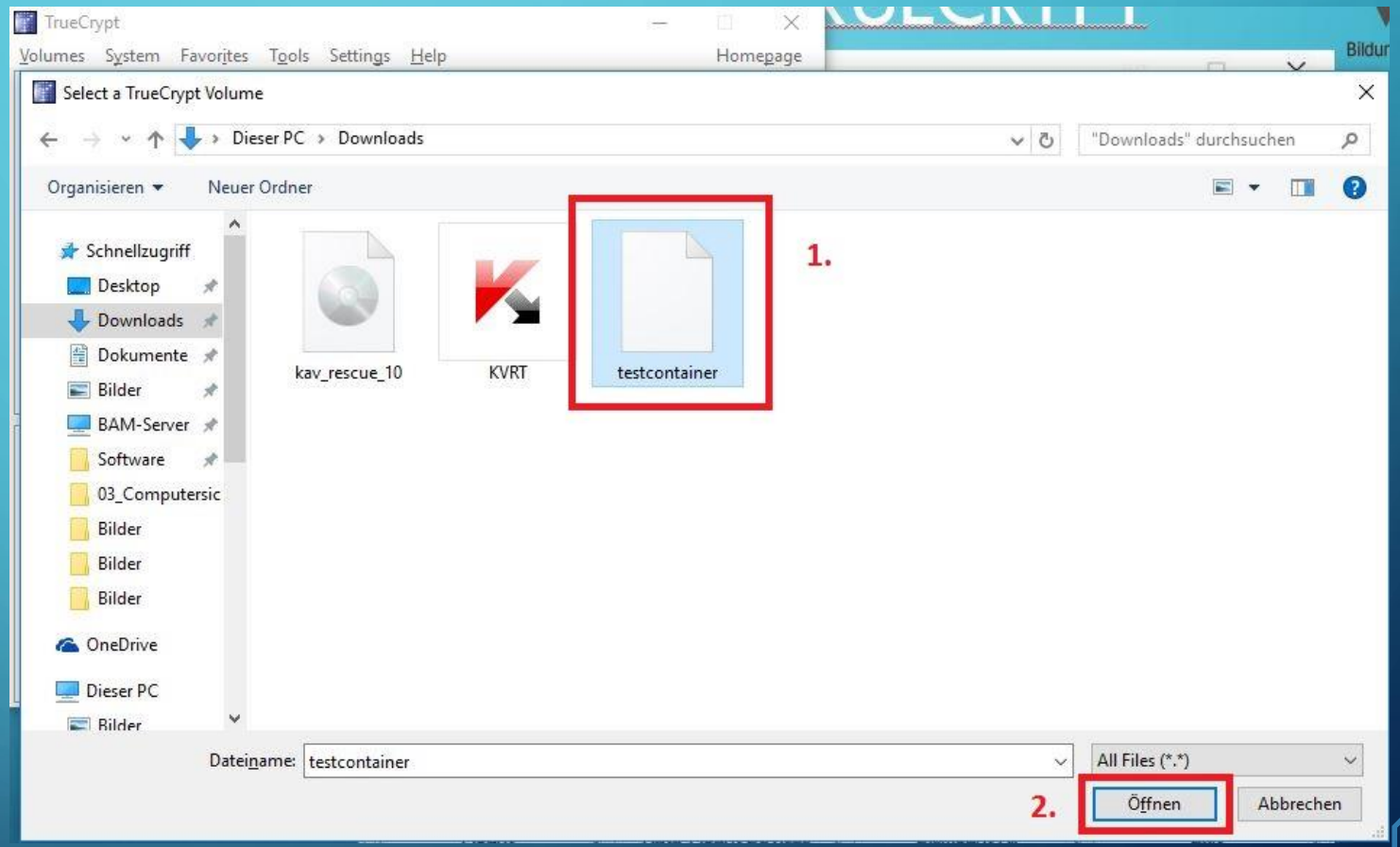
- Um auf unseren Verschlüsselten Container zuzugreifen, wählen wir „Select File“.



DATEIEN VERSCHLÜSSELN MIT TRUECRYPT

Bildungsakademie Mittweida e.V.

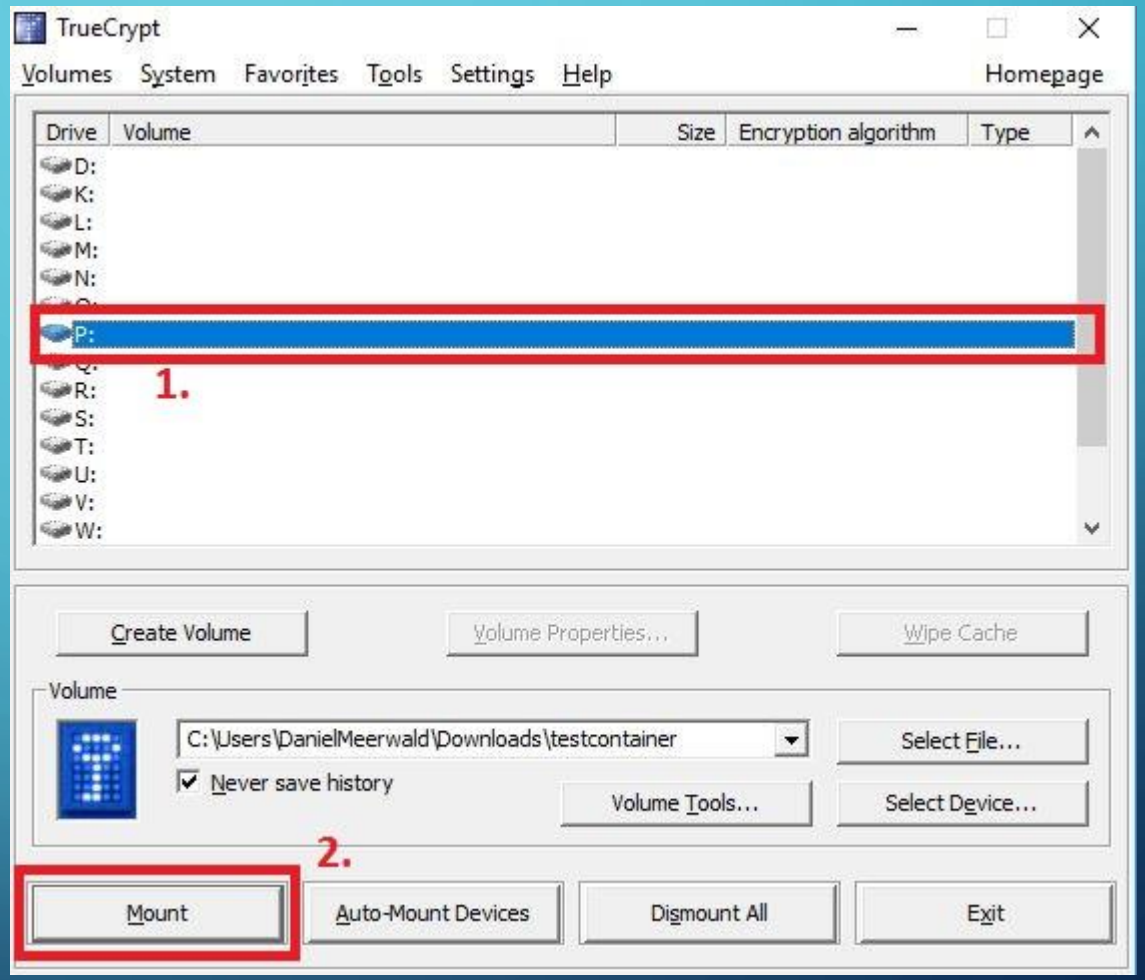
- Nun wählen wir die Datei aus (1.), die wir in einem der Vergangenen Schritte erstellt und benannt haben und clicken anschließend auf „Öffnen“ (2.).



DATEIEN VERSCHLÜSSELN MIT TRUECRYPT

Bildungsakademie Mittweida e.V.

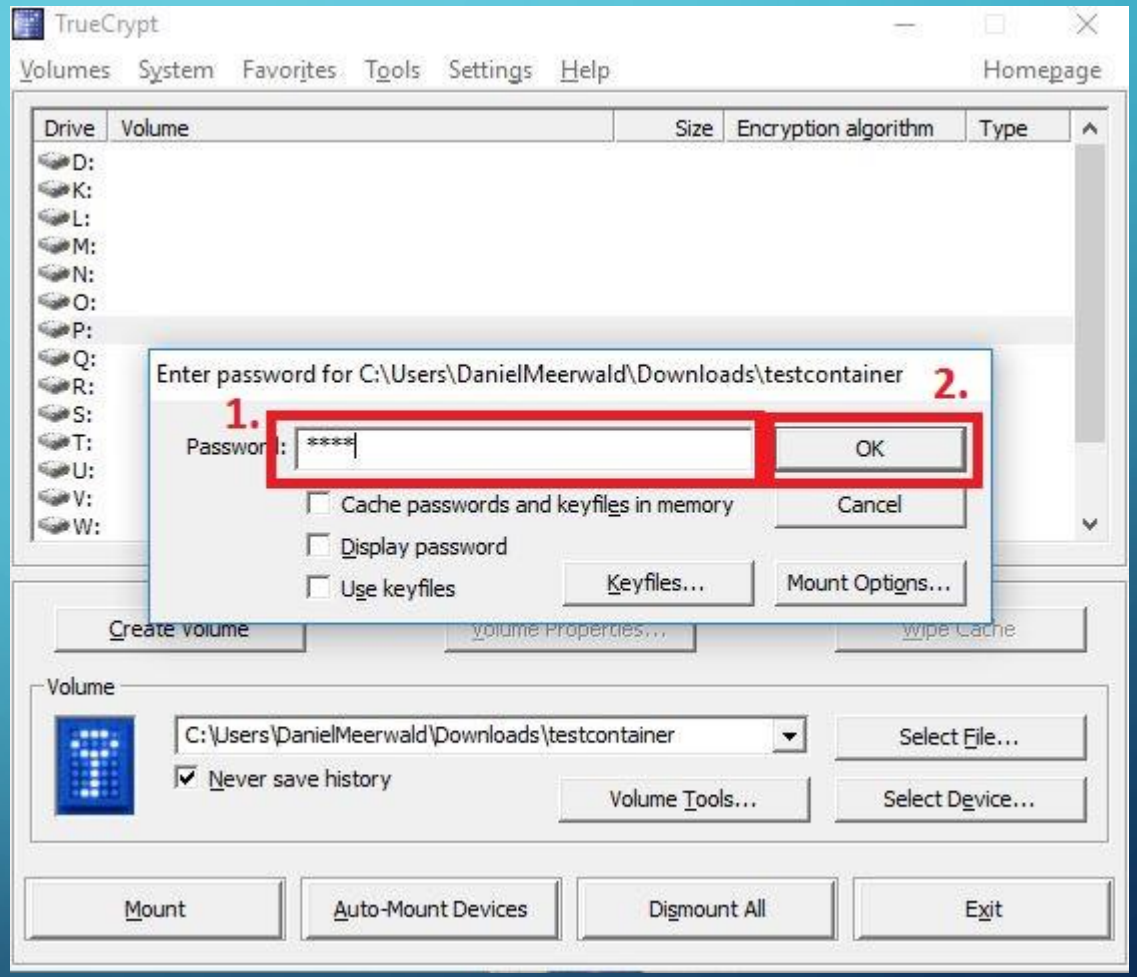
- Nun müssen wir einen Buchstaben wählen unter dem der Container begehbar wird. Dieser kann frei gewählt werden (1.).
- Danach drücken wir „Mount“ (2.)



DATEIEN VERSCHLÜSSELN MIT TRUECRYPT

Bildungsakademie Mittweida e.V.

- Wir werden nun aufgefordert, das sichere Passwort welches wir in einem der vorherigen Schritte erstellt haben, einzugeben(1.), damit die Dateien entschlüsselt werden können.
- Damach müssen wir mit „OK“ bestätigen (2.).

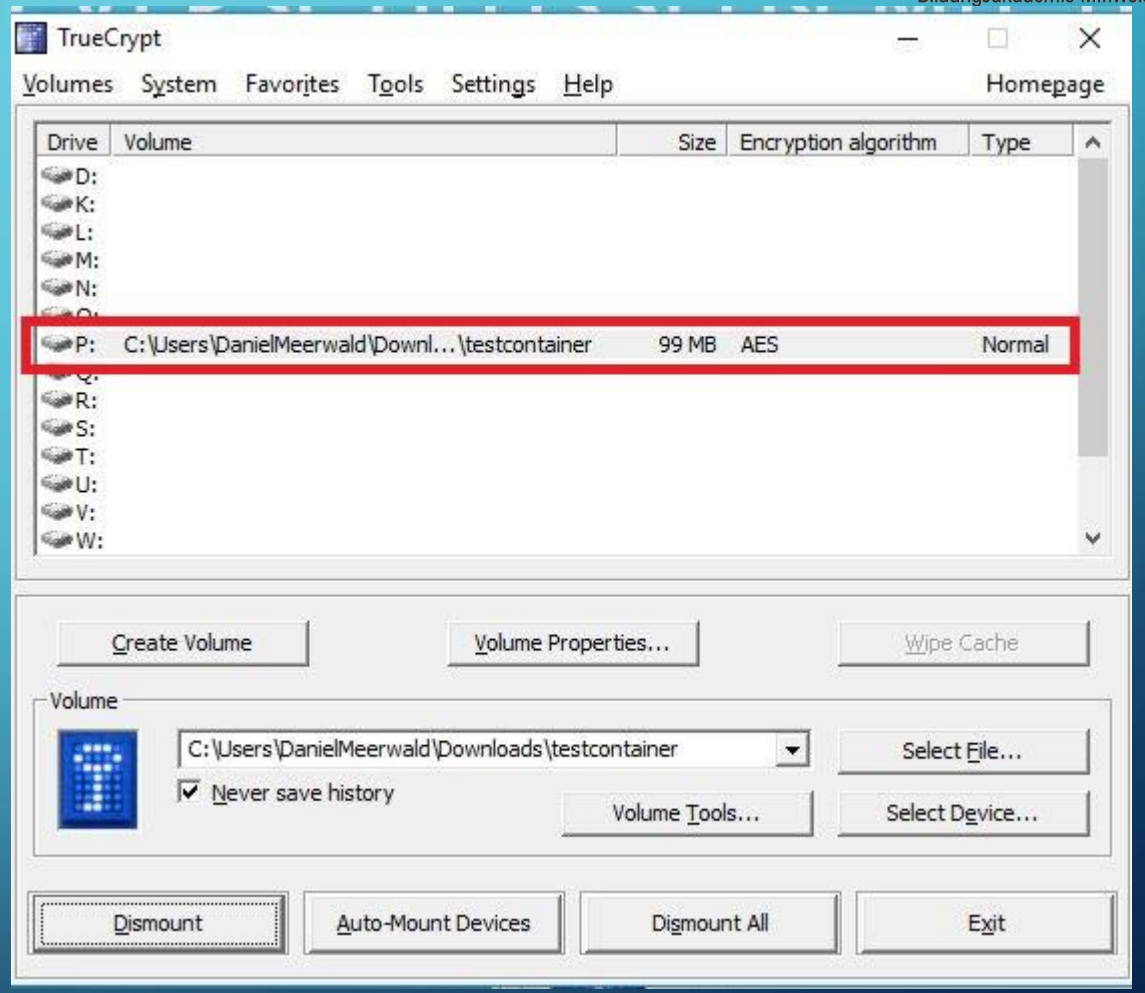


DATEIEN VERSCHLÜSSELN MIT TRUECRYPT

Bildungsakademie Mittweida e.V.

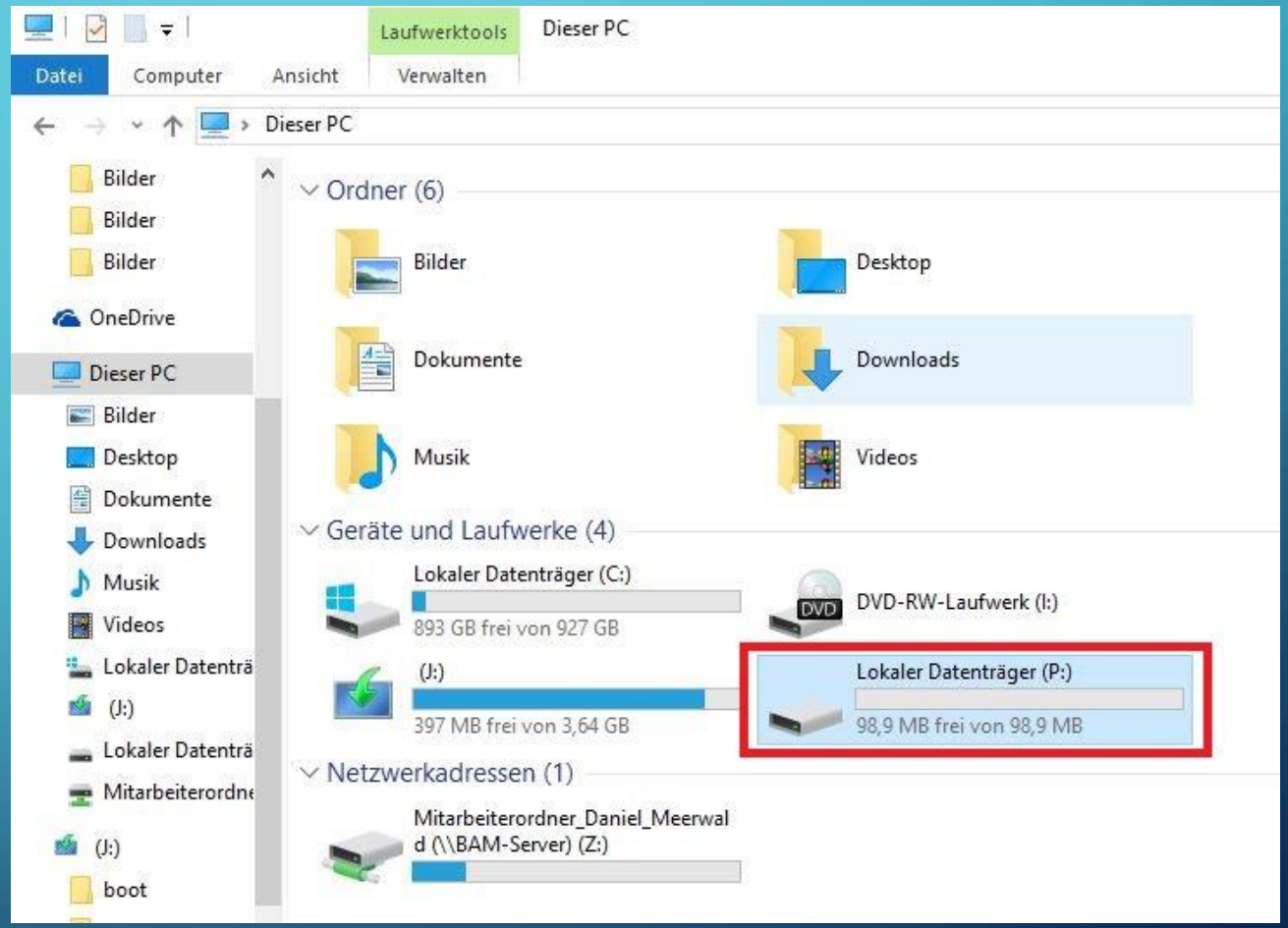
- Wenn alles funktioniert hat, ist unter dem gewählten Buchstaben, der Pfad unserer Verschlüsselten Container-Datei zu sehen.
- Wir wechsen nun in den normalen Dateibrowser.

(Tastenkombination: Win+E)



DATEIEN VERSCHLÜSSELN MIT TRUECRYPT

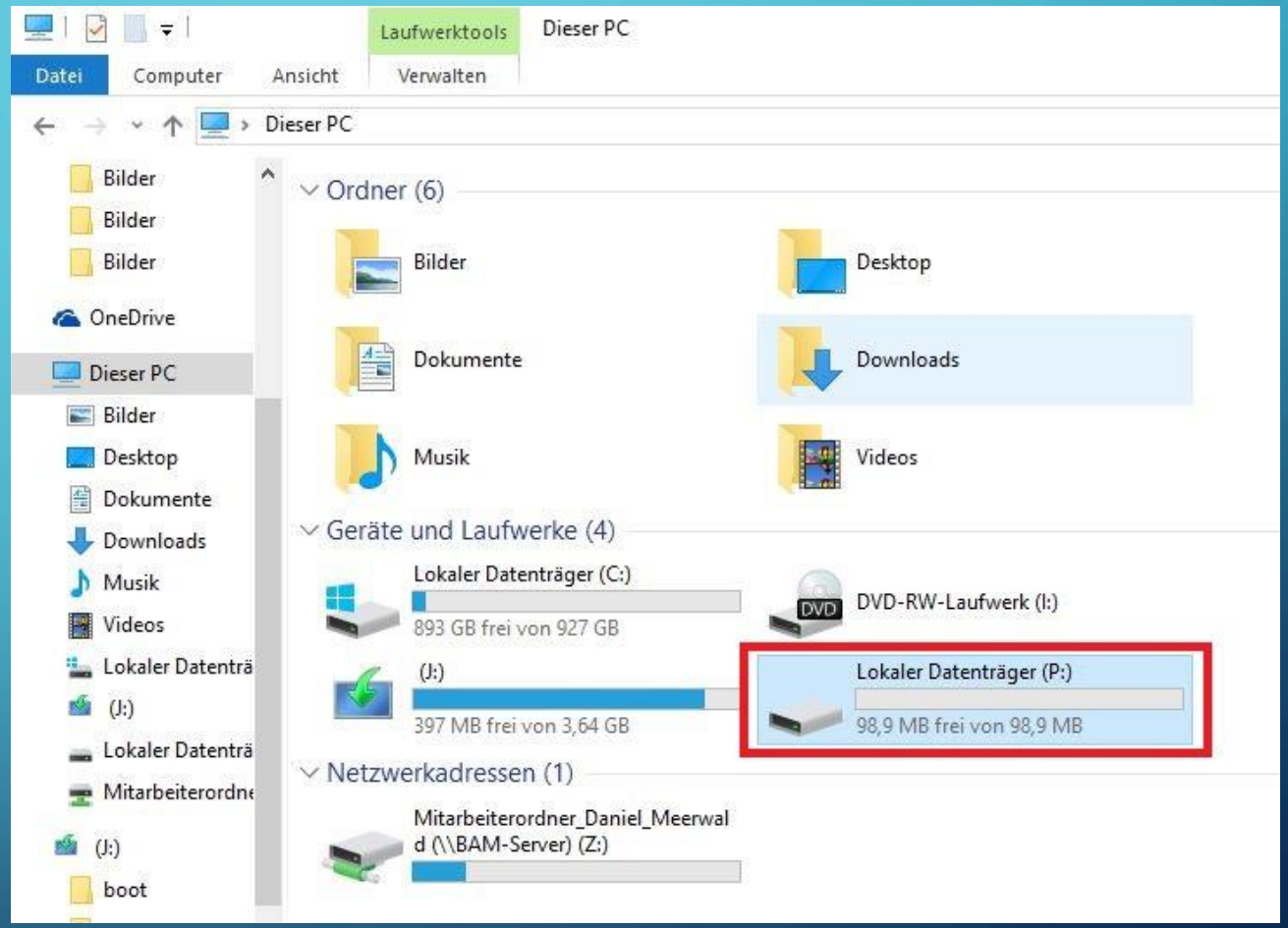
- Hier ist unser erstelltes 100MB Volumen nun wie ein normaler USB Stick zu sehen und kann genau so benutzt werden.



DATEIEN VERSCHLÜSSELN MIT TRUECRYPT

Bildungsakademie Mittweida e.V.

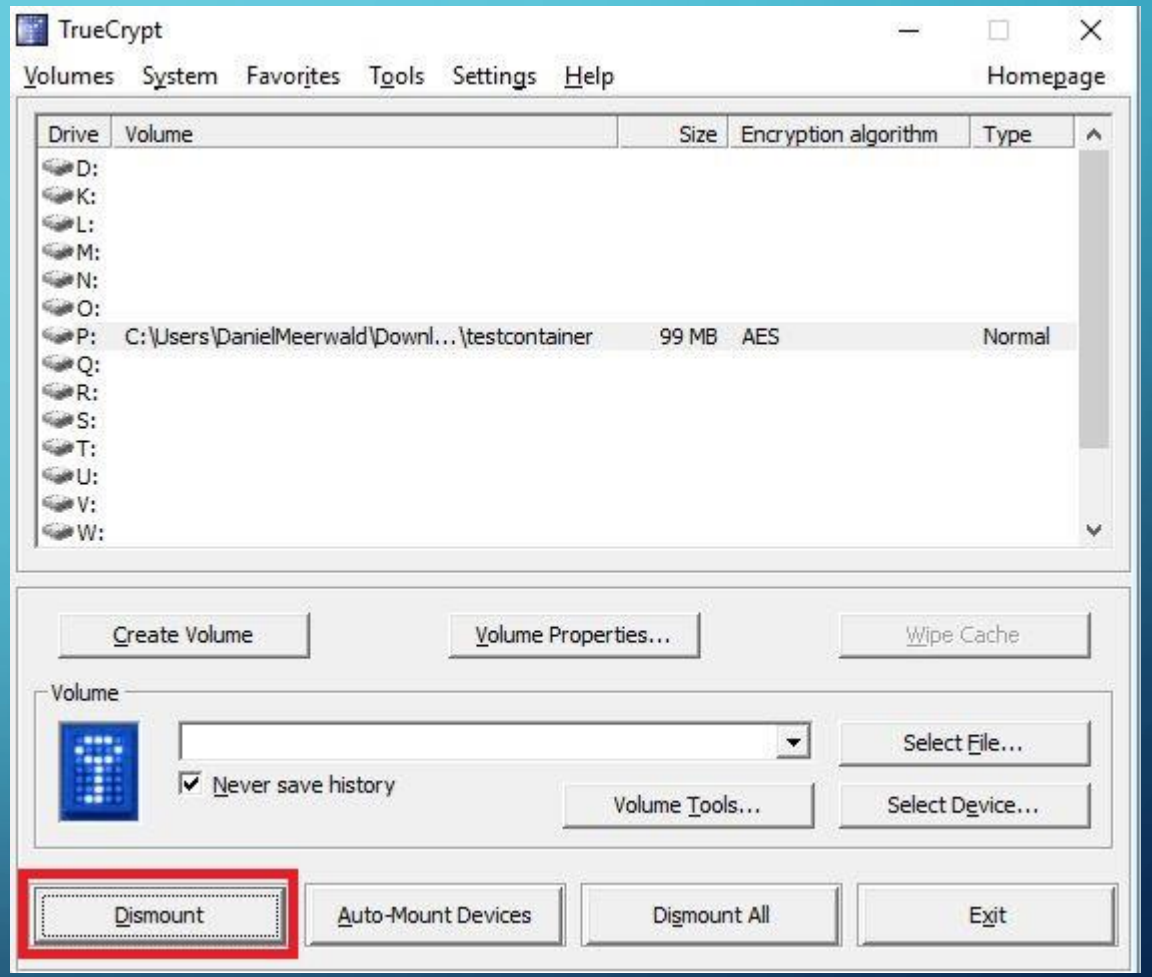
- Hier ist unser erstelltes 100MB Volumen nun wie ein normaler USB Stick zu sehen und kann genau so benutzt werden.



DATEIEN VERSCHLÜSSELN MIT TRUECRYPT

Bildungsakademie Mittweida e.V.

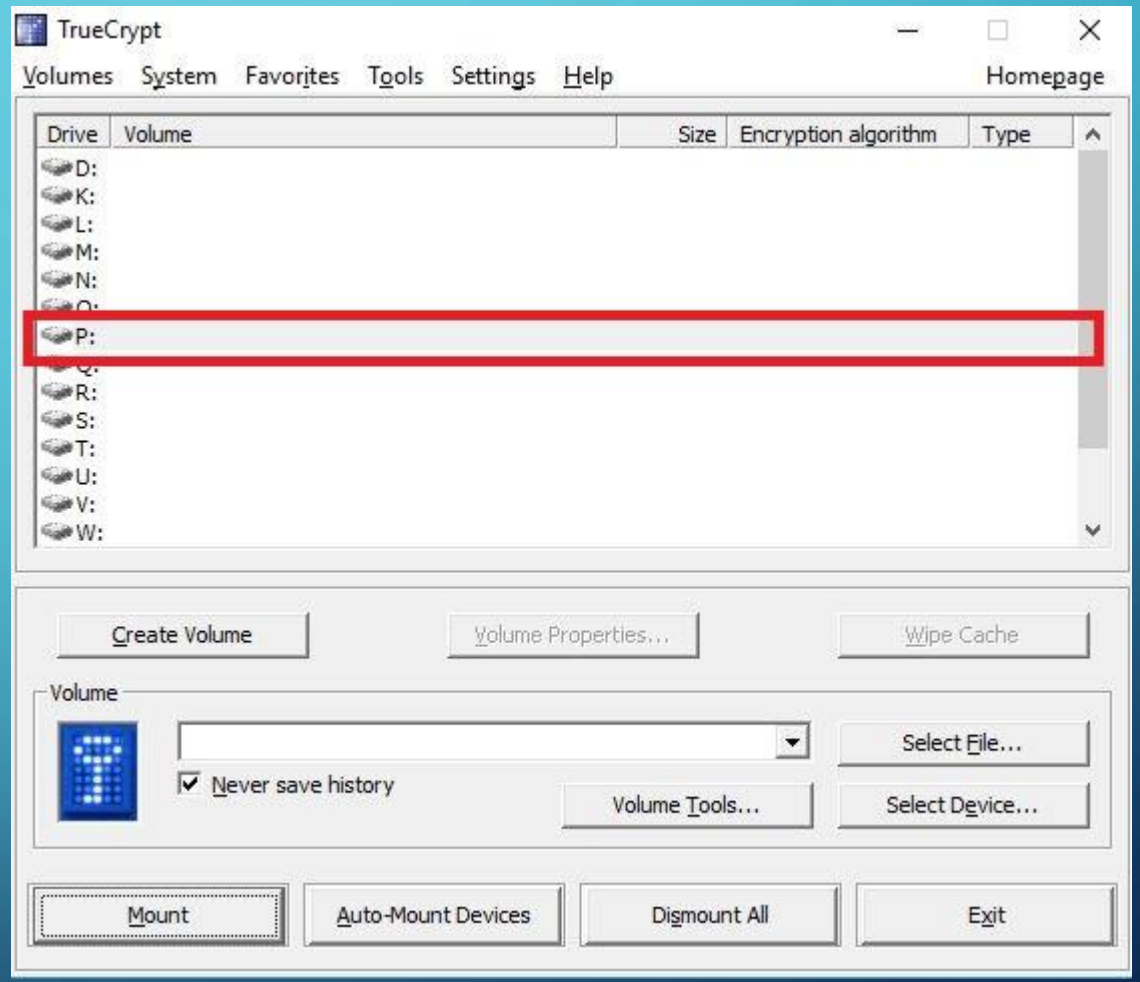
- Damit niemand unsere Dateien mehr lesen kann müssen wir nach getaner Arbeit das Volumen wieder „Aushängen“ dafür clicken wir auf „Dismount“ (dt. Aushängen).



DATEIEN VERSCHLÜSSELN MIT TRUECRYPT

Bildungsakademie Mittweida e.V.

- Wenn das „Aushängen“ funktioniert hat, ist unter dem Buchstaben kein Pfad der Datei mehr zu sehen.
- Das Ausschalten des PC‘s ohne aushängen hat den selben Effekt, die Dateien sind erst wieder nach „Einhängen“ über Truecrypt und nach Eingabe des Passwortes lesbar



KONTAKTDATEN

Daniel Meerwald

Erreichbar:

Di.-Mi.: 10:00 – 16:00 Uhr

Telefon: 03727/9817577

E-Mail: Meerwald@bildungsakademie-mittweida.de

Bildungsakademie Mittweida e.V.