

Benutzerordnung

Räume mit Datenverarbeitungs-Technik

1. Allgemeine Bedingungen

- 1.1. Mobilien und Geräte in den BBS Cuxhaven sind pfleglich zu behandeln.
- 1.2. Jegliches Essen und Trinken sind in unmittelbarer Nähe zu Datenverarbeitungs-Geräten (DV-Geräten) untersagt. In speziellen DV-Räumen ist das Essen und Trinken generell verboten! Getränke in offenen Behältnissen dürfen nicht mit in den Raum gebracht werden.
- 1.3. Nach Beendigung der Arbeiten an den DV-Geräten ist der Raum aufgeräumt zu verlassen.
- 1.4. Beim Auftreten von Funktionsstörungen der PCs informieren Schülerinnen und Schüler (SuS) die Lehrerinnen und Lehrer (LK). Jede LK meldet auftretende Fehler an Hard- oder Software umgehend der EDV-Abteilung.
- 1.5. Hardwaremäßige Veränderungen an den PCs erfolgen nur durch die EDV-Abteilung. Die meisten Räume sind mit einem Beamer ausgestattet. Für diesen liegt in den Räumen ein freies Kabel bereit, wenn z.B. ein externes Notebook angeschlossen werden soll. Gibt es dabei Probleme, beachten Sie bitte Punkt 1.4.
- 1.6. SuS dürfen den Raum i.d.R. nur nutzen, wenn eine LK anwesend ist. Abweichungen von dieser Regel verantwortet die aufsichtführende Person.
- 1.7. Montags bis donnerstags werden die PCs nach 15.30 Uhr automatisch heruntergefahren, wenn kein Benutzer angemeldet ist. Ist ein Benutzer angemeldet, wird die Aktivität des PCs geprüft. Nach 1 Stunde Inaktivität wird dieser PC zum Herunterfahren gezwungen. Freitags erfolgt diese Prüfung ab 14 Uhr.
- 1.8. Eigene mobile Datenträger (z.B. USB-Speichersticks) dürfen nur verwendet werden, wenn sie nach bestem Wissen und Gewissen virusfrei sind.
- 1.9. Die BBS Cuxhaven können trotz aller Sorgfalt nicht garantieren, dass die DV-Systeme virusfrei sind.
- 1.10. Jeder Nutzer erhält einen Benutzernamen und ein persönliches Passwort. Für unter der Nutzerkennung erfolgte unerlaubte Handlungen werden SuS und LK verantwortlich gemacht. Deshalb sind die Zugangsdaten geheim zu halten. Bei der Anmeldung verwendet jeder Nutzer nur seine eigenen Kenndaten. Für die missbräuchliche Benutzung haftet der Inhaber.
- 1.11. Alle Nutzer verpflichten sich zu einem verantwortungsvollen Umgang mit den EDV-Geräten. Beim allgemeinen Umgang und insbesondere bei der Nutzung des Internets sind die gesetzlichen Bestimmungen insbesondere des Strafrechts, Urheberrechts (EULA), Datenschutzes und des Jugendschutzrechts zu beachten. Es ist verboten, pornographische, Gewalt verherrlichende oder rassistische Inhalte aufzurufen oder zu versenden. Werden solche Inhalte versehentlich aufgerufen, ist die Anwendung umgehend zu schließen. Die im Internet bereitgestellten Informationen sind von der Fachlehrerin/vom Fachlehrer grundsätzlich auf ihre Tauglichkeit für den Unterrichtseinsatz zu prüfen. Sollten dennoch Informationen angezeigt werden, durch die sich LK wie SuS verletzt, entwürdigt oder in anderer Weise angegriffen fühlen, muss sie/er diesen Sachverhalt mit der Urheberin/dem Urheber der Information klären. Die Berufsbildenden Schulen Cuxhaven sind in keiner Weise für den Inhalt von Onlineinformationen verantwortlich.
- 1.12. Werden Informationen durch das Internet versendet, geschieht dies unter dem Absender der BBS Cuxhaven. Es ist deshalb untersagt, Informationen zu versenden, die dazu geeignet sind, den BBS Cuxhaven in irgendeiner Weise Schaden zuzufügen.
- 1.13. Der Benutzer hat nicht das Recht, vertragliche Vereinbarungen via Internet einzugehen.
- 1.14. Die BBS Cuxhaven ist in Wahrnehmung ihrer Aufsichtspflicht berechtigt, den Datenverkehr zu speichern und im Bedarfsfall der Polizei zur Verfügung zu stellen.
- 1.15. Jeder PC der BBS Cuxhaven kann von der EDV-Abteilung ferngesteuert werden. Nähere Informationen werden auf dem „Info-Hinweis 2 DameWare“ gegeben.
- 1.16. Zur Nutzung der Daten auf den PCs bitte den „Info-Hinweis 3 Netzwerk BBSCUXSCHUL“ beachten.
- 1.17. Die auf den Arbeitsstationen und im Netzwerk zur Verfügung stehende Software ist Eigentum des Herstellers bzw. der Schule. Die Berufsbildenden Schulen Cuxhaven sind berechtigt diese Software für Bildungszwecke zu nutzen. Eine Nutzung für andere Zwecke sowie eine Vervielfältigung oder Veräußerung ist nicht gestattet.
- 1.18. Jegliches manipulatives Umgehen der Sicherungsvorkehrungen (z.B. „Hacken“) ist untersagt.
- 1.19. Für Schäden, die durch die Nichtbeachtung dieser Regeln entstehen, haften SuS wie LK.
- 1.20. Mit Benutzung der EDV-Anlagen der BBS Cuxhaven werden diese Benutzerordnung vom Anwender anerkannt.

2. Ergänzende Bedingungen Lehrer

- 2.1. Werden neue Programme benötigt, so installiert diese die EDV-Abteilung i. d. R. innerhalb von 2 Wochen. Dieses gilt auch für die Deinstallation. Eine Absprache mit dem Raumhüter und der EDV-Abteilung sollte daher rechtzeitig erfolgen.
- 2.2. Nur das Fachteam bzw. Bildungsteam bestimmt, welche Software im jeweiligen Unterricht verwendet wird, d. h. SuS dürfen nur diejenigen Programme verwenden, die ihnen von der Fachlehrerin/vom Fachlehrer zugewiesen wurden.
- 2.3. LK beachten zusätzlich den „Info-Hinweis 4 Zusätzliche Informationen für Lehrkräfte“.

- 2.4. Diese Ordnung ist jedem SuS zu Beginn eines Schuljahres bzw. Unterrichtet und bei Änderungen durch den Klassenlehrer mitzuteilen (Vermerk im Klassenbuch).
- 3. Ergänzende Bedingungen Bibliothek**
- 3.1. Betreuungsperson der Bibliothek ist Herr Dräger. Ist Herr Dräger verhindert, übernimmt eine Vertretung seinen Dienst.
- 3.2. Weisungsberechtigt ist die zuständige Betreuungsperson der Bibliothek und / oder die anwesende LK.
- 3.3. Jeder PC-Nutzer trägt sich in die ausliegende Benutzerliste ein.
- 3.4. Die Arbeitsruhe ist einzuhalten.
- 3.5. LK und SuS/innen der BBS Cuxhaven dürfen die Bibliothek im Rahmen des Unterrichts sowie allgemeiner Nutzung im Zusammenhang mit schulischen Aufgaben nutzen.
- 3.6. Drucken kostet 0,05 € pro Seite. Nutzt eine LK die Bibliothek für seinen Unterricht, sind die daraus resultierenden Ausdrucke kostenfrei. Die Druckaufträge sind durch die zuständige Betreuungsperson freizugeben.
- 3.7. Die PCs nach der Nutzung nicht ausschalten. Die geöffneten Programme sind vor Verlassen des PCs zu schließen.
- 4. Ergänzende Bedingungen Selbstlernzentrum (SLC)**
- 4.1. Betreuungsperson des SLCs ist Herr Petzold. Ist Herr Petzold verhindert, übernimmt eine Vertretung seinen Dienst.
- 4.2. Weisungsberechtigt ist die zuständige Betreuungsperson des SLCs und / oder die anwesende LK.
- 4.3. Jeder PC-Nutzer trägt sich in die ausliegende Benutzerliste ein.
- 4.4. LK und SuS der BBS Cuxhaven dürfen das SLC im Rahmen des Unterrichts, für Arbeitsgemeinschaften sowie allgemeiner Nutzung im Zusammenhang mit schulischen Aufgaben nutzen.
- 4.5. SuS können während der festgelegten Öffnungszeiten des SLCs die dort vorhanden Medien unter Aufsicht der zuständigen Betreuungsperson und / oder einer LK nutzen, sofern die Medien verfügbar sind.
- 4.6. In den Belegungsplan eingetragene LK haben mit ihren Klassen das Hauptnutzungsrecht.
- 4.7. SuS benutzen nur unter Aufsicht das Selbstlerncenter. (Während der normalen Unterrichtszeiten haben die jeweiligen LK die Aufsichtspflicht. Diese ist nicht auf die Betreuungsperson übertragbar.)
- 4.8. Die Beschäftigung an den PC-Arbeitsplätzen darf die Arbeitsruhe im SLC nicht stören.
- 4.9. Drucken kostet 0,05 € pro Seite. Nutzt eine LK das SLC für seinen Unterricht, sind die daraus resultierenden Ausdrucke kostenfrei. Die Druckaufträge sind durch die zuständige Betreuungsperson freizugeben.
- 4.10. Die PCs nach der Nutzung nicht ausschalten. Die geöffneten Programme sind vor Verlassen des PCs zu schließen.
- 4.11. Das SLC wird videoüberwacht.
- 5. Ergänzende Bedingungen R110/R113/R114**
- 5.1. Taschen und Kleidungsstücke dürfen nicht auf Tischen abgelegt werden, auf denen Geräte stehen.
- 5.2. Jegliches Essen und Trinken in diesen Klassenräumen sind untersagt.
- 5.3. Während der Pausen sind die Fenster mit Notausgängen zu schließen. Nach der letzten Stunde müssen alle Fenster geschlossen werden.
- 5.4. Aushänge an den Wänden sollen bitte nur mit Magneten vorgenommen werden. Sie sind nach max. einem viertel Jahr zu entfernen.
- 5.5. Jede LK - dies betrifft auch reinen Theorieunterricht - trägt sich in das ausliegende "Nutzerverzeichnis" ein.
- 5.6. Schüler-PC's: Nach Beendigung der Arbeit sind die Programme ordnungsgemäß zu schließen. Insbesondere Windows ist herunterzufahren. Die PC's schalten sich selbst ab. Die Monitore werden nicht ausgeschaltet.
- 5.7. Lehrer-PC's: Die Lehrkräfte melden sich nach dem Unterricht vom Lehrer-PC lediglich ab. Die Lehrer-PC's werden nicht heruntergefahren! Die Beamer sind bitte in den Stand-by-Modus zu schalten. Die Lehrer-PC's werden – soweit kein Nutzer angemeldet ist - um 15.30 Uhr automatisch heruntergefahren. Der Strom in den Räumen wird bitte nicht abgeschaltet!

DameWare

Seit Ende 2009 setzen wir an den BBS Cuxhaven zur Fernwartung der Rechner die Software „DameWare“ ein. Diese ist auf jedem Client im Netzwerk installiert, wodurch die EDV-Administratoren die Möglichkeit haben, sich im Fehlerfall auf den PC zu schalten, um den Fehler schnellstmöglich zu beheben. Vorteilhaft ist bei DameWare, dass schnell auch für den Anwender ersichtlich ist, wenn sich ein Administrator auf den PC schaltet.

Standardmäßig, wenn keine Verbindung vom Administrator besteht, sieht man rechts im systray folgendes Symbol (vgl. Abb. 1). Wichtig sind dabei die Farben: rot und grün.



Abb. 1

Schaltet sich ein Administrator auf den PC, erscheint kurz ein Fenster zur Information (vgl. Abb. 2) und das Symbol von DameWare verändert die Farbe in rot und rot (vgl. Abb. 3)



Abb. 2



Abb. 3

Möchte der Anwender die Fernwartung vom Administrator trennen, kann er dafür mit der rechten Maustaste auf das DameWare-Symbol klicken. Es öffnet sich ein Kontextmenü (vgl. Abb. 4). Dort kann mit der linken Maustaste auf „Disconnect“ geklickt werden, um die Fernwartung zu trennen.

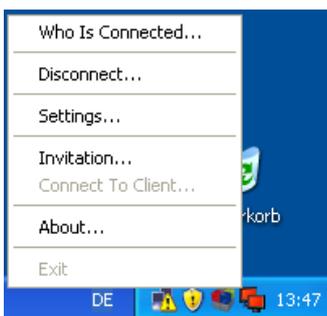


Abb. 4

Netzwerk

1. Jeder SuS und jede LK erhält einen eigenen Benutzeraccount. Die Daten sind vertraulich zu behandeln.
2. Jeder User hat im Netzwerk ein eigenes Laufwerk Z. Auf dieses Laufwerk hat nur der jeweilige Benutzer und im Fehlerfall die EDV Zugriff. (Ein Ausnahmefall stellen die Prüfungskonten dar.)
3. Jeder User hat ein Netzlaufwerk O. Dort befinden sich die Gruppenordner, die der Klasse entsprechen. LKe haben auf allen Gruppenordner Zugriff. Schüler nur auf ihre Klasse.
4. Jede LK erhält 30 eigene Prüfungskonten für den Unterricht. Die SuS können sich damit anmelden, haben damit keine Internetverbindung und im Netzwerk nur Zugriff auf das Laufwerk Z, welches das eigene Laufwerk vom Prüfungskonto ist. Auf dieses Laufwerk Z kann außerdem die LK über sein Laufwerk P zugreifen. Außerdem wird der LK ein Script zur Verfügung gestellt, worüber diese Prüfungskonten aktiviert und deaktiviert werden können.
5. Internetzugang wird über einen Proxy realisiert.
6. Es gibt täglich eine Datensicherung der Netzlaufwerke. Aufgrund technischer Gegebenheiten ist das aber keine Garantie auf Datensicherheit.
7. Wir empfehlen wichtige Daten mehrmals zu speichern. Z.B. im Netzwerk und auf einen USB Stick. Zu beachten ist dabei auch, dass ein USB Stick zum Transport von Daten dient. Die Daten sollten nicht nur auf dem USB Stick gespeichert sein.
8. Die LKe haben zusätzlich Zugriff auf das Laufwerk L. Dort haben alle LKe Zugriff.
9. An den PCs in den Klassenräumen kann sich auch lokal angemeldet werden. Zu beachten ist, dass es standardmäßig keinen Internetzugang und keinen Zugriff auf die Netzlaufwerke gibt. Hilfe zur lokalen Anmeldung finden Sie im *Info – Hinweis ↗ Windows ↗*.

Info-Hinweis 4

Zusätzliche Informationen für Lehrkräfte

1. Jede LK hat ein eigenes Mailpostfach. Nähere Informationen dazu finden Sie auf unserer Intranetseite unter <http://www.bbscux.de/intranet/mail/bbs-mail-installation-und-nutzung/index.php>
2. Die Datenschutzbestimmungen im Umgang mit den Schülerdaten sind zu beachten. Nähere Informationen dazu finden Sie auf unserer Intranetseite unter <http://www.bbscux.de/intranet/themen/datenschutz/index.php>
3. Jede LK verteilt zu Beginn des Schuljahres die Zugangsdaten an die SuS. Mit diesen Daten ist bedacht und vertraulich umzugehen !
4. Die Passwörter sind im Verwaltungsnetz (z.B. an den Lehrerarbeitsplätzen im Lehrerraum) pro Klasse einzusehen und auszudrucken.
5. Jede LK erhält 30 eigene Prüfungskonten für den Unterricht. Die Schüler können sich damit anmelden, haben damit keine Internetverbindung und im Netzwerk nur Zugriff auf das Laufwerk Z, welches das eigene Laufwerk vom Prüfungskonto ist. Auf dieses Laufwerk Z kann die Lehrkraft über sein Laufwerk P zugreifen. Außerdem wird der LK ein Script zur Verfügung gestellt, worüber diese Prüfungskonten aktiviert und deaktiviert werden können.
6. Es gibt täglich eine Datensicherung der Netzlaufwerke. Aufgrund technischer Gegebenheiten ist das aber keine Garantie auf Datensicherheit. Im Bedarfsfall kann eine eventuell versehentlich gelöschte Datei durch die EDV wieder hergestellt werden. Bitte greifen Sie darauf nur im Notfall zurück, da dieser Vorgang zeitaufwendig für die EDV-Mitarbeiter ist.

Kurzanleitung VGA-Matrix Splitter

Linke Spalte (1) zeigt an,
was auf dem Monitor
wiedergegeben wird.

Rechte Spalte (2) zeigt an,
was auf dem Beamer
wiedergegeben wird.

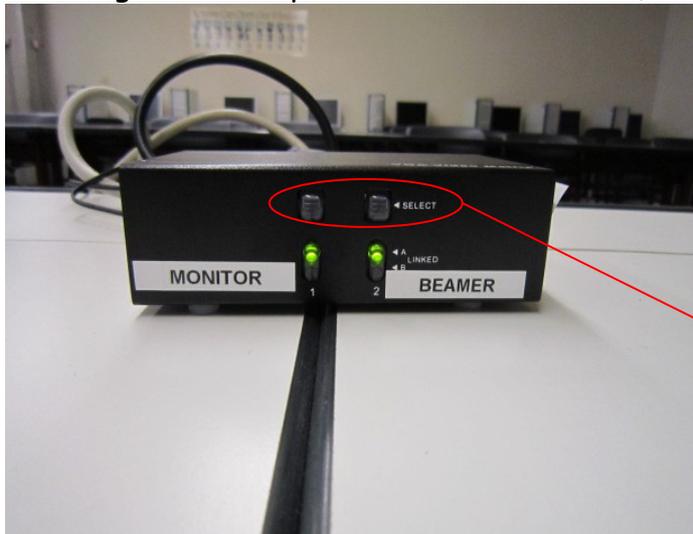
Quelle

Lehrer-PC (A=grün)

Notebook (B=rot)

Beispiele:

Wiedergabe Lehrerpcauf Monitor+ Beamer (Lampengrün)



Auswahl über
Select

Wiedergabe Notebook auf Monitor + Beamer (Lampen rot)



Gebrauch VGA-Matrix Splitter

Liebe Kolleginnen, liebe Kollegen,

in diesem Klassenraum befindet sich nun ein sogenannter *VGA-Matrix-Splitter*. Damit können Sie auf dem Beamer und auf dem Monitor entweder das Bild vom Lehrer-PC oder von einem anderen PC / Notebook wieder geben.

In diesem Raum ist als zweites *Gerät* ein Notebook anzuschließen. Das dazugehörige Monitorkabel, sollten Sie auf dem Tisch finden.

Der Lehrer-PC ist hier an Anschluss A angeschlossen
Das Notebook ist hier an Anschluss B angeschlossen.

Der Monitor ist an Anschluss 1 angeschlossen

Und der Beamer ist an Anschluss 2 angeschlossen.

An dem Matrix-Splitter sehen Sie zwei Reihen von Knöpfen (vgl. Abb. 1). Mit den oberen Knöpfen können Sie die Quelle (Lehrer-PC oder Notebook) für den jeweiligen Bildschirm (Monitor oder Beamer) auswählen.

An der unteren Reihe der Knöpfe erkennen Sie, welche Quelle gerade auf dem jeweiligem Bildschirm angezeigt wird.



Abb. 1

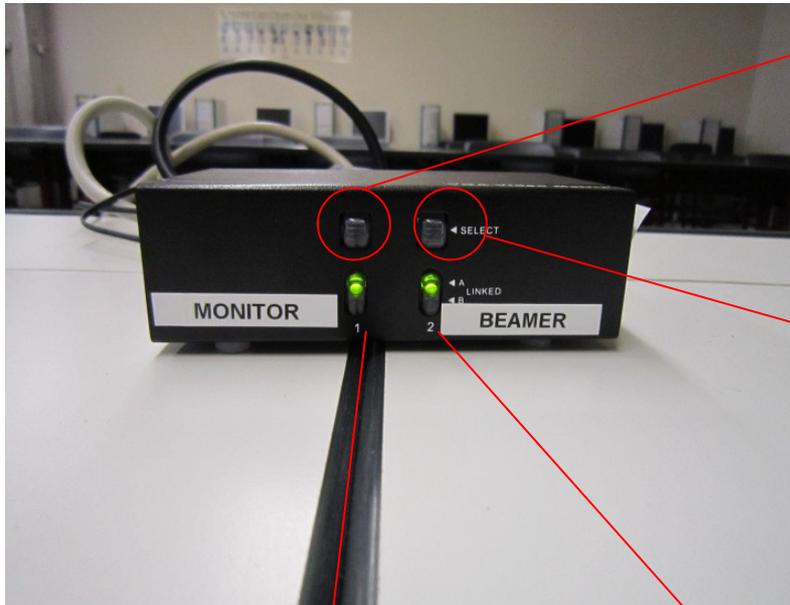
Die linke Spalte zeigt an, was auf dem Monitor (1) angezeigt wird. Leuchtet die Lampe grün, so wird auf dem Monitor die Quelle Lehrer-PC (A) angezeigt. Bei der rechten Spalte wird angezeigt, was auf dem Beamer angezeigt wird. Leuchtet auch hier die Lampe grün, so wird auf dem Beamer die Quelle Lehrer-PC (A) angezeigt.

Soll auf Monitor (1) oder Beamer (2) die Quelle Notebook (B) angezeigt, so muss in der entsprechenden Spalte auf den Select-Knopf gedrückt werden. Wird dieser Knopf in der linken Spalte (Reihe 1) gedrückt, wechselt die Lampe unten auf Rot  d.h., dass die Quelle auf Notebook (B) wechselt. Würde man noch mal den Select-Knopf betätigen, würde die Lampe darunter gar nicht mehr leuchten, somit würde auf dem Monitor (1) kein Signal angezeigt werden.

Leuchten die beiden Lampen also unten rot, so wird das Signal vom Notebook (B) auf Monitor (1) und Beamer (2) angezeigt (vgl. Abb. 2)



Abb. 2



Select-Knopf, um bei Anzeigegerät Monitor (1) die Quelle Lehrer-PC (A=grün) oder Notebook (B=rot) auszuwählen

Select-Knopf, um bei Anzeigegerät Beamer (2) die Quelle Lehrer-PC (A=grün) oder Notebook (B=rot) auszuwählen

Abb. 3h

Linke Spalte (1) zeigt an, was auf Anzeigegerät Monitor wiedergegeben wird

Rechte Spalte (2) zeigt an, was auf Anzeigegerät Beamer wiedergegeben wird.

Zu Anfang ist der Gebrauch bestimmt ungewohnt. Wir hoffen, dass diese kurze Beschreibung, Ihren Einstieg erleichtert.

Bei Fragen stehen wir natürlich gerne zur Verfügung.

Mit freundlichen Grüßen
Ihre EDV

Einleitung

Aufgrund der „Verordnung personenbezogener Daten auf privaten Informationstechnischen System (IT Systemen) von Lehrkräften“ ist es unter Anderem notwendig, dass personenbezogene Daten auf USB Sticks verschlüsselt werden. An den BBS Cuxhaven kann dafür das Programm TrueCrypt verwendet werden.

Auf den Lehrer-PCs wird das Programm von der EDV-Abteilung installiert. An den Heim-PCs müssten Sie es selber installieren.

In dieser Anleitung wird daher folgendes beschrieben:

TrueCrypt Installation	Seite 2-4
Einen Container in TrueCrypt vorbereiten	Seite 5-12
TrueCrypt verwenden – auf einen Container zugreifen	Seite 13-18
Hinweise zum Gebrauch	Seite 19

Da die Verordnung nur von personenbezogenen Daten spricht, und dies meist Daten betrifft, die nicht so groß sind, wird in dieser Anleitung ein so genannter Container auf einem USB Stick erstellt. Dieser Container ist verschlüsselt. Wird der USB Stick mit dem Arbeitsplatz geöffnet, sieht man auf dem USB Stick eine Datei, die dieser Container ist. Auf diesem Container kann nur mit einem Passwort zugegriffen werden. Innerhalb dieses Containers können dann personenbezogene Daten gespeichert werden.

Die Setup-Datei „*TrueCrypt Setup 7.1a.exe*“ ist im Schulnetz unter
\\172.16.7.7\iso\TrueCrypt
zu finden.

Im Verwaltungsnetz finden Sie die Setup-Datei „*TrueCrypt Setup 7.1a.exe*“ unter
i:\install

Nähere Informationen finden Sie im Intranet unter
<http://bbs-cux.de/intranet/themen/datenschutz/index.php>.

TrueCrypt installieren

1. Starten Sie das Setup-Programm „*TrueCrypt Setup 7.1a.exe*“ mit einem Doppelklick. Es öffnet sich das Setup-Fenster mit den Lizenzbedingungen. Akzeptieren Sie die Lizenzbedingungen mit einem Klick in das Kontrollkästchen bei „*I accept the license terms*“ (vgl. Abb 1) und klicken dann auf den Butten *Next*.

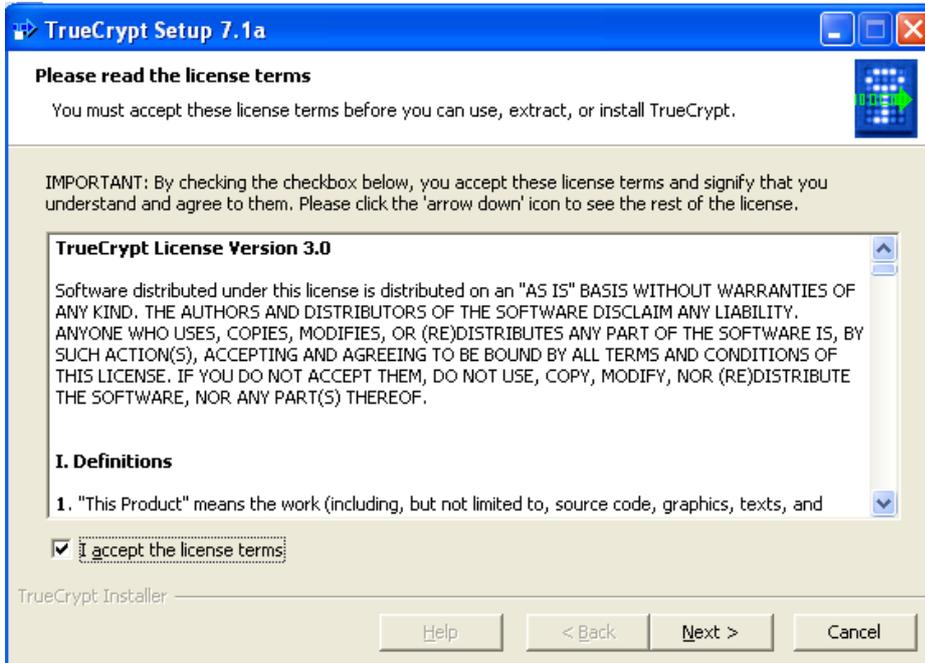


Abb. 1

2. Im nächsten Fenster wählen Sie die Installationsart. Lassen Sie die Einstellung auf „*Install*“ (vgl. Abb. 2) und bestätigen Sie die Eingabe mit einem Klick auf den Butten *Next*.

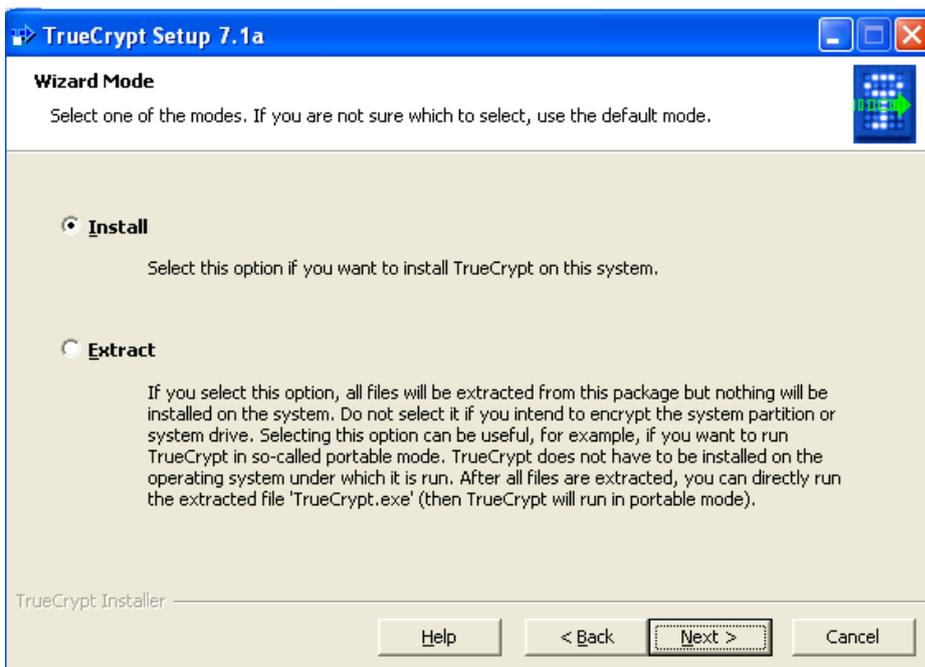


Abb. 2

- Im sich öffnenden Fenster können die Setup-Optionen eingestellt werden. Diese können auch so gelassen werden, wie Sie vorgeschlagen werden (vgl. Abb. 3). Eingabe mit einem Klick auf *Install* bestätigen.

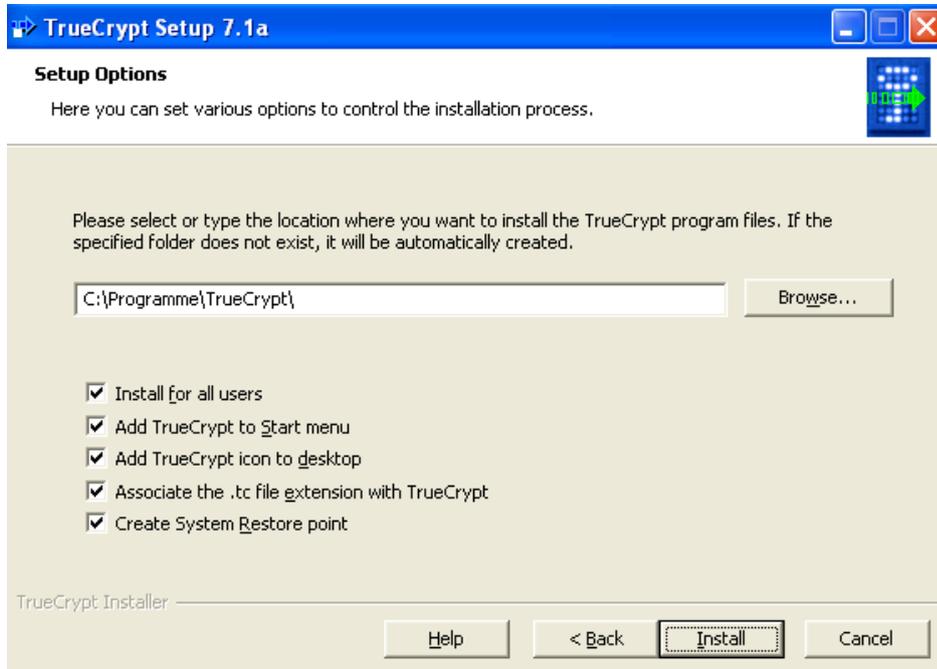


Abb. 3

- Die Installation beginnt. Ist die Installation abgeschlossen, so erscheint folgende Erfolgsmeldung (vgl. Abb. 4). Bestätigen Sie diese mit einem Klick auf *OK*.

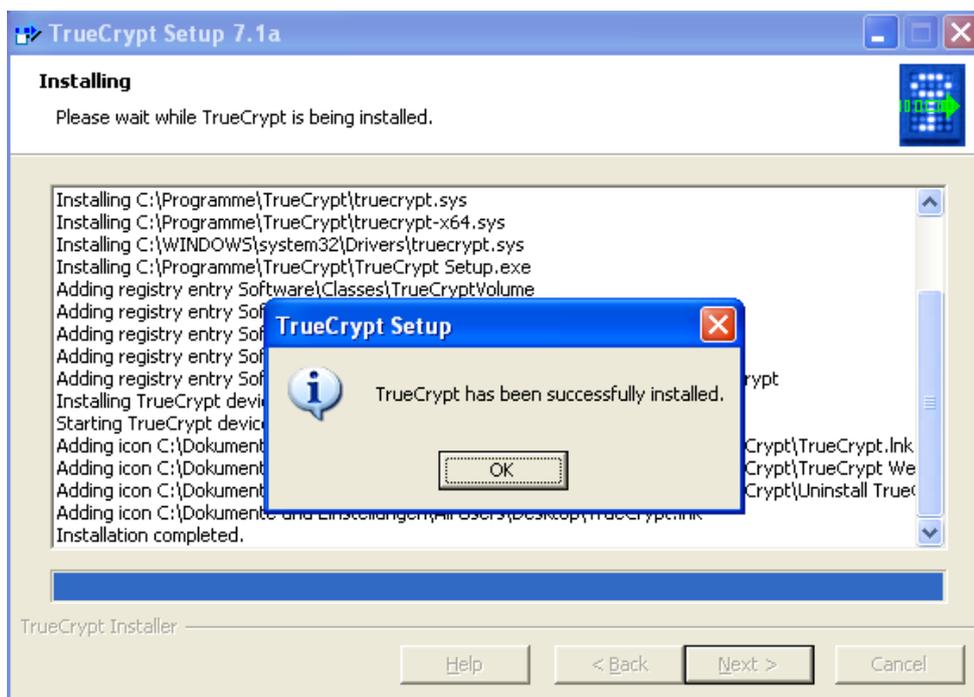


Abb. 4

5. Es öffnet sich das Fenster aus Abb. 5. Bestätigen Sie dieses mit einem Klick auf den Button *Finish*.

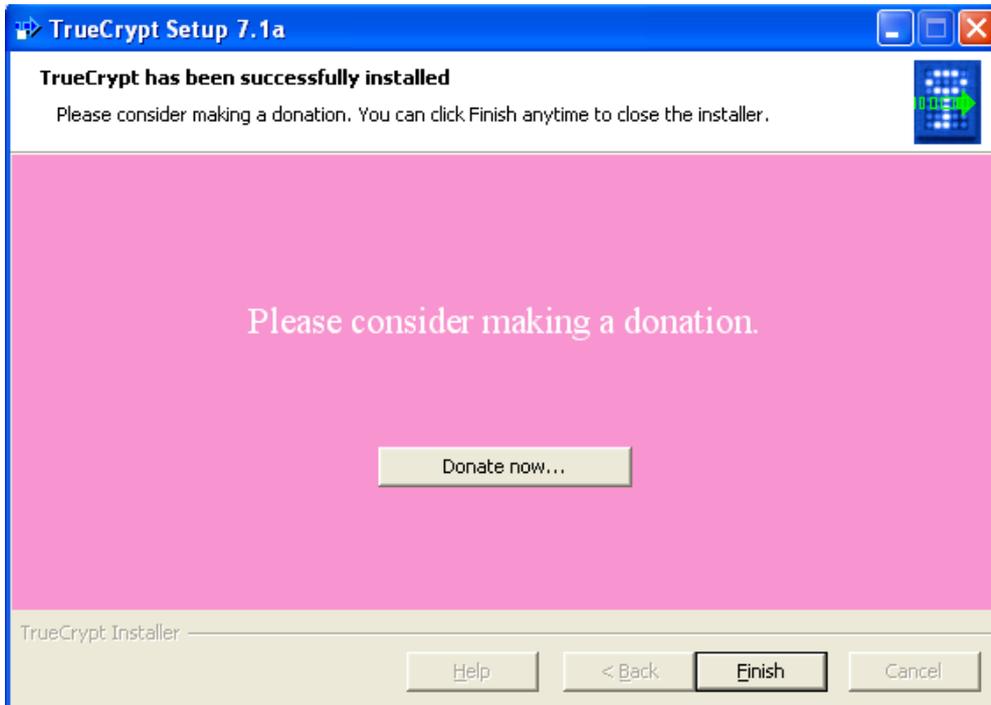


Abb. 5

6. Es erscheint eine Meldung, dass Ihnen empfiehlt, das Tutorial zu lesen (vgl. Abb. 6). Möchten Sie das Tutorial lesen, klicken Sie auf den Button *Ja*. Möchten Sie es jetzt nicht lesen, klicken Sie entsprechend auf den Button *Nein*.

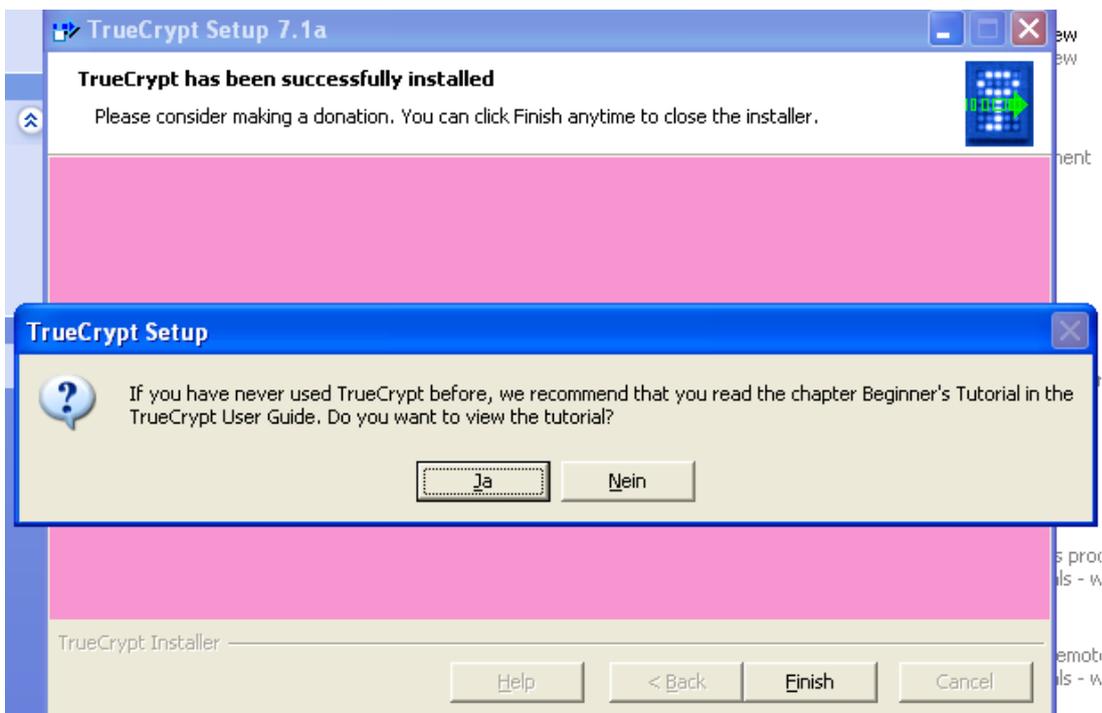


Abb. 6

Einen Container in TrueCrypt vorbereiten

7. Schließen Sie Ihren USB Stick, den Sie vorbereiten möchten, an dem PC an. Öffnen Sie das Programm TrueCrypt über den Startmenüeintrag „Start/Programme/TrueCrypt/TrueCrypt“. Sie sehen das Programmfenster von TrueCrypt (vgl. Abb. 7). Da wir noch keinen USB Stick vorbereitet haben, werden wir dies nun durchführen. Dazu klicken Sie auf den Button *Create Volume*.

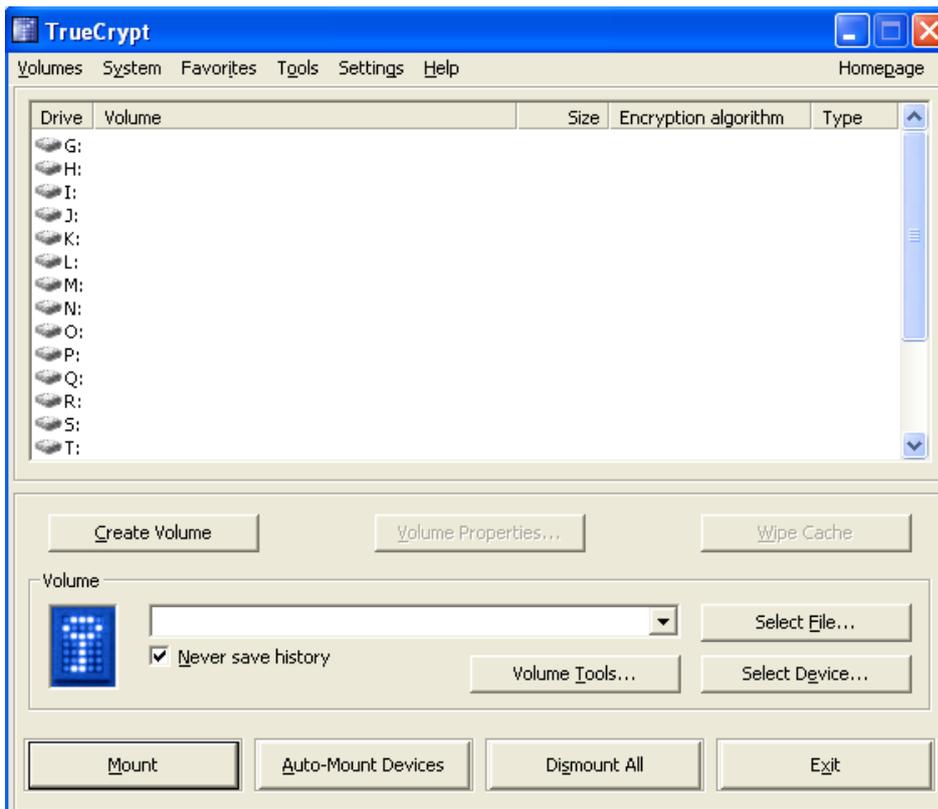


Abb. 7

8. Es erscheint der Assistent, um einen Datenträger vorzubereiten (vgl. Abb. 8). Wir verwenden die bereits ausgewählte Standardeinstellung „*Create an encrypted file container*“ und klicken auf den Button *Next*.



Abb. 8

9. Im sich öffnenden Fenster kann die bereits ausgewählte Einstellung „*Standard TrueCrypt volume*“ beibehalten werden (vgl. Abb. 9). Klicken Sie im Anschluss wieder auf den Button *Next*.

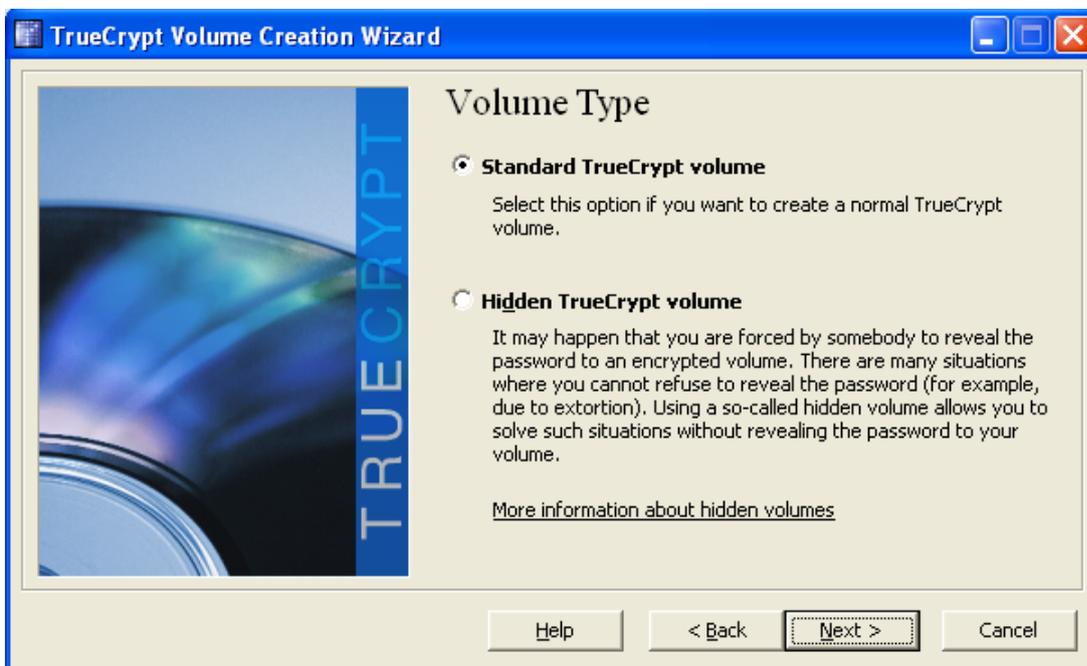


Abb. 9

10. Im nächsten Schritt wird der USB Stick ausgewählt. Klicken Sie im sich öffnenden Fenster (vgl. Abb. 10) auf den Button *Select File...*

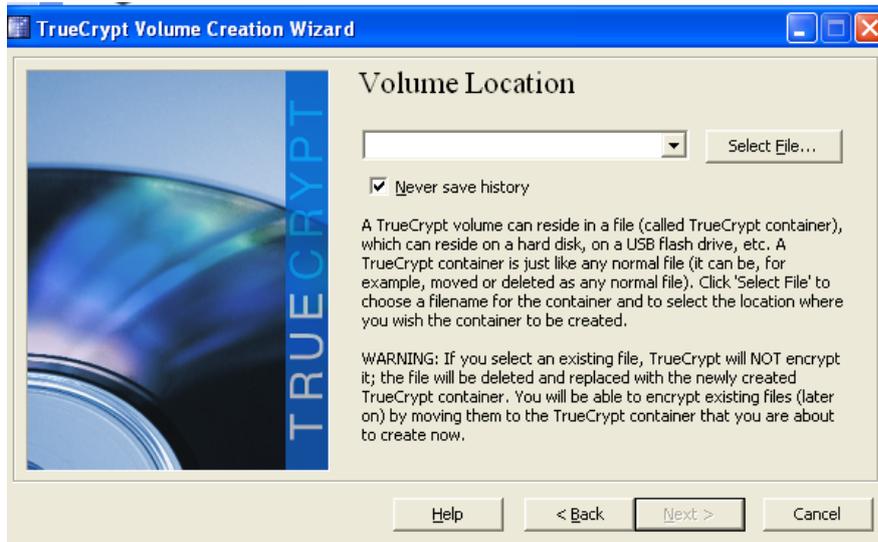


Abb. 10

11. Es öffnet sich ein Fenster, wo Sie den USB Stick auswählen können. Klicken Sie dazu auf die Pfeilschaltfläche am Ende der Zeile bei „Speichern in:“. Ist Ihr USB Stick ausgewählt, können Sie dem Container einen Namen geben. Dazu geben Sie den Namen in der Zeile „Dateiname:“ ein. In unserem Beispiel heißt unser Container „truecrypt“ (vgl. Abb. 11). Übernehmen Sie die Einstellungen mit einem Klick auf den Button *Speichern*.
Hinweis: Sie können die Datei auch mit der Endung „.tc“ speichern. Dazu später mehr.

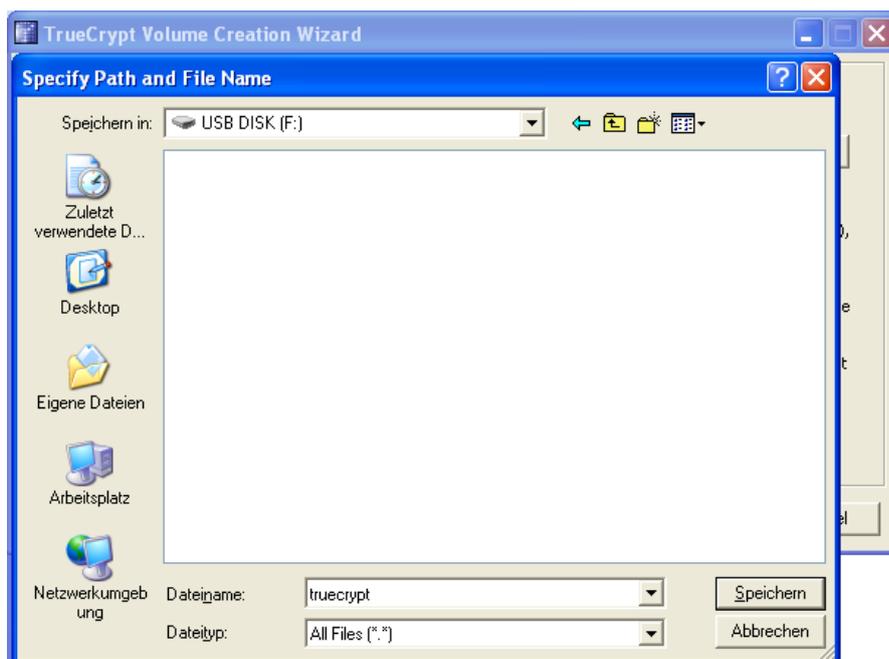


Abb. 11

12. Die Werte wurden nun im vorherigen Fenster übernehmen (vgl. Abb. 12). Bestätigen Sie die Eingabe mit einem Klick auf den Button *Next*.

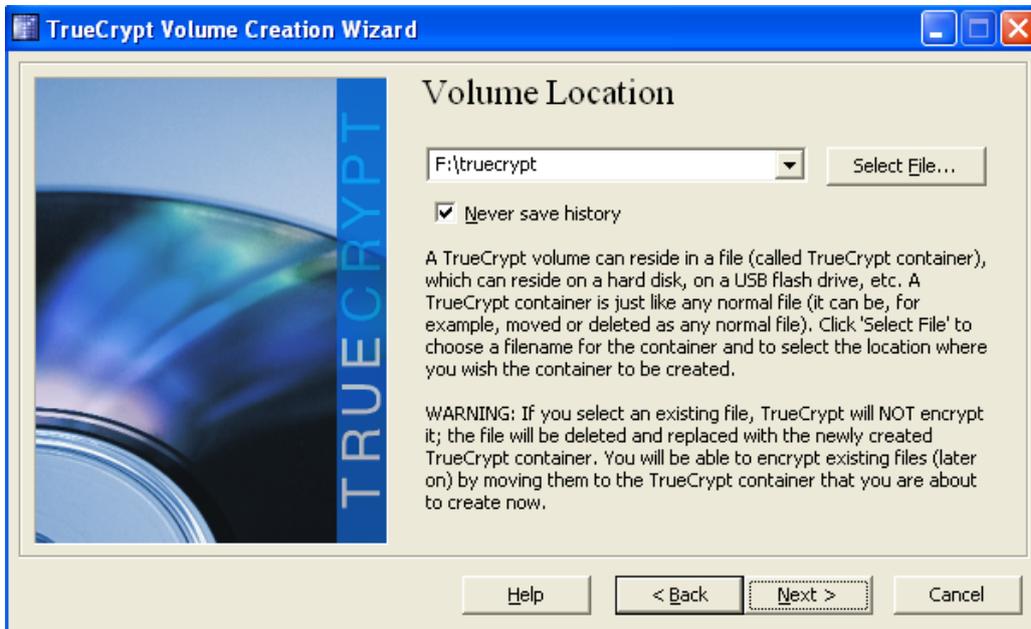


Abb. 12

13. Im folgenden Fenster wird der Verschlüsselungsalgorithmus ausgewählt. Die Standardeinstellungen können übernommen werden (vgl. Abb. 13) und mit einem Klick auf *Next* ausgewählt werden.



Abb. 13

14. Im nächsten Fenster wird die Größe des Containers ausgewählt. In unserem Beispiel ist der USB Stick 4GB groß. Und da wir den Container nur für personenbezogene Daten verwenden möchten, soll der Container 1GB groß sein. Die restlichen 3GB können wir dann unverschlüsselt für nicht personenbezogene Daten verwenden. Daher wählen wir in unserem Beispiel „1GB“ aus (vgl. Abb. 14) und bestätigen mit einem Klick auf den Button *Next*.

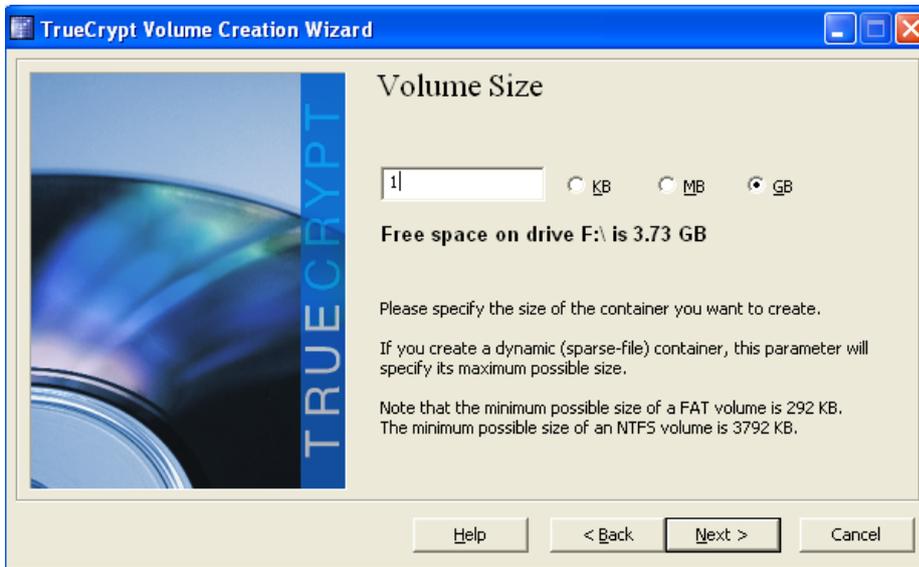


Abb. 14

15. Im nächsten Schritt werden Sie aufgefordert ein Passwort einzugeben. Geben Sie Ihr Passwort in dem Feld „*Password:*“ ein und wiederholen Sie dies im Feld „*Confirm:*“ (vgl. Abb. 15). Bestätigen Sie Ihre Eingabe mit einem Klick auf *Next*.

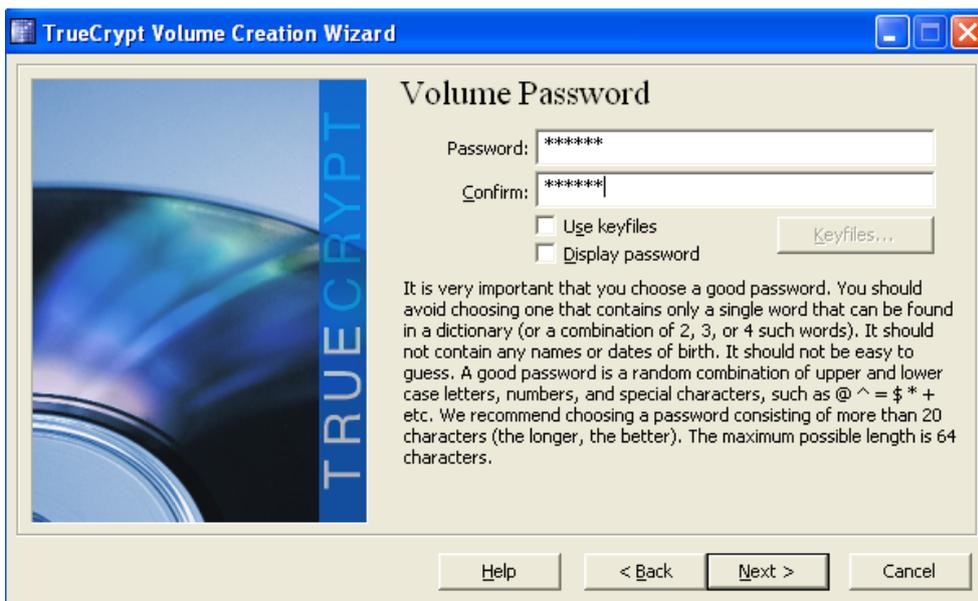


Abb. 15

16. Besteht Ihr Passwort aus weniger als 20 Zeichen, so erscheint eine Warnmeldung, da das Programm ein Passwort mit mehr als 20 Zeichen vorschlägt (vgl. Abb. 16). Sie können Ihr Passwort auch mit weniger als 20 Zeichen verwenden. Klicken Sie dazu im Fenster der Warnmeldung auf den Button *Ja*.



Abb. 16

17. Im nächsten Schritt kann der Container formatiert werden. Im Fenster Volume Format wechselt die Zeichenfolge beim Eintrag „Random Pool:“ (vgl. Abb. 17). Hier wechselt der Schlüssel zur Verschlüsselung des Containers. Klicken Sie irgendwann auf den Button *Format*.



Abb. 17

18. Der Container wird mit dem Schlüssel formatiert, der zu dem Zeitpunkt des Klicks ausgewählt war (vgl. Abb. 18). Dieser Vorgang kann einige Zeit in Anspruch nehmen.

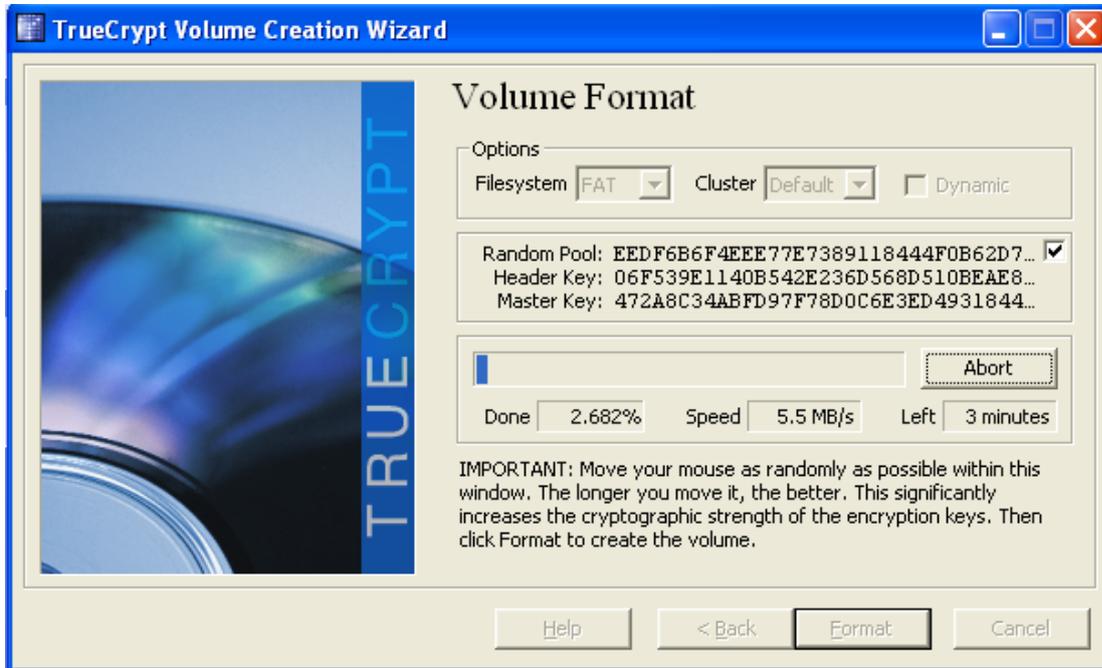


Abb. 18

19. Ist die Formatierung abgeschlossen erscheint das Fenster. Bestätigen Sie mit einem Klick auf *OK*.



Abb. 19

20. Unser Container wurde erstellt. Da wir keinen weiteren Container hier erstellen möchten, können wir das sich öffnende Fenster mit einem Klick auf *Exit* schließen (vgl. Abb. 20).

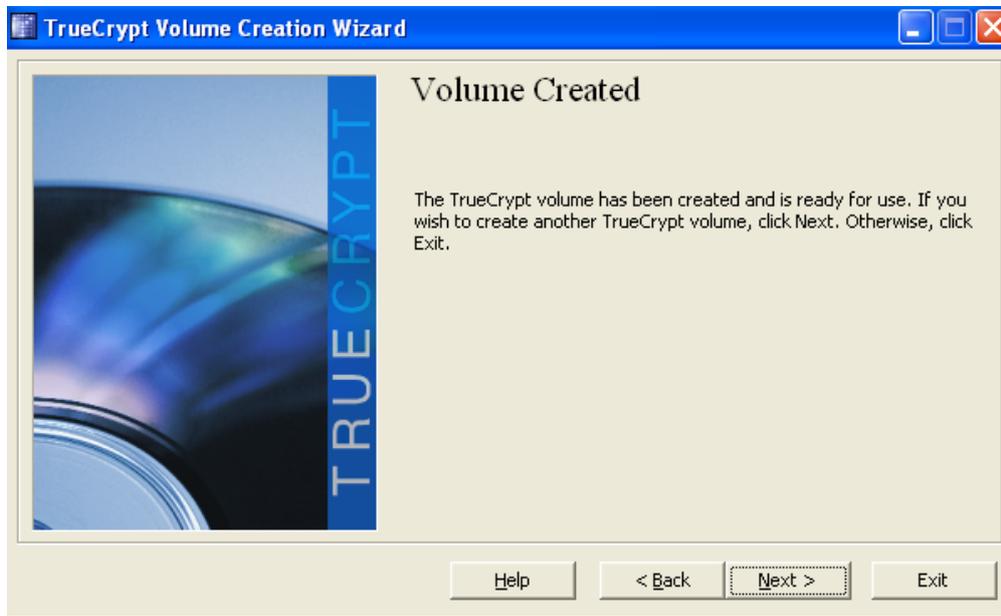


Abb. 20

21. Auf unserem USB Stick befindet sich jetzt eine Datei mit dem Namen *truecrypt* (vgl. Abb. 21). Diesen Dateinamen wählten wir in Schritt 11 und 12 aus. Dies ist unser Container. In dieser Datei können unsere personenbezogenen Daten gespeichert werden und sind dann auf dem USB Stick für den Transport verschlüsselt.

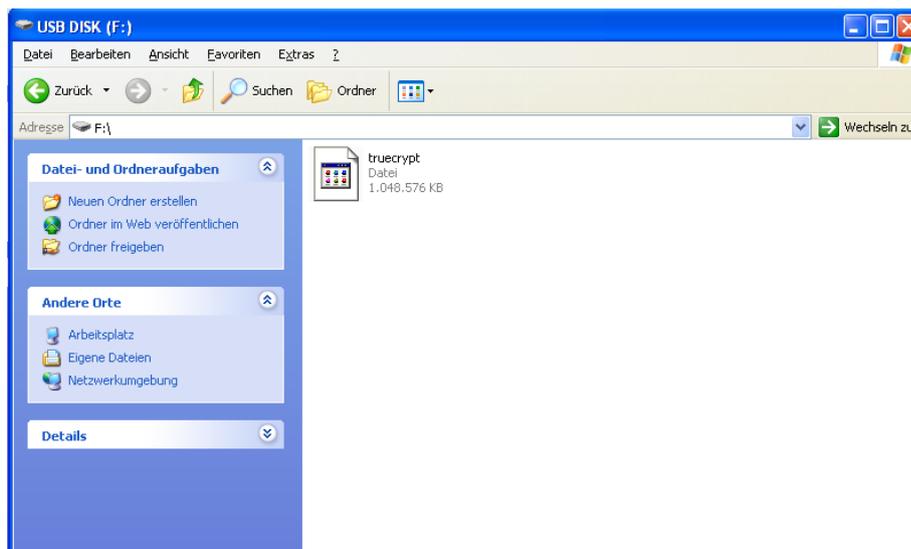


Abb. 21

Unser USB-Stick ist vorbereitet: er enthält unseren Container. Nun können wir mit dem Container arbeiten.

TrueCrypt verwenden – auf einen Container zugreifen

22. Um auf den Container truecrypt nun zugreifen zu können, müssen wir diesen einbinden. Dieser Vorgang wird auch „Mounten“ genannt. Dazu öffnen wir das Programm TrueCrypt, falls es nicht schon offen ist. Wir sehen das Fenster aus Abb. 22. Zunächst wählen wir den Container aus. Dazu klicken wir auf den Button *Select File...*

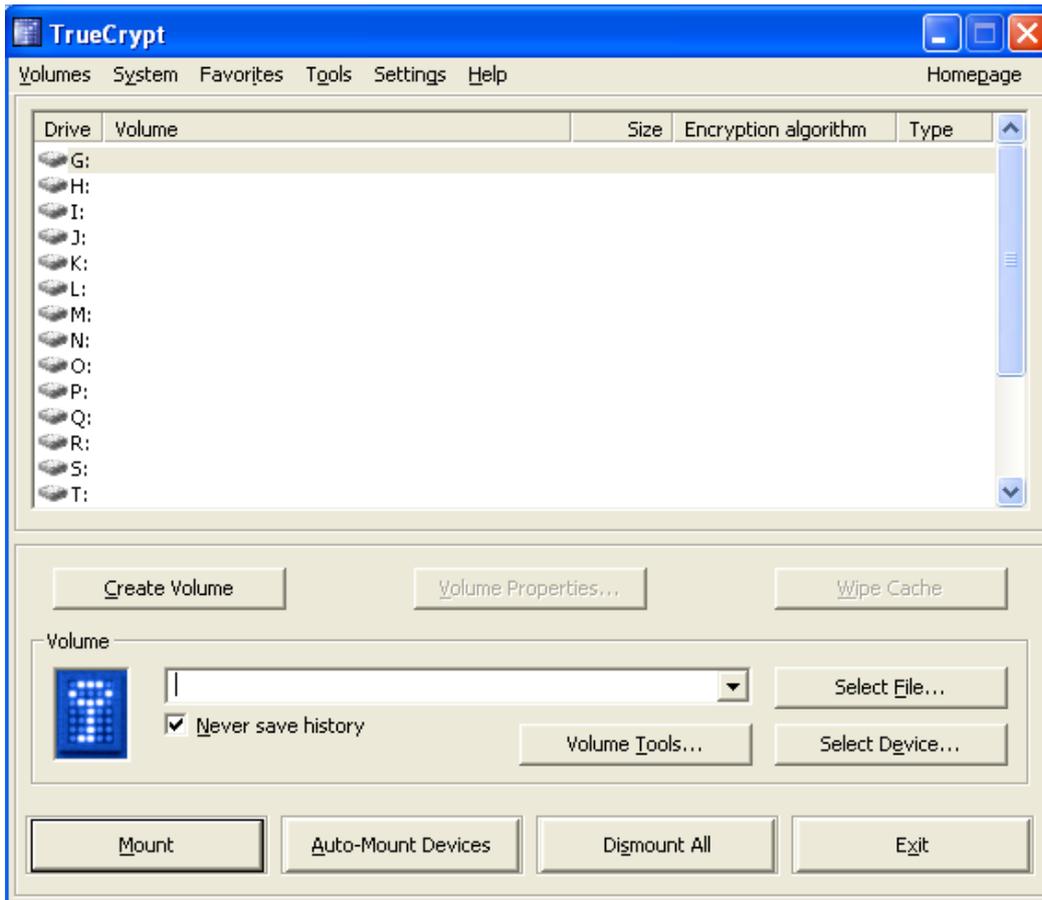


Abb. 22

23. Es öffnet sich ein Fenster, wo wir unseren Container auswählen. In unserem Fall wählen wir die Datei *truecrypt* auf unserem USB Stick aus (vgl. Abb. 23). Ist die Datei ausgewählt, klicken Sie auf den Button *Öffnen*.

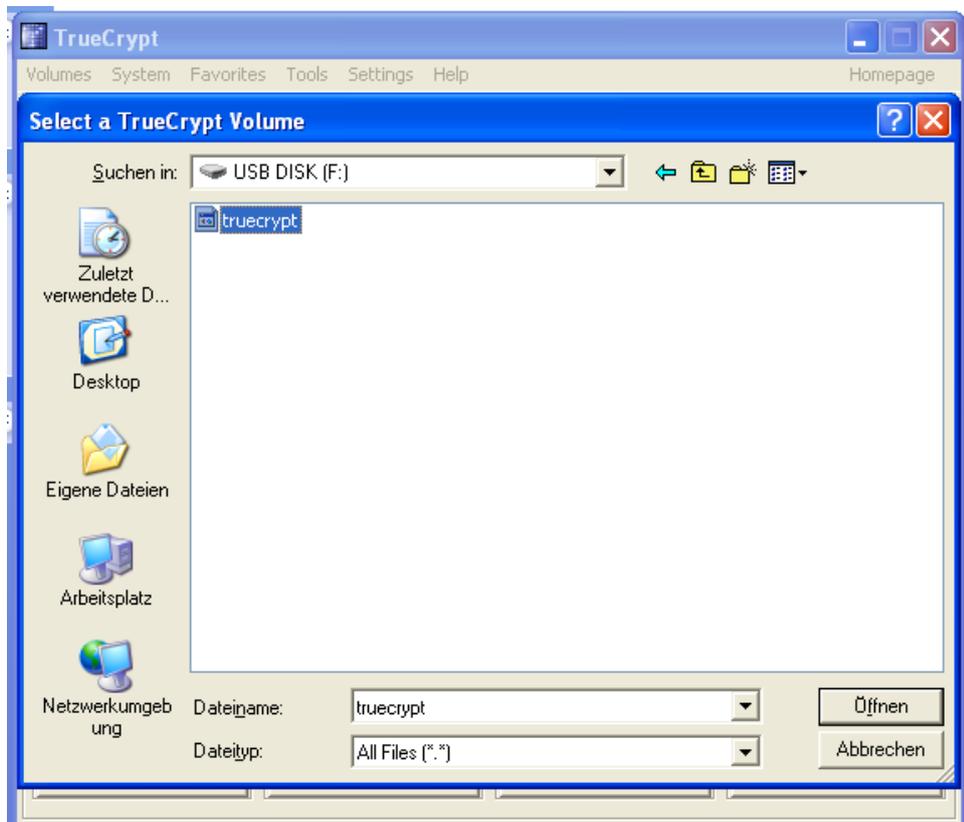


Abb. 23

24. Der Pfad zur Datei von unserem Container ist nun in dem Abschnitt „Volume“ eingetragen (vgl. Abb. 24). Markieren Sie im oberen Bereich des Fensters einen Laufwerksbuchstaben. Über diesen Buchstaben greifen Sie dann auf dem Inhalt des Containers zu. In unserem Beispiel wählen wir den Buchstaben „G:“ aus (vgl. Abb. 24). Dieser ist dann blau hinterlegt.

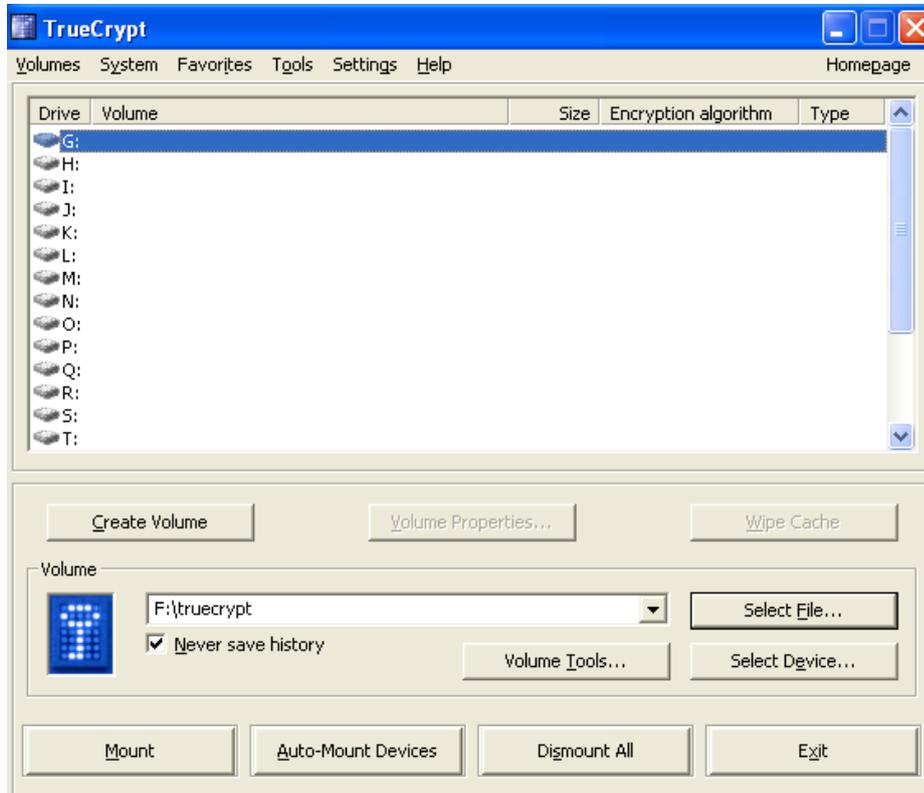


Abb. 24

25. Klicken Sie nun auf den Button *Mount* aus Abb. 24. Es öffnet sich ein Fenster, wo Sie das Passwort für Ihren Container eingeben (vgl. Abb. 25). Dies Passwort haben Sie in Schritt 15 und 16 vergeben. Geben Sie Ihr Passwort dort ein und bestätigen Sie es mit einem Klick auf *OK*.

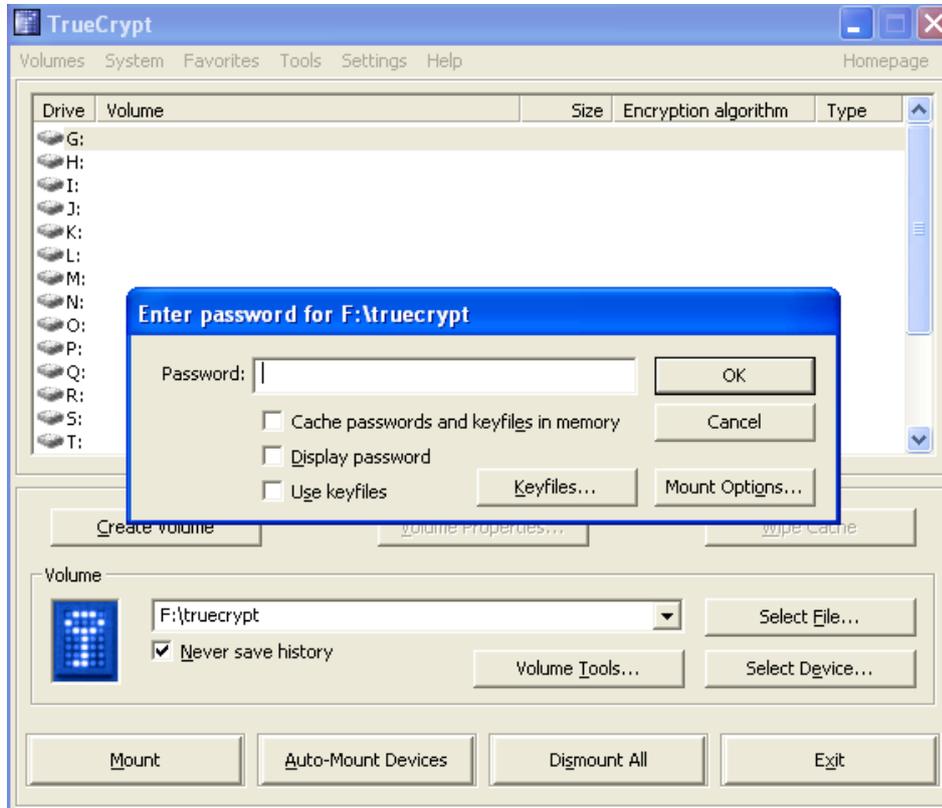


Abb. 25

26. Sie können nun auf Ihren Container zugreifen. Er ist sozusagen „gemountet“. Dies erkennen Sie daran, dass hinter dem ausgewählten Laufwerksbuchstaben im oberen Teil des Fensters, der Dateipfad zum Container ausgewählt ist (vgl. Abb. 26). Außerdem steht anstelle des Buttons *Mount* aus Abb. 24 nun *Dismount* (vgl. Abb. 26).

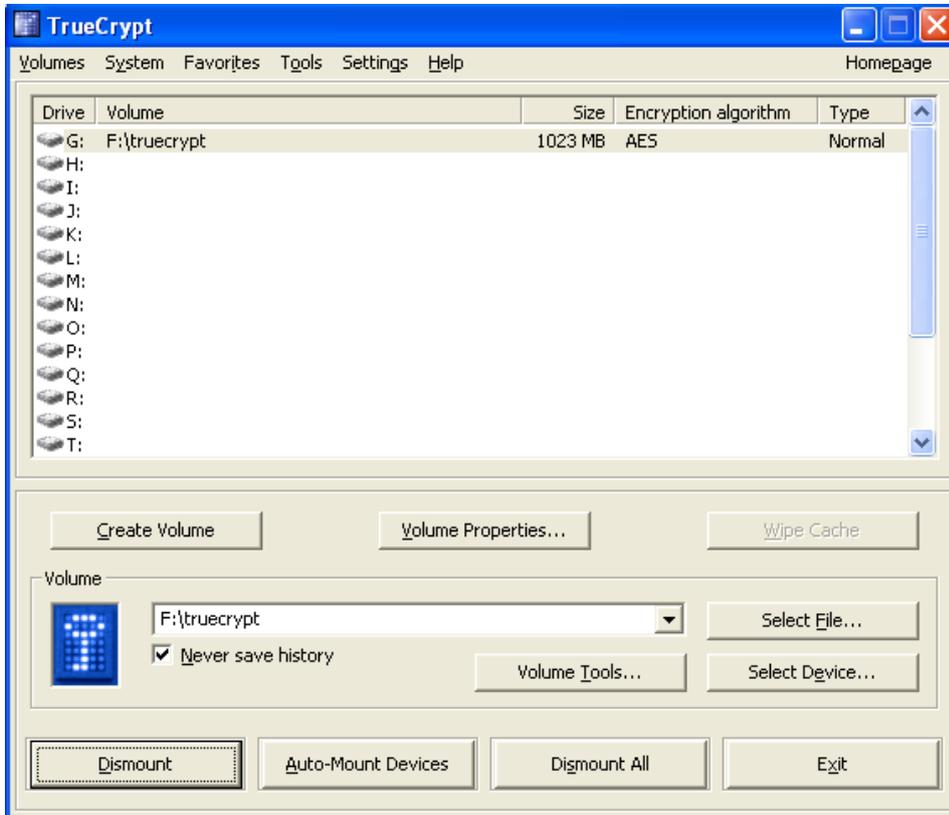


Abb. 26

27. Im Arbeitsplatz sehen Sie nun also auch das Laufwerk G (vgl. Abb. 27) und können so auf Ihren Container zugreifen, um z.B. personenbezogene Daten dort abzuspeichern.

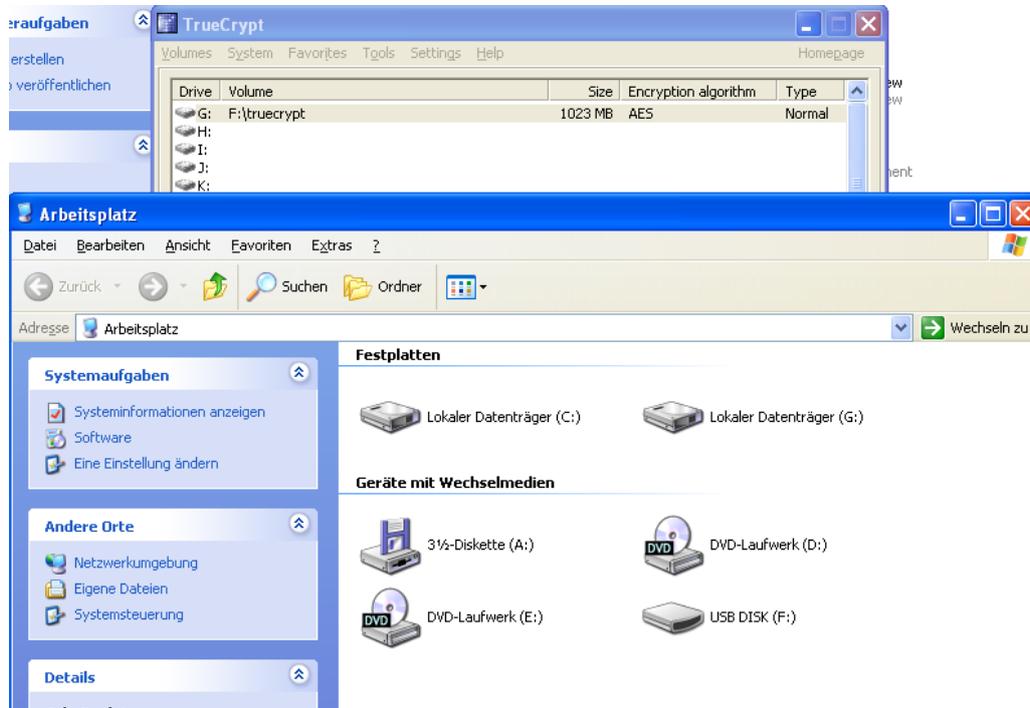


Abb. 27

28. Möchten Sie den USB Stick von Ihrem PC entfernen, klicken Sie im TrueCrypt Fenster zunächst auf den Button *Dismount*. Erst dann können Sie den USB Stick wie gewohnt auswerfen und dann abziehen. Bitte nicht vergessen, den USB Stick vor dem Abziehen auch am Rechner zu beenden ! Es kann ansonsten zu Datenverlust kommen.

Hinweise zum Gebrauch

29. Eine andere Alternative zur Verwendung ist, den Container mit der Endung „.tc“ zu speichern. In unserem Beispiel würde der Container dann „*truecrypt.tc*“ heißen. Wenn Sie den USB Stick dann öffnen und doppelt auf die Datei klicken, erscheint gleich das Programmfenster von TrueCrypt, wo der Container bereits ausgewählt ist (vgl. Abb. 24). Sie müssen dann nur noch auf den Button „Mount“ klicken und nach erfolgreicher Passwortabfrage, ist der Container gemountet – Sie sehen Abb. 26.
30. Wenn Sie während des Arbeitens das Programmfenster von TrueCrypt schließen, gibt es einen weiteren Weg, wie Sie leicht das Programmfenster öffnen können. Während das Programm läuft, befindet sich unten rechts in Ihrem Systray das Symbol von TrueCrypt (vgl. Abb. 30). Klicken Sie mit der linken Maustaste einmal auf dieses Symbol, öffnet sich das Programm TrueCrypt. Klicken Sie mit der rechten Maustaste auf dieses Symbol, öffnet sich ein Kontextmenü, wo Sie auch den Befehl „*Dismount*“ auswählen können.



Abb. 30

Es gibt zwei Arten, um sich anzumelden:

1. In der Domäne BBSCUXSCHUL
2. Lokal am PC

Gibt man bei Windows 7 einen Benutzer ein, so geht der PC standardmäßig davon aus, dass der Benutzer Mitglied der Domäne ist.

Dies kann auch daran erkannt werden, dass unter dem Kennwort-Feld steht „Anmelden an: BBSCUXSCHUL“ (vgl. Abb. 1)

Hier können nun der gewünschte Benutzername und Passwort eingegeben werden. Mit einem Klick auf den Pfeil nach rechts oder mit Drücken auf die Taste Enter wird die Anmeldung vorgenommen.



Abb. 1

War bereits ein Benutzer angemeldet, sieht der Anmeldebildschirm ähnlich Abb. 2 aus. In unserem Beispiel war der Benutzer „bruhmela“ zuletzt angemeldet. Dieser User müsste nur sein Kennwort eingeben und die Eingabe bestätigen. Möchte man sich nun mit einem anderen Benutzer anmelden, kann dafür auf den Button **„Benutzer wechseln“** geklickt werden. Es erscheint dann ein ähnliches Bild wie in Abb. 3.



Abb. 2

Hier kann man den zuletzt verwendeten Benutzer auswählen oder auf die Schaltfläche **„Anderer Benutzer“** klicken. Wird auf **„Anderer Benutzer“** geklickt, kann wie in Abb. 1 sein eigener Benutzername und Passwort eingegeben werden.

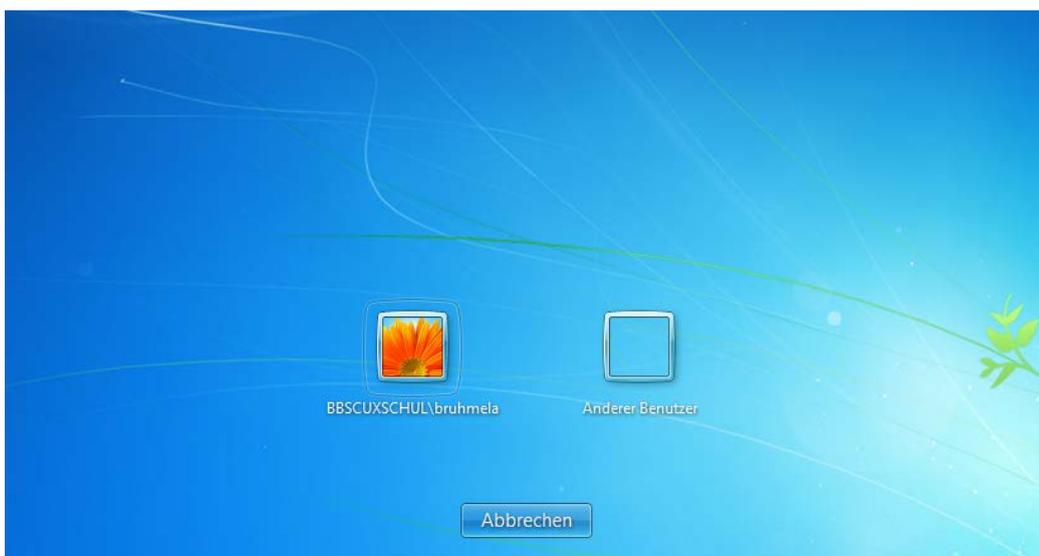


Abb. 3

Wird eine lokale Anmeldung gewünscht, wie an den Lehrerpcs mit dem Benutzernamen „pc50“ beispielsweise, so muss vor dem Benutzernamen folgende Zeichenfolge auftauchen:

.\

In unserem Beispiel wird also als Benutzername

.\pc50

Eingegeben (vgl. Abb. 4). Unter dem Feld für das Kennwort steht in unserem Beispiel nun „Anmelden an: R102-PC50“

In dem Fall entspricht „r102-pc50“ dem Computernamen. Und daraus kann der Benutzername pc50 erkannt werden.

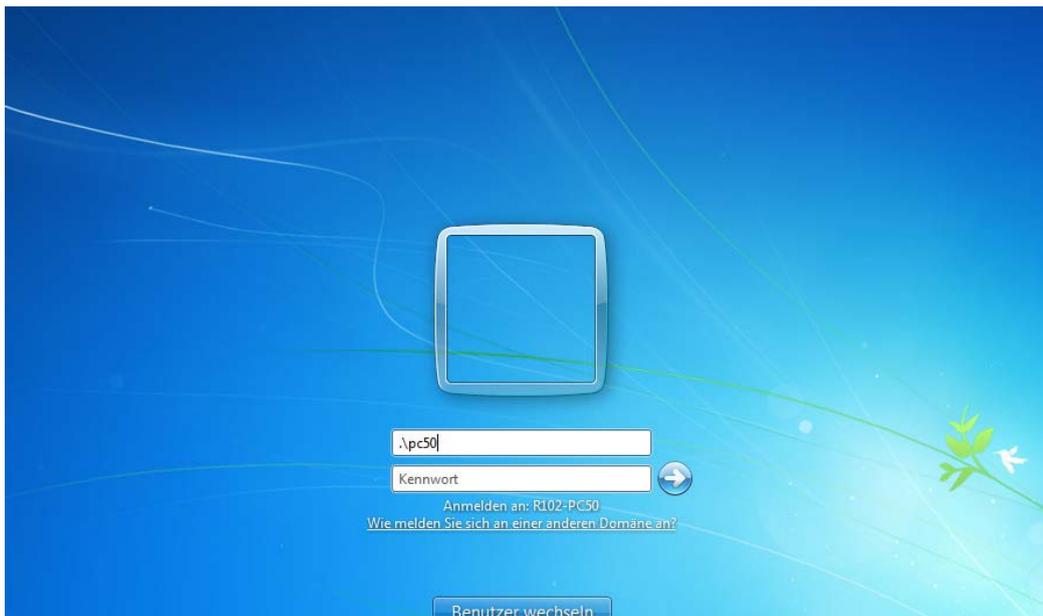


Abb. 4.

1. Wenn Sie sich an den Lehrerarbeitsplätzen mit „lehrer1“ anmelden, haben Sie eine Verknüpfung auf dem Desktop mit der Datenbank „bbscuxschul-fe“. Sie können aber auch über Start/Programme die Datenbank starten (vgl. Abb. 1). Unter Programme existiert der Aufruf der Datenbank auch, wenn Sie sich mit Ihrem eigenen Benutzeraccount an den PCs anmelden.

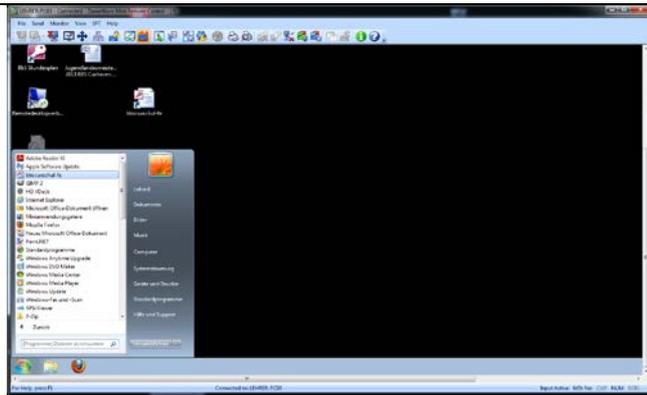


Abb. 1

2. Ist die Datenbank geöffnet, erscheint folgende Maske (vgl. Abb. 1):

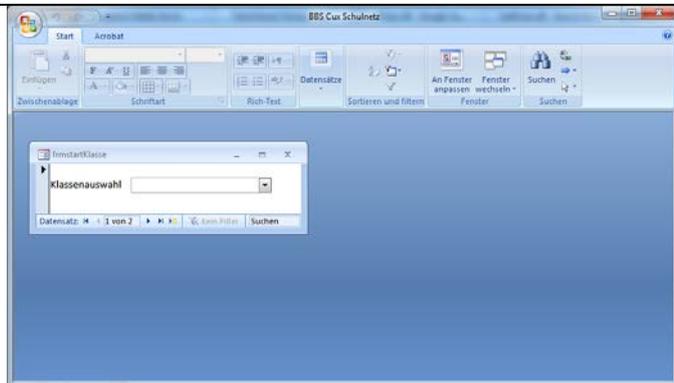


Abb. 2

3. Im Auswahlfeld, kann die Klasse ausgewählt werden (vgl. Abb. 2).

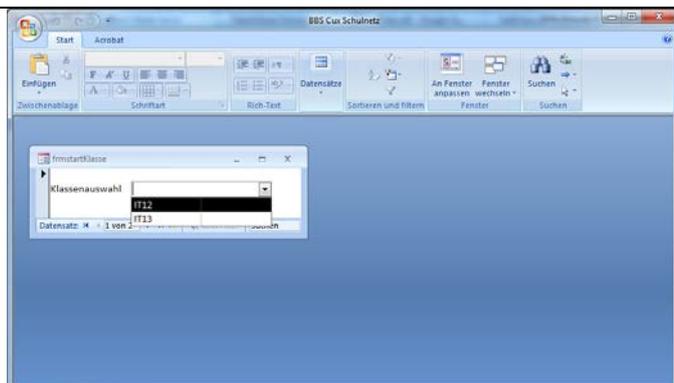


Abb. 3

4. Ist die Klasse ausgewählt, wird automatisch das folgende Fenster angezeigt (vgl. Abb. 3). Wird auf den Button oben rechts geklickt, öffnet sich die Klasseneinträge in Berichtsform, die aufbereitet ausgedrückt werden können (vgl. Abb. 3.2).

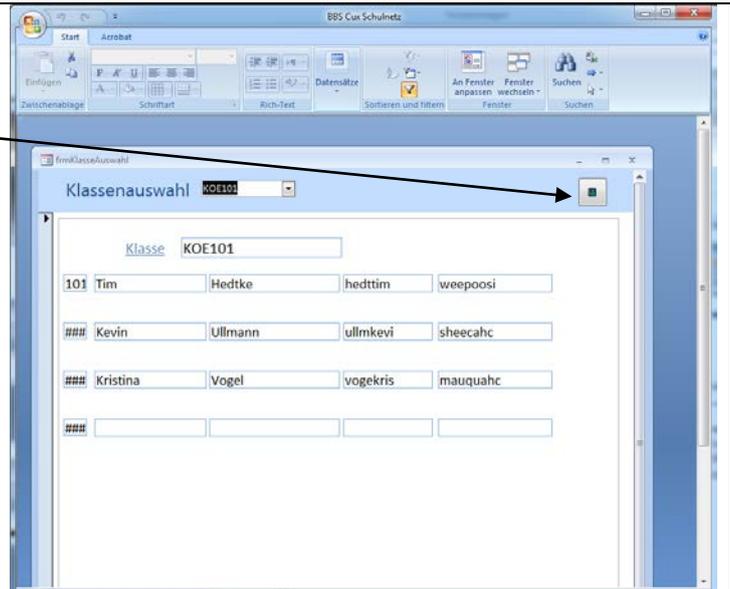


Abb. 4.1

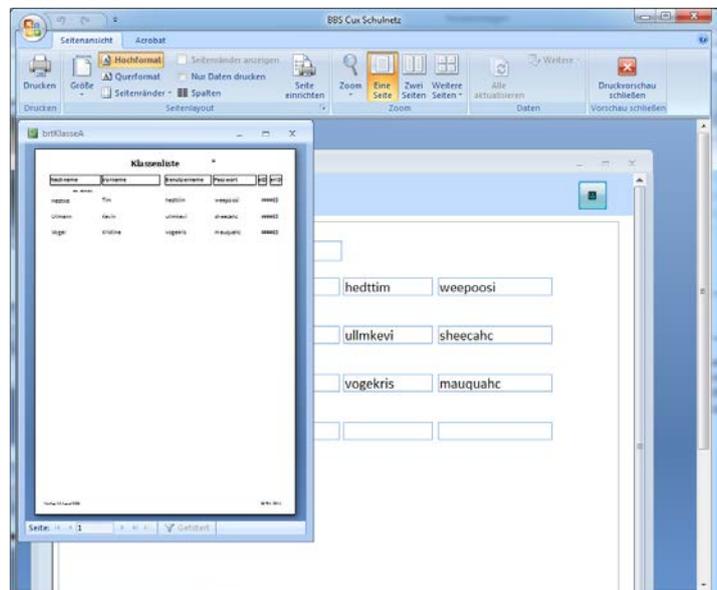


Abb. 4.2

Hinweis: Wenn Sie sich mit Ihrem Benutzer an den PCs angemeldet haben, kann es sein, dass beim Öffnen der Datenbank im oberen Teil eine Sicherheitswarnung erscheint. Wenn die Meldung erscheint, klicken Sie bitte auf den Button „Optionen“. Im sich öffnenden Fenster aktivieren Sie bitte den Eintrag „Diesen Inhalt aktivieren“ und bestätigen die Eingabe mit OK.

Prüfungskonten

1. Allgemeines

- 1.1. Jede LK erhält 30 Prüfungskonten.
- 1.2. Die Lehrkraft erreicht die Prüfungskonten über das Netzlaufwerk P.
- 1.3. In diesem Netzlaufwerk befindet sich zunächst sein Prüfungsgruppenordner. Dieser Name setzt sich aus „PR“ und dem Benutzernamen des Lehrers zusammen. Heißt ein Benutzer z.B. „Max Mustermann“ ist sein Benutzername „mustmax“. Sein Prüfungsordner heißt demnach „prmustmax“.
- 1.4. Die Prüfungskonten setzen sich aus dem Prüfungsordner und einer fortlaufenden Zahl von 01-30 zusammen. In unserem Beispiel heißt das, dass die Konten von „prmustmax01-prmustmax30“ gehen.
- 1.5. Jedes Prüfungskonto hat im Prüfungsordner einen Ordner. Der Name ist gleich dem Prüfungskonto. Jedes Prüfungskonto hat nur auf „seinen“ Ordner Zugriff. Die LK hat auf alle Prüfungsordner Zugriff. Der Prüfungsordner wird bei dem Prüfungskonto mit dem Laufwerk P verbunden. Die Prüfungskonten sehen unter dem Laufwerk P, wie die LK unter dem Laufwerk P den Prüfungsgruppenordner. In unserem Beispiel wäre das „prmustmax“. Öffnen die Prüfungskonten diesen, sehen sie aber nur „ihren“ Prüfungsordner – also Benutzer „prmustmax02“ sieht nur den Ordner „prmustmax02“. Die LK sieht aber alle seine Ordner.
- 1.6. So hat die LK die Möglichkeit vor der Klausur, Daten in die Ordner zu stellen oder auch, die einzelnen Daten zu kopieren.
- 1.7. Auf das persönliche Laufwerk Z der LK liegt ein Ordner „Script“. Bitte ändern Sie nichts in diesem Ordner. In diesem Ordner liegen unter Anderem Scripte (vgl. Abb. 7.1). Diese Scripte funktionieren nur auf Windows 7 PCs und auch nur an den Lehrerpcs in den EDV-Klassenräumen. Mit Hilfe der Scripte können die Prüfungskonten aktiviert und deaktiviert werden. Außerdem gibt es ein Script zum Löschen der Ordnerinhalte der Prüfungskonten und zum Kopieren von Dateien in den Prüfungsordner. Auf die einzelnen Scripte wird im Folgenden näher drauf eingegangen.

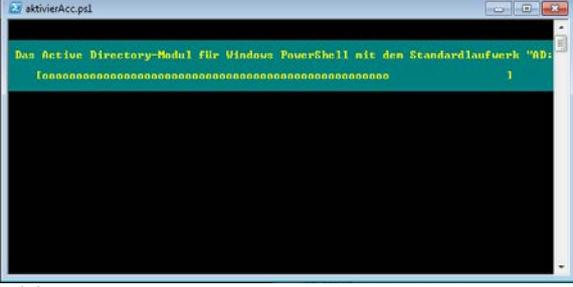
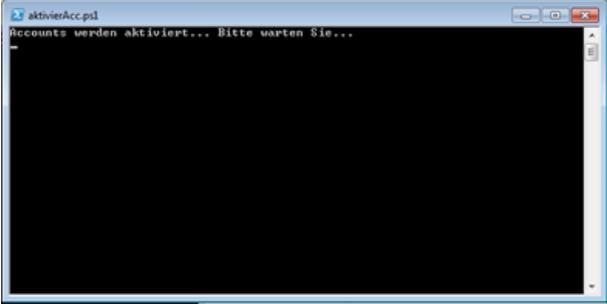
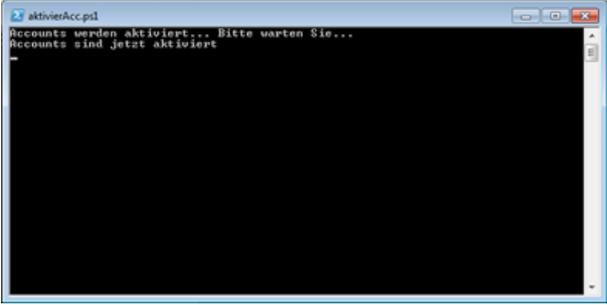
 aktivierAcc.ps1	20.08.2013 07:34	Verknüpfung	1 KB
 deaktivierAcc.ps1	30.08.2013 12:59	Verknüpfung	1 KB
 KopierInhalt.ps1	24.09.2013 12:20	Verknüpfung	1 KB
 loeschInhalt.ps1	24.09.2013 11:36	Verknüpfung	1 KB
 output.txt	24.09.2013 13:15	Textdokument	58 KB
 output2.txt	24.09.2013 13:16	Textdokument	47 KB

Abb. 7.1

- 1.8. Die Prüfungskonten haben keinen Internetzugriff.

2. Umgang mit den Scripten

2.1. Prüfungskonten aktivieren

<p>2.1.1. Starten Sie das Script <i>aktivierAcc.ps1</i> mit einem Doppelklick. Sie sehen zunächst eine Meldung (vgl. Abb. 2.1.1.).</p>	 <p>Abb. 2.1.1</p>
<p>2.1.2. Es erscheint dann eine Meldung, dass die Prüfungskonten jetzt aktiviert werden (vgl. Abb. 2.1.2.).</p>	 <p>Abb. 2.1.2.</p>
<p>2.1.3. Wurden die Befehle ausgeführt, erscheint die Meldung, dass die Accounts aktiviert wurden (vgl. Abb. 2.1.3). Das Fenster schließt automatisch. Die Schüler können sich jetzt mit den Anmeldedaten anmelden.</p>	 <p>Abb. 2.1.3</p>

2.2. Prüfungskonten deaktivieren

2.2.1. Zum Deaktivieren klicken Sie doppelt auf deaktivierAcc.ps1. Zunächst sehen Sie eine Meldung (vgl. Abb. 2.2.1.).

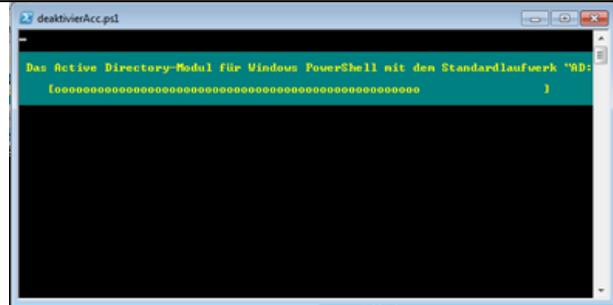


Abb. 2.2.1.

2.2.2. Es erscheint dann die Meldung, dass Prüfungskonten deaktiviert werden (vgl. Abb. 2.2.2.)



Abb. 2.2.2.

2.2.3. Sind die Konten deaktiviert, erscheint die Meldung laut Abb. 2.2.3. Das Fenster schließt automatisch. Die Konten sind nun deaktiviert. Somit haben die Schüler keinen Zugriff auf die Daten, Sie als Lehrer können aber über Ihr Laufwerk P: immer noch auf die Daten zugreifen.

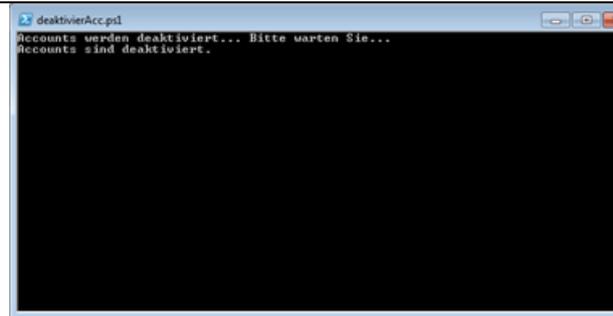
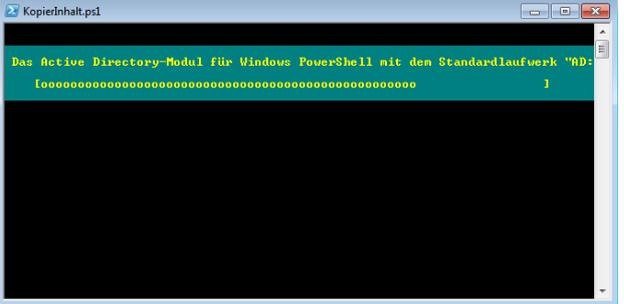
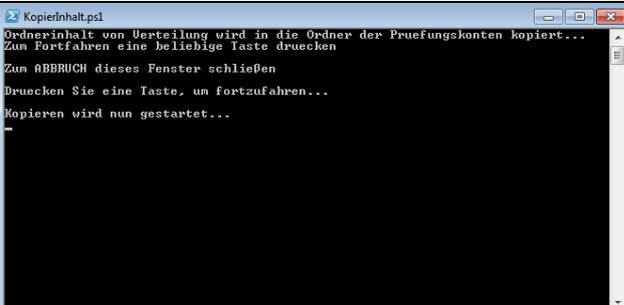
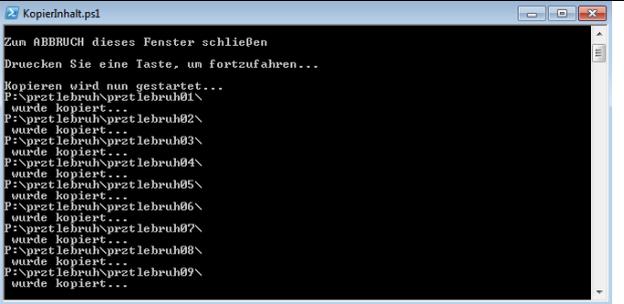


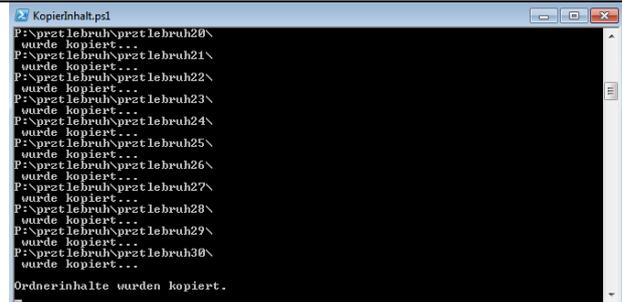
Abb. 2.2.3.

2.3. Prüfungsordner automatisch Daten kopieren

Unter Ihrem Laufwerk P: gibt es einen Ordner „Verteilung“. Wenn Sie das Script *Kopierinhalt.ps1* auführen, wird der Inhalt vom Ordner „Verteilung“ in jeden Ihrer Prüfungsordner kopiert.

<p>2.3.1. Starten Sie den Kopiervorgang mit einem Doppelklick auf <i>Kopierinhalt.ps1</i>. Es erscheint eine Meldung (vgl. Abb. 2.3.1.).</p>	 <p>Abb. 2.3.1</p>
<p>2.3.2. Es erscheint eine Meldung, dass der Ordnerinhalt von Verteilung in die Ordner der Pruefungsordner kopiert werden soll (vgl. Abb. 2.3.2.). Zum Fortfahren müssen Sie allerdings eine beliebige Taste auf der Tastatur drücken. Möchten Sie das Script doch abbrechen, schließen Sie das Fenster mit einem Klick auf das X rechts oben am Fenster.</p>	 <p>Abb. 2.3.2</p>
<p>2.3.3. Haben Sie mit einem Tastaturdruck das Fortführen bestätigt, erscheint eine Meldung, dass das Kopieren gestartet wird (vgl. Abb. 2.3.3.).</p>	 <p>Abb. 2.3.3</p>
<p>2.3.4. Das Script listet im Folgenden die Ordner auf (vgl. Abb. 2.3.4).</p>	 <p>Abb. 2.3.4</p>

2.3.5. Zum Schluss erscheint die Meldung, dass der Ordnerinhalt kopiert wurde (vgl. Abb. 2.3.5.). Das Fenster schließt automatisch.

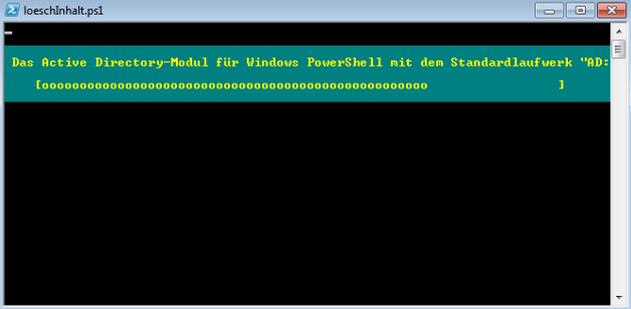
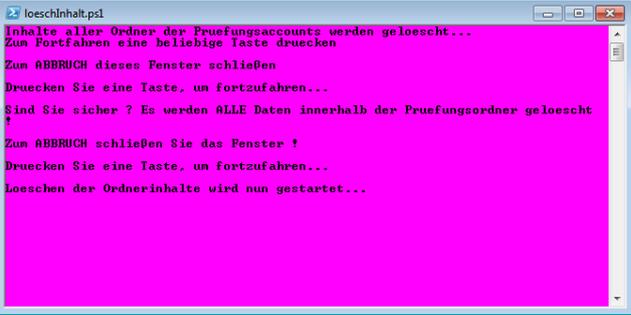
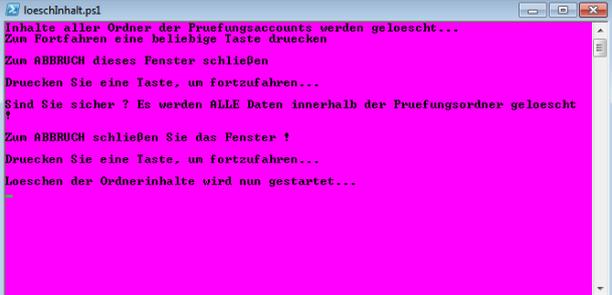


```
Kopierinhalt.ps1
P:\ppzt\lehruh\ppzt\lehruh20\
wurde kopiert...
P:\ppzt\lehruh\ppzt\lehruh21\
wurde kopiert...
P:\ppzt\lehruh\ppzt\lehruh22\
wurde kopiert...
P:\ppzt\lehruh\ppzt\lehruh23\
wurde kopiert...
P:\ppzt\lehruh\ppzt\lehruh24\
wurde kopiert...
P:\ppzt\lehruh\ppzt\lehruh25\
wurde kopiert...
P:\ppzt\lehruh\ppzt\lehruh26\
wurde kopiert...
P:\ppzt\lehruh\ppzt\lehruh27\
wurde kopiert...
P:\ppzt\lehruh\ppzt\lehruh28\
wurde kopiert...
P:\ppzt\lehruh\ppzt\lehruh29\
wurde kopiert...
P:\ppzt\lehruh\ppzt\lehruh30\
wurde kopiert...
Ordnerinhalte wurden kopiert.
```

Abb. 2.3.5

2.4. Inhalt der Prüfungsordner löschen

Möchten Sie beispielsweise vor einer neuen Klausur, die bisherigen Ordnerinhalte der Prüfungskonten löschen, können Sie dies mit dem Script loeschInhalt.ps1 machen. Aber ACHTUNG: Dadurch werden alle Inhalte innerhalb Ihrer Prüfungsordner der Prüfungsaccounts gelöscht !

<p>2.4.1. Mit einem Doppelklick auf loeschInhalt.ps1 starten Sie den Löschvorgang. Es erscheint die Meldung in Abb. 2.4.1.</p>	 <p>Abb. 2.4.1</p>
<p>2.4.2. Dann erscheint eine Meldung, dass die Ordnerinhalte der Prüfungsaccounts gelöscht werden können. Zum Abbrechen des Vorgangs schließen Sie bitte das Fenster mit einem Klick auf das X rechts oben in der Ecke des Fensters. Möchten Sie das Script fortfahren, drücken Sie auf eine beliebige Taste auf der Tastatur. (vgl. Abb. 2.4.2)</p>	 <p>Abb. 2.4.2</p>
<p>2.4.3. Haben Sie das Script mit einer beliebigen Taste bestätigt, folgt zur Sicherheit noch eine Abfrage. Sie haben noch mal die Möglichkeit den Löschvorgang durch Schließen des Fensters abbrechen. Möchten Sie fortfahren, drücken Sie eine beliebige Taste auf der Tastatur (vgl. Abb. 2.4.3)</p>	 <p>Abb. 2.4.3</p>
<p>2.4.4. Haben Sie auch diese Meldung mit einem Tastendruck bestätigt, folgt die Meldung, dass der Löschvorgang nun beginnt (vgl. Abb. 2.4.4.).</p>	 <p>Abb. 2.4.4</p>

2.4.5. Während des Löschvorgangs zeigt die Ausgabe an, welchen Ordnerinhalt gerade gelöscht wird (vgl. Abb. 2.4.5.)

```
P:\przt lebruh\przt lebruh04\*
wird gelöscht...
P:\przt lebruh\przt lebruh05\*
wird gelöscht...
P:\przt lebruh\przt lebruh06\*
wird gelöscht...
P:\przt lebruh\przt lebruh07\*
wird gelöscht...
P:\przt lebruh\przt lebruh08\*
wird gelöscht...
P:\przt lebruh\przt lebruh09\*
wird gelöscht...
P:\przt lebruh\przt lebruh10\*
wird gelöscht...
P:\przt lebruh\przt lebruh11\*
wird gelöscht...
P:\przt lebruh\przt lebruh12\*
wird gelöscht...
P:\przt lebruh\przt lebruh13\*
wird gelöscht...
P:\przt lebruh\przt lebruh14\*
wird gelöscht...
P:\przt lebruh\przt lebruh15\*
wird gelöscht...
```

Abb. 2.4.5

2.4.6. Zum Schluss kommt die Ausgabe, dass die Ordnerinhalte gelöscht wurden (vgl. Abb. 2.4.6). Das Fenster schließt automatisch.

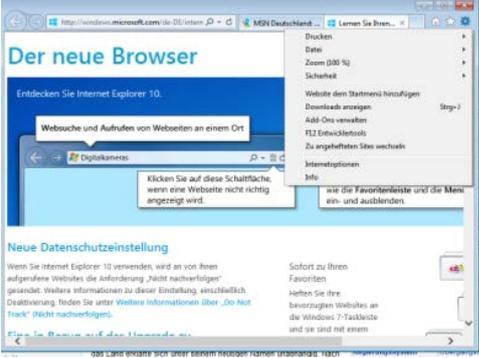
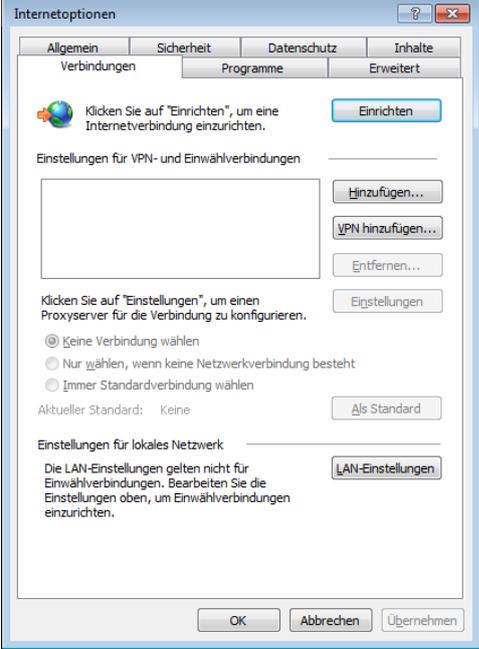
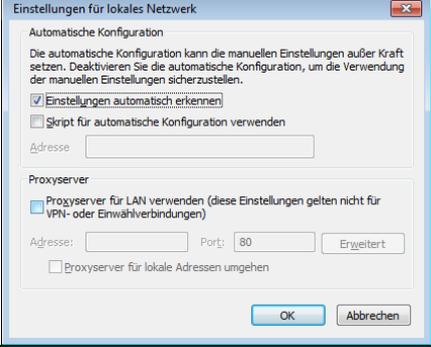
```
P:\przt lebruh\przt lebruh20\*
wird gelöscht...
P:\przt lebruh\przt lebruh21\*
wird gelöscht...
P:\przt lebruh\przt lebruh22\*
wird gelöscht...
P:\przt lebruh\przt lebruh23\*
wird gelöscht...
P:\przt lebruh\przt lebruh24\*
wird gelöscht...
P:\przt lebruh\przt lebruh25\*
wird gelöscht...
P:\przt lebruh\przt lebruh26\*
wird gelöscht...
P:\przt lebruh\przt lebruh27\*
wird gelöscht...
P:\przt lebruh\przt lebruh28\*
wird gelöscht...
P:\przt lebruh\przt lebruh29\*
wird gelöscht...
P:\przt lebruh\przt lebruh30\*
wird gelöscht...
Ordnerinhalte wurden gelöscht.
```

Abb. 2.4.6

Info-Hinweis 10

Proxy-Einstellungen Schulnetz

Möchten Sie die Proxy Einstellungen am PC selber konfigurieren, können Sie dies am Beispiel vom Internet Explorer oder Mozilla Firefox folgendermaßen machen:

<p>Internet Explorer</p> <ol style="list-style-type: none"> 1. Im Internet Explorer klicken Sie rechts auf das Symbol, um weitere Einstellungen vorzunehmen. Es klappt ein Menü auf (vgl. Abb. 1). Dort klicken Sie auf den Eintrag Internetoptionen. 	 <p>Abb. 1</p>
<ol style="list-style-type: none"> 2. Im sich öffnenden Fenster „<i>Internetoptionen</i>“ klicken Sie auf die Registerkarte Verbindungen (vgl. Abb. 2). Dort klicken Sie auf den Button LAN-Einstellungen. 	 <p>Abb. 2</p>
<ol style="list-style-type: none"> 3. Im sich öffnenden Fenster „<i>Einstellungen für lokales Netzwerk</i>“ sollte der Haken bei <i>Einstellungen automatisch erkennen</i> aktiviert sein. Diese Einstellung hat sich bisher auch im Schulnetz als sehr gut erwiesen. Wenn der Haken also nicht aktiviert ist, aktivieren Sie diesen bitte. 	

Mozilla Firefox

4. Im Firefox klicken Sie in der Menüleiste **Firefox** auf die Einträge **Einstellungen/Einstellungen** (vgl. Abb. 4)

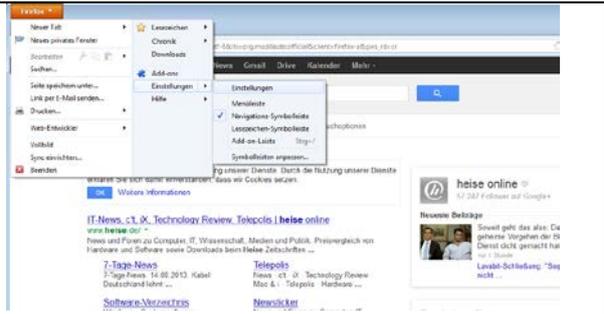


Abb. 4

5. Im sich öffnenden Fenster „*Einstellungen*“ klicken Sie auf den Registerreiter **Netzwerk** (vgl. Abb. 5). Im oberen Bereich unter **Verbindung** klicken Sie auf den Button **Einstellungen**.

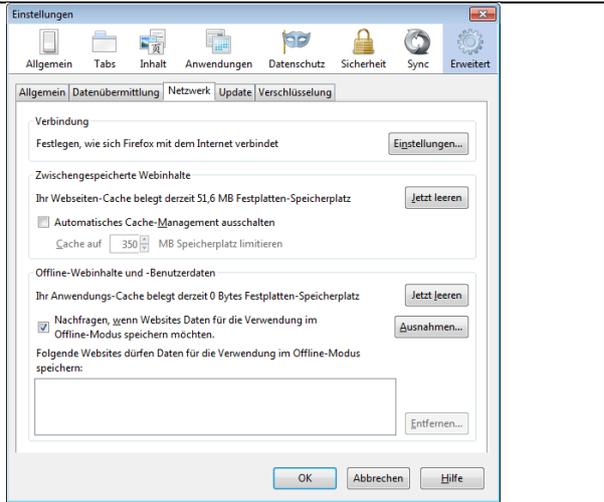


Abb. 5

6. Im sich öffnenden Fenster „*Verbindung-Einstellungen*“ hat sich im Schulnetz die Einstellung

Die Proxy-Einstellungen für dieses Netzwerk automatisch erkennen

bewährt. Ist dieser Eintrag nicht gesetzt, setzen Sie diesen bitte (vgl. Abb. 6.1).

Möchten Sie die Proxy-Einstellungen manuell vornehmen, richten Sie es gemäß Abb. 6.2 ein.

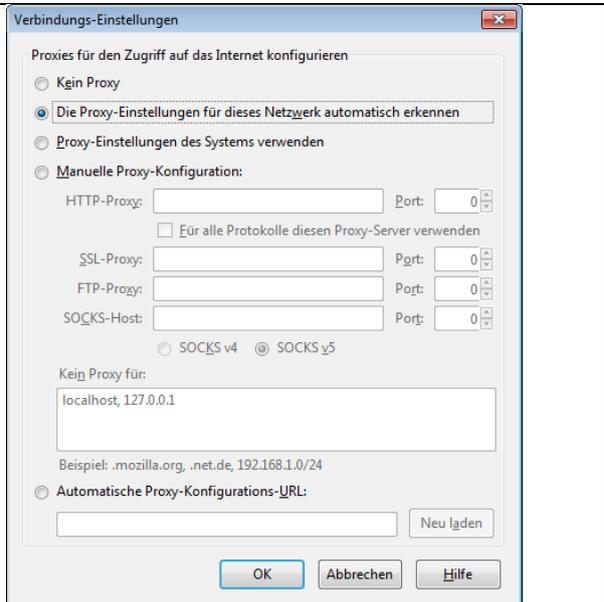


Abb. 6.1

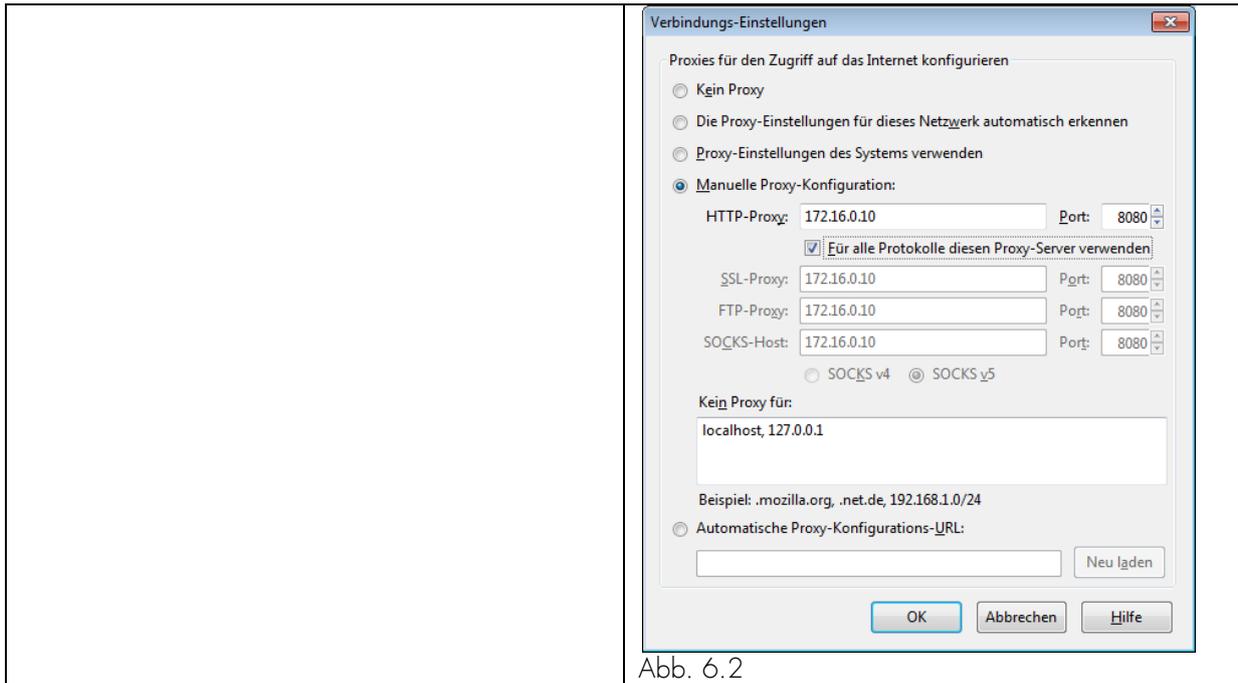


Abb. 6.2