Universität Bielefeld

➔ http://www.uni-bielefeld.de/informationssicherheit/

# Anleitung: Sicheres Verschlüsseln mit VeraCrypt

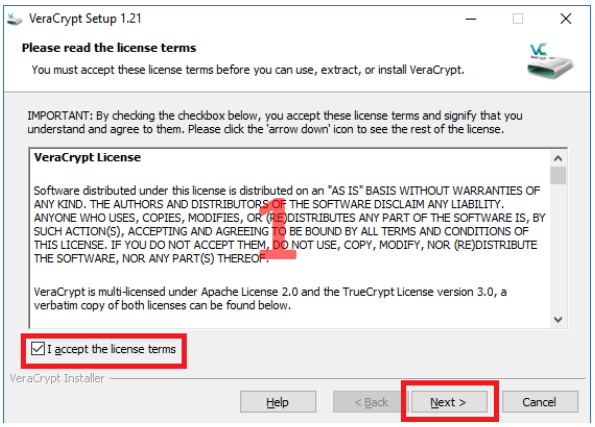
**VeraCrypt** ist eine Software zum Verschlüsseln von Containern/Volumes (entspricht passwortgeschützten Ordnern), Partitionen oder gesamter Laufwerke. Diese Anleitung zeigt Schritt für Schritt, wie ein verschlüsselter Container erstellt werden kann.

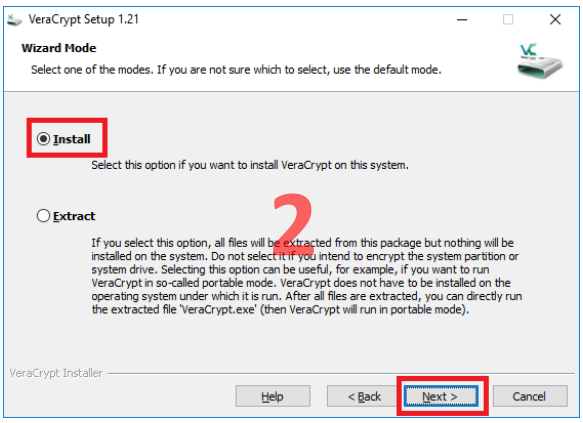
## 1. VeraCrypt herunterladen

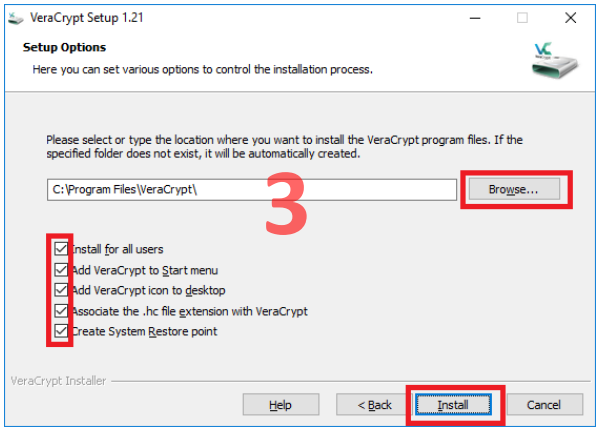
Laden Sie VeraCrypt von der Herstellerseite herunter: https://www.veracrypt.fr/en/Downloads.html

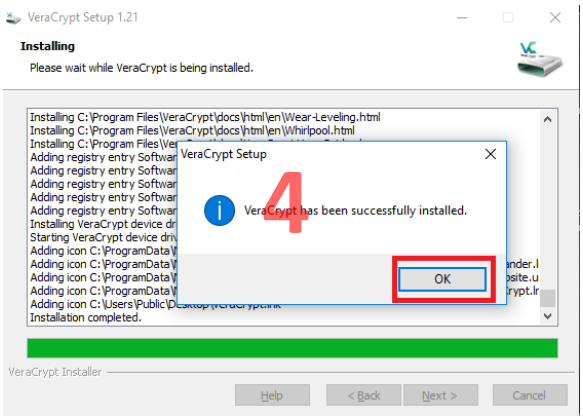
## 2. Installation

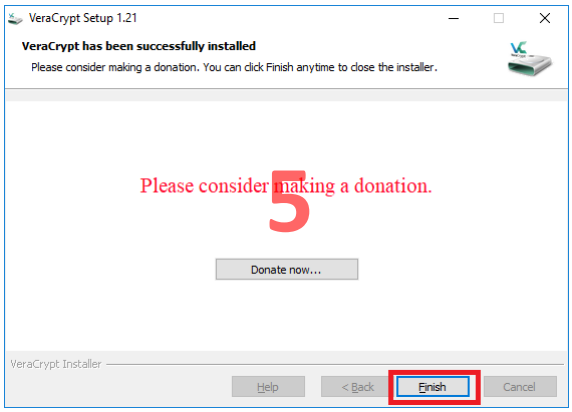
Installieren Sie VeraCrypt auf Ihrem Betriebssystem. Die anzuklickenden Bereiche sind rot-markiert.





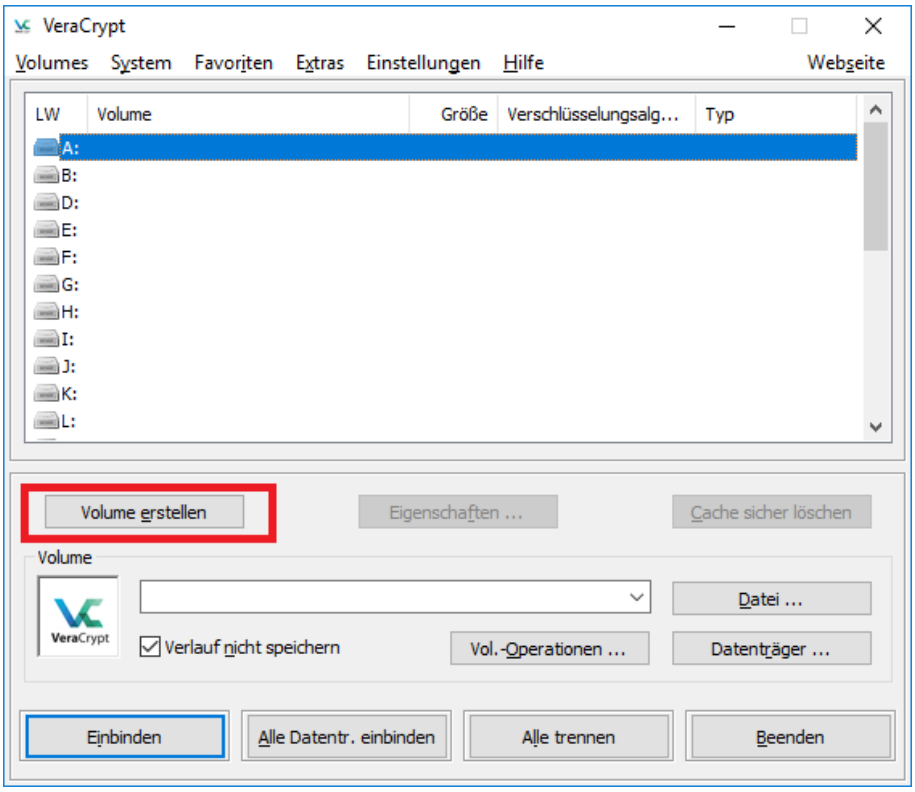




## 3. Sprache wählen

Starten Sie das Programm durch Doppelklicken der Desktop-Verknüpfung. Wählen Sie anschließend unter „Settings“ -> „Language“ „Deutsch“ als Standardsprache.

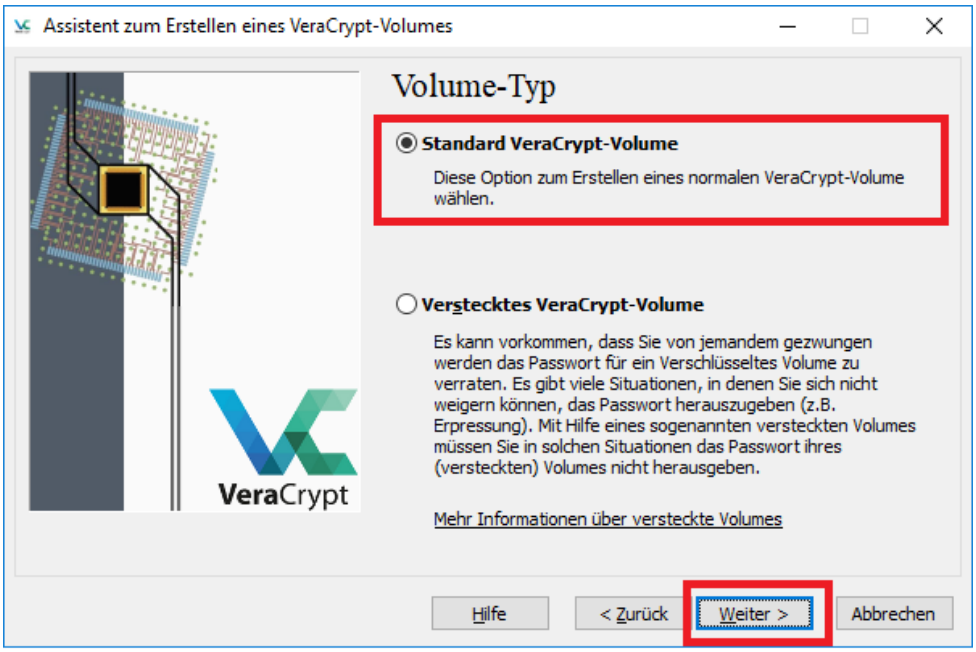
## 4. Container erstellen

**4.1.** Um eine verschlüsselte Container zu erstellen, klicken sie auf „Volume erstellen“.

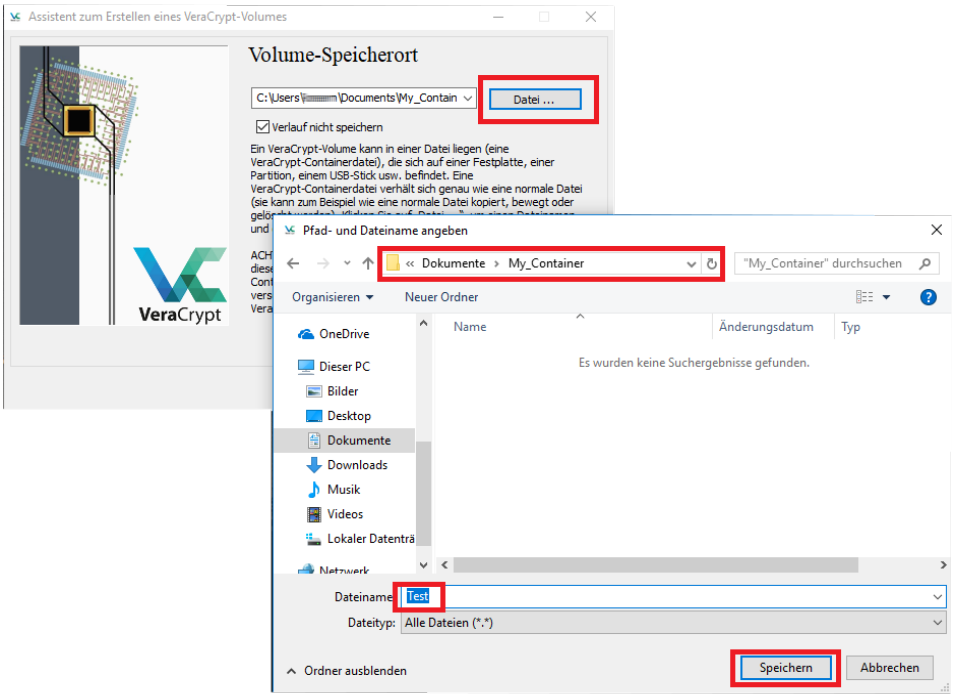


**4.2.** Wählen Sie „Eine verschlüsselte Containerdatei erstellen“ und klicken Sie auf „Weiter“.


**4.3.** Wählen Sie „Standard VeraCrypt-Volume erstellen“ und klicken Sie auf „Weiter“.

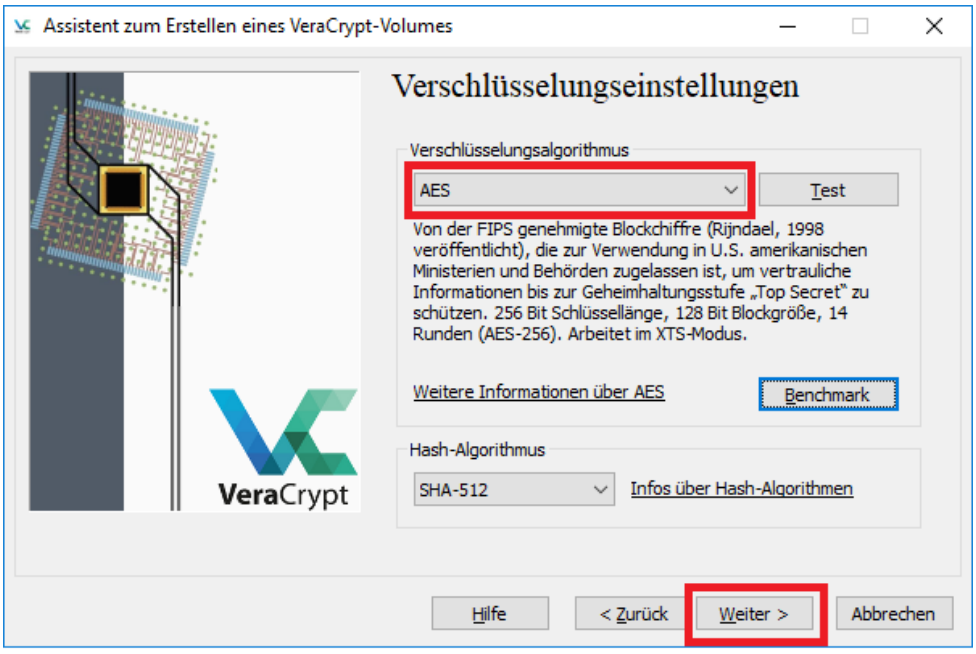


**4.4.** Wählen Sie einen Speicherort für Ihren Container. Der Beispiel-Container in dieser Anleitung befindet sich in C:\Users*Benutzername*\Documents\My_Container\ und trägt den Namen „Test“. Sie können natürlich einen beliebigen Namen und Speicherort wählen, solange Sie die entsprechenden Zugriffsrechte haben.

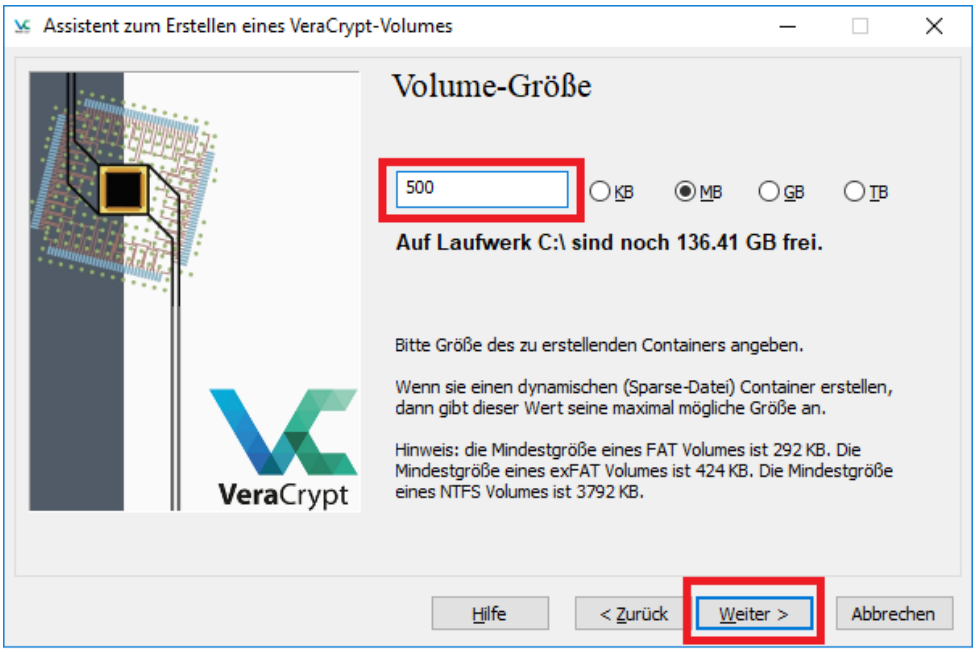



**WICHTIG:** Wenn Sie eine bereits existierende Datei wählen wird diese nicht verschlüsselt sondern gelöscht und durch die neue Datei ersetzt. Erstellen sie daher eine neue Datei, indem Sie einen neuen Dateinamen eingeben. Das Verschlüsseln von bereits existierenden Dateien wird im nächsten Kapitel erläutert.

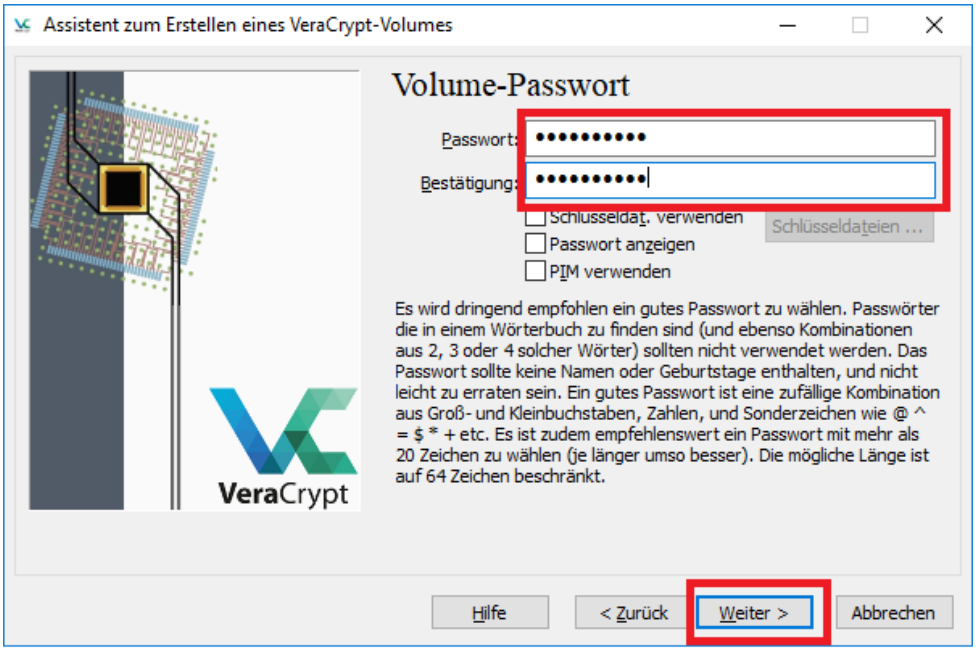
**4.5.** Wählen Sie im nächsten Fenster den Verschlüsselungsalgorithmus aus. Der voreingestellte AES-Algorithmus bietet die schnellste Ver- und Entschlüsselungsgeschwindigkeit, bei einer sehr hohen Sicherheit.



**4.6.** Geben Sie die Größe des künftigen Containers an, die für Ihr Vorhaben angemessen ist. Die Containergröße kann nach dem Erstellen des Containers nicht mehr verändert werden. In diesem Beispiel soll die Größe des Containers 500 MB betragen.



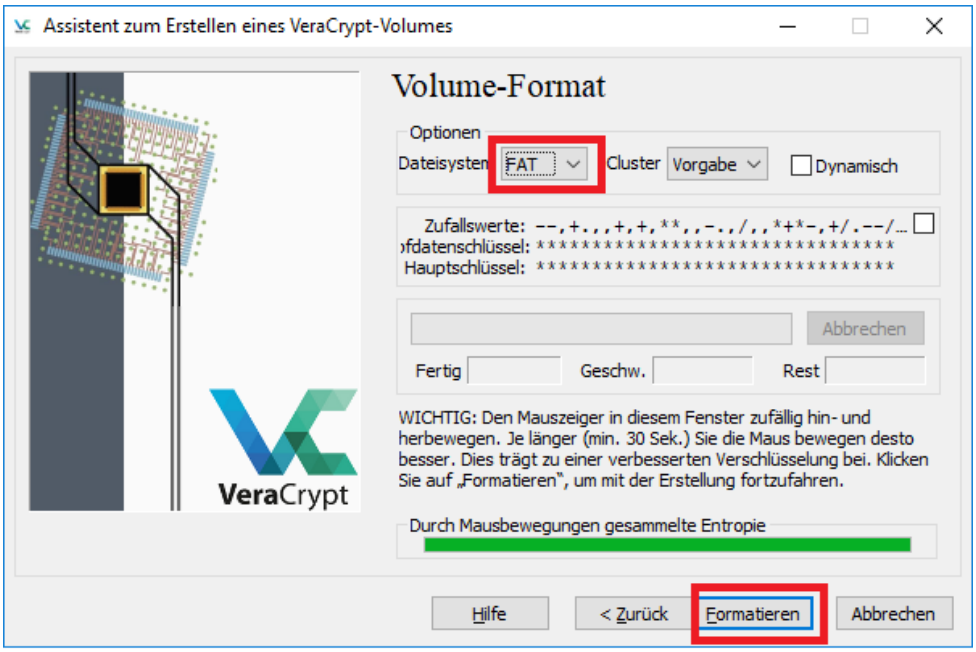

**4.7.** Geben Sie nun das Passwort für Ihren Container an. Ein sicheres Passwort sollte mindestens zehn Zeichen lang sein, Buchstaben, Zahlen und Sonderzeichen enthalten und nicht einfach zu erraten sein (keine Namen, Geburtsdaten etc.).




**4.8.** Wählen Sie ein Dateisystem. Falls Sie vorhaben, Dateien die größer als 4GB sind, zu verschlüsseln, wählen Sie NTFS. Ansonsten wählen Sie FAT.

Bewegen sie den Mauszeiger möglichst zufällig innerhalb des VeraCrypt Fensters für mindestens 30 Sekunden. Die Zufälligkeit der Mauszeigerbewegungen erhöht die kryptographische Stärke der Kodierungsschlüssel und somit auch die Verschlüsselungssicherheit.

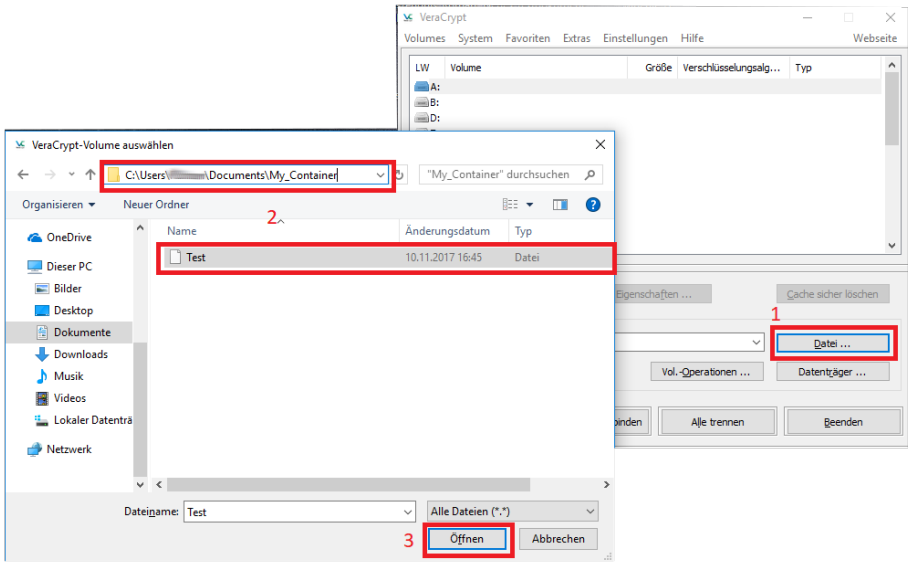
Klicken Sie auf „Formatieren“ um den Container zu erstellen und anschließend auf „Beenden“.




Herzlichen Glückwunsch, Sie haben erfolgreich einen verschlüsselten Container erstellt! Wie Sie diesen nutzen, erfahren Sie in dem folgenden Abschnitt.

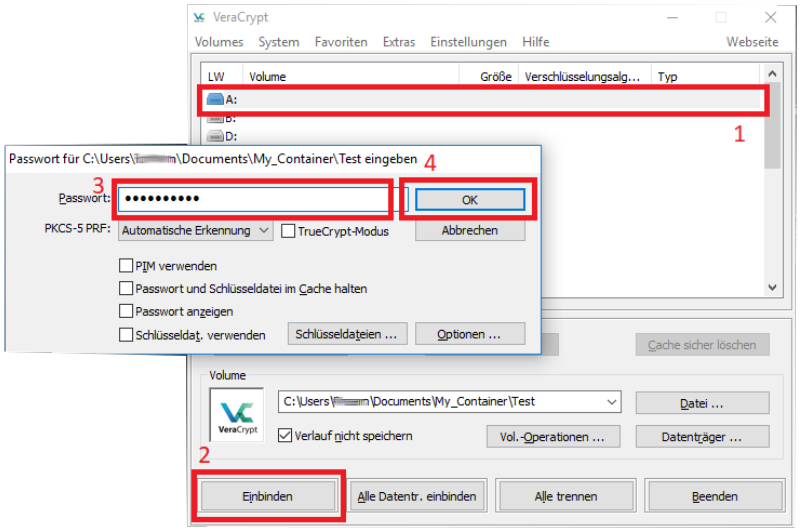
## 5. Container nutzen

**5.1.** Um die Container zu nutzen kehren Sie zurück zum VeraCrypt-Hauptfenster. Klicken Sie auf „Datei“ (1) und suchen Sie die Container-Datei unter dem Pfad aus, den Sie beim Erstellen des Containers angegeben haben (2). Klicken Sie auf die Container-Datei und anschließend auf Öffnen (3).

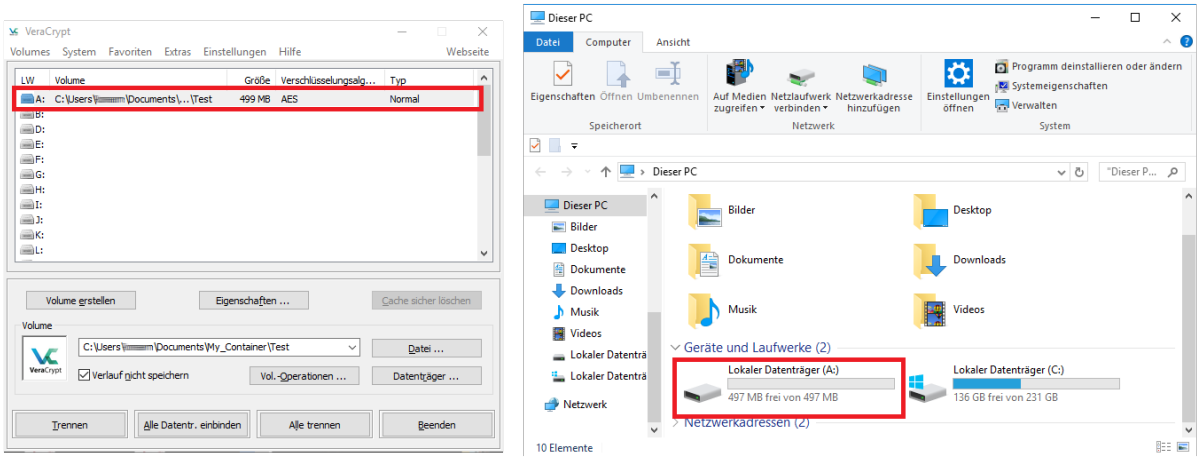



**5.2.** Wählen Sie nun einen beliebigen Laufwerksbuchstaben aus (1) (der Container erscheint als Laufwerk unter diesem Buchstaben) und klicken Sie anschließend auf „Einbinden“ (2).

Geben Sie im neuen Fenster Ihr Passwort (3) ein und klicken Sie anschließend auf „OK“ (4).

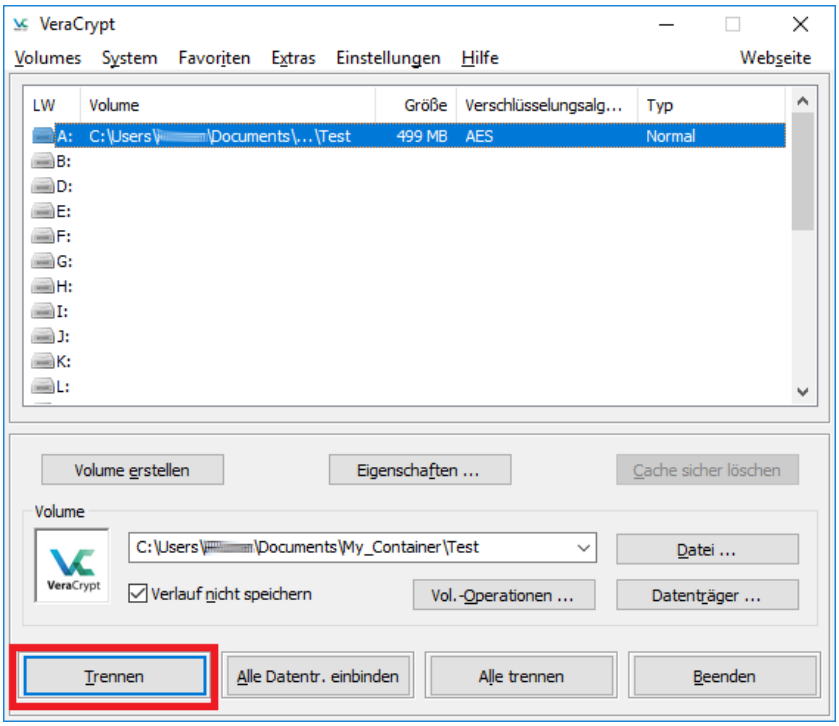



**5.3.** Sollte das Passwort korrekt sein, wird der Container entschlüsselt und eingebunden und kann wie ein ganz normaler Ordner bzw. Datenträger benutzt werden.




**5.4.** Beachten Sie bitte: Der Container besteht in dieser Form solange fort, bis Sie diese auswerfen oder Ihren Rechner neustarten. Bis zu diesem Zeitpunkt können die Daten für unbefugte Dritte zugänglich sein, sofern diese sich den Zugang zu Ihrem Rechner verschaffen. Dies ist besonders bei Dienstlaptops kritisch, weil diese seltener neugestartet werden und aufgrund ihrer geringen Größe leichter verloren gehen bzw. entwendet werden können. Es empfiehlt sich daher den Container nach jeder Arbeitssitzung wieder auszuwerfen.

Um den Container auszuwerfen klicken Sie auf „Trennen“.




Gratulation! Sie wissen nun wie man die Daten sicher verschlüsselt und können den Datendieben trotzen! ☺

Mehr Tipps und Informationen rund um die Informationssicherheit finden Sie unter: http://www.uni-bielefeld.de/informationssicherheit