# Dateien und Datenträger verschlüsseln


digitalcourage
Hochschulgruppe

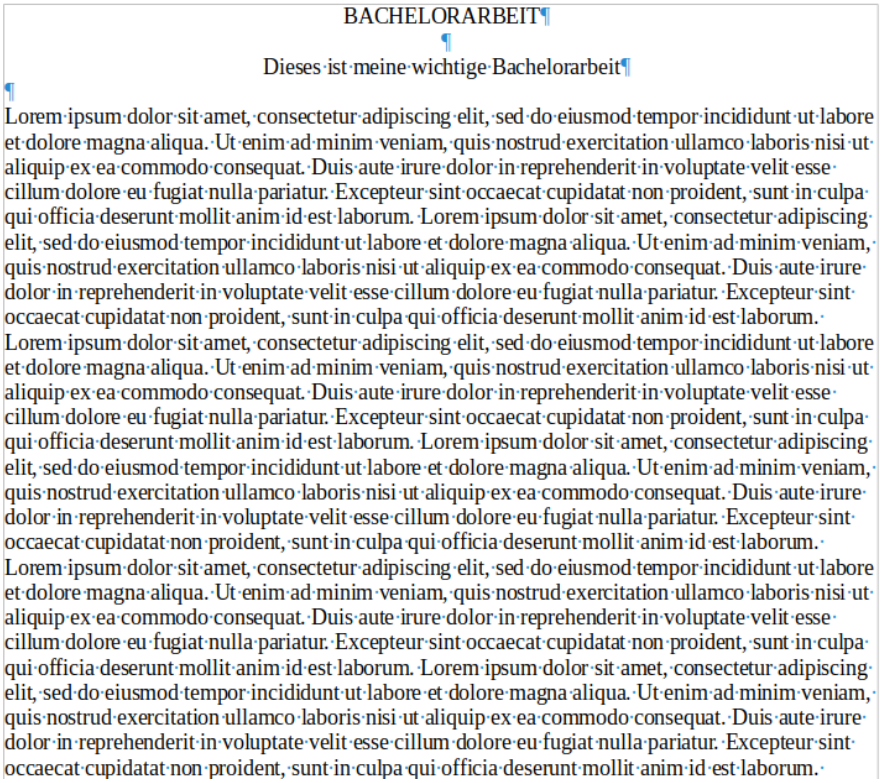
# Warum überhaupt verschlüsseln?

- Genereller Schutz sensibler und vertraulicher Daten
  - bei Verlust/Diebstahl des Laptops oder USB-Stick
  - alle, die personenbezogene Daten speichern
- DSGVO-konforme Verarbeitung von personenbezogenen Daten auf den eigenen Geräten oder im Homeoffice
- Weil Ihr ein Grundrecht auf digitale Privat- und Intimsphäre habt!
  - „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ – sogenanntes IT-Grundrecht
    - Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG

# Sinnbild: Tresor mit Kombination

# Was bedeutet "Verschlüsseln"?

- Beispiel: Ihr schreibt eure Bachelorarbeit. Nach jeder Änderung wird ein Backup der Abschlussarbeit auf einem USB-Stick gespeichert. Nun steht eine längere Zugfahrt zu den Eltern in die Heimat an. Während der Zugfahrt arbeitet ihr an eurer Arbeit weiter. Leider fällt euch euer USB-Stick beim aussteigen aus der Tasche. Problem: Jeder kann die Bachelorarbeit nun lesen und bearbeiten.

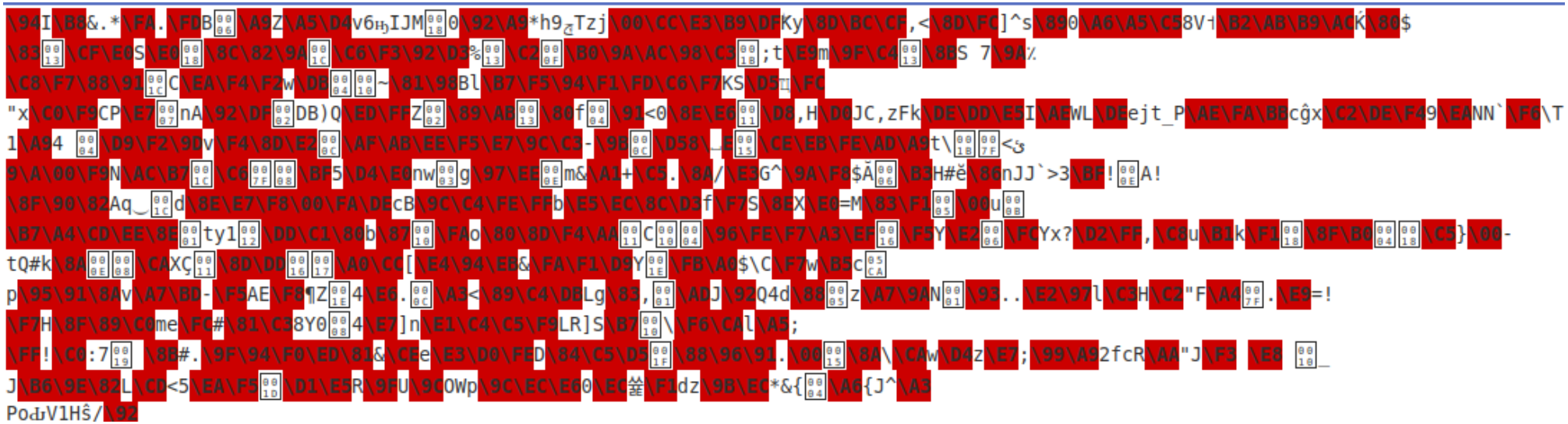


BACHELORARBEIT¶
¶
Dieses ist meine wichtige Bachelorarbeit¶
¶

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

# Fortsetzung: Was bedeutet "Verschlüsseln"?

- Doch keine Panik! Dank deinem verschlüsselten USB-Stick sehen andere, die die Datei öffnen wollen, nur folgendes Bild



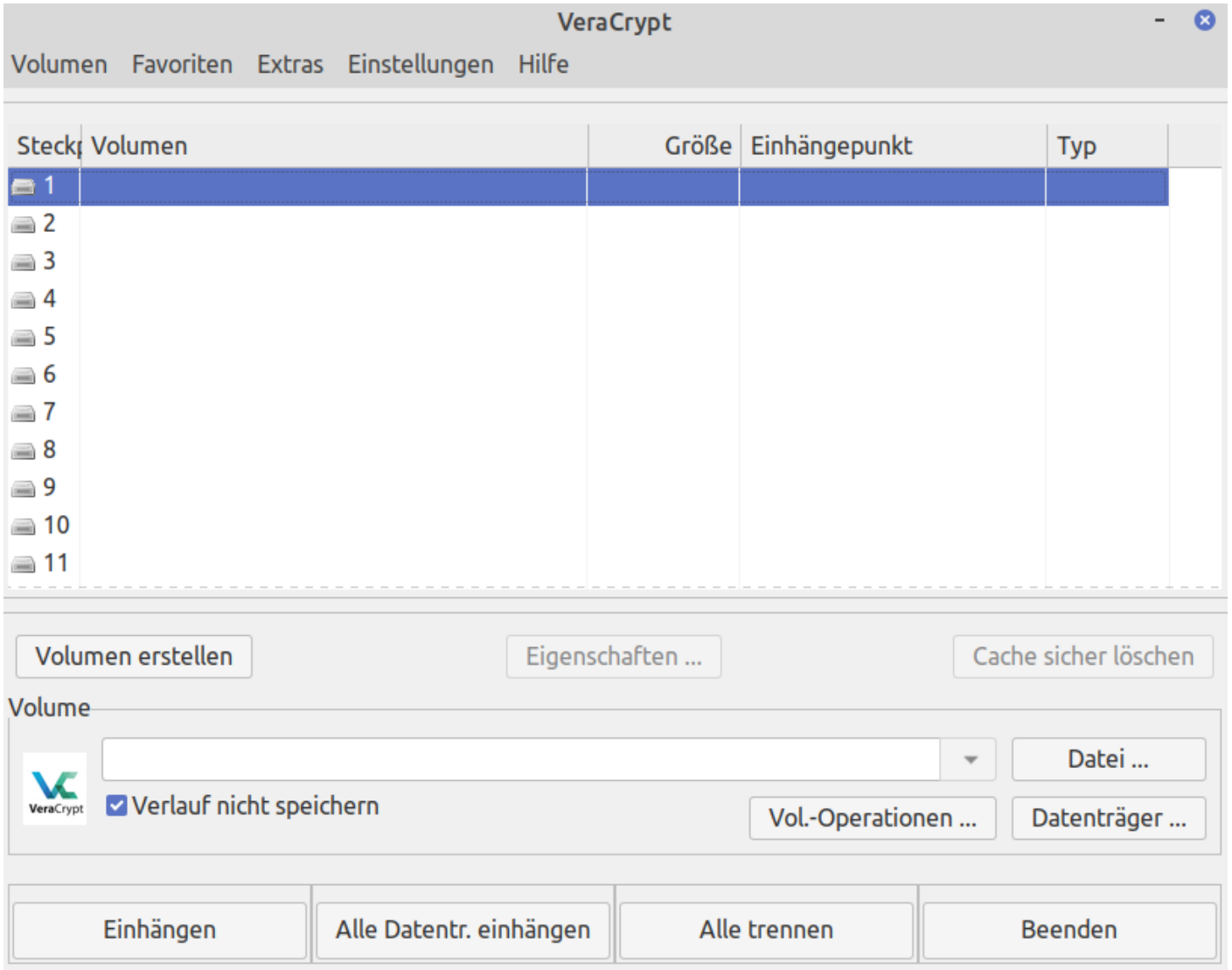
# Software-Auswahl: VeraCrypt

- Software zur Dateiverschlüsselung
- quelloffen und auf allen gängigen Plattformen verfügbar
- Freie Software
- Lösung für viele Anwendungsfälle

# Was kann ich mit VeraCrypt verschlüsseln?

- Container (verschlüsselte Ordner)
  - Dateien, die als Behälter für ein Dateisystem dienen, in dem andere Dateien abgespeichert werden können
- Datenträger:
  - Festplatten/SSDs
  - CDs, DVDs, … (Container)
  - USB-Sticks
- Systempartition
  - Achtung: vorher unbedingt ein Backup erstellen!

# Screenshot VeraCrypt



# VeraCrypt: Vorteile und Nachteile

## Vorteile

- quelloffen, freie Software
- nachvollziehbare Änderungen am Code
- plattformübergreifend
- auf USB-Stick transportierbar
- unabhängiger Audit

## Nachteile

- Komfortverlust
- Passwortverlust = Datenverlust

# Umgang mit VeraCrypt

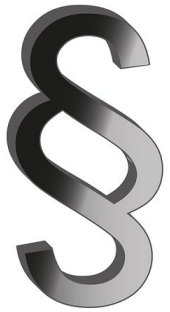
- Was will ich verschlüsseln?
- Starkes Passwort wählen
- Adminrechte notwendig
- Auf Ziel-PC muss ebenfalls VeraCrypt installiert/ausführbar sein
- Vorsicht bei fremden Geräten!
- Generell: Benutzerhandbuch zu VeraCrypt lesen
- **Größtes Sicherheitsrisiko ist fast immer der Nutzer!**

# Alternativen zu VeraCrypt

- **dm-crypt** (Teil des Linux-Kernels ab Version 2.6)
  - z.B. Ubuntu und Mint erlauben Systemverschlüsselung bei Installation
- **7-Zip**: freie Software, unterstützt AES256-Verschlüsselung
- Nicht vertrauenswürdig, da nicht quelloffen:
  - Windows: **BitLocker**
  - MacOS: **FileVault**
  - zahllose weitere kommerzielle Produkte

# Rechtliches

- Deutschland: Kein Zwang zur Herausgabe eines Passworts/Schlüssels bei möglicher Selbstbelastung
- Vorsicht im Ausland:
  - Großbritannien: Pflicht zur Herausgabe (→ RIPA), auch Beugehaft möglich!
  - USA: Ein- und Ausreise mit verschlüsselten Datenträgern problematisch



– Ende Datei-/Datenträgerverschlüsselung –