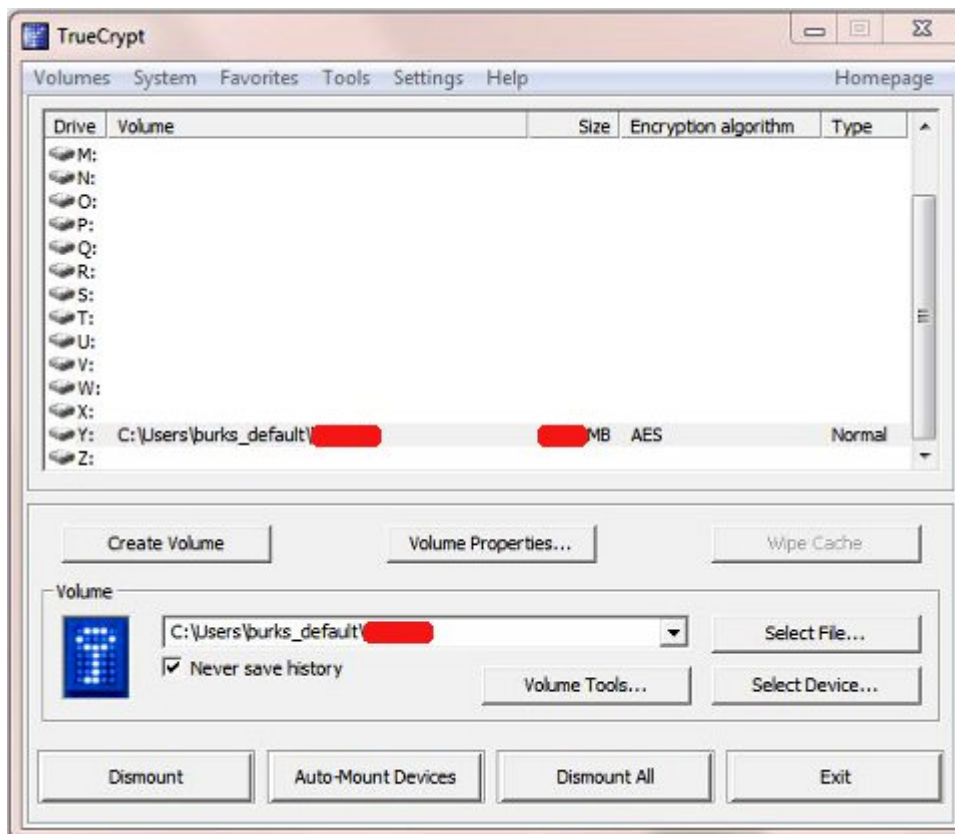


# Thunderbird und Truecrypt



Wie ich gestern schon sagte, habe ich nach der Neuinstallation eines meiner Rechner endlich konsequent auch meine digitale Korrespondenz vor den Augen derjenigen verborgen, die [Rechner beschlagnahmen](#), stehlen oder mit irgendwelchen Methoden durchsuchen wollten – gegen meinen Willen.

Für Laien und die, die das noch nicht gemacht haben, hier die Arbeitsschritte für einen Computer mit dem Betriebssystem [Windows 7 \(64 bit\)](#) und Thunderbird 14.0:

1. [Truecrypt](#) installieren. ([ausführliche Anleitung](#) mit Screenshots)
2. Truecrypt aufrufen und ein verschlüsseltes Laufwerk („container“) erzeugen (meines ist 1 Gigabyte groß – das sollte reichen).
3. Das E-Mail-Programm [Thunderbird](#) herunterladen, *aber noch nicht installieren*.
4. Das verschlüsselte Laufwerk öffnen („mounten“, vgl.

Screenshot oben) und die ausführbare Datei mit Thunderbird dort hineinschieben. Erst *dann* Thunderbird installieren und bei jeder Frage, wo es installiert werden soll, den geöffneten Truecrypt-Container (im Windows-Dateimanager „lokaler Datenträger“ genannt) angeben. Bei mir wäre das das verschlüsselte „Laufwerk“ Y. (vgl. den Screenshot unten)



Jetzt kommt der wichtige Arbeitsschritt, wenn ein E-Mail-Konto eingerichtet wird:

5. Bei den „Account Settings“ (Voreinstellungen des eigenen E-Mail-Accounts, *sorry, ich habe alles in Englisch*) und den dortigen Optionen („Server Settings“) muss der Dateipfad geändert werden („local directory“, vgl. Screenshot unten), so dass die eingehenden Mails innerhalb des verschlüsselten Truecrypt-Containers gespeichert werden.

Nicht vergessen: Um mit Thunderbird arbeiten zu können, muss jetzt natürlich immer erst das verschlüsselte Laufwerk geöffnet („gemounted“) werden.

Ab jetzt ist auf dem so abgesicherten Rechner gar kein E-Mail-Programm mehr zu sehen, auch die unverschlüsselten E-Mails sind verborgen. (Liebe Drehbuch-Autoren von Vorabend-Krimiserien und Tatorten: Da kann auch „die IT-Abteilung“ nichts machen, die bei euch immer zaubern soll, wenn es mit dem Passwort-Raten ausnahmsweise nicht klappt.)

Truecrypt ist nicht „knackbar“. Die Angriffsszenarien, die im

Wikipedia-Artikel geschildert werden, beziehen sich alle auf die Situation, dass das Passwort zum Öffnen eines Truecrypt-Containers dann abgegriffen werden könnte, wenn der Rechner eingeschaltet und das Laufwerk geöffnet ist oder man vergessen hat, es zu schließen („dismount“).

Und jetzt wieder einmal viel Spaß beim Offline- und „Online-Durchsuchen“.

The image shows two overlapping dialog boxes from a mail client. The top dialog, titled 'Server Settings', has a blue header bar. It contains the following fields: 'Server Type' set to 'IMAP Mail Server', 'Server Name' (redacted), 'Port' set to '143' (with 'Default: 143' next to it), and 'User Name' set to 'burks'. Below these is a 'Security Settings' section with 'Connection security' set to 'STARTTLS'. The bottom dialog, titled 'Message Storage', contains two unchecked checkboxes: 'Clean up ("Expunge") Inbox on Exit' and 'Empty Trash on Exit'. It also has a 'Local directory:' field with a redacted path and a 'Browse...' button. An 'Advanced...' button is located to the right of the checkboxes.

**Server Settings**

Server Type: IMAP Mail Server

Server Name: [REDACTED] Port: 143 Default: 143

User Name: burks

Security Settings

Connection security: STARTTLS

**Message Storage**

☐ Clean up ("Expunge") Inbox on Exit

☐ Empty Trash on Exit

Local directory: Y:\[REDACTED]

Advanced...

Browse...