

You gotta fight  
for your right  
to party



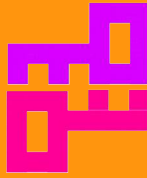
V 0. 150129 Cologne

Jochim Selzer

[jselzer@vorratsdatenspeicherung.de](mailto:jselzer@vorratsdatenspeicherung.de)

<https://cryptoparty.in/cryptopartykbn>

a57a 4e28 a59d 0385 d33d 6301 763d ce1b 65f4 c445



**It's my party  
and I crypt if I want to**

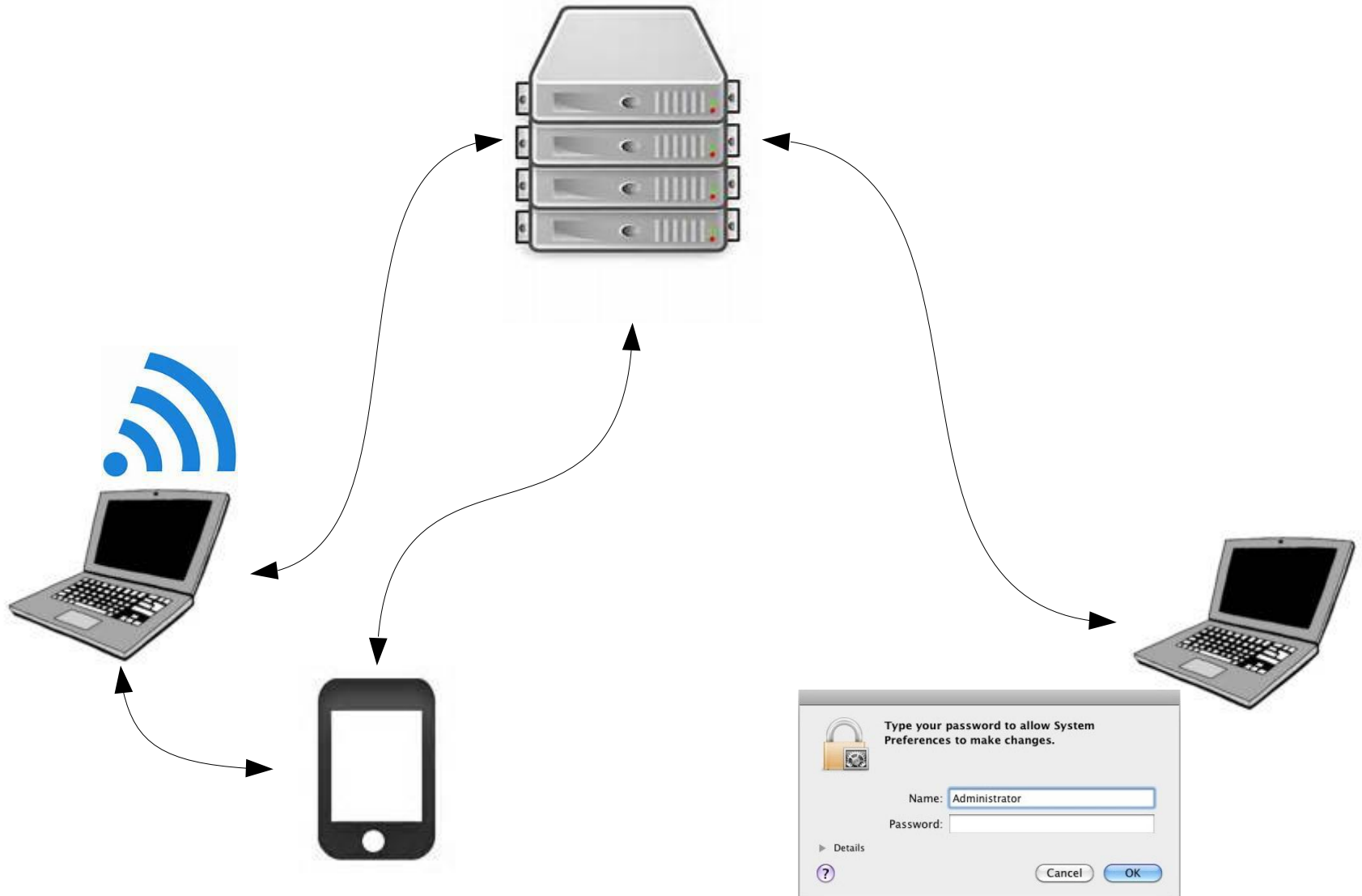
**Privatsphäre ist ein Grundrecht.  
Wir müssen es nicht begründen.  
Wir müssen es nicht entschuldigen.  
Wir müssen es einfordern und  
verteidigen.**

# Pleased to meet you

## Cryptoparty

- Digitaler Erste-Hilfe-Kurs
- Frei wie „freie Rede“
- Frei wie „Freibier“
- Überparteilich
- Unterwegs

Trouble, set me free



# Am I just paranoid?

# Am I just stoned?

- Mailverschlüsselung mit GnuPG
- Chatverschlüsselung mit OTR
- Datenträgerverschlüsselung mit TCnext
- Anonymisierung mit Tor
- Passwortverwaltung mit Keepass

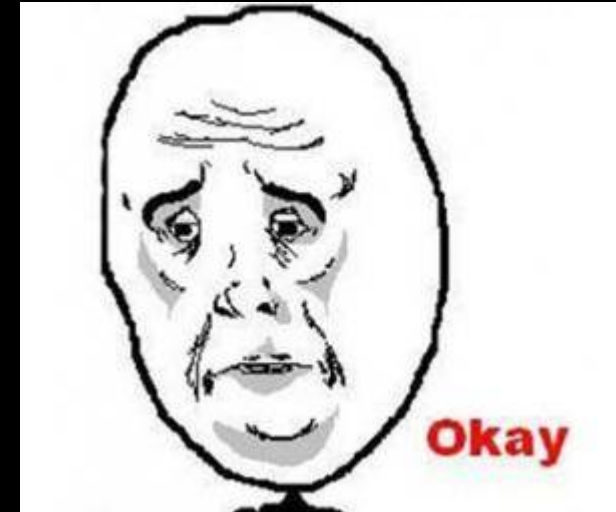
und reichlich neue Programme zum Ausprobieren

# Ende-zu-Ende- Verschlüsselung



# Remember Mama's golden rules

1. HTTPS benutzen
2. Mails verschlüsseln. Immer
3. Lokale Daten verschlüsseln
4. Viele und starke Passworte benutzen
5. Tracker im Browser blockieren
6. Persönlichkeit aufspalten
7. In offenen WLANs besonders vorsichtig sein
8. Software aktuell halten
9. Vor einer Installation zweimal nachdenken



Es kann keine perfekte Sicherheit geben.  
Sicherheit ist ein Vorgehen, kein Werkzeug.

# My baby just wrote me a letter

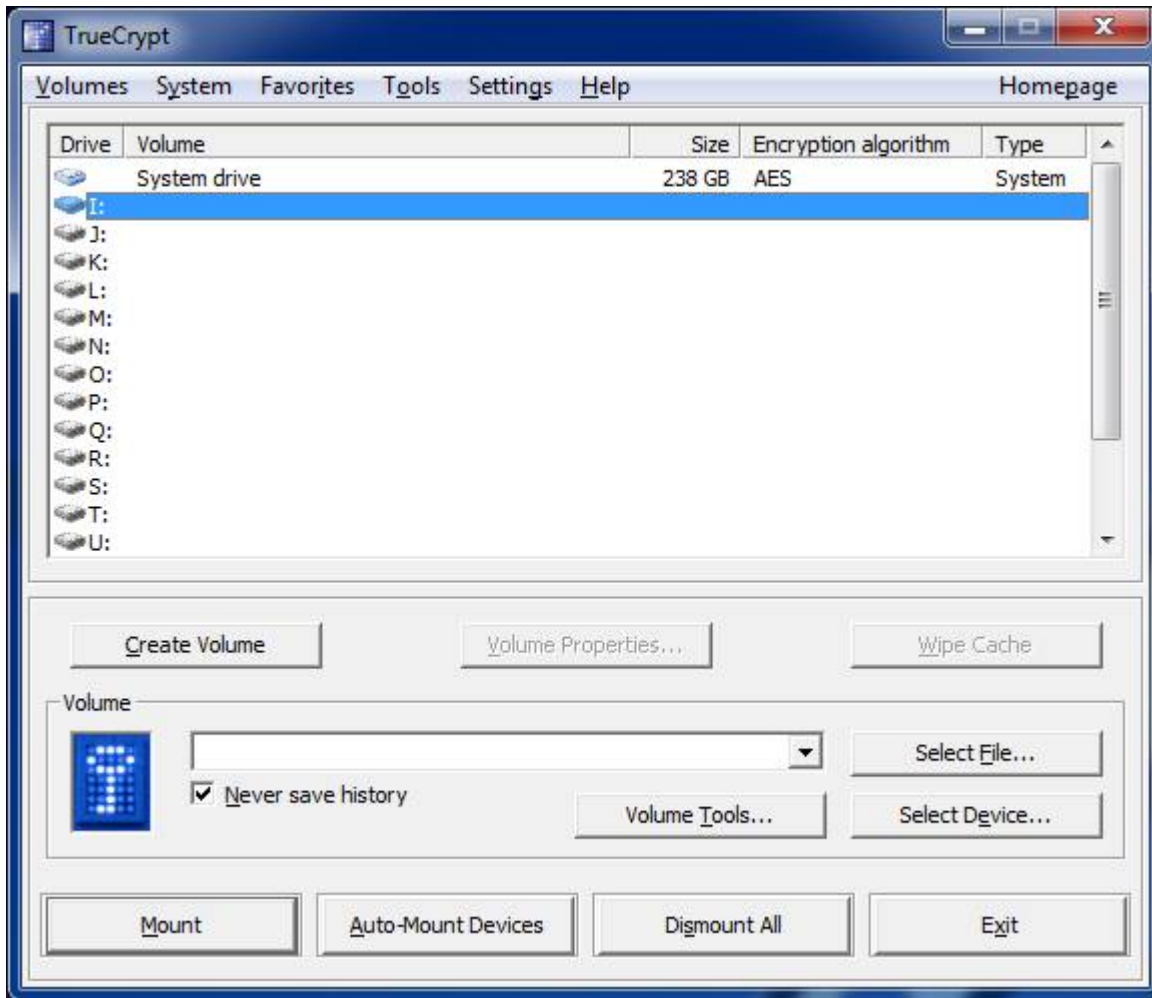
- <https://www.mozilla.org/thunderbird>
- <http://www.gpg4win.org/>
- <https://gpgtools.org/>
- <https://enigmail.mozdev.org>





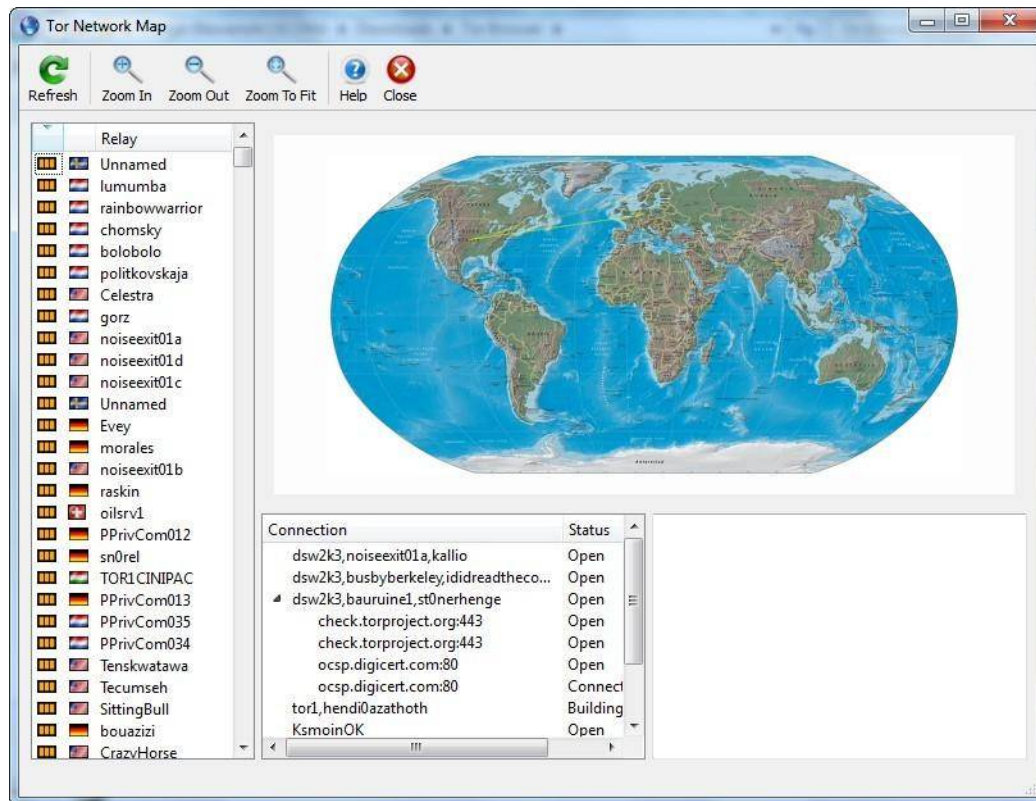
# You belong with me

<https://truecrypt.ch>



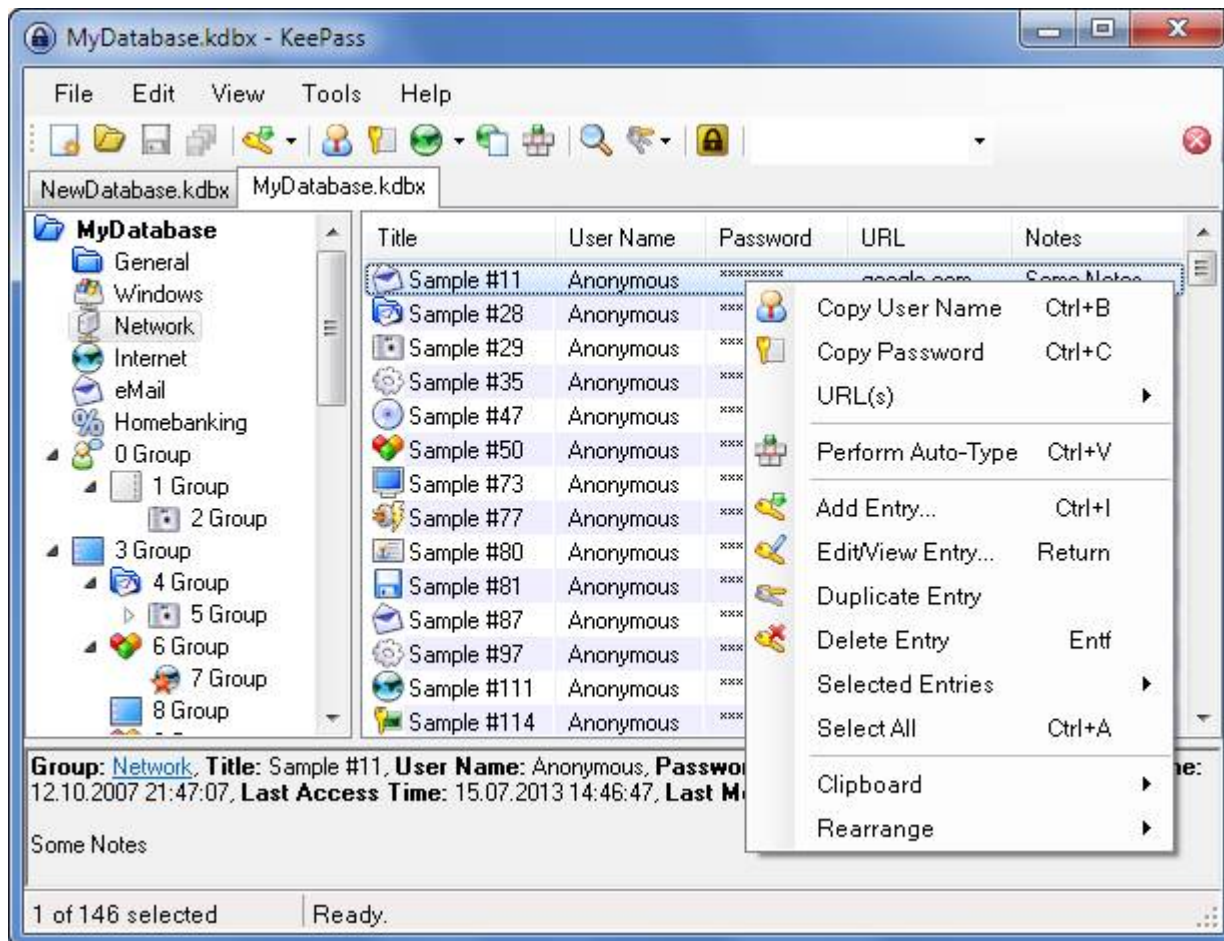
And it's hard to hold on  
to what you've found  
When what comes around  
always goes around

<https://www.torproject.org/>



# I can't remember

<http://keepass.info/>



# Automatic For The People

<https://tails.boum.org/>



**Tails**  
The Amnesic  
Incognito Live System



# Somewhere over the rainbow

- Skype-Ersatz <http://tox.im/>
- P2P-Messenger <https://pond.imperialviolet.org/>
- Anonymes-IM <http://www.bitmessage.org/>
- PGP im Browser <https://lavaboom.com/>
- Truecrypt-Nachfolger <http://veracrypt.codeplex.com/>
- Crypto-IM <https://www.cameonet.de/>
- Crypto-IM <https://www.peerio.com/>



# Never can say goodbye

<https://cryptoparty.in/cryptopartykbn>



**VUELVE  
SEGURAS TUS  
COMUNICACIONES  
Y DEJA A LA REINA  
DE CORAZONES  
CON TRAGEDIA**

**cryptopartycl**

**¿QUÉ HAREMOS?**  
Nos reuniremos para enseñar, compartir y aprender las herramientas esenciales para la supervivencia en la red, tales como PGP/GPG, Tor, OTR, TrueCrypt, etc. ¿Retención de datos? ¿Intercepción de mensajes? ¿Acoso?... HAGÁMOSLES LA PEGA MÁS DIFÍCIL QUE LA CHUCHA.

**¿CUÁNDO?**  
**28 SEP.**  
**20:00 HRS.**  
**CASA VOLNITZA**  
Vidaurre 1629,  
Santiago centro

**¿MÁS INFO?**  
[cryptoparty.org](https://cryptoparty.org)

**-----BEGIN PGP MESSAGE-----**  
VERSION: GnuPG V1.4.11 (GNU/LINUX)  
HqEMAZHQRRRVJ3VAQ//RDZNCZKQZYU9VIVAXALIHQ+Q3UTLOA  
HFPVDKZGMI/6YUUI8HYFLTUM6ZATVPRMVLWQC1TLXA2002ZY  
Zw9F+MEPSYNORDBPRQJXLJD/+NSE/TNBC8B4K06UAFHXTOPNDC  
GM27P3HNYERNYGFVC31DR3UCVT7ONNSLGVJKTED+NILAIYLBND  
TDXND38M1P00J79QK9FTBAKFLXAB7VNBCPSF85G

**-----BEGIN PGP MESSAGE-----**  
VERSION: GnuPG V2.0.18 (FREEBSD).  
DwHS+QDAUBU2M1SPCHBPAQVFRUXFIKKQAGOLYB5DAQSVEARGISH  
SMPV7VGRQRQSFQETORRZQKIBEXZX7M3ZXP93PVUE/F73VF73W2TV  
SQM1SDCTPRRVBOLIZEAKOZ69RGDAP2RKGBZOLM5YF5ZCWE6UG9VT  
CMMJ8Z+UTJ3B5UHFNVT+XQZw+SCJTSOPRULGCCXKUDBKUJIKGDZY  
BAQHSDLPEHLAPMLFPULOOKIEE/SPN2TQDHUC1EVH2L3UEZZMCMNR  
BHCKSLRNVFS8XGSA8C8MGUISHPKIP1FNEHKDKJTXBDE8BYLX0YD7

