Computer-Sicherheit/Praxis

anonymous

Linke Hochschulgruppe Stuttgart

12. März. 2009

Inhalt

Vortragsziele

Ziele

- Jeder kann E-Mails verschlüsseln
- Jeder weiss, wie man Daten verschlüsselt
- Jeder weiss, wie man Daten sicher löscht
- Jeder kennt grundlegende Verhaltensregeln im Netz

Was nicht behandelt wird

- juristisches

Motivation

- politische Kämpfe nehmen zu
- Zunehmen staatlicher Repression
- Überwachung ist etabliert
- Überwachung wird juristisch fundiert
- „Stasi 2.0“

Festplatten

Festplatten verschlüsseln

Festplatten verschlüsseln

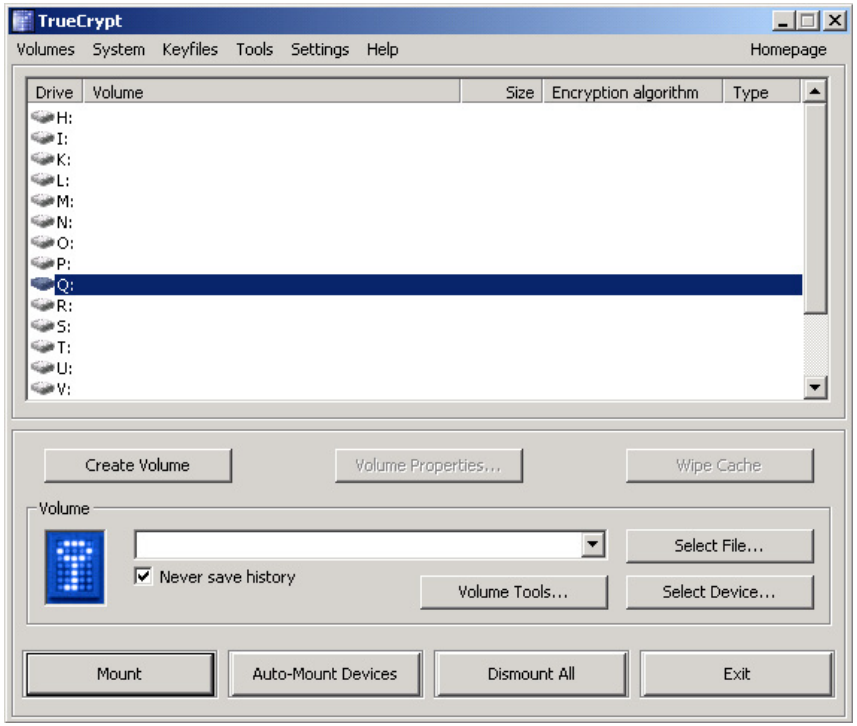
Festplatten verschlüsseln: TrueCrypt

- für Windows, Linux, Mac OS (ab 10.4)
- AES, Twofish, Serpent
- Open Source

Festplatten verschlüsseln: TrueCrypt

- Arbeitsmodi
  - Container
  - komplette Partition (auch Systempartition)
- Container
  - Volume
  - Hidden-Volume
- Traveller Mode
- http://www.truecrypt.org

Festplatten verschlüsseln: TrueCrypt



Create Volume Erzeugt neuen verschlüsselten Bereich

Select File Wählt Container aus

Mount Öffnet verschlüsselten Bereich zur Bearbeitung

Dismount Schließt verschlüsselten Bereich wieder

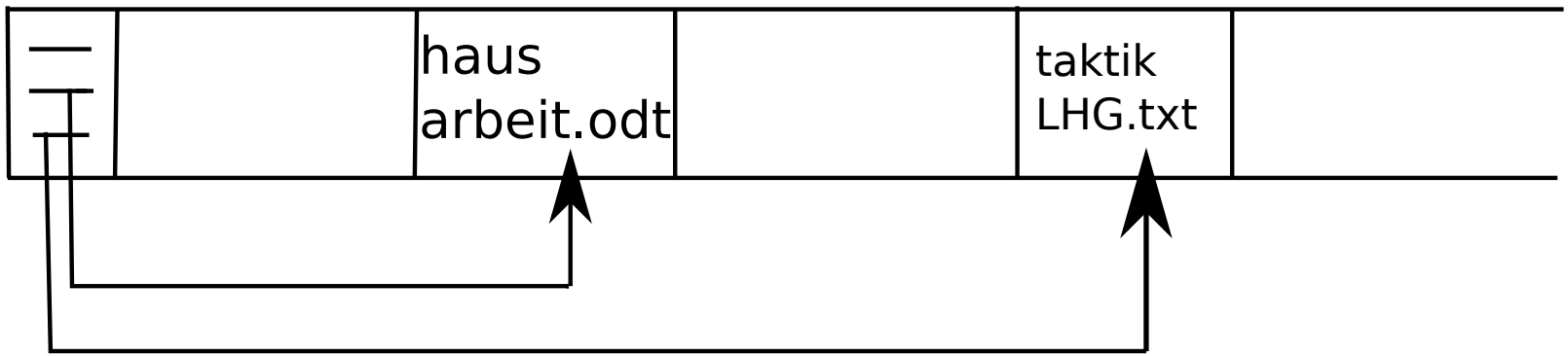
Festplatten verschlüsseln: TrueCrypt

Festplatten löschen

Festplatten löschen

Festplatten löschen

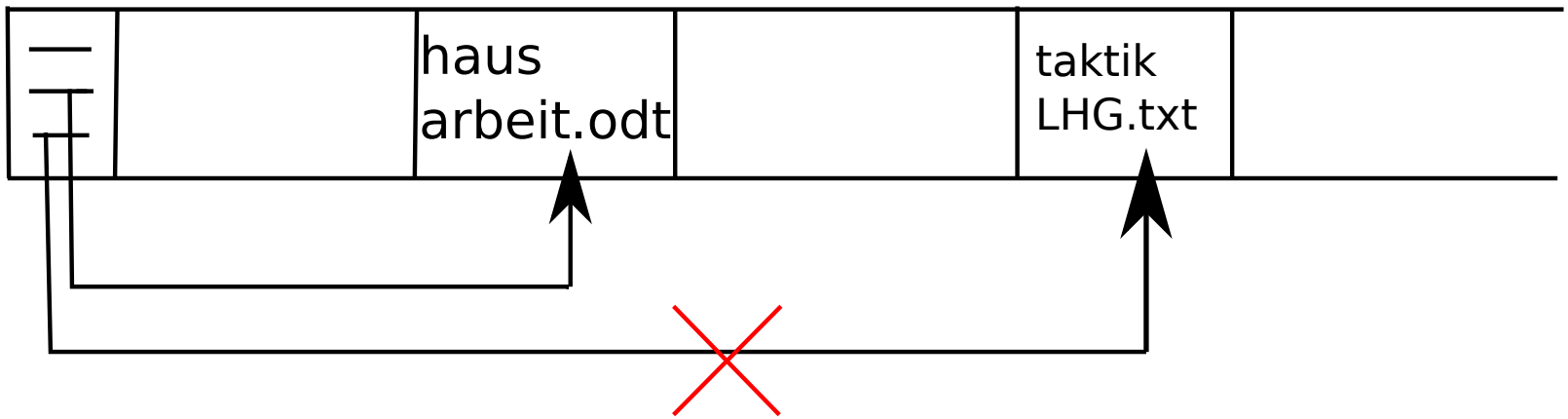
"Inhaltsverzeichnis"



Festplatte mit Daten

Festplatten löschen

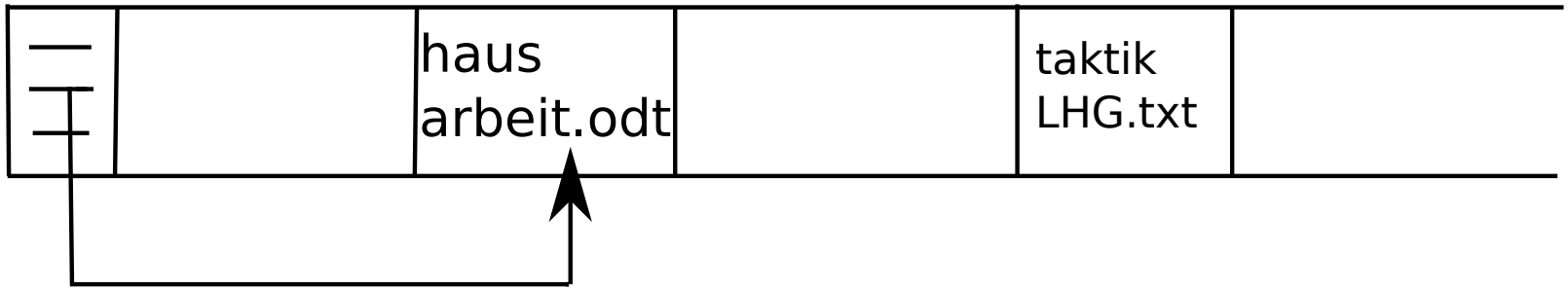
"Inhaltsverzeichnis"



"Datei löschen"

Festplatten löschen

"Inhaltsverzeichnis"



Problem: Nur „Link“wird gelöscht

Festplatten löschen

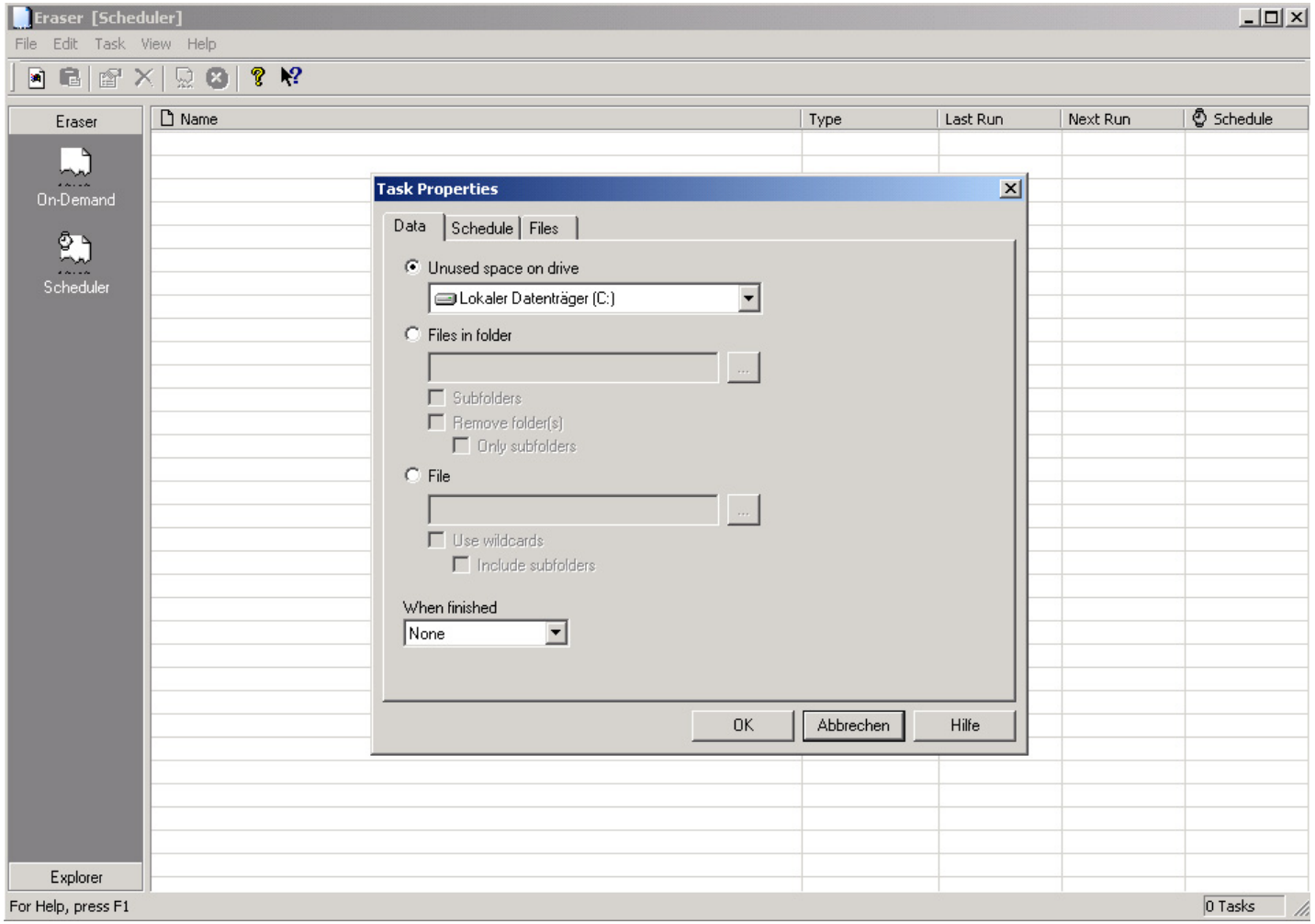
- Bereiche nach löschen nicht „frei“
- nur zum Überschreiben freigegeben
- Idee: Überschreibe „gelöschte“ Dateien mit Zufallswerten, mehrmals(!)

Festplatten löschen

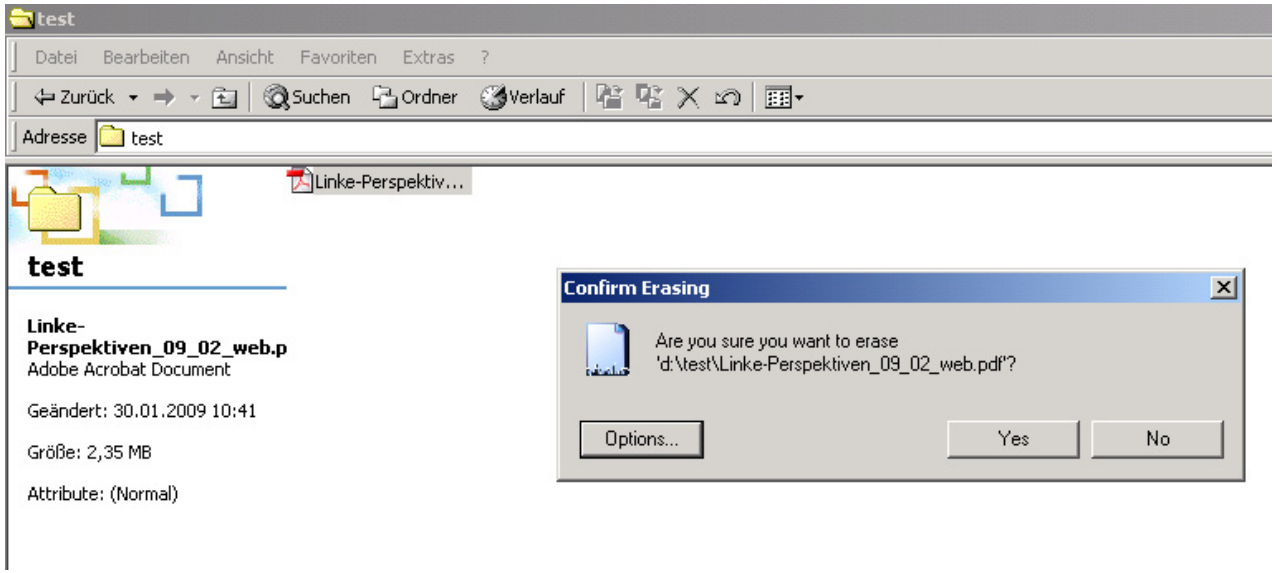
- Windows
  - Eraser http://www.heidi.ie
  - bcwipe http://www.jetico.com
- Linux
  - schon im System vorhanden
  - Befehl: `wipe [options] path1 path2 ... pathn`
- Mac
  - schon im System vorhanden
  - „Papierkorb sicher löschen“
  - Fesplattentools -> „Freien Speicherplatz überschreiben“
- Komplette Festplatte zerstören
  - Darik's Boot And Nuke
  - http://www.dban.org
  - läuft von bootfähiger CD

Festplatten löschen

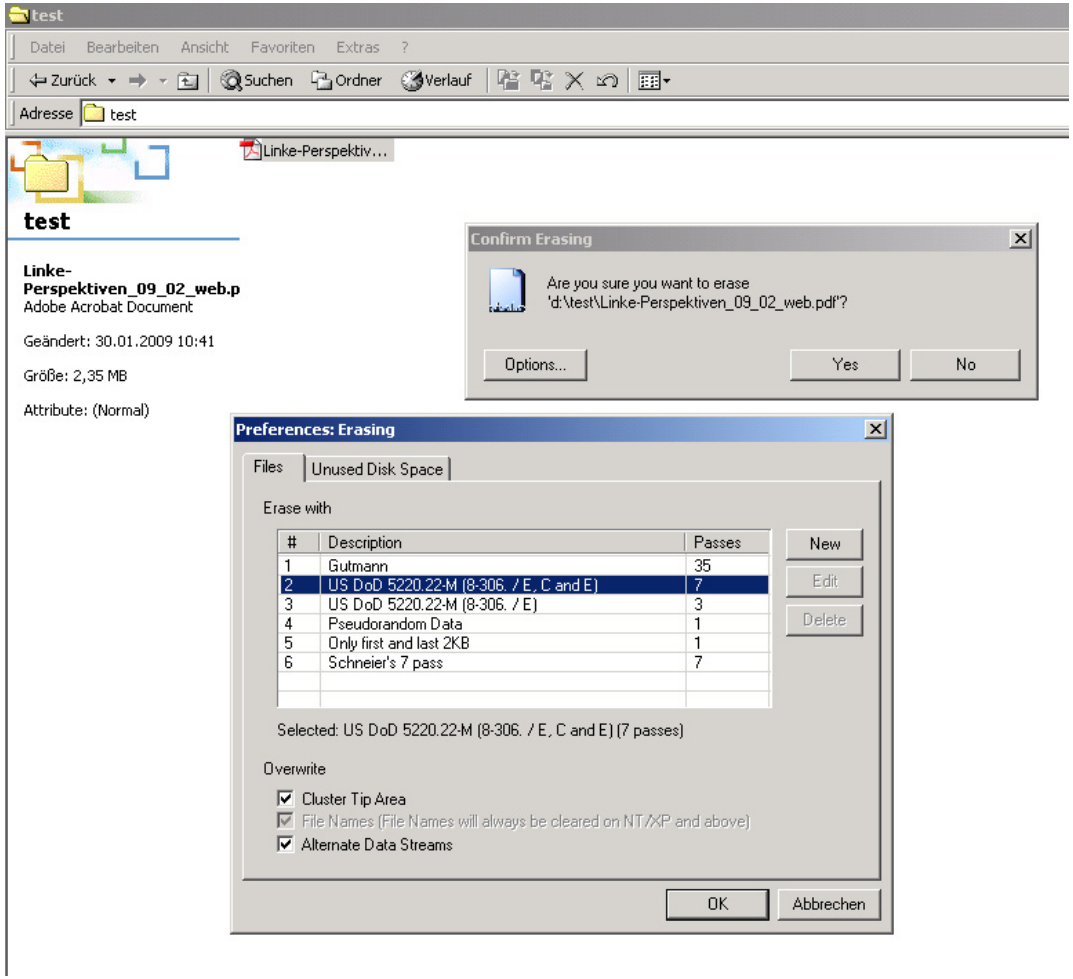
Beispiel: Eraser



Festplatten löschen



Festplatten löschen



Festplatten löschen

weiteres

- Im Kontextmenü gibt es jetzt eine Erase-Option
- Wieviele Durchläufe sind ausreichend?
  - 35 sind overhead
  - 7 reichen auch

Festplatten löschen

Beispiel: Darik's Boot And Nuke

Internet

Internetzugang

Internetzugang

Internetzugang

Router sichern

- Standardpasswort durch gutes Passwort ersetzen

WLAN sichern

- Offenes WLAN schließen
- WEP nicht verwenden (http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/)
- WPA2 verwenden (basiert auf AES)

Browser

Browser

Browser

- Internet Explorer
  - sollte auf gar keinen Fall verwendet werden
  - leider durch illegale Bündelung vorinstalliert
  - immer wieder grobe Sicherheitslücken
- Firefox 3.0
  - frei, schnell und sicher
  - viele nützliche Plugins („Erweiterungen“) vorhanden
  - http://www.mozilla-europe.org
- weitere Browser
  - Opera
  - Lynx ;-)

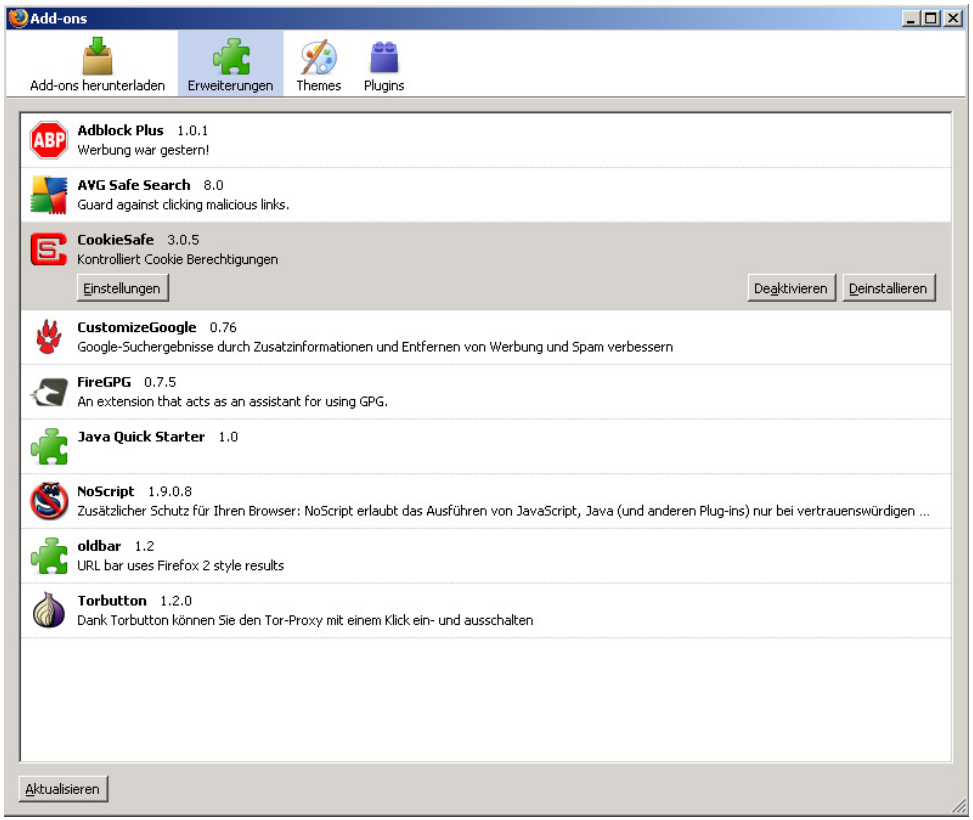
Browser

Nützliche Plugins für Mozilla Firefox

- Adblock Plus
  - blockiert Werbung automatisch
- CookieSafe
  - kontrolliert Cookies
  - blockiert Cookies
- NoScript
  - blockiert Skripte auf Seiten
  - blockiert Skripte von „Dritt-Seiten“, wie z.B. Google-Analyse-Skripte
  - man muss die Seiten explizit freigeben
- FireGPG
  - Verschlüsseln von Webmail
  - siehe später

Browser

Unter „Extras“-> „Add-Ons“ gibt es beim Firefox einen Add-On-Manager. Hier lassen sich Plugins installieren, deinstallieren usw:



E-Mail

E-Mails verschlüsseln

E-Mail

- PGP: „Pretty Good Privacy“
- Verschlüsselungssuite von Phil Zimmermann (1991)
- asymmetrisches Verschlüsselungsverfahren
- Für Windows, Linux, Mac, ...

E-Mail

Installation

- PGP-Basispaket wird zunächst unabhängig installiert
- Windows
  - Komplettpaket gpg4win
  - http://www.gpg4win.org/
- Mac
  - Mac GNU Privacy Guard („macgpg“)
  - GUI: GPG Schlüsselbund
  - http://macgpg.sourceforge.net/de/

E-Mail

Vorgehen:

1. eigenes Schlüsselpaar erzeugen/Passphrase wählen
2. (nur!) öffentlichen Schlüssel publizieren
   - auf Keyserver laden
   - auf Website stellen
   - verschicken
3. öffentliche Schlüssel von Freunden, Genossen etc. importieren

Ergebnis

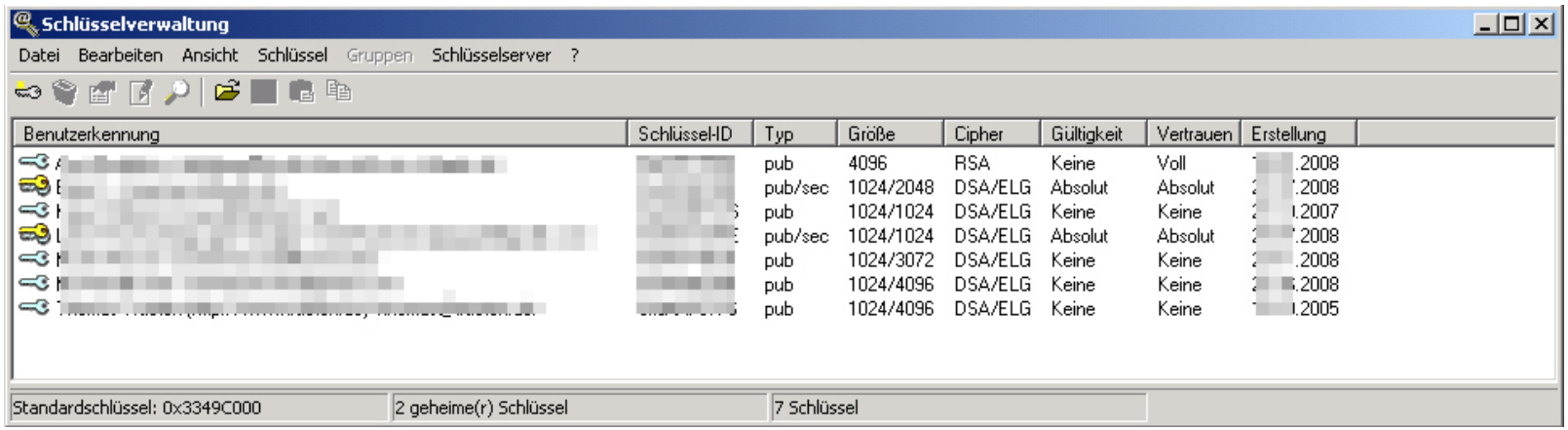
- Nachrichten können mit den **fremden öffentlichen Schlüsseln verschlüsselt** werden
- Nachrichten können mit dem **eigenen geheimen Schlüssel unterschrieben** werden

E-Mail

- Grafische Nutzeroberfläche wie WinPT, Mac Schlüsselbund, etc hilfreich
- für einfache Nutzung: Plugins!
  - Thunderbird mit Enigmail
  - Firefox mit FireGPG

E-Mail

Schlüsselverwaltungstool WinPT

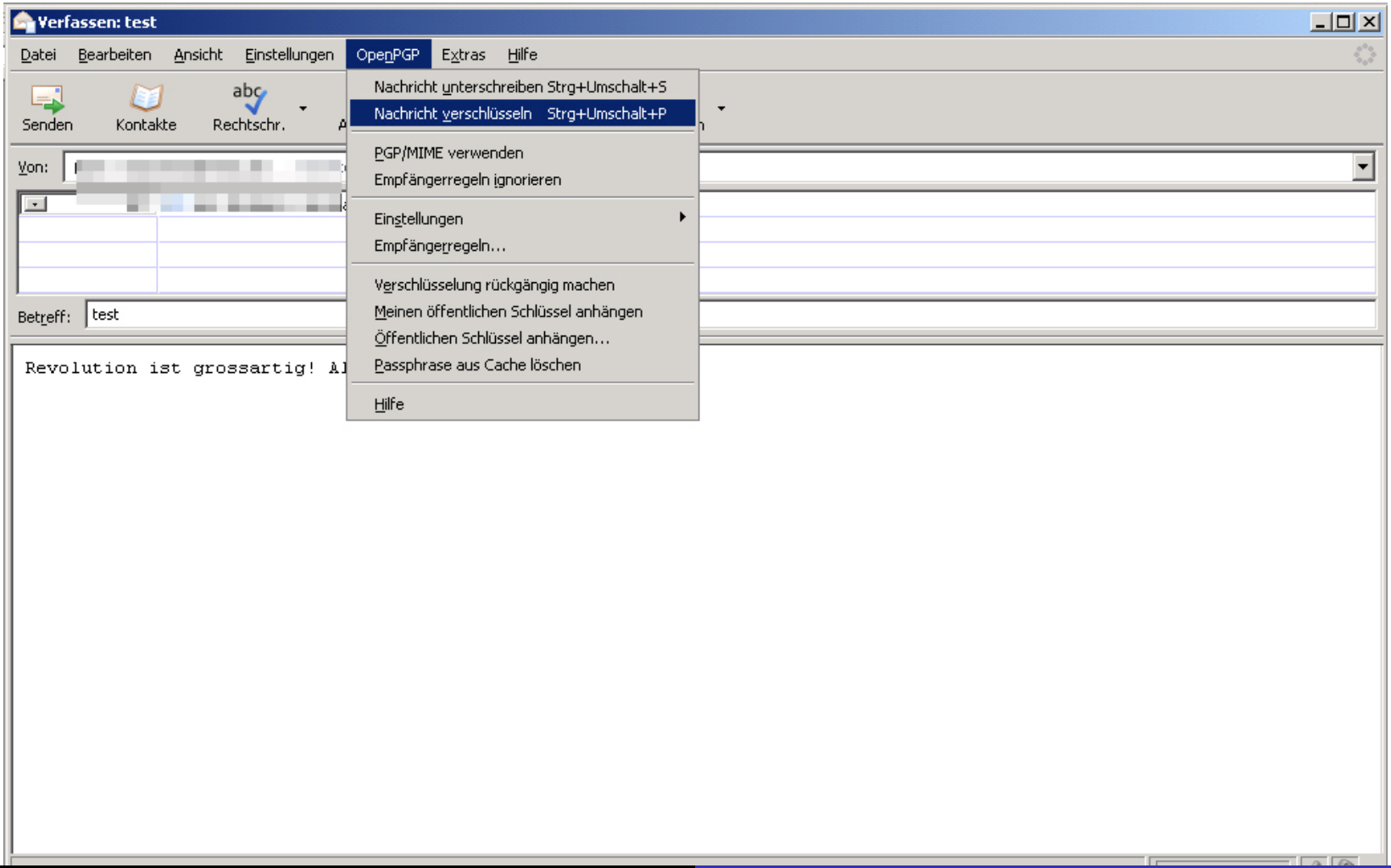


Schlüssel Erzeugt neuen Schlüssel oder Import/Export von Schlüsseln

Schlüsselserver Fremde Schlüssel über Server beziehen

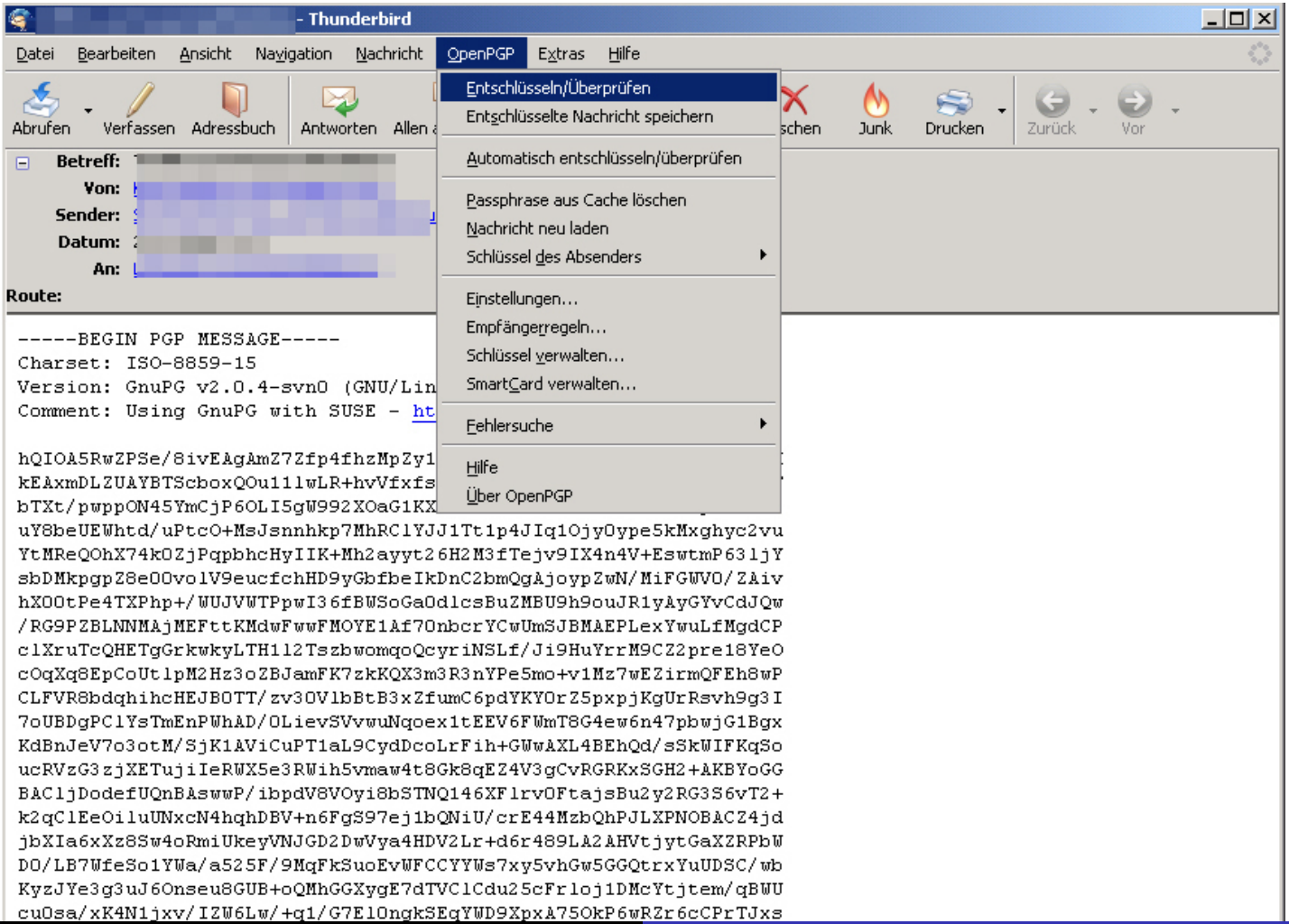
E-Mail

Thunderbird mit Enigmail: Verschlüsseln



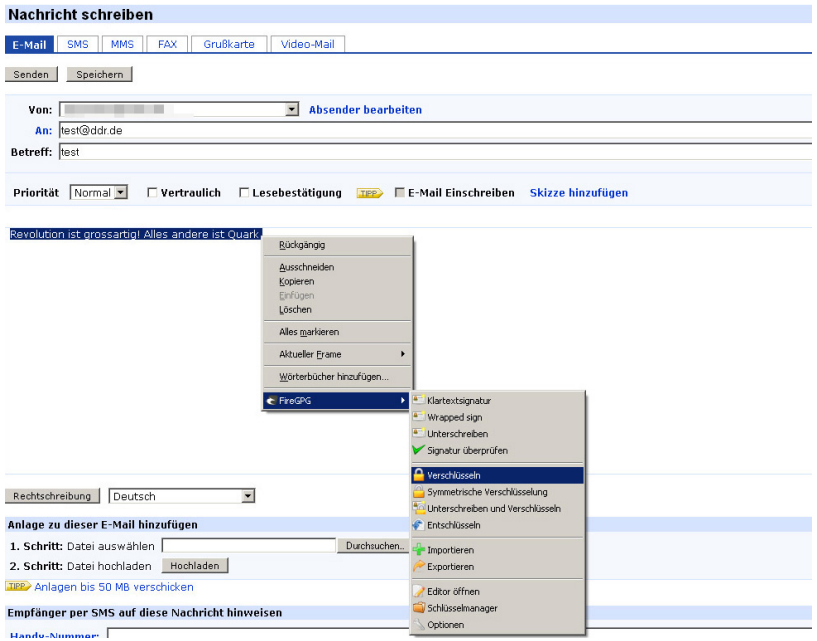
E-Mail

Thunderbird mit Enigmail: Entschlüsseln



E-Mail

Firefox mit FireGPG



Jetzt gibt es im Kontextmenü (Rechtsklick) einen weiteren Menüpunkt „FireGPG“, durch den sich alle wichtigen Verschlüsselungsoptionen auch im Browser und so auch für Webmail nutzen lassen können.

Anonymität im Internet

Anonymität im Internet

Anonymität im Internet

Probleme

- Internet nur scheinbar anonym
- im Hintergrund wird vieles mitgeloggt
- IP-Adressen erlauben eindeutige Zuordnung: Mittels Zeitpunkt + IP-Adresse lässt sich Benutzer identifizieren.
- Cookies und Analysesoftware beobachten Benutzerverhalten
- „Social Networking“ problematisch

Lösungen

- Anonymisierungsdienste
- Onion-Routing: Tor

Anonymität im Internet

Anonymisierungsdienste

- http://anonymouse.org
  - ältester Anonymisierungsdienst
  - Verschlüsselt den Verkehr nicht
- http://www.behidden.com/
  - verschlüsselt Verkehr
  - löscht auch History usw
- weitere auf
  http://meineipadresse.de/html/anonym_surfen_2.php

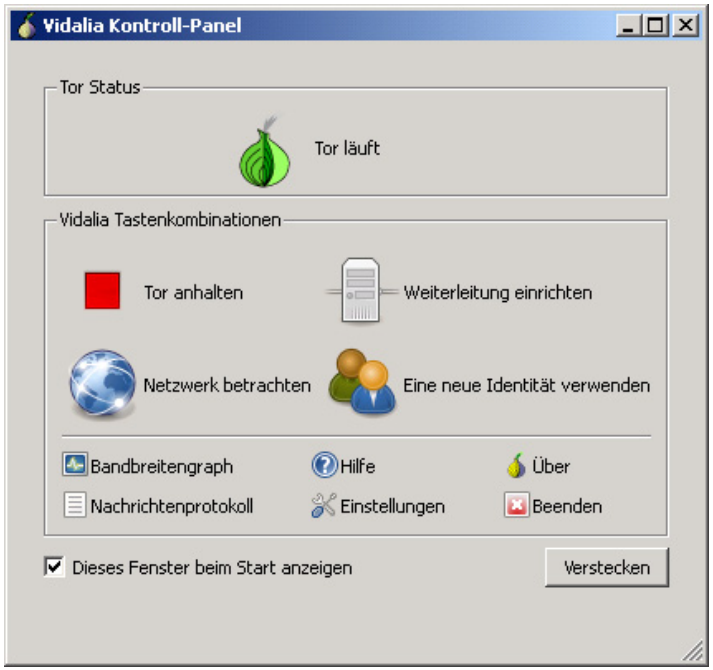
Problem Anonymisierungsdienste sind eine Vertrauensinstanz, d.h. sie kennen die korrekte IP des Benutzers. Dies ist dann problematisch, wenn der Staat bspw. fingierte Dienste betreibt etc.

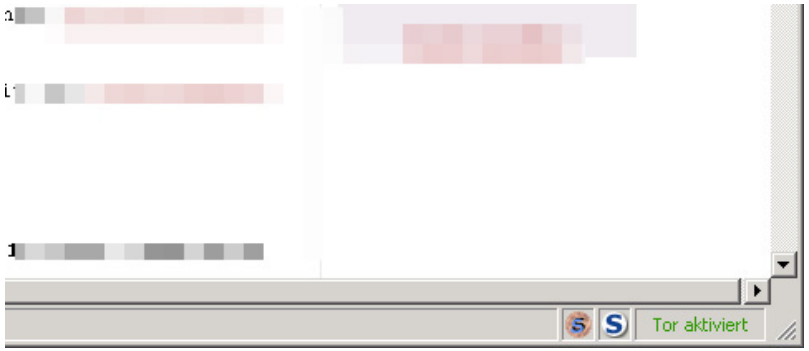
Anonymität im Internet

Abhilfe schafft Onion Routing mit Tor

- Anonymisiert alle Verbindungsdaten (nicht nur Internet)
- Schützt vor Analyse des Verkehrs
- für Windows, Linux, Mac
- Tor-Basissoftware: https://www.torproject.org
- GUI: http://vidalia-project.net
- Torbutton-Plugin für Firefox: https://addons.mozilla.org/de/firefox/addon/2275
- wichtig: Anwendungen (Firefox, Mail, ICQ, usw) für Tor einrichten

Anonymität im Internet





Systeme

Systemupdates

Systemupdates

Systemupdates

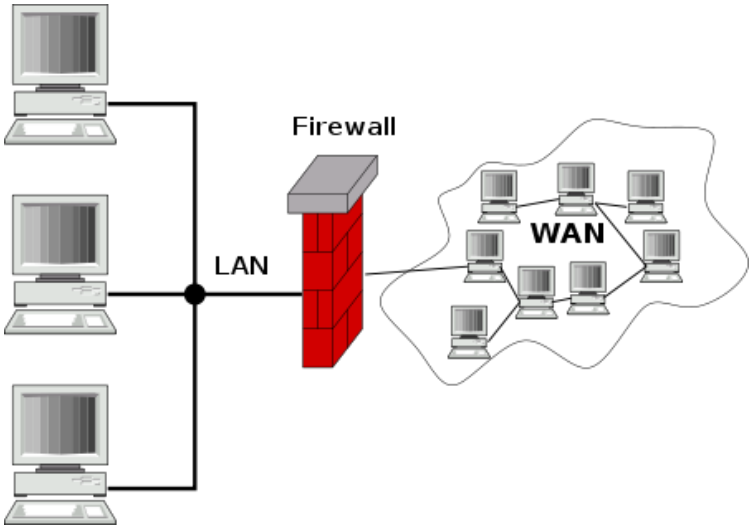
- Lücken in Systemen werden nach und nach gefunden
- darum immer aktuelle Updates installieren
- dies gilt auch für Anwendungsprogramme (Browser, Office, ...)
- heute: Automatische Updatefunktion (Vorsicht)

Firewall

Firewall

Firewall

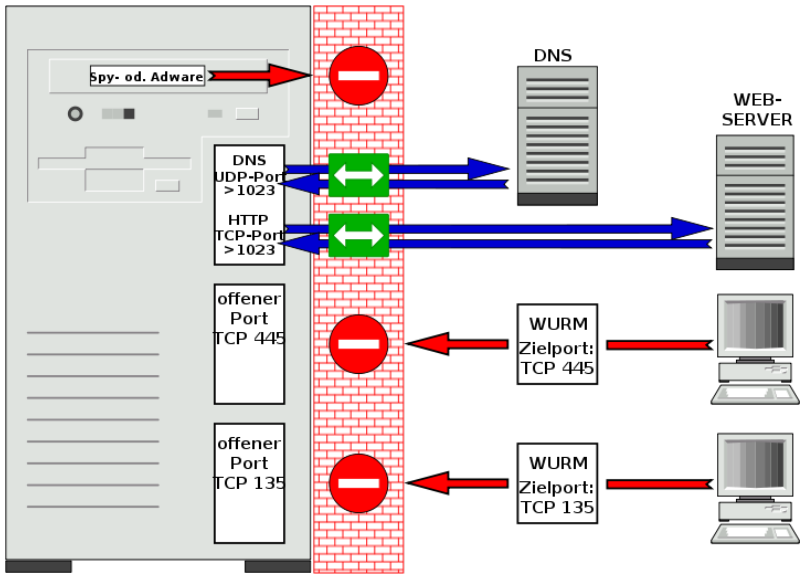
Netzwerkfirewall



- hier nicht besprochen
- Firewall in/als extra Gerät
- oft in Routern enthalten

Firewall

Personal Firewall



- Firewall auf Computer als Software
- seit Windows XP: Windows Firewall
- besser: Zonealarm (http://www.zonealarm.com)

Virenscanner

Virenscanner

Virenscanner

- Begrifflichkeit „Virus“ fasst auch Würmer, Trojaner, Malware
- dies ist eine eklatante Gefahrenquelle
- Virenscanner schützen davor
- automatische Updatefunktion nutzen!
- gute kostenlose Virenscanner verfügbar
  - AVIRA AntiVir http://www.avira.com
  - AVG Free Anti Virus http://free.avg.com

Betriebsystem

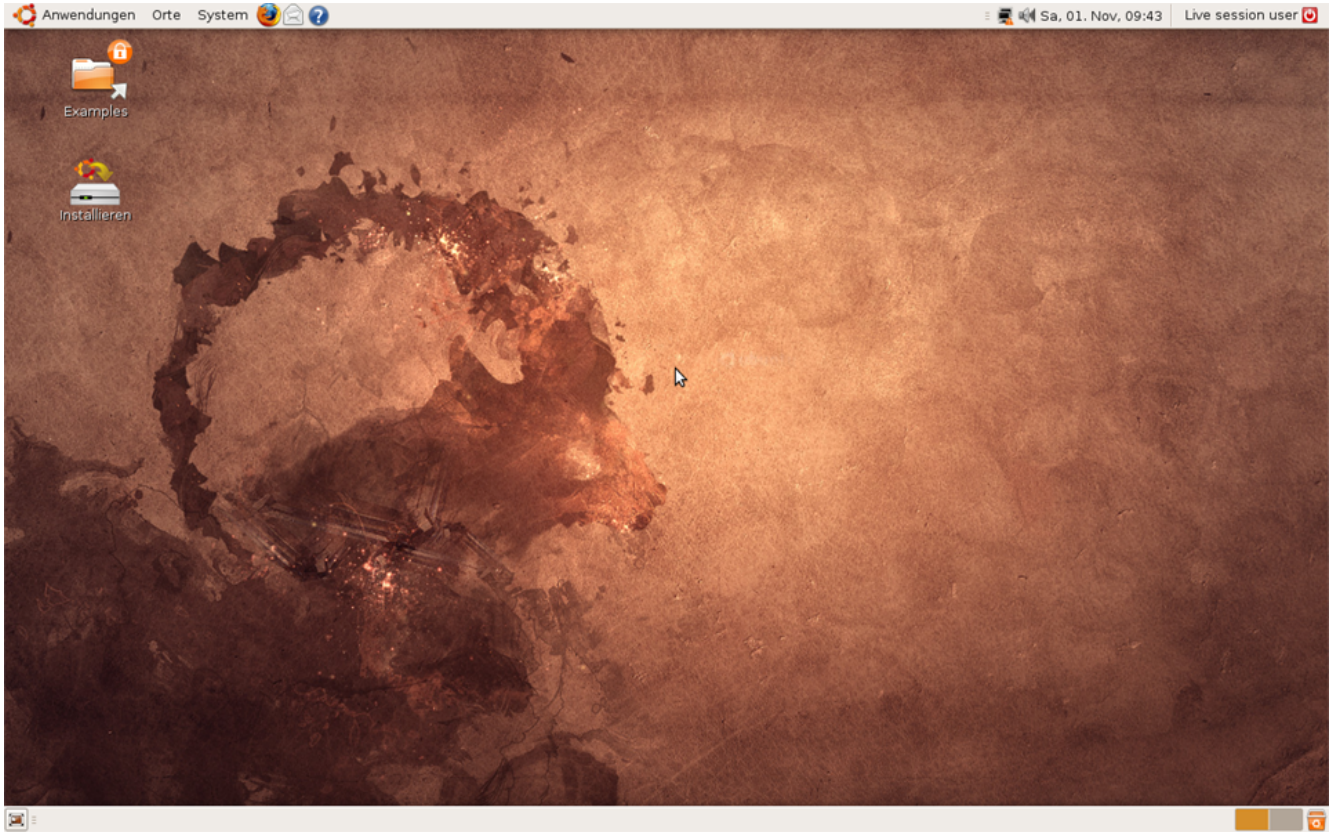
Betriebssystem

Betriebsystem

- von der Wahl des Betriebssystems hängt vieles ab
- Windows unsicher, proprietär und nicht offen
- aber: hoher Marktanteil
- Linux holt auch im Desktop-Bereich auf

Betriebsystem

Beispiel für Easy-to-use Linux: Ubuntu



http://www.ubuntu.com

Betriebsystem

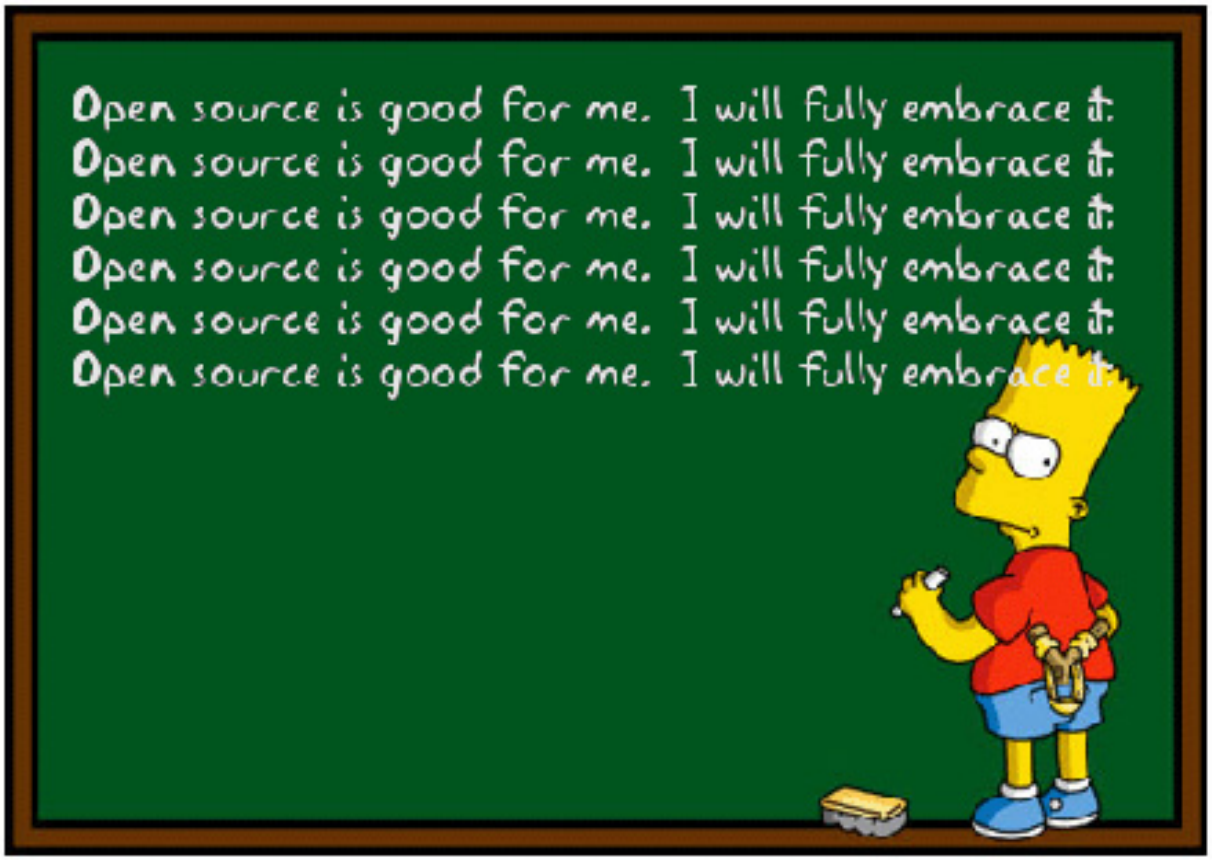
Weiteres interessantes zu Linux

- Debian
  - professionelle Distribution
  - http://www.debian.org
- Knoppix
  - „Live-Linux“: läuft voll von CD
  - http://www.knopper.net/knoppix/

Betriebsystem

- Knoppicillin
  - „Live-Linux“zur Datenrettung
  - steriles Medium, mit dem man Virenbefall ausmerzen kann oder auch Festplatten löschen (siehe Abschnitt „Festplatten löschen“)
  - http://www.heise.de/software/download/knoppicillin_download_edition/37894
- Ubuntu Privacy Remix
  - „Bastion Live-Linux“: Abgeschottet vom Netzwerk
  - steriles Linux, ist abgeschottet und arbeitet nur auf Wechselmedien
  - https://www.privacy-cd.org/

Betriebsystem



Fragen?

Fragen?