Linux User Group **O**ttobrunn - **M**ünchen **S**üd**O**st - LOMSO

Mit Sicherheit Linux

über mich

- Richard Albrecht, Jahrgang 1949
  - Physiker / Uni Halle-Wittenberg
  - Fernstudium Theologie (in der DDR)
  - 1988 - 2000 am MPI für Biochemie Martinsried
    - 3-D Licht-Mikroskopie in der Zellbiologie
    - Bildverarbeitung, C/C++ Entwicklung
  - bis 2011: Middleware, Datenbanken, .NET, Webanwendungen
  - jetzt: Software für CCD Kameras bei SVS-Vistek in Seefeld

  - Linux ist seit 2006 Hobby Nr.1
  - Vorträge, Linuxtage, Hilfen

- Hilfe bei der Umstellung von PCs nach Linux
  - **kein** Virenscanner, **keine** Firewall, **keine** Viren**, keine** Trojaner**,**
  - Installation wird von mir vorbereitet
    - eine kurze Einweisung
    - weitere Wartung durch den Benutzer
    - 'Altlasten' umlagern nach Windows 7 mit KVM
  - www.rleofield.de

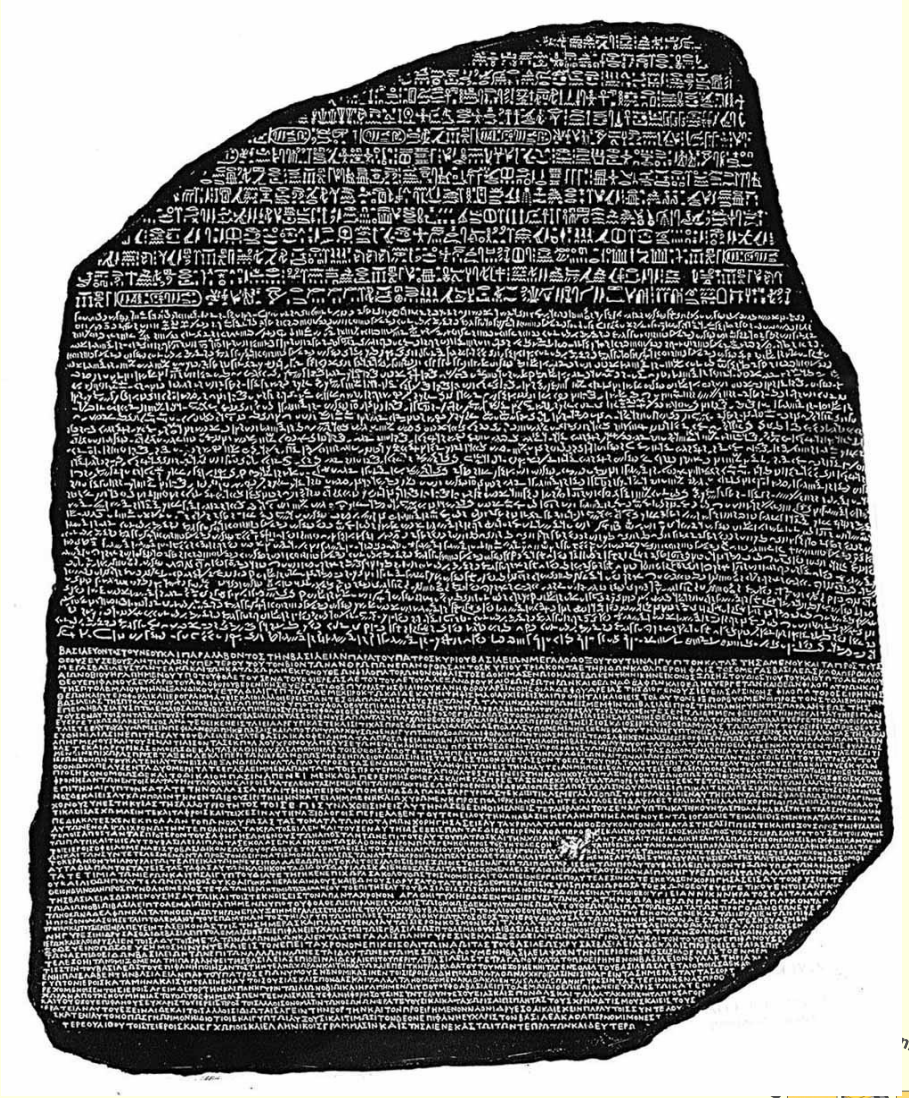
Themen

- Warum Sicherheit der privaten Daten?
  - Grundrecht
  - Privatsphäre
  - Unabhängigkeit
- Sicherheit ist 'out of the box' vorhanden
  - unkompliziert, mit Linux für alle einsetzbar
- gemeinsame Rechnerwelt für die ganze Familie
  - sicheres privates Netz in unsicheren Zeiten
  - Einsatz von SSH zum Aufbau eines sicheren Netzes unter Freunden
  - Ressourcen bleiben zu Hause und sind von überall her erreichbar
- Virtualisierung für alle mit Linux
  - Was ist Virtualisierung?
  - Warum brauchen wir virtuelle PCs?
    - 'Altlasten weiter betreiben', Aufgaben verteilen, dedizierter Server, uvam.
- Was zeige ich nicht?
  - komplizierte lange Rezepte und Anleitungen
- Was zeige ich?
  - was mit wenig Aufwand möglich ist,
  - 'Keep it simple and stupid', (Eric Raymond The Art of Unix Usability)
  - SSH Simple LUG Ottobrunn

Mit Sicherheit Linux

- Stein von Rosetta
- heute noch lesbar, weil:
  - sehr haltbares Speichermedium
  - kein digitales Rechtemanagment
  - kein Trusted Computing
  - keine Format-Geheimhaltung
  - reengineering war nach 2000 Jahren noch möglich
- ohne freie Software
  - werden wir selbst zur Ware
  - geben wir unsere Persönlichkeit ab
  - verlieren wir unsere Identität
  - verlieren wir unsere Geschichte

http://de.wikipedia.org/wiki/Stein_von_Rosetta



Zeitenwechsel

- PC ist zur Privatsphäre geworden
  - private Sicherheit der Daten wird immer wichtiger
  - Bundesverfassungsgericht in DE, 27. Februar 2008
    - „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“
- Sicherheit ist anders geworden
  - Bundestrojaner entdeckt
    - Bericht CCC, FAZ 8.10.2011
    - Super GAU der Computersicherheit
    - Trojaner werden kommerziell hergestellt und verkauft
      … und man verliert die Kontrolle darüber
    - Websperren, Vorratsdatenspeicherung
  - Stuxnet, Conficker-Wurm
  - 'drohender Cyberwar' (in den Medien und bei Politikern)
- Unsicherheit am PC ist Alltag
  - „Microsoft-warnt-vor-PPTP-und-MS-CHAP“ Heise online, 21.08.2012
  - „Microsoft-Sicherheitsbericht sieht Deutschland als SpyEye-Hochburg“
    (Online-Banking-Trojaner) Heise online 24.04.2012
  - Linux sei "in vielerlei Hinsicht sogar stärker betroffen",
    (Bill Gates 2005 im Spiegel, Initiative "Deutschland sicher im Netz") Heise online 31.01.2005

Fragen

- Sind wir davon betroffen?
  - nein, Linuxviren gibt es nicht
  - ja, wenn wir mit Linux so umgehen, wie wir das mit Windows gewohnt waren

- Lösung
  - sich auf Linux einlassen und **selbst** lernen
    - Wikis lesen, Linuxtage besuchen
    - Community kennenlernen (LUG vor Ort)
  - Linux ist nicht wie der bisherige PC
    - Erfahrungen aus der bisherigen PC Welt werden gegenstandslos
    - Vorsicht! Sie können 'Freunde' verlieren (und den Job)
    - ein Windows-Nutzer mit langer Erfahrung muss erkennen,
      dass er wieder ein Anfänger geworden ist
  - dem ***'allwissenden PC-Guru'*** kündigen *(Nachbar, PC-Freak, 'guter Freund' ...)*
  - niemanden an den Linux-PC lassen, der sich '***mit PCs auskennt***'

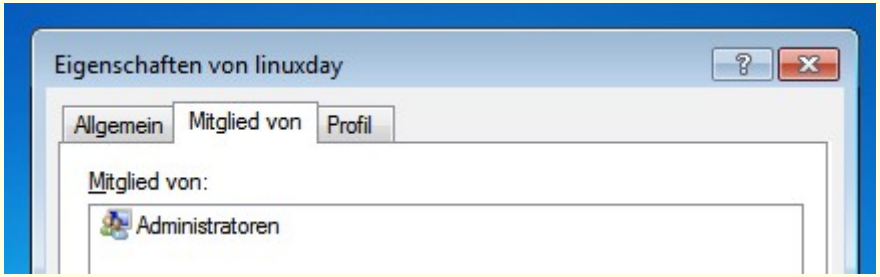
es ist Ihre Entscheidung, Linux einzusetzen . . .

passive Sicherheit

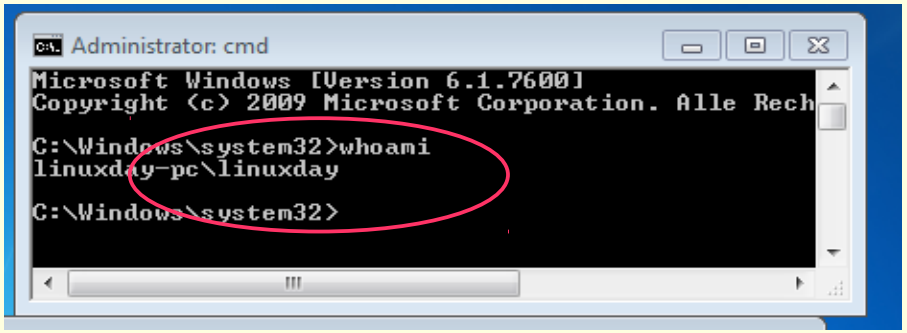
- Rechtetrennung
  - Benutzer <-> root, war unter Linux/Unix nie anders
- Logging
  - Warum? Mein PC funktioniert doch?
    - Fehlersuche
    - Kontrolle der Zugriffe
    - **/var/log/auth.log** --> logging root logins, ssh logins
    - andere Systeme loggen viel weniger
      - wesentliche Ursache für Unsicherheit,
      - 'stille Fehler' werden schwer gefunden,
- Sicherheit per Default
  - restriktive Voreinstellungen
  - 'sudo' Konzept, keine Freigaben in das Netz, ...
  - Warum geht das in Linux nicht, woanders geht es doch?
- es sind die kleinen Unterschiede, die Linux sehr sicher machen
  - einige davon zeige ich jetzt (nur ein kleine Auswahl, sehr unvollständig)

Default Sicherheit, Beispiele aus Windows 7 und Ubuntu

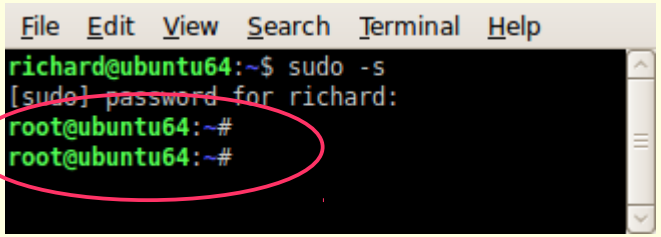
Benutzer nach Installation ist Admin, kein Hinweis darauf
(sehr viele Nutzer wissen es nicht)



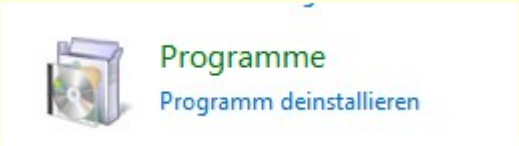
User ***linuxday*** bekommt mit UAC ***Administrator-Rechte***
(ohne PW, nur mit Klick, Zustand ist nicht gut sichtbar)



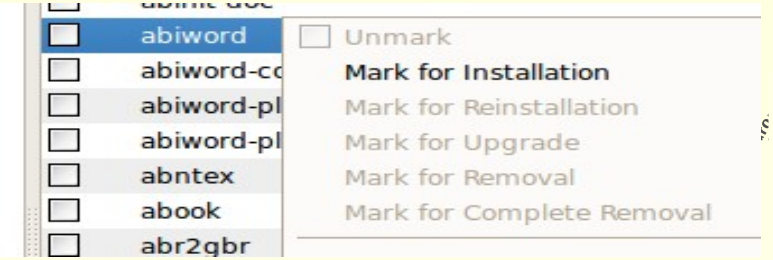
User ***richard*** bekommt keine ***Administrator-Rechte***
richard wird mit 'sudo' für ein Programm ***root***
(nur mit Passwort, Zustand ist gut sichtbar '#',
alle Linux-Benutzer kennen den Unterschied)



Programme, nur deinstallieren, nicht installieren
(Systemsteuerung, nur mit GUI)



in **Ubuntu** installieren und deinstallieren
(viele Möglichkeiten, mit Signatur-Key gesichert)



Sicherheit im Netz (für Windows und Linux)

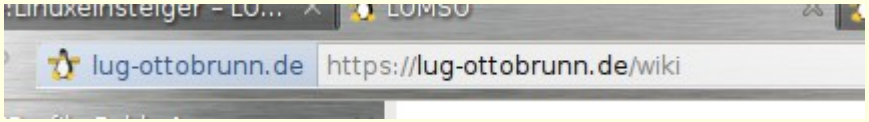
- PGP für Mails
  - ***Schlüssel unter voller Kontrolle***
  - Mails müssen dabei unter eigener Kontrolle sein
  - in Linux: GPG = Gnu Privacy Guard
  - bei den angebotenen Lösungen in DE fehlt die Kontrolle über die Schlüssel
    - DE-Mail, E-Postbrief, aus Sicht des Nutzers unsicher, Rechtsvorschriften als Ersatz ?

- HTTPS gegen 'Abhören'
  - *Schlüssel über CA, der man vertrauen muss* (?)
  - CA = Certificate Authority
  - Surfen über unsichere Netze
  - sichere Authentifizierung des Benutzers (eBanking, Shops)

- SSH zur privaten Kommunikation unter Freunden
  - ***Schlüssel unter voller Kontrolle***
  - sicherer **Tunnel** zum Zugriff auf andere Rechner
  - Erlaubnis des Besitzers nötig
  - SSH bei Windows nicht dabei, es gibt aber OpenSSH

HTTPS (Demo)

LUG-Ottobrunn



General | Details

Could not verify this certificate for unknown reasons.

Issued To

Common Name (CN)	*.lug-ottobrunn.de
Organisation (O)	<Not Part Of Certificate>
Organisational Unit (OU)	<Not Part Of Certificate>
Serial Number	00:D1:D6

Issued By

Common Name (CN)	CAcert Class 3 Root
Organisation (O)	CAcert Inc.
Organisational Unit (OU)	http://www.CAcert.org

Validity

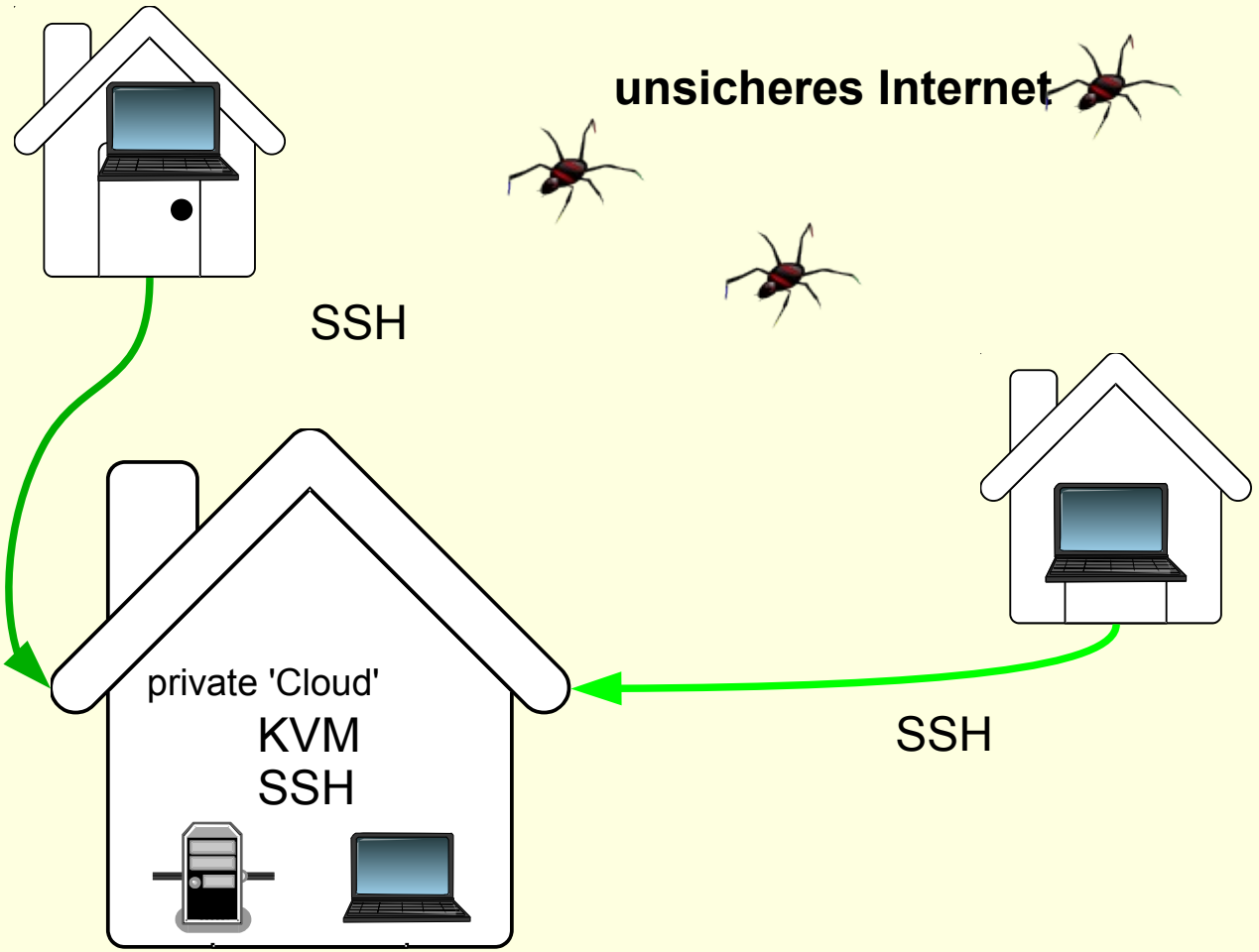
Issued On	21/05/11
Expires On	20/05/13

Fingerprints

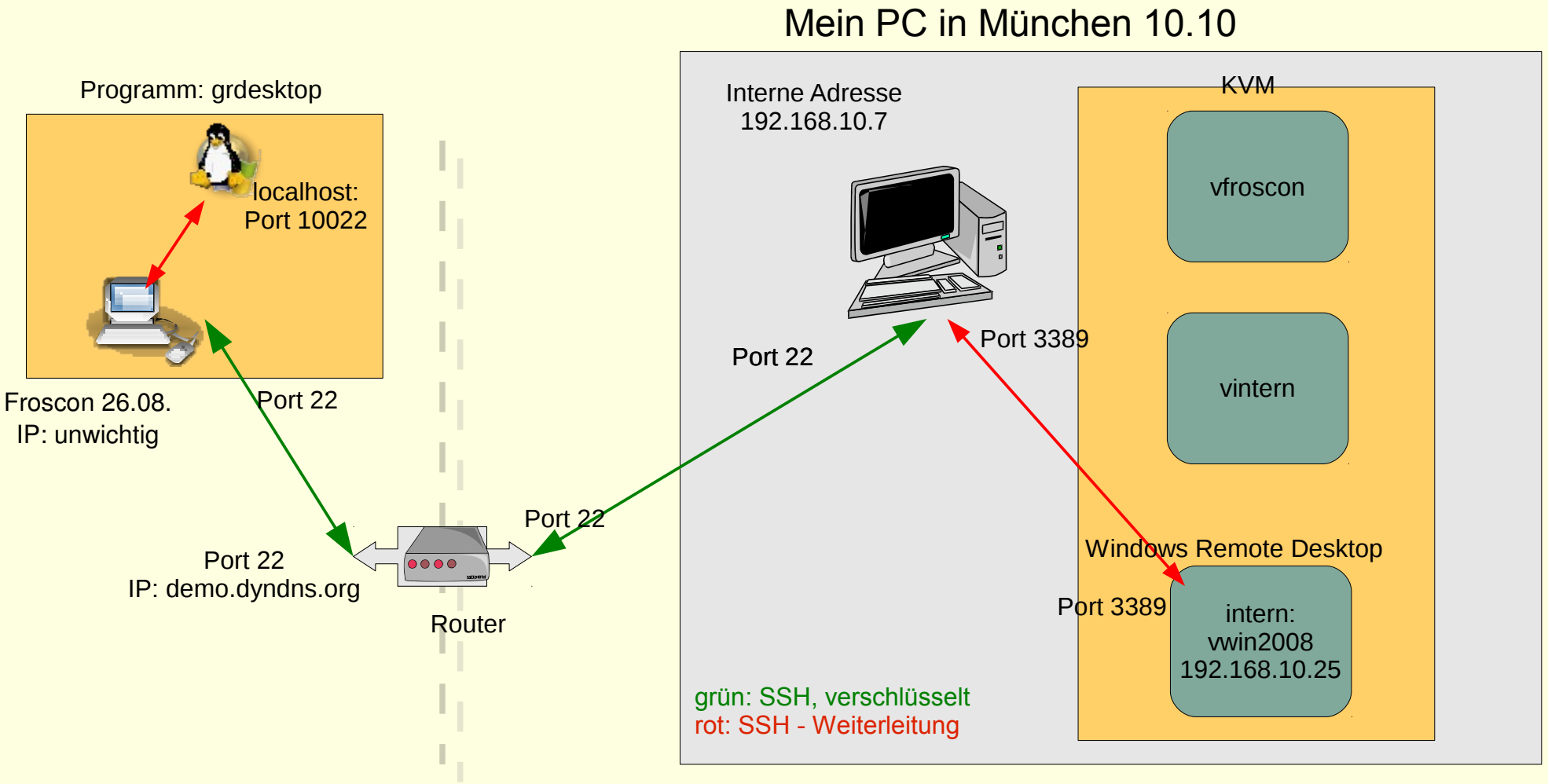
SHA1 Fingerprint	24:14:1E:C9:EE:8C:E3:F4:55:3E:AF:1E:20:BD:3B:C2:17:EE:7E:6C
MD5 Fingerprint	99:16:CC:E9:E3:17:B9:74:08:EF:7F:3E:1B:9D:4F:19

Sicheres Netz mit SSH

privates sicheres Netz, Sie haben die Kontrolle und die Sicherheit



SSH Tunnel



ssh -L 10022:vwin2008:3389 demo@PC.dyndns.org

sicheres Netz für die Familie

- Warum?
  - Überwachung des Datenstroms nimmt zu
  - 'Deep Paket Inspection' ist sehr wahrscheinlich
  - Inhalte können vom Provider im Auftrag kontrolliert werden
- SSH
  - universelle sichere Verbindung (verschlüsselt)
    - Peer to Peer
- Was kann ich damit tun?
  - einfache Terminal Verbindung
  - Ausgabe von grafischen Programmen umleiten
  - Filemanager verteilt verwenden
  - beliebige Programme 'tunneln'
- Familiennetzwerk mit SSH
  - Netz zwischen Benutzern, die sich gegenseitig vertrauen
  - in Linux ohne Zusatzsoftware, '*out of the box*'

Sicherheit von SSH

- SSH installieren (auf allen beteiligten PCs)
  - # apt-get install **ssh**
  - Schlüsselpaar erzeugen und sichern ($ ssh-keygen)
    - für jeden Benutzer auf dem Client
  - öffentliche Schlüssel auf die Server verteilen
    - Privater Schlüssel verbleibt auf dem Client (in ~./.ssh/id_dsa)
    - Öffentlicher Schlüssel kommt auf den Server (~/.ssh/authorized_keys2)
- Passwort Login sperren
  - **Server absichern**
  - **/etc/ssh/sshd_config editieren**
  - Passwort-Login über SSH für alle Benutzer sperren

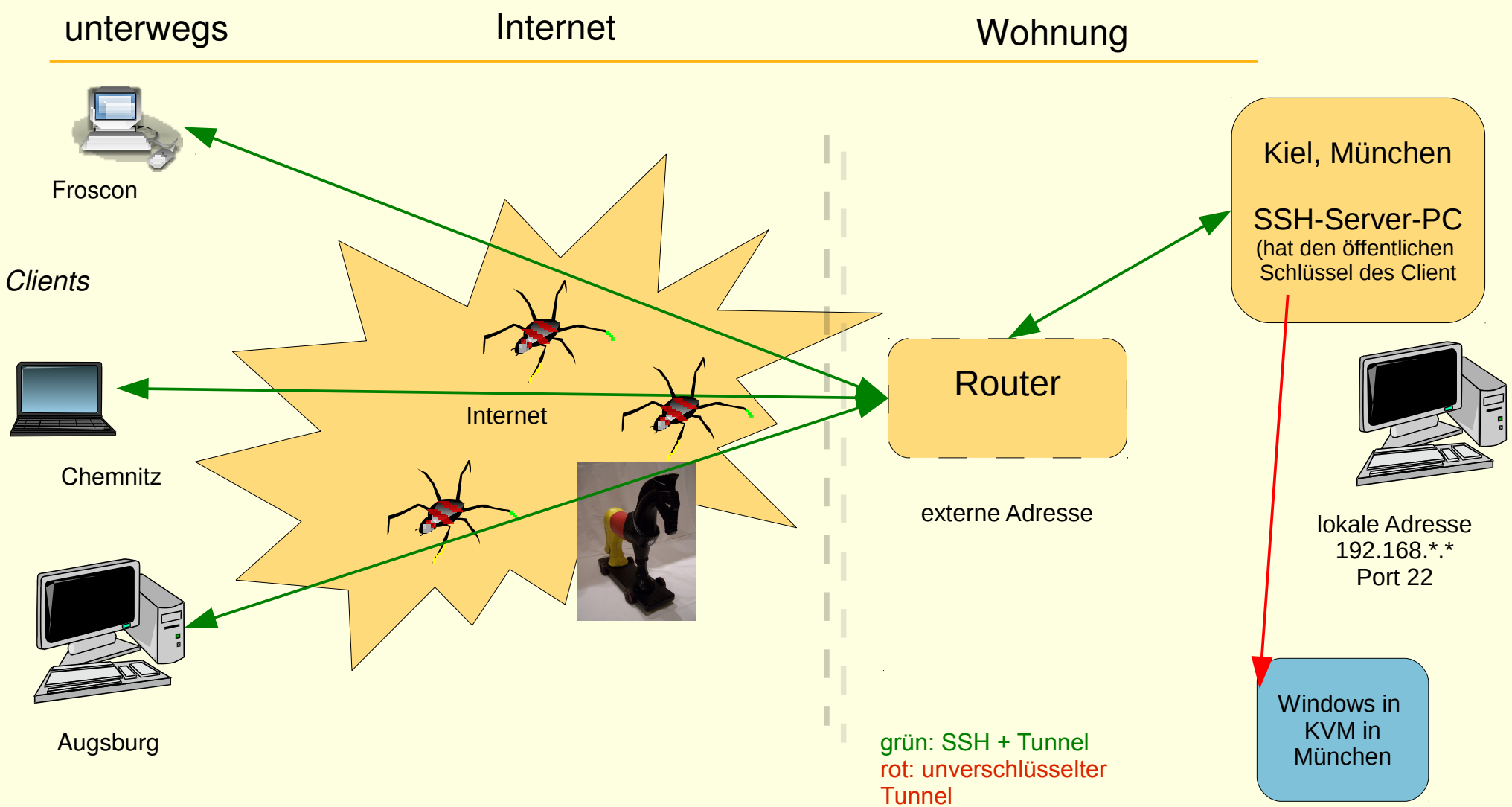
PermitRootLogin no
PasswordAuthentication no

- Router freischalten, nach dem Sperren des Logins
  - SSH-Port muss zum Server-PC weitergeleitet werden
  - Firewall im Router abschalten, bzw. den SSH Port freischalten
    in Doku des Routers nachlesen

SSH - Netz

- Client-Server Struktur
  - jeder PC kann gleichzeitig Client und Server sein
  - Client-Benutzer hat beide Schlüssel
  - Server-Benutzer hat den öffentlichen Schlüssel des Client
- Wer → Wohin ?
  - Client initiiert Verbindung zu einem Benutzer auf dem Server
  - ***ssh -X -C benutzer@server_IP_Adresse***
  - Client bekommt die Rechte von ***'benutzer'*** auf dem Server
  - d.h. der '***benutzer***' am Server stellt seinen Account zur Verfügung
  - Vertrauen untereinander nötig (Familie,Freunde)
  - oder sicheren Account anlegen
- Links bei der LUG-Ottobrunn
  - http://www.lug-ottobrunn.de/wiki/SSH_Simple
  - http://www.lug-ottobrunn.de/wiki/SSH_Spickzettel

so sieht es aus



SSH Anwendungen

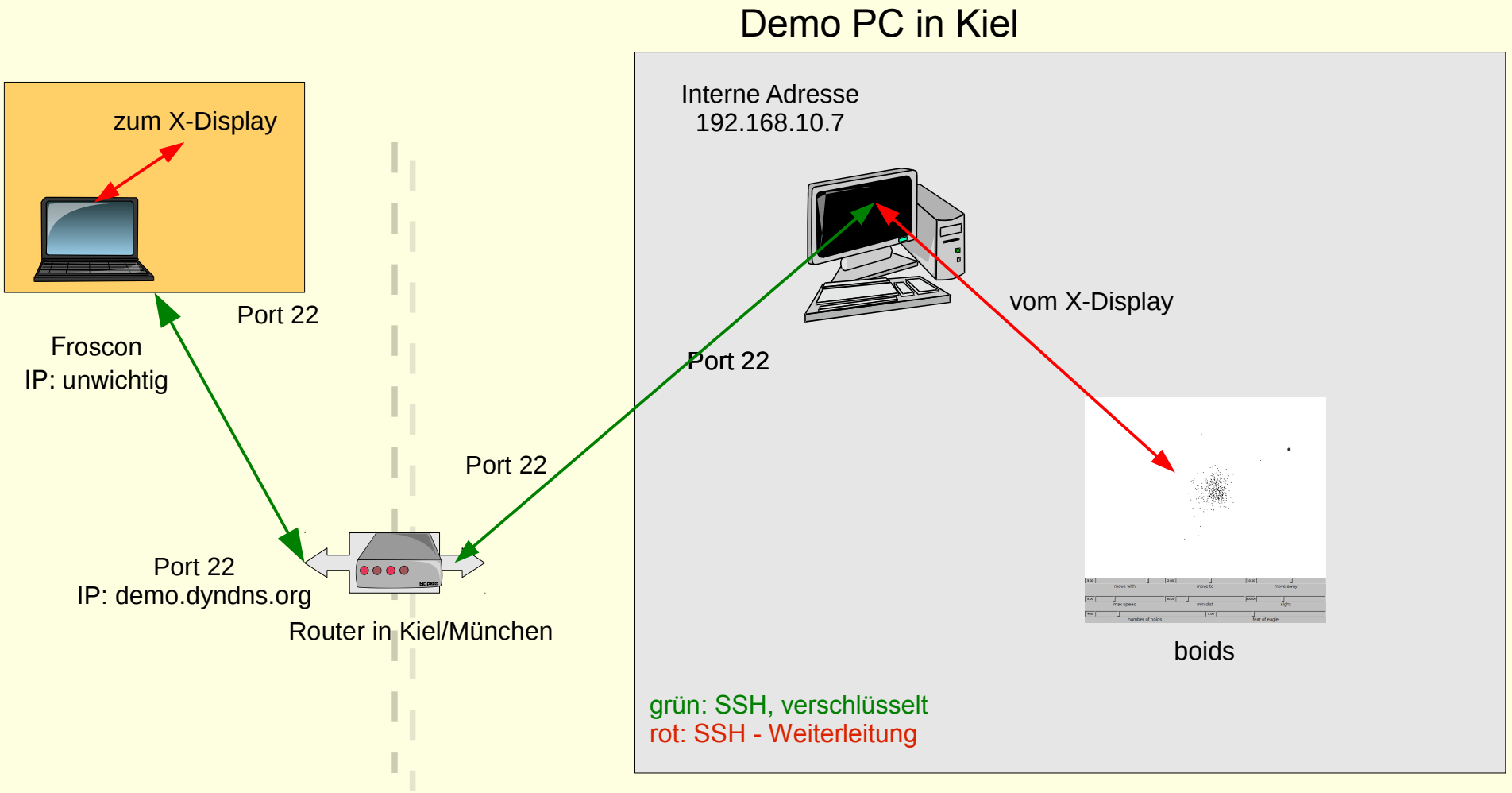
- Terminal
  - ssh -X -C richard@kiel.ath.cx
- Filemanager
  - ssh://richard@kiel.ath.cx/home/richard
  - Demo Liste der Bookmarks in Nautilus
- X Forward
  - in Kiel, Demoprogramm: cd boids, ./boids
- SSH Tunnel
  - Durchleitung vom Ports eines anderen Programms
    Z.B. Remote-Desktop von Windows (Port 3398)
  -
- X2GO
  - Remote Desktop unter Linux

SSH Anwendungen - Terminal

- Terminal
  - ssh -X -C rleo@kiel-example.dyndns.org
  - -X leitet die grafische Ausgabe um
  - -C komprimiert

  - Demo: Zugriff auf einen PC in Kiel

SSH, so sieht es aus, Terminal



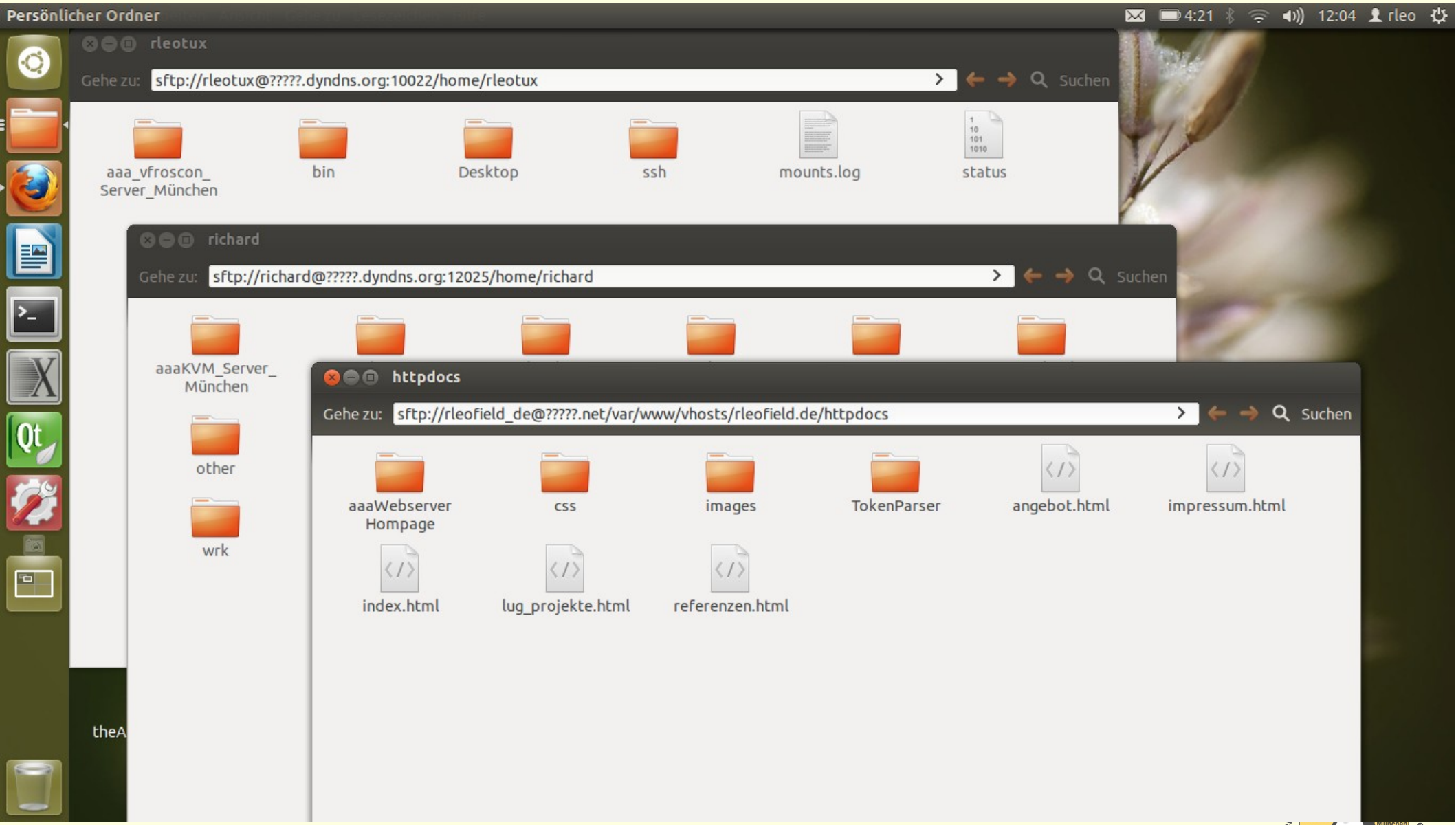
ssh -X -C demo@kiel.dyndns.org:/home/rleo/

SSH Anwendungen

- Filemanager
  - In die Adressleiste eines Filemangers eingeben:
  - **ssh://richard@PC.ath.cx/home/richard**

  - Demo: Liste der Bookmarks in Nautilus

SSH Anwendungen - Filemanager



SSH Anwendungen - Tunnel

- SSH Tunnel
  - Durchleitung von Ports eines anderen Programms
    z.B. Remote-Desktop auf Port 3389
  -
  - Rdesktop über KVM-Host:
  -

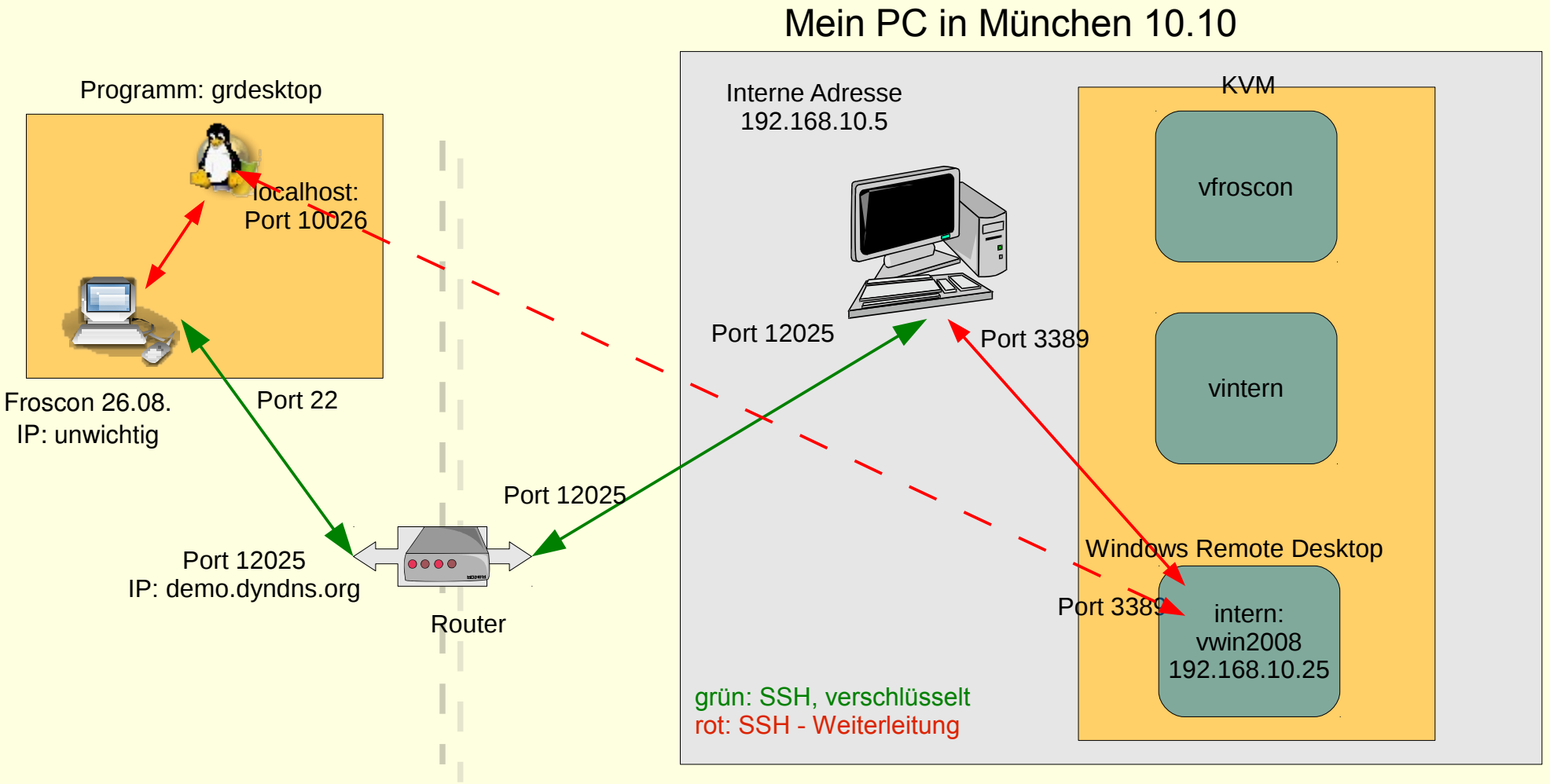
    1.
    ssh -p 12025 -L 10026:vwin2008de:3389 richard@KVM_Host.dyndns.org

    Port 3389 von 'vwin2008de' ist auf 'localhost' Port 10026 erreichbar.

  - 2. in einem anderen Terminal
    rdesktop -g 800x600 -a 16 -k de -u administrator -p passwort localhost:10026

  - 'KVM_Host.dyndns.org' = Brückenrechner
  - 'vwin2008de' = Zielrechner, lokaler Name

SSH Tunnel



ssh -p 12025-L 10026:vwin2008:3389 demo@PC.dyndns.org

SSH Anwendungen - X2GO

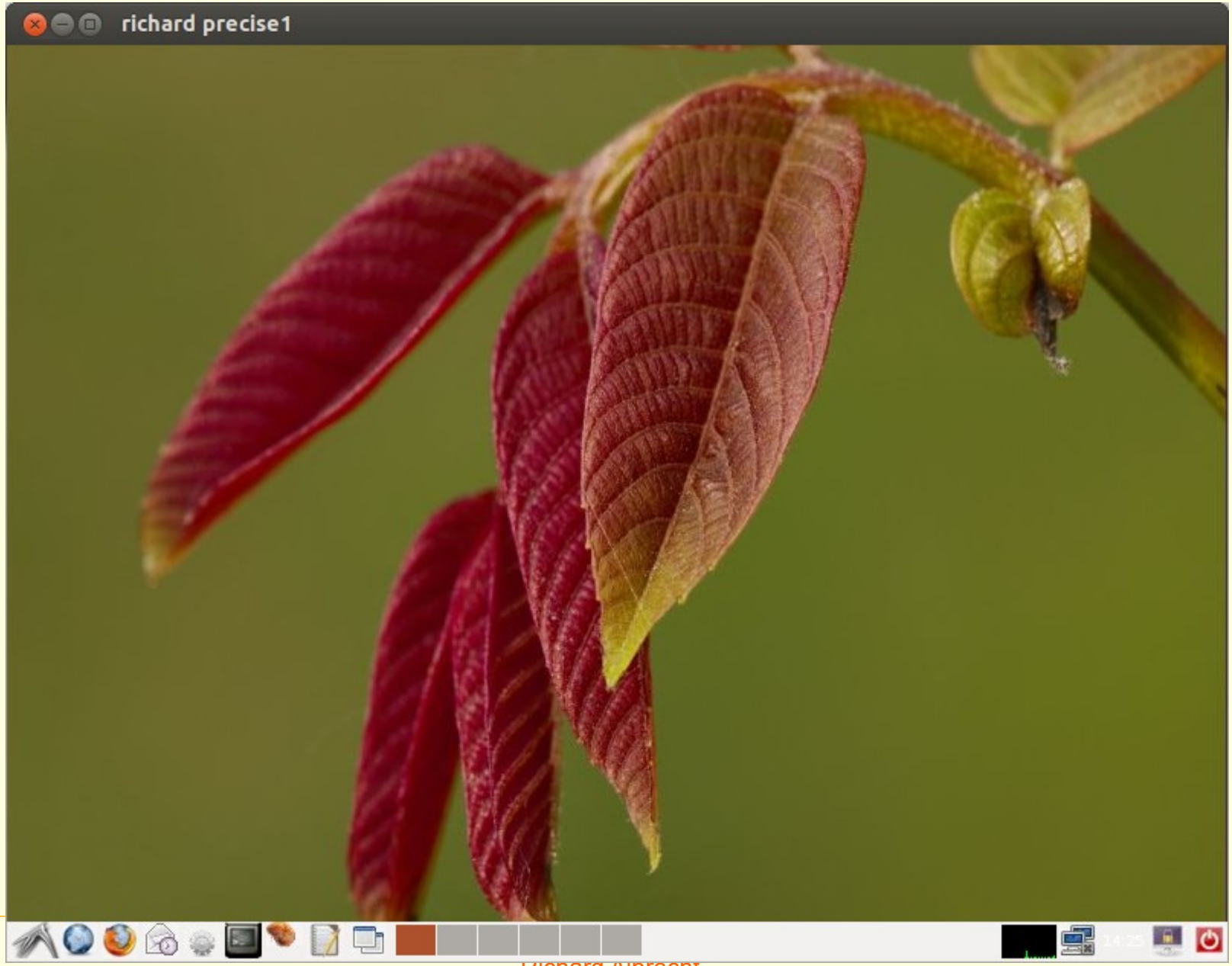
- X2GO
  - Remote Desktop unter Linux
  - http://www.x2go.org/
  - http://lug-ottobrunn.de/wiki/Remote_Desktop_mit_X2GO
  -
  - https://launchpad.net/~x2go/+archive/stable
  -
  - Installation, als root (sudo -s)::

```
# apt-add-repository ppa:x2go/stable
# apt-get update
# apt-get install x2goserver
# apt-get install x2goclient
```

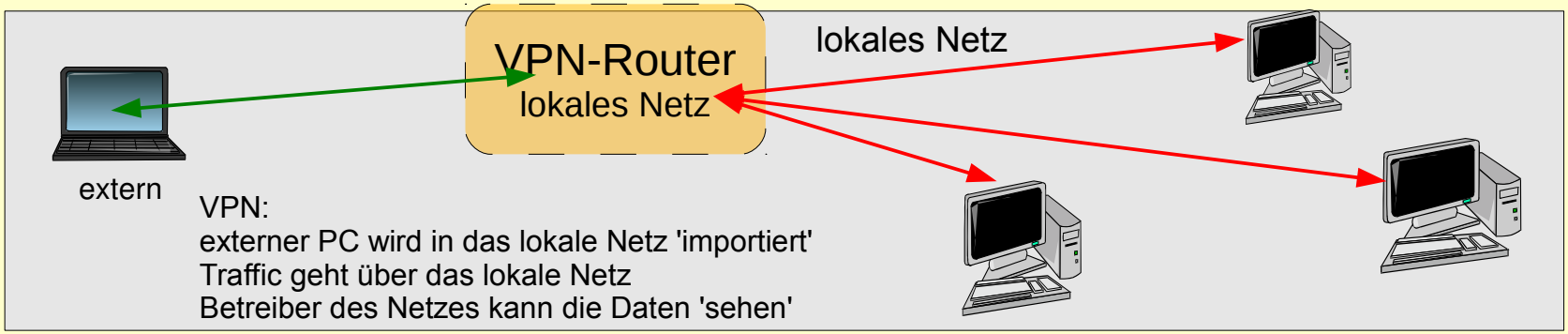
  - Tunnel aufbauen:
    ssh -p 12025 -L 10029:vprecise1:9022 richard@PC.dyndns.org

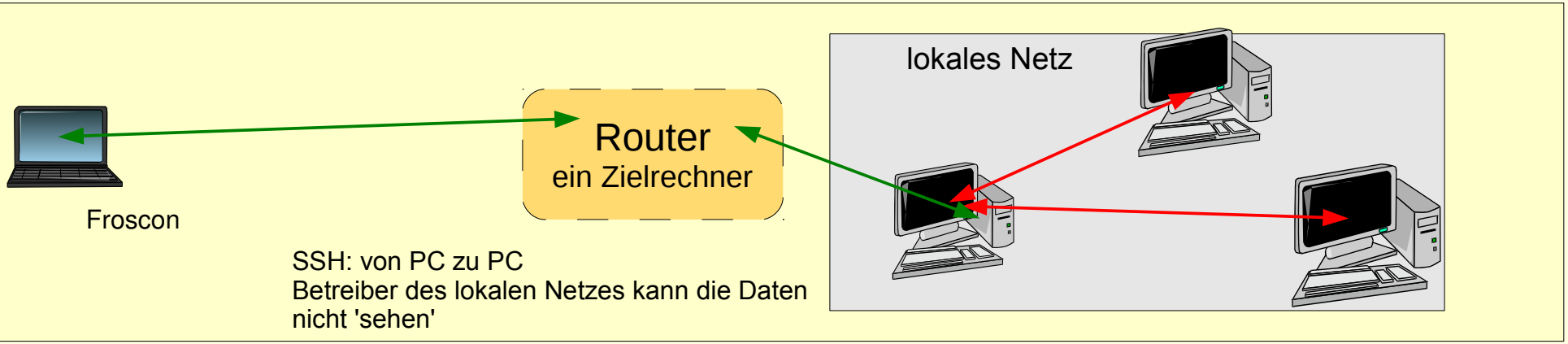
    X2GO ist auf 'localhost:10029' erreichbar

SSH Anwendungen - X2GO



VPN oder SSH ?



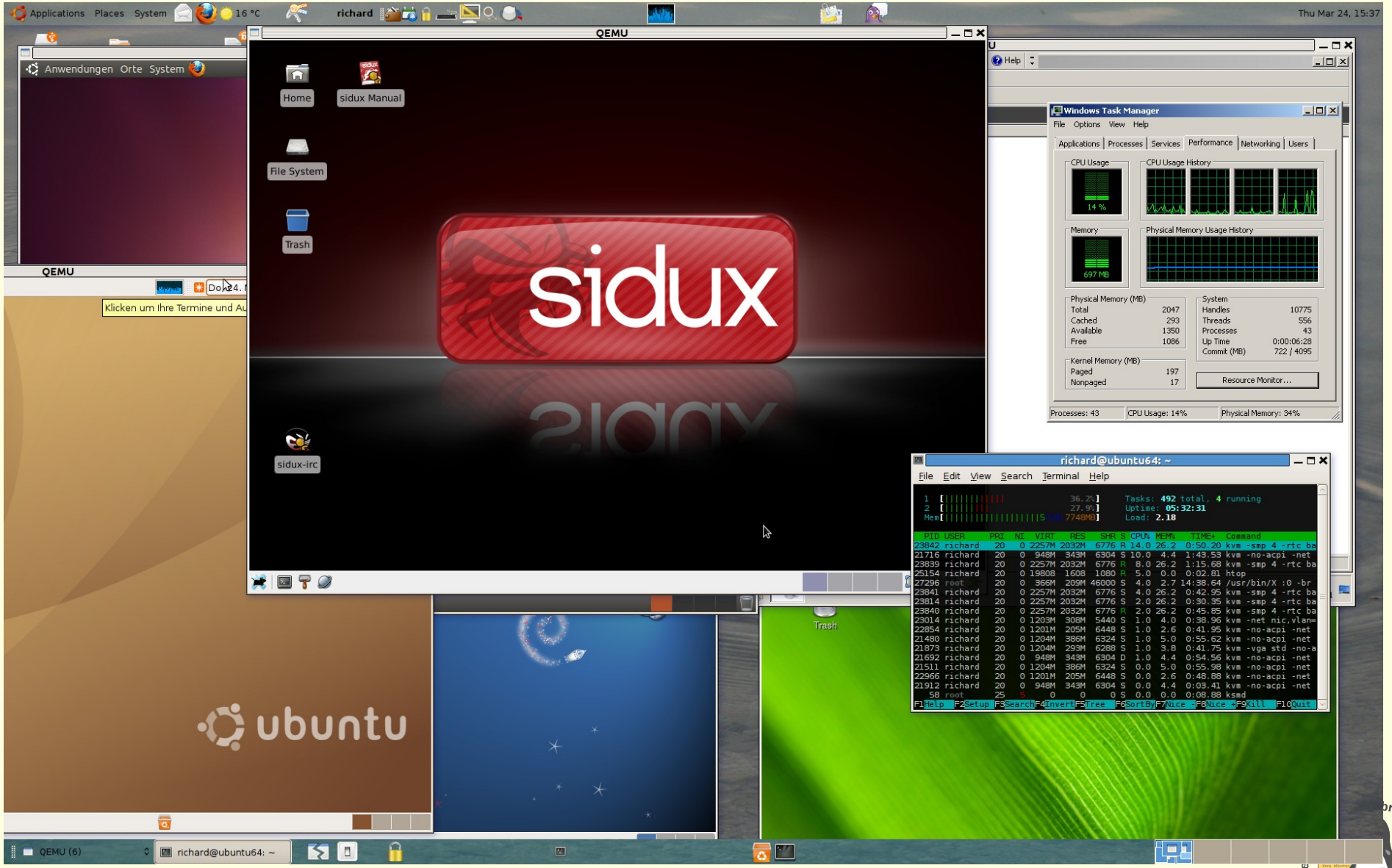


grün: verschlüsselt
rot: Klartext

Checkliste SSH

- Installation Server und Client
  - # apt-get ssh
  - Account auf dem Server anlegen, mit starkem Passwort
- Erster Start
  - In den Server einloggen
  - Schlüssel erzeugen, auf dem Client
  -
  - Schlüssel zum Server kopieren (copy / paste)
  - Passwort-Login zum Server abschalten (sshd_config, nicht ausloggen!)
  - SSH auf den Server neu starten, immer noch nicht ausloggen
  -
  - erster Login Versuch zum Server mit Schlüssel
  - wenn erfolgreich, ausloggen
  - alles ok

Virtualisierung mit KVM



Installation von KVM unter Ubuntu

- Kernel Based Virtual Machine
  - von Ubuntu favorisiert
  - PC 'Altlasten' weiter betreiben (Lizenzen beachten)
  - z.B. Finanzbuchhaltung, Steuererklärung, Branchensoftware
  - Aufgabenteilung

- Siehe Webseiten von 'ubuntuusers.de' und 'ubuntu.com'
  - http://wiki.ubuntuusers.de/KVM
  - https://help.ubuntu.com/community/KVM
  - http://www.linux-kvm.org/page/Management_Tools

  - Install **qemu-kvm** und testen
    - # apt-get install kvm
    - $ **kvm-ok**

      INFO: Your CPU supports KVM extensions

      INFO: /dev/kvm exists

      KVM acceleration can be used

  - http://lug-ottobrunn.de/wiki/Virtualisierung_mit_KVM

Einbinden in das lokale Netz

- *bridge utils* für Einbindung in das lokale Netz (192.168.*.*)
  - default ist 10.2.0.2, d.h. die VM ist 'unsichtbar'
  - https://help.ubuntu.com/community/KVM/Networking
  - nicht ganz einfach, aber gut dokumentiert
  - http://lug-ottobrunn.de/wiki/Virtualisierung_mit_KVM

- Demos
  - Windows 2008 Server, in KVM im lokalen Netz in München
  - Zugriff mit Remote Desktop
  - Windows kann kein SSH, Ubuntu schon
  - **ssh -L 10022:vwin2008:3389 lugdemo@meinPC.dyndns.org**
  - Zugriff mit Remote-Desktop, localhost
  - **rdesktop -x l -g 1100x720 -a 16 -k de -u Administrator -p xxxxxxx localhost:10022**

  - Demo 2: Windows 7 lokal
  - **kvm win2008de.ovl -m 2048 -smp 2 -net nic -net user,hostfwd=tcp::3389-:3389**
  - Zugriff zum Remote-Desktop mit localhost
  - **rdesktop -x l -g 1200x720 -a 16 -k de -u rleo localhost**

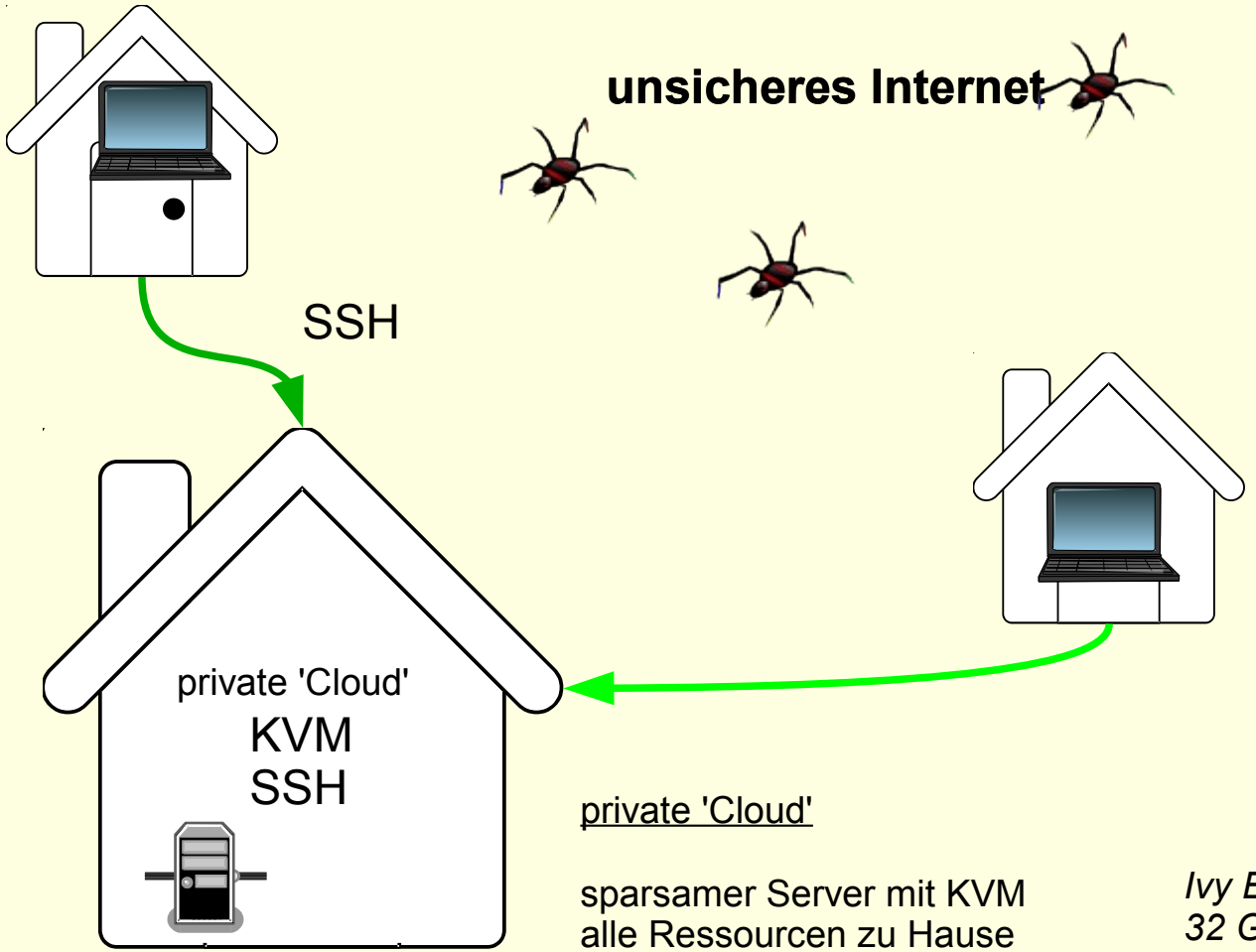
Checkliste KVM

- Installation
  - kvm, bridge-utils, uml-utilities
  - http://lug-ottobrunn.de/wiki/Virtualisierung_mit_KVM

- Betrieb
  - ohne 'virsh' – simple Skripte sind einfacher
  - Konfiguration in Textfile
  - VMs in Folder mit dem Namen den VM
  - Start / Stop
  - running / notrunning
  - Images mit Overlays anlegen → stabiler Betrieb
  - Backup auf externes Medium mit 'rsync'
  - alle VMs mit Remote-Zugruff installieren (SSH od. Rdesktop)

  alles auf Host -PC im lokalen Netz ohne Grafik
  - (Scripte bei mir oder bei der LUG-Ottobrunn)

privates sicheres Netz, Sie haben die Kontrolle



private 'Cloud'

sparsamer Server mit KVM
alle Ressourcen zu Hause
in Verbindung mit Freunden
sicher, einfach, vertrauenswürdig

Ivy Bridge, i7
32 GB RAM


THE HIGHWAY TO
FREEDOM IS NOW
OPEN FOR
EVERYONE
it's your turn to go ...

Ende des Vortrages, kein Ende mit Linux ;-)

- Lernprozess
  - bessere Kenntnisse im Umgang mit dem Computer
  - bessere Sicherheit des eigenen PC
- Ergebnis
  - **Sie** werden staunen, was **Sie** alles im Umgang mit Linux lernen
- sicheres privates Netz
  - einfach, transparent, sicher
- KVM
  - alter PC lebt virtuell weiter
  - jedem sein PC, egal, wo man sich aufhält
  - besonders gesicherter PC in einer VM
- Weitere Infomationen und Skripte: http://www.lug-ottobrunn.de/wiki/

Vielen Dank für Ihre Aufmerksamkeit
und eine schöne Heimreise
Richard Albrecht

Mini Workshop SSH

- Installation SSH auf dem eigenen Notebook
  - # apt-get ssh
  -
- Erster Start
  - Schlüssel erzeugen, auf dem Client
    - $ ssh-keygen
  -
  - public Schlüssel zum Server kopieren (copy / paste), mache ich mit USB-Stick
  -
  - erster Login Versuch zum Server mit Schlüssel
  - $ ssh -X -C frc1@example.org
  - 'xclock' aufrufen
  - mit 'traceroute' testen
  - uvam.
  -