Grml-Forensic

Michael Prokop <prokop@grml-forensic.org>

Fraunhofer SIT
ANWENDERTAG IT-FORENSIK

Über den Vortragenden

- Projektleiter von Grml.org
- Offizieller Debian-Entwickler
- Mitglied/Admin im Debian-Forensic-Team
- Gründer des Security-Treff-Graz
- IT- und Open-Source-Consultat
- Autor des Buches „Open Source Projektmanagement - Softwareentwicklung von der Idee zur Marktreife“

Definition Live-System

- Bekannt als Live-CD
- Kann heutzutage aber wesentlich mehr:
  - DVD ☺
  - USB
  - Netzwerkboot
  - ....

Grml?

- Erstes Release 2004
- Debian-basiertes Live-System
- speziell für Systemadministratoren
- viele Tausend Anwender
- >7 Jahre Erfahrung in Entwicklung von Live-Systemen (Kernel, initramfs-tools, FAI/grml-live,...)

Vorteile von Live-Systemen

+ Kein Hardware-Schreibschutz notwendig
+ Kein Disassemblieren der Hardware
+ Vielfältige Einsatzmöglichkeiten
+ Komplexe Szenarien (FC-SAN, RAID, LVM,...)
+ Anpassbarkeit (Software, Workflow,...)

Risiken von Live-Systemen

- Bootreihenfolge
- Sicherheit: Angriffsmöglichkeiten, Netzwerkzugriffe,...
- Root-Rechte
- Murphy

Beseitigung der Risiken

- Bootreihenfolge: Dokumentation, Schulung
- Sicherheit: Qualitätssicherung, Testen
- Root-Rechte: normaler Benutzer, sudo
- Murphy: Support ☺

Journal Replays

- ro-Mountoption nicht ausreichend
- loop-Mountoption
- sysctl -w vm.block_dump=1

```
[  647.755575] flush-8:0(3510): dirtied inode 131 (?) on sda1
[  648.287774] xfsdatad/0(310): dirtied inode 131 (?) on sda1
[  648.289441] flush-8:0(3510): dirtied inode 131 (?) on sda1
[  648.289480] flush-8:0(3510): WRITE block 96420 on sda1
```

```
[  433.935615] umount(3859): WRITE block 0 on loop1
[  433.936198] umount(3859): WRITE block 96402 on loop1
[  434.038875] umount(3859): WRITE block 0 on loop1
[  434.039460] umount(3859): WRITE block 96404 on loop1
```

Hacking Live-Systems

```
Begin: Mounting root file system ... [    2.001610] EXT2-fs
nting ext3 filesystem as ext2
[    2.017980] EXT2-fs (sda2): warning: mounting ext3 files
[    2.031453] aufs 2-standalone.tree-35-rcN-20100705
done.
Begin: Running /scripts/init-bottom ... done.


System information - found deft

WARNING: Automatically executing malicious actions now...
(This output is visible for demonstration purposes)
-> Done.
```

Hacking Live-Systems

```
+ [ ! -x /root/sbin/init ]
+ [ -z /sbin/init ]
+ [ ! -x /root/sbin/init ]
+ [ -n y ]
+ unset debug
+ maybe_break init
+ egrep -q (,|^)init(,|$)
+ echo
+ exec run-init /root /sbin/init text


System information - found caine

WARNING: Automatically executing malicious actions now...
(This output is visible for demonstration purposes)
-> Done.
```

Hacking Live-Systems

```
System information - found ubuntu

WARNING: Automatically executing malicious actions now...
(This output is visible for demonstration purposes)
-> Done.

/ # mknod /dev/sr0 b 11 0
/ # mount /dev/sr0 /mnt
/ # ls /mnt/
AutoPlay            casper              md5sum.txt
EULA.pdf            dists               pool
IR                  helix.exe           preseed
Language            helix.ico           ubuntu
README.diskdefines  install
autorun.inf         isolinux
/ # uname -a
Linux ubuntu 2.6.24-19-generic #1 SMP Wed Aug 20 22:56:21 UTC 2008 i686 GNU/Linu
x
/ # cat /proc/cmdline
BOOT_IMAGE=/casper/vmlinuz file=/cdrom/preseed/xubuntu.seed boot=casper initrd=/
casper/initrd.gz splash --
/ # _
```

Hacking Live-Systems

```
Done.
+ mount -n -o move /sys /root/sys
+ mount -n -o move /proc /root/proc
+ [ -n /sbin/init ]
+ [ ! -x /root/sbin/init ]
+ [ -z /sbin/init ]
+ [ ! -x /root/sbin/init ]
+ [ -n y ]
+ unset debug
+ maybe_break init
+ [  = init ]
+ exec run-init /root /sbin/init


System information - found ubuntu

WARNING: Automatically executing malicious actions now...
(This output is visible for demonstration purposes)
-> Done.

Execute /bin/mksh -T/dev/tty2 and switch to tty2
to get a fully working /bin/sh with job control.
/bin/mksh: No controlling tty: open /dev/tty: No such device or address
/bin/mksh: warning: won't have full job control
# _
```

Hacking Live-Systems

<< back | track 龍

```
+ [  = y ]
+ /scripts/init-bottom/udev
+ [ -e /conf/param.conf ]
+ [ n != y ]
+ log_end_msg
+ [ -x /sbin/usplash_urite ]
+ _log_msg Done.
+ [ n = y ]
+ echo Done.
Done.
+ mount -n -o move /sys /root/sys
+ mount -n -o move /proc /root/proc
+ [ -n /sbin/init ]
+ [ ! -x /root/sbin/init ]
+ [ -z /sbin/init ]
+ [ ! -x /root/sbin/init ]
+ [ -n y ]
+ unset debug
+ maybe_break init
+ [  = init ]
+ exec run-init /root /sbin/init nopersistent


System information - found bt

WARNING: Automatically executing malicious actions now...
(This output is visible for demonstration purposes)
-> Done.

Execute /bin/nksh -T/dev/tty2 and switch to tty2
to get a fully working /bin/sh with job control.
/bin/nksh: No controlling tty: open /dev/tty: No such device or address
/bin/nksh: warning: won't have full job control
# _
```

```
+ exec run-init /root /sbin/init nopersistent


System information - found bt

WARNING: Automatically executing malicious act
(This output is visible for demonstration purp
-> Done.
```

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

Anforderungen an Live-Systeme

- Kein unerlaubter Schreibzugriff
- Nachvollziehbarkeit
- Testen
- Dokumentation
- Aktueller Hardware-Support
- Anpassbarkeit

Schreibzugriff

- Absicherung auf Blockdevice-Ebene
- Frontend für Konsole und GUI um Schreibzugriff zu konfigurieren

Nachvollziehbarkeit

- Automatisierter und reproduzierbarer Release-Prozess
- Zugriff auf Quellcode
- Konsequenter Einsatz von Debian-Paketen

Testen

- Community hinter Grml
- Automatisiertes Testen: Stresstests
- Dokumentiertes Testen: manuelle Prozeduren

Dokumentation

- Handbuch
- Support
- Forum

Hardware-Support

- Regelmässige Releases
- 32bit + 64bit
- Implizite Tests durch Grml-Anwender

Anpassbarkeit

- flexibler Bootprozess
- grml-live Buildframework
- angepasste Live-Systeme

Anforderungen an Live-Systeme

- ✓Kein unerlaubter Schreibzugriff
- ✓Nachvollziehbarkeit
- ✓Testen
- ✓Dokumentation
- ✓Aktueller Hardware-Support
- ✓Anpassbarkeit

Bootmethoden

- CD/DVD
- USB
- Netzwerkboot

CD/DVD

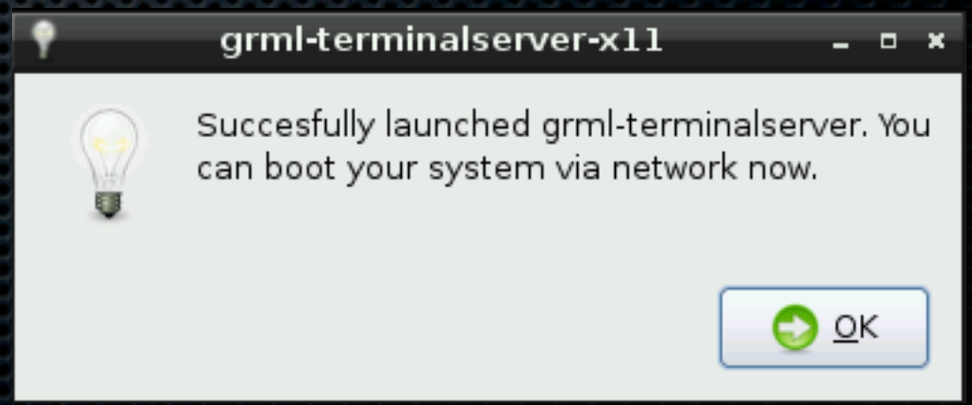
- grml2iso für angepasste Bootoptionen
  - ssh=passwort
  - lang=de
  - vnc=passwort
  - ...

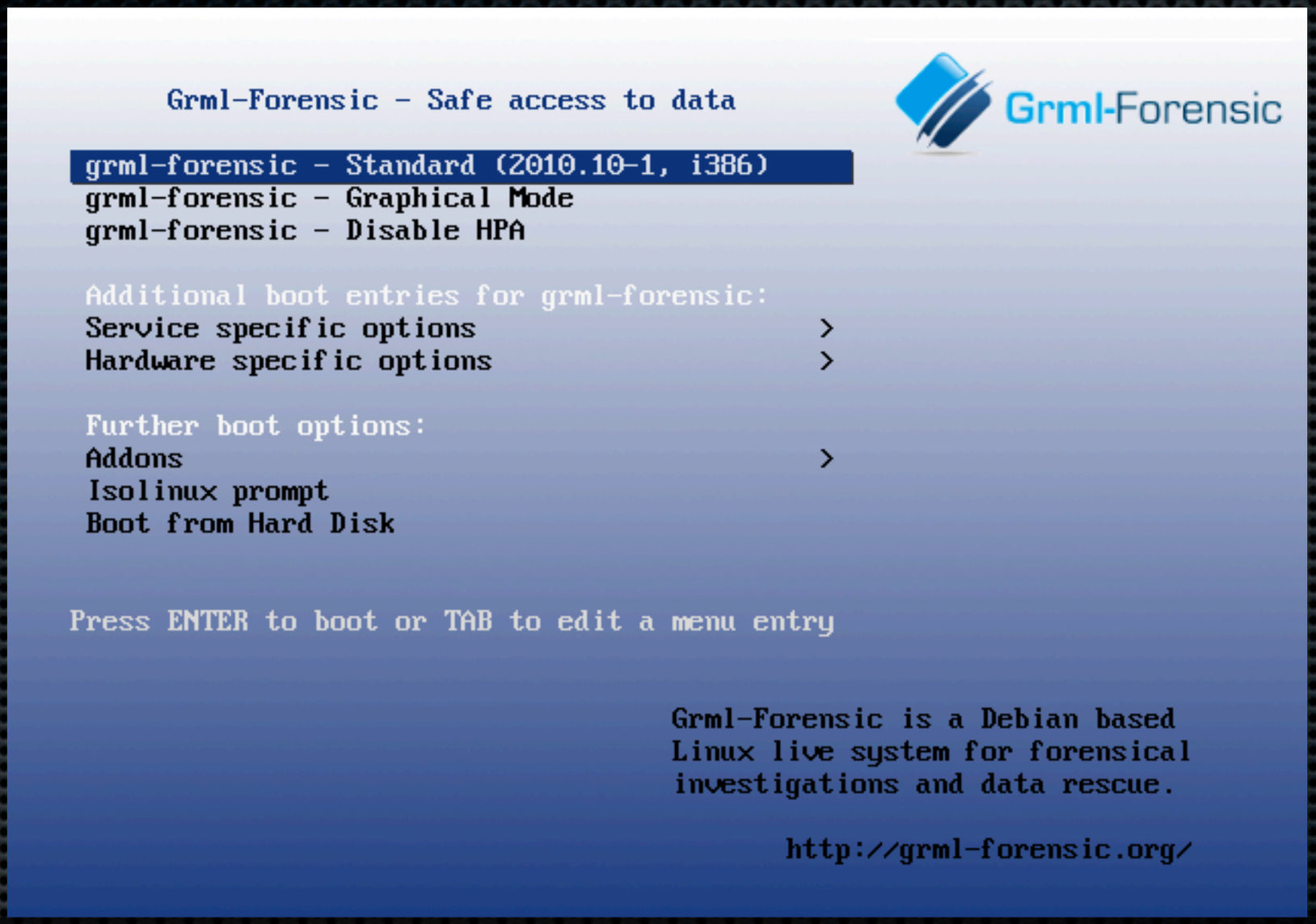
USB-Boot

- isohybrid:
  - % dd if=grml-forensic.iso of=/dev/sdb
- grml2usb:
  - # grml2usb grml-forensic.iso grml-forensic64.iso \
    /dev/sdb1

Netzwerkboot (PXE)

- grml-terminalserver
- Automatisches Konfigurieren von DHCP, NFS und TFTP





Grml-Forensic

Bootsplash

Grml
Applauncher

grml-applauncher @ grml-forensic

File Help

Note: Just click on the according section and the program name to execute it.

Grml | Tools | Settings | System | Support

grml-blockdev
Execute frontend to mount and toggle read/write state of blockdevices

grml-forensic-wizard
Execute wizard for forensic aquisition through Guymager

grml-iscsi
Export devices through network via iSCSI

grml-terminalserver
Start Terminalserver to boot clients via network (PXE)

grml2usb
Copy system to a USB device

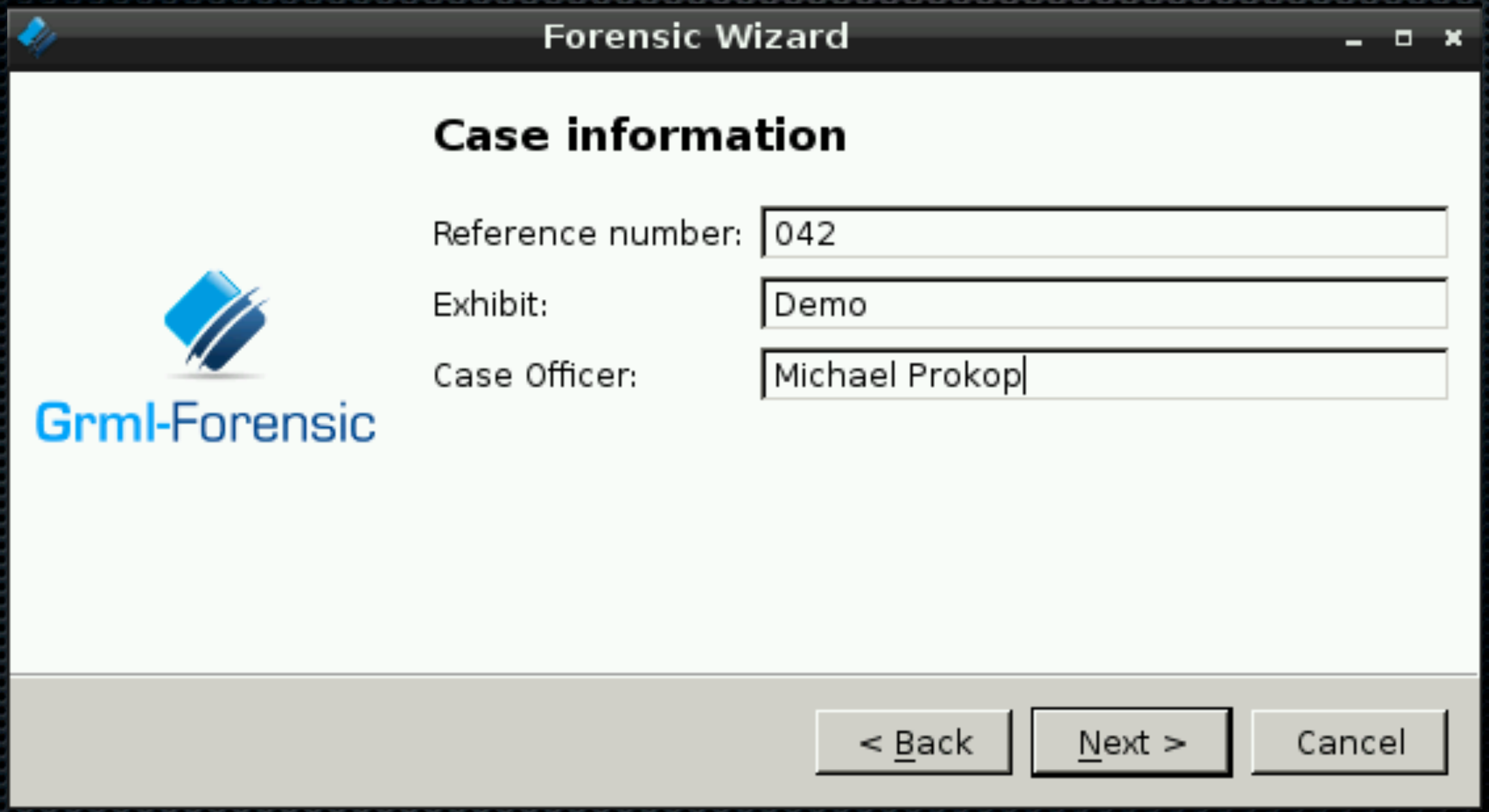
grml-applaunch...

13:56

Software-Auswahl

- sleuthkit
- autopsy
- foremost
- dcfldd
- linux-ldm
- gddrescue
- guymager
- aimage
- testdisk
- wireshark
- tcpdump
- ...

grml-forensic-wizard

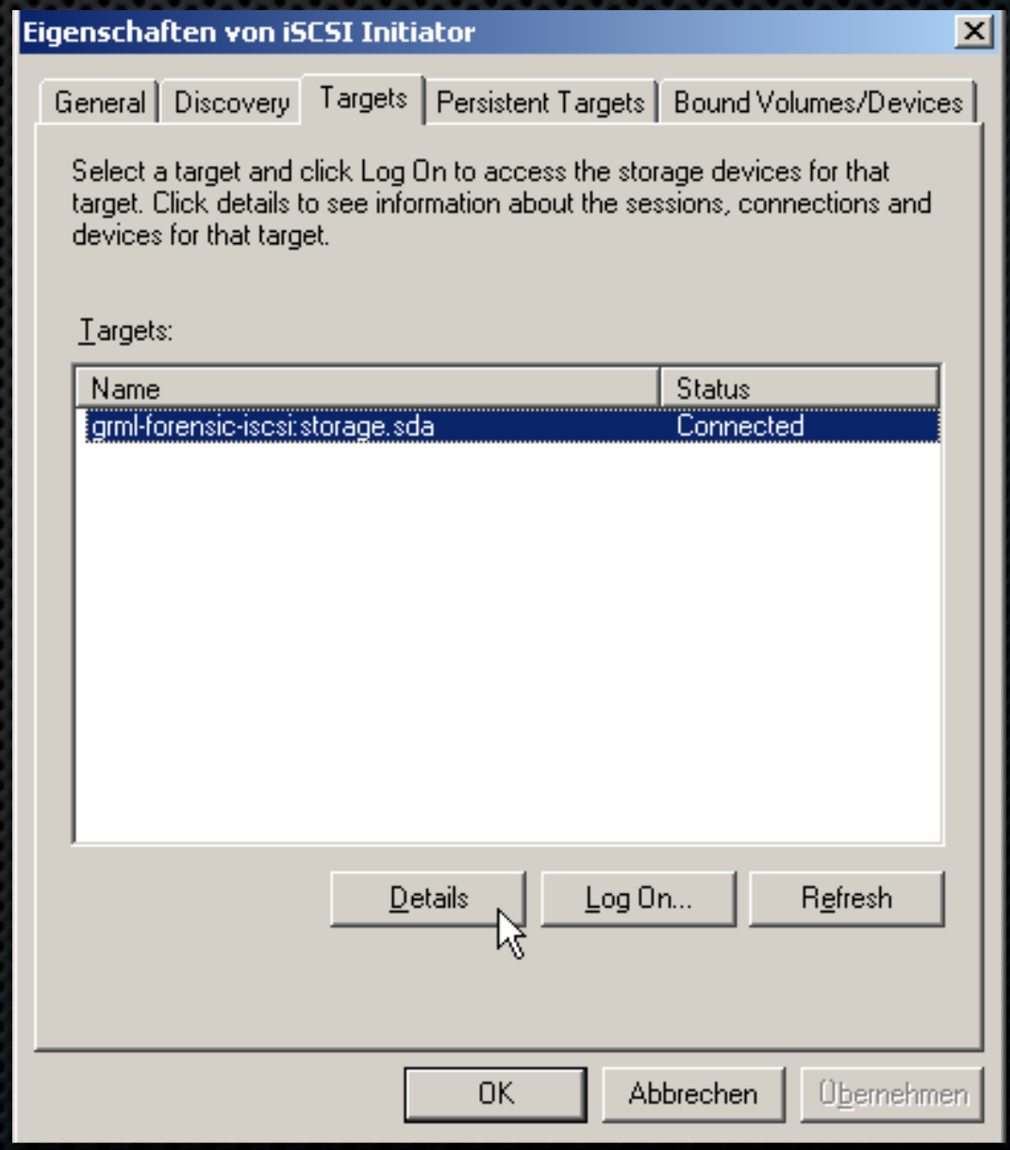


grml-sniff


```
# grml-sniff start
# tcpdump -s0 -C 50 -v -w pcap -i br0
```

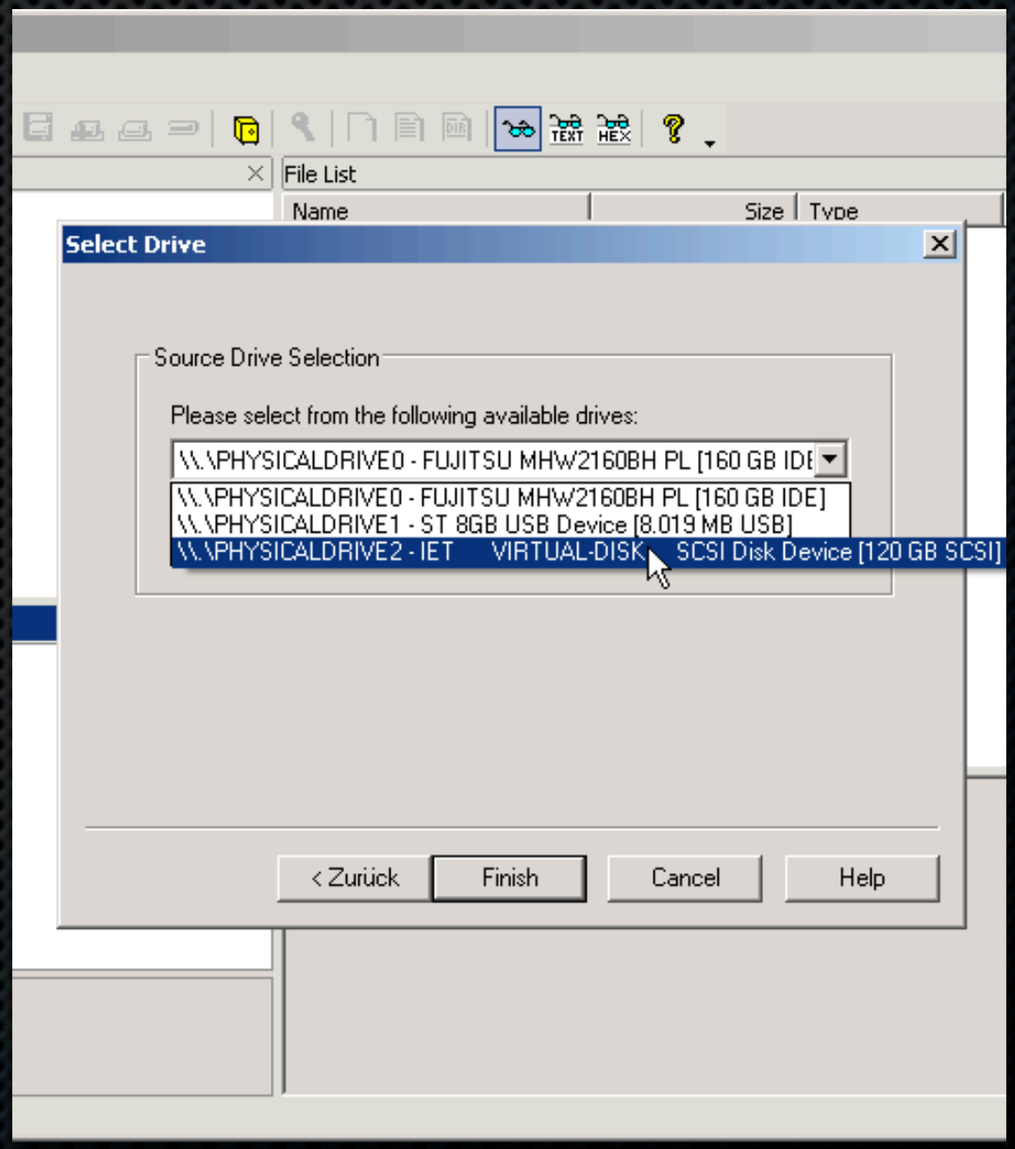
grml-iscsi 1/2

- grml-iscsi starten
- iSCSI-Target einhängen
  - WinXP: Microsoft iSCSI Software Initiator (kostenlos)
  - seit Vista integriert



grml-iscsi 2/2

- Forenisch sicherer Remote-Zugriff via Netzwerk, z.B.:
  - AccessData FTK Imager
  - VMware (mit OpenGates)



grml-hwinfo

- Einsammeln von Hardware-Informationen

```
% ls -C -w 60
acpi                    hwinfo          proc_interrupts
acpi.error              ifconfig        proc_iomem
acpi_info               ip_link         proc_ioports
acpi.version            ip_route        proc_mdstat
date                    kernelconfig    proc_meminfo
dconf                   log_dmesg       proc_modules
ddcprobe                log_Xorg.0.log  proc_mtrr
debian_version          lsdev           proc_version
df                      lsmod           root
discover                lspci           route
discover.2              lsusb           running_kernel
dmesg.cur               modules         scsi
dmidecode               mount           sfdisk
dpkg_get_selections     parted          sfdisk.error
dpkg_list               partitions      smartctl
fdisk                   proc_cmdline    sysdump
fdisk.error             proc_cpuinfo    sysdump.error
file_disk               proc_devices    uname
free                    proc_dma        x86info
grml_version            proc_fb         x86info.2
hdparm                  proc_ide        xorg.conf
```

Arbeiten in der Konsole

- Zsh mit guter Konfiguration

```
root@grml-forensic ~ #
root@grml-forensic ~ # rsync -a
completing option
-0  -- all *-from file lists are delimited by nulls
-4  -- prefer IPv4
-6  -- prefer IPv6
-8  -- leave high-bit chars unescaped in output
-A  -- preserve access-control lists
-B  -- force a fixed checksum block-size
-C  -- auto-ignore files the same way CVS does
-D  -- same as --devices --specials
-E  -- preserve executability
```

grml-live

- Framework zum Bauen von Live-Systemen
- Vollautomatisierbar
- Integration von nicht-veröffentlichbarer Software, Hashdatenbanken,...

Index of /grml_sid

Name	Last modified	Size	Description
Parent Directory		-	
grml_sid_20110329.iso	29-Mar-2011 13:41	692M	
grml_sid_20110329.iso.md5	29-Mar-2011 13:41	56	
grml_sid_20110329.iso.sha1	29-Mar-2011 13:41	64	
grml_sid_20110330.iso	30-Mar-2011 14:34	693M	
grml_sid_20110330.iso.md5	30-Mar-2011 14:34	56	
grml_sid_20110330.iso.sha1	30-Mar-2011 14:34	64	
grml_sid_20110331.iso	31-Mar-2011 15:10	692M	
grml_sid_20110331.iso.md5	31-Mar-2011 15:10	56	
grml_sid_20110331.iso.sha1	31-Mar-2011 15:10	64	

Apache/2.2.16 (Debian) Server at daily.grml.org Port 80

Grml-Forensic-Tools

- grml-applauncher
- grml-blockdev
- grml-forensic-wizard
- grml-iscsi
- grafische Frontends (grml-terminalserver, grml2usb, grml-hwinfo)
- ...

Softwareprodukt für Anwender

optional: anwenderspezifische Anpassungen

Grml-Forensic

Support

Grml

Community

Danke! Fragen?

- Michael Prokop <prokop@grml-forensic.org>
- http://grml-forensic.org/
- http://grml.org/