grml-forensic

Debian based Live System for Forensic Investigations

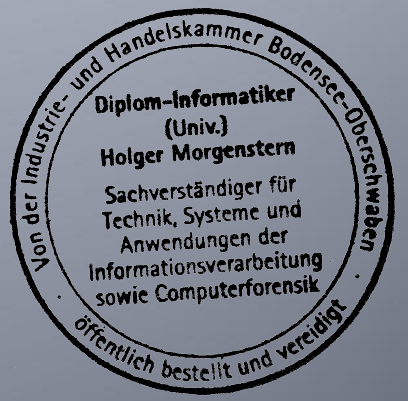
Holger Morgenstern <morgenstern@gutachten.info>
Ralf Moll <Ralf.Moll@lka.bwl.de>
Michael Prokop <prokop@grml-forensic.org>

IMF 2009
5th International Conference on
IT Security Incident Management & IT Forensics

Holger Morgenstern

Diplom-Informatiker

www.gutachten.info



Entitled by the chamber of commerce Bodensee-Oberschwaben, Germany as official approved and sworn expert witness for IT-Engineering, IT-Systems, IT-Applications and computer forensics

Ralf Moll

LKA Baden-Württemberg
State bureau of investigation

IT-Forensics

Since 2001 in the area of IT-Forensics

Use of Linux-Boot-CDs since 2002

Michael Prokop

Project leader of Grml

Official Debian Developer

Member/Admin of the Debian Forensic team

Founder of Security-Treff-Graz

IT and Open Source consultant

Author of a german book named „Open Source Projektmanagement – Softwareentwicklung von der Idee zur Marktreife“
[Release date: end of 09]

Boot CDs - Pros

Why use Boot CDs?

- No need for hardware-write-blockers
- Complex „multi-harddisk-scenario“
  like FC-SAN, RAID6
- Difficult disassembling
- More possibilities than plain
  acquisition

Boot CDs - Cons

Be aware of:

- Boot-order
- Warranty / Validation
- Linux and Mr. Root
- Mr. Murphy

Boot Requirements

Requirements Specification:

- No write access
- Traceability
- Testing
- Documentation
- Periodic release cycle
- Customizing

Supply of Boot CDs

Grml!

Grml?

- first official release in 2004
- Debian based Linux Live system
- especially for sysadmins
- i386 + amd64

Known for „unusual“ release names

Lackdose-Allergie

Hustenstopper

Schluchtenscheisser

Skunk

Winterschlapfn

Funkenzutzler

Dioptrienotto

Meilenschwein

Eierspass

Bootenschnitzl

Tokolytika

Some selected Grml users

credativ

LINBIT
YOUR WAY TO HIGH AVAILABILITY

Globalways AG
München | Stuttgart | Frankfurt am Main

UNIVERSITÀ DI BOLOGNA A.D.1088

SuccessFactors
People Performance

TU Graz

lola!

INQNET

LINZ AG TELEKOM

Hardworx Netzwerke

sip:wise

proNet
INTERNET & MULTIMEDIA SERVICES

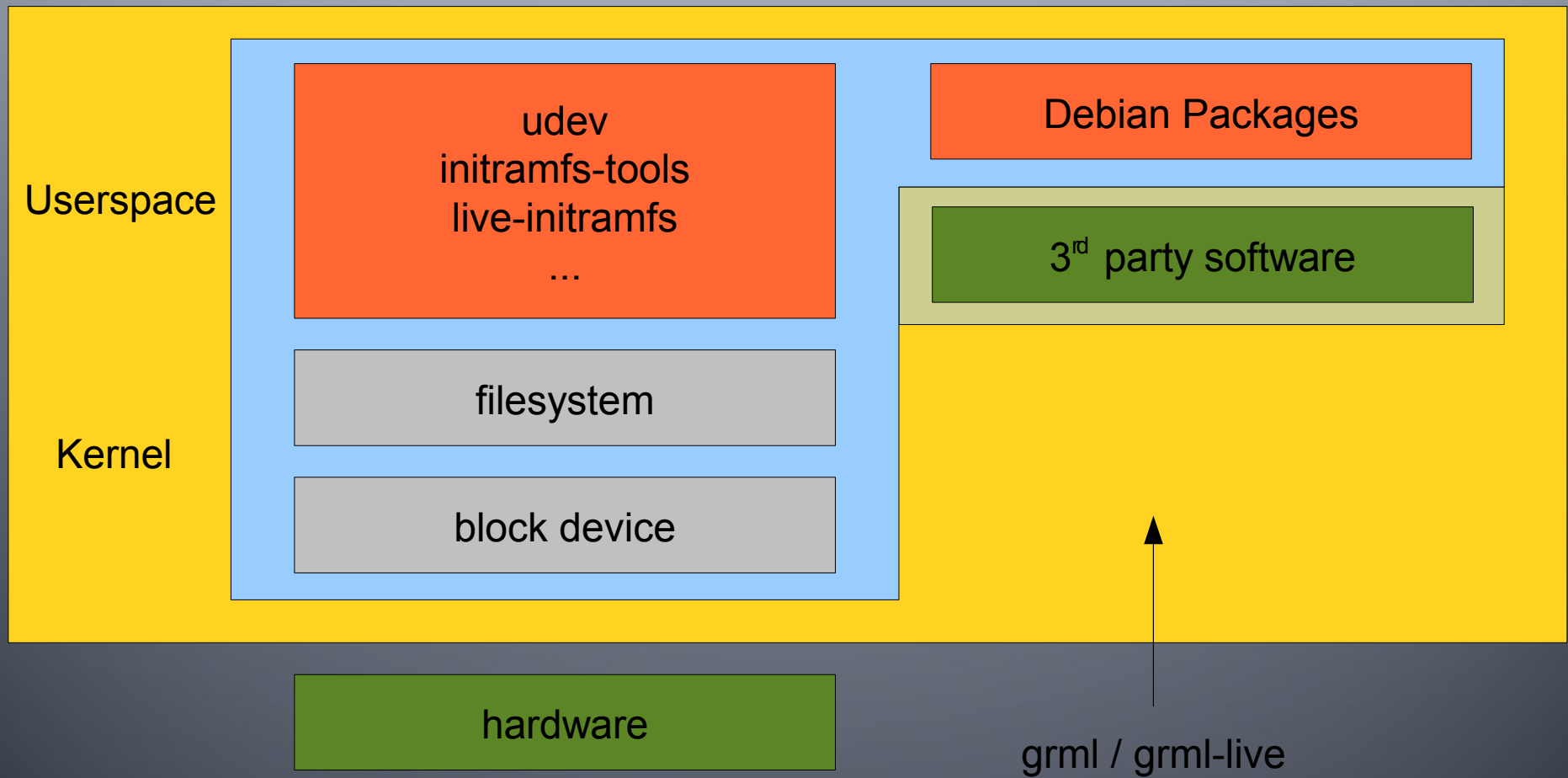
Why another forensic live system? 1/2

- Most forensic systems are „hacks“:
  - no clean packaging work
  - undocumented modifications
  - lack of contribution back to base distribution
  - no sources (or not easy) available/ accessible
  - no/small communities
  - modify existing blockdevices (e.g. journal replays)

Why another forensic live system? 2/2

- Advantages of Grml:
  - clean Debian packaging work
  - documented (build system, tools,...)
  - official Debian developer + member of Debian forensic team
  - sources fully available to the public
  - well established community
  - verified system which doesn't modify any blockdevices
  - excellent knowledge in core technologies (maintenance of and contributions to kernel, initramfs-tools, live-initramfs, udev,...) + upstream of grml-live

Core technologies?



What's under the hood

- Debian
- official Debian packages
  - several of the Debian Forensic project
- grml packages (Open Source and publically available)
- Aufs used as overlay system
- SquashFS as compressed root-fs

Zsh?

- Zsh!
  - great pre-configuration on grml
  - powerful and modular
  - useful aliases+functions
  - great tab-completion!
  - zsh-lovers: http://grml.org/zsh/
  - Configuration can be used on non-grml systems as well: http://grml.org/console

Zsh – Nice stuff

- sharehistory
- hashing (~doc, ~deb, ~www,...)
- which? =vim
- vared PATH
- vcs_info
- power completion – abbreviation expansion (grml special):
  - $CMD L,. → $CMD | less
  - $CMD C,. → $CMD | wc -l
  - ...

Zsh - Keybindings

- Ctrl-e d → 2009-04-30
- Esc-e → open cmdline in editor
- Esc-h → run-help
- Esc-. → insert-last-word
- Esc-m → insert-last-typed-word
- Ctrl-o s → sudo-command-line
- Ctrl-_ → undo
- Esc-d → transpose-words
- Cursor up → up-line-or-search

Commonly used boot options

- grml nodhcp
- grml ssh=password
- grml2ram / grml toram=file.squashfs
- grml lang=de / keyboard=de
- ...

grml2usb

- Install grml bootable on USB pen
- grml2usb provides support for multi-ISO:

```
# grml2usb \
   --bootoptions „ssh=IMF09“ \
   grml-medium_2009.05.iso \
   grml64-medium_2009.05.iso \
   /dev/sdb1
```

grml-x

- wrapper for starting Xorg
- generates xorg.conf automatically
- starts specified Window Manager

grml-bridge

Simple bridge setup for sniffing:

- 2 NICs
- boot Grml with „grml nodhcp“
- bridge setup:

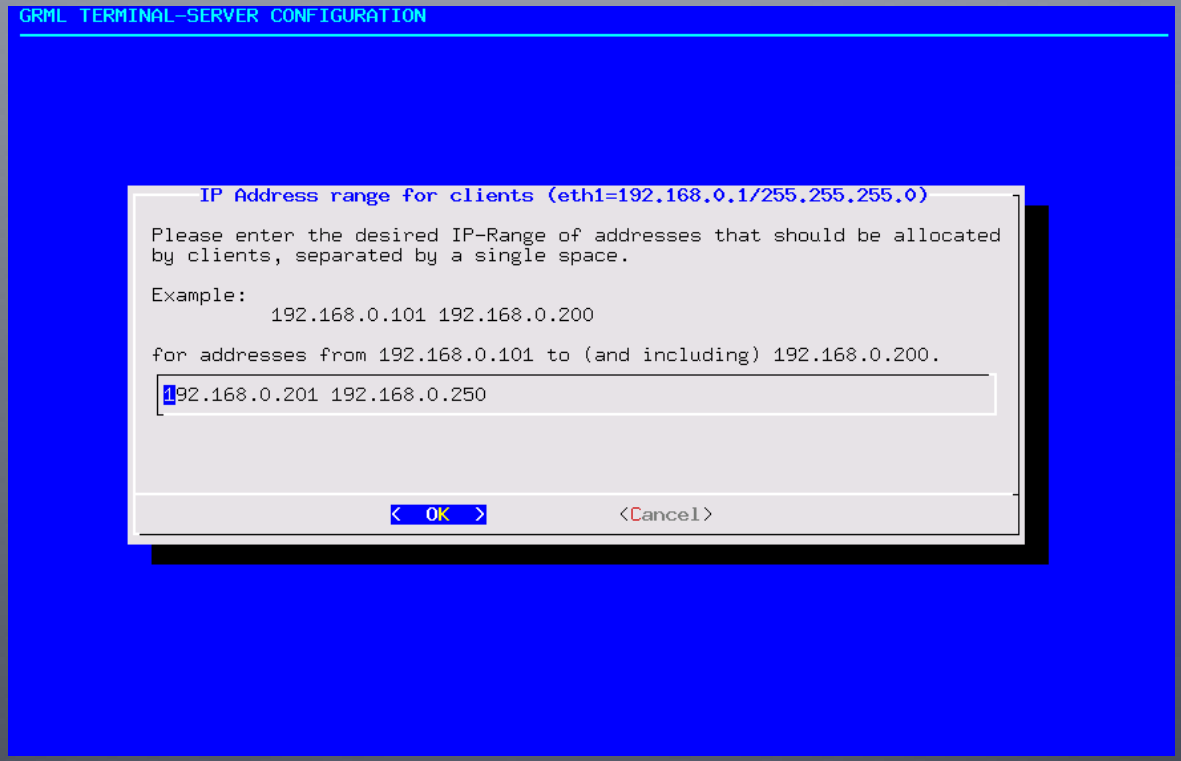
```
# sed -i 's/BRIDGE_CONFIG=.*/BRIDGE_CONFIG=NONE/' \
    /etc/grml/routersetup
# grml-bridge start
```

- PS: grml-sniff will be shipped with next grml release

grml-terminalserver

- Use Case: boot grml on several clients
- boot grml via PXE – fast, simple and easy:

```
# grml-terminalserver
```



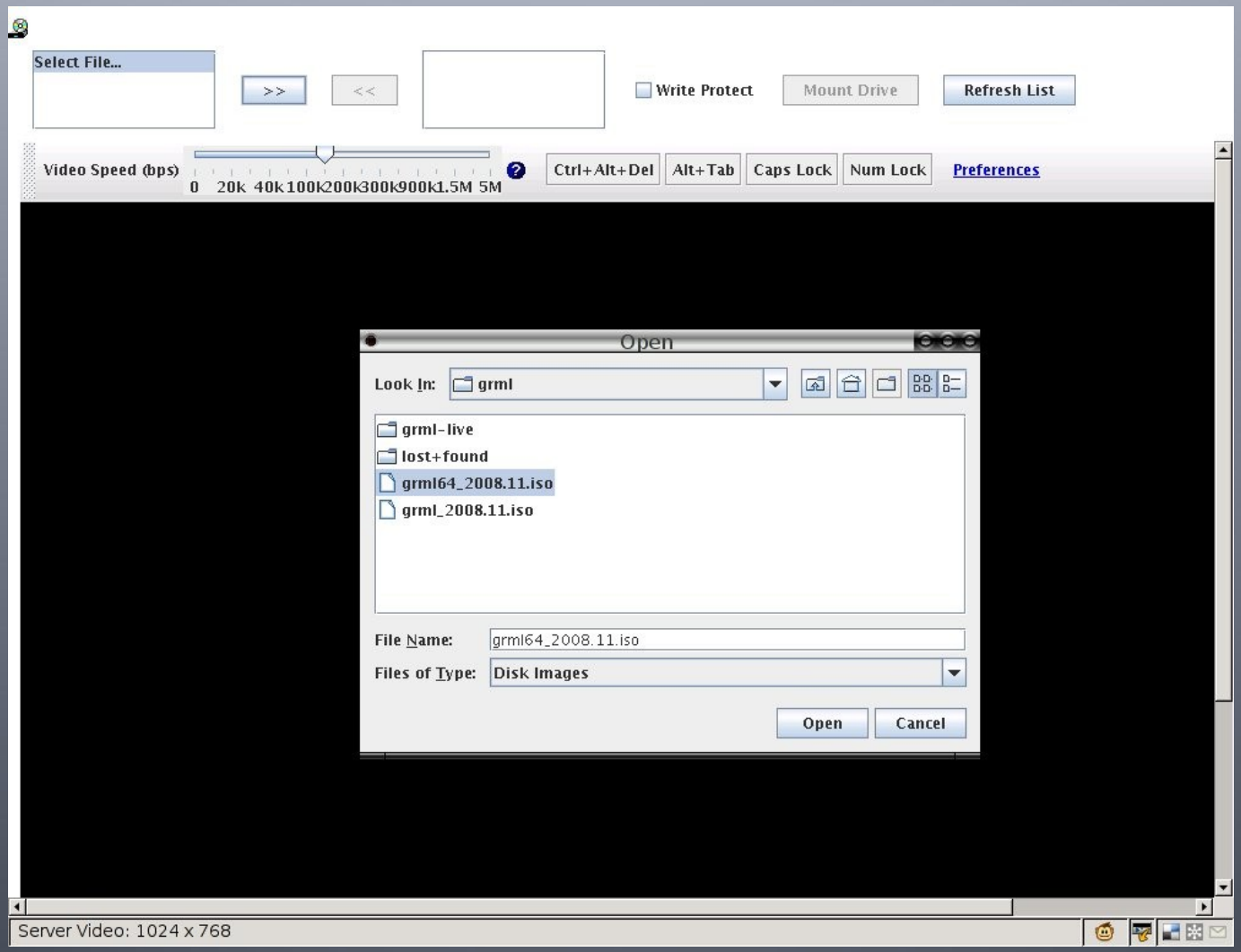
Boot Grml via PXE *without* NFS

- Extract kernel, initrd + squashfs from ISO
- Webserver provides files
- pxelinux.cfg/default:

```
LABEL grml-small-2009.05
   MENU LABEL grml-small 2009.05 (HTTP)
   kernel grml/2009.05/small-linux26
   append initrd=grml/2009.05/small-minirt26.gz \
   boot=live \
   fetch=http://example.org/grml/grml-
   small.squashfs \
   nodhcp noeject vga=791 ssh=IMF09
```

- see http://www.pro-linux.de/news/2008/13569.html

Boot via Remote Adapter



grml-live

- Framework for remastering Debian based Live Systems
  - official build system for grml
- Based on FAI
  - Full Automated Installation
- Class based
  - Software selection is just a simple plain text file!
- Fully automatable
  - daily.grml.org

Forensic branch in grml-live

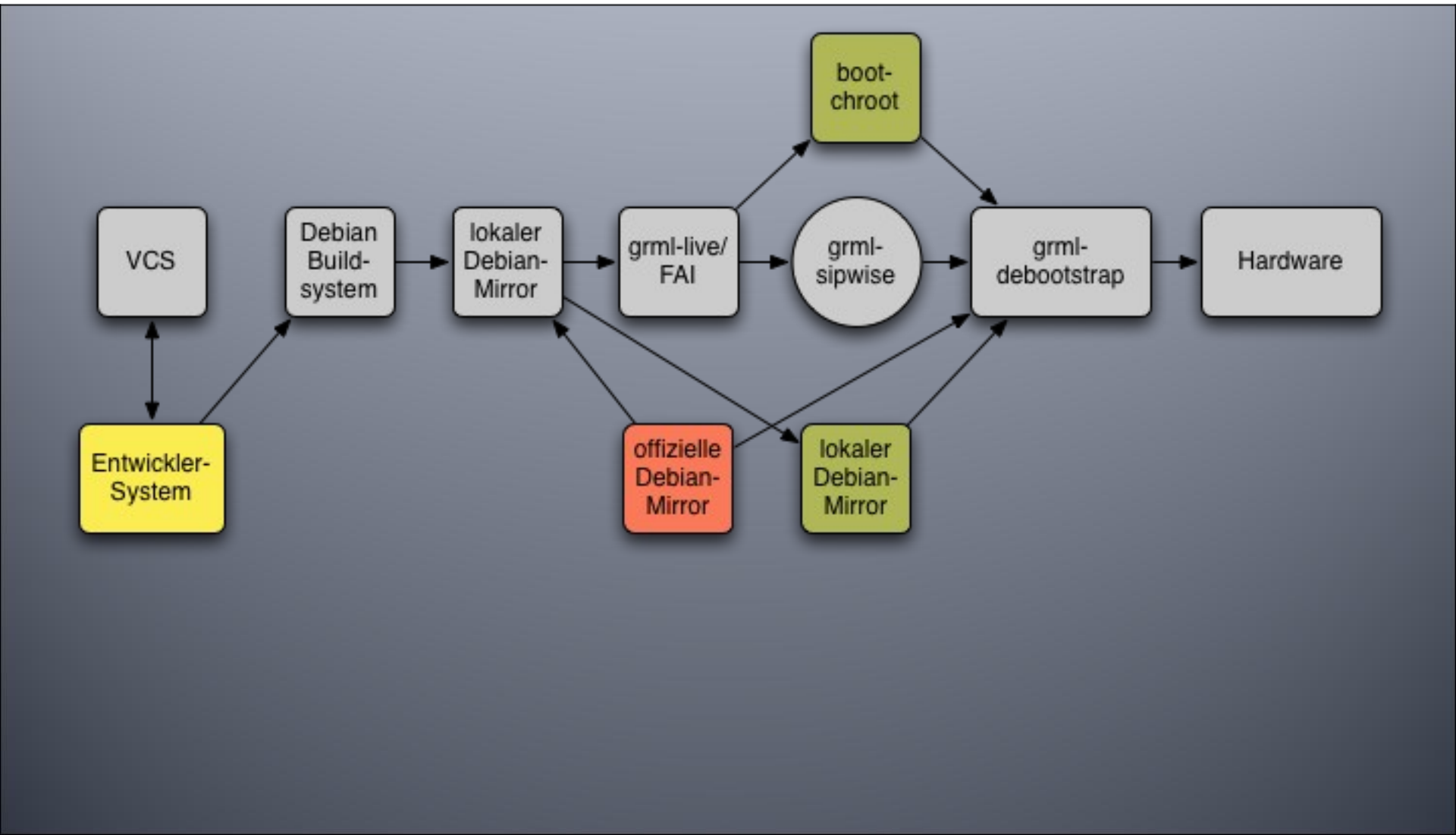
- Package definition:
  /etc/grml/fai/config/package_config/GRML_FORENSIC

  → let's have a look at it

Use case: Juxlala

- Juxlala = Live System for small kids
- grml-live as build framework
- Customised Live System without the need to maintain Kernel & CO

Use case: Sipwise



Tricks for booting the ISO

- `grml bootfrom=/dev/sda1`
  → „force“ a device
- `grml isofrom=/dev/sda1/grml.iso`
  → directly boot specified ISO
- `grml findiso=/grml_2009.05.iso`
  → search for specified ISO

Custom Configuration 1/2

- DCS (Debs, Configuration + Scripts)
  - save-config / restore-config
  - FS-Label GRMLCFG:
    - grml.sh → your own script
    - config.tbz → configuration
  - http://grml.org/config/

Custom Configuration 2/2

Root-Persistency:

- live-snapshot -d ...
- FS-Label „live-rw“
- Bootoption „persistent“
- http://wiki.grml.org/doku.php?id=persistency

iSCSI-Setup

- Boot
- iSCSI-Setup:

```
# cat > /etc/ietd.conf << EOF
Target grml-forensic-iscsi:storage.sda
Lun 0
Path=/dev/sda,Type=fileio,IOMode=ro
Alias sda.file
HeaderDigest CRC32C
DataDigest CRC32C
EOF
# sed -i 's/false/true/' /etc/default/iscsitarget
# /etc/init.d/iscsitarget start
```

- Access via Windows:
  - Vista: native / XP: Microsoft iSCSI Software Initiator
  - Access with Forensic Software (FTK Imager, EnCase, XWF,...)

Live-Demo

- Let's have a look at the iSCSI setup using grml-terminalserver

Grml-Forensic?

- special flavour of Grml
- developed + backed by Grml Solutions + the Forensic-Geeks e.V..
- to be released soon...

grml vs. grml-forensic

	grml	grml-forensic
Debian release	unstable (→ testing?)	testing (planned)
Default boot method	forensic just as option	secure forensic mode enabled by default
Default Boot mode	console	X Window System („nostartx“ to disable that)
Software	mainly sysadmin stuff	especially for forensic and data rescue investigations
Backing	community	business

Contribute / Become a partner / Contact

- http://grml-forensic.org/ (WIP)
- Inform about release of grml-forensic?
  - notify-me (at) grml-forensic.org
- Contribute?
  - http://ml.grml.org/mailman/listinfo/grml-forensic
  - #grml-forensic on irc.freenode.org
- Contact?
  - contact (at) grml-forensic.org
  - GPG Key-ID: 0x37E272E8
  - +43 664 1646346

Thanks

Holger Morgenstern
morgenstern@gutachten.info

Ralf Moll
Ralf.Moll@lka.bwl.de

Michael Prokop
prokop@grml-forensic.org

http://grml.org/
http://grml-forensic.org/