BACKUP – Datensicherung unter Linux

Von Anwendern – Für Anwender:
Datensicherung in Theorie und Praxis!

Teil 4: Datenrettung

Eine Vortragsreihe der
Linux-User-Group Ingolstadt e.V. (LUG-IN)
in 4 Teilen

Die Vortragsreihe

1. Datensicherung – Eine Einführung
2. Eine Ebene tiefer – Konsolenwerkzeuge
3. Bacula – Backup im großen Maßstab
4. Datenrettung – Wenn nichts mehr hilft

Heutiger Vortrag

Datenrettung – Wenn nichts mehr hilft

oder auch:

Was kommt nach der **Panik?**

Was lässt sich wiederherstellen?

Was eher nicht ...

Die Gliederung

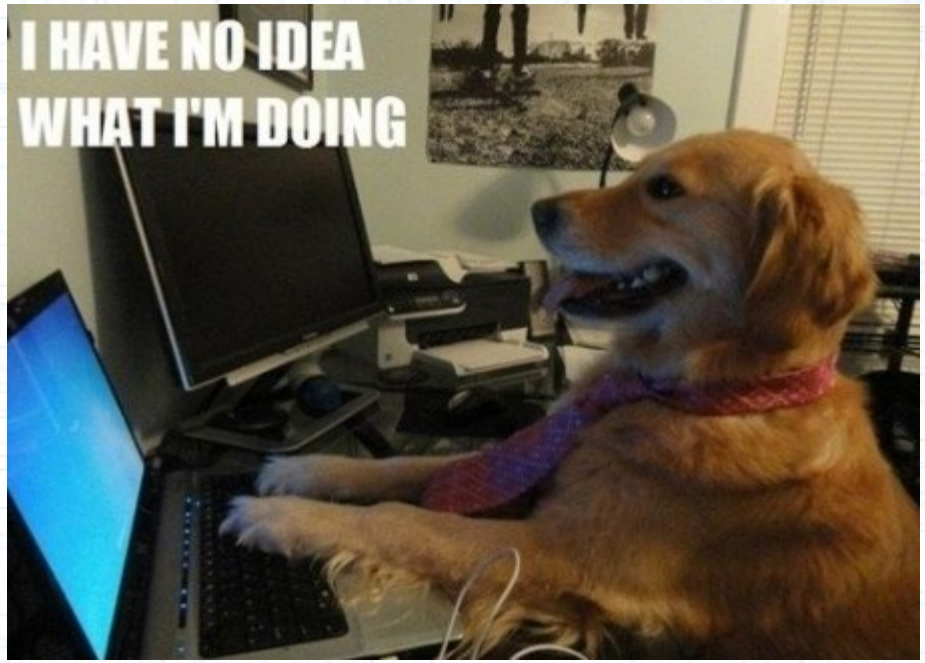
I. Vorwort

II. Theorie – Aufbau einer Festplatte

III. Praxis – Diagnose und Wiederherstellungsversuch

IV. Sonstiges

I. Vorwort



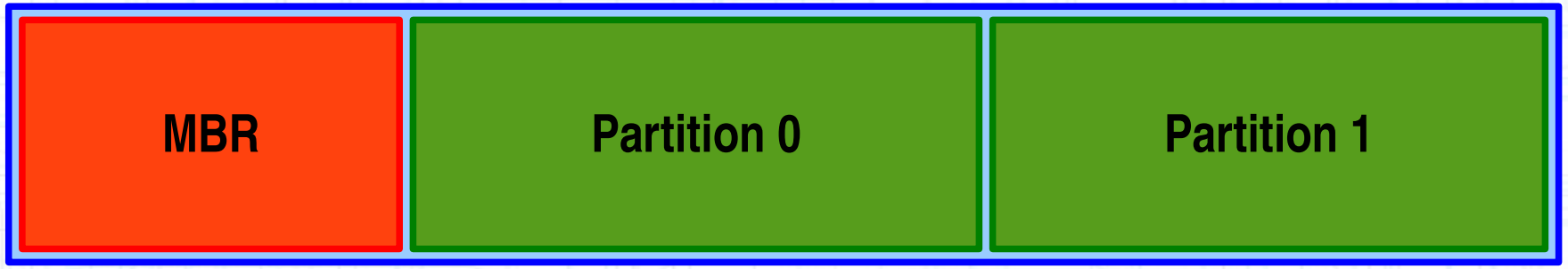
Wie wichtig sind mir meine Daten?

Wichtig!? => **FINGER WEG**

II. Theorie – Aufbau einer Festplatte

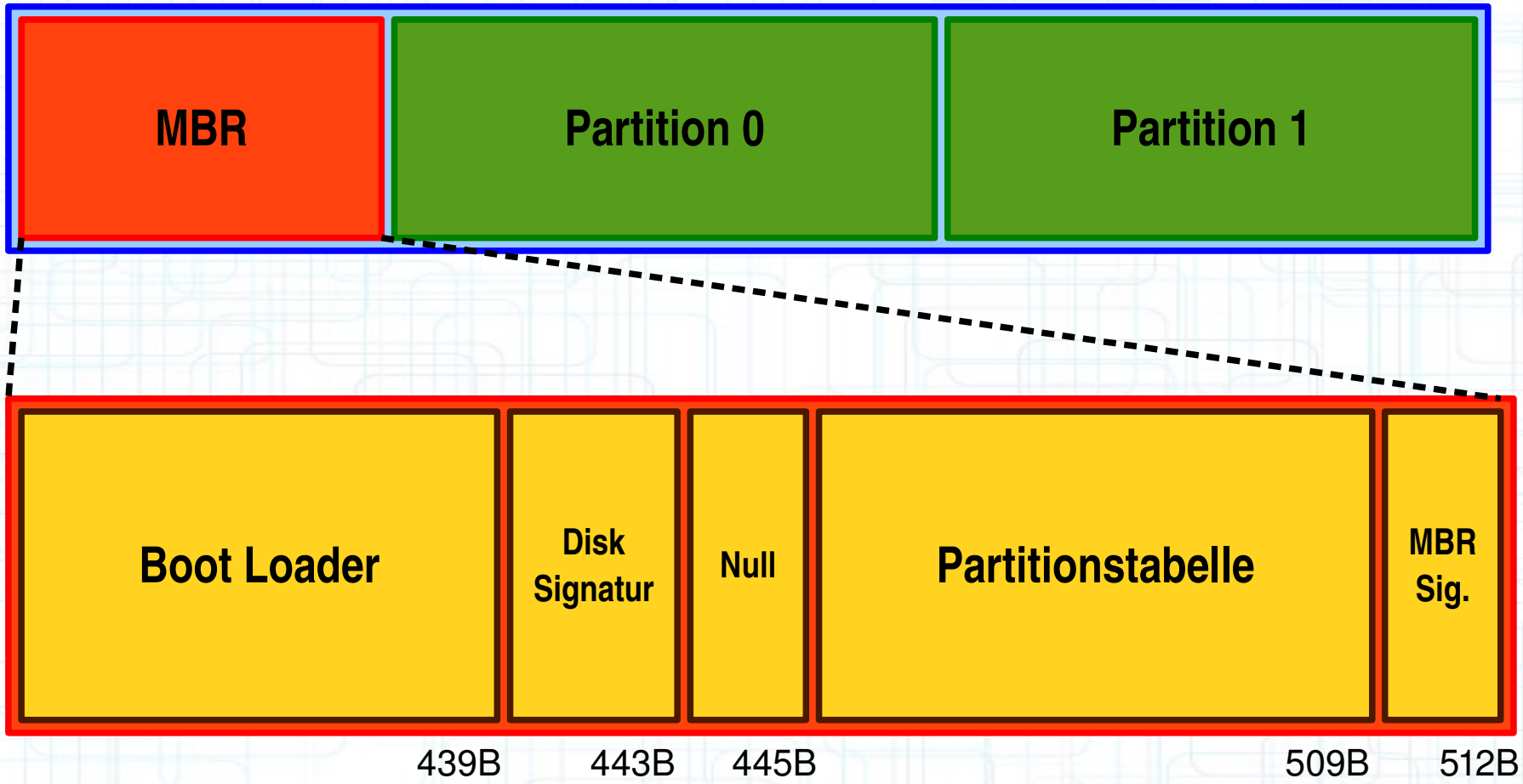
1. MBR
2. Partitionstabelle
3. Boot Loader
4. Dateisystem Aufbau (ext3)

1. MBR



1. Boot Loader wird vom BIOS aufgerufen
2. Sucht in Partitionstabelle nach primären Partitionen
3. Lädt den Bootsektor
4. Betriebssystem wird ausgeführt

1. MBR


MBR
Partition 0
Partition 1
Boot Loader
Disk Signatur
Null
Partitionstabelle
MBR Sig.
439B
443B
445B
509B
512B

2. Partitionstabelle

Enthält die folgenden Einträge:

1. Bootfähig: Ja/Nein
2. CHS Eintrag des ersten Sektors
3. Partitionstyp
4. CHS Eintrag des letzten Sektors
5. Startsektor
6. Anzahl der Sektoren in der Partition

3. Boot Loader: Grub (legacy)

Grub arbeitet in Abschnitten (stages):

- **Stage 1:** Einstiegspunkt ist der MBR, da MBR zu klein, zeigt auf Stage 2. Pointer über:
  - Sektor → Stage 2
  - Partitionsnr. + Dateipfad → Stage 1.5
- **Stage 1.5:** Lädt Dateisystemtreiber, stößt Stage 2 an
- **Stage 2:** Kann sich überall auf der Festplatte befinden, liest die Konfigurationsdatei (menu.lst / grub.cfg) ein. Zeigt das Bootmenü, läd Kernel, initrd, ...

4. Dateisystem Aufbau (ext3): Superblock + Inodes + Verzeichnisse

Informationen im Superblock (Superblock ist immer 1024 Byte groß):

- Dateisystem Typ
- Größe des Dateisystems
- Informationen über Metadaten (z.B: Liste freier Inodes)

Inodes:

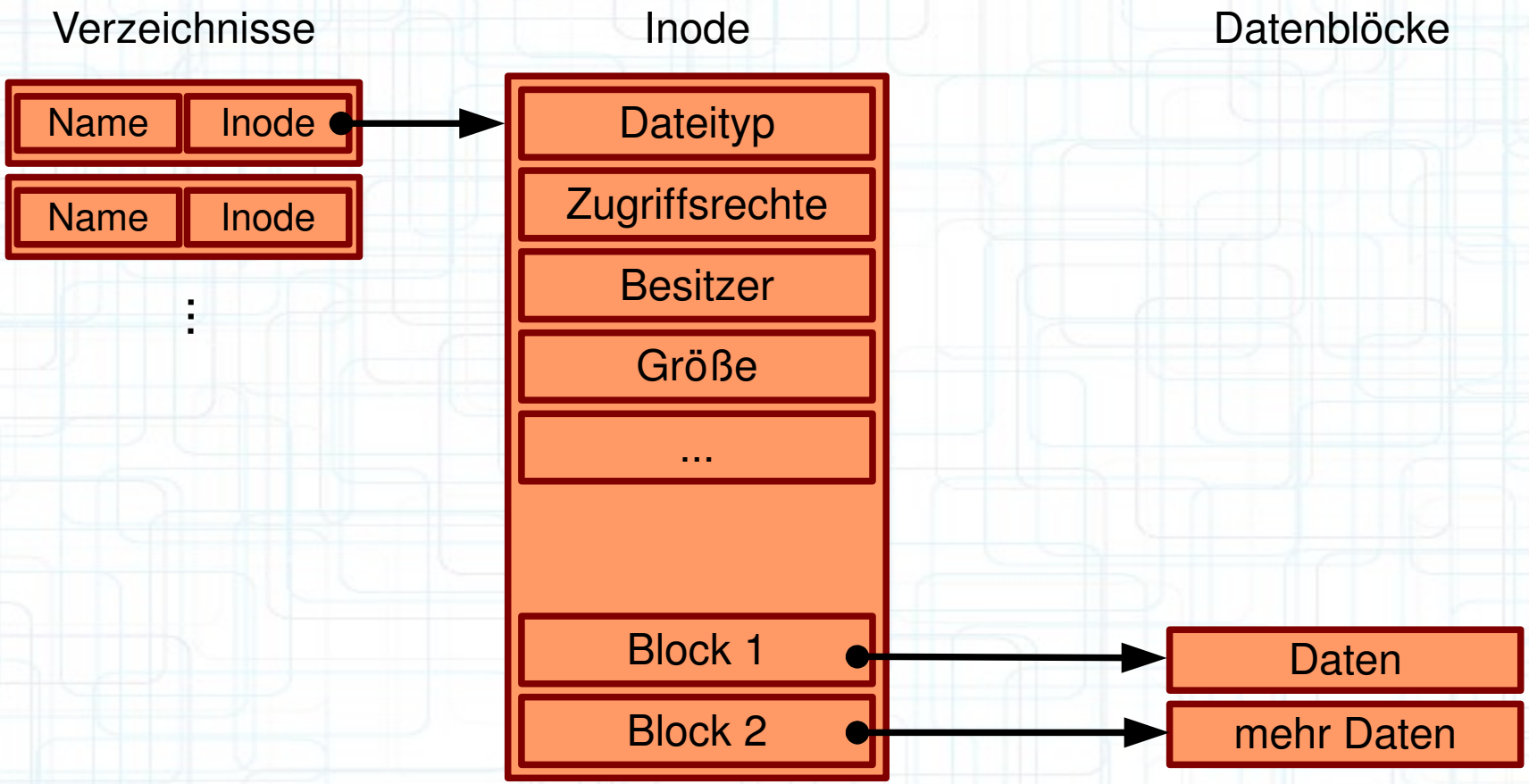
- „Ein Inode ist eine komplette Datei ohne den Dateiinhalt“
- Enthält Metadaten der Datei (laut POSIX Standard: Rechte, Zeitstempel, Größe, ...)
- Mapping zwischen „Inode Nummer“ und Blöcken auf der Festplatte

4. Dateisystem Aufbau (ext3): Superblock + Inodes + Verzeichnisse

„Verzeichnisse sind auch nur Inodes“

- Das Wurzel Verzeichnis von Linux („/“) ist auch ein Inode. Inode Nr. 2 enthält immer diese Daten (Nr. 1 enthält defekte Blöcke)
- Innerhalb von Inode Nr. 2 sind wiederum die Inode Nummern der Verzeichnisse unterhalb von Root („/“)
- Dieser wiederum enthalten die Inode Nummern für Verzeichnisse unterhalb ihres eigenen Verzeichnisses ...

4. Dateisystem Aufbau (ext3): Superblock + Inodes + Verzeichnisse



Ich wiederhole...

III. Praxis – Diagnose und Wiederherstellungsversuch

1. Einzelne Datei gelöscht
2. Boot Loader
3. Partitionstabelle
4. Hardware defekt
   - 4.1. S.M.A.R.T
   - 4.2. ddrescue (dd_rescue + dd_rhelp)

1. Einzelne Dateien gelöscht - Allgemeine Tipps

1. Cool bleiben / keine Panik
2. Überschreibt mein nächstes Backup mein jetztiges mit Müll?
3. Schreibzugriffe verhindern / Single User Mode (init 1)
4. Partition aushängen / Read Only mounten
5. An das Journal denken
6. Kopie des Datenträgers erstellen (dd / ddrescue)

1. Einzelne Dateien gelöscht

- Problem: ext3 überschreibt Block Pointer mit Nullen
- Ansätze:
  - Datei noch lesend geöffnet?
    - „lsof“ ist dein Freund: „lsof -a +L1 /“
    - Zeigt offene Dateien die „unlinked“ sind:

```
COMMAND  PID   USER   FD   TYPE DEVICE SIZE/OFF NLINK    NODE NAME
roxterm 1366 daniel  12u   REG    8,5    14552     0 2383883 /tmp/vteBVB8AW (deleted)

cat /proc/1366/fd/12 > gerettet.txt
```

  - Das Journal:

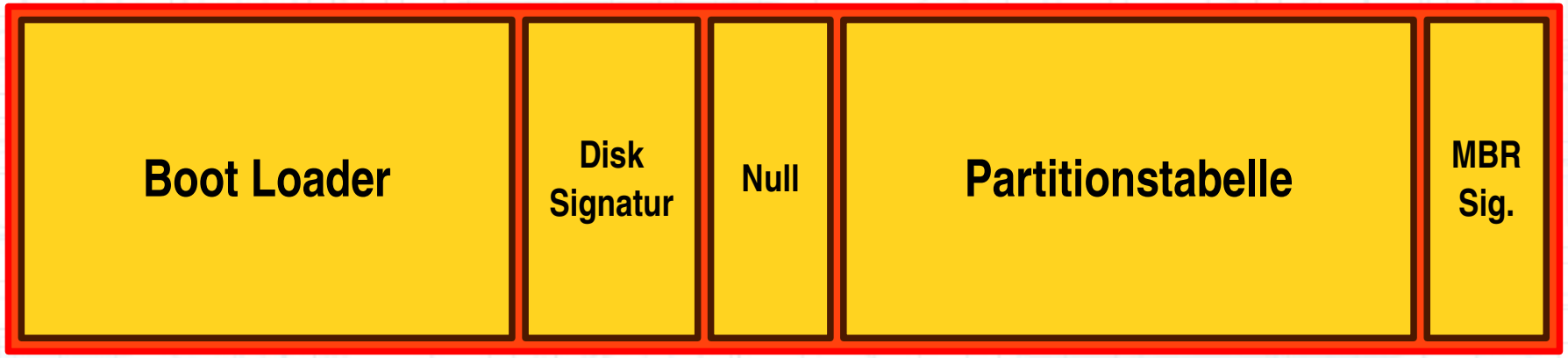
    - ext3grep (Carlo Wood): sehr mächtiges Tool, nutzt das Journal des Dateisystems aus
    - ext3undelete
    - ext4magic

1. Einzelne Dateien gelöscht

- Weitere Ansätze:
  - Header / Footer
    - foremost
    - scalpel
    - Photorec (Christophe Grenier):
      - durchsucht Superblock / Boot Sektor um Blockgröße heraus zu finden
      - Checkt jeden Block mit Hilfe von Signaturen

- Viele Tools die ich vergessen habe ...

Wir erinnern uns...



2. Boot Loader defekt

- Nachträgliche Installation von Windows
  - Windows überschreibt Boot Loader ohne zu fragen!
  - Danach kein Zugriff auf Linux System möglich
- Abhilfe:
  - Neu schreiben des Boot Loaders mithilfe einer Live CD
  - z.B.: http://www.supergrubdisk.org/

3. Partitionstabelle korrupt

- Gründe: Anwender, Virus, …
- Tool der Wahl: „TestDisk“ (Christophe Grenier)
- TestDisk kann:
  - Partitionstabellen wiederherstellen
  - Boot Sektoren wiederherstellen
  - Backups von Superblöcken wiederherstellen

4. Hardware defekt – S.M.A.R.T.

- Self-Monitoring, Analysis, and Reporting Technology
- Selbstdiagnose der Festplatte auf Hardwareebene
- Läuft im Hintergrund ab
- 3 Kategorieren von Werten
  - Online aktualisiert
  - Offline aktualisiert
  - Self Test (nur manuell)
- Tool der Wahl: smartctl
  - sudo smartctl -A /dev/sda
  - sudo smartctl -t long /dev/sda
- Nur Indiz, kein Beweis

4. Hardware defekt - ddrescue

1. Kopieren der defekten Festplatte **VOR** Wiederherstellungsversuchen
2. Auslesen der Festplatte Bit für Bit mit dd
3. Vorteile von dd_rescue im Vergleich zu dd
   - Bricht bei Lesefehlern nicht ab, sondern schreibt statt dessen Nullen
   - dd_rescue kopiert mit zwei Blockgrößen:
     - Wenn kein Fehler auftritt: große Blöcke
     - Nach einem Fehler: kleinere Blockgrößen

4. Hardware defekt - ddrescue

4. Problem von dd_rescue:
   - defekte Blöcke treten häufig in großen Gruppen auf
   - das Abtasten aller dieser Böcke dauert extrem lange
   - sind in diesen defekten „Abschnitten“ überhaupt interessante Daten?
5. Lösung(en):
   - dd_rhelp: Bashscript, Wrapper um dd_rescue
   - ddrescue: komplett neues Tool, in C geschrieben
6. dd_rescue + dd_rhelp ≈ ddrescue

IV. Sonstiges

1. Demo

2. Weitere Informationen

1. Demonstration

Demo

2. Weitere Informationen

Weitere Informationen zum Vortrag (Folien der Vorträge, Links zum Download) unter:

http://www.luga.de

http://www.lug-in.de

Vielen Dank für Ihr Interesse!

Noch Fragen?

Quellen

- Hirnschmalz
- Wikipedia
- http://wiki.ubuntuusers.de
- http://www.pixelbeat.org/docs/disk/
- http://people.apache.org/~skitching/MineOfInformation/linux/Booting_Linux_on_x86_with_Grub2.html
- http://de.wikipedia.org/wiki/Master_Boot_Record
- http://tldp.org/HOWTO/Filesystems-HOWTO-6.html
- http://www.heise.de/open/artikel/Aufbau-224370.html
- http://www.kalysto.org/utilities/dd_rhelp/index.en.html
- http://carlo17.home.xs4all.nl/howto/undelete_ext3.html
- http://www.linupedia.org/opensuse/Verlorene_Dateien_wiederherstellen_ext3_ext4
- http://www.cgsecurity.org
- http://www.cyberciti.biz/tips/understanding-unixlinux-file-system-part-i.html