KNMDI: Computertechnik

Arbeiten mit Linux : Images

04 Juni 2016

Image erstellen

dd

- Byteweises kopieren und konvertieren
- aus zeichen- und blockorientierten Geräten
- sequentiell
- GNU core utilities

ddrescue und dd_rescue

- ddrescue (GNU)
  - überspringt defekte Blöcke und kehrt zurück
  - Logging in einer Textdatei
- dd_rescue (Kurt Garloff)
  - erlaubt Ausgabe an Pipe
- https://lwn.net/Articles/430000/
- https://www.gnu.org/software/ddrescue/ddrescue.html
- http://www.garloff.de/kurt/linux/ddrescue/

Allgemeiner Hinweis

Beim Erstellen eines Images ist das Gerät nicht gemountet!

Beispiele dd

- dd if=/dev/sdb of=disk_20160704.img
- dd if=/dev/sdb1 of=mbr.img bs=512 count=1
- dd if=/dev/random of=elephant bs=256 count=1
- dd if=/dev/urandom of=uelephant bs=256 count=1
  - Beobachtung random und urandom

Beispiel ddrescue

- ddrescue /dev/sdb image.img mapfile

Hashsummen

(md5 || sha1) && (sha2 || sha3)

- md5 : Kollisionen
- sha1 : Kollisionen bald* wahrscheinlich
- sha2 : noch keine Hinweise
- sha3 : aktuell verlässlich und schnell

Hashsummen berechnen

- GNU core utilities
  - md5sum $FILE
  - sha1sum $FILE
  - sha256sum $FILE
- sha3sum
  - https://github.com/maandree/sha3sum

Identifikation

- file -s FILE.img

Offset feststellen

- fdisk -lu disk.img
- parted disk.img
  - unit
  - B
  - print

Images mounten

- mount -o loop FILE.img /mnt/image
- mount -o loop,ro,offset=OFFSET FILE.img /mnt/image
- mount -o loop,ro,offset=$((OFFSET*BLOCKSIZE)) FILE.img /mnt/image

Übungen

- Erstelle jeweils Image und Hashsummen von
  - CD
  - Diskette
  - USB-Stick
  - dem MBR des aktuell genutzten PC
- Mounte alle Images in
  - getrennte Mountpoints
  - read only.
  - Öffne einige Dateien.
  - Hänge alle Images wieder aus.

Dateien wiederherstellen

- foremost
  - /etc/foremost
- scalpel (sleuthkit)