!!! ACHTUNG - evtl. veraltet - ACHTUNG !!!

Diese Seite wurde zuletzt am 9. Juli 2014 um 08:51 Uhr geändert.

Untersuchungsrechner

- Aktuelles grml-iso-Image für i386 von http://www.grml.org/ downloaden...
  - Grundlage dieser Kurzanleitung war 2009.10
- grml-iso-Image für i386 brennen...
- grml-iso-Image für i386 booten (frisch gebrannte CD im Laufwerk belassen und neustarten)...

Wenn **/dev/sdb** der **grml-USB-Stick** ist...

- USB-Stick wipen...

```
root@grml ~ # dd if=/dev/zero of=/dev/sdb bs=4k
```

- USB-Stick partitionieren...

```
root@grml ~ # fdisk /dev/sdb
n
p
1
return
return
t
c
a
1
w
```

(Ergebnis sollte eine Fat32-Partition mit aktiviertem Bootflag sein.)

- USB-Stick formatieren...

```
root@grml ~ # mkfs.vfat -n grml /dev/sdb1
```

- bootfähiges grml auf den USB-Stick schreiben...

```
root@grml ~ # grml2usb /live/image /dev/sdb1
```

(Die Fehlermeldung, dass grub-install keine „device.map“ finden kann, kann ignoriert werden!)

- Rebooten (CD aus dem Laufwerk nehmen) und EnCase schonmal starten...

zu untersuchender Recher

- *USB-Stick sollte vor dem Anschalten im System stecken, damit das BIOS die Möglichkeit hat, ihn zu erkennen!*
- BIOS-Bootmenü „betreten“ (z. B. F12) bzw. im BIOS erste Alternative „booten von USB“

einstellen…
- USB-Stick auswählen (wenn nicht erste Alternative in der Bootreihenfolge im BIOS)…
- grml-**forensic** auswählen…
- USB-Zielfestplatte einstecken…

Wenn **/dev/sdc** die **USB-Zielfestplatte** der DVG ist…

- USB-Zielfestplatte wipen…

```
root@grml ~ # dd if=/dev/zero of=/dev/sdc bs=4k
```

- USB-Zielfestplatte partitionieren…

```
root@grml ~ # fdisk /dev/sdc
n
p
1
return
return
t
7
w
```

(Ergebnis sollte eine HPFS/NTFS-Partition sein.)

- USB-Zielfestplatte formatieren (fast)…

```
root@grml ~ # mkfs.ntfs -f -L dvg /dev/sdc1
```

- „mountpoint“ erstellen…

```
root@grml ~ # mkdir /mnt/dvg
```

- USB-Zielfestplatte einbinden…

```
root@grml ~ # mount -t ntfs-3g /dev/sdc1 /mnt/dvg
```

- „Encase-Image“ erstellen…

```
root@grml ~ # ewfacquire /dev/sda /mnt/dvg
```

(Für die Zieldatei braucht kein Pfad und keine Dateierweiterung angegeben zu werden.)

(Als Kompression sollte fast gewählt werden.)

- *sicherstellen, dass alle Daten auf die USB-Zielfestplatte geschrieben wurden…*

```
root@grml ~ # sync
```

- Die Einbindung der USB-Zielfestplatte aufheben…

```
root@grml ~ # umount /mnt/dvg
```

- USB-Zielfestplatte herausziehen…
- zu untersuchenden Rechner runterfahren (wenn zum Entfernen der CD aufgefordert wird, den USB-Stick herausziehen!)…

```
root@grml ~ # shutdown -h now
```

zurück auf dem Untersuchungsrechner

Das „Encase-Image“ wie gewohnt auswerten…

… **F E R T I G !**