

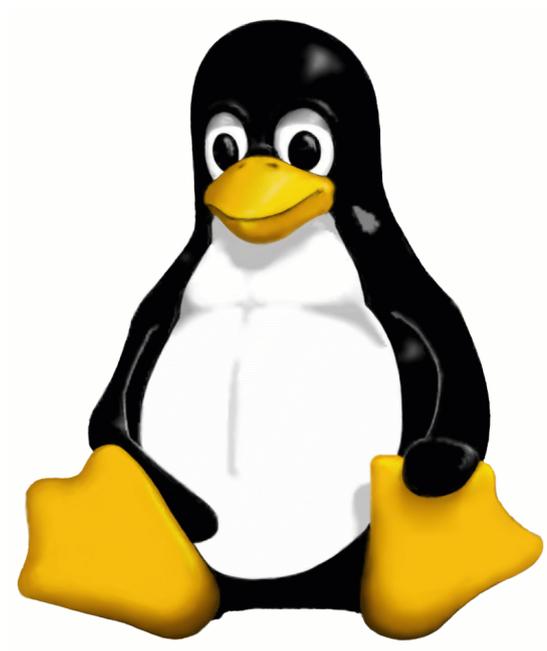
# Linux auf der Xbox



Ein Vortrag von Jens Kühnel  
Freier Linux-Trainer (SuSE und RH)  
Buchautor von  
„Samba 3 – Wanderer zwischen den Welten“



trifft



# Linux auf der Xbox

## Inhalt

- Was ist drin!
  - Hardware
  - Software
- Install Linux
  - Mod-Chip
  - Cromwell
  - Software Hack
- freie Software
- Thanks

# Hardware

- 733 Mhz Intel Celeron CPU (PIII Basis)
- 64 MB RAM (erweiterbar auf 128M löten!)
- 10/100MBit Netzwerkkarte (Nvidia)
- NVidia GForce 3,5 Grafikkarte mit TV-Out – XV Acceleration funktioniert, 3D Acceleration nicht
- 8 oder 10 GB Festplatte (ATAPI-Lock)
- 4 USB-1.1 Ports mit speziellen Steckern
- DVD Rom Laufwerk (einige können keine CD-R/RW lesen)

# Versionen

- Zur Zeit 7 Versionen bekannt:  
1.0 1.1 1.2 1.3 1.4 1.5 1.6 (ganz neu)
- Erkennung anhand des Geburtsdatums nicht zuverlässig, da verschieden Fabriken und Produktionslinien.
- Xbox-Linux-Team hat Datenbank für Versionen Geburtsdaten



# Xbox - Versionen

- 1.0 Boxen
  - Extra Lüfter auf Grafikkarte
  - TV-Chip Conexant
  - TSOP (1024KB) und AT-ähnlicher Stromstecker
- 1.1 Boxen
  - Neuer MCPX (Chipsatz)
- 1.2 Boxen
  - verkleinertes TSOP (256KB)
  - Neuer Strom-Stecker ATX-ähnlich
- 1.3 Boxen
  - Ein Signalleitung vom LPC-Port entfernt

# Xbox - Versionen

- 1.4 Boxen
  - Neuer TV-Chip FOCUS
- 1.5 Boxen
  - Entfernen der 3.3 V und GND LPC-Port
  - Keine Beweise für Existenz der 1.5-Boxen!
- 1.6 Boxen
  - ganz neue Boxen mit TV-Chip xcalibur
  - LPC-Port komplett zerlegt, aber noch auf der Platine
  - Kein Flash mehr, Kernel im ROM

# Festplatten

- Festplatten sind nicht Versionsabhängig
- Festplatten sind austauschbar. Achtung Lock!
- Schlüssel für den ATAPI-Lock liegt im EEPROM
- Zwei Hersteller 4 Platten:

Seagate 10GB



Western Digital 8GB



# Festplatten Partitionierung

- Normalerweise keine Partitionstabelle
- Zeichenfolge BRFR zum Erkennen
- 5 „Partitionen“ an festgelegten Positionen
  - 3\*750MB (X: Y: Z:) Temporäre Daten
  - 500MB (C:) System
  - 4.7GB (E:) Save-Games und Audio-CD-Rips
- FATX-Filesystem (aufgeräumtes FAT-Derivat)

# DVD-Laufwerke

- DVD-Laufwerke sind nicht versionsabhängig
- Spezieller Strom-Stecker mit Ejectdetection
- 3 Hersteller bekannt:

- Thomson

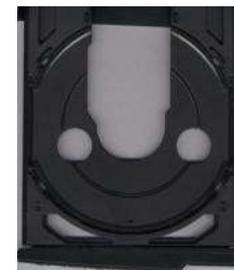
- Probleme: CD-R und CD-RW

- Philips

- Probleme: CD-R
- Neue Versionen scheinbar OK

- Samsung

- kann alles lesen
- schwierig zu bekommen



# TV – OUT und andere

- normalerweise nur TV-OUT (1 + 2Audio Cynch mit Scart-Adapter) oder Scart direkt
- Xbox unterstützt HD-TV bis 1024 (1280x1024)
- VGA-Adpater mit SDIF 5.1 für alle Boxen und viele Spiele/Linux verfügbar (80€)
- Conexant-Chip ermöglicht VGA-Out mit selfmade-Kabel für Linux-only

# Memory-Modul

- original Memory-Modul
  - 8MB USB-Stick mit spezial Stecker
  - sehr teuer (40€)
- Mit Adapter-Kabel funktionieren viele USB-Sticks
  - Kompatibilität ist nur durch Testen zu erkennen.
  - Versuch einer Kompatibilitätsliste unter: <http://unmodded.mine.nu/docs/XboxUsbCompatibilityList>



# LPC - Port

- Offenes Bus-System als Nachfolger von ISA
- Ist in allen Xboxen verfügbar.
- Bei neueren Xboxen sind einzelne Signale/Spannungsleitungen entfernt worden.
- Bei Fehlern im Flash-Inhalt wird vom LPC-Port gebootet
- Fehler kann durch die Kanalleitung D0 ausgelöst werden z.B. bei Mod-Chips

# Original Software / Firmware

- Spezieller Windows 2000–Kernel
  - stark abgespeckt ~ 500 KB
  - kein User-Mode
  - kein Speicherschutz
  - kein Caching
  - kein Swaping
  - kein dynamische Linken
  - kein NTFS, aber FATX, GDF und UDF
  - im TSOP geflasht (schreibgeschützt)

# Dash

- Dash
  - Das Dash-Board ist die Oberfläche das gestartet wird, wenn beim booten kein Spiel im Laufwerk ist.
  - Es ermöglicht es Audio-CDs zu rippen und Savegames zu verwalten.



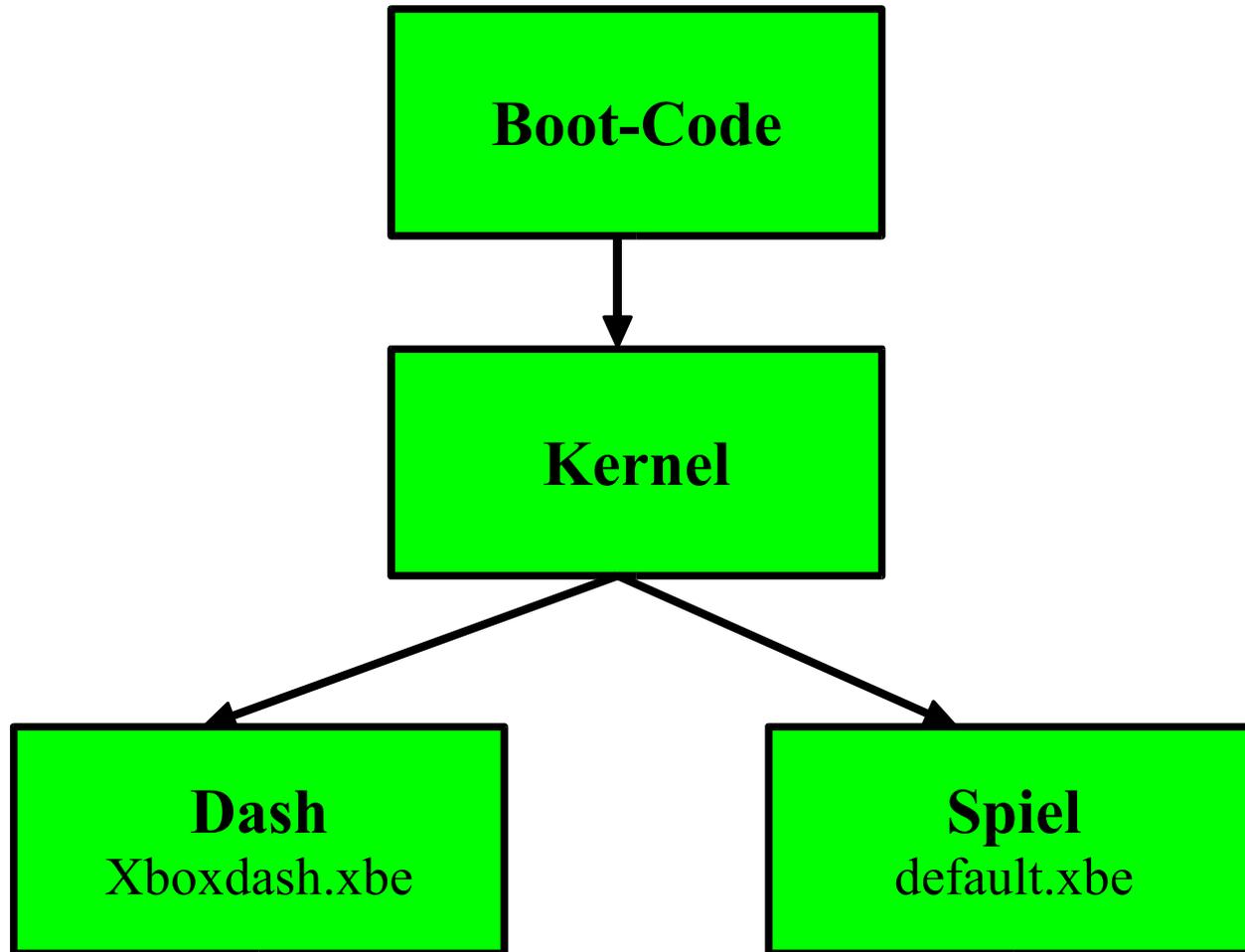
# Xbox Live

- Xbox-Live
  - Online-Spiele-System
  - Überträgt beim Auswählen des Menüpunkts automatisch die Xbox-ID und updatet das Dash
  - Ermöglicht es die Xbox-ID und die .NET-ID miteinander zu verbinden.
  - Xbox-Live verwendet Kerberos (Port 88) und die Ports 3074 upd und tcp.
  - Wenn der Update-Balken noch unter 90% ist, kann man den Uploadvorgang abbrechen!

# Anti-Linux Protection

- MCPX (Chipsatz) enthält Bootcode
- Bootcode startet den Kernel
- Kernel überprüft ATAPI-Lock und die digitale Signatur (RSA-2048Bit) der Binärdateien (XBE Binary)
- Wenn kein Spiel im DVD-Laufwerk (default.xbe), wird Dash-Board Xboxdash.xbe geprüft und gestartet
- Im XBE-Format steht ob Programm von DVD oder von Platte lauffähig ist.

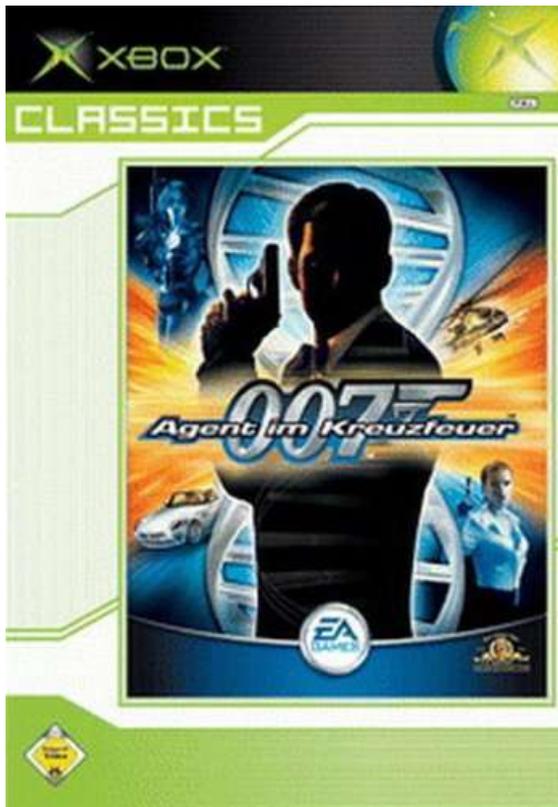
# Trust-Path



# Software-Bugs 1

- Spiele:
  - Bufferoverflow in den Laderoutinen der Savegames
  - Benötigt speziell präparierte Spielstände
  - Microsoft hat begonnen Spiele zu fixen
- Verfügbare Spiele:
  - 007 Agent im Kreuzfeuer
  - Mechassault (Game of the Year Edition ist gefixt!)
  - Splinter Cell (noch Beta)

# Savegames verfügbar für

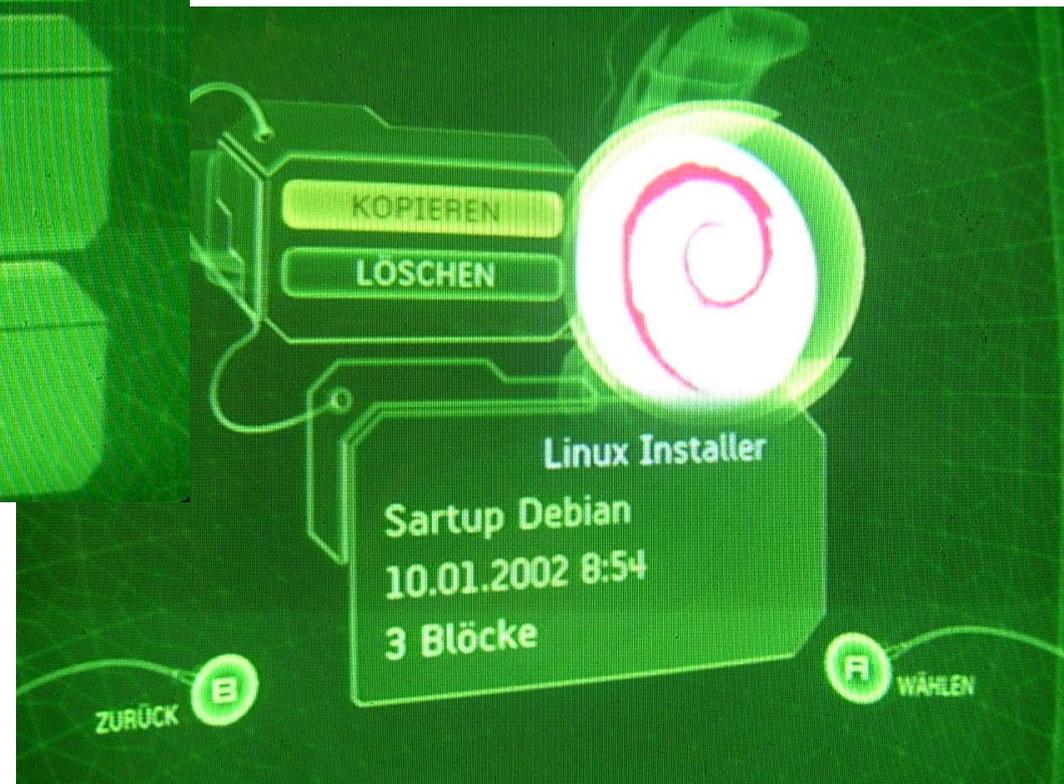


# Installation der Savegames

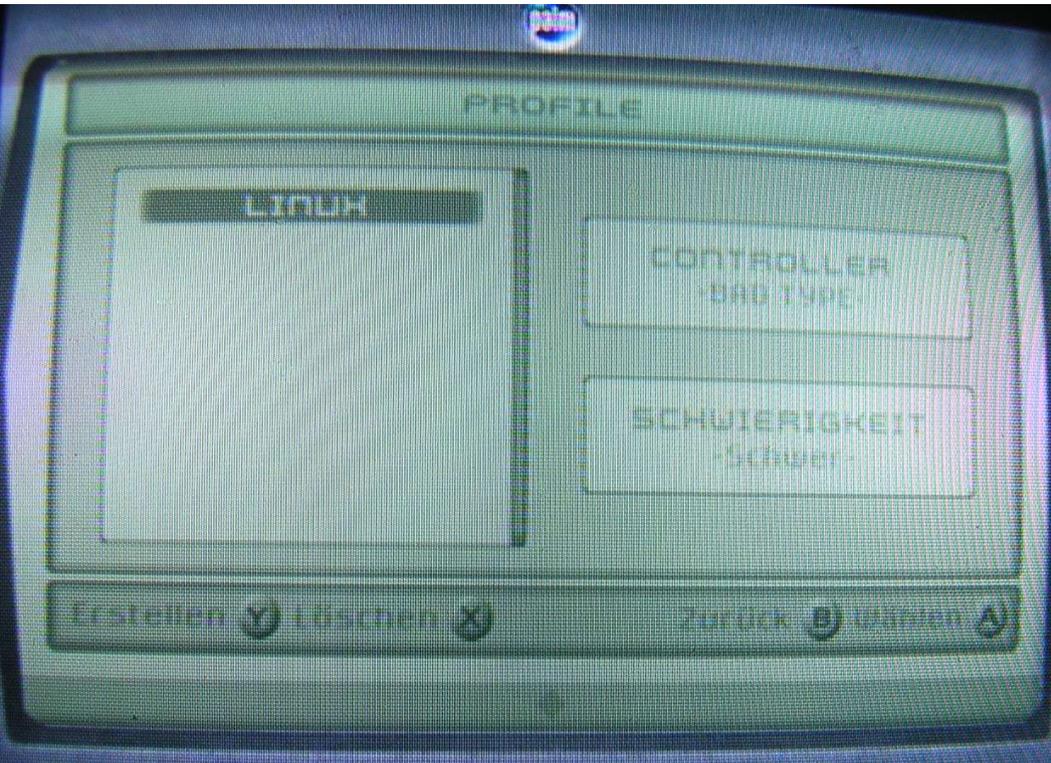
- USB-Kabel
  - spezielles USB-Kabel und „normalen“ USB-Stick (nicht alle Modelle funktionieren)
- Original 8MB-USB-Stick mit dem speziellen Xbox-Stecker an gemoddeter Xbox bespielen.
- Festplatten HDD
  - Die Festplatte wird beim Booten der Xbox entsperrt und die Festplatte wird im laufenden Betrieb an einen Linux-PC mit FATX-Unterstützung angeschlossen.  
!!! RISIKO !!!

# Kopieren der Savegames

Kopiere alle Savegames  
von USB-Memory auf  
Festplatte



# Laden der Spielstände



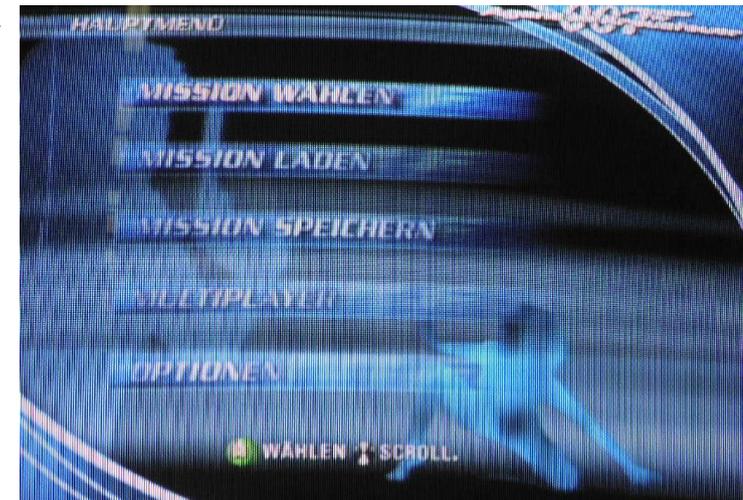
Splinter Cell



Mechassault

Und Linux bootet!  
root Password ist xbox

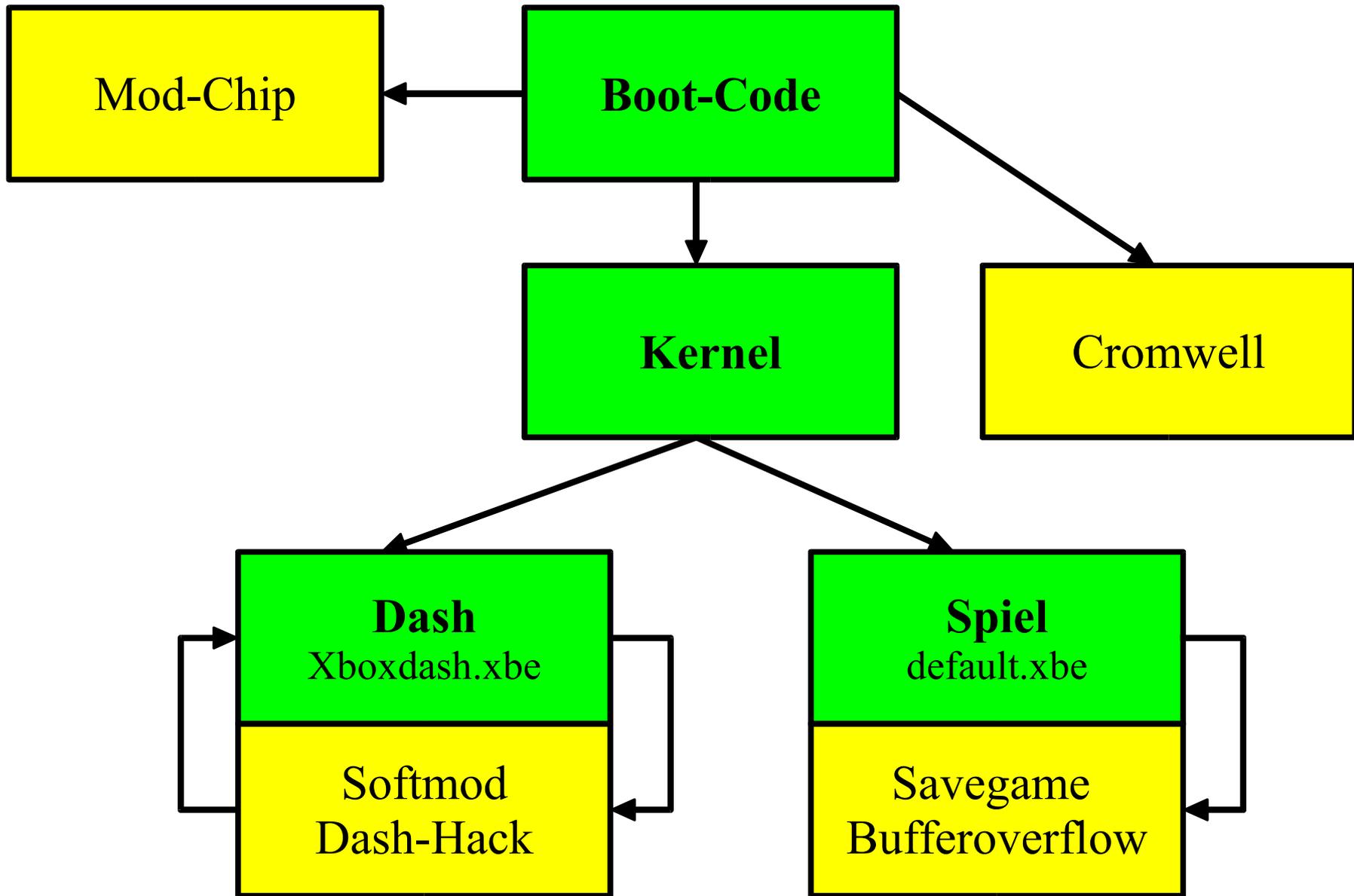
007



# Möglichkeiten für die Permanente Installation

- Mod-Chip
  - alles ist möglich
- Cromwell
  - Linux-Only
- Software-Hack
  - Spiele noch möglich

# Our new Trust-Path :-)



# Modchip

- Mod-Chips leer oder mit Cromwell sind legal!
- Xbox muss geöffnet werden
- Garantie Problem
- Teuer
- Zu kompliziert für die meisten User
  - löten oder
  - unsichere Piggy-Packs
- Nötig für 1.6-Boxen

# Cromwell

- Überschreiben des Microsoft-Kernels mit dem Linux-Bootloader Cromwell.
- Xbox muss geöffnet werden
- Festplatte- oder DVD-Laufwerk kann leicht gegen ein anderes getauscht werden
- Keine Xbox-Spiele mehr möglich
- 100% offener (eigener) Code, daher legal!

# Cromwell Install

- Xbox zerlegen
- Motherboard ausbauen
- TSOP Schreibschutzschieber überbrücken
- Mit Spiele-Bug Linux booten
- mit raincoat neuen TSOP flashen

# Öffnen der Xbox

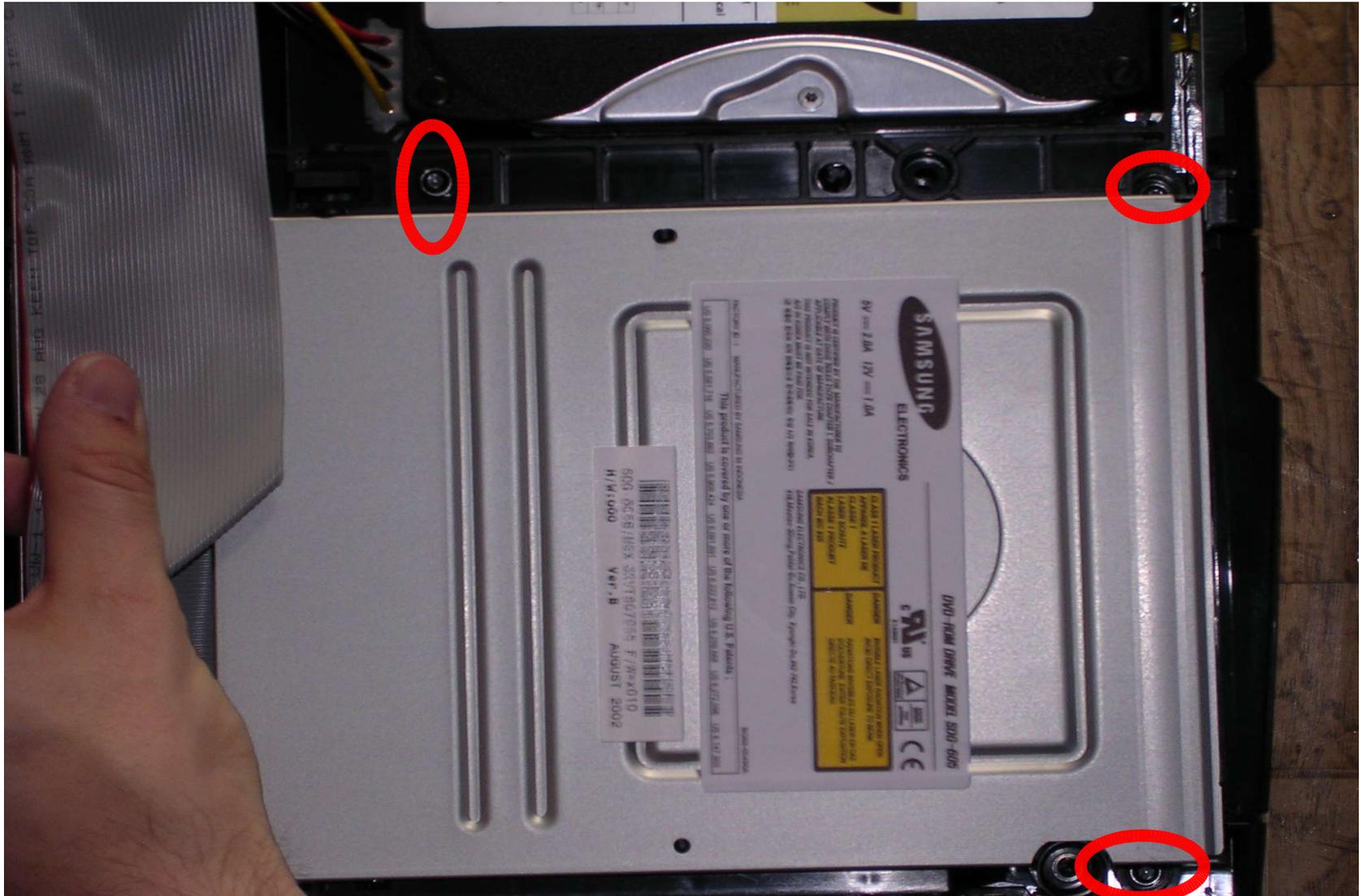


Es gibt 6 Torx-Schrauben.  
Positionen Siehe nächstes Photo

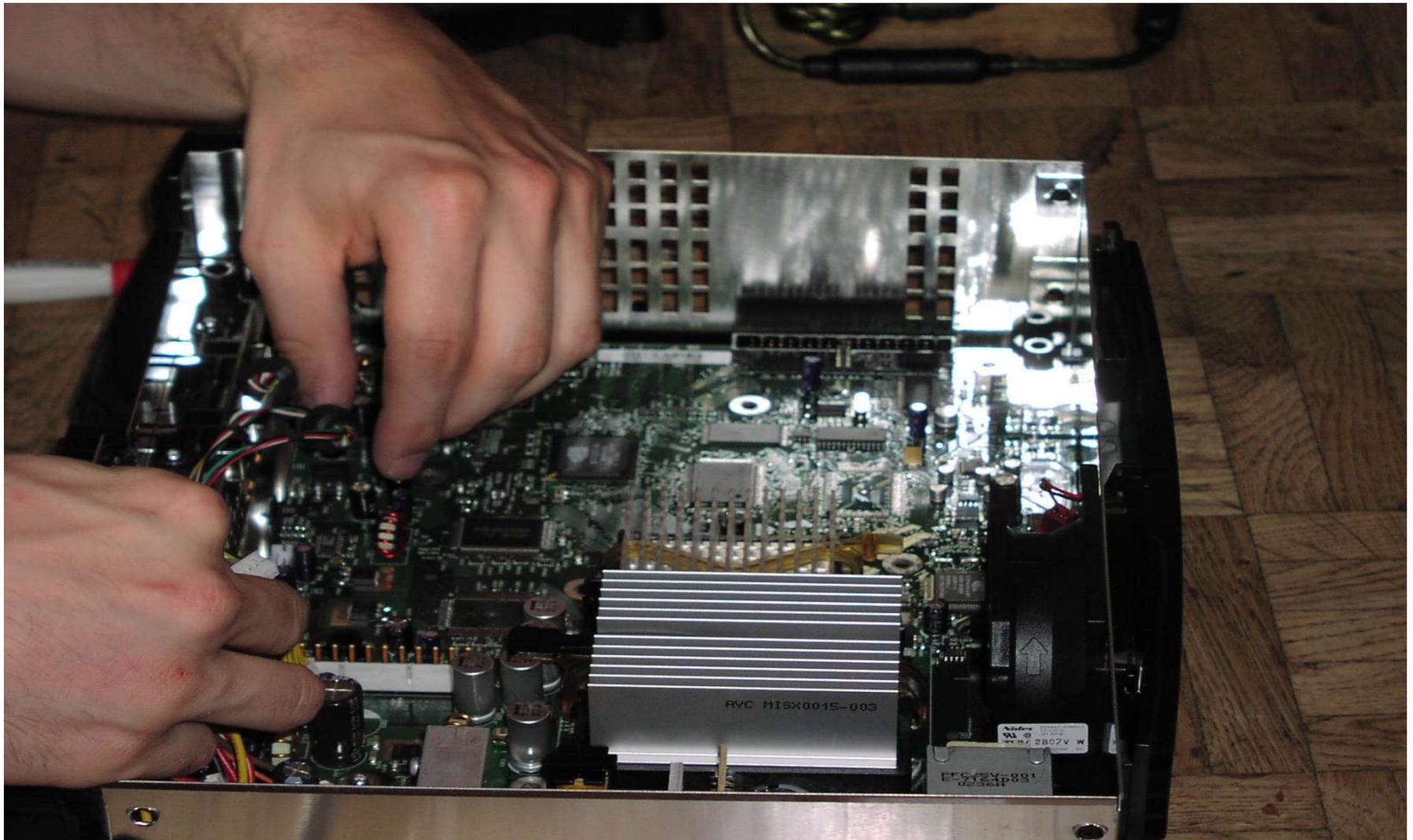
# Öffnen der Xbox



# Lösen der Laufwerke (Festplatte und DVD)

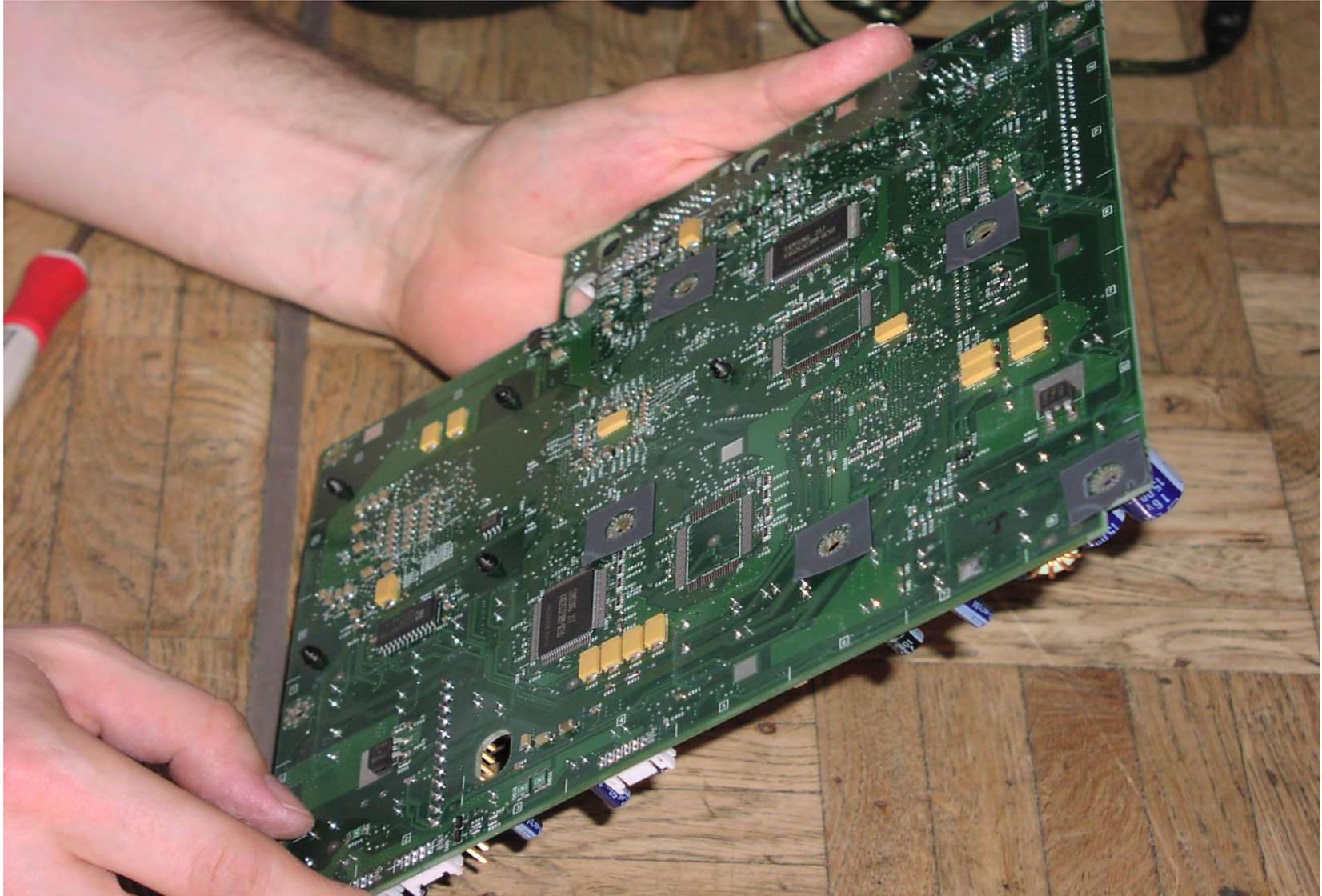


# Motherboard komplett ausbauen

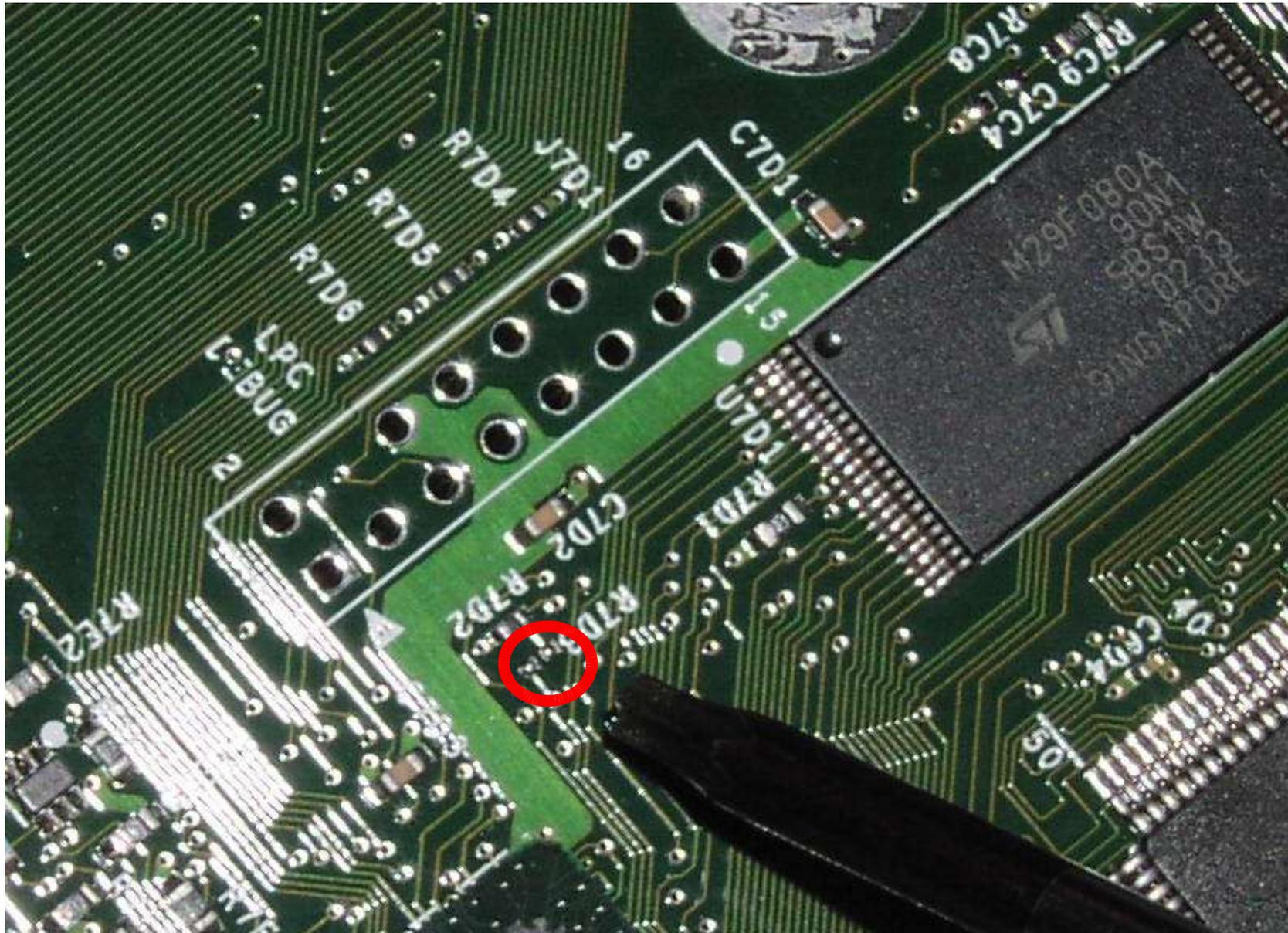


- Alle Schrauben und Stecker (5) loesen
- Motherboard herausnehmen

# Das Motherboard



# Schreibschutz Oberseite

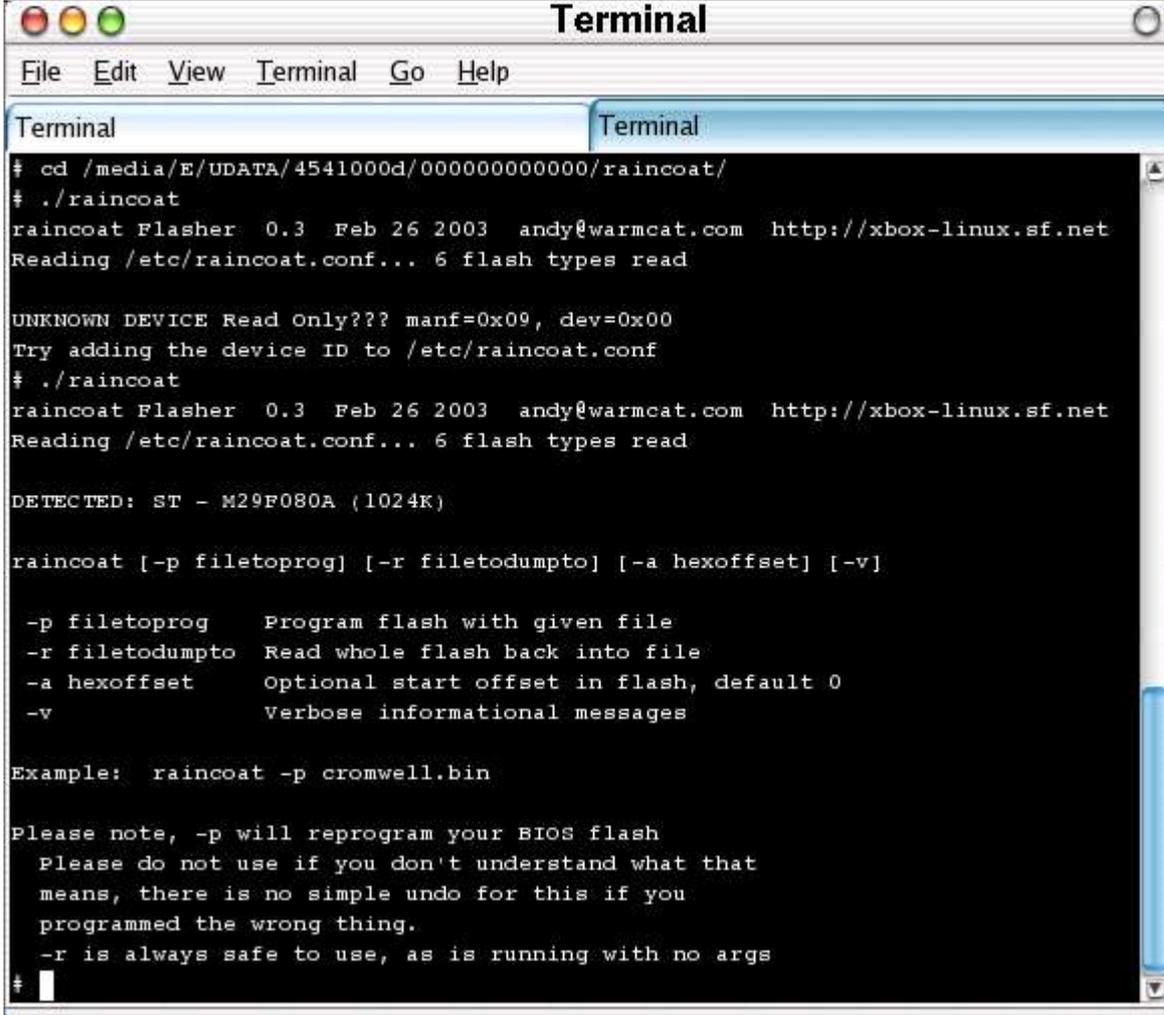


Die Schreibschutzkontakte werden miteinander verbunden.



# Cromwell installieren

- Spiel starten
- Linux-Savegame laden
- Mit raincoat flashen
- Auf richtige Größe aufpassen!!!
- rebooten



```
Terminal
File Edit View Terminal Go Help

Terminal
# cd /media/E/UDATA/4541000d/000000000000/raincoat/
# ./raincoat
raincoat Flasher 0.3 Feb 26 2003 andy@warmcat.com http://xbox-linux.sf.net
Reading /etc/raincoat.conf... 6 flash types read

UNKNOWN DEVICE Read Only??? manf=0x09, dev=0x00
Try adding the device ID to /etc/raincoat.conf
# ./raincoat
raincoat Flasher 0.3 Feb 26 2003 andy@warmcat.com http://xbox-linux.sf.net
Reading /etc/raincoat.conf... 6 flash types read

DETECTED: ST - M29F080A (1024K)

raincoat [-p filetoprog] [-r filetodumpto] [-a hexoffset] [-v]

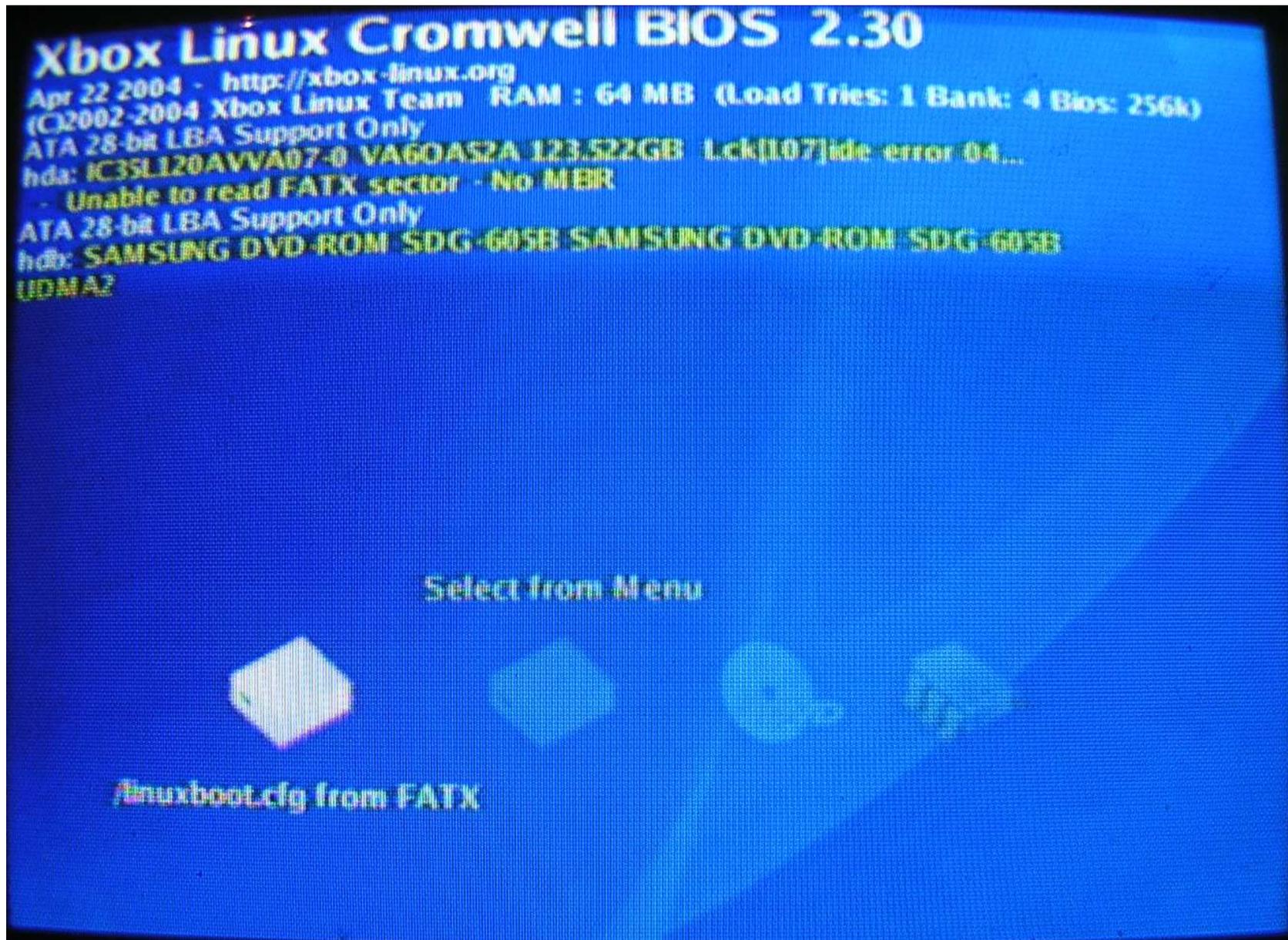
-p filetoprog      Program flash with given file
-r filetodumpto    Read whole flash back into file
-a hexoffset       Optional start offset in flash, default 0
-v                 Verbose informational messages

Example: raincoat -p cromwell.bin

Please note, -p will reprogram your BIOS flash
Please do not use if you don't understand what that
means, there is no simple undo for this if you
programmed the wrong thing.
-r is always safe to use, as is running with no args

#
```

# Cromwell



# Software Hack

- Software-Hack (aka Mechinstaller)
- Kein Öffnen der Box
- Garantie ??
- Verwendet Fehler im Microsoft Dash und in Spiel Mechassault
- Neuere Version für Splinter Cell ist im Beta

# Software Bug 2

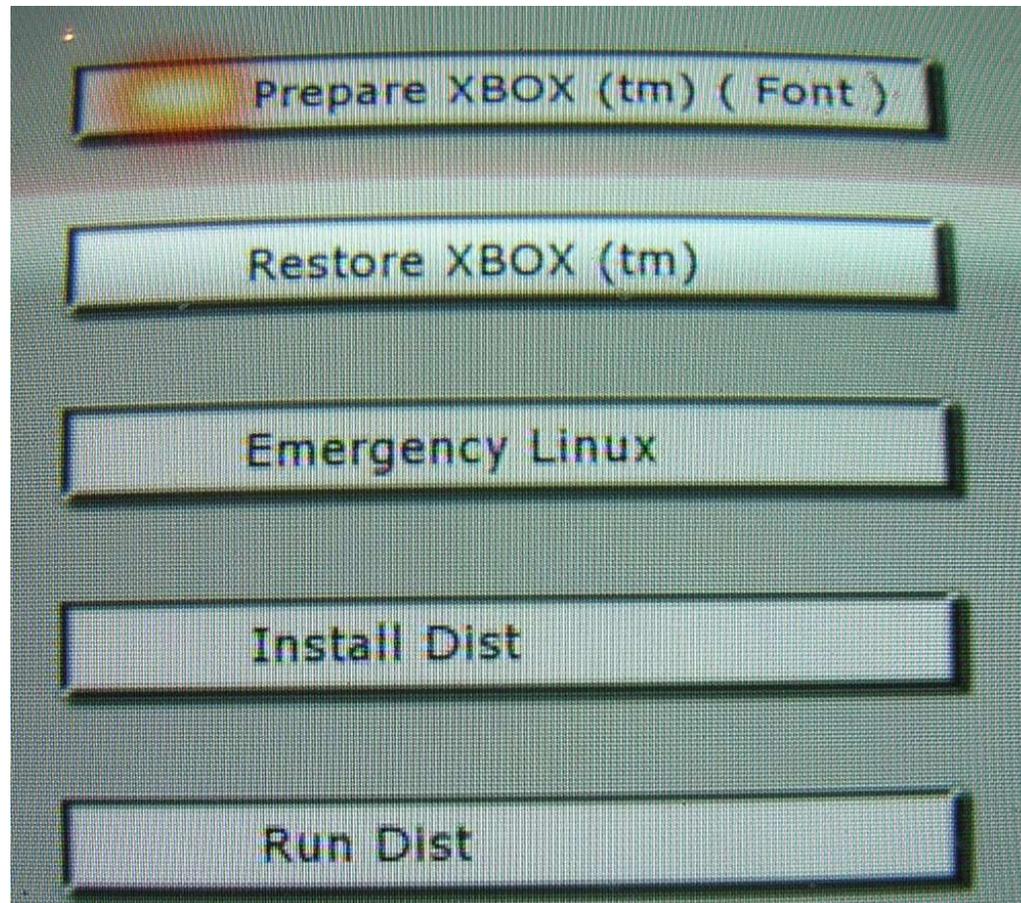
- Dash:
  - Font-Bug
    - Schriftarten sind nicht digital signiert und HEAP-Overflow im Font-System
  - Audio-Bug
    - Integer-Overflow im Index-File der selbst gerippen Audio-CDs-Datenbank

# Software Hacks Probleme

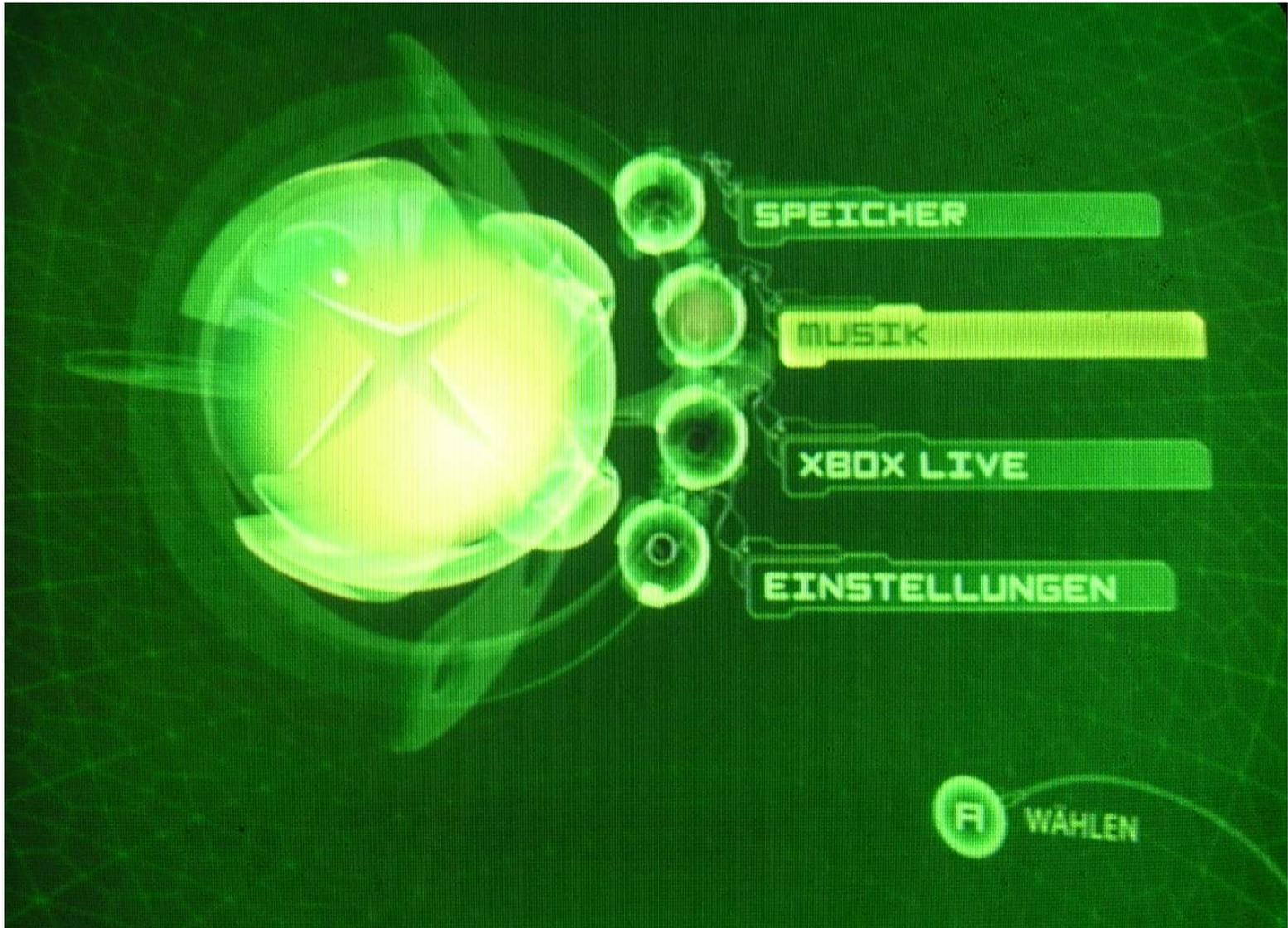
- Neuere Dashes sind gefixt
  - Microsoft Xbox-Live updatet automatisch das Dash.
  - Downgrade auf eine alte Version sollte erlaubt sein.
- Neue Kernel (ab 5713) erlauben kein Downgrade
  - Entweder neuflashen mit altem Kernel (legal??)
  - andere Installationsmöglichkeiten auswählen!
  - Neuer Hack (UDE/UDE2) ist möglich!

# Installation

- Beim Mechinstaller Auswahl beim Laden
- Bei Splinter Cell neues Auswahlmenü



# Vorher



# Nachher: Das neue Auswahlmenü



# Xebian install

- CD einlegen und booten
- Terminalfenster aufmachen
- su -
- XBOXLinuxInstall
  - Auswahl des Installationsortes
    - 1 Savegame (e) Partition
    - 2 unbenutzer Platz einer Platte größer 8GB
    - 3 Platte komplett für Linux (Nicht für Soft-Mod!!)

# The Xbox-Linux Project

- Die offizielle Webseite des Xbox-Linux-Projekts:
  - <http://www.xbox-linux.org/>
  - Xbox-Linux Versionsdatenbank:
    - <http://www.xbox-linux.org/docs/versionentry.html>
    - <http://www.xbox-linux.org/docs/versionfdb.html>
  - Chocolate-Liste: Leute die gerne Helfen
    - <http://www.xbox-linux.org/docs/usershelpusers.html>
- Interessante andere Webseiten zum Thema Xbox:
  - <http://www.xbox-scene.com/>
  - <http://hackingthexbox.com/>

# Software für die Xbox

## •Xebian

- Debian für die Xbox
- <http://www.xbox-linux.org/debian/>

## •freevo

- Frontend zum Filme anschauen

## •Gentoox

- <http://gentoox.shallax.com/>

## •Cromwell das Open-Source Xbox-Bios

- <http://www.xbox-linux.org/download.html>

# Neue Distries

- TODO für neue Distries
  - Kernel
  - i2c
  - alsa
  - X-Server

# HomeBrew-Software (xbins)

- OpenSource -Software mit rechtlichen Problemen
- Zum Kompilieren wird das Microsoft-XDK benötigt.
- Das XDK ist nur für offizielle Xbox-Entwickler in strengen Richtlinien legal.
- Die Binärprogramme sind damit illegal.
- Bekanntestes Beispiel : XBMC / XBMP
- **Das Linux-XBox-Projekt ist nicht mit diesen Projekten verbunden.**

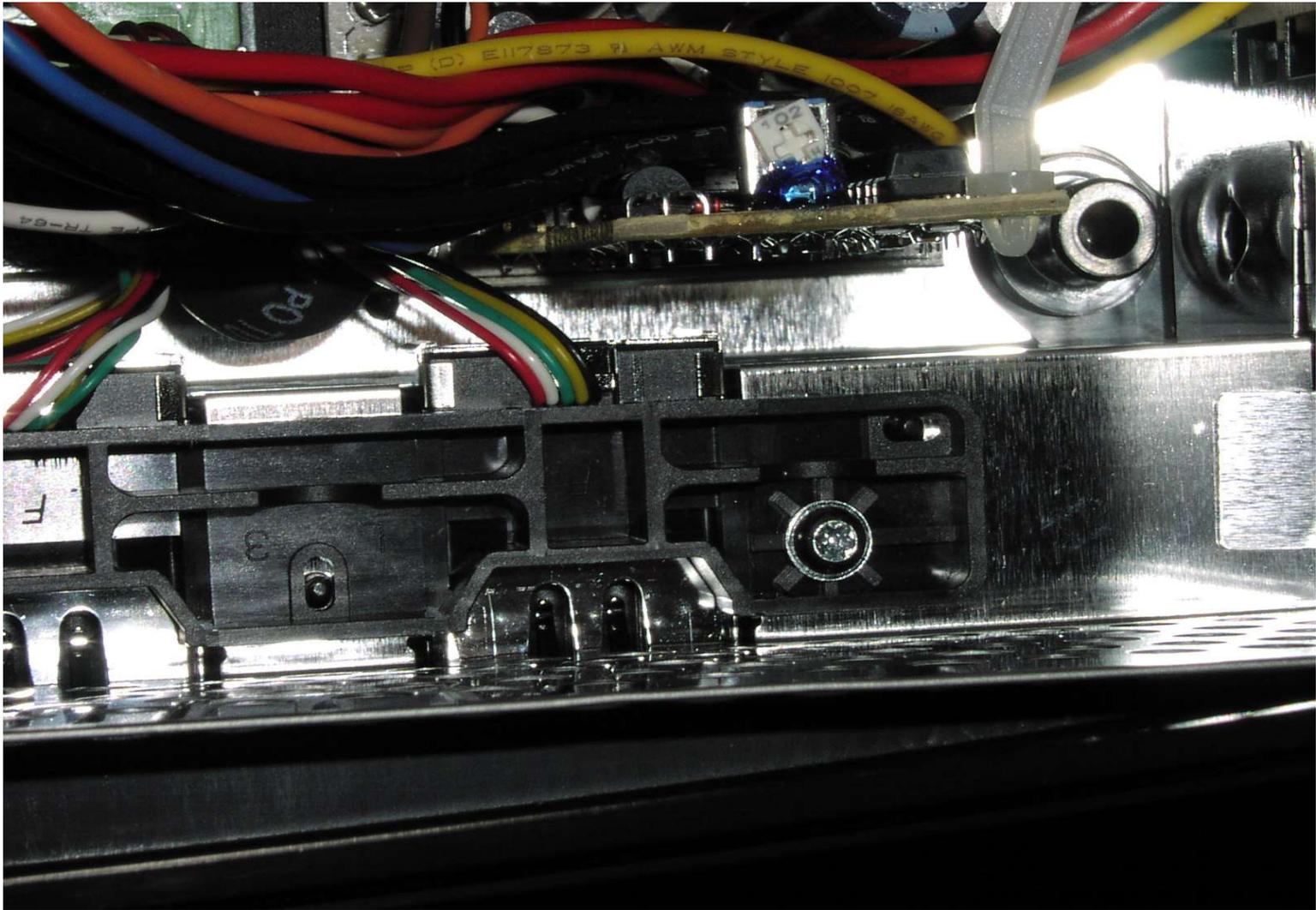
# Dank an:

- Michael Steil:
  - Er hat Xbox-Linux zum Rollen gebracht
- Marvin (Lug-AL)
  - Für seinen Foliensatz als Vorlage
- Das gesamte Xbox-Linux-Team
  - ohne Sie hätte ich nichts zum rumspielen
- und Microsoft für die gesponserte Hardware :-)

Anhang:

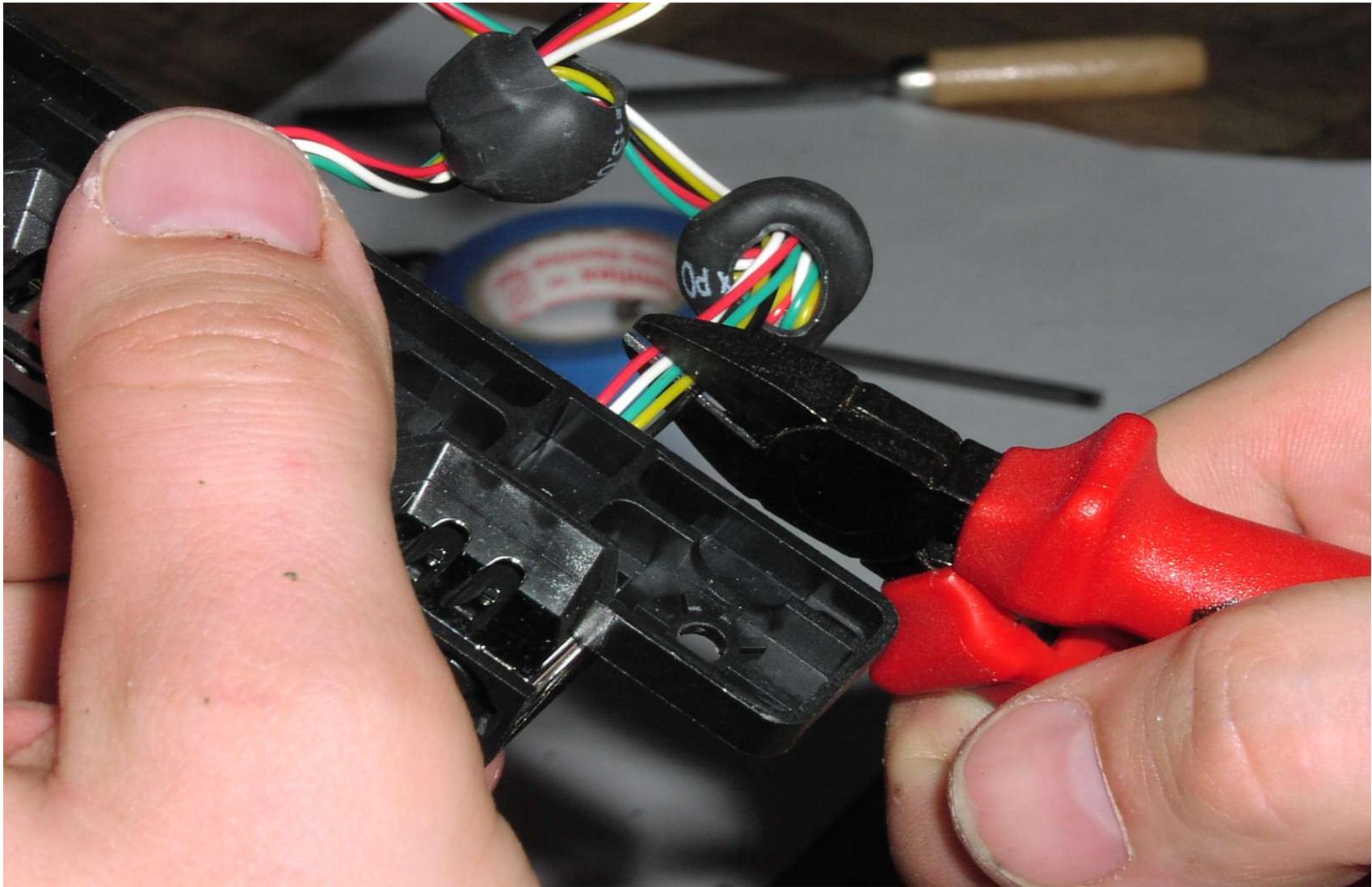
USB-Modding

Umgebaut wird der rechteste USB-Stecker.



Den rechten Traeger herausbauen.

# Herausbauen des Spezialsteckers



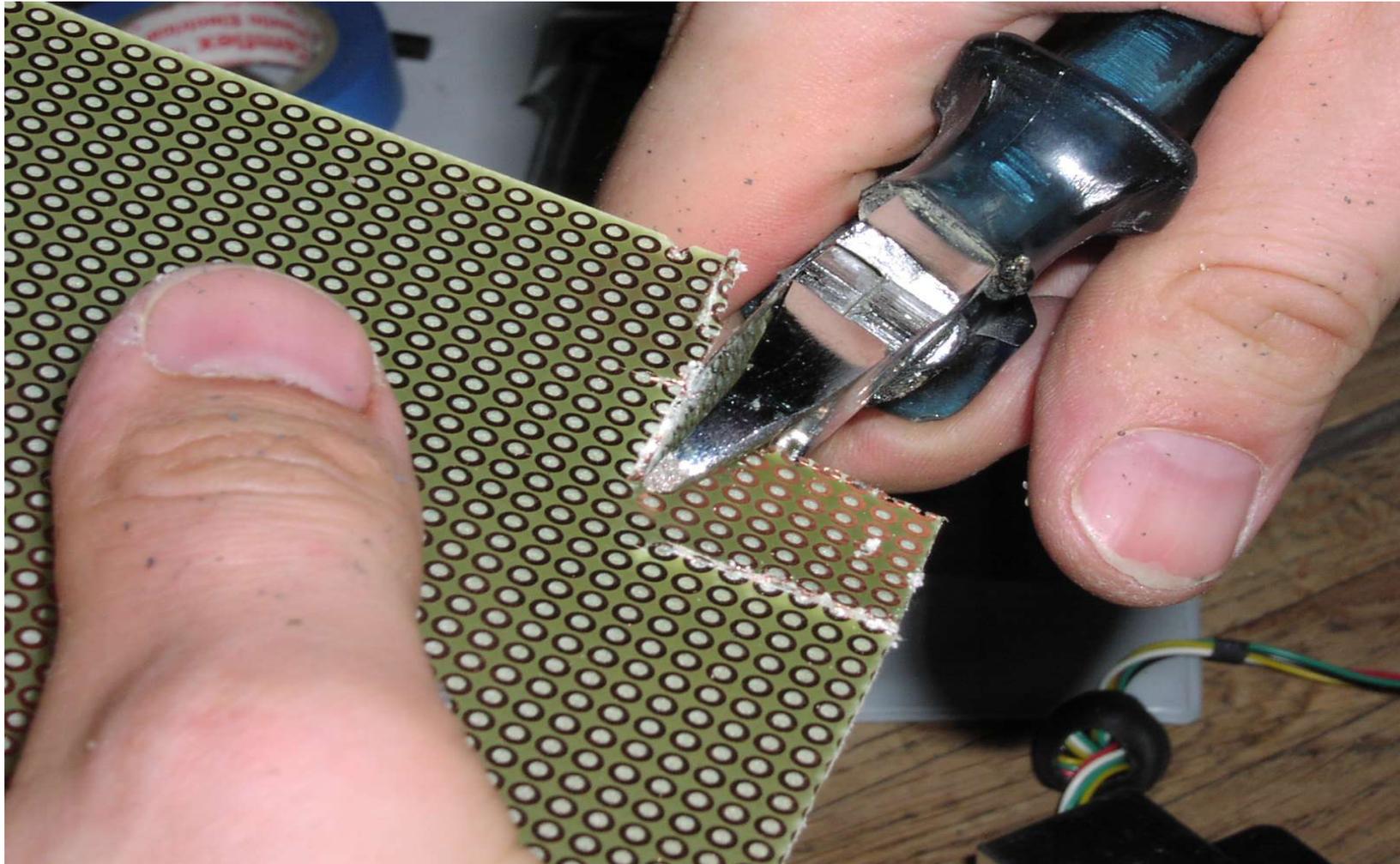
Die Kabel einfach in der Naehе der USB-Buchse abzwicken.

# Herausbauen des Spezialsteckers



Den alten Stecker heraustrennen....

# Halterung fuer die USB-Buchse bauen



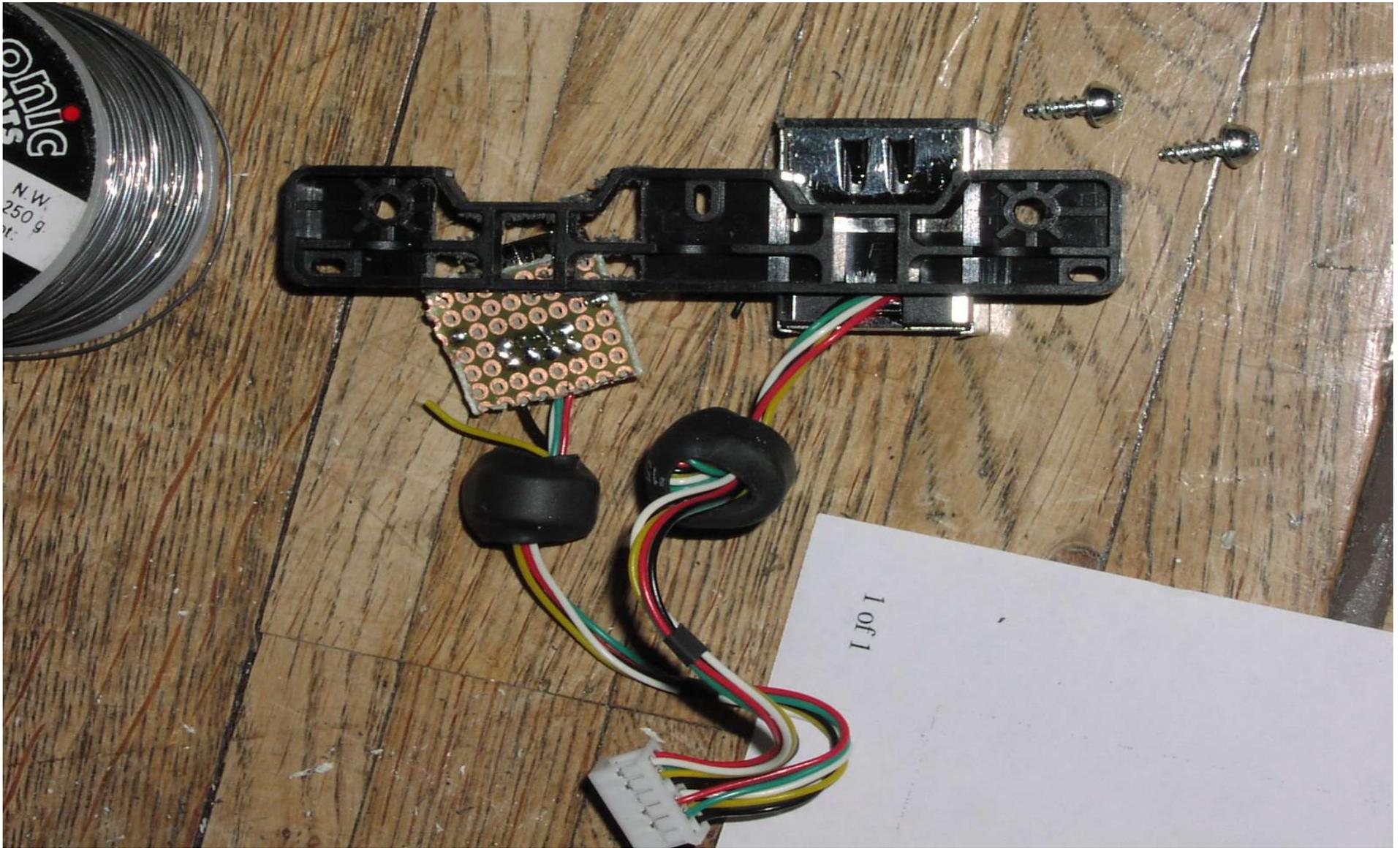
Einfach ein kleines Stueck Platinchen heraustrennen.

# Halterung fuer die USB-Buchse bauen



Die USB-Buchse auf das Platinchen loeten.

# USB-Buchse anschliessen



Die Kabel anhand der USB-Farbkodierung anschliessen. Details siehe naechste Seite.

# USB-Buchse anschliessen

Frontansicht



**1 2 3 4**

- 1 – VBUS / +5V – Red**
- 2 – D- / Data - – White**
- 3 – D+ / Data + – Green**
- 4 – GND / Ground – Black**

## USB-Buchse fixieren



Etwas Heissleim und die Sache klebt....  
Vorher ist es empfehlenswert die Sache grob einzupassen..

Und so sieht das ganze dann fertig aus

