Linux on the Xbox

A Lecture by Jens Kühnel

Freelance linux trainer for
SuSE/Novell and RedHat

author of the german book
„Samba 3 – Wanderer zwischen den Welten"

meets

Linux on the Xbox content

- What's inside!
  - Hardware
  - Software

- Install Linux
  - Mod-Chip
  - Cromwell
  - Software Hack

- free Software

- Thanks

Hardware

- 733 Mhz Intel Celeron CPU (PIII -based)

- 64 MB RAM (expandable to 128M,soldering!)

- 10/100MBit Network card (Nvidia)

- NVidia GForce 3,5 graphic card with TV-Out – only 2D XV Acceleration available, no 3D

- 8 or 10 GB Hard disc (ATAPI-Lock)

- 4 USB-1.1 Ports with special Connector

- DVD Rom Drives (Problems reading some CD-R/RW)

Versions

- 7 known Versions at the moment:
  1.0 1.1 1.2 1.3 1.4 1.5 1.6

- Not Identifiable by production date, because of different factories and assembly lines

- Xbox-Linux-Team has a Version-Howto http://www.xbox-linux.org/Xbox_Versions_HOWTO

The Birth date

MICROSOFT CORPORATION   2002 — 03 — 03   :MFG. DATE

1166356 20903   :SERIAL NO.

54471   SILVER   713 1166356 20903 :PRODUCT ID

Xbox - Versions

- 1.0 Boxes

  - extra fan on the Graphic card

  - TV-Chip Conexant

  - TSOP (1024KB) and AT-like power conector

- 1.1 Boxes

  - New MCPX (Chipset)

- 1.2 Boxes

  - smaller TSOP (256KB)

  - New ATX-like power connector

Xbox - Versions

- 1.3 Boxes
  - one Signal is removed from the LPC-Port
- 1.4 Boxes
  - New TV-Chip FOCUS
- 1.5 Boxes
  - Removing of the 3.3 V and GND from the LPC-Port
  - There is no proof of real 1.5-Boxes
- 1.6 Boxes
  - New Boxes with TV-Chip xcalibur
  - LPC-Port is hidden, but still on the board
  - No Flash any more, Kernel is now in ROM

Hard disc

- Hard disc is not version depended

- Hard discs are swappable Mind the Lock!

- Key/Serial of the ATAPI-Lock is in the EEProm

- Two Manufacturers 4 Drives:

Seagate 10GB

Western Digital 8GB

Hard disc partitioning

- Normal no real Partition table
- String BRFR is used to detect Xbox-HDD
- 5 „Partitions" at predefined Positions
  - 3*750MB (X: Y: Z:) Temp FS
  - 500MB (C:) System
  - 4.7GB (E:) Save-Games and Audio-CD-Rips
- FATX-Filesystem (cleaned FAT-Derivat)

DVD-Drives

- DVD-Drives are not Version dependent

- special Power connector with Eject detection

- 3 known Manufactures:
  - Thomson
    - Problems: CD-R and CD-RW
  - Philips
    - Problems: CD-R
    - New Versions looks OK
  - Samsung
    - can read anything
    - hard to get

TV – OUT and other

- normally only TV-OUT (1 + 2 Audio Cinch with Scart-Adapter) or Scart directly

- Xbox supports HD-TV up to 1080i

- VGA-adapter with SDIF 5.1 for all Boxes and many Games/Linux available (80€)

- Owner Conexant-Chip-boxes can make a self-made Cable for Linux only

Memory-Module

- original Memory-Module

  - 8MB USB-Stick
    with special Connector

  - very expensive (40€)

- Many USB-Sticks working with a
  simple Adapter

  - Compatibility only recognisable by testing

  - The Try of a Compatibility list is available at:http://
    unmodded.mine.nu/docs/XboxUsbCompatibilityList

LPC - Port

- Open Bus-System as the successor of ISA

- Available in every Xbox.

- The signals are scattered over the board at 1.6-Boxes

- In case of an error in the flash the LPC-port is used as the booting device

- An error can be created by grounding the Signal D0, this is used by the mod-Chips

Original Software / Firmware

- special Windows 2000–Kernel

  - very small ~ 500 KB

  - no User-Mode

  - no Memory protection

  - no Caching

  - no Swapping

  - no dynamic linking

  - no NTFS, but FATX, GDF and UDF

  - flashed into the TSOP (write protected)

Dash

- Dash
  - The Dash-Board is the User interface shown when no Game is put into the DVD-Drive
 - It´s possible to to rip Audio-CDs and to manage Save games

Xbox Live

- Xbox-Live
  - Online-Game-System
  - Tries to send the Xbox-ID to Microsoft and updates the Dash whenever the menu item xbox-live is selected.
  - Makes it possible to connect the Xbox-ID and the .NET-ID
  - Xbox-Live uses Kerberos (Port 88) and the Ports 3074 upd and tcp.
  - When the Progessbar is under 90% you can still reset the box.

Anti-Linux Protection

- The Boot code is inside the MCPX (Chipset)

- The Boot code starts the Kernel

- Kernel tests the ATAPI-Lock and the digital Signature(RSA-2048Bit) of the binaries (XBE)

- When a game is in the DVD-Drive the default.xbe is tested and started.

- When no game is available the Xboxdash.xbe is used.

- The XBE-Binary-Format defines, if a Program can be run from HDD or DVD.

Trust-Path
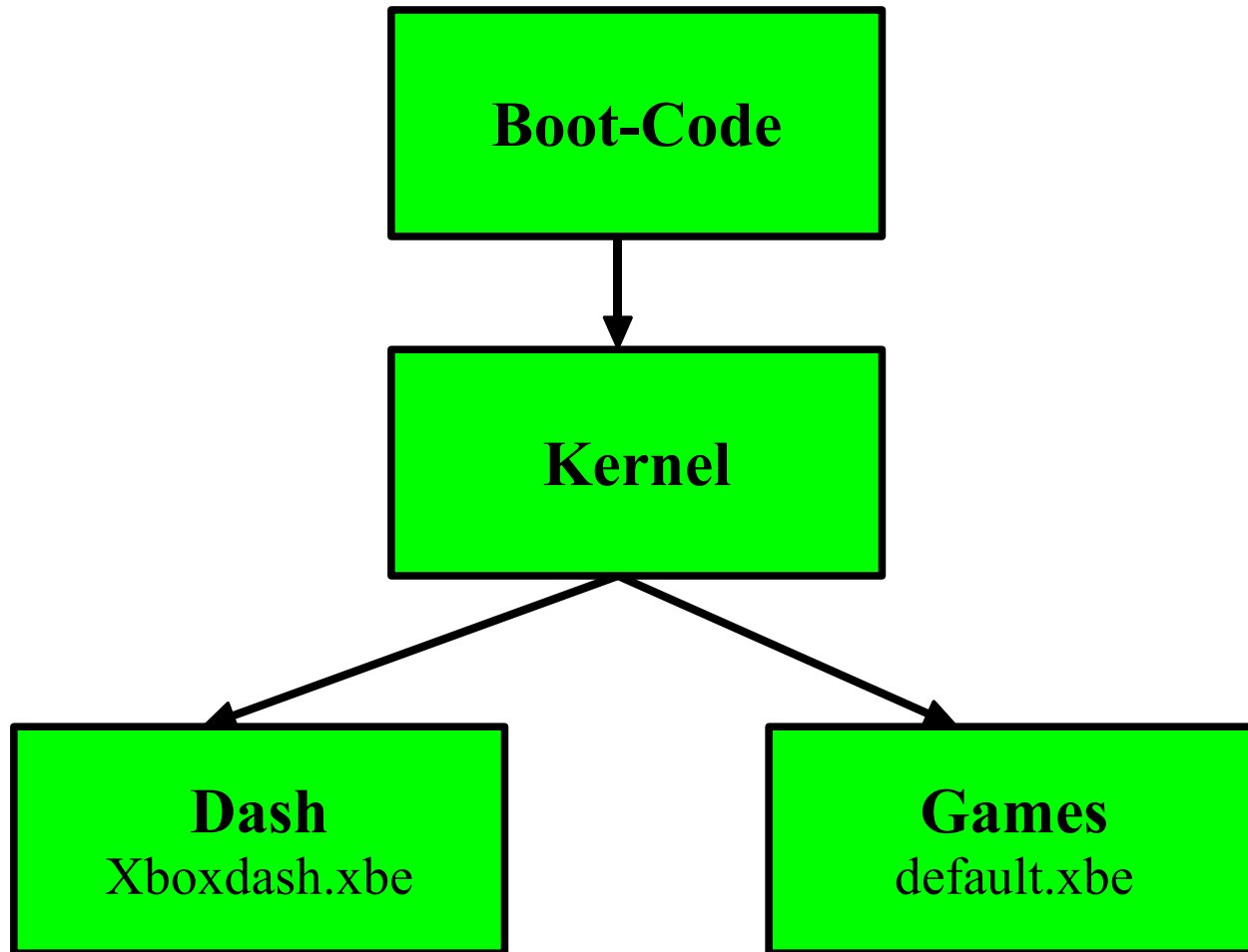
Software-Bugs 1

- Game:
  - Buffer overflow in the Loader of the Save games
  - We need a special prepared Save game
  - Microsoft has started to fix Games.

- Available Games :
  - 007 Agent in Crossfire (Kreuzfeuer)
  - Mechassault (Game of the Year Edition is fixed !)
  - Splinter Cell (still Beta)

Save games available for

Installation of the Save games

- USB-Cabel
  - special USB cable and „normal" USB-Stick (not all models work)
- Original 8MB-USB-Stick with the special Xbox-Connector is used on a already modded Xbox.
- HDD
  - The Hard disc is unlocked during the boot of the Xbox. After the boot the still running HDD is removed from the Xbox and connected to a Linux-PC with FATX-Support! !!! DANGEROUS!!!

Copying of the Save games

Copy all Savegames from USB-Memory to Harddisc
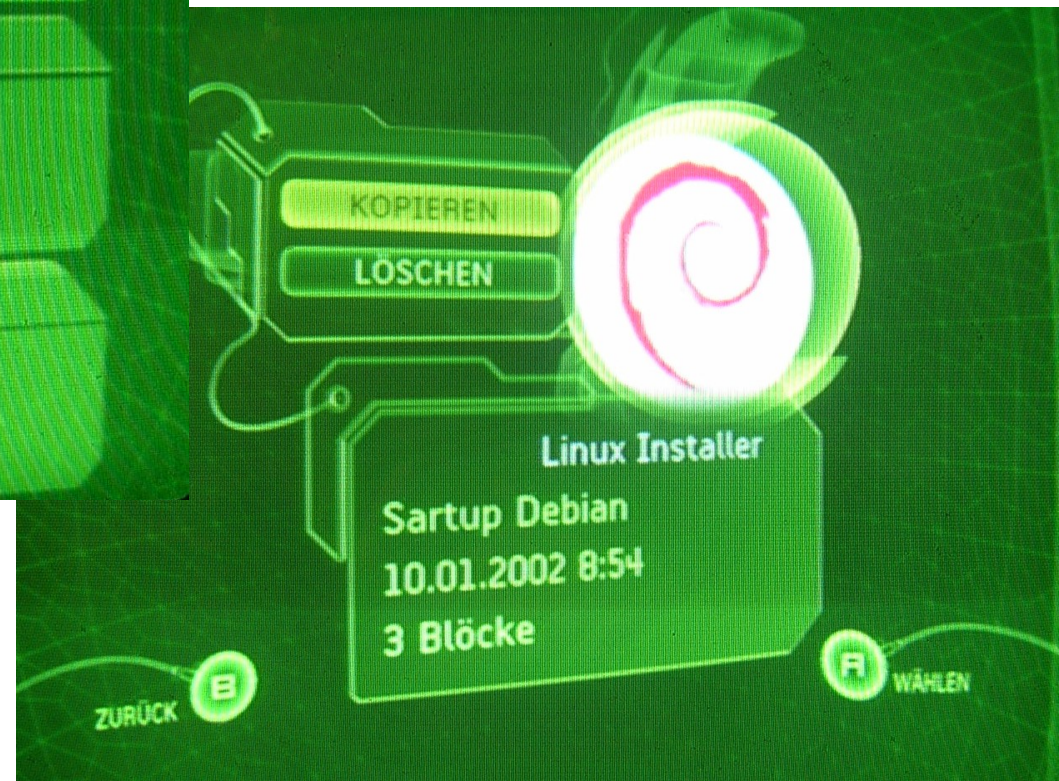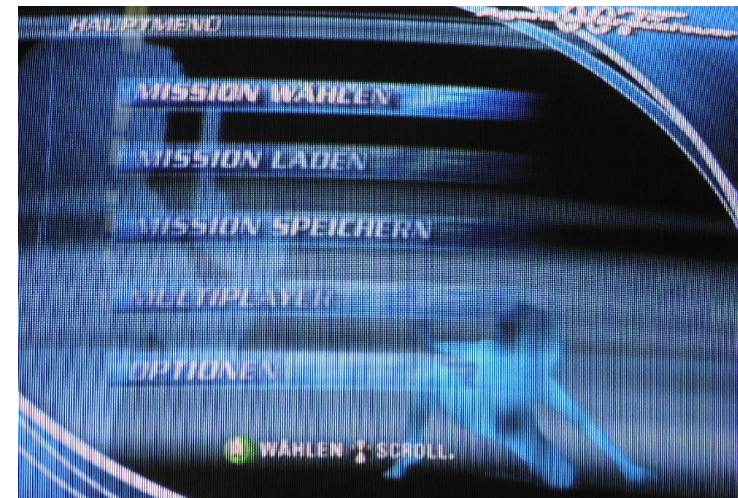
Loading the Save games
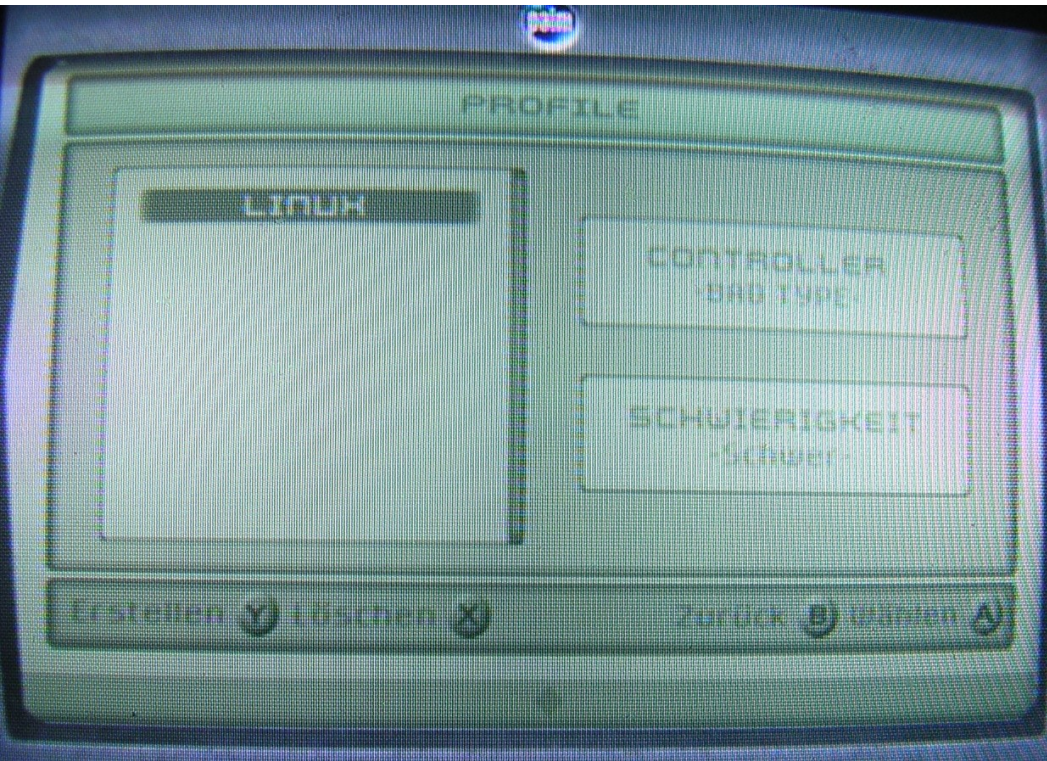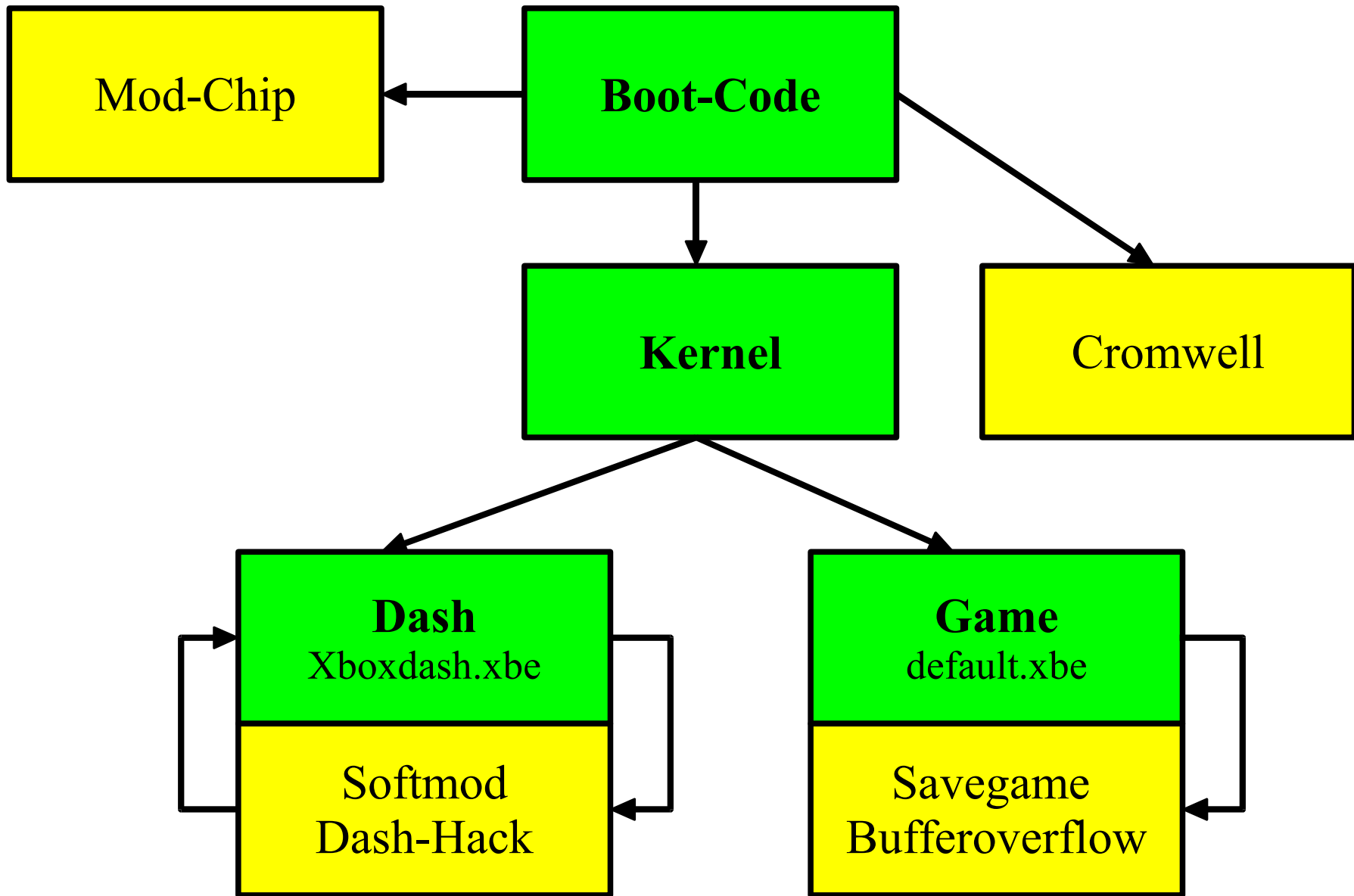

Splinter Cell

Mechassault

007

and Linux is booting!
The root password is xbox

Possibilities for a permanent installation

- Mod-Chip
  - everything is possible

- Cromwell
  - Linux-Only

- Software-Hack
  - Games are still possible

Our new Trust-Path :-)

Modchip

- Only empty Mod-Chips or loaded with Cromwell are legal!
- Xbox has to be opened
- No Warranty
- Expensive (20-50€)
- to complicated for the average User
  - solder or insecure Piggy-Packs
- Available for all Boxes

Cromwell

- Override the Microsoft-Kernel with the Linux-Boot loader Cromwell.

- You have to open your Xbox

- HDD- and DVD-Drive can be swapped very easy.

- No Xbox games possible any more

- 100% open (own) Code, therefore 100% legal!
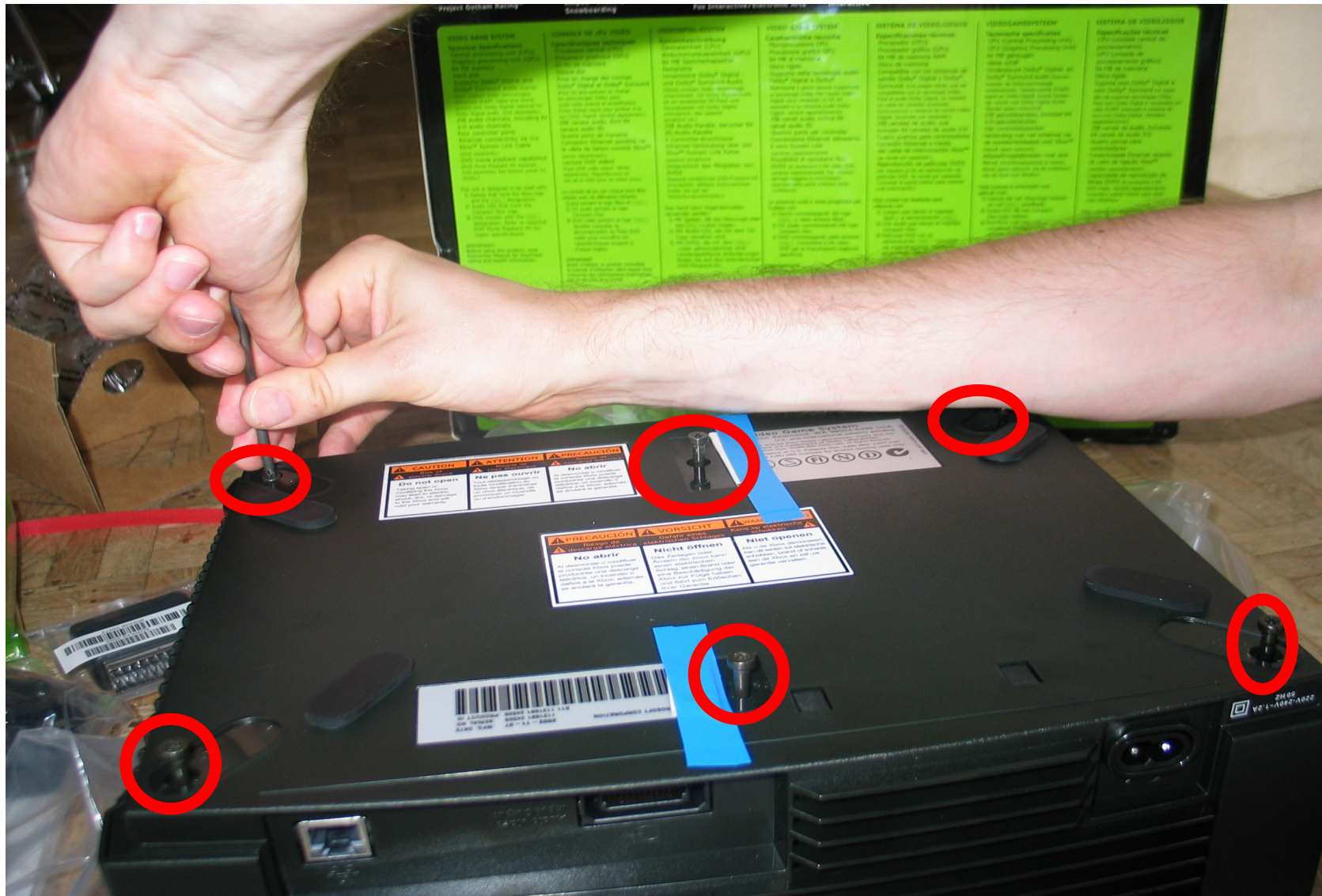
Cromwell Install

- Take you Xbox apart
- Take out your Motherboard
- remove TSOP write protection
- Boot Linux with buggy game
- write new TSOP flash with raincoat

Opening the Xbox

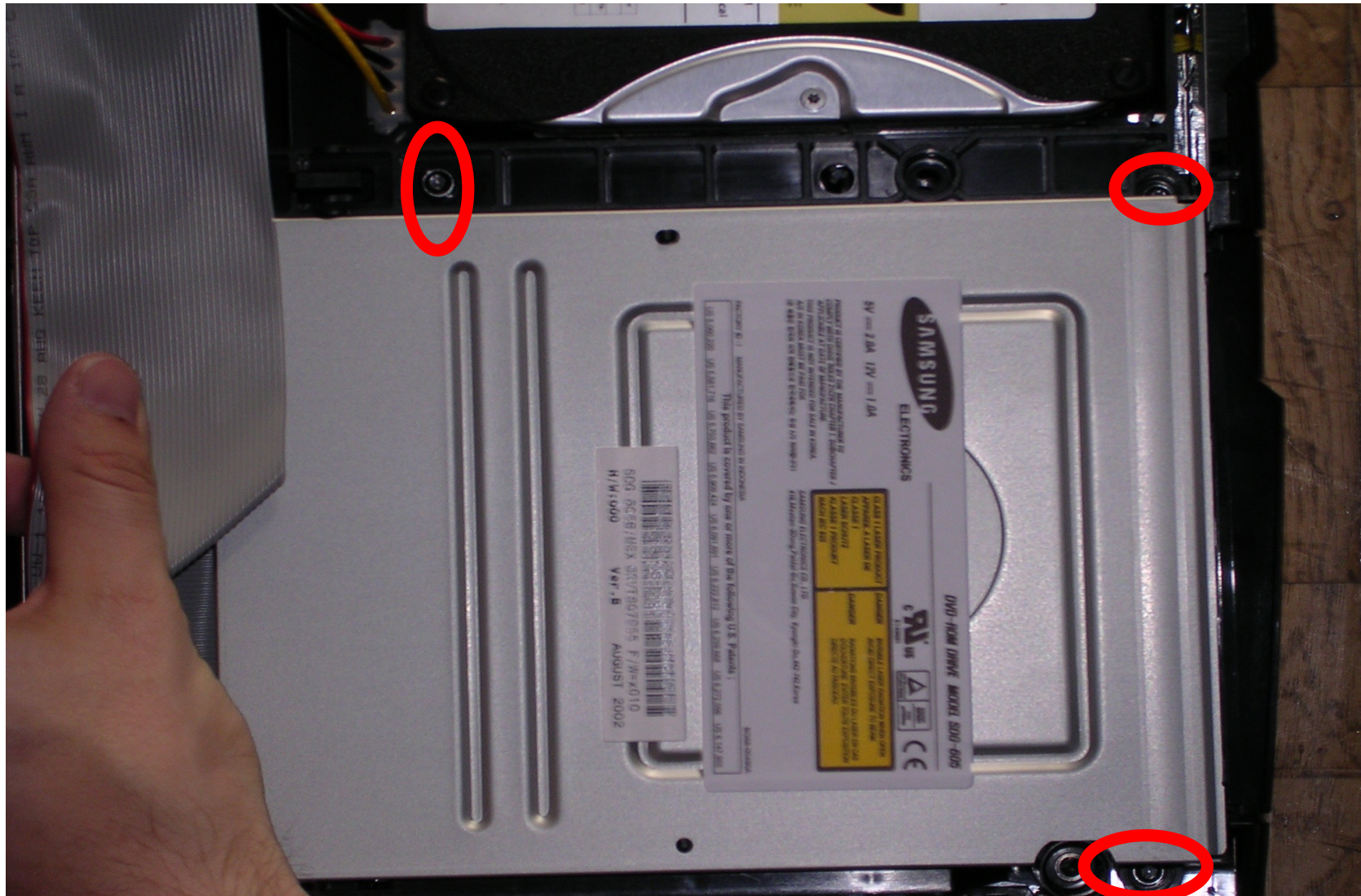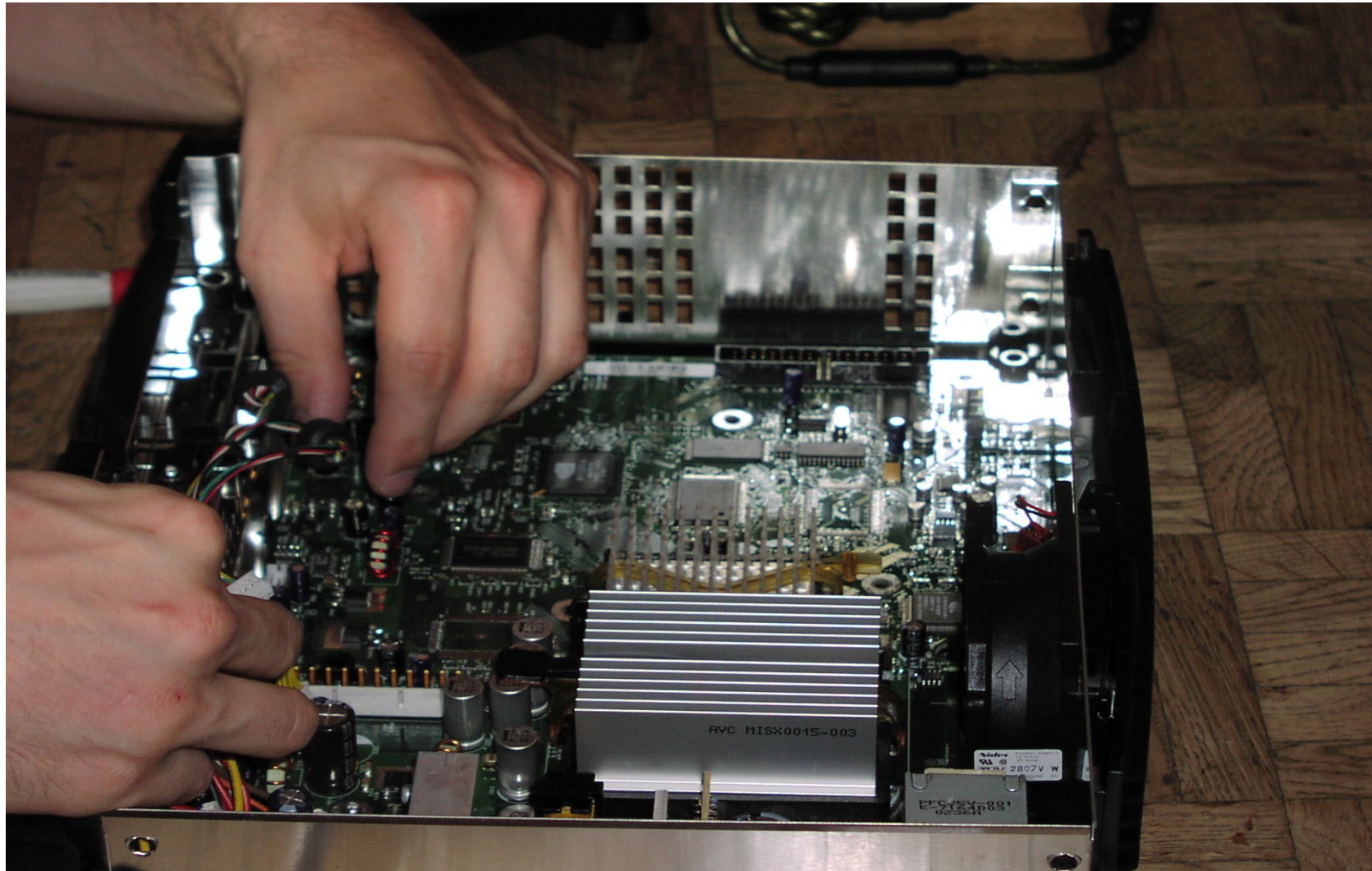There are 6 Torx-Screws.

Opening the Xbox

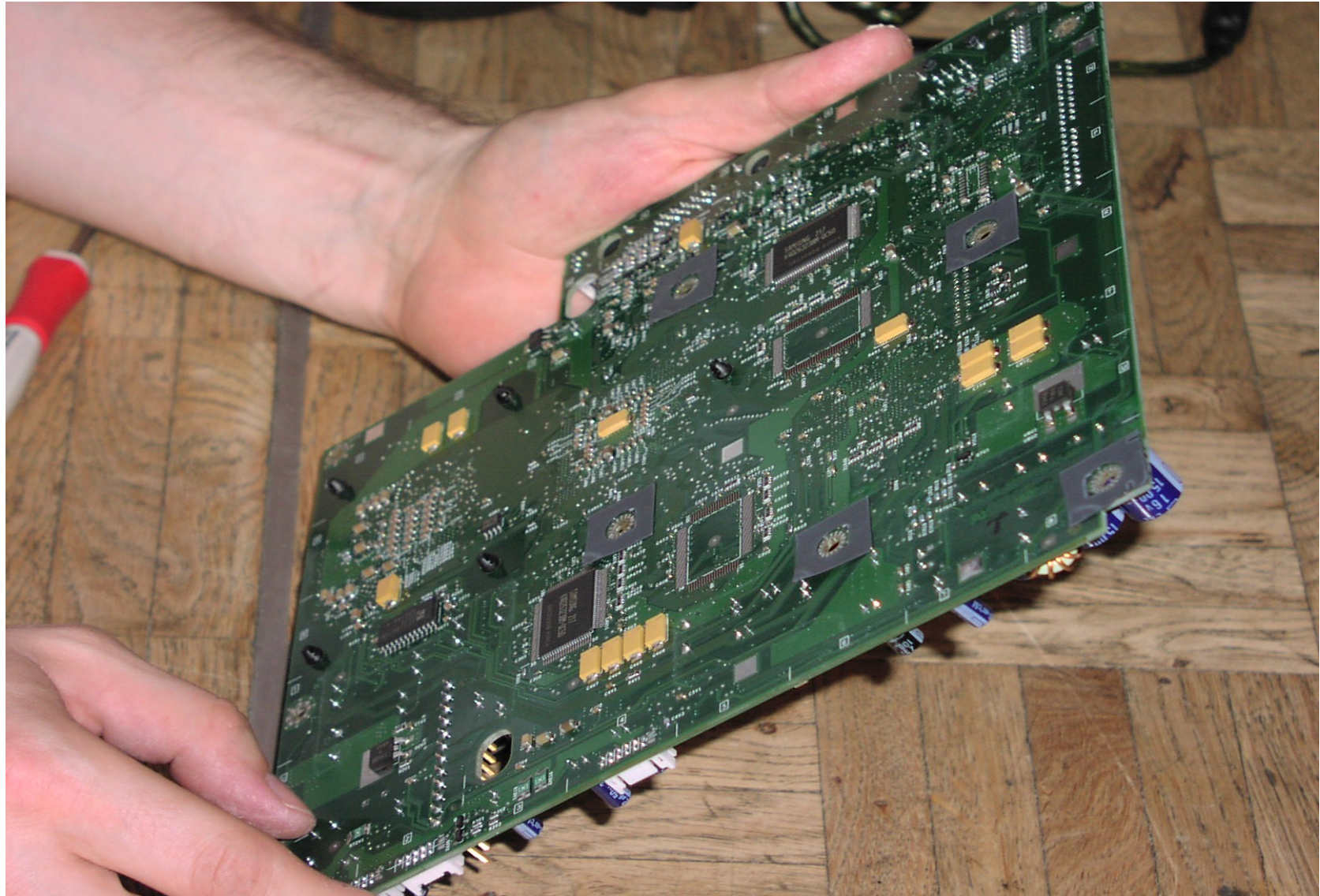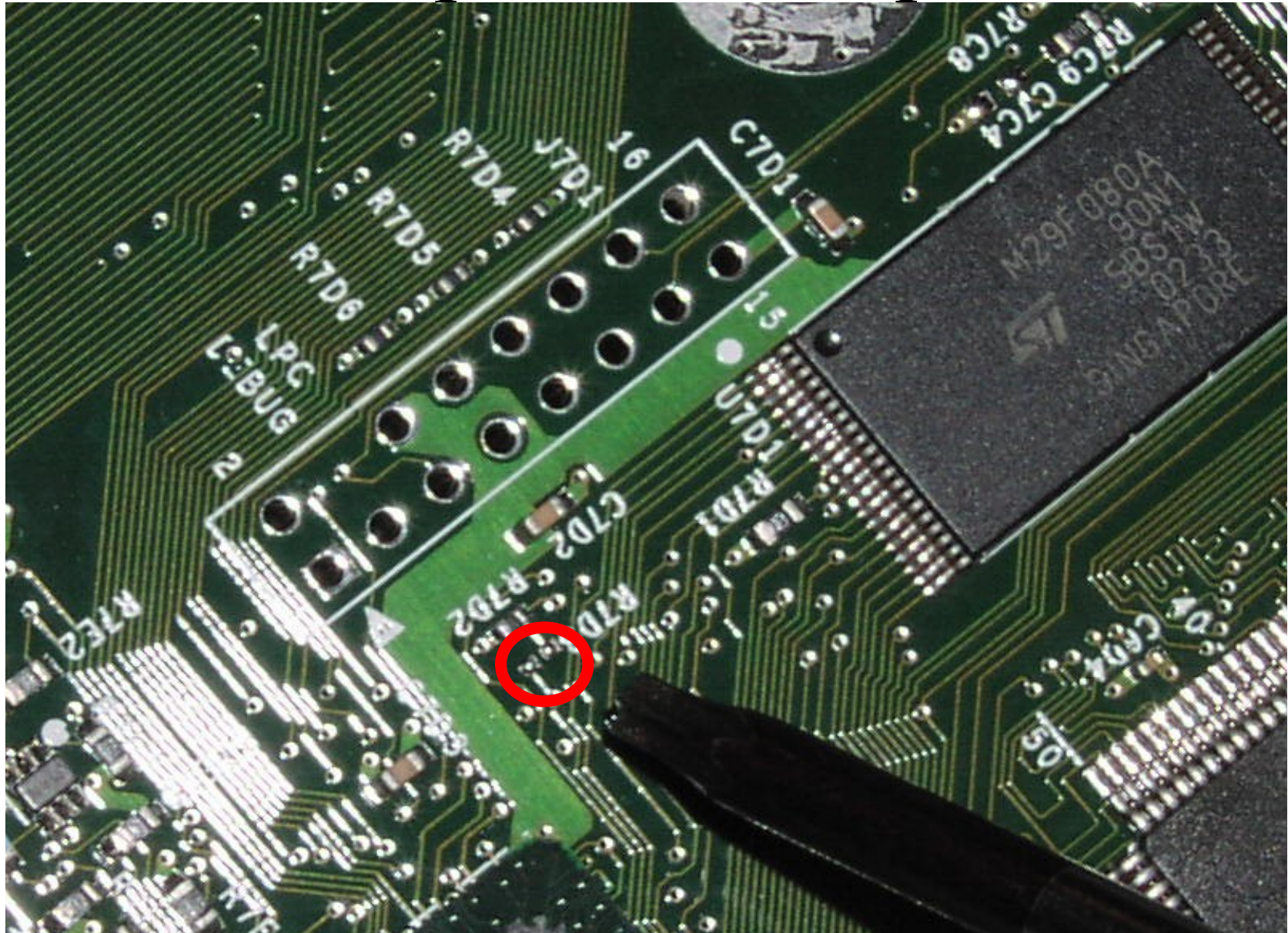# Remove the Drives (HDD and DVD)

take Motherboard out

- Remove all Screws (13) and Connectors (5)
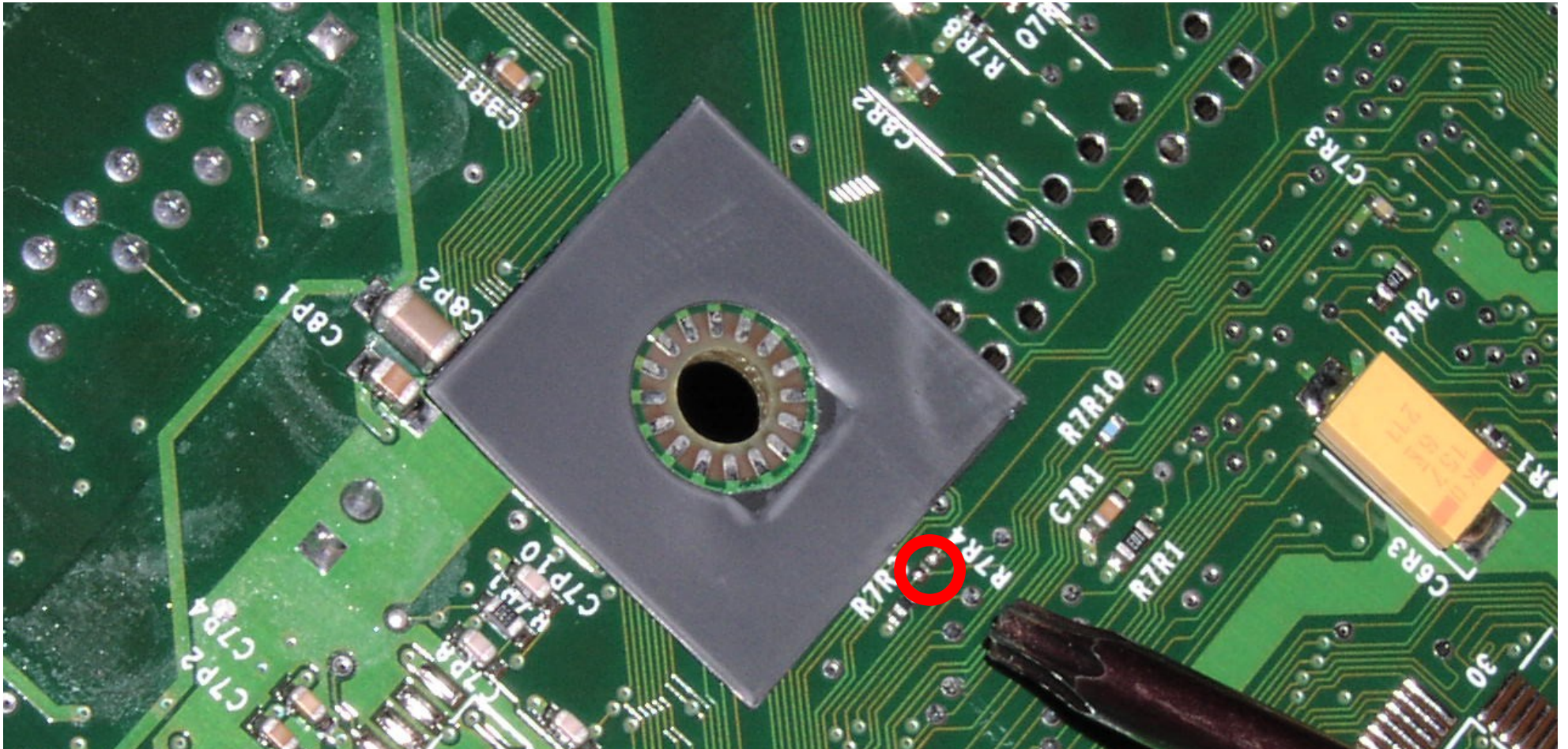- Take motherboard out

The Motherboard

Write protection topside
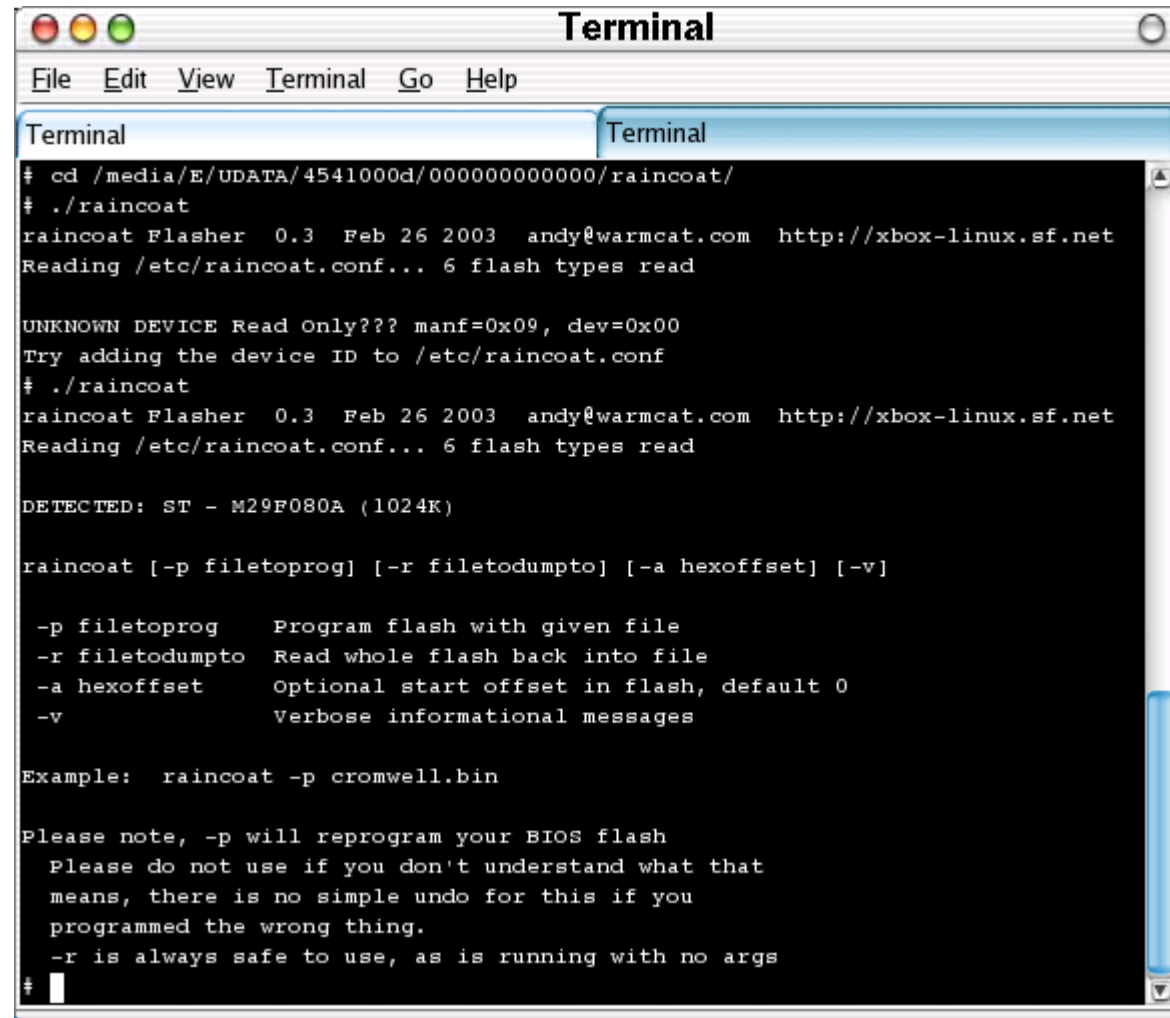

The solderpoints are crossed.

Solder points button

Samething on the button.

Installing Cromwell

- Start buggy Game

- load Linux-Sagegame

- Flashing with raincoat

- Watch the size of the TSOP

- reboot


```
# 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
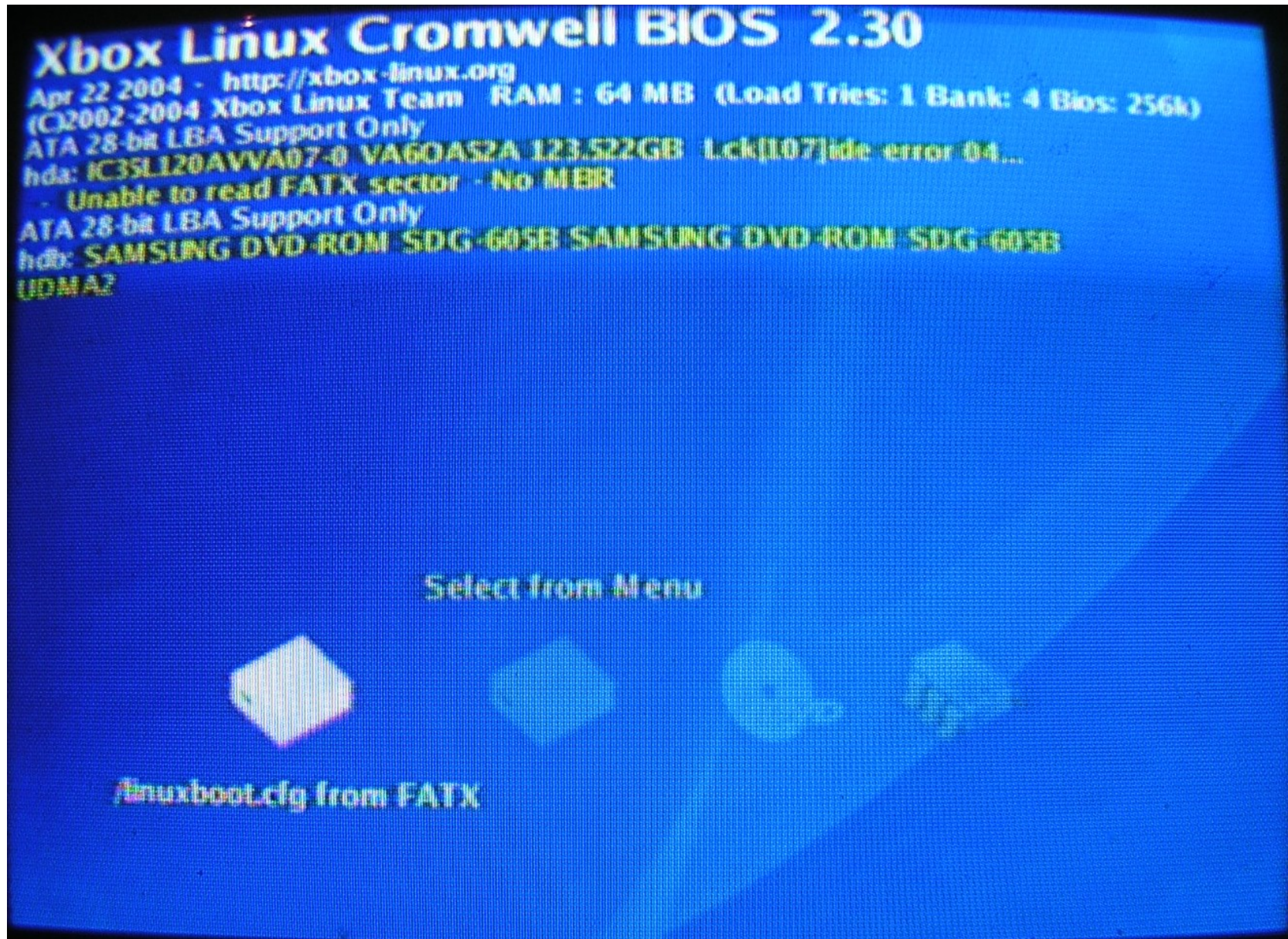
Software Hack

- Software-Hack (aka Mechinstaller)
- No opening the Xbox
- Warranty ??
- Uses a Error in the Microsoft Dash and the Game Mechassault
- New Version for Splinter Cell is in Beta-Status

Software Bug 2

- Dash:
  - Font-Bug
    - The Font files are not digital signed and there is a HEAP-Overflow in the Font-System
  - Audio-Bug
    - Integer-Overflow in the Index-File of the self ripped Audio-CDs-Database

Software Hacks Problems

- New Dashes are fixed
  - Microsoft Xbox-Live updates the Dash automatically
  - A downgrade to an older Version should be legal
- Newer Kernels (since 5713) down allow downgrading
  - Chose other installation Method
  - A new Hack is under Development (UDE/UDE2/UDX)

Installation

- Chose before loading by Mechinstaller
- Use the new Select menu by Splinter Cell
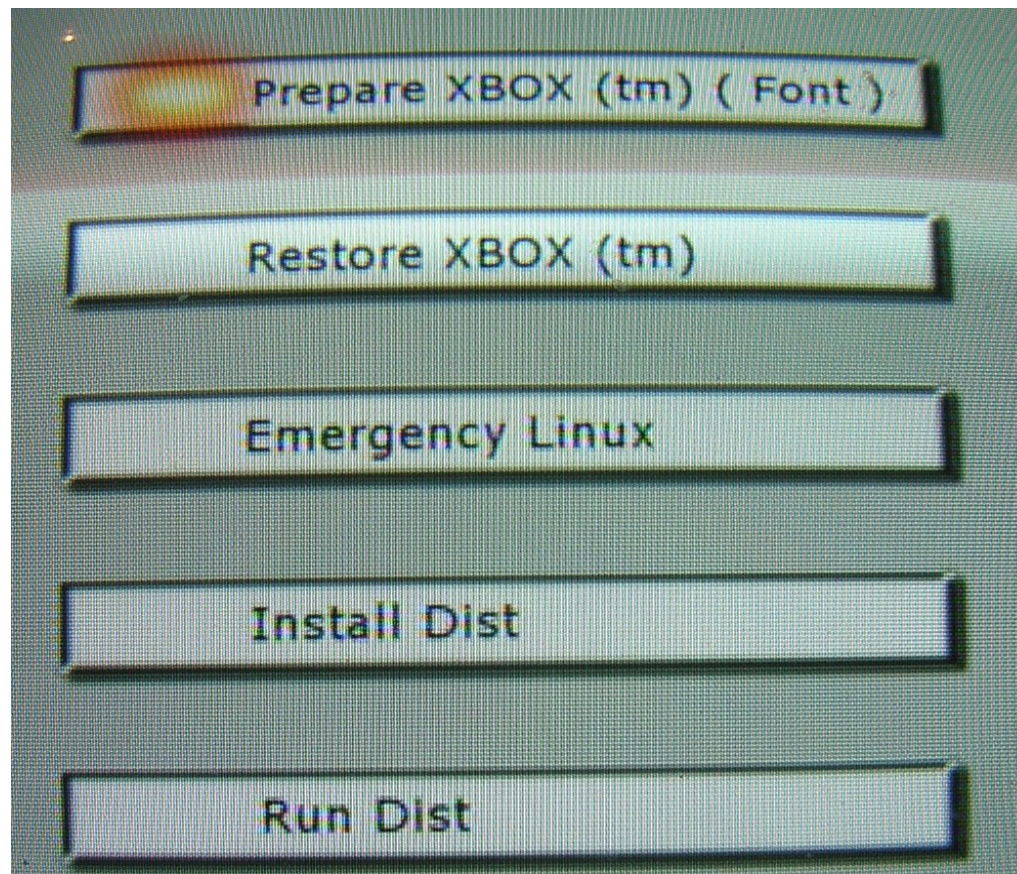
Before

before:
The new select menu

Xebian install

- CD install and boot

- open terminal

- su -

- XBOXLinuxInstall

  - Select the installation target

    - 1 Save game (e) partition
    - 2 unused Space with HDD bigger than 8 GB
    - 3 use HDD completely (not for Soft-Mod!)

The Xbox-Linux Project

- The official Website of the Xbox-Linux-Project:
  - http://www.xbox-linux.org/
  - Xbox-Linux Version database:
    - http://www.xbox-linux.org/docs/versionsentry.html
    - http://www.xbox-linux.org/docs/versionsdb.html
  - Chocolate-List: Users help users
    - http://www.xbox-linux.org/docs/usershelpusers.html
- Other interesting websites:
  - http://www.xbox-scene.com/
  - http://hackingthexbox.com/

Software for the Xbox

- **Xebian**
  - Debian for the Xbox
  - http://www.xbox-linux.org/debian/
- **freevo**
  - Frontend to watch Movies
- **Gentoox**
  - http://gentoox.shallax.com/
- **Cromwell** the Open-Source Xbox-Bios
  - http://www.xbox-linux.org/download.html

Building new Distributions

- TODO list for new Distributions
  - Kernel
  - i2c
  - alsa
  - X-Server

home-brew-Software (xbins)

- open source -Software some legal problems.

- needed the Microsoft-XDK for compilation

- The XDK is only available for official Xbox-Developers inside limited guideline

- **The Binaries are illegal.**

- Well known Examples: XBMC / XBMP

- **The Xbox-Linux-Project is not related at all with these Projects.**
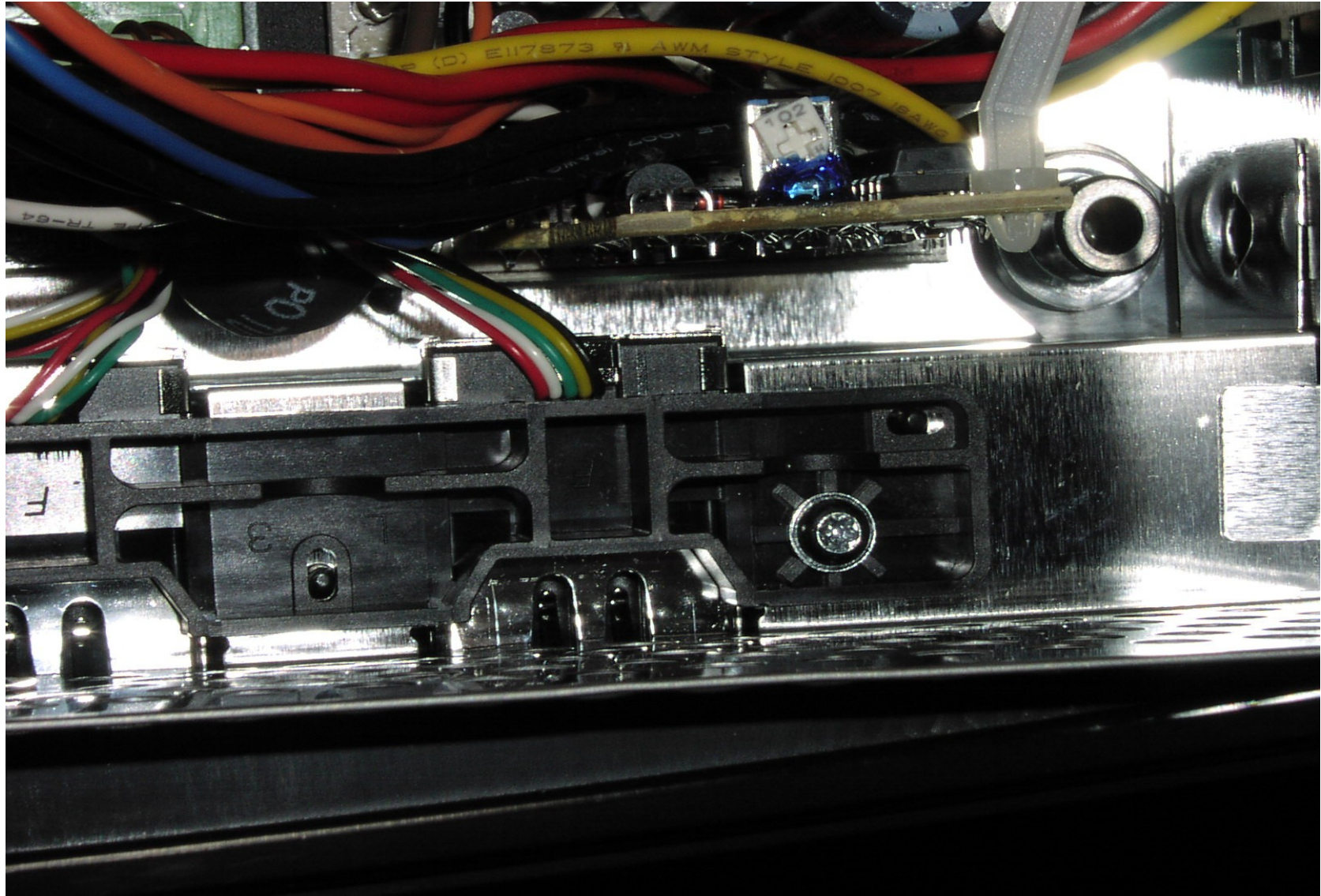
Thanks goes to:

- Michael Steil:
  - Who started the Xbox-Linux-project
- Marvin (Lug-AL)
  - For his slide as a starting point
- The whole Xbox-Linux-Team
  - otherwise I had nothing to play with
- and Microsoft for generously sponsoring the Hardware :-)
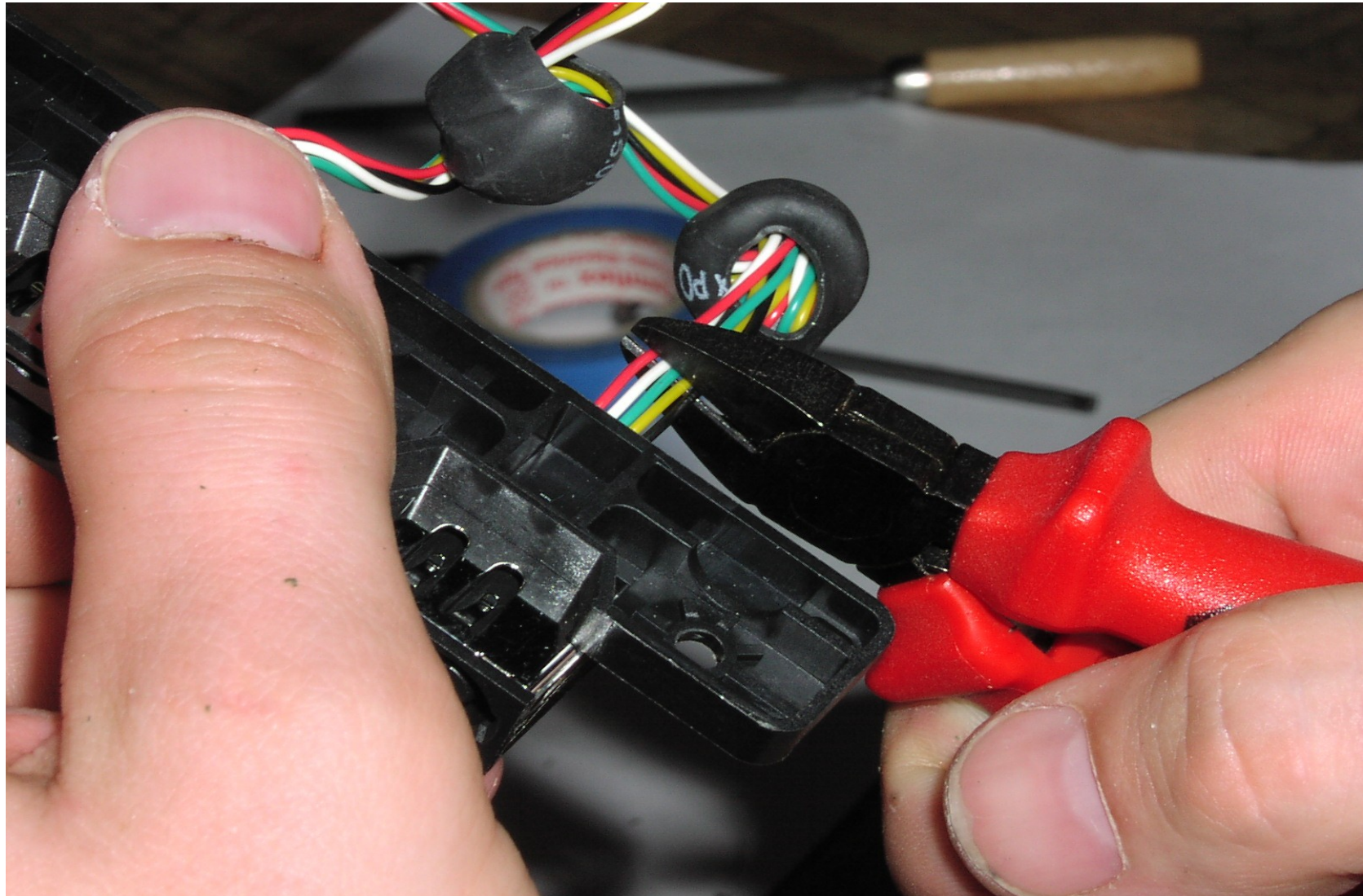
Appendix:

USB-Modding

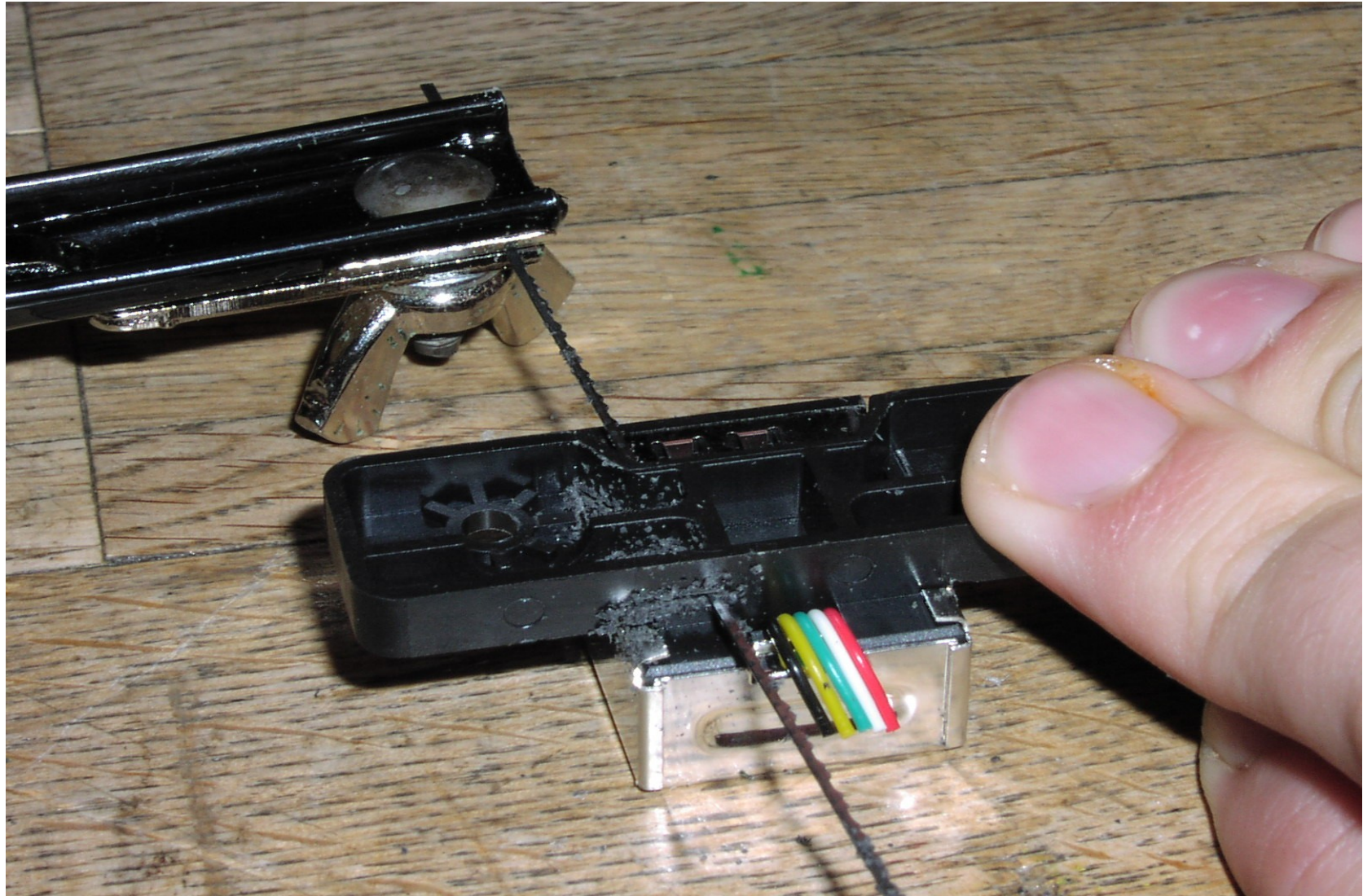# Replaces the right USB-Connector

Remove the right bracket
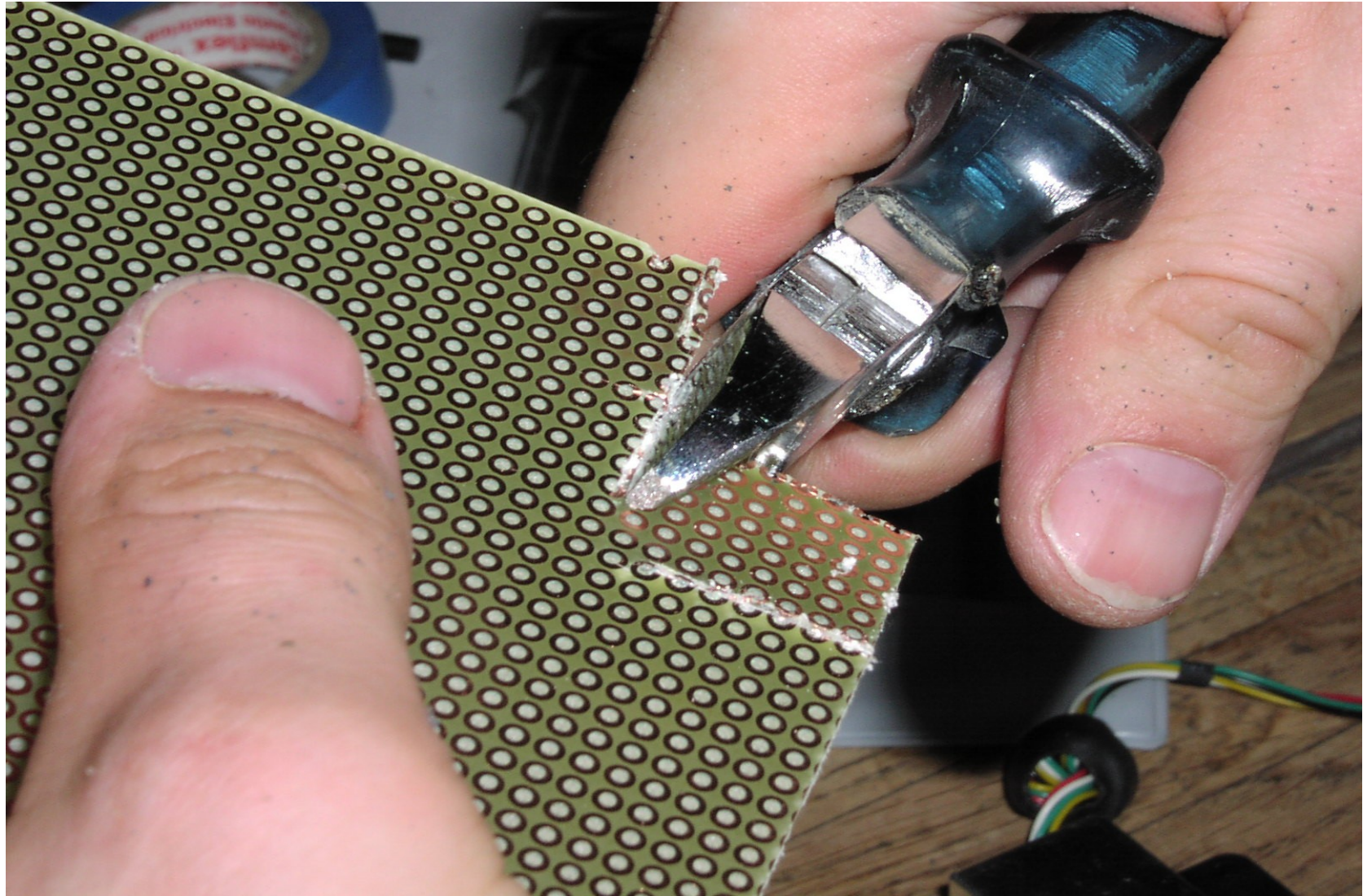
Disconnect the USB-Connector

Cut the cabel nearby the female USB
leave some room if you wan´t to connect the female USB to your PC

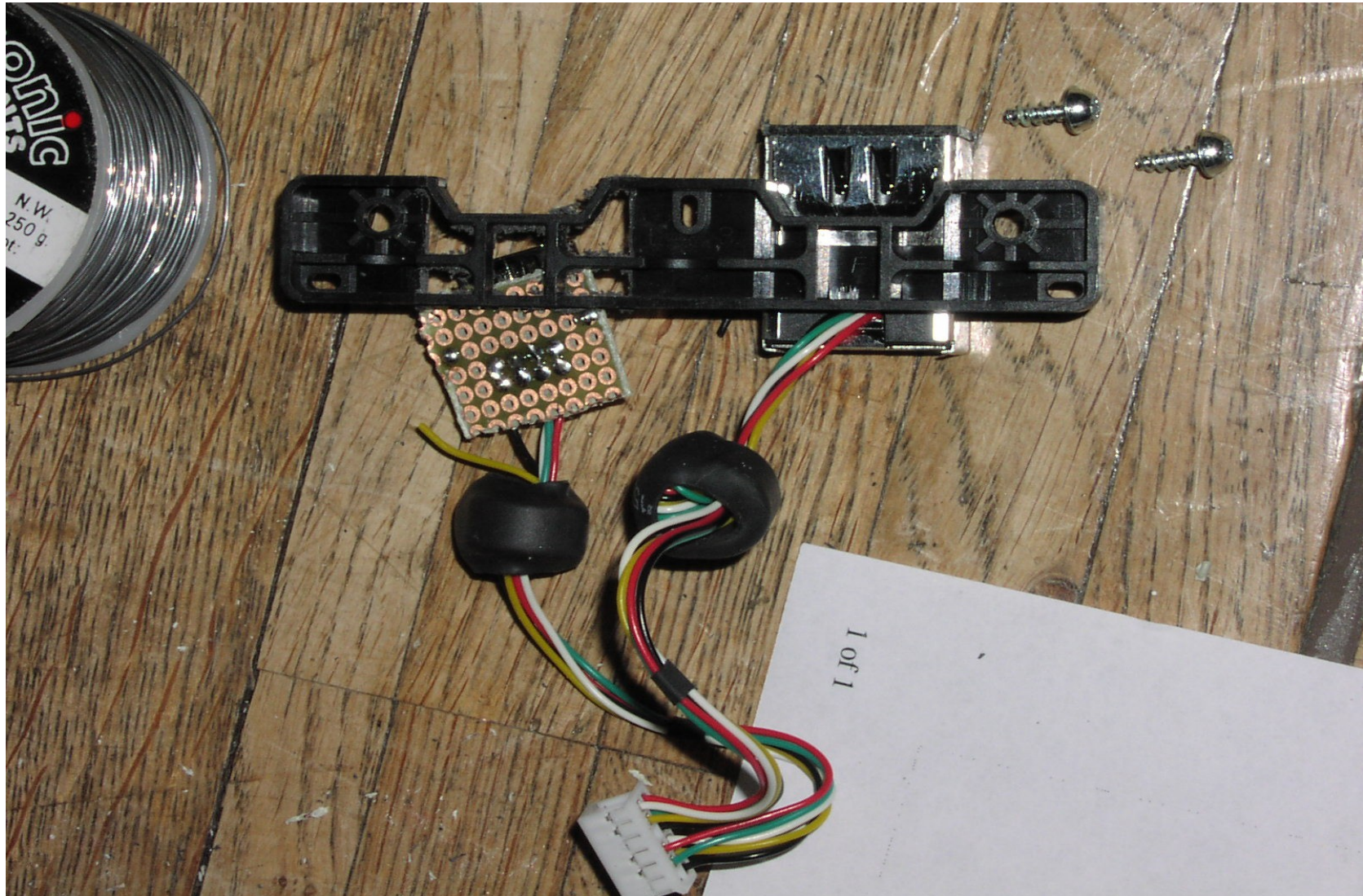# Remove the Connector

Cut the old one out

Building a new bracket

Cut a small piece circutboard

Building a bracket for the female USB

Solder the female USB to the circutboard

connect the cable with the Help of the colorcoding.
Details see next side.

Connect the female USB

front view

1 2 3 4

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

fixating the female USB

A little bit of hot glue and every things adherence
Try to fit in befor glueing

Everything is finished