

Hard Disk Heart Attack

Felix Bauer

IT-Sicherheitsmensch

felix-tuebix@ai4me.de

11.06.2016

Disclaimer

Das folgende Material enthält Szenen brutaler Gewalt gegenüber Festplatten



Inhalt

- Hard Disks
- Seitenkanäle
- Werkzeuge
- Analyse
- Hacking
- Angriffe
- Demos

Hard Disks

Gibt's in unterschiedlichen Größen, Formen, Kapazitäten als Modelle von Herstellern.



**\$3398
10MB**

THE HARD DISK YOU'VE BEEN WAITING FOR

XCOMP introduces a complete micro-size disk subsystem with more ...

- MORE STORAGE
- MORE SPEED
- MORE VALUE
- MORE SUPPORT

S100 users ... The XCOMP subsystem is now available with 10 megabytes of storage; 5 megabytes also available at \$2,698.00. Compare the price and features of any other 5½" inch — or even 8" inch system, and you'll agree that XCOMP's value is unbeatable.

OUTPERFORMS OTHER HARD DISKS
 Floppy disk and larger, more expensive hard disks are no match for this powerful little system. More data is available on every track: 64K on 10MB and 32K on 5MB. Faster seek time too — an average of 70MS. It provides solid performance anywhere with only 20 watts of power. Data is protected in the sealed enclosure and the landing zone for heads provides another margin of safety. The optional power board plugs directly into the S100 bus and provides power for the drive.

FAST CONTROLLER
 The XCOMP controller is the key to this system's high efficiency operation. Speed-up features include interleaving with cache table lookup, block-deblock with controller buffer, and read lookahead. OEM world-wide have already proven the outstanding performance of the XCOMP controller.

MORE SOFTWARE
 Included with the system is software for testing, formating, I/O drivers for CP/M®, plus an automatic driver for MP/M® and Oasis® are also available. The sophisticated formating program designs alternate sectors for any weak sectors detected during formating, assuring the lowest possible error rate — at least ten times better than floppies.

WARRANTY
 The system has a full one-year warranty on parts and workmanship.

ALSO AVAILABLE FROM XCOMP

- General Purpose controllers (8 bit interface), with easy interface to microprocessor-based systems.
- GP controller adapter that plugs directly into most Z80 computers.
- ST/R GP controller for the SMB and 10MB drive above, and ST50B type interface.
- SG/R GP controller for SA1000 interface.
- SMA, SG/S, and SM/S, same as above, for the S100 bus.

Quantity discounts available. Distributor, Dealer, and OEM inquiries invited.
 See your local Dealer, or call:
XCOMP, Inc.
 7566 Trade Street
 San Diego, CA 92121
 Tel: (714) 471-8730
 Telex: 152786

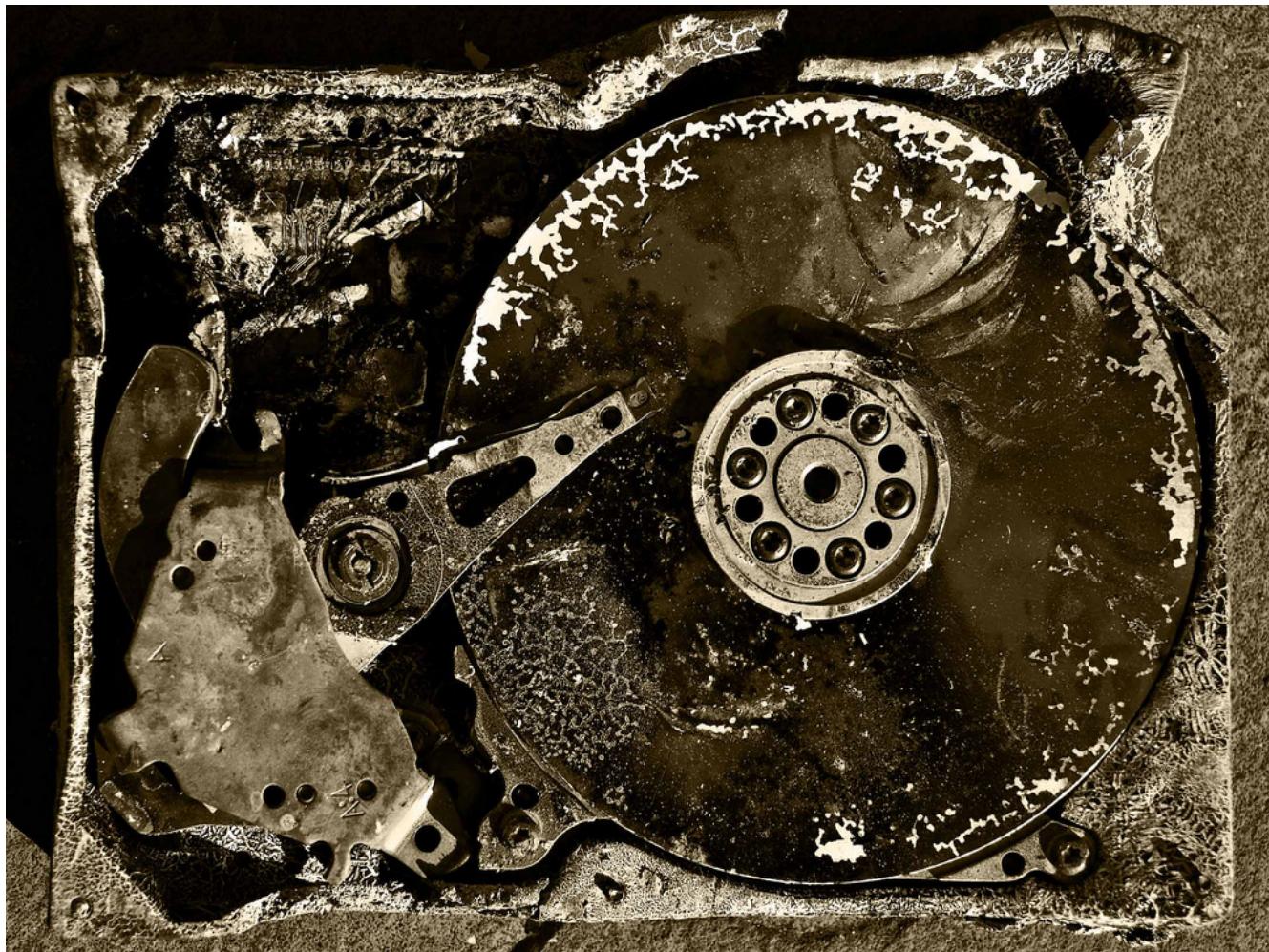
Circle 405 on Inquiry card.

XCOMP

www.coolpicturegallery.net

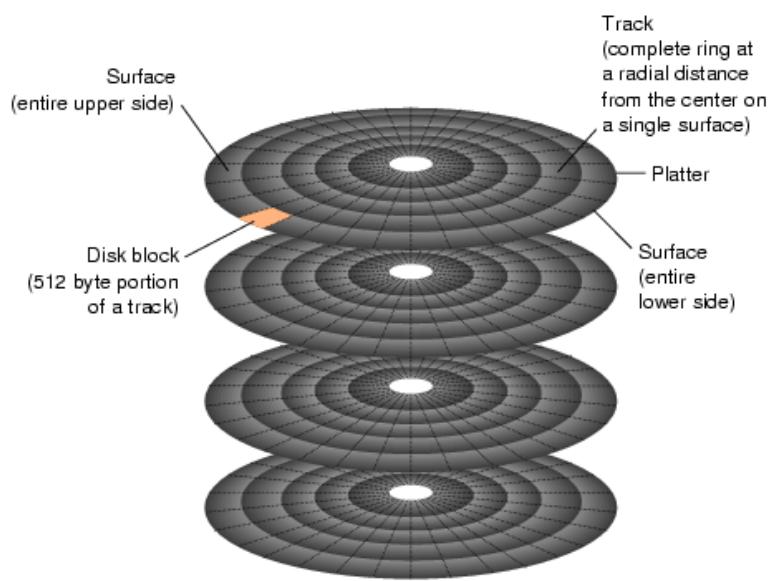






davidrvetter @ flickr.com

Ein Block Device



techpubs.sgi.com

Aber es braucht mehr

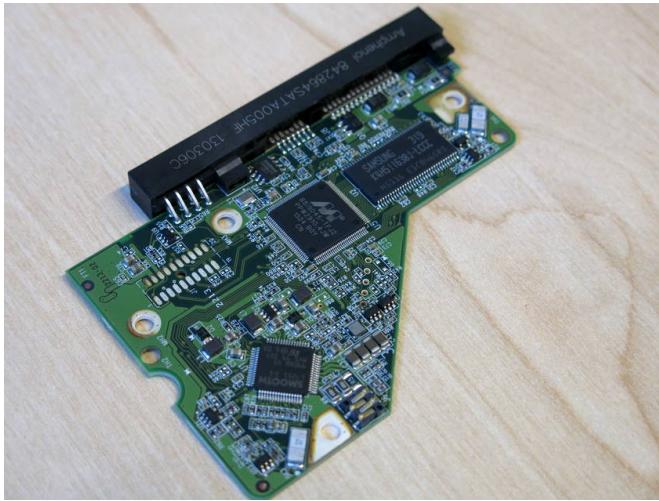
- Partitionen
- Dateisysteme
- ...



www.opensourceforu.com

Aber Moment !

Da ist mindestens ein Prozessor, Speicher und ziemlich viel Plattspeicher



Also ist es eher sowas?



Vielleicht nicht ganz

- es ist closed source
- keine öffentliche Dokumentation
- wenig Informationen verfügbar

Man findet da:

- +/- 400 MHz controller (multicore)
- 64 MB RAM
- 256 KB ROM
- 1.5 bis 6 Gbit SATA interface

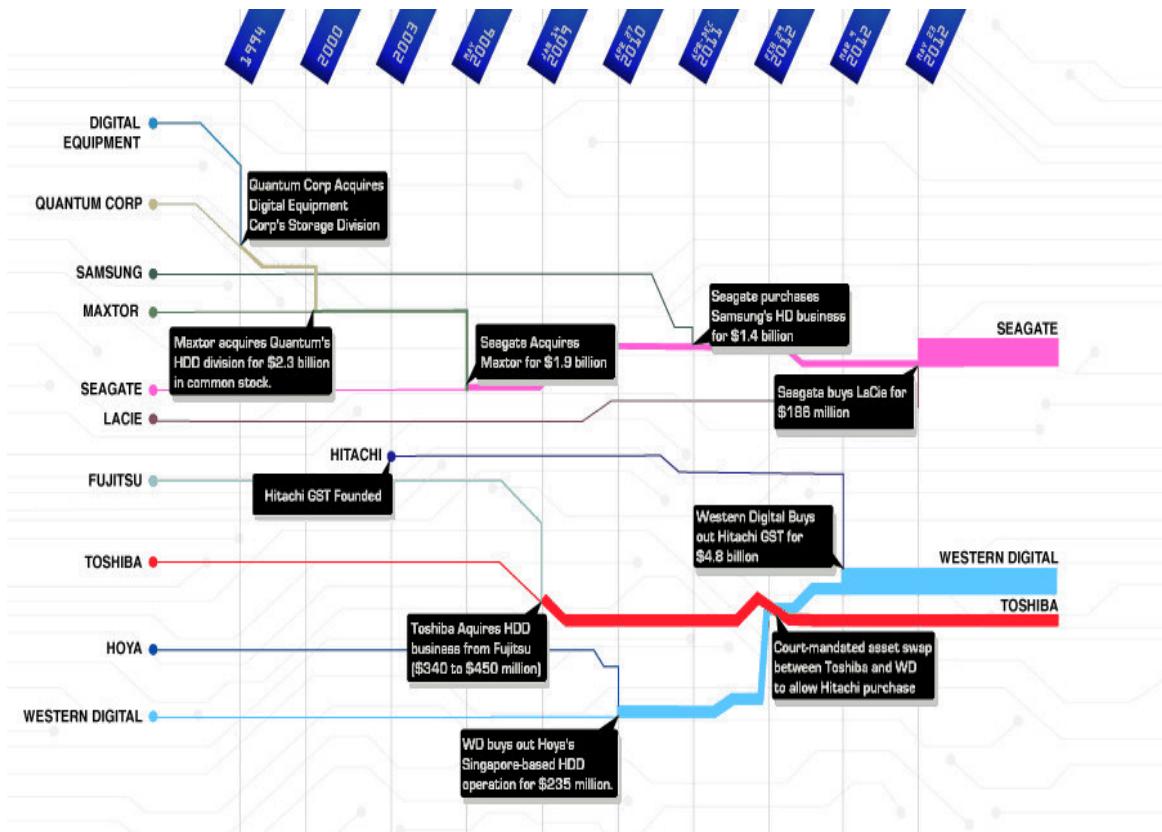
Außerdem kennt man:

- Software Updates für Festplatten
- Herstellerspezifische ATA Kommandos
- Versteckte Bereiche
- und weitere Anschlüsse

Mal schauen was man damit anstellen können!







Seitenkanäle

- Geräusche
- Wärme
- Energieverbrauch
- Elektromagnetische Abstrahlung

Geräusch



Wärme

- die Fingerspitze ist ein gutes Messgerät
- wird doof über 60°C
- keine Infrarotkamera
- ENDE

Energieverbrauch



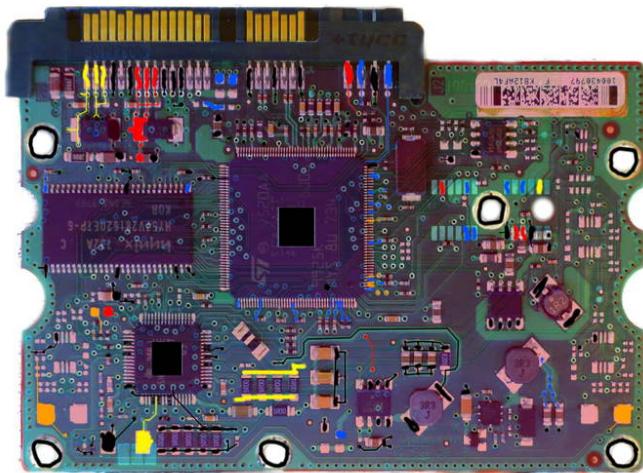
NIEMALS eine laufende Festplatte schütteln!

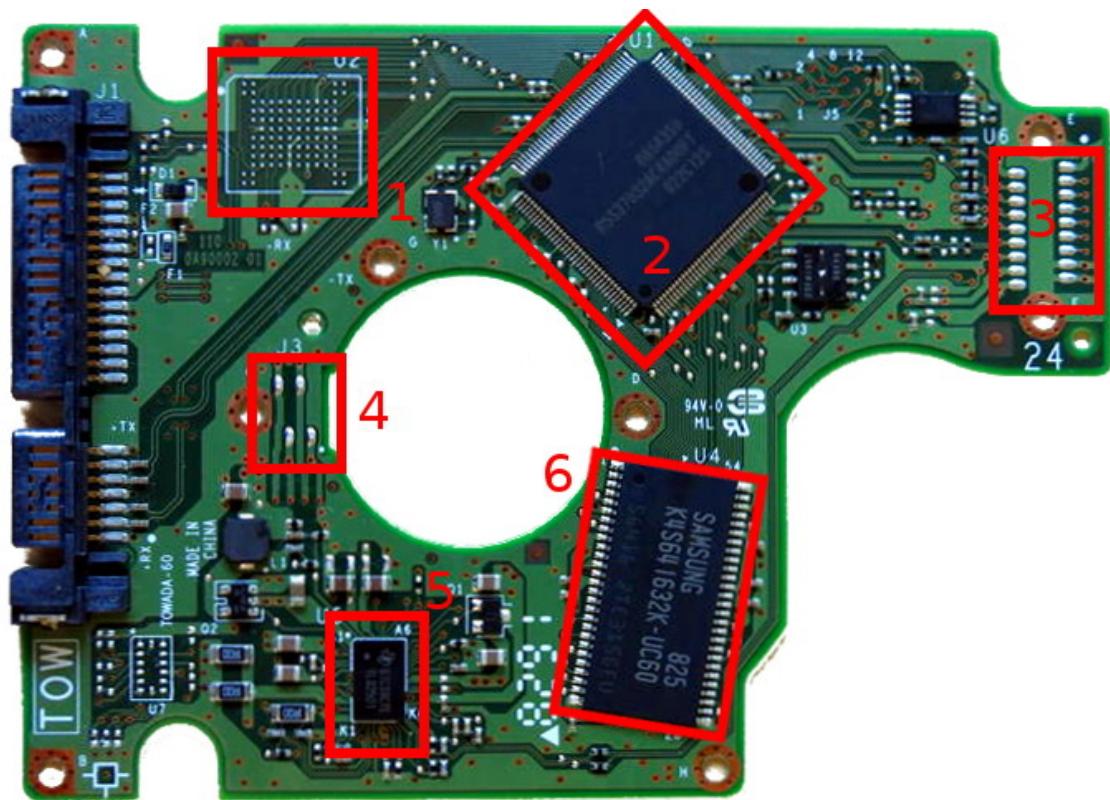
aber wenn man's tut verbraucht sie mehr Strom

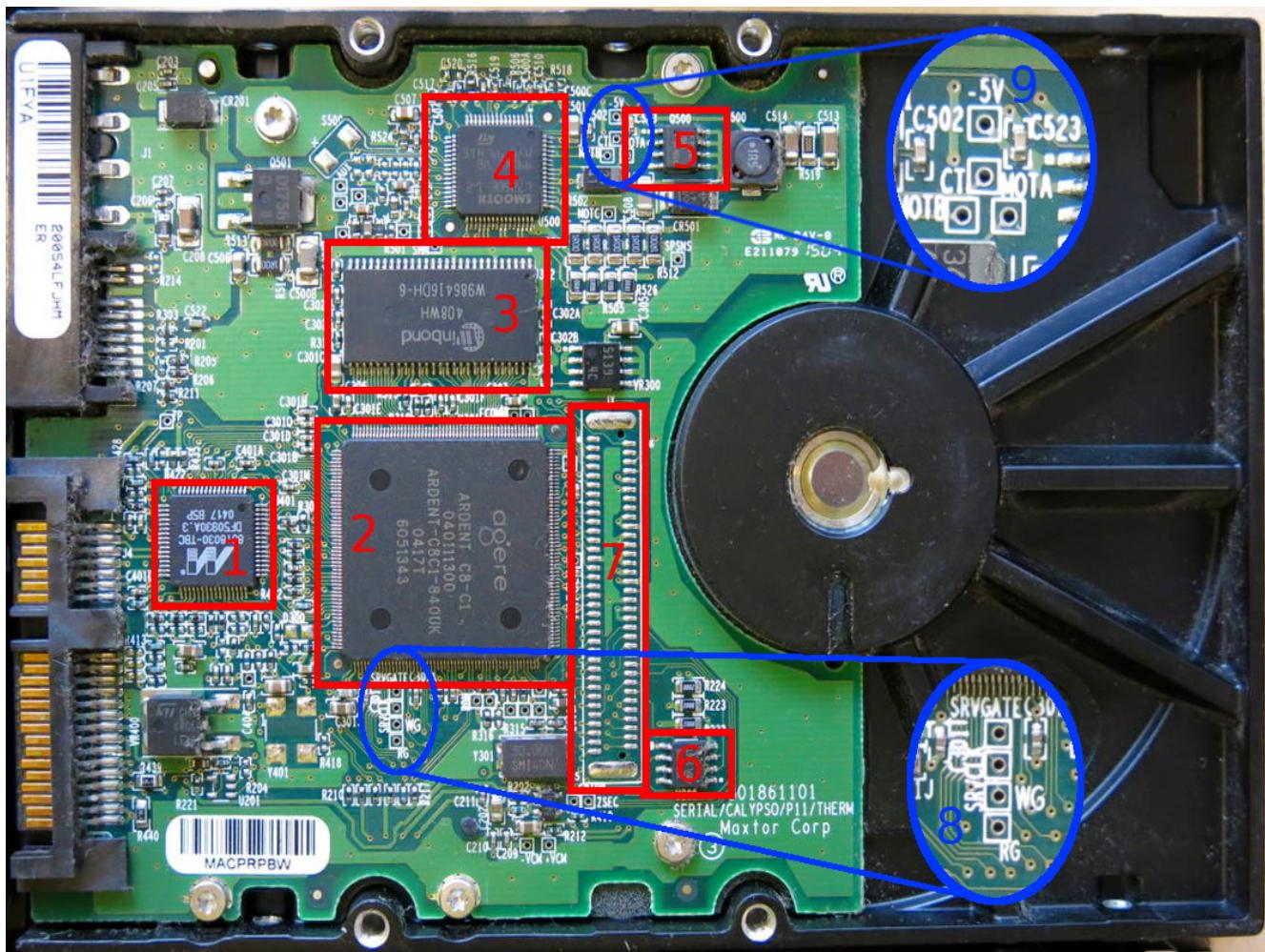
Elektromagnetische Abstrahlung

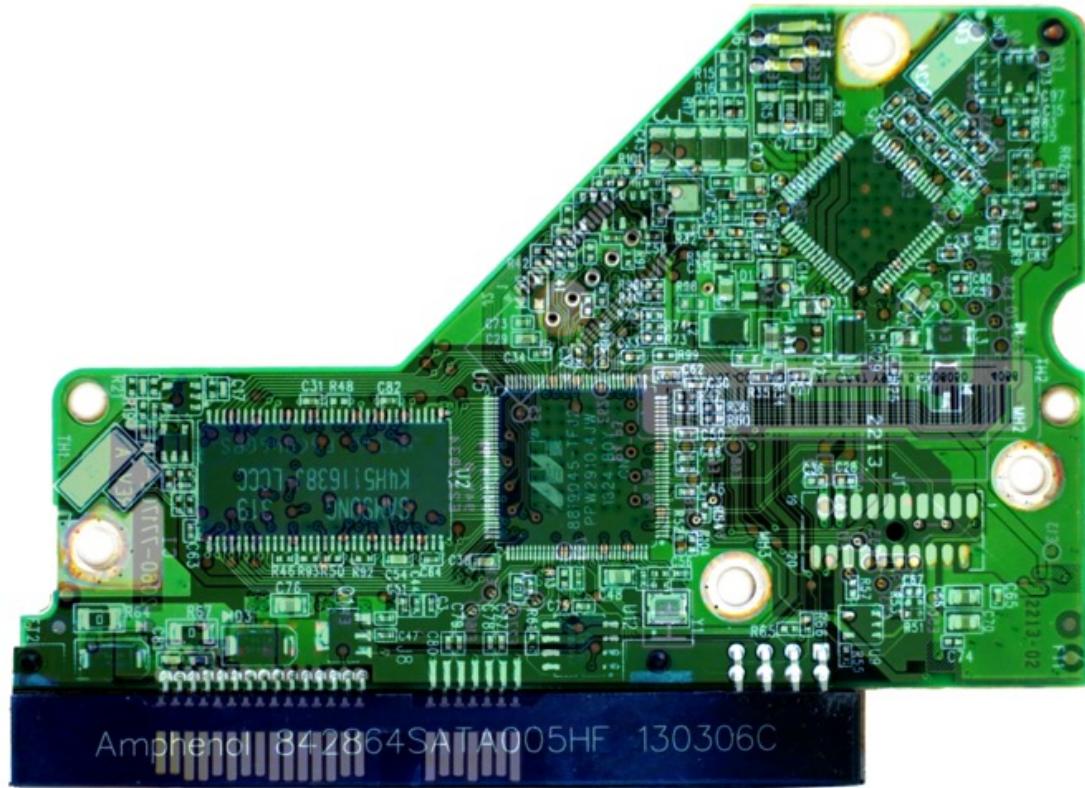


Schauen wir uns die Elektronik an





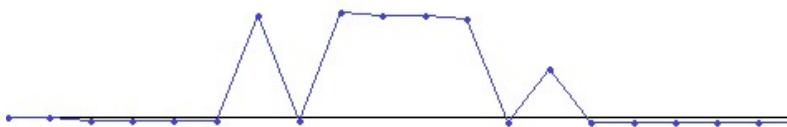
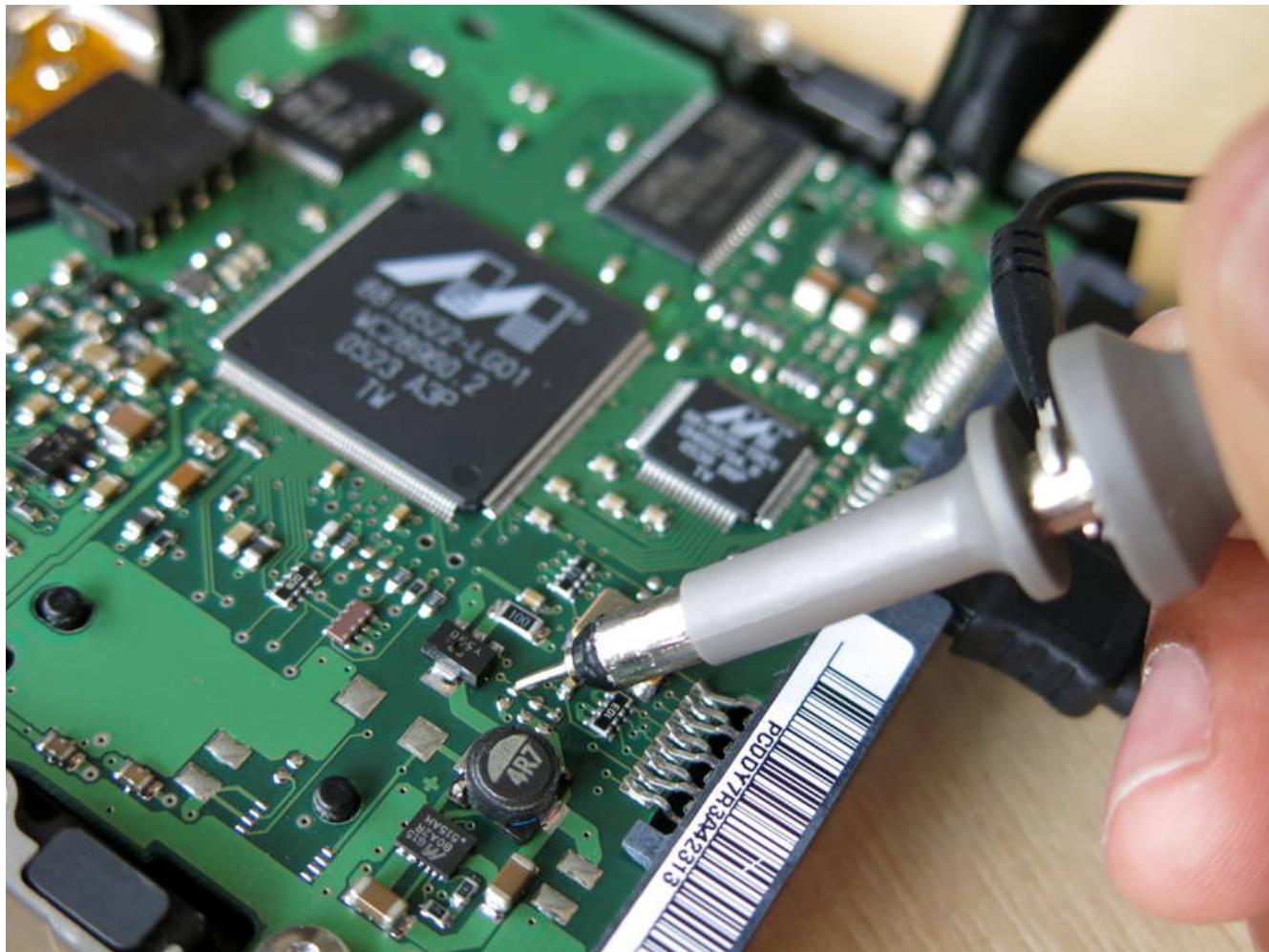




Ein Oszilloskop muss her



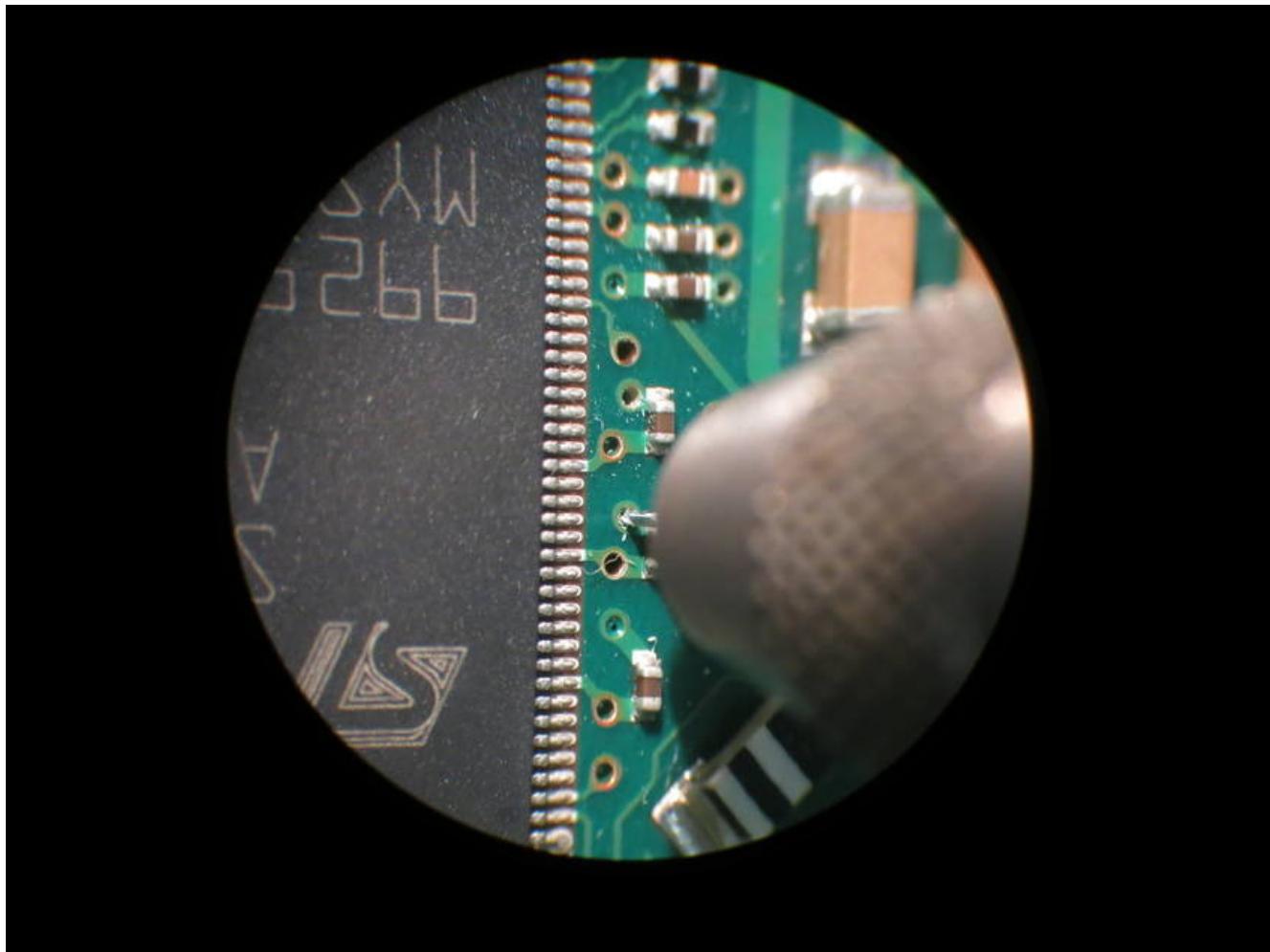
by Paul Marsh



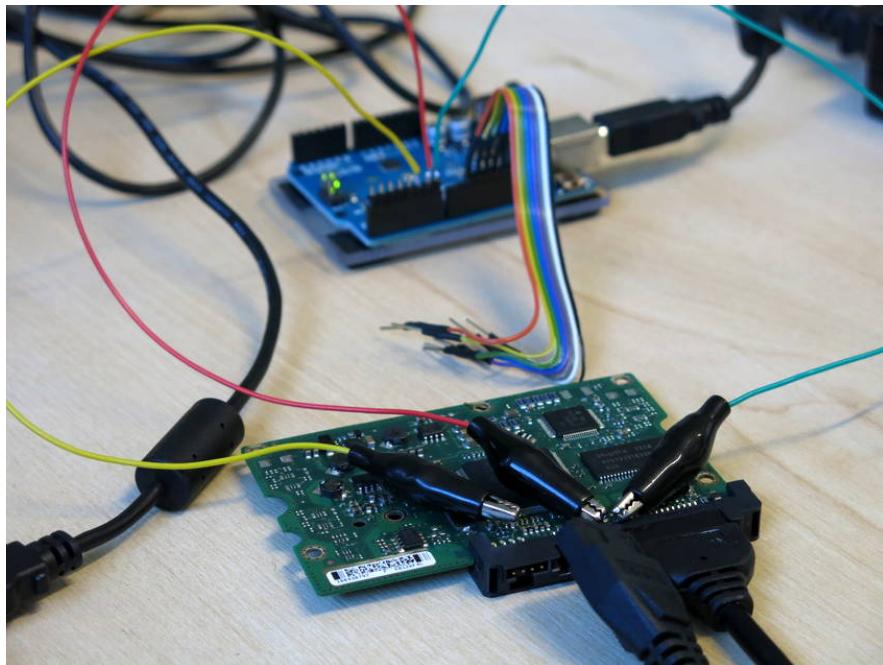
0 0 0 0 0 0 0 1 0 1 1 1 0 1 0 0 0 0 0
- - - - S 0 1 1 1 1 0 1 S - - -

011 1101 (*-1)
100 0010
0x42
B

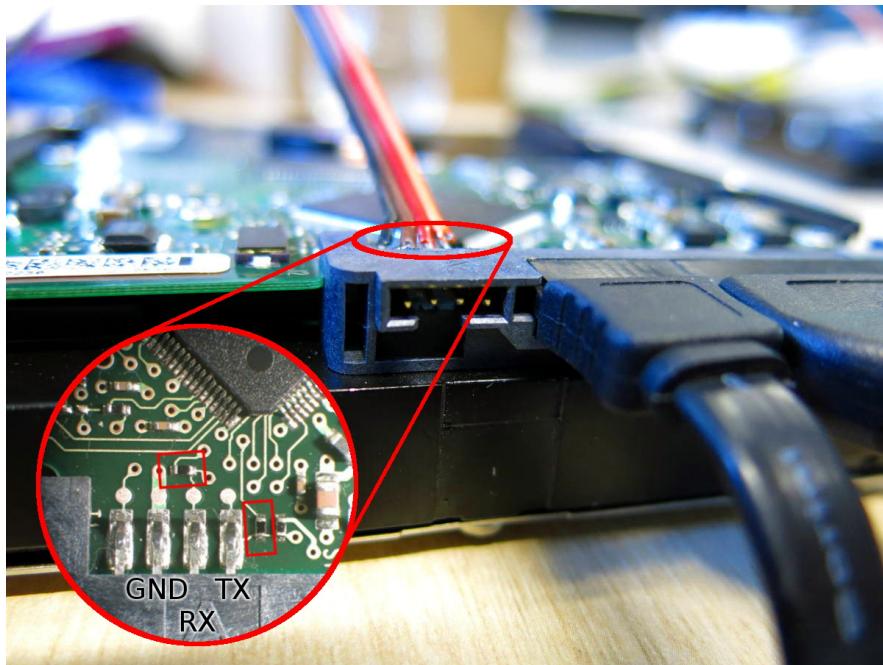
Und jetzt mehr und parallel



Arduino und RS232enum



YAY



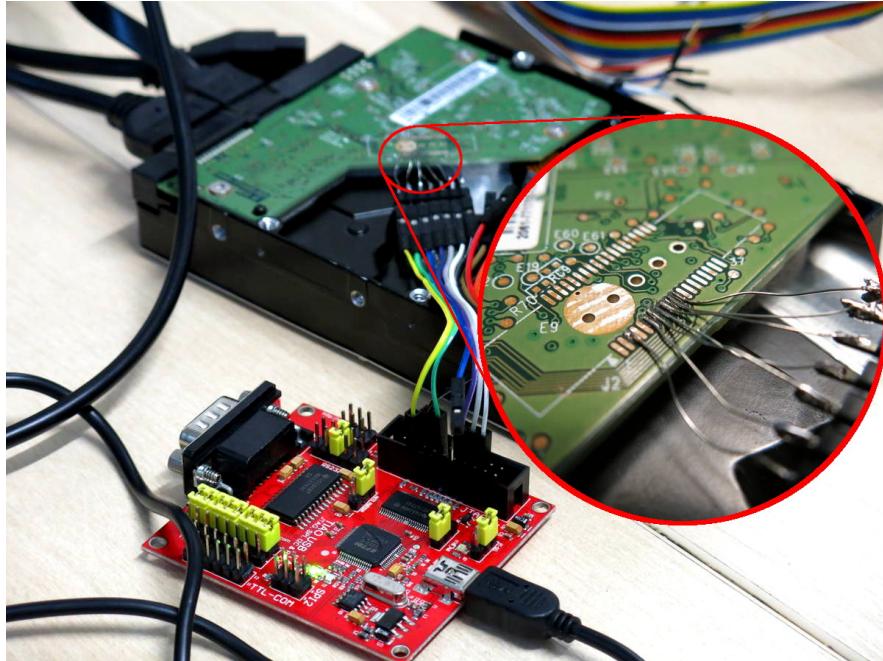
Terminal Mode

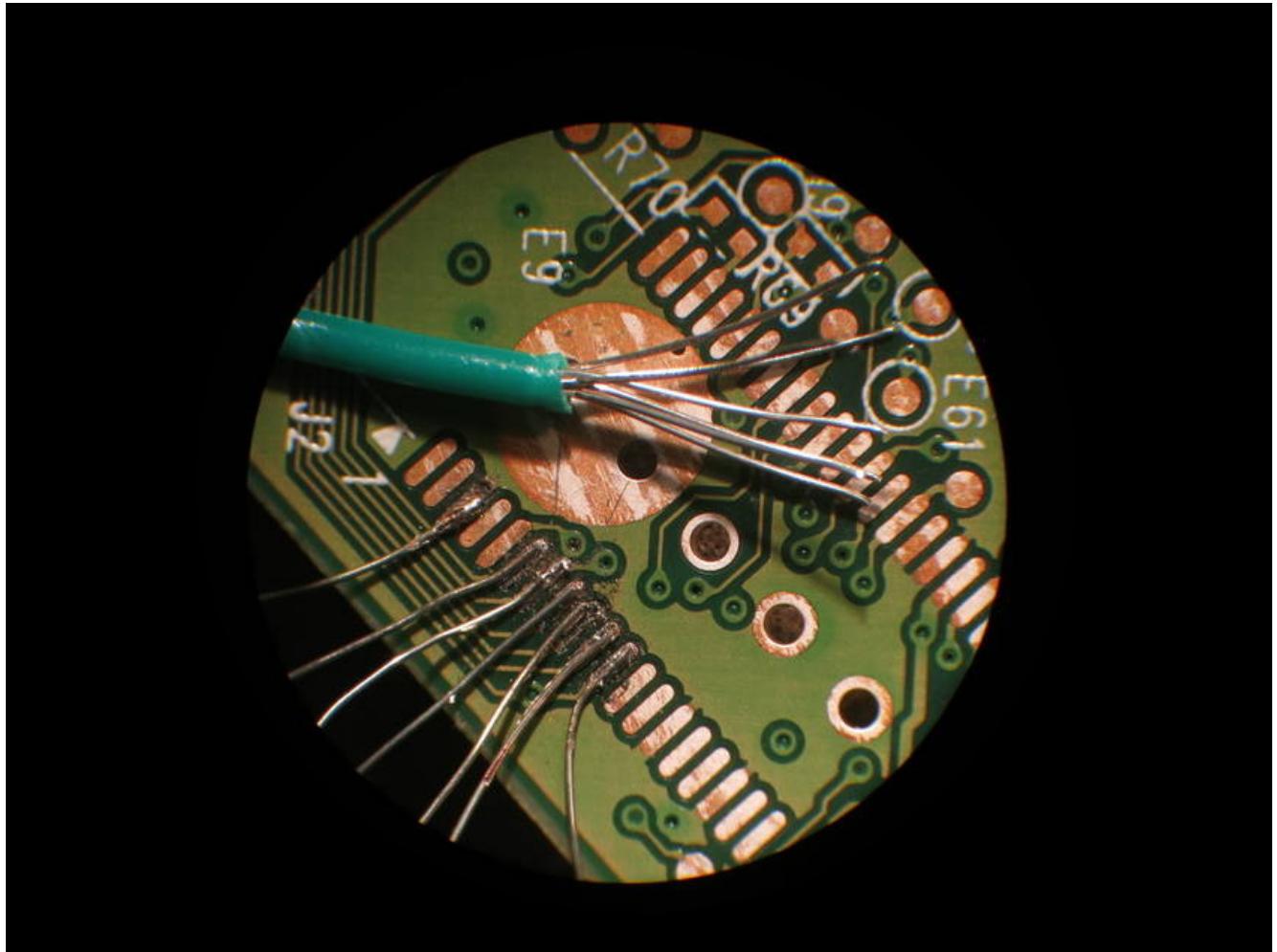
```
# boot up message  
Interface task reset
```

```
4096k x 16 buffer detected  
TONKA - 1 Disk M-27 03-30-05 11:42
```

```
Buzz - Head Mask FFFF - Switch to full int.  
Spin Ready  
3.03 05-06-05 15:43  
(P)(H)SATA Reset  
SATA core D1 Yuma 6192 No LED Native mode  
  
# ctrl+z is used as the wakeup message  
# it gives F> for a faulty/missing disk  
T>
```

Wie siehts mit JTAG aus?

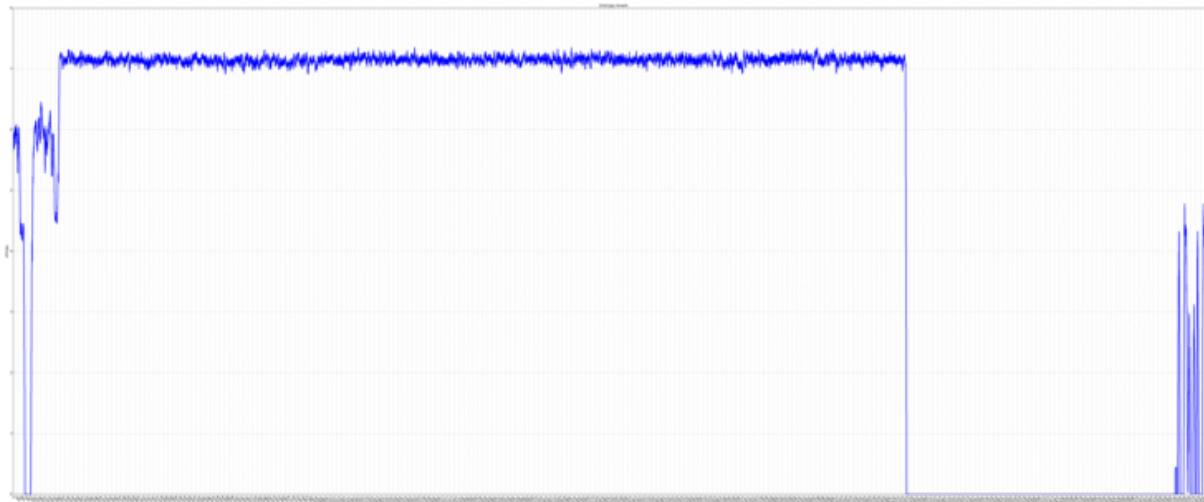




Was kommt als Nächstes?

- openOCD
- debugging
- firmware dump

Die Firmware



Und jetzt mehr böse Dinge



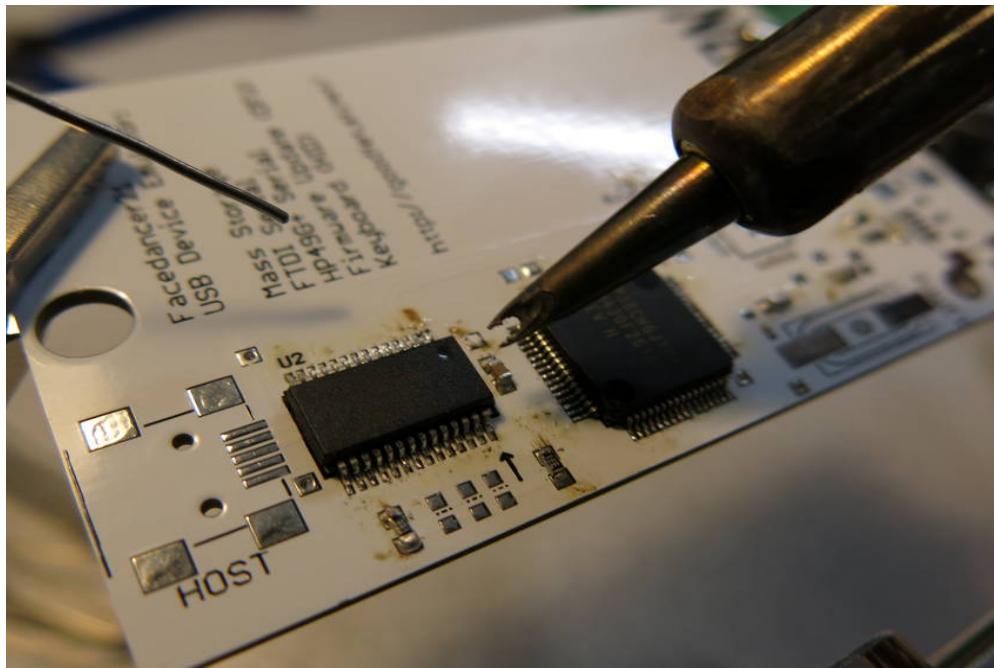
Sachen verstecken



POC mit facedancer



Sauron's Lötkolben



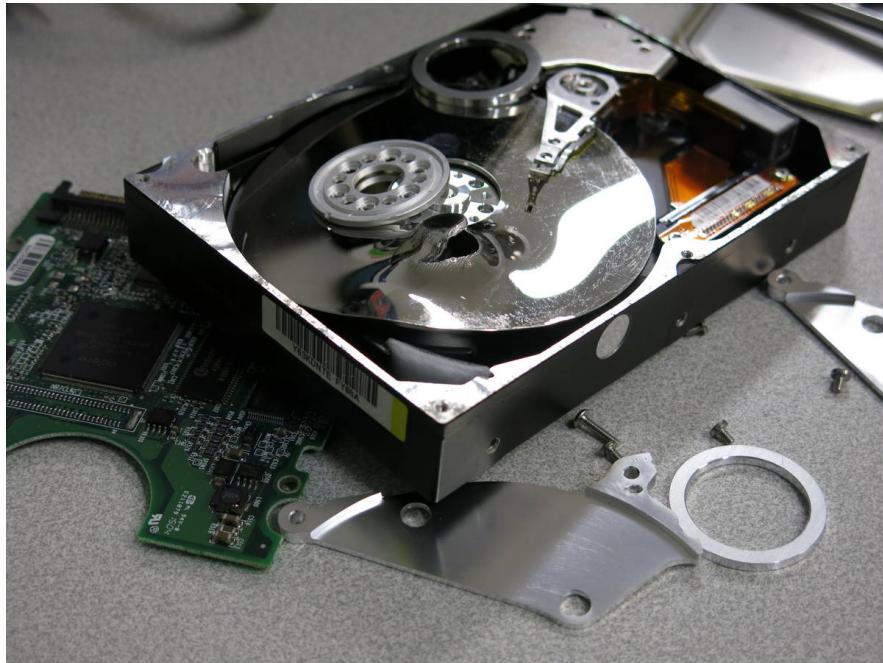
Was geht mit dem Facedancer?

- funktioniert
- schön und funkeln
- zum Tastatur emulieren
- oder als Massenspeicher
- aber leider VIEL zu langsam

Zum Glück gibt es FUSE

- scriptbar in Python
- schön und einfach
- schnell und flexibel
- mächtig genug alles zu zeigen

DEMO



Universeller Hack

- Kommando zum Extrahieren/Schreiben eines Blocks
- Webserver
- Datenbank
- Disk
- Datenbank
- Webserver

Resultat



- versuch neue Sachen
- es gibt viel was man tun kann
- Hardware macht spaß
- Lötkolben sind heiß



ENDE

Dokumentation und Folien sind zu finden unter:

<https://ai4me.de/msc>

Vielen Dank!

Felix Bauer

`felix-tuebix@ai4me.de`
GPG: 7389D488
Threema: K7H2MW5N
Signal: 0160-1256636
054001253c3bda1c5581db04bd7251d2f
8a14e8870a5474eba7a178d57c38c371f